CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

LOCKED
SHIELDS

Locked Shields 2013

Kaur Kasak

24 Sept 2013

Disclaimer:

This briefing is a product of the CCD COE. It does not represent the opinions or policies of NATO and is designed to provide an independent position.

Introduction

- Main aspects of Locked Shields (LS) exercises:
  - **„Live fire“**
  - **Technical**
  - **Blue**/**Red** Team
  - **Game**: teams in fictional roles, lab networks
  - Friendly **competition**
  - **Defence** is the focus of training

Scale of LS13

- 10 Blue Teams vs. 1 Red Team
- 10 persons in each Blue Team accompanied by 1-2 **legal advisors**
- 120 + 20 persons in training audience
- 250 persons and 20+ organizations engaged altogether

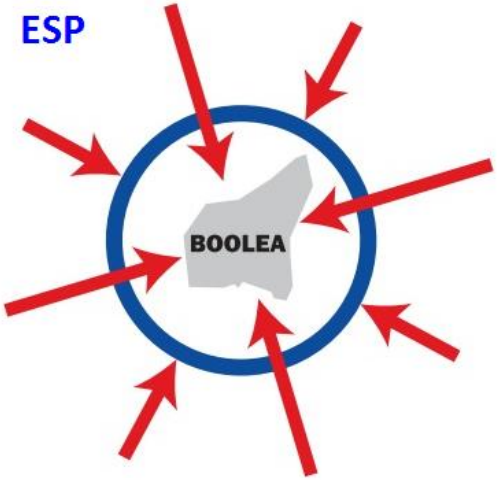
Participants

Blue Teams:

FIN
EST
LTU
POL
SVK
DEU
ITA
NLD
NATO CIRC
ESP

Others:

