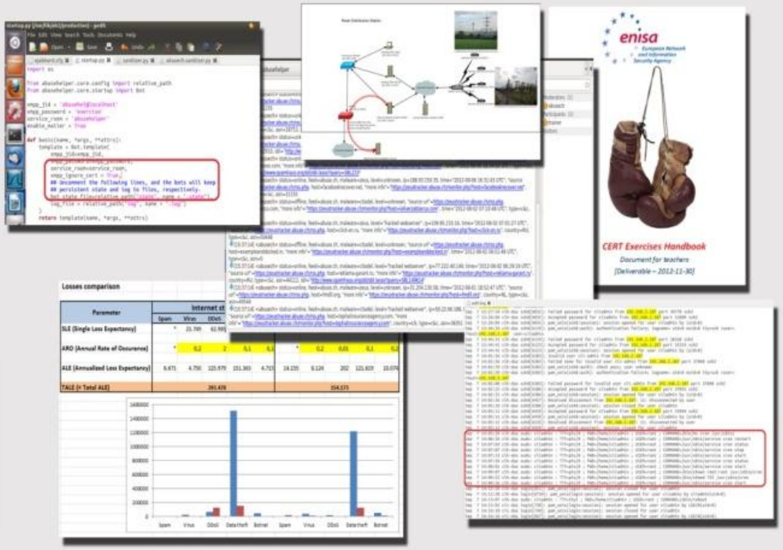
Technical trainings for CERTs

ENISA Supporting the CERT community

Supporting the CERT community

ENISA Annual **CERT workshops**
focus on national and governmental CERTs
preparedness and response capabilities

New Exercise material 2012
- Technical trainings for CERTs
- Handbook for teachers
- Toolset for students
- SW ready to use from our website:
www.enisa.europa.eu/activities/cert/support