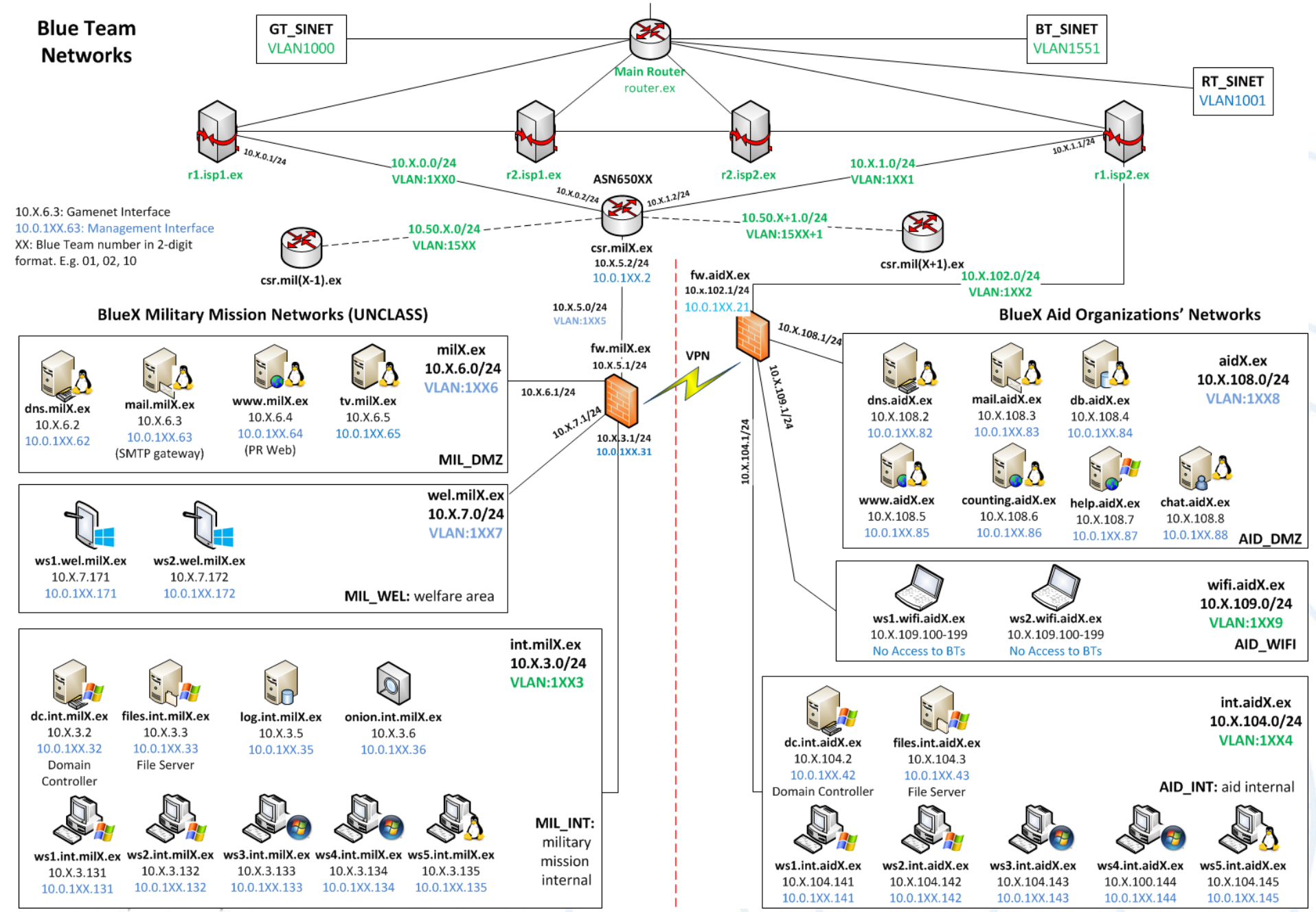
SWE
GBR
FRA
LVA



High-Level Objectives

- **Testing** whether the **defensive teams** are ready to face full-speed cyber attacks
- Similar experience cannot be gained during every day work
  - Massive amount of events
  - Lot of stress: teamwork, communication and leadership skills become essential
- Providing opportunity to compare the progress of your team with others
- Providing opportunity to test new tools and technologies

Blue Team Networks



Pre-built Vulnerabilities

In the beginning, Blue Teams got a really **crappy infra**:

- Un-patched operating systems and application software
- Web applications with well-known security issues
- Configuration mistakes
- Backdoored binaries
- Backdoored web applications
- Pre-planted malware

Red Team Campaign

Obj	Description	Target
1	**Deface** with BIT message and point to malware for distraction.	counting.aidX.ex
2	**Delete content**, **destroy** the host as much possible to keep BT busy in AID_DMZ. Steal at this phase and destroy in next. Successful compromise can be proved by providing the hash from **/etc/hash**	chat.aidX.ex
3	**Change** bank **account numbers** for donations. File where the bank account details are written is **/var/www/app/templates/donate.tpl**	www.aidX.ex
4	Compromise and **steal volunteers database**: database **www** and table **volunteers**	db.aidX.ex
…	…	…
20	Replace the video feed streamed from the TV tower. By default, the following file is streamed and therefore should be replaced: **/var/www/stream/1.mp4**	tv.milX.ex