FIRST – to improve CERT capabilities

TRANSITS framework:
support the basic and
advanced training
courses for CERTs

Cross-communities Support

INTERPOL
Atomic exercise 2012

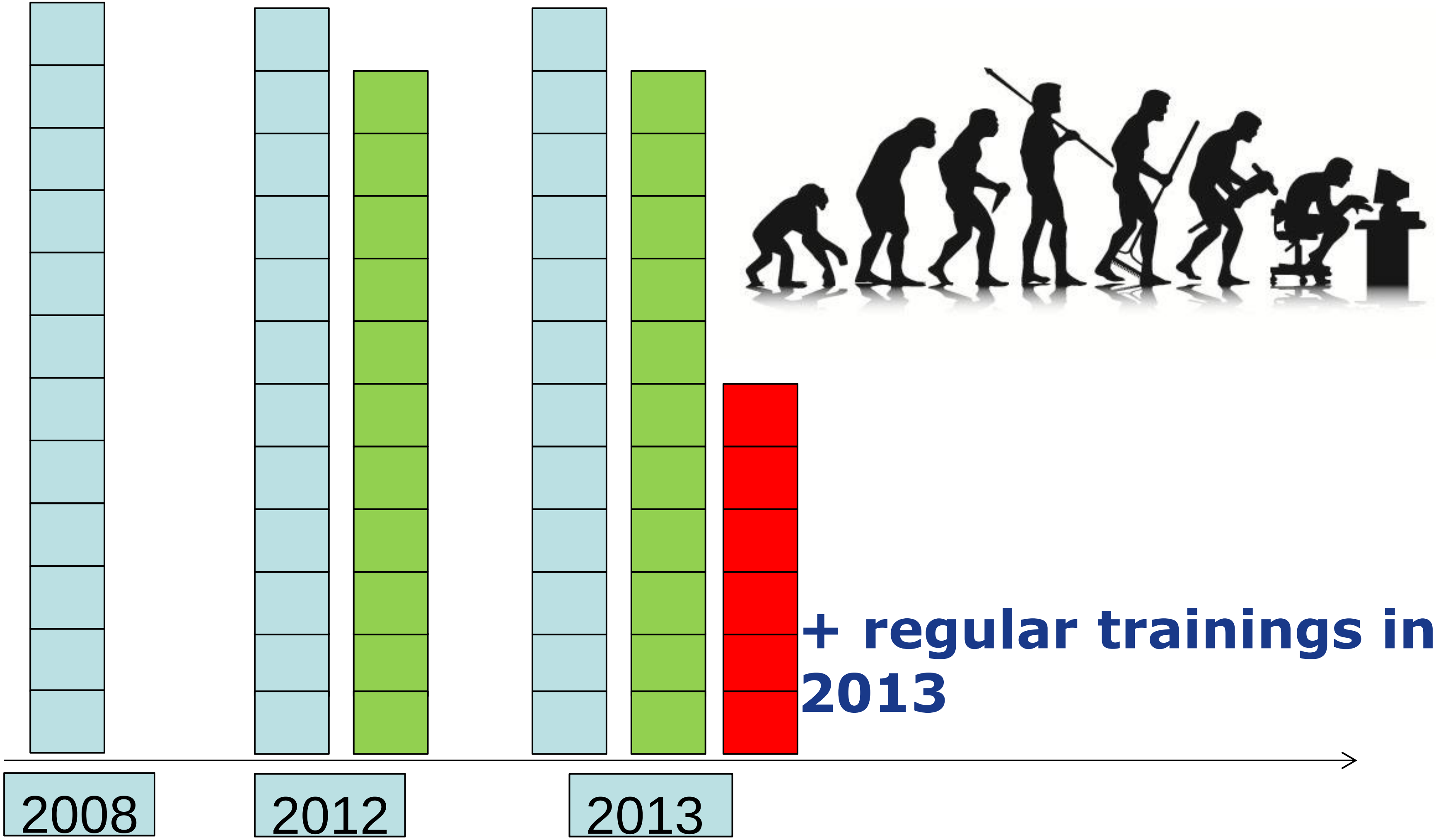
ENISA-EUROPOL joint workshop:
“Addressing NIS aspects of cybercrime”

EU FI-ISAC exercise
for CERTs, LEA and
banks

CEPOL courses:
(operational security unit
supports cyber work-
shops for police)