Red Team Arsenal

KALI LINUX

..and lots of different tools and scripts from BT5r3 and Kali Linux

Defensive Methods and Tactics

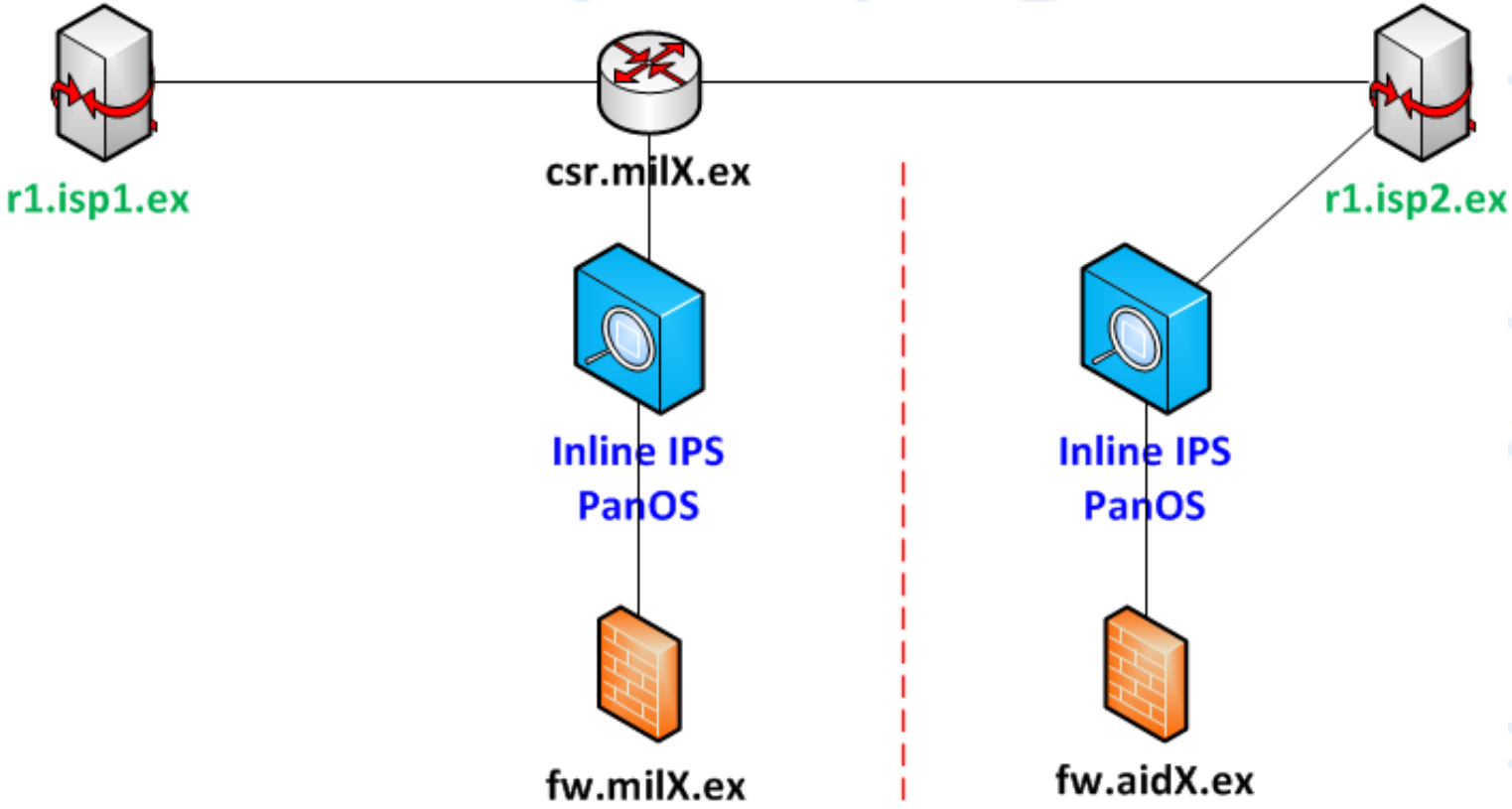
- In general, Blue Teams used **standard security practices** and some custom solutions useful in the context of the exercise
- The key factors of success:
  - Preparation
  - Having expertice to secure all components of the infrastructure
  - Monitoring
  - Teamwork, communication and division of roles

More Unique Actions

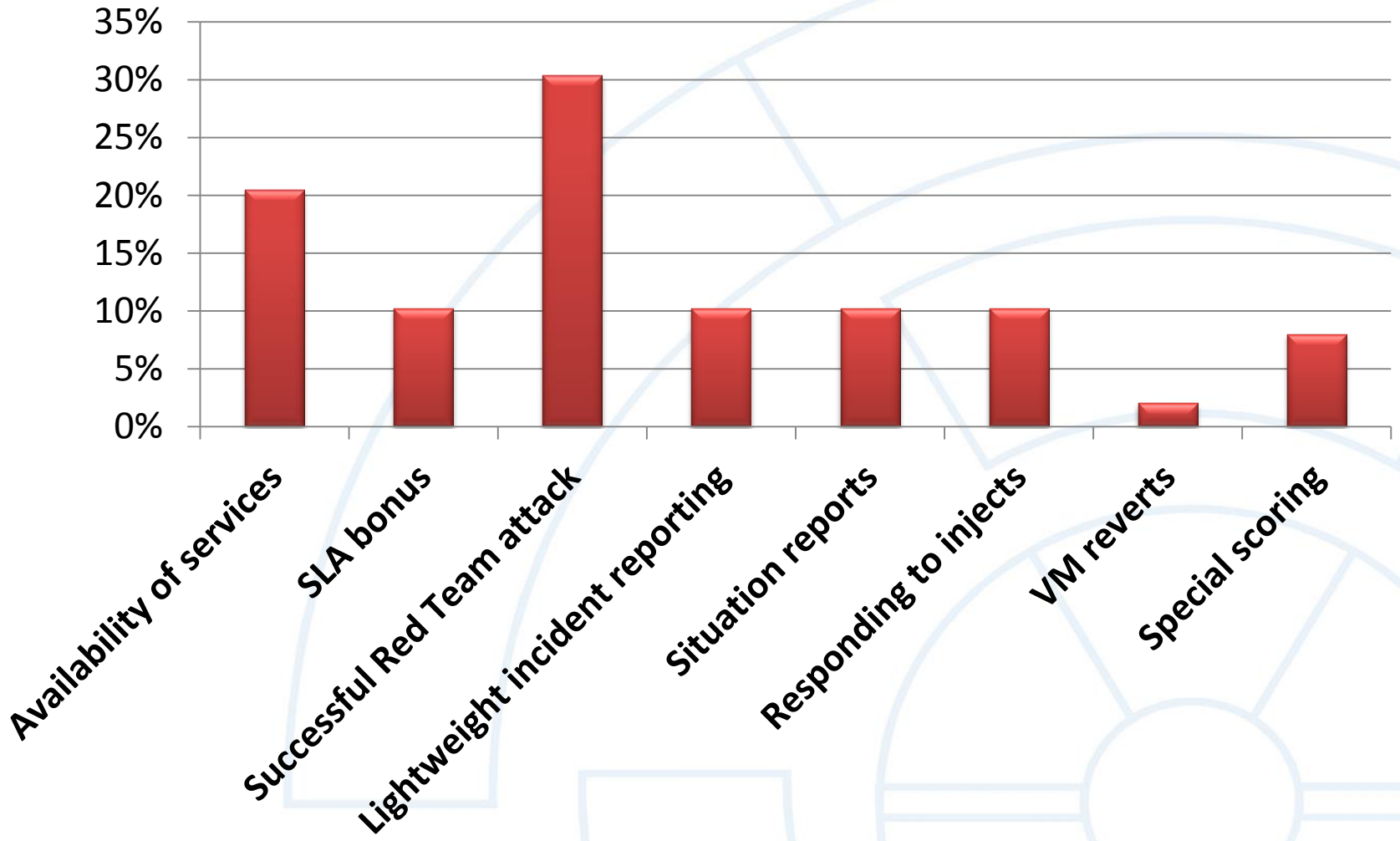
- **Sandboxing** applications especially web browsers (*Sandboxie*)
- **Encrypting** communication between servers (IPSEC)
- Encrypting and **password protecting** files considered sensitive
  - "Blondes" perspective> suddenly, you find that all your important documents have been encrypted by IT department…
- **Custom scripts**
  - monitoring process execution and new connections, creating
- **Inline own IPS**