https://www.enisa.europa.eu/activities/cert

ENISA CERT training

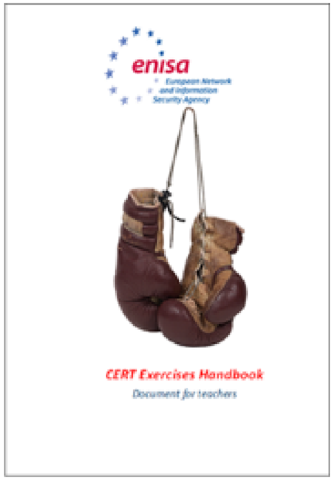


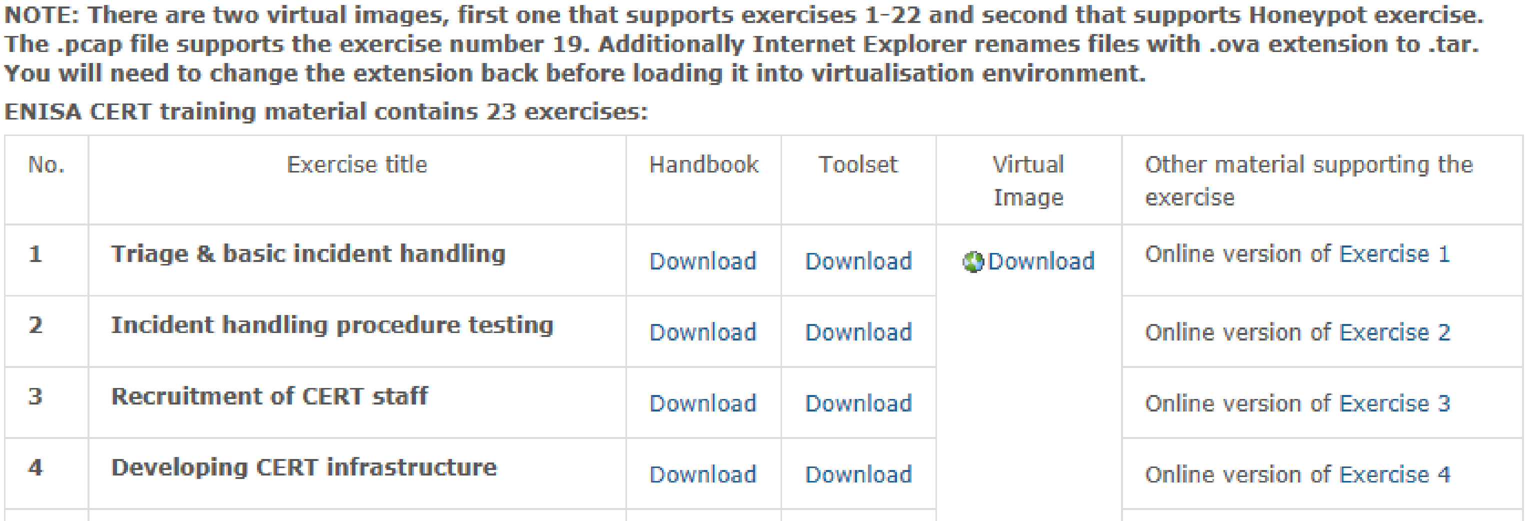
+ regular trainings in 2013

Content regularly updated and renewed with the help of community

- The creation process of material involves community
- The target audiences feedback will lead to better material

Material available on website





NOTE: There are two virtual images, first one that supports exercises 1-22 and second that supports Honeypot exercise. The .pcap file supports the exercise number 19. Additionally Internet Explorer renames files with .ova extension to .tar. You will need to change the extension back before loading it into virtualisation environment.

ENISA CERT training material contains 23 exercises:

No.	Exercise title	Handbook	Toolset	Virtual Image	Other material supporting the exercise
1	**Triage & basic incident handling**	Download	Download	Download	Online version of Exercise 1
2	**Incident handling procedure testing**	Download	Download		Online version of Exercise 2
3	**Recruitment of CERT staff**	Download	Download		Online version of Exercise 3
4	**Developing CERT infrastructure**	Download	Download		Online version of Exercise 4

https://www.enisa.europa.eu/activities/cert/support/exercise

14. Exercise: Proactive incident detection

Main Objective	Setting up and working with AbuseHelper
Targeted Audience	Technical and management CERT staff

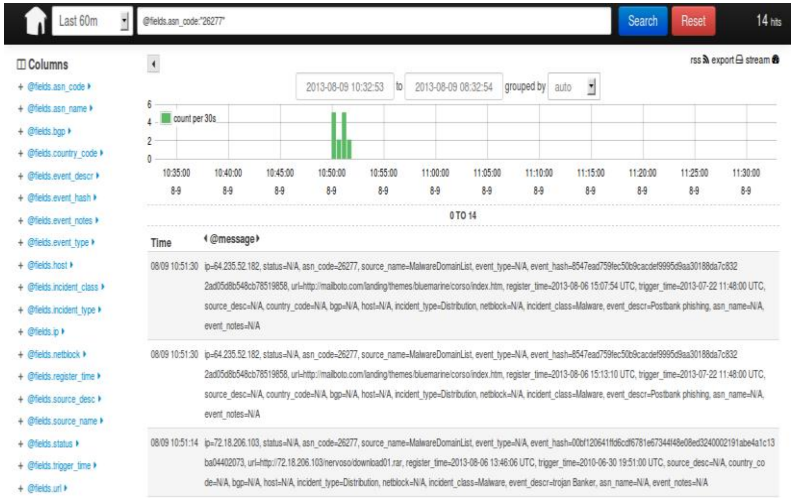
+ Visualising the feeds

Proactive Detection of Network Security Incidents

Proactive Detection of Security Incidents

Honeypots

2012-11-20



Last 60m

@fields.asn_code:"26277"

Search Reset 14 hits

2013-08-09 10:32:53 to 2013-08-09 08:32:54 grouped by auto

```
Time            @message
08/09 10:51:30  ip=64.235.52.182, status=N/A, asn_code=26277, source_name=MalwareDomainList, event_type=N/A, event_hash=8547ead759fec50b9cacdef9995d9aa30188da7c832
                2ad05d8b548cb78519858, url=http://mailboto.com/landing/themes/bluemarine/corso/index.htm, register_time=2013-08-06 15:07:54 UTC, trigger_time=2013-07-22 11:48:00 UTC,
                source_desc=N/A, country_code=N/A, bgp=N/A, host=N/A, incident_type=Distribution, netblock=N/A, incident_class=Malware, event_descr=Postbank phishing, asn_name=N/A,
                event_notes=N/A
08/09 10:51:30  ip=64.235.52.182, status=N/A, asn_code=26277, source_name=MalwareDomainList, event_type=N/A, event_hash=8547ead759fec50b9cacdef9995d9aa30188da7c832
                2ad05d8b548cb78519858, url=http://mailboto.com/landing/themes/bluemarine/corso/index.htm, register_time=2013-08-06 15:13:10 UTC, trigger_time=2013-07-22 11:48:00 UTC,
                source_desc=N/A, country_code=N/A, bgp=N/A, host=N/A, incident_type=Distribution, netblock=N/A, incident_class=Malware, event_descr=Postbank phishing, asn_name=N/A,
                event_notes=N/A
08/09 10:51:14  ip=72.18.206.103, status=N/A, asn_code=26277, source_name=MalwareDomainList, event_type=N/A, event_hash=00bf120641ffd6cdf6781e67344f48e08ed3240002191abe4a1c13
                ba04402073, url=http://72.18.206.103/nervoso/download01.rar, register_time=2013-08-06 13:46:06 UTC, trigger_time=2010-06-30 19:51:00 UTC, source_desc=N/A, country_co
                de=N/A, bgp=N/A, host=N/A, incident_type=Distribution, netblock=N/A, incident_class=Malware, event_descr=trojan Banker, asn_name=N/A, event_notes=N/A
```

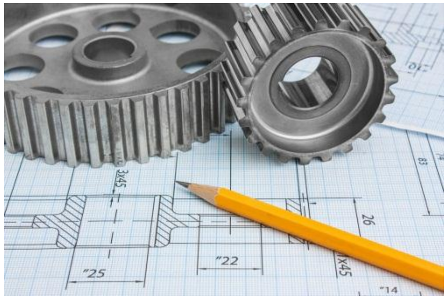
2011

2012

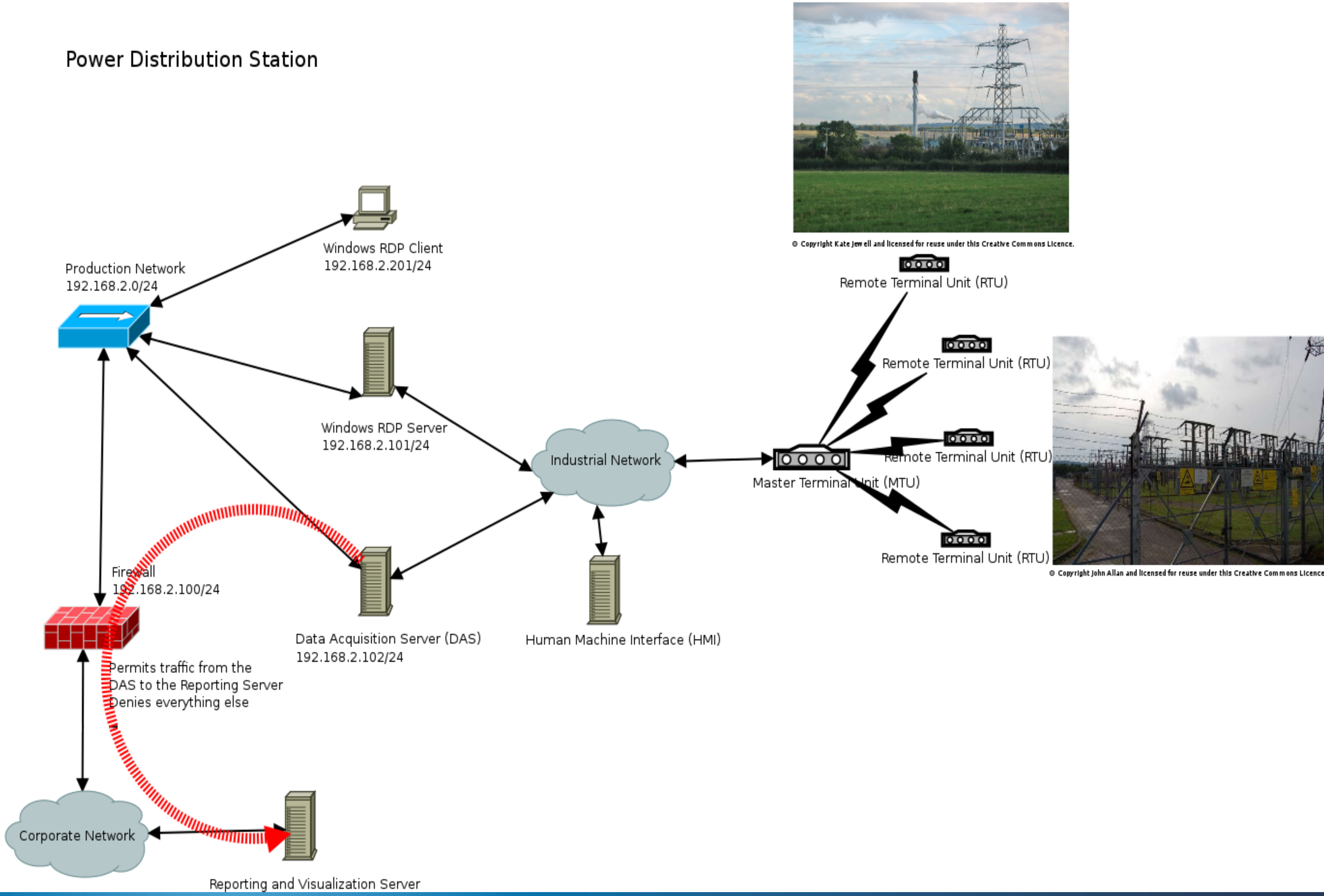
2013

Variety of trainings

- For a different levels of experience and expertise
  - – Legal
  - – Operational
  - – Technical
  - – Cooperation



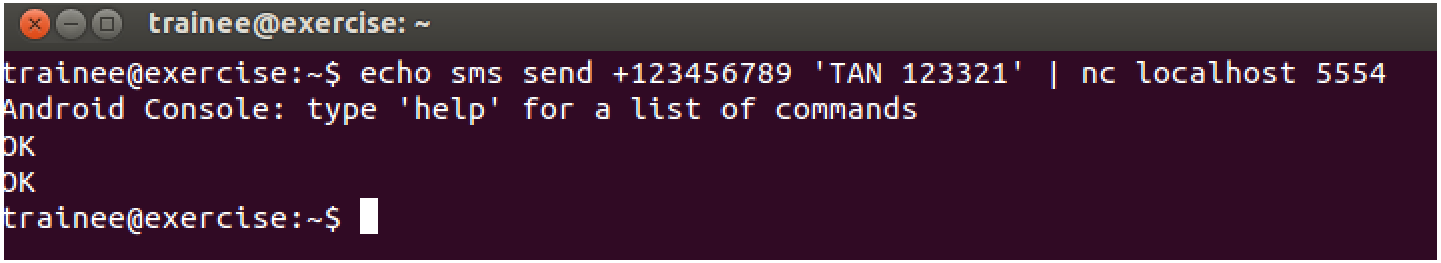
Power Distribution Station


Production Network
192.168.2.0/24
Windows RDP Client
192.168.2.201/24
Windows RDP Server
192.168.2.101/24
Industrial Network
Master Terminal Unit (MTU)
Remote Terminal Unit (RTU)
Remote Terminal Unit (RTU)
Remote Terminal Unit (RTU)
Remote Terminal Unit (RTU)
Firewall
192.168.2.100/24
Data Acquisition Server (DAS)
192.168.2.102/24
Human Machine Interface (HMI)
Corporate Network
Reporting and Visualization Server

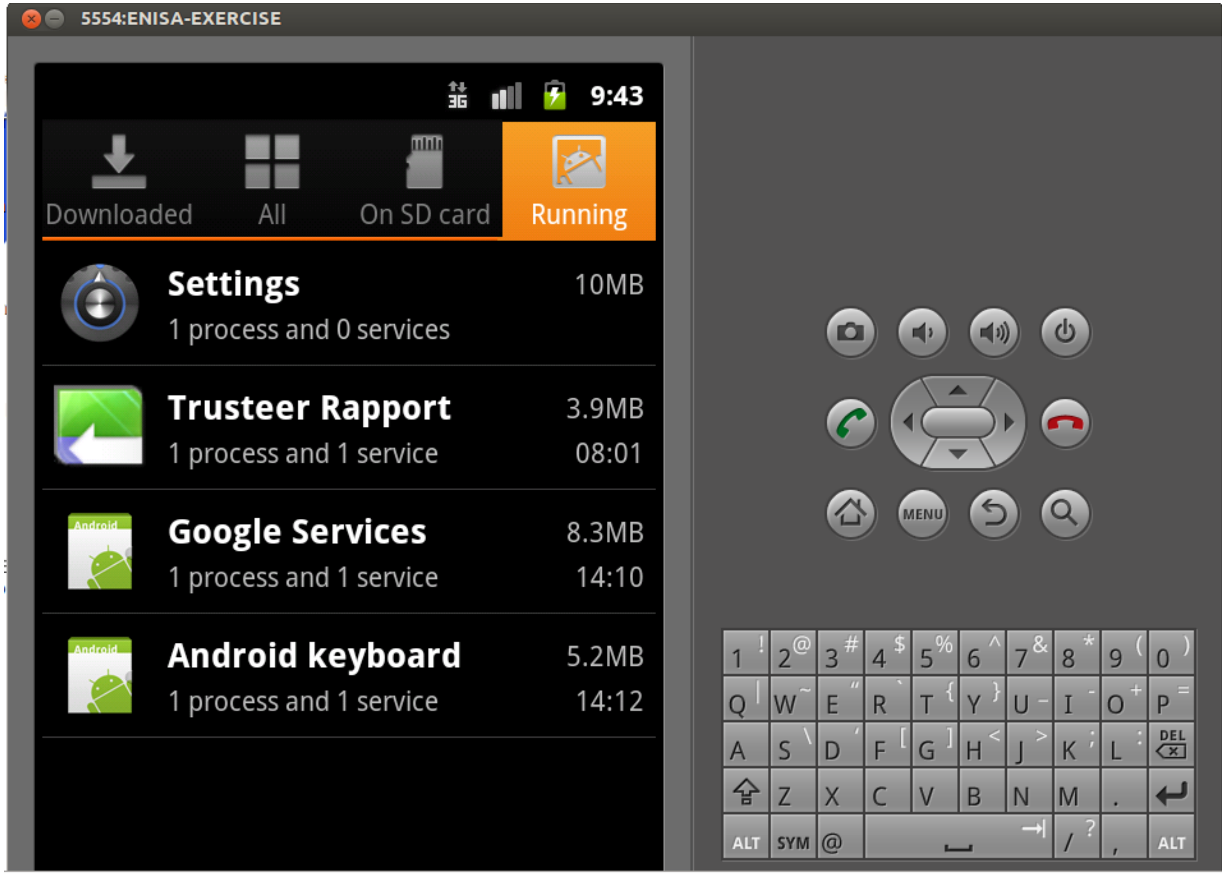
Permits traffic from the DAS to the Reporting Server
Denies everything else

© Copyright Kate Jewell and licensed for reuse under this Creative Commons Licence.

© Copyright John Allan and licensed for reuse under this Creative Commons Licence



```
trainee@exercise:~$ echo sms send +123456789 'TAN 123321' | nc localhost 5554
Android Console: type 'help' for a list of commands
OK
OK
trainee@exercise:~$ 
```



```
Settings                          10MB
1 process and 0 services

Trusteer Rapport                 3.9MB
1 process and 1 service          08:01

Google Services                  8.3MB
1 process and 1 service          14:10

Android keyboard                 5.2MB
1 process and 1 service          14:12
```

What is the file from the Remote file inclusion?

(See in /opt/glaspot/trunk/files/)

50:50 ☎ 👥

A: a SIP OPTIONS scanner in PHP

B: a malicious PDF

[✓ C: a PHP shell]

D: a PHP photo album

New material presented in 2013

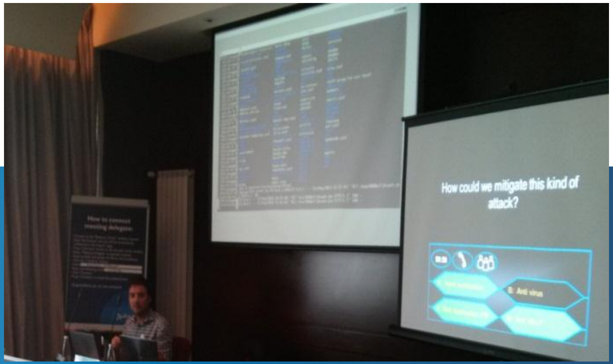
	Title	Experts
1	**Digital forensics**	12
2	**Identifying and handling of electronic evidence**	13
3	**Identifying and handling cyber-crime traces**	12
4	**Incident handling and cooperation during phishing campaign**	9
5	**Presenting, correlating and filtering various feeds**	6
6	**Cooperation in the Area of Cybercrime**	7

ENISA 8th annual workshop 'CERTs in Europe' - Part I

ENISA 8th annual workshop 'CERTs in Europe' - Part I

- 3 scenarios from ENISA CERT training/exercise material presented by ENISA trainers
  - **Honeypots**
  - **Incident handling during an attack on Critical Information Infrastructure**
  - **Mobile threats incident handling**
- Participants rated ENISA training

with 4,4 out of 5 points



ENISA 8th annual workshop 'CERTs in Europe' - Part II

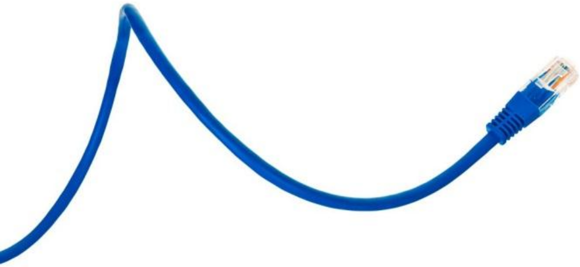
- 2 scenarios from ENISA CERT training/exercise material presented by ENISA trainers
  - **Presenting, correlating and filtering various feeds**
  - **Identifying and handling of electronic evidence**

Recommendations

- Online training material, and handing out material for self-study is good, but…
- Talking with each other actually is useful
- People, who have created or worked together, tend to cooperate in the future
- Every training is a performance and every trainer is an actor

Methodology of ENISA training

- Trainers can come on-site
- Each training is tailored to fulfil the needs of this specific event and audience



Thank you for your attention!

Contact details

European Union Agency for Network and Information Security
Science and Technology Park of Crete
P.O. Box 1309
71001 Heraklion
Crete
Greece
http://www.enisa.europa.eu