Inline IPS

- Only winning team deployed their own IPS **inline** to both segments (*Palo Alto Networks*)



Scoring System




NATO proclaimed winner of Locked Shi...
www.theregister.co.uk/2013/04/29/nato_locked_shield_wargame/
SECURITY
NATO proclaimed winner of Locked Shield online wargame
Games without frontiers, war without tears
By Iain Thomson, 29th April 2013
Follow
1,627 followers
8
RELATED STORIES
RAF graduates first class of new groundbased 'pilots'
Free virtual event : Learn how to leverage change for better IT
NATO has – not surprisingly – been named the winner of the Locked Shield online wargames held last week at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.
The 48-hour exercise, which has been held annually for the last five years, simulates a coordinated attack by "Red" forces (a continuing affectation from the days when the Red Flag of the Soviets still flew) on the electronic infrastructure of ten Blue teams, using and and all online means at their disposal.

Lessons: The Blues

- Blue Teams are getting better every year. Well-known free tools without customization do not work against them
- **Custom coded** malicious programs and payloads remain **challenging** to prevent and detect, as expected
- Fixing and **securing custom web applications has not** considerably **improved** over the years
- Most of the Blue Teams **seemed** to **lack experience** with **WAN** routing issues:
  - BGP route hijacking attack was successfully mitigated only by one team
  - Countermeasure would have been easy

Lessons: The Blues II

- Blue Teams **failed** to initiate proper **information sharing**
  - A lot of very useful information was shared.
  - However, it was done using a chat channel which got flooded with data – **teams could not follow**.
  - **Backdoors** or vulnerabilities reported to everyone in the beginning of the exercise **still worked** for many teams on Day2
  - **Competition** may have had a **negative impact** as well although teams get bonus for good information sharing

Lessons: The Reds

- Better trained and **team-working Red Team** is required
  - Knowing each other skills
  - Mastering AV and IDS/IPS evasion techniques
  - Using customised or commercial versions of exploitation frameworks
  - Ability to kill AV products
  - More experts for network infra attacks

Anyone interested in assembling a more permanent Red Team which could support several CDXes?

Issues and Challenges

1. Preparing challenging **Red Team** campaign
   - Simulating **0-days**?
2. After action analysis and **telling the offensive story**
3. Providing **interesting network** to defend and attack
   - Smartphones, IPv6, industrial contr.ol system, weapon control systems and other military stuff,...
4. Legitimate **traffic** generation. User simulation
5. Bringing more **Blue Teams** to the game
6. Gaining **situational awareness** from infrastructure

We are continuously looking for new partners

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia