Cyber Defence Exercise Locked Shields 2012

After Action Report

Tallinn 2012

Executive Summary

Locked Shields 2012 (LS12) was an international technical cyber defence exercise (CDX) conducted on 26-28 March 2012 with more than 250 participants in total. It was organised in cooperation with the Swiss Armed Forces (SAF) Command Support Organisation, Finnish Defence Forces (FDF), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), and the Estonian Cyber Defence League (ECDL).

Nine Blue Teams representing small telecommunications companies had to defend a pre-built network against hostile attacks conducted by 40 Red Team members. Each Blue Team had a similar network consisting of approximately 25 virtual machines. Initially, their systems were full of vulnerabilities and configuration mistakes. Events were observed and analysed by a Legal Team consisting of an international group of lawyers. The Blue Teams were competing with each other and their progress was evaluated by the White Team.

The main objectives of LS12 were: to train Blue and Legal Team members; to support the campaign of the Multinational Experiment 7 (MNE7); to explore situational awareness technologies in the cyber domain; and learn from the activities of Blue and Red Team members.

The organisers succeeded in providing an interesting and complex environment for the Blue Teams to defend. In addition to an intensive attack campaign, Blue Teams were challenged by additional tasks and media pressure, requiring them to have a wide range of skills to be successful. All Blue Team members were interested in being engaged in similar future events.

The second main training audience, the Legal Team members, had a good opportunity to learn about the technical aspects of IT systems attack and defence. However, due to the way teams were organised, with simple scenarios and fictional legislation, the lawyers were not actively engaged in the game.

Lightweight Human Reporting proved to be effective in establishing situational awareness about defensive and offensive campaigns. The solution should be further developed and participants better trained to increase the frequency and accuracy of reports provided by human experts.

Regarding the attack and defence activities, we observed only known and standard practices on both sides. It was clear that vulnerabilities in web applications turned out to be the Achilles' heel of LS12 Blue Teams.

Locked Shields should remain as a live technical cyber defence exercise, as there is a clear need for more and similar training events. In this report, we have listed numerous observations as to how to improve Locked Shields in the future.

Table of Contents

1 Introduction

Locked Shields 2012 (LS12) was an international technical cyber defence exercise (CDX) conducted on 26-28 March 2012. Nine Blue Teams had to defend a pre-built network against the Red Team attacks. Each Blue Team had a similar network consisting of approximately 25 virtual machines. Initially, their systems were full of vulnerabilities and configuration mistakes. Events were observed and analysed by a Legal Team consisting of an international group of lawyers. A friendly competition took place between the Blue Teams and their progress was evaluated by a White Team.

The teams engaged in LS12 included participants from multiple nations. For instance, Blue Teams consisted of experts and specialists from governmental organisations, military units, CERT teams and private sector companies. There were Blue Teams from Switzerland, Germany, Spain, Finland, Italy, NATO Computer Incident Response Capability - Technical Centre (NCIRC-TC), Slovakia, and combined teams from Germany-Austria and Denmark-Norway. The core of the Red Team was composed of specialists and volunteers from Finland and Estonia, with additional contributors from Germany, Latvia, NCIRC-TC and Italy.

LS12 was organised in cooperation with the Swiss Armed Forces (SAF) Command Support Organisation, Finnish Defence Forces (FDF), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), and the Estonian Cyber Defence League (ECDL). Situational Awareness solutions were provided by the private companies Clarified Networks (Finland) and RUAG Defence (Switzerland). Contributors from many other organisations were also involved.

The purpose of this document is to provide an overview of the exercise, describe the events that happened during the Execution phase, and list observations and recommendations as to how to improve the next Locked Shields exercises. The report includes a situation analysis based on human reports and the most important parts from the information package describing and regulating the Game. Although the findings are mostly very specific to Locked Shields, we hope that the report will also be useful for other parties organising similar technical exercises.

2 Overview of Locked Shields 2012

2.1 Concept

Locked Shields 2012 was a technical Blue/Red Team exercise. The general format of the CDX was a game: no organisation which participated played their real-life role and the scenario was fictional. Blue Teams had to defend partially pre-built computer systems against attacks from the Red Teams. All Blue Teams had similar systems, simulating the network of a small telecommunications company. The initial configuration of the Blue Teams' infrastructure included vulnerable and wrongly configured systems.

To motivate the teams and measure the success of different strategies and tactics, there was a competition between the Blue Teams. The progress of the teams was measured by automatic and manual scoring. Red Team members did not compete with each other. Their objective was to provide equally balanced attacks on all the Blue Teams' networks.

LS12 was related to the cyber campaign of the Multinational Experiment 7 (MNE7). Yellow Team members used the exercise environment to explore and test different solutions for situation awareness (SA) in the cyber domain. Some of the Legal Team members were also contributing to MNE7 objectives. The Legal Team defined fictional legislation for the CDX.

2.2 Objectives

The high-level objectives of LS12 were the following:

1. **Support MNE7** to achieve a technical cyber objective. The aim of the respective MNE7 technical objective is to explore relevant technologies that decision-makers require to gain and maintain effective collaborative situational awareness of the cyber environment.
2. **Train teams of IT specialists** to detect and mitigate large-scale cyber attacks and handle incidents by providing them with an interesting and challenging training environment. The following list outlines the main training objectives for the Blue Teams:
    a. Testing skills.
    b. Testing teamwork, designing an environment and rules in a way that teams with better cooperation would perform better.
    c. Teaching national level cooperation.
    d. Teaching international communication and cooperation.
3. **Train legal experts** by involving them to analyse and observe the events. Another objective for the legal experts was to come up with a plan to make the Legal Team's involvement more valuable for future exercises.
4. **Learn from the activities of Blue and Red Teams: i**n case of similar real-world scenarios, which tactics and methods of defence are the best and what kind of steps from the attackers to expect.
5. **Search opportunities to integrate the technical CDX with an exercise that involves political and high-level decision-making processes**. The aim was to test and develop tools and methods that provide decision-makers with situational awareness about the cyber environment.
6. **Create the technical infrastructure** in such a way that it would be easy to **reuse the components** and set it up again for a new exercise. Compile good documentation and automate the installation processes of the environment as much as possible.

7. **Improve international cooperation** in cyber defence by involving cyber defence practitioners from many different nations.
8. **Strengthen the international security community** by exchanging information and experiences.
9. **Improve the capability to conduct exercises**.

2.3 Participants

More than 250 participants in total were engaged in LS12.

Approximately 110 persons participated as defending Blue Team members:

- Blue Teams for the Test Run were assembled from specialists from kapsi.fi (FIN) and ECDL (EST).
- Blue Teams for the Execution were assembled from specialists from FIN, CHE, ITA, DEU, DEU-AUT (2 persons from DEU and 8 from AUT, winning team), DNK-NOR-SWE, ESP, SVK, NATO Computer Incident Response Capability Technical Centre (NCIRC-TC).

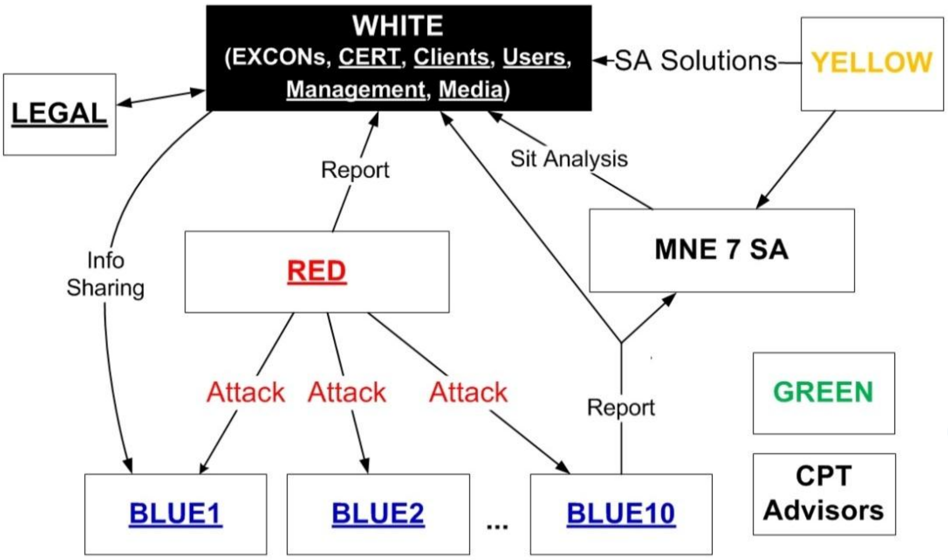
Approximately 165 persons participated in other teams:

- 40 Red Team members
- 15 Green Team members
- 15 White Team members
- 15 Legal Team members
- 30 Yellow Team members
- 50 MNE7 SA team members.

2.4 Teams

2.4.1 Overview

The participants of LS12 were divided between many different teams. The following diagram provides a generic overview of the teams and the relationships between them. Teams with underlined names were considered as players, that is, they played some role according to the scenario.



2.4.2 Blue Teams

2.4.2.1 Description

The **Blue Teams** were the main training audience. Their task was to secure the virtual IT infrastructure of a small telecommunications company and defend it against the Red Team's attacks. Blue Teams had to maintain services as described in documentation, assuring confidentiality, integrity and availability of the systems. In addition, Blue Teams were supposed to report detected incidents to the White Team (CERT, Management) and complete business tasks injected by the White Team. Business tasks included requests from clients and employees, information requests from journalists, etc.

The majority of Blue Team systems were pre-built by the Green Team. In addition, each Blue Team could deploy its own Virtual Machines (VM), for network traffic analysis, for example. The network consisted of typical network devices and virtual servers and workstations. Blue Teams were allowed to use their own tools and software provided they did not contravene any licensing terms.

Blue Teams' success was measured by both automatic and manual scoring.

2.4.2.2 Number of Teams, Size and Location

Team	Number of Teams	Team Size	Location
Blue	9	6-10	Various, each team has to find the location

The number of available slots was limited due to technical constraints and the capabilities of the Red Team. Blue Team slots were divided 50%-50% between NATO CCD COE Sponsoring Nations (SN) and MNE7 nations.

Blue Team members were not supposed to be physically co-located during the execution of the CDX. Everyone could access the CDX environment remotely over OpenVPN. Still, all the teams preferred to stay in the same place with all their team members.

2.4.2.3 Roles

The following were supposed to be present in each team:

- **Team Leader** – overall management of team's activities and Point of Contact (POC) to exercise controllers.
- **Deputy Team Leader** - alternative POC for the team.
- **IT specialists** – administering and securing the systems, defending the systems against Red Team's attacks.
- **PR manager** – communicating with inquisitive journalists and the 'media'.
- **Reporter** – reporting the Blue Team activities to the White Team, which helps the White and other teams to receive situational awareness.

The distribution of the roles and responsibilities for the participants was up to each individual team.

2.4.2.4 Expected Skillset

Taking into account the components of the technical infrastructure the Blue Teams had to secure, they were expected to have knowledge in and experience of the following areas:

- 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 (Endian distribution will be used), proxy servers
  - Common network protocols, services and technologies like DNS, NTP, DHCP, HTTP and HTTPS, SMTP, POP3, IMAP, SSH, FTP, RADIUS
  - KVM virtualization platform.
- Web application technologies and development (HTML, client-side and server-side scripting such as JavaScript and PHP, SQL databases such as MySQL).
- Administration of network devices (switches and routers running Cisco IOS, OSPF routing protocol).
- Some programming skills in Perl, as the automatic scoring bot was implemented in Perl.

2.4.3 Red Team

2.4.3.1 Description

Red Team's mission was to compromise or degrade the performance of the systems that were protected by Blue Teams. The phases and objectives for the Red Team were pre-planned.

The focus of LS12 was to train the Blue Teams. Therefore Red Team members were mainly considered as the 'work-force' to challenge the Blue Teams. In principle, the Red Team used a **white-box** approach. The technical details of the initial configuration of the Blue Team systems were available for the Red Team beforehand, along with the opportunity to scan Blue Team systems for vulnerabilities before the execution. However, as the team was composed of volunteers, many of them did not have time to learn the target environment in detail. The white-box approach was chosen to balance the fact that in a real-world situation, motivated attackers would have no significant time constraints as there were during the exercise.

2.4.3.2 *Number of Teams, Size and Location*

Team	Number of Teams	Team Size	Location
Red	1 with many sub-teams	40	Tallinn

Red Team members were divided between 6 sub-teams:

1. Web attacks
2. Hosting and KVM attacks
3. Network attacks
4. Client-side attacks
5. Advanced campaigns
6. Various tasks.

In addition, there were four Liaison Officers between Red and White Teams. They were responsible for reporting and coordinating Red Team's successful actions to the White Team.

2.4.3.3 *Expected Skillset*

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).
- Web application pen-testing skills (SQL injection, file inclusion, input validation bypassing, etc.).

Desirable additional/specialised skills included:

- The ability to hide and stay resistant in compromised hosts and networks (backdoors, rootkits, and 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 fuzz testing protocols, making use of found vulnerabilities during the short game execution period, crashing of services during destructive phases.

2.4.4 White Team

2.4.4.1 *Description*

White Team's tasks during the preparation period were:

1. Defining exercise objectives and **objectives** for the **Red Team**.
2. **Developing the rules,** including scoring rules. The rules cover general aspects such as how the exercise will be run, regulations for Blue Team activities and rules of engagement for the

Red Team. Scoring rules specify how the Blue Teams will be assigned both positive and negative manual scores.
3. Preparing **business tasks** for the Blue Teams and the **inject list**.
4. Contributing to the **development** of the high-level **scenario**.
5. Developing a communication plan.

During the Execution phase, the White Team acts as the exercise controllers' cell. White Team's main tasks during Execution were:

1. **Controlling** the exercise and the Red Team campaign. White Team decides when different phases start and stop, and when the Red Team has to wait or slow its activities down.
2. Acting as the **CERT**: receiving and evaluating incident reports, providing advisories and abuse notifications. In reality, the CERT team was mainly engaged in evaluating Blue Team reports and did not play the role of overall coordinator of Blue Team efforts.
3. **Evaluating** the progress of the Blue and Red Teams and assigning manual scores. The White Team evaluates the reports of successful compromises issued by the Red Team which will result in a negative score. Successful detection of attacks described in incident reports, the ability to respond to business injects, and new creative ideas as to how to defend (and collaborate with other Blue Teams) will generate a positive score.
4. Simulating the activities of Blue Team organisations' **clients**.
5. Simulating the **management** and the **users** of the organisations whose networks the Blue Teams are defending.
6. Simulating the **media**. For instance, injecting news stories and acting as journalists contacting the Blue Teams.

2.4.4.2 Team Size and Location

Team	Number of Teams	Team Size	Location
White	1	15	Tallinn

White Team members were divided into the following roles or sub-teams during execution of LS12:

- Judging and Control
- CERT
- Communications Officers
- Blue-White Team Liaison Officers
- Media Simulation
- Management and Clients Simulation
- Users' Simulation.

2.4.5 Green Team

2.4.5.1 Description

The **Green Team** was responsible for preparing the technical infrastructure in the lab. Typical tasks for Green Team included:

- setting up the core infrastructure: computing nodes, virtualization platform, storage, networking.
- setting up routing and VPN access to the environment.

- designing and building Blue Team networks.
- developing management interfaces for the Blue Teams.
- programming the automatic scoring bot and agents.
- setting up solutions required for monitoring the general exercise infrastructure.
- installing the recording and logging facilities.

Building the exercise infrastructure is the most critical factor for having a successful technical environment. Therefore Green Team's tasks were most challenging and work-intensive.

2.4.5.2 Number of Teams, Size and Location

Team	Number of Teams	Team Size	Location
Green	1	14	Madrid, Tallinn, Bern

2.4.6 Yellow Team

2.4.6.1 Description

The **Yellow Team's** role was to explore the technologies for obtaining situational awareness in the cyber domain. The Yellow Team was responsible for selecting solutions and methods to be tested in the experiment, developing appropriate set-ups, and analysing the experiment results.

2.4.6.2 Number of Teams, Team Size and Location

Team	Number of Teams	Team Size	Location
Yellow	1	NA	Bern, Helsinki

There were two principal sub-teams providing situational awareness solutions for LS12:

- The Finnish Team, primarily consisting of experts from Clarified Networks.
- The Swiss Team, primarily consisting of experts from RUAG.

2.4.7 Legal Team

2.4.7.1 Description

The **Legal Team** (LT) was part of the training audience but also contributed to the preparation of LS12. Legal experts were engaged in the following activities:

a. Developing fictional legislation for LS12.
b. Analysing and observing the events from a legal perspective.
c. Providing advice to the Blue Teams in terms of the legal aspects.
d. Learning about the technical side of the attacks.

2.4.7.2 Number of Teams, Size and Location

Team	Number of Teams	Team Size	Location
Legal	1	15, Negotiable	Helsinki

2.5 Scenario

2.5.1 Role of the Blue Teams

The Blue Teams of LS12 represented telecommunications companies. Blue Teams had to comply with fictional legislation (Appendix C: Legislation) and provide the following services to their clients:

- Simulated DSL connectivity to the internet.
- Shared web hosting.
- Email hosting.
- Providing virtual private servers.

Blue Teams had also to manage the back-office infrastructure of their company. In addition, Blue Teams 'shared' a common data centre. It was simulated that the cooling system of this server room was controlled by a lab SCADA system, which could be accessed only through each Blue Team's internal network. Therefore every Blue Team had to keep the Red Team out of their internal network segment to avoid the 'blow-up' of the shared cooling system.

2.5.2 Role of the Red Team

The attacks occurring during the exercise originated from two different groups:

- An organised crime group 'RadicalBattalioN' (RBN), motivated by commercial gain.
- A group identifying itself as 'The Janitors', an anonymous network of neutrality activists disappointed with recent news stories about ISPs admitting using a data mining tool to gather and analyse data on some of their users. The group's goal was to get access to a list of these clients, details of the search method and parameters, and publish everything they could get access to.

2.5.3 News Feeds

The background scenario was defined by several news feeds:

2.5.3.1 14 Hackers Arrested by Interpol

Interpol announced today that a major international police operation had succeeded in identifying and arresting 14 people in connection to the organized crime group Radical BattalioN (RBN). The group has been involved in providing bulletproof hosting services, identity theft, money laundering, spamming and DDoS-based extortion using the global botnet some researchers have dubbed Prometheus.

Interpol offered thanks to several Internet Service Providers: Blue 1, Blue 2 and Blue 9. Without the assistance of these ISPs, the police would never have been able to track and identify the suspects.

The chief investigator commented: 'While it is still too early to celebrate, we are confident that this has dealt a mighty blow against the criminal underworld. We are already seeing a 48% drop in the number of spam emails around the world and the Prometheus botnet has not been active since we took its suspected administrator into custody.'

2.5.3.2 Biggest ISP Conference Held in Cape Town

The premier ISP conference is taking place in South Africa this week. Participants include IT security personnel and chief system administrators of most of the world's leading ISPs, as the conference also boasts a live-fire exercise for the gathered ISP teams, in order to determine the best one. A lot of fireworks are expected before the week is over and the winning team gets to go home with the coveted Turing trophy.

2.5.3.3 CoolAirz Hacked

The commercial air-conditioning provider, CoolAirz, reported a security breach in their systems yesterday. While a representative of the company claims no serious harm was done, some web commentators speculate that the attackers may have had access to the source code of the remote administration tool used to manage the temperature in most commercial server rooms.

2.5.3.4 ISPs admit spying

Several ISPs in Europe have admitted using a data mining tool to determine the risk profile of tens of thousands of customers. The story was revealed by a group of students in France who noticed peculiar redirects of their web traffic. Web activists have claimed that this is unethical and that the companies may have collected personal information about the habits and interests of the customers. If that is the case, the recording industry may be very interested in the database, as it would help in deploying targeted ads.

2.5.4 Initial Inject for Blue Teams

'You are in charge of the Reserve Administration and Security Team of the ISP where you work. The Primary team is off to South Africa (see news) and is likely to stay there for the entire week.

You have just noticed that somebody is trying to map your network and has tried to gain unauthorised access to the public web server. It is not known if this has anything to do with the criminals that your team helped to capture last week.'

2.6 Technical Environment

The exercise infrastructure was provided by the Swiss Armed Forces Command Support Organisation and was located in a central place. The environment (virtual machines, network elements) was set up and deployed for the CDX in a private cloud. This private cloud was running on Supermicro Superblades. OpenNebula was used for cloud management and KVM as the underlying virtualization solution.

There were, in total, eight AMD Opteron blades (4 x 12 Core CPUs @2.2 GHz, 64GB RAM) and two Intel Xeon blades (2 x 6 core CPU @2.93GHz, 48 GB RAM).

Infortrend SAN (two enclosures with a total of 32 disks and 40GBs iSCSI bandwidth) was used for the storage. However, the initial solution did not provide enough IOPS and had to be redesigned after the test run. A ZFS file system was used with a Openindiana-based storage accelerator to boost IOPS. A 4GB DDRDrive acted as a write cache and 96GB RAMDisk as a read cache.

The participants were provided with an OpenVPN access to the management segment of their virtual machines and they could use SSH, RDP or VNC for remote administration.

3 Planning

Exercise preparation activities were built around three main planning conference events: Stakeholder's (SPC), Main (MPC) and Final Planning Conference (FPC). In addition, all teams had individual or partially mixed meetings. The topics related to LS12 were also discussed in MNE7 Workshops (Helsinki, Lillehammer). GoToMeeting and Skype were used to connect distributed participants. Although the concept for the exercise had already been agreed during SPC in May 2011, the majority of the preparations were carried out from the MPC stage to Execution.

The main planning events were:

- **23-24 May 2011**: Stakeholder's Planning Conference, Tallinn
- **18 Aug 2011**: Core Planning Team Meeting, Bern
- **11-13 Oct 2011**: MNE7 Workshop 1, Helsinki
- **27-28 Oct 2011**: Main Planning Conference, Helsinki
- **10-12 Jan 2012**: MNE7 Workshop 2, Lillehammer
- **2-3 Feb 2012**: Final Planning Conference, Bern
- **15 Feb 2012**: Test Run, key players in Bern, Helsinki, Oulu and Tallinn
- **26-28 Mar 2012**: Execution
- **29 Mar 2012**: Hot Wash-Up
- **31 Aug 2012**: After Action Report Review, Tallinn.

4 Execution

4.1 Day 0

4.1.1 Objectives

The pre-CDX day was dedicated to preparations before the STARTEX:

1. Testing access to the Collab environment and other communication channels (GoToMeeting, chat, email, Skype, telephones).
2. Testing remote access to Gamenet.
3. Helping Blue Teams to deploy their own VMs.
4. Explaining rules, scoring principles and reporting.
5. Running test attacks by Red Team to exercise reporting.

This day proved to be absolutely necessary, as several access problems were identified and solved.

4.1.2 Communication and Connectivity Tests

Planned activities started at **07:00Z**. Firstly, all Blue Teams were expected to join the GoToMeeting session and establish VPN connectivity into the Out-Of-Game Zone (see Appendix A for an explanation of the Zones) where the Gamenet collaboration environment was located. At **07:40Z** we were still missing two Blue Teams from GoToMeeting. Regarding VPN, the main issue was to connect MNE7 team in Riihimäki, as their router and server-side configuration was not scaled to the number of workstations that required access. Some Blue Teams also had issues with the stability of their VPN box, preconfigured by the Green Team, and had to restart it several times.

The second major task related to communication methods was to have all participants connected to the wiki and chat-based collaboration environment (Collab) and joining all required chat channels (see Appendices G, H and I for communications and reporting processes). Collab had been moved from an internet-facing hosting environment to the Gamenet the night before. This caused account synchronisation issues and problems were reported with 28 user accounts out of 330. The main issues were the following:

- Forgotten passwords: password reset was possible only through the internet-facing Collab, after which additional synchronisation had to be done by the administrators.
- Changed passwords which were not synchronised between the internet-facing Collab and Gamenet Collab.
- Forgotten invitations by team leaders.

Two Red Team members could not access Gamenet Collab until the end of the game, but all other issues were solved on Day 0.

In parallel to troubleshooting access problems in the Collab environment, Skype accounts were also tested.

4.1.3 Briefings and Full Access to Gamenet

At **10:45Z**, a short reminder of rules and scoring principles was given by the White Team. Yellow Team briefed others on Lightweight Human Reporting (see Appendix I). After that (**11:10Z**), VPN access to all Zones was opened. Full access to the whole environment was given on Day 0 to fulfil the following goals:

- Test access to all VMs. A few password issues and some VMs in a non-operational state were identified and fixed.
- Test in-game email accounts. Some configuration mistakes were identified and (partially) fixed. Blue Team 9 (BT9) had trouble with getting access over POP3 and IMAP. BT1 had a non-functional DNS server which prevented the team having initial success. BT6 reported having problems with an internal mail server during the whole exercise.
- Give the Blue Teams the opportunity to upload and test own VM. This process turned out to be overly complex. Firstly, teams using specific SFTP clients experienced error messages and could not upload their images. Secondly, Blue Teams lacked experience or guidelines on how to customize VM definition files. This resulted in machines being in FAILED state after the deployment.
- Run a couple of attacks in order to exercise the incident reporting. We observed five (BT1, BT3, BT5, BT8, BT9) out of nine Blue Teams testing out Lightweight Human Reporting using tweets. Others tested reporting only in the wiki.

4.1.4 Test Attacks

The Red Team used Day 0 to finalise a division of members between sub-teams, prepare the campaign, set up infrastructure, generate payloads for exploits, coordinate work with White Team, etc.

At **11:40Z** the Red Team started to conduct some simple hostile activities like network and web application scanning, password brute-forcing and web attacks against e-shops (shop.dmz.bluex.ex). Before VPN access was closed at **13:10Z**, attacks were stopped.

4.1.5 Other Activities

In addition to fixing problems reported by the Blue Teams, the Green and Yellow Teams were busy tweaking the traffic-capturing infrastructure, improving monitoring systems (the Munin server was not graphing for all the blades properly) and fixing other issues with the infrastructure. The biggest concern was the high amount of IOPS observed on the storage layer.

All Blue Team VMs were reverted to the vulnerable snapshots before STARTEX on Day 1; thus the Blue Teams lost all the changes.

4.1.6 Conclusions for Day 0

To conclude the discussion of the events on Day 0, the following aspects should be highlighted:

1. The objective of testing all communication channels and remote access was met.
    - It did not go as quickly and as smoothly as expected but, in the end, only a few Red Team members did not get access to the Collab environment.

2. The objective of briefing Blue Teams on rules and scoring principles, and to test reporting was partially met.
    - Some Blue Teams were expecting more detailed briefings by the White Team. In addition, Blue Teams did not get detailed feedback from the Red Team on which test attacks were performed during Day 0.
3. The objective of having all Blue Team owned VMs running by the end of Day 0 was partially met.
    - Some teams never got their own VM properly deployed into the exercise environment.

4.2 Day 1

4.2.1 Introduction

At **06:40Z**, before the official start of Day 1, the Locked Shields News Portal was updated with a fresh story: ‘ISPs admit spying’. This was meant to provide a context for the first hacktivist attacks. A few minutes after **07:00Z**, the White Team requested a status brief from all the Blue Teams, and then full VPN access to Gamenet was opened.

4.2.2 Web Attacks

Red Team started the campaign (Appendix B: Red Team Campaign Plan Prior to Execution) at **07:30Z** with defacements against web portals in DMZ (www.dmz.bluex.ex and webmail.dmz.bluex.ex). The Blue Teams clearly did not have any time to take precautions against these scripted attacks, as defacements were effective against all but BT5. The web servers of BT5 were not accessible from the Red Zone where the scoring bots and Red Team members were located. However, it appears that this was not the team’s fault but was caused by networking problems in the infrastructure.

At **09:00Z** as previously planned, persons in the role of RBN launched their hacks to steal client databases:

1. From shop.dmz.bluex.ex. Customers of BT1, BT2, BT4, BT6, BT8 and BT9 lost their data at once, BT5 later during Day 1 (at **14:50Z**). Remaining databases were lifted first time on Day 2: BT7 at **09:00Z** and BT3 at **12:15Z**.
2. From portal.dmz.bluex.ex. Customers of BT1, BT2, BT3, BT8 and BT9 were hacked right at the beginning, BT4, BT5, BT6 and BT7 later on Day 1.

Red Team was allowed to repeat each type of attack every two hours. The second defacement round started at **11:00Z** and was successful against all Blue Teams. However, different Red Team members attacked different targets. The following sites were defaced: shop.dmz.bluex.ex (BT1, BT2, BT3, BT6, BT7), webmail.dmz.bluex.ex (BT4, BT9), portal.dmz.bluex.ex (BT5), and shared-web.dmz.bluex.ex (BT8).

The third defacement round started at **13:00Z**. There were no significant differences when compared to the previous round - all teams were defaced. This time the targets were different for all but BT5 and BT9: www.dmz.bluex.ex (BT1, BT4, BT7), portal.dmz.bluex.ex (BT2, BT3, BT5), webmail.dmz.bluex.ex (BT6, BT9), and shop.dmz.bluex.ex (BT8). It is interesting to note that, according to Red Team reports, the attack against BT5 was accomplished at **14:40Z**. This was more than one hour later than the others. BT5 was using web application firewalls, had good monitoring and fixed problems on the fly (three minutes after specific SQL injection attempts, the vulnerability was fixed). However, Red Team was finally capable of bypassing all of BT5's protection mechanisms.

Other teams that received good feedback from Web-Attacks team were BT4 ('Good reaction and fixed things after attacks') and BT8 ('Good reaction and fixing. Good active monitoring').

4.2.3 Network Attacks

The first successful attack against routers and switches to acquire their configuration was reported at **07.37Z** against BT1. During Day 1, Red Team also managed to compromise BT2, BT5 and BT9's network devices. Other teams changed the default passwords (such as cisco:cisco) and fixed the configuration which then prevented Red Team also accessing SNMP. However, it should be noted that, on Day 2, Red Team reported achieving this objective also against BT4 and BT6. This raises the question why this was not possible in Day 1? One option could be that the teams' VMs were redeployed. Still, there was no evidence that BT4 or BT6 would have requested reverting themselves.

4.2.4 Client-side Attacks

During the morning of Day 1, the client-side team focused on compromising Windows 7 workstations in INTERNAL Zone to steal confidential memo. Executable files with malicious payloads were generated and then hosted from Red Team's web servers. Links to files named 'paycheck.exe', 'run.exe', 'java_update.exe', 'fun.exe' and 'reiska_12_variant.exe' were sent to Blondes who had to click and run them (a Blonde being a person simulating the ordinary computer users of Blue Team companies). In some cases, the exploitation of vulnerabilities in client-side software was also practised. The Red Team started with payloads without obfuscation, then adding more and more encoding to avoid detection by AV signatures. This was effective against all Blue Teams whose workstations were accessible to the Blondes: BT1 (**08:15Z**, first report), BT2, BT3 (**10:44Z**, last report), BT4, BT5, BT6 and BT9. Workstations of BT7 were down due to infrastructure issues. The Blondes also could not access the workstations of BT8. Apparently their IDS blocked access over RDP.

In addition to stealing the memo, a side-task was to maintain access in the networks for future objectives such keystroke logging to capture the password of the SCADA system. Red Team gained full access with SYSTEM privileges on compromised hosts. Pass-the-hash allowed them to pivot through the networks, dump and crack additional hashes and create new accounts. A few times, Red Team members mixed up the chat channels and announced new accounts on 'cdx12', which was observable by everyone.

The afternoon was not so successful for the Red Team. The Blue Teams had finally had a chance to apply some countermeasures. Red Team's sessions were killed, operating systems patched.

At **12:00Z** Red Team started a phishing campaign with the purpose of:

1. Firstly, stealing credentials on a faked 'Outlook Web Access' page.
2. Secondly, tricking the Blondes into running an executable file named 'OutlookClient_NEW.exe' which, after successful execution, would spawn a Meterpreter session.

The credentials were successfully stolen from BT1, BT2, BT3, BT5, BT8 and BT9. Malware used in the phishing campaign was reported as successful only on BT1, BT2 and BT3 (all around **12:00Z**). It is not clear whether this was because other Blue Teams were just better in defence or the Red Team members focusing on BT4-BT6 and BT7-BT9 were not so proficient. Even when user level compromise was achieved, Red Team could not escalate privileges to SYSTEM. On some Windows 7 systems, the 'bad guys' were kicked off after a few seconds of successful client-side exploitation.

4.2.5 Various Attacks

From other activities conducted by Red Team on Day 1, the following should be pointed out:

- Customer emails were successfully stolen after the compromise of mail.dmz.bluex.ex from the following Blue Teams: BT1 (**08:00Z**), BT8 (**08:18Z**) and BT9 (**08:20Z**).
- Availability attacks (PHP hash table DDoS) against web-shops shop.dmz.bluex.ex were conducted between **12:05Z** and **12:20Z**. These were reported successful against BT1, BT2, BT4 and BT6.

NB: for approximately two hours on Day 1, all Red Team IPs were NATed (network address translated) because of a configuration mistake with the firewall in the CCD COE control room. Red Team could not touch any systems on Blue Team networks where the address 10.32.2.33 had been blocked.

4.2.6 Business Injects

The following additional tasks were given to the Blue Teams on Day 1:

1. A customer sent an email to sales@int.bluex.ex requesting to host a new website.
2. The customer asked for clarification about the security of their data, after reading an alarming article in the press.
3. Journalists asked the Blue Teams to provide comments to the press about the incidents, notably defacements. The Media Team then published stories in the news portal based on these answers.

4.2.7 Conclusions for Day 1

The main conclusions from the first day were:

1. Web attacks were successful against all the teams, although some of them were much more difficult to hack.
2. It was not specifically measured how long it took to detect and recover from attacks, but this would be important when estimating real business impact.
3. BT1 was always targeted first, giving them less time for prevention.
4. Blue Teams which had their systems down, either through their own or Green Team's fault, were initially higher in the scoring table. However, they still faced most of the same attacks later when the systems were brought online.

4.3 Day 2

4.3.1 Introduction

Day 2 started with a presentation of the previous day's activities by Red Team. Unfortunately, the GoToMeeting session had serious performance issues and Blue Teams could hardly understand it. VPN was opened at **07:20Z**.

4.3.2 Web Attacks

The following defacement campaign was executed on Day 2:

1. A fourth round of defacements lasted from **08:35Z** - **09:55Z** and targeted portal.dmz.bluex.ex and www.dmz.bluex.ex. All but BT3 were hacked. According to reports, BT5 was compromised 50 minutes later than the previous team. This could again indicate that, until this point, their web application firewall was not fine-tuned enough and code fixes did not help to stop the attacks, only delayed them.
2. The fifth and final round of defacements started at **11:00Z**. Within several minutes, the customer portals, www sites, webmail servers and web shops of BT7, BT2, BT9, BT1, BT6, BT4, BT8 and BT3 fell again... however, BT5 survived!

According to reports, the customer database on portal.dmz.bluex.ex was stolen only from BT9 (**08:30Z**) and BT1 (**11:00Z**). Based on our intelligence sources, the attacker who left behind a signature 'Nuri' had some special feelings against BT9. Therefore there is good reason to doubt whether these attacks followed the 'equally balanced' principle and were, in fact, coordinated with Red Team leader.

4.3.3 Network Attacks

A second round of configuration stealing from network devices was initiated at **09:10Z** on Day 2. In 40 minutes, BT1, BT2 and BT9 had their routers (routerx.sroute.ex) owned again. In addition, this time the objective was also accomplished against BT4 and BT6. From a technical perspective, the attacks were rather trivial. Routers were accessed over SSH due to an unchanged password (BT9), or using SNMP with initial read-write community name ('cdx12'). It is known that at least BT4 fixed its device so that, after **10:30Z**, Red Team did not get any more access.

4.3.4 Client-side Attacks

The Client-side team continued to target Windows hosts in the INTERNAL Zone. Their main goal was to keep persistent access in order to have the capability to steal the VNC password of SCADA components, and use the workstation to access SCADA at a specific moment.

On the morning of Day 2, the Red Team could get access to BT1, BT2, BT4 and BT9 machines. Blue Teams had deployed various anti-malware solutions which made standard tools like MSF or SET fail. It was possible to defeat the Blue Teams with encoded payloads, but BT2 and BT4 discovered the attackers in a few seconds and killed the sessions. Red Team still had SYSTEM level privileges on BT1 and BT9 and started keyloggers. The workstations of BT3, BT7 and BT8 were not available for exploitation attempts.

4.3.5 SCADA Blow-Up

All Blue Teams had to jointly protect a lab SCADA installation which simulated the process of controlling conditioners in the Blue Teams' shared data centre. The default rule set of the firewalls allowed access to the components (HMI, control PC and development PC) over VNC only from one workstation in each Blue Team INTERNAL Zone. In fact, all the Blue Teams could do was to keep Red Team out of those workstations and protect the shared VNC password. The White Team was role-playing as a SCADA administrator who periodically logged in.

By **10:00Z** on Day 2, Red Team had managed to install a keylogger into the workstation in BT1 network and steal the SCADA password. At **11:30Z** a 'David Hasselhoff attack' was conducted (the background image of HMI was modified) and, 10 minutes later, the system was 'blown-up' from

BT4’s workstation. Red Team had also maintained access through BT6 and BT9’s Windows XP machines. Therefore, altogether four out of nine teams failed to protect the SCADA.

4.3.6 Breaking the Infrastructure

The second exercise day put the gaming environment under serious test. There were two major breakdowns when the number of blades hosting the VMs became overloaded. Most of the systems were not accessible or usable. The network traffic-capturing infrastructure was not designed to handle high traffic peaks.

1. The first downtime started around **09:50Z**. The game was stopped and, at **10:00Z**, players were advised to go for lunch. The exercise continued at **11:00Z** after all Blue Teams had confirmed their systems were accessible again.
2. Later, there were two other short periods with load issues, both caused by the activities of Red Team.
    a. There was a miscommunication between Red and White Teams: uncertainty regarding the phrase ‘all attacks are allowed’ during the mayhem phase. Red Team was still expected to follow Rules of Engagement. Particularly, they were not expected to start DDoSing but this was exactly what happened.
    b. Red Team created a routing loop on purpose inside the SROUTE segment by injecting fake OSPF routes. As Green Team had not defined traffic limits on virtual network interfaces, the blades were again overloaded.

4.3.7 Various Attacks

From other Red Team activities, destroying the mail servers in DMZ (mail.dmz.bluex.ex) and customer portals (portal.dmz.bluex.ex) were directly scored. Mail servers were taken over and ‘shredded’ from BT1, BT2, BT4, BT8 and BT9, and portals from BT1, BT2 and BT7.

Red Team also conducted OSPF route injections to break the customers’ internet service. This resulted in a routing loop and high traffic peak, affecting the whole exercise infrastructure.

Red Team had prepared Linux workstations mimicking an unauthorized contractor's laptop infected with malware and plugged into the INTERNAL Zone. The malware tried to phone home over the DNS tunnel. This method was not successful. For instance, BT7 did not even lease an IP address to the machine. BT8 noticed an abnormal amount of DNS traffic and killed the tunnel.

4.3.8 Business Injects

The following additional tasks were given to the Blue Teams on Day 2:

1. A customer contacted a Blue Team to host a new website (repeated).
2. A Data Protection Agency requested information regarding if there was any sensitive personal data that could have been compromised.
3. Blue Teams were interviewed by telephone. This did not add much pressure because the situation regarding defacements and data theft had not escalated to the public. SCADA attacks could have made a good story but occurred too late for media involvement.

4.3.9 Conclusions for Day 2

1. Custom web applications were so vulnerable that eight out of nine Blue Teams could not avoid successful hackings.
2. Problems in infrastructure interrupted the game a few times.
3. The SCADA scenario was probably too artificial to have all the Blue Teams seriously focusing on it.
4. Standard anti-malware tools and good monitoring made the client-side attacks less successful.

4.4 Blue Team Defensive Actions

During LS12 it was not observed that any Blue Team came up with unique methods or techniques to prevent, detect and mitigate the attacks. This is a little in contrast to Baltic Cyber Shield 2010, where the winners from Sweden were the only Blue Team who did not use any patching but decided to focus on hardening, white-listing and, in general, locking the systems down. The following, mostly standard, practices were used by LS12 Blue Teams. It should be noted that the list is only based on the feedback forms and reports received from the teams, and not on detailed technical analysis.

- Patching the systems.
- System hardening:
  - Securing the configuration of applications and services.
  - Applying security-related Group Policies.
  - Disabling unnecessary modules. Removing unnecessary services.
- Hardening firewall rules, installing software firewalls on systems, blacklisting Red Team IP addresses (scans, login brute-force attacks, exploitation attempts, malware C&C servers, IPs learned from others).
- Changing passwords. Replacing weak SSH-keys (that were generated on vulnerable Debian distribution).
- Enhancing access control. Removing unnecessary user accounts. Running password audits. Changing file permissions.
- Removing most critical services from initial VM images to own trusted VMs. Substituting vulnerable services with other vendor's products.
- Scanning networks and web applications for vulnerabilities: Nessus, Appscan, Netsparker
- Finding and removing backdoors and rootkits (KBEAST, PHP shells).
- Protecting workstations with antivirus software and detecting malicious behaviour with different monitoring tools: Security Task Manager for Window, System Explorer, ESET Smart Security, MS Security Essentials, hosts3d.
- Network traffic monitoring: tcpdump, Wireshark, Colasoft Capsa,...
- Collecting and analysing security events and logs: Splunk, OSSEC,...
- Collecting and analysing netflows.
- Deploying IDS/IPS systems: Snort.
- Monitoring network services: Nagios.
- Securing web applications:
  - Using Web Application Firewalls (WAF): mod_security, WAF based on NGINX.
  - Filtering of malicious input with quick hacks.
  - Fixing vulnerabilities in code.
  - Placing reverse proxies in front of the application, rate-limiting to prevent DoS attacks.
- Using custom scripts:

    - Triggering alerts when the web-page was changed (checking the integrity of home page).
- Sharing information with each other: detected attacks and malicious IP addresses, tips for quick fixes of vulnerabilities, found backdoors.
- Fooling the Red Team with fake service version numbers (BT6).

Some teams, especially BT7, also ‘fixed’ problems by removing functionality (access to vulnerable Perl or PHP scripts was disabled). This was not allowed according to the rules but the White Team was too overloaded to penalise all such activities.

4.5 Information Sharing

This section describes what kind of information Blue Teams were sharing with each other through WT-CERT or directly on CDX12 Blue chat channel. In general, notifications about found vulnerabilities, backdoors, detected attacks and attacker's IP addresses were exchanged. A few Blue Teams also provided hints on how to (quickly) fix the problems. It is interesting to note that some backdoors were reported several times by different Blue Teams, which indicates that the information was not always effectively picked up.

On Day 1, BT5 and BT7 were most active. During the next day, BT5 continued to be the number one contributor, both in terms of quantity and quality of hints. A proposal was made by BT3 to change the password of scada.ex. However, there was no active response from others, similarly to the proposal to secure OSPF route exchanges.

4.5.1 Day1

BT1:

1. Netcat was running on mail.int.
2. mail.int had listening shell on port 31337 which was configured in `/etc/inetd.conf/`.
3. shop.dmz was defaced from 10.32.2.33. Make sure that customers can't upload PHP files through the feedback form.
4. We found an ICMP backdoor (`usr/bin/ppm4i`) on our webmail server. Someone (damn you RTs) had used it with root permissions.

BT2:

1. Block IP 10.32.2.33 - Shop Attackers!

BT3:

1. The SSH service on firewall.bluex.ex has to be updated to newer version (5.9p1).
2. We believe that the Router Attack could be due to OSPF route Injection and man in the middle attack. Therefore we propose as solution to protect the OSPF route exchange with a shared key between all the Blue Teams.

BT4:

1. 10.32.139.217 is scanning our 10.4.0.24 www.dmz reported by SNORT.

2. shop.dmz.bluex.ex is attacked by uploading PHP file named ‘`conf.php`’ using the feedback forms.

BT5:

1. KBEAST rootkit was running on DNS server on port 13377. Remove it by editing the grub config: `/etc/init.d/grub-common` and blacklisting the kernel module.
2. We got shellcode exploits to our internal clients from 10.35.255.10.
3. Possible drive-by exploits on 10.21.0.4, shellcode detected!
4. Add to blacklist: 10.32.2.33 continues to scan, enumerate and try to exploit web applications.
5. New Red Team IP tries to flood log files by brute-forcing SSH: 10.32.1.32.
6. Hint from BT5 to BT4: to fix your shop.dmz quickly insert this in `addFeedback.php`, line 10

   ```
   if (! preg_match(“/(txt|gif|png|jpg|jpeg)$/I”, $_FILES['image']['name'] ))
   die(‘Sorry, filetype not txt, gif, png, jp(e)g’);
   ```

7. Advisory on avoiding path traversal. We implemented a small handmade proxy tool in Python that parses the HTTP and HTTPS protocol. We check for path traversal attacks with a simple regular expression that counts “`\<..\>`”.
8. 10.35.255.10 is probing port 80 in the whole 10.x.0.10 range. We are going to block this IP.

BT6:

1. We still see 10.32.2.33 hitting various services on our networks.

BT7:

1. Windows 7 is installed in Test Mode. This allows install any software even if it is not signed by Microsoft.
2. Wordpress installed on www.dmz has backdoors in the code. Check:

   ```
   /var/www/wordpress/.mysql.info.php;
   /s1.php; s2.php;
   wp-includes/class.wp-db.php.
   ```

3. SSH version installed on the systems has well-known vulnerability. It's vital to patch. It's is very easy and fast to exploit it.
4. Nearly all the third party software installed on the workstations is outdated and must be upgraded. Well known exploits are available in Metasploit.
5. There are external IPs which are trying to attack to our systems. Blacklist: 10.32.3.33; 10.32.139.228.
6. Add to blacklist: 10.32.2.33.
7. Add to blacklist: 10.34.18.119: possible SQL Injection.
8. New scans detected from IPs 10.32.0.2 &ip 10.32.0.5, add to blacklist.
   - These were in fact some IPs used by the scoring bot...
9. Detected new IP scanning our network: 10.4.32.2. We are going to block it.
10. To BT2: detected new IP scanning our network: 10.20.0.2 (BT2 FW). Are you launching these scans?
11. Workaround how to quickly fix web defacement from Janitors hacking group. Replace line 182 in `wp-login.php`wordpress with

    ```
    if ( empty( $key ) || is_array( $key ) )
    ```

BT8:

1. There is a malware hosting site on http://10.35.153.32 including files new.exe (Rozenatrojan).
2. Attacker from IP 10.32.139.217 is connecting to www.dmz.blue7.ex to gain access using backdoors.
3. There is a malware hosting site on http://10.34.18.133, including a variant of 'Win32/Rozeta' trojan.
4. There is another solution how to hot-patch net-tools script on portal.dmz.bluex.ex - Perl regexp:

$addr =~ /^([a-zA-Z0-9\.])+$/

4.5.2 Day2

BT1:

1. An attacker (10.32.56.176) tried PHP injection attack against our web shop. After very short investigation we did not found any signs of successful actions.
2. One fix for shop.dmz: protect the feedback folder with .htaccess that turns PHP off. One thing they are trying is to upload PHP file via feedback that messes up with index.php and MySQL tables.
3. Source 10.32.139.213 attacks our web shop. Tries to overflow Apache.
4. 10.32.139.219 is trying to attack our portal through SQL injection.
5. 10.35.153.20 attacks our portal, PHP injection, tries to delete files.
6. We found netcat at var/www/portalnc-c 10.32.139.218.
7. Web pages of our portal were defaced through tbl_update.php in /var/www/portal/phpMyAdmin. Attacker's IP was 10.35.153.20.

BT2:

1. Attention to the vmgate, we were defaced!
2. We found authorized_keys in /root/.ssh which were not one of ours keys. Maybe it would be better to delete it.
3. Ongoing attack against our shared-web.dmz from 10.35.153.44.

BT3:

1. For safety reasons we propose to change the (shared) system password for scada.ex.

BT4:

1. Another vulnerability in mail.dmz.bluex.ex: user al.bundy with valid password.
2. In portal.dmz it is possible to inject PHP code through cooky in feedback.php on line 45: eval($ cookie['C']). Second vulnerability in portal.dmz: SQL injection in track_fault.php. Fix intval($phone_nr).
3. We found a Perl backdoor in /tmp/bdpl on www.dmz.
4. To BT9: we detected some login attempts on our servers from your IP range (10.9.32.9). Please check for potential compromise.

5. The shared-web.dmz sees several attacks. We set up mod_security on it and now see some of the web attacks in its log.

BT5:

1. To patch your RUNNING kernel against local root exploit on webmail.dmz and mail.dmz run as as root the following commands:

   ```
   wget  http://www.ping.uio.no/~mortehu/disable-vmsplice-if-exploitable.c
   gcc  disable-vmsplice-if-exploitable.c -o disable--exploitable
   ./disable-exploitable
   ```

2. Until we got to the root cause of defacements on webmail.dmz we did the following as root:

   ```
                # chattr +A /usr/share/squirrelmail/src/login.php
   ```

3. There are 'legacy' users like test, tst or admin2, they have a shell. And they are coming back. Workaround is to add an entry in crontab:

   ```
      * *   * * *   root    usermod -s /usr/sbin/nologintest ;pkill -U 1003
   ```

   where the number is the PID of the user.

4. ProFTP with backdoor on www.dmz. Easy fix for all:
   a. install Vsftp and at same time disable Proftpd--> so you have a minor outage of 1-2 secs (it's like an hickup of the network)
   b. update-rcproftpd disable --> so it doesn't come up at next reboot anymore
5. To disable random users on chost.mgmt to sign up to the VM upload system (without banning existing users), you can edit the file/opt/web2py/applications/uploadvm/models/db.py by doing:

   ```
             s/auth.settings.registration_requires_verification =
             False/auth.settings.registration_requires_verification = True/
   ```

6. To find unauthorized users on chost.mgmt you can go to /opt/web2py/applications/uploadvm/databases/ and edit the users database:

   ```
              $ sqlite3 storage.sqlite
             select email from auth_user where email not like '%cust.blue%';
   ```

   Then delete the users which pop up.

7. Will we do auth on OSPF?
8. 'GET /phpMyAdmin/tbl_update.php?f=system&v=cp%20/tmp/d%20/var/www/portal/index.html HTTP/1.0' 200 244 '-' 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:11.0) Gecko/20100101 Firefox/11.0'.
   We recommend to disable resource in sites-enabled:

   ```
   <Directory /var/www/portal/phpMyAdmin>
   AllowOverride None
       Deny from all
   <Directory>
   ```

9. DoS attack to firewall! We're facing heavy DoS Attack on our Firewall.
10. Preventing upload of unwanted files to the private contract area can be fixed by applying the following patch on `/var/www/portal/private_customers/contracts.php`:

```
if (filesize($_FILES['uploaded_file']['tmp_name']) == 0) {
return 0;
}else{
if (! preg_match("/(\.pdf)$/i", $_FILES['image']['name'] )) die("Sorry pdfs only");
  }
```

11. We hardened php.ini file on portal.dmz and shop.dmz by changing the display_errorsconfig variable to 'false'. It is set to 'true' by default and can help attackers to learn inside information about our production code.

BT6:

1. We discovered a backdoor on mail.dmz running on tcp port 31337 giving a `/bin/sh` shell. It was set up in the `inetd.conf` file. It was fixed by commenting the lines out and restarting inetd.
2. We found a backdoor on DNS server: kbeast v.1 kernel rootkit found running and listening on TCP port 13377. Removed the startup entries (kernel module) hidden in `/etc/rc4.d/S99grub-common` and deleted the rootkit itself from `/usr/_h4x_/*`. This hidden rootkithave features such as keylogger, more info here: http://core.ipsecs.com/rootkit/kernel-rootkit/kbeast-v1/.
3. ProFTPd daemon on www.dmz is running a backdoored version (1.3.3c) which gives attackers root shell when doing a 'HELP ACIDBITCHEZ' command without any credentials needed. Upgrade or patch the vulnerability. ProFTPD was upgraded to newest version but kept the old version number for fooling attackers.
4. Be aware that the kernel on webmail.dmz is vulnerable to a local root exploit (vmsplice).
5. Regarding attack on BT6 portal.dmz. When researching the incident we also uncovered reconnaissance and attack using the following IPs/domains 10.11.32.2, 10.35.255.9, 10.32.2.33, http://10.35.255.9/x/, http://elar.lap.ee/glogo.png (real internet).
6. Webmail server has been defaced by (janitors). They deleted files that require root access.
7. Vulnerability in shop.dmz. We fixed website against file injection attempts in the `addFeedback.php` file. Limited type of uploaded files to only include image and txt files.
8. Attacks on our portal from 10.32.139.216.
9. We've seen attacks against our shared-web.dmz (failed so far) today from 10.34.18.119. He seems to have been using Perl to script his attack and is hiding his useragent poorly (adding ‘‘ in the UA and removing spaces).

BT7:

1. Warning: scan from IP 10.32.139.219 using Havij SQL Injection Tool.
2. Backdoors used to access confidential information in portal. Check this!
3. 10.35.153.21 is trying to access vmgate.dmz.
4. New attacks from 10.33.37.36, 10.9.32.10, 10.35.153.44.
5. To BT9: your IP 10.9.32.10 is trying to attack us using SQL injection.
6. We detected attack on www server using a backdoor located in `/var/www/wordpress/wp-content/themes/twentyten/general.php`. Attackers who used this backdoor: 10.32.139.204, 10.32.139.228, 10.34.52.212.

BT8:

1. Administrators of portal.dmz: check files in `/var/www/portal/templates_c/`. We found some backdoors. Fix this vulnerability via php.ini:

   ```
   /usr/local/lib/php.ini:
   disable_functions  = phpinfo, dir, readfile, shell_exec, exec, dl, virtual, passthru,  proc_close, proc_get_status, proc_open, proc_terminate, system, curl_multi_exec,   parse_ini_file,   show_source,   apache_child_terminate, apache_setenv,  define_syslog_variables,  escapeshellarg,  escapeshellcmd, eval, inject_code
   ```
2. Administrators of portal.dmz. It is fine to setup mod_security and apply small patch to `/var/www/portal/index.php` on line 2:

   ```
   error_reporting(0);
   if (eregi('(system|\.\.|passwd|union)',$_SERVER['REQUEST_URI'])) die();
   ```

3. We have noticed our ISP partners are using net-tools with vulnerability. We would like to share a simple patch with them: portal.dmz.bluex.ex, file `/usr/lib/cgi-bin/net-tools`, add to line 133 this text

   ```
   if ($addr =~ /^([a-zA-Z0-9\.])+$/) {‘, on line 140 ‘}’
   ```

4. We have noticed our ISP partners are using web shop with vulnerability. We would like to share a simple patch with them: shop.dmz.bluex.ex, file `businesslogic\cartManager.php`

   change line 20 from ‘`$this->id=$idIn;`’ to ‘`$this->id=intval($idIn);`’.

5. Configure passive-interface for vlan10 and ethernet0/0 on your routerX.sroute.ex to prevent accepting neigbourship from the host in VLAN10. BT9 floods us with fake routes.
6. There is a backdoor in `/var/www/portal/private_customers/contracts/d2.php`. Maybe some team has not fixed it yet.

BT9:

1. Red Team is attacking our portal, SQL Injection, 10.32.139.219.
2. Red Team is attempting reverse shell at 10.x.0.25 from 10.35.153.33.
3. 10.32.56.176 attacked our webshop too.
4. We were also scanned by Havij from the same IP 10.32.139.219.
5. Appears 10.35.153.20 is trying multiple logins to portal.
6. Attacks on our portal.dmz from 10.35.153.20, exploiting `d2.php` to deface (we removed this yesterday but it came back) and ‘malicious picture’ served from 10.35.255.5

4.6 Scores

The following teams ended up in the top three on the LS12 scoreboard:

1. BT5
   - Highest availability score.
   - Best at reporting incidents to CERT. A lot of very detailed Lightweight Human Reports. Very good at sharing their fixes with other teams.
   - Second best at reporting to management (Executive Reports).
   - Best at web-application security.
2. BT8
   - Best at reacting to business injects.
   - Second best in terms of negative points assigned for successful attacks. However, also considerably low availability.
   - Most active team during preparations.
3. BT7
   - Fewest negative points assigned for successful attacks. However, they had also very poor availability, making many objectives impossible for Red Team to reach.
   - High score for CERT reporting.
   - Good information sharing.
   - No disk resets requested.

5 Situation Analysis Based on Lightweight Human Reporting

Lightweight Human Reporting was a concept brought to the exercise by the Finnish Yellow Team. The analysis in the current chapter has been written by an expert from Clarified Networks, the company that was primarily behind the idea and its implementation.

5.1 Event Categories

Based on the information provided in the human reports, we tagged the team reports to more generic categories. Below are the most common activity types and the number of corresponding Blue Team reports.

Category	Count	Description
defacement	51	Defacement is an attack on a website that changes the visual appearance of the site or a webpage.
exploitation attempt	46	An exploitation attempt is an attempt to break into resources without confirmed success.
backdoored	38	The term backdoor refers to a method of bypassing normal authentication and ensuring remote access to a computer.
scan	30	Enumerating potentially vulnerable services.
DoS	21	An attempt to make a computer or network resource unavailable to its intended users.
brute-force	17	Brute-force attacks are an application of brute-force search, the general problem-solving technique of enumerating all candidates and checking each one. As the reports rarely indicated the number of attempts, this analysis covers all trivial attempts to discover usernames, passwords or other necessary for attacks.
user accounts	13	Unauthorised user accounts found from the system
compromise	10	An attacker has gained access to a resource. See also backdoored, which could be the natural consequence of compromise.
SQL injection	9	An SQL injection is often used to attack the security of a website by inputting SQL statements in a web form to get a poorly designed website to perform operations on the database.

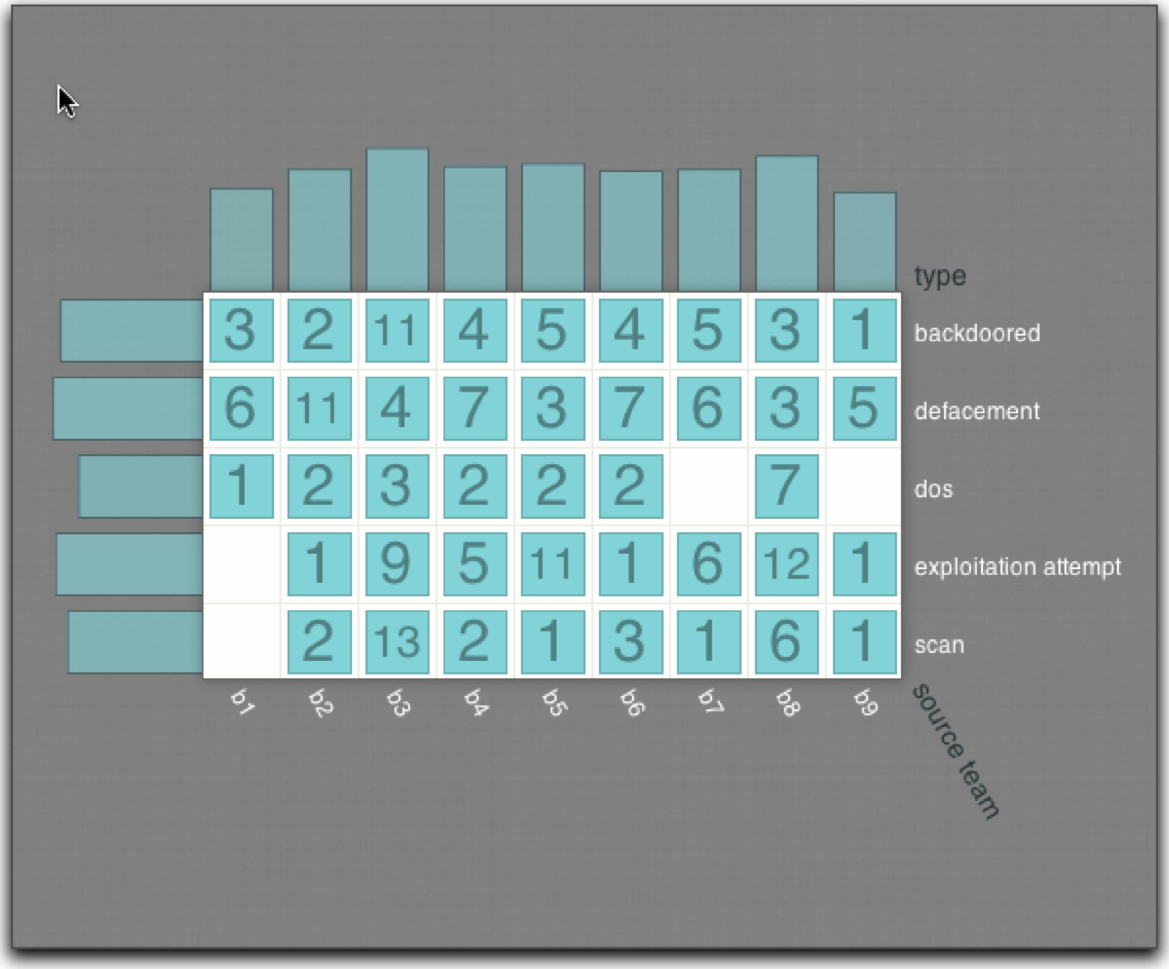
5.2 Observations from the Perspective of the Control Room Analyst

The analysis below is written from an in-game perspective, to reflect the point of view of a control room analyst.

As the Report Type Distribution #1 (below) shows, hacktivists have carried out a large defacement campaign against all teams (ISPs). Furthermore, due to the high number of reports regarding backdoored machines, we suspect that another group is targeting us with another objective. We estimate that cyber criminals with a financial motivation, or a state actor with a focus on espionage may be behind these attacks. Denial-of-service (DoS) activity has been ongoing for several months and, with few exceptions, is not affecting our normal operations.

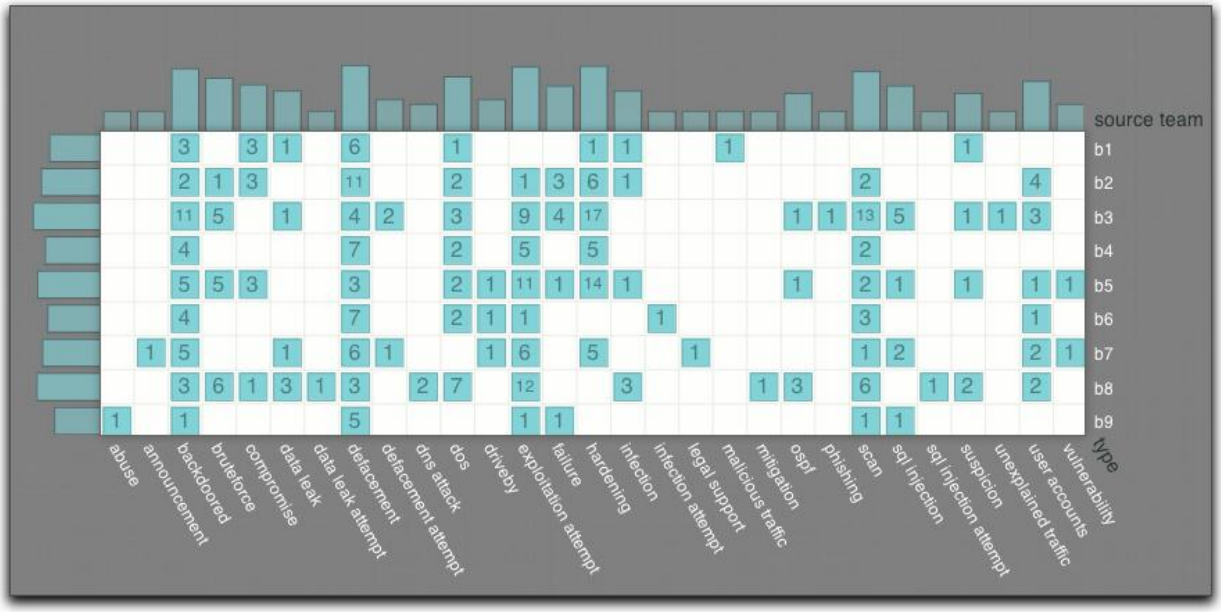
Defacements and successful backdoor installations have been discovered by all teams. Few teams have not reported other common attack types, such as DoS, failed exploitation attempts or scanning activity. We have contacted these teams and advised them to monitor more closely these types of malicious activity.

A wide variety of malicious activity implies that either a large number of different groups have activated at the same time or, alternatively, there are one or two large and loosely coordinated groups attacking us.



type	b1	b2	b3	b4	b5	b6	b7	b8	b9
backdoored	3	2	11	4	5	4	5	3	1
defacement	6	11	4	7	3	7	6	3	5
dos	1	2	3	2	2	2		7	
exploitation attempt		1	9	5	11	1	6	12	1
scan		2	13	2	1	3	1	6	1

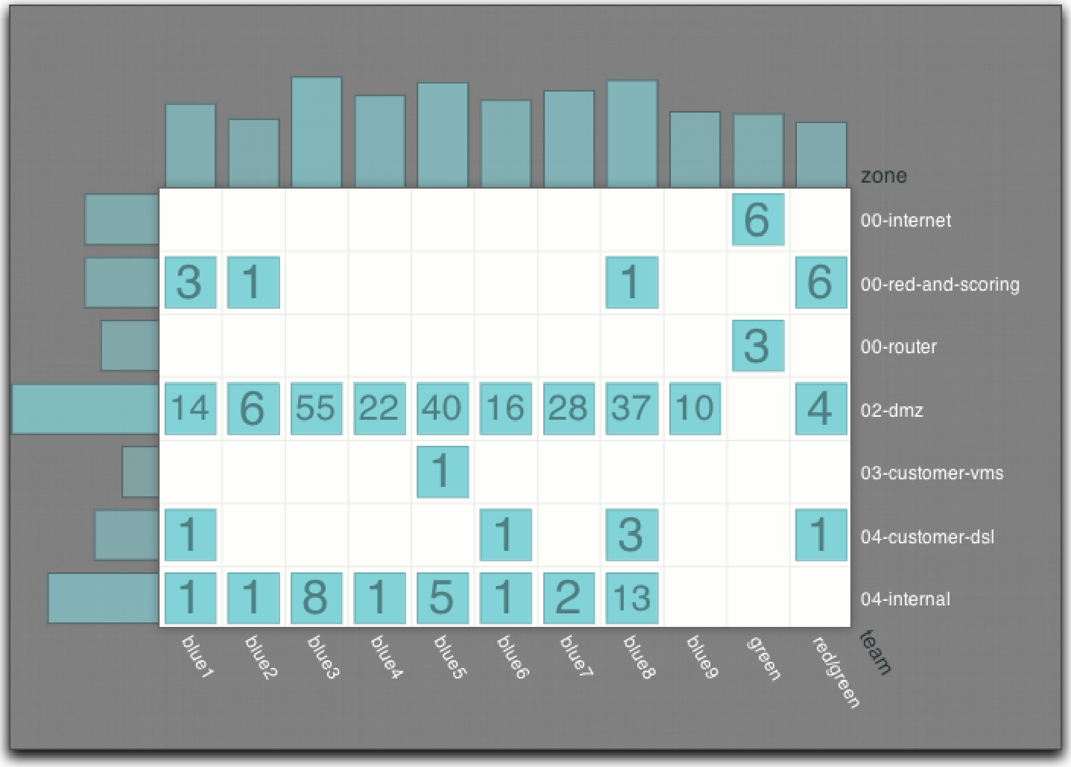
Report Type Distribution #1: *Almost all teams observed almost all common attack types.*



	abuse	announcement	backdoored	bruteforce	compromise	data leak	data leak attempt	defacement	defacement attempt	dns attack	dos	driveby	exploitation attempt	failure	hardening	infection	infection attempt	legal support	malicious traffic	mitigation	ospf	phishing	scan	sql injection	sql injection attempt	suspicion	unexplained traffic	user accounts	vulnerability
b1			3		3	1		6			1				1	1			1							1			
b2			2	1	3			11			2		1	3	6	1							2					4	
b3			11	5		1		4	2		3		9	4	17						1	1	13	5		1	1	3	
b4			4					7			2		5		5								2						
b5			5	5	3			3			2	1	11	1	14	1					1		2	1		1		1	1
b6			4					7			2	1	1				1						3					1	
b7		1	5			1		6	1			1	6		5			1					1	2				2	1
b8			3	6	1	3	1	3		2	7		12			3				1	3		6		1	2		2	
b9	1		1					5					1	1									1	1					

Report Type Distribution #2: *Trends over all malicious activity*.

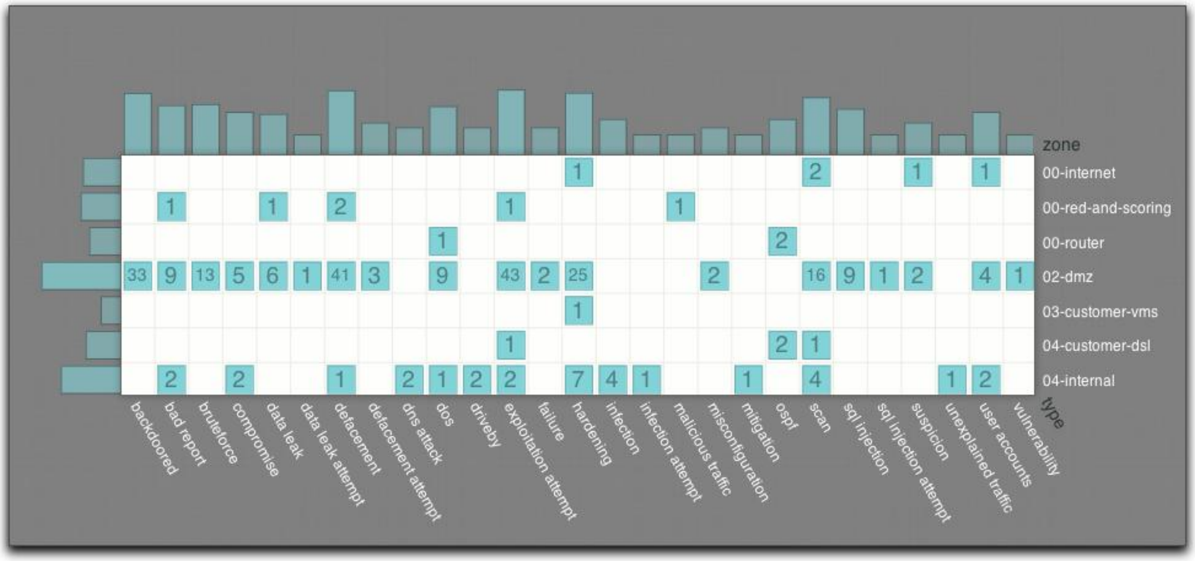
Report Type Distribution #3 (below) shows that most of the discovered attacks have focused on the demilitarised zone (DMZ). Typically, our organisations do not store their most confidential information in the DMZ. As a result, our losses are mostly attributed to negative PR impact and the availability of specialist work, as the teams are focused on mitigating further loss.



	blue1	blue2	blue3	blue4	blue5	blue6	blue7	blue8	blue9	green	red/green
00-internet										6	
00-red-and-scoring	3	1						1			6
00-router										3	
02-dmz	14	6	55	22	40	16	28	37	10		4
03-customer-vms					1						
04-customer-dsl	1					1		3			1
04-internal	1	1	8	1	5	1	2	13			

Report Type Distribution #3: *Teams and zones.*

Even though most activity is focused in the DMZ, we deduce from the reports that attackers have gained a foothold in our internal networks and have conducted further reconnaissance (scans) or denial of service attacks (DoS). Our teams have already taken proactive actions (hardening) of our internal networks.



zone	backdoored	bad report	bruteforce	compromise	data leak	data leak attempt	defacement	defacement attempt	dns attack	dos	driveby	exploitation attempt	failure	hardening	infection	infection attempt	malicious traffic	misconfiguration	mitigation	ospf	scan	sql injection	sql injection attempt	suspicion	unexplained traffic	user accounts	vulnerability
00-internet														1							2			1		1	
00-red-and-scoring		1			1		2					1					1										
00-router										1										2							
02-dmz	33	9	13	5	6	1	41	3		9		43	2	25				2			16	9	1	2		4	1
03-customer-vms														1													
04-customer-dsl												1								2	1						
04-internal		2		2			1		2	1	2	2		7	4	1			1		4				1	2	

Report Type Distribution #4: *Activity types and zones.*

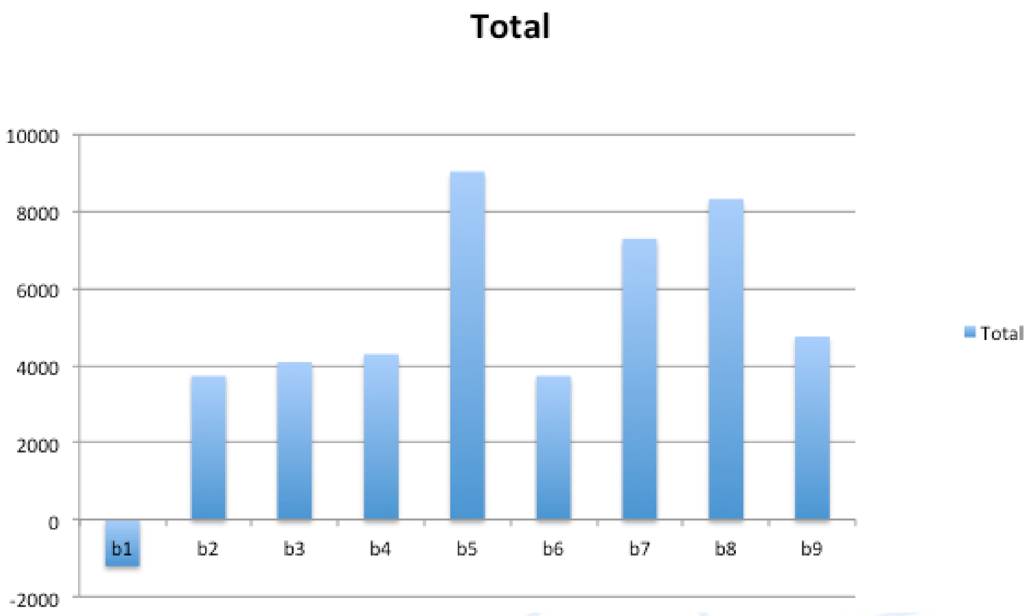
5.3 Viewing the Exercise: Strategy and Tactics

5.3.1 Introduction

One of the hypotheses was that, by introducing Lightweight Human Reporting to the exercise, some insight would be gained as to how the strategies and tactics of different teams worked in practice. In addition, we wanted to find out how the reports reflect a given team's overall skillset. Below are some example comparisons.

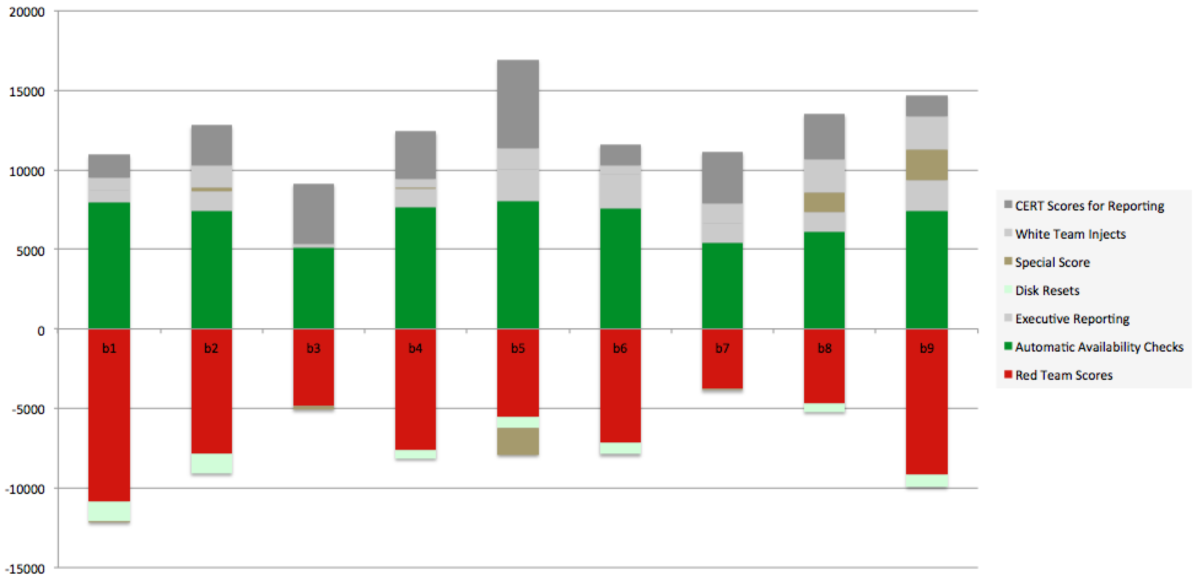
5.3.2 Total Scores

The Clarified Networks collaboration environment and VSRoom provided the technical solution to the scoring. To reduce the overhead of the White Team and to provide quick feedback to the Blue Teams, the scoring system was tightly integrated into the reporting system. Automatic service availability checks were also integrated into the overall scoring system.



5.3.3 Comparison of Team Performance

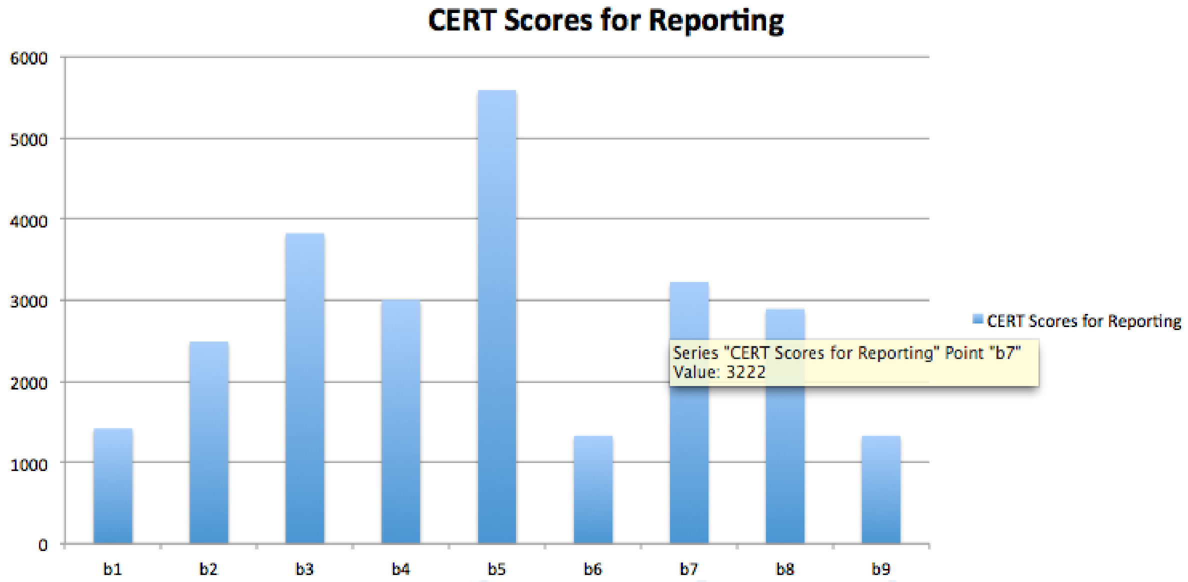
Surprisingly, the automatic availability check scores did not correlate significantly to a team's overall performance. Scoring differences were achieved with proactive work to mitigate the attack surface (to prevent successful Red Team attacks) and with the quality of the reporting. Additionally, BT9 got a rather significant reward (special score) from cooperating with other Blue Teams, as well as the exercise CERT team.



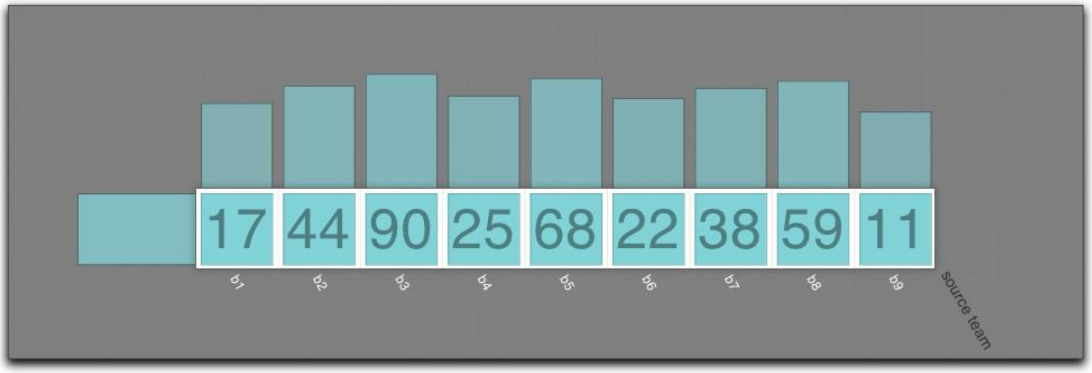
Performance overview: *An overview of team performance, based on various scoring categories.*

5.3.4 A Closer Look at the Quality of Human Reporting

BT5 and BT3 provided the best quality reports from the CERT team's perspective. BT5 obtained a higher score with smaller number of reports.



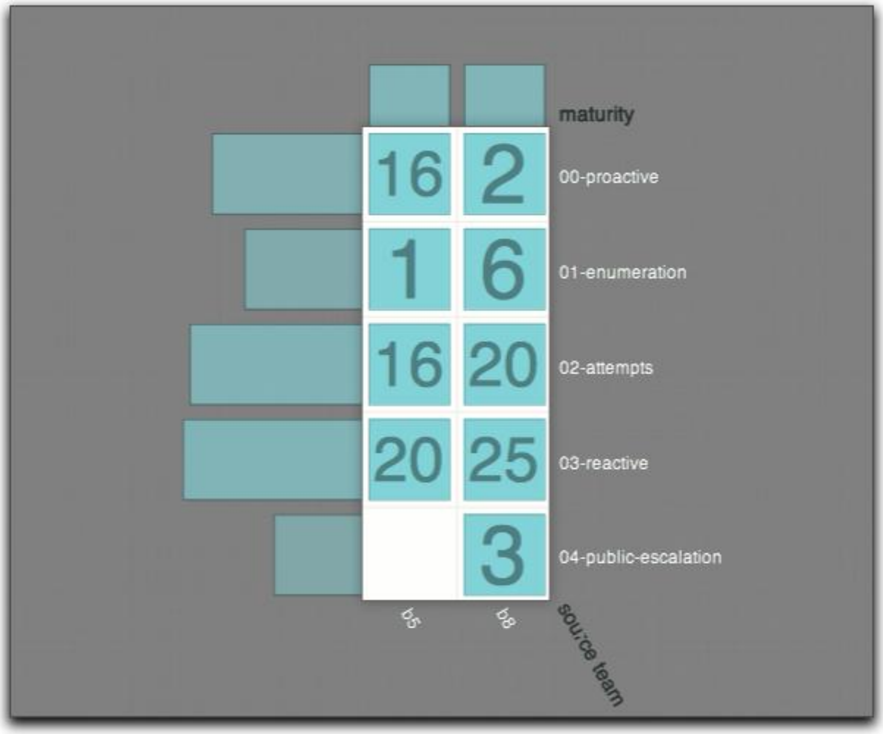
Human reporting performance: *Detailed view of the human-reporting part, which was within the focus area of the Yellow Team*



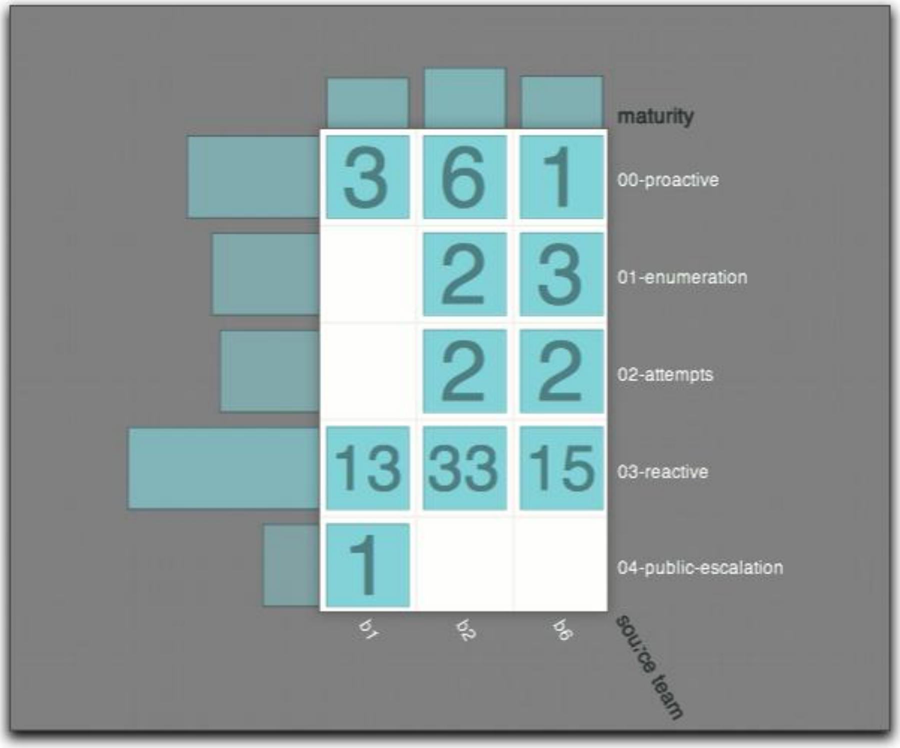
Reporting quantity vs quality: *Quantity was not enough. For example, a comparison of BT5 and BT3 reports shows that BT5 scored better with a smaller number of reports.*

5.3.5 Comparison of Top and Bottom Teams

The reports of the top teams (BT5, BT8) were more equally balanced between proactive measures (limiting attack surface, observing attacker enumeration methods and failed attack attempts), while the bottom two team reports were biased towards reactive reporting.



Reporting maturity: *The top teams' reports were balanced more equally between proactive and reactive measures.*



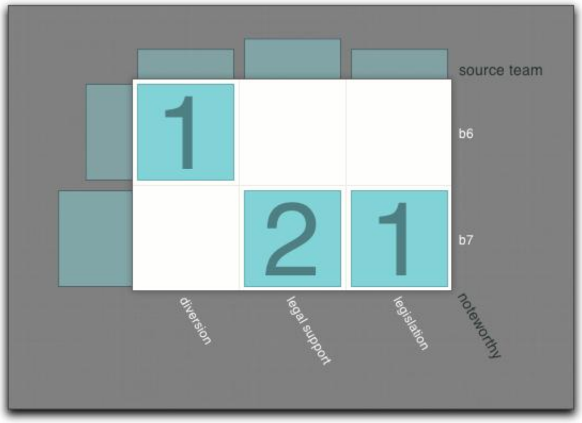
Reporting maturity: *The bottom teams' reports were mainly focused on reactive actions.*

5.3.6 Team Comments on Strategy and Tactics

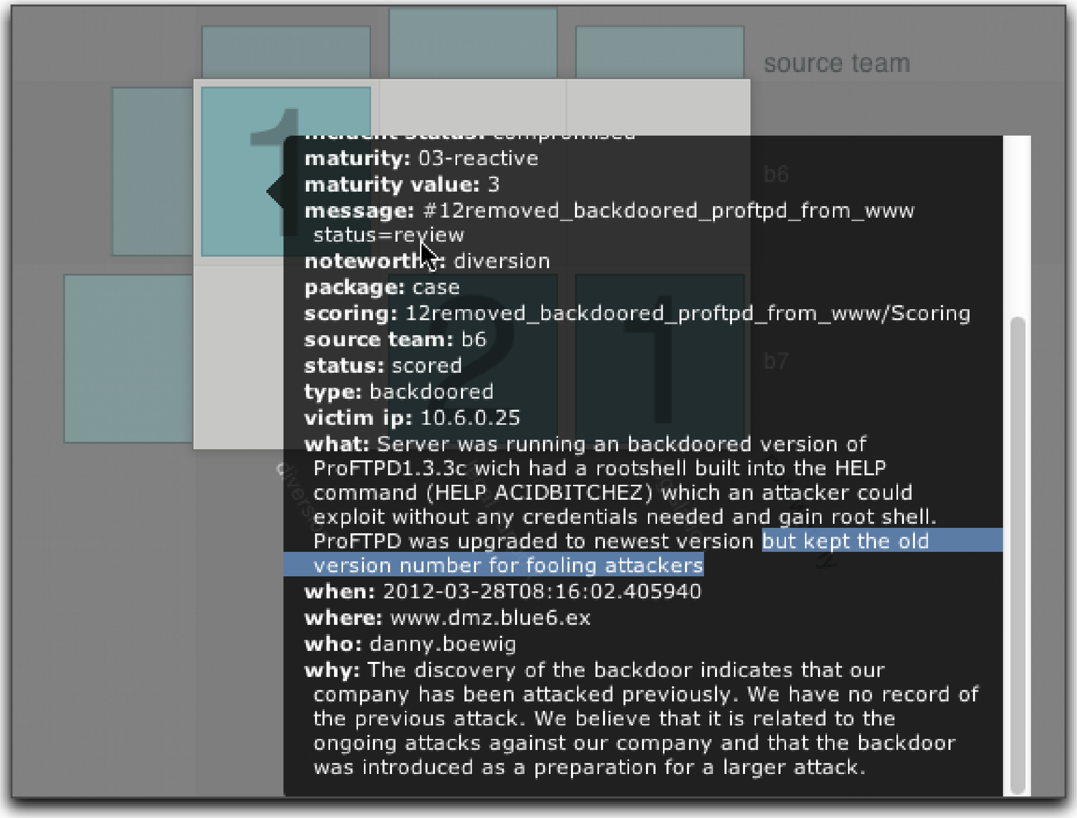
Team	Strategy/Tactics based on Feedback	Reflecting to Incident Reports
BT5	Comment: *Our strategy was: find vulnerabilities first and close them. We were not able to follow it.* Potential reason: *As some of our services did not work from the beginning (shared-web, VMgate) we tried to get them going. That deflected us a little bit from focusing on the attacks.*	The team reported many more proactive methods and failed attack attempts than the losing teams, so it seems that they were better off with their strategy than they think.
BT8	Comment: *During prep week, we had outlined a strategy from multiple points of view. We were able to follow it roughly but we had to adjust as well.* Adjustment: *We learned some things from the attacks and used them against attackers. We 'shifted priority' to machines according to attacks.*	This team reported the largest number of attack attempts, so the team's comment on learning from the attacks is in line with the reporting.
BT1	Comment: *We had a plan what we going to do, but Red Team totally destroyed that in the beginning.* Potential reason: *Our team was too much orientated to network side. We noticed already on Monday that we should have more unix and Windows server guys.*	It is likely that seven of the 14 reactive reports were a result of network observations. The number was deduced by the Yellow Team, based on the information provided in the BT1 reports.
BT2	No pre-planned strategy/tactics. According to BT2, the system matched their skillset.	BT2 exercised a moderate amount of proactive methods, mostly patching the systems. However, patching was not sufficient and a number of attacks succeeded.

5.3.7 Highlights

We would like to highlight that some of the teams demonstrated consideration beyond the technical aspects of this exercise. Examples of these findings are listed below.



Noteworthy items in reports 1: *BT6 used diversion to let attackers believe that they were still running a backdoored FTP-server. BT7 demonstrated consideration of the contractual and legal implications of their actions.*



```
incident status: compromised
maturity: 03-reactive
maturity value: 3
message: #12removed_backdoored_proftpd_from_www
 status=review
noteworthy: diversion
package: case
scoring: 12removed_backdoored_proftpd_from_www/Scoring
source team: b6
status: scored
type: backdoored
victim ip: 10.6.0.25
what: Server was running an backdoored version of
 ProFTPD1.3.3c wich had a rootshell built into the HELP
 command (HELP ACIDBITCHEZ) which an attacker could
 exploit without any credentials needed and gain root shell.
 ProFTPD was upgraded to newest version but kept the old
 version number for fooling attackers
when: 2012-03-28T08:16:02.405940
where: www.dmz.blue6.ex
who: danny.boewig
why: The discovery of the backdoor indicates that our
 company has been attacked previously. We have no record of
 the previous attack. We believe that it is related to the
 ongoing attacks against our company and that the backdoor
 was introduced as a preparation for a larger attack.
```

Noteworthy items in reports 2: *Drill-down on BT6 diversion.*

Report Name	Team	Noteworthy	What
12removed_backdoored_ proftpd_from_www	b6	diversion	Server was running a backdoored version of ProFTPD1.3.3c which had a rootshell built into the HELP command (HELP ACIDBITCHEZ) which an attacker could exploit without any credentials needed and gain root shell. ProFTPD was upgraded to newest version but kept the old version number for fooling attackers
25cookiestealing	b6	attribution	One of our green-zone clients (172.168.6.62) has visited BlueTeam 3 customer-portal, which has an injected Javascript that steals credentials from the login form and session cookies. This happened 2012-03-27 12:22 (UTC Time). They took the clients session cookie. The javascript named CarrietPigon was written by Elar Lang, and posted the information on http://10.35.255.9/x/store.php
b7-Incident19	b7	legislation 5.2	user 'user' exploits vmslice in server. The account has been deleted due to incompliance with current law.
b7-Incident23	b7	legal support	Unauthorized access to confidential information of our customers due to backdoors in the server. We have deleted these backdoor. Customers are going to be prevented. We are going to ask legal support to take the appropriate legal actions.
b7-incident24	b7	legal support	Defacement caused by the internal user 'manager' in www server He has downloaded an exploit to escalate privileges from http://git.zx2c4.com/CVE-2012-0056/plain/mempodipper.c He has modified the web with the file index.php. DEFACEMENT (below) which includes an image hosted in the server http://10.35.255.5/pics/Janitor_pink.jpeg We also include the file with the exploit he intended to run. Actions taken to fix that: block user notify legal department about the incident Index.php`<font size='+4'>nom nom nom...</font><br/><br/><imgsrc='http://10.35.255.5/pics/Janitor_pink.jpeg'>` the exploit he was intended to run mempodipper.c

Noteworthy items in reports 3: *Tabular representation, accompanied with links to actual reports.*

6 Observations and Recommendations to Improve Locked Shields

6.1 Objectives

1. The training objectives should be made clearer. Organisers should make sure that these are properly communicated to the participants.
   - A description of the Blue Team, including a detailed list of required roles and skillsets, had been previously provided in the first information package attached to the invitation to participate. Still, some teams missed that information or it was not clear enough.
   - A concrete suggestion made by one Blue Team was to make it clear whether the exercise is designed for system administrators or Computer Network Defence (CND) personnel.
2. Shifting the main training audience requires a redesign of the exercise. For instance, providing a good learning experience simultaneously for both Blue and Red Team members will probably not work.
   - The next exercise should clearly define the primary goal in terms of who is going to be trained.
3. Incident detection, analysis and reporting should have higher priority in future technical exercises.
   - Several Blue Teams found that LS12 was too focused on common system administration tasks.
   - The scoring system also favoured prevention more than detection and fast response. For instance, defacement generated a lot of negative points even if it was discovered and repaired within a minute and the ‘business impact’ could be considered low.
4. If PR managers are to be part of the training audience, specific training objectives have to be also clearly defined.

6.2 Exercise Organisation

1. More focus and time should be spent on giving feedback to the Blue Teams.
   - The environment that Blue Teams had to protect was complex and full of vulnerabilities. Therefore the Red Team's campaign was highly successful. Some Blue Teams expected full technical details on the attacks and suggestions on countermeasures they should have deployed.
   - For instance, at the end of Day 1, the Red Team could reveal information about vulnerabilities they had already exploited. There would be fewer successful repeat attacks and Blue Teams could then focus on new areas to gain more learning.
   - The Red Team should also share some of their attack scripts with the Blue Teams at the end of exercise.
2. Blue Teams need more ‘official exercise time’ for preparations.
   - Final documentation and access to the game environment was available for the Blue Teams one week before the Execution. Some teams missed that information. Some could not allocate time during the pre-CDX week for preparations.
   - Prolonging the CDX by one day should be considered. Alternatively, attempts could be made to solve the majority of communication issues before the official start. Then Day 0 would have less focus on solving access and communication issues and Blue Teams could spend most of Day 0 learning the systems, rules and testing out reporting channels.
   - A training day should be considered as part of the preparations week. This would help to get better reports and solve most access issues.

3. Two full exercise days should be devoted to gaming and short feedback sessions. Announcing final results, filling in feedback forms and participating in longer Hot Wash-Up meetings should be carried out on the next day.
   - After ENDEX was announced and the Red Team stopped attacking, the White Team still had many reports to evaluate. Therefore the final results on the scoreboard were not announced in the end of Day 2 as previously promised. In addition, it was common that several aspects of the scoring needed further investigation to ensure fairness.
4. The Test Run was very useful and necessary but needs to be prepared better next time. The exercise environment for the Test Run should be almost identical to the one used during Execution.
5. Zulu time (UTC) has to be enforced on all systems supporting the exercise and used in scheduling all events from the beginning of the planning process.
   - Most of the control cells of LS12 were located in Tallinn and Helsinki. Therefore the UTC+2 (and UTC+3) timezone was used when planning events, but UTC was configured on Blue Team systems. This worked fine until the Execution phase, when Blue Team members were confused.
6. The exercise timetable should be communicated at least one week before the start and last-minute changes should be avoided.
   - One Blue Team made a comment that the timetable was communicated too late and it was not obvious.
   - Another Blue Team was disappointed that, on Day 0, much less time was spent on explaining the setup, rules, scoring principles, etc., than was previously announced in the timetable.
7. CDX should be run multiple times on the same (refined) setup to improve return on investment. The focus should be on improving the learning experience and measuring.
8. The plans for data collection and other activities after the action should be improved.
   - Feedback forms and human reporting are not enough to draw firm conclusions about what actually happened, if the scoring was fair and if Red Team attacks were equally balanced. Network traffic and log analysis should be used to verify claims.
   - The current after action report does not include deep analysis and comparison of the strategy and tactics different Blue Teams were using.
9. Locked Shields should continue to be live-fire exercises. Detailed forensic analysis tasks could be conducted on the attacked systems after the exercise.
10. Small-scale exercises should be conducted as well, where it is feasible to require more from the participants.

6.3 Scenario and Injects

1. Although the exercise scenario and setup was considered good, the organisers should try to bring the game closer to the real world in the future.
   - The following lists some points made by the participating Blue Teams:
     - ‘Exercise itself was good but not realistic. Exercise would be more efficient if Blue Teams had at least one day to repair and prepare their systems. Situation where Red Team starts the attacks straight after we get access – we were too much behind of them. It's not realistic to start maintaining unknown environment just like that.’
     - ‘Good idea for the aims of the exercise.’
     - ‘Players are influenced by scoring a lot. In reality we would take our systems offline under such heavy attacks.’

        - ‘Having a scenario helps to build context for the attacks. This is very important.’
        - ‘The commercial ISP scenario did not really match the MoD profile of the players.’
        - ‘The fact it is a game does not allow real-world risk management and system hardening decisions to be made.’
    - The fact that the high-level background scenario was simple and had only a fictional country involved did not provide the Legal Team with an opportunity to have serious discussions.
2. Number of injects (media, customers, employees) should be increased.
    - In general, Blue Teams found the injects good and useful to make the scenario interesting and more varied.
    - At least three teams remarked that they had expected more injects:
        - ‘Media pressure and customer pressure were very light.’
        - ‘Not enough injects.’
        - ‘We were under the impression, that some of injects never reached us.’
        - ‘Media should cooperate with the Red Team to blame Blue Teams and force them to react.’
    - The teams were very responsive to media requests, meaning that the number of media injects could be increased in the future. Delays were caused because some of the teams were not expecting media inquiries on the specific email addresses.
3. Blue Teams should be required to report receiving injects.
4. More context and background about the scenario has to be provided to the players in order to introduce more management and strategic aspects to the exercise. More pressure from simulated management towards Blue Teams would also be required.
    - Red Team was supposed to play two different roles during the game - hacktivists and cyber criminals. According to Executive Reports, most of the Blue Teams related the attacks only occurred from one of the groups. It was not easy or possible to differentiate between the different attacks in terms of motivation or who was behind the attack. Three Blue Teams did not mention anything in reports to management about who was attacking them and why.
5. More information about the flags (targets, data) that Red Team is expected to compromise should be provided to the Blue Teams.
    - Even with some preparation time, the environment was still new and unfamiliar. Many Blue Teams had difficulties in even noticing that the database of their clients or secret memo documents had been stolen by attackers.
    - More detailed documentation could be provided emphasizing the important assets and giving more detailed feedback after successful compromises.

6.4 Situational Awareness

1. The wiki-based Executive Reporting (See Appendix H) worked well and should be used in the next exercises. The following issues need attention:
    - One team did not use the designated wiki-based form and saved the reports to another location.
    - The wiki-based form needs some modifications. For instance, reporting time-frames should be predefined and selectable from a drop-down list.
    - The purpose of the Executive Report seemed to be misinterpreted by some teams - they provided very a technical overview about the actions taken. ‘Techies’ need more training or guidelines on how to write good management reports.

    - The number of required Executive Reports was changed during the game and did not match what was said in the reporting instructions. This generated confusion, ending up with some Blue Teams providing three and some four Executive Reports.
    - Blue Team members were not familiar with the syntax of the particular wiki installation and therefore the reports themselves would have been better formatted when using text editors.
2. Feedback regarding the wiki and chat-based Lightweight Human Reporting was somewhat controversial. In general, it was considered a good idea by the Blue Teams. From the White Team's perspective, it greatly simplified the exercise control in gaining situational awareness and ensured the after-action analysis was much easier. This reporting method should be used again in future exercises.
    - One Blue Team was not happy with the Tweetbot and would have preferred a web application.
    - One Blue Team remarked that the chat channel was not easy to follow.
    - The 'Who' field in the report form caused some confusion, as the general description page was different from the one on the report form itself.
3. The frequency and quality of Lightweight Human Reporting should be increased. This applies also to reporting carried out by the Red Team.
    - LS12 Red Team reports usually do not provide any information on how the objective was achieved, what kind of vulnerabilities were exploited or backdoors used. The reports alone do not allow us to analyse whether considerably more complex patterns had to be used against some Blue Teams compared to others (e.g., different SQL injection points, more effort required to bypass filters or malware detection). Work-intensive network traffic analysis and VM forensics would be needed for that.
    - Red Team members should be encouraged to provide more information on activities that were not directly scored. This is especially important from the Green Team's perspective: sometimes it was not easy to understand whether Blue Teams had problems with infrastructure or whether the problems were caused by the attacks (e.g., Red Team changing the passwords on owned systems or destroying targets).
4. Providing situational awareness to the Blue Teams should have a high priority.
    - Scoring visualisations in the VSRoom designed for Blue Teams were not available at the beginning of Day 1. Blue Teams did not know how to use the software and were missing feedback on their progress.
    - Service up-time visualisation should be improved (or teams better trained), as it was difficult for Blue Teams to know whether the availability checks of the scoring bot succeeded or not.
    - A description of experimental software (RUAG ESOM Mapper Prototype) was not available at the beginning of Day 1.
    - Blue Teams were, in general, missing the lifeline of events to understand what was going on.
    - Articles generated by the media simulation cell were a good way of providing awareness to Blue Teams. This should have more focus.
5. The need for new and better technologies providing situational awareness on defensive and offensive cyber campaigns is widely known. This is no different in the context of technical exercises. All teams would benefit from better means that would help to assess and visualise the effects of activities and status of systems.

6.5 Rules

1. From the Blue Teams' perspective, the rules need further simplification.

  - A modified and simplified version of the rules set from Baltic Cyber Shield 2010 was used for LS12. It was still considered complex. Sophistication was added by fictional legislation and company policy which also regulated the environment.

2. Rules for password management have to be redesigned or better communicated.
    - Blue Teams were allowed to change the passwords of their regular computer users only if a breach or a weak password was suspected. They were required to document these changes on a special wiki page so that White Team members role-playing those users could still log in. These principles were not followed and no one documented any changes in the wiki.

6.6 Scoring System

1. The process of designing the scoring table for the next exercise should define the priorities between score groups in the beginning.
    - There were issues with the weighting of availability scores, as some argued they were not high enough. The issue was that the 10,000 points for availability were spread over (in the end) too many services, so that locking down a single service was not penalised enough. From the Blue Teams' perspective, it would have been a better approach just to take the service off-line than to risk successful attacks from the Red Team.
    - 'Non-capped' scoring categories should be avoided. The cap for Red Team attacks and CERT reporting was removed in the end. The former, particularly, led to the situation that some teams were 'beaten to death' by web defacements.
2. The scoring bot should be further developed to be able to check more application level services.
    - The White Team did not have enough resources to manually check the functionality of services. For instance, some Blue Teams made fixes to the web applications that also broke the functionality but they were not penalised for that.
3. Scoring rules favoured prevention more than detection and quick response.
    - Initially, the scoring system was designed such that successful detection and mitigation of an attack would cancel out part of the negative points assigned for compromise. However, that became too challenging to enforce with the resources available in the White Team. In the end, Blue Teams got many more negative points due to successful Red Team attacks compared to the positive points they could earn from fast detection, mitigation and reporting.
4. The negative score assigned for successful Red Team attacks should be better aligned with the business impact.
    - Successful defacement gave many minus scores, even if the problem was detected and fixed in few minutes.
5. The scoring categories and visualisation of results should be more transparent to the Blue Teams.
    - VSRoom visualizations were provided too late and were not explained to Blue Teams.
    - Situations covered by VSRoom were interpreted differently. For instance, one Blue Team thought that patching had the main focus but another team focused on detection and reporting after getting access to VSRoom.
    - Detailed scoring table was not provided to the Blue Teams on purpose to avoid the teams focusing on how to beat the scoring system. As expected, this caused disappointment and confusion for the Blue Team members.
6. For the Blue Teams, it was difficult to know and measure what services were scored and therefore needed to be up.
    - Preconfigured Nagios could be deployed into the Blue Team infrastructure.

7. Competition is essential to motivate the teams and provide them an opportunity to measure their skills in different areas. However, the conditions were not always equally the same for all the teams.
    - Automatic scoring checks are debatable, as some services were down due to technical issues with the infrastructure. In general, downtime caused by faulty infrastructure was compensated by the White Team but we cannot assume that White Team was capable of tracking all the complaints.
    - Client-side attacks could not be carried out equally against all teams. Firstly, RDP access was automatically allowed after cloning only on Windows 7 workstations. For Windows XP, Blue Teams were tasked to do it themselves but not everyone did it in time. In short, the teams who followed White Team's requests were actually penalized by Red Team's attacks.
    - Some reporting errors were discovered during post-mortem analysis.
    - BT1 was in most cases the first victim.

6.7 Communication and Information Sharing

1. The structure of information in the wiki-based collaboration portal needs careful design. A better summary of the most important aspects has to be provided.
    - Feedback from Blue Teams is again controversial. Some did not have any problems with the platform, some teams found it difficult to navigate and find information.
    - Another reported problem was that team members lacked time to delve into the vast amount of information related to the exercise.
2. Blue Team leaders should be contacted in person (e.g., over the phone) at least one month before the execution to make sure they have understood their expected role.
    - Although a detailed description of required skillset was provided in the information package and collaboration portal, some Blue Teams were lacking persons with required skillset to cover all the areas and systems. The role of the team was not clear. For instance, one Blue Team brought a lot of network security personnel to participate but was lacking Windows and Linux specialists. Others thought that Blue Teams should be staffed only by CND personnel and were also lacking experienced system administrators.
3. White Team-Blue Team Liaison Officers should be appointed at least a month before the exercise to start direct communication between POCs.
4. Major changes related to communication means have to be avoided.
    - The main communication platform (wiki, chat) and related addresses were moved from the internet to the Gamenet straight before Day 0. This was counter-productive, caused a lot of confusing account synchronisation problems.
        - A few of the Red Team members did not get access to Jabber and the wiki till the end of exercise.
5. All means of communication have to be tested and participants trained before Day 0.
    - Before the exercise, two webinars were conducted with Blue Teams using GoToWebinar software. However, not all Blue Teams had a representative attending these webinars. During the exercise, GoToMeeting was used as a permanent video channel between the White Team and Blue Teams but it was not tested for everyone. Strict firewall rules probably prevented at least one team from properly connecting over GoToMeeting: this rendered the virtual meetings ineffective for them.
6. Final documentation should be provided to the Blue Teams at least two weeks before the Execution.
    - One week was considered too short a time-frame.

7. The Communication Plan should be cross-checked several times before finalising and advertising to the players. The number of channels should be reduced if possible.
    - The main problem was regarding the email addresses. It was not possible to reach some of the teams through the mail servers hosted by the teams themselves. Therefore the White Team switched to alternative accounts to inject additional tasks.
    - The Blue Team communications sheet was missing contact addresses for the Media (journalists).
    - There were many chat channels with different purposes but it was difficult to keep the discussions on specific topics on the specific channel.
    - GoToMeeting supported 15 simultaneous attendees. Four control cells, nine Blue Team cells and a video of SCADA installation needed to be connected. Therefore we could afford only one connection per Blue Team, but this was not clearly communicated at the beginning. Several persons from some teams connected, blocking other teams having access completely.
8. Email accounts used to deliver injects to the Blue Teams had to be hosted on the Green Team's mail server off-limits to the Red Team. The number of accounts should be limited to those that are actually used. The availability of the email service hosted by Blue Teams themselves could only be checked automatically.
    - Originally, Blue Teams were required to monitor several accounts (abuse, service, sales, info) on their own mail server. There were also backup accounts hosted on a mail server administered by the Green Team which the Red Team was not allowed to attack. This complexity caused confusion.
    - After Red Team started the campaign, some Blue Teams lost proper access to their own mail infrastructure. BT6 reported issues with its mail systems from the beginning of the exercise which the Green Team was not able to solve.
    - In conclusion, the White Team had difficulties in reaching the Blue Teams to inject tasks in time.
9. The chat and wiki-based tools provided by the organisers for collaboration and information sharing were considered good, but alternative methods were still used.
    - The wiki was not considered the best way to share information due to the need for simultaneous writing.
    - At least two teams preferred Google Docs for information sharing and also for keeping track of the incidents. Flip charts and whiteboards were also handy, as expected.
10. Short instructions should be provided to the Blue Teams in case they need to use non-standard software to accomplish business tasks.
    - There were no instructions as to how to use the ISP control panels to set up new domains and websites for clients. To understand how the VM hosting system (vmgate, chost) works, Blue Teams needed to analyse the code of the interface.
11. A list of customers was not provided to the Blue Teams. Therefore it was not possible differentiate between legitimate and 'hacker' accounts.
12. Much information about attacks and vulnerabilities was shared by the Blue Teams, e.g., on cdx12blue channel. However, there was limited or no real cooperation. The scenario should have more emphasis on defining common tasks for Blue Teams and there should be more dependencies between the systems of different Blue Teams.
    - Routers of different Blue Teams were connected to form a common OSPF routing infrastructure. BT3 suggested protecting route exchanges by a shared secret key but they did not succeed in motivating all others to collaborate.
    - Blue Teams also had a shared SCADA system which was simulated to control the cooling of the shared server room. SCADA could have been accessed only through specific workstations from each Blue Team INTERNAL network. The Red Team was still able to sniff the shared password of SCADA management interface, access it

through the compromised workstations of several teams and ‘blow it up’. This setup was too artificial and several teams did not really understand the role of it and what they should have done.

13. The naming scheme in chat should be re-thought, as it was difficult to find the right people. One option would be to use team (and sub-team) names in the beginning of the alias, as the chat clients sort the names alphabetically. A few examples would be:
    - RT_adv_firstname.lastname (Red Team member responsible for advanced campaigns).
    - RT_cli_direstname.lastname (Red Team member responsible for client-side attacks).
    - WT_firstname.lastname (White Team member).
    - +WT_firstname.lastname (White Team Leader).
    - GT_firstname.lastname (Green Team member).

6.8 Blue Teams

1. There should be a CERT team playing a similar role to real life, cooperating with the Blue Teams.
    - In the context of LS12, CERT was mainly responsible for evaluating Lightweight incident reports. They did not have time for providing advisories and coordinating the incident response between the Blue Teams. Blue Teams often shared information about vulnerabilities or backdoors which had been already reported by others.
    - One option would be to have a separate Blue Team (BT_CERT) providing a subset of typical CERT services to other Blue Teams. BT_CERT would not be part of the exercise control and would not have information about Red Team's campaigns but would be entirely dependent on the quality of information provided by other Blue Teams.
2. Blue Teams should be advised to engage a professional PR manager in the team. Then the Media Team can focus on providing learning opportunities to people who really need it.
    - No previous experience in PR was required from the designated PR managers of the teams. The aim of the media activity was to help communicate some of injects, add pressure to the Blue Teams and illustrate the exercise with information filtered by the media. The latter was achieved mainly via the news portal. The stories seemed to receive good feedback and attracted many contributions from anonymous commentators.

6.9 Red Team

1. It was not possible to accomplish all the pre-planned attacks on all Blue Teams. This affected fair game play. Avoiding overly complex and unfamiliar infrastructure, providing better documentation and more testing should help in the future.
    - There was space limitation on the VMs Blue Team customers could run on the hosting infrastructure (chost and vmgate). Blue Teams were not familiar with related systems and many were not able to keep the services running and accessible. Probably, the systems themselves were also unstable. Therefore Red Team could play the bad customer and upload infected VM images only in the case of a few teams.
    - A ‘Contractor's laptop’ was deployed only into three Blue Team networks. This was done at the end of game and was affected by infrastructure downtime (OSPF loop).
2. Web attacks were considered ‘too successful’. It should be emphasized to Blue Teams that they needed to engage members with skills in protecting web applications.
    - The Red Team had many web application developers and pen-testers.

   - Web attacks were mostly scripted to be fair, but this made them very quick and easy to repeat. Thus there was a large amount of successful defacements which dominated too much of the game.
   - Web Application Firewalls deployed by some Blue Teams did not provide ultimate protection.
3. The Red Team's objectives should go further than exploiting single web application vulnerabilities. Real 'flags' could be hidden deeper in the systems, giving the Blue Teams more time and options to detect the attacks and react.
4. Assembling a strong core Red Team competence required a lot of effort in planning, scenario and game environment development, vulnerability research and tie-in, defining scoring and success metrics, scripting automated attacks, organising the Red Team sub-teams and the pre-execution practice of volunteers. One way to reduce the Red Team contribution and keep the learning curve lower is not to change the scenario and environment radically every time. If novelty and radical changes in game play are prioritised, Red Team preparations will need a higher budget.
5. If the Red Team's goal remains to provide learning experiences to the Blue Teams, engaging ad hoc volunteers who do not commit to preparing in advance should be avoided.
6. The Red Team needs to participate more in building the target systems. The Green Team could build the initial infrastructure and the Red Team then fine-tune it. This work is time-consuming and cannot be expected to be carried out by volunteers.
7. White Team Blondes could do more in cooperation with the Red Team.
   - They could provide information about which defensive programs (Antivirus, Antimeter) have been installed on the workstations or why some exploit attempts failed.
8. The copy of the Blue Team network was provided only to the Red Team for testing purposes and was very helpful. However, Red Team members have to be provided with a convenient interface with typical operations with the VMs such as power-on, reboot, revert to snapshot, etc. The same applies to Red Team's own BackTrack VMs.
   - The OpenNebula-based VM management interface was not configured for the Red Team.
9. Manually simulating real-life attack activities probably provides the best learning opportunity for the Blue Teams. Manual attacks are noisy and relatively slow compared to scripted, automated attacks. Still, anomaly detection with good centralised monitoring tools should be the focus of the next CDX, so that even fast and sudden attacks would be noticed and reported. Many Blue Teams did not even realise how often their intranets had been compromised or how much information had been exfiltrated.

6.10 Green Team

1. The Green Team should be better staffed with experienced Windows administrators. For example, there was no-one who could set up an Exchange server for Blue Team internal email communication. More experience would have also been needed to create deployment scripts for automatically changing all required parameters.

6.11 White Team

1. The roles of Blonde (simulating the ordinary computer users of Blue Team companies) and Blue Team-White Team Liaison Officer could be merged. Ideally, there would be one dedicated Blonde/Liaison per Blue Team and they should have rehearsed temporary handovers.

2. There should be a coordinator for Blondes and Blue Team-White Team Liaison Officers who keeps a current overview of their status and helps them to be on top of the situation.
    - The sub-team of the Red Team which was responsible for client-side attacks needed a status report at least once every 60 minutes describing which workstations the Blondes could access and which not. Co-location of Blondes and client-side attack team members could be another option. However, it is clear that the roles have to be separated and Red Team members must not be allowed to play the Blondes themselves.
3. White Team-Blue Team Liaison Officers should have a detailed overview of the exercise and in-depth knowledge of the rules. Guidelines given to Blue Teams have to be concrete.
    - Information provided to Blue Teams was not always accurate.
4. Technical infrastructure has to be prepared such that Blondes can have guaranteed access to the workstations.
    - Simulation of user activities partially failed because White Team members had challenges in accessing the workstations in the Blue Team infrastructure. Remote access over RDP was initially not possible to all VMs, due to group policies preventing it.
    - Console access should be reserved for White Team members and remote access over RDP for Blue Team members.
5. There should be a dedicated press/VIP briefer.
    - This person should have sufficient ‘rank’ and perhaps an ‘honorary’ title in the exercise in order to calm the VIPs.
6. The White Team needs more staffing for verifying the situation (e.g., was a special task accomplished, is a website defaced, etc...).
7. The traffic generation system should have components that simulate interactions with customers.

6.12 Legal Team

1. General comments:
    - The incidents that took place in the exercise were quite trivial from the point of view of national legislation. From the point of view of international legislation, further background information would have been required to draw more detailed conclusions.
    - The Legal Team is probably not able to participate ‘live’ in such an exercise with the technical experts. Therefore the Legal Team does not need live-feeds of tech-chats. An idea would be to conduct briefings for the Legal Team and give them a ‘case’: a political situation, real-life events, subsequent electronic attacks (DDoS, defacement, hacking and compromise of data in the network, publication of data, statements on websites, etc).
    - If one of the objectives of the exercise is to focus on international law and conflict, on- and offline situational awareness needs to be provided.
    - It is difficult to draw a situational picture by evaluating only what is going on in the networks. For a better understanding, it is always important to look at real-world facts, as those tend to be mirrored in the virtual environment.
    - To really engage the Legal Team it would be necessary to draw a sophisticated scenario and have a news-feed and a feedback loop of ‘ongoing events’ in the real world (an exercise equivalent which could be fictional). Real-world examples might suit better than fictional ones.
    - It is critical to have technical experts to explain what is happening in the networks to the Legal Team.

2. Future exercises:
    - If the exercise is for general everyday training, lawyers might be embedded with Blue Teams to be educated about the technology, and Blue Teams could be advised on how to collect, save and share data in compliance with the law and for a possible police investigation.
    - Legal Team members could also be distributed between Blue Teams and the central cell.
        - There could be a legal expert in all of the Blue Teams. That expert would be the contact point of the Legal Team.
        - The separate Legal Team would focus mainly on international law.

6.13 Technical Environment

1. Providing a preconfigured gateway to the Blue Teams for accessing the game environment was a good idea and should be continued. Still, testing and documentation of the device needs improvement.
    - Several Blue Teams had problems with the device because of configuration mistakes. They had to continuously reboot it. It seems that some teams also extensively used a wireless interface although it was not suggested.
2. Backup procedures were required to reset/revert the whole infrastructure.
3. Straight after the end of exercise, snapshots of all systems should be taken and the environment 'frozen'.
4. Although the infrastructure built on top of OpenNebula, Libvirt and KVM was lacking some features compared to commercial products, it provided the flexibility to fulfil all kinds of unique requirements. Therefore the choice of the platform is considered good.
5. The selection of a proper storage solution is extremely important. The large-scale exercise environment has to cope with running more than 300 virtual machines simultaneously and has high requirements.
    - The initial storage solution (SAN storage was used through iSCSI) did not perform as expected. This was firstly discovered during a Test-Run conducted two months before the Execution.
    - Later, an NFS server was installed on one of the blades. It had OpenIndiana (http://openindiana.org/) as the operating system and used a ZFS file system. IOPS was boosted by two caches: one RAMdisk (92GB) for read and one extra DDRDrive (4GB) for write cache. This solution performed well.
6. The networking setup and traffic mirroring solution has to be redesigned. The setup was complex and challenging to debug. Traffic mirroring was not reliable.
    - These are the main requirements:
        - Yellow Teams must have the option to get all the traffic from all the Zones as required for visualization and situational awareness solutions.
        - Blue Teams must have the option to get all the traffic from all the Zones under their control (but naturally not from any other Zones).
        - All traffic has to be recorded for after-action analysis.
    - The Linux bridges for the 2.6 kernel that was configured on the blades did not support mirror ports. Therefore other kind of solutions had to be used. The Green Team chose to use:
        - iptables -t mangle -j TEE
        - tcpdump
    - Many different problems were observed with this setup. For instance:
        - Recorded pcaps were missing interesting parts of the game, as some files got overwritten. Also, the timestamps are not accurate.

  - At some point in time, it was discovered that the first packet of a session often got lost if it had to traverse from one blade to another. For example, it took five seconds (two UDP packets) for a DNS name to resolve. Many hours were needed by several specialists to tweak kernel parameters and ebtables rules to solve the issue.
  - Lot of tweaking of iptables and ebtables rules had to be carried out to enable the traffic mirroring system to work.
  - The whole Gamenet was inaccessible twice during Day 2, which was caused by high traffic peaks.
- Linux vSwitches could be considered as an alternative of Linux bridges. This has not been tested yet.

7. The bandwidth of network interfaces should be limited to avoid high traffic volumes overloading the infrastructure. There were two major outages during the second exercise day. Both of them were caused by high traffic peaks. Blades were overloaded and not accessible.
    - The first problem happened after the Red Team started to create denial of service traffic (in fact, they were breaking rules of engagement as DDoS was not allowed). The tcpdump processes had too high a priority and load on the blades rose to 300. After renicing tcpdumps, the issue was solved. Red Team was also asked to stop any traffic-intensive actions.
    - The second problem was also caused due to Red Team activities. They deliberately generated a routing loop inside a Blue Team shared OSPF routing infrastructure. This also resulted in high traffic peaks and overloading the servers.
8. Several times MAC address conflicts occurred in the network.
    - In the beginning it was not clear to all Green Team members how exactly OpenNebula generates MAC addresses for fresh VMs. It was based on IP addresses which had to be specified for every NIC in the host definition file. If this was not done (as for DHCP clients including the scoring bot), the deployed machines ended up with the same MAC addresses. An initial workaround was to use artificial IPs and it was fixed later.
9. For people with no previous experience of the platform the learning curve was high. This could be made easier with better documentation.
    - Two or three days were needed to understand in general how the infrastructure worked and how one could create virtual machines on it. One had to know the logic behind OpenNebula, how to create definition files for virtual machines, networks and disk images. At least basic knowledge about the libvirt command line front end was also needed.
    - For 'newbies', OpenNebula has strange logic and one needs to know small but significant details, e.g., 'onevm shutdown' actually deletes the deployed VM if the disk is not marked as 'PERSISTENT'. This is the default setting. All changes could be lost by 'shutting down' a VM.
    - The fact that it takes a day to properly deploy first VM is in contradiction to what we require for many people (volunteers) with low commitment and not much time who would like to help and build some components.
10. The environment was in general inconvenient to use but this was compensated for by having all tasks scripted, which allowed automatic redeployment of the whole infrastructure.
    - Sunstone GUI often had errors. Therefore command line utilities had to be relied upon, even for small tasks. This meant high productivity loss for people coming from the Windows world who were not so comfortable with CLI. On the other hand, one of the goals was to make everything easily re-deployable. This meant doing a lot of scripting but it was, in the end, very beneficial to be able to automatically redeploy the whole infrastructure.

   - Simple operations like connecting the VM into different network segments were inconvenient and took time. For instance, one option to connect the VM into a new network without GUI was to:
     - log to the blade where the VM was deployed;
     - shut down the VM;
     - look up the correct VNET ID and respective bridge number;
     - edit the deployment file (KVM definition file) of the VM and change the bridge number;
     - start the machine again (virsh create).
   - Quite often, accessing VNC consoles from Sunstone did not work.
   - The most reliable way to access the console of the VM was to use the native VNC client: the ID assigned by OpenNebula had to be identified, the node (blade) where it was deployed, and then connected to the respective port (5900+VM_ID) and respective IP address using vncviewer.
11. Network segments used for development should have a more relaxed internet connectivity to increase productivity.
    - VMs inside the Blue Team networks which were used for developing did not have direct internet access. There was a transparent proxy (SSL was dissected). This made the whole process work-intensive in some cases. Some software updates did not work over the proxy, or additional efforts were needed (e.g., updating some components of Red Team BackTracks).
12. Blue and Red Team members should be provided with a good user interface to manage their machines. They should have a convenient way to perform the following operations:
    - Reboot, start, shutdown VMs.
    - Revert VMs to snapshot.
    - Upload and create their own VMs and connect to their network segments.
    - Access their VMs over a console.
    - Optionally, also control other parameters such as the amount of RAM allocated to specific VMs.
13. The modified version of OpenNebula Sunstone that was provided to the Blue Teams for managing their VMs did not work reliably.
    - After the Blue Teams were given access, the VM Management Server was still in deployment for at least one day.
    - There were issues with accessing VNC consoles from Sunstone. Eventually, Blue Teams were given access to a native VNC console.
    - Sometimes virtual machines did not boot up after restart. If the Blue Team VM did not come up properly, the team members were missing feedback as to what happened. Often the Green Team had to check what went wrong.
    - Sometimes VMs were reported to disappear from the Sunstone interface after a disk reset.
14. The interface provided to the Blue Teams to upload their own VM was buggy.
    - The process was the following:
      - Prepare KVM compatible VM image on team’s own infrastructure
      - Upload it over SFTP to the NFS share on CDX12 infrastructure (from Out-of-Game network)
      - Use Sunstone to create host definition file, define image and add disk, set up networks, etc.
    - Firstly, with some SFTP clients, the Blue Teams received error messages such as ‘no supported authentication methods available’, ‘subsystem request failed on channel 0’. It did, however, work with FileZilla.
    - Secondly, Blue Teams had also problems with creating the image with the following error message: ‘Error [ImageAllocate] Error allocating a new image. Template

includes a restricted attribute SOURCE'. Probably, this was associated with inconsistent access lists.

15. Preparing VMs with Windows operating systems was time consuming.
    - Windows VMs without virtio drivers for network interfaces and disk did not boot up. To get an acceptable performance, using paravirtualized device drivers is unavoidable.
    - Persons with no previous experience of OpenNebula/libvirt/KVM needed several days to solve all the issues and get virtio drivers properly working on Windows images.
    - There was a problem with USB implementation on KVM, which seemed to have bugs. It was not possible to get a mouse working correctly (the pointer was not in the correct place) without adding a 'tablet device' to Windows VMs. However, that constantly consumed 30% of the CPU of the host machine.
    - No scripts existed for Windows machines to change the parameters according to the Blue Team network where they had to be deployed. All those had to be created from scratch.
16. OpenNebula seems not yet mature enough, or significant experience is needed to set it up properly. Examples of some problems observed are listed below:
    - There were different issues with getting some basic commands working, e.g., 'onevmsaveas' should be used for saving the changes you had made but it did not work.
    - After deploying a lot of VMs the interface started to be very slow and consumed 100% of CPU on the cloud control host. A simple listing of all VMs took more than five seconds. The problem was solved after replacing an xml parser library.
    - The required daemon (oned) was somewhat unstable and sometimes crashed.
17. Some VMs (especially the sensors used for traffic recording) had problems with high CPU wait. There may also have been issues with over-provisioning of resources.
18. Keeping accurate time in cloned VMs hosted on heavily loaded servers proved to be a challenge. The Green Team should plan more time to research the issue and configure the systems such that, after cloning and frequent reverts, the VMs would still have clocks synchronized.
19. The rules for building the VMs into the exercise environment should be agreed early before major development activities.
    - This includes somewhat unified platforms (e.g., using the same popular Linux distribution), same administrative passwords on all systems, common NTP and time zone settings, keyboard layout, etc.
20. There was no point in providing Blue Teams with machines with completely unpatched operating systems. Automatically applying patches is a trivial task but requires a lot of time and I/O operations when done simultaneously on hundreds of systems.
21. For a two- to three-day exercise, the network scheme for Blue Teams should be simplified compared to LS12.
    - The number of Zones and complex IP addressing scheme confused the Blue Teams. In the real world, IT administrators would have a good understanding of their own networks.
22. OpenVPN worked reliably and is a good choice for providing remote access to the teams. VPN access rules need more consideration, as some Green Team systems (mail.ex, news.ex) should be always accessible to the Blue Teams.

6.14 Facilities

1. Red Team members should have more space on their table to attach larger monitors to the laptop and to be able to use an external keyboard.
    - There were two rooms set up for Red Team cells in NATO CCD COE. In one of the rooms there was more space for team members and therefore it was more convenient.
2. All Red Team members should have an opportunity to follow and participate in feedback sessions.
    - As the White Team control room was crowded, only the Red Team leader and a few members participated in GoToMeeting sessions. The video from GoToMeeting was not broadcast to the Red Team rooms.
3. The Media Team should have a quiet room for conducting interviews. In general, all simulation cells could be located in separate room from the main White Team control cell.

7 Conclusions

Locked Shields 2012 was a successful cyber defence exercise, meeting the expectations of both organisers and participants. There is a clear need for more and similar live trainings, as all Blue Teams were interested in attending the next event.

A considerable amount of resource is required to set up the exercise. Organising it is an international effort and not a trivial task. There are also many areas that need to be improved. Some of the observations and recommendations have been listed below:

1. Blue Teams have to be provided with more detailed feedback about the attacks conducted by the Red Team and countermeasures they should have implemented for mitigation.

2. The evaluation of the Blue Teams' efforts should be more balanced regarding how important skills in common IT systems administration tasks are when compared to incident detection, analysis and reporting. Several Blue Teams found that LS12 was too much focused on common system administration tasks.

3. The scenario and organisation of the exercise need adaptations in order to engage the Legal Team actively in the Game. Scenarios should have some complex elements and Legal Team members could be part of the Blue Teams.

4. Lightweight Human Reporting proved to be effective in establishing situational awareness of defensive and offensive campaigns. The solution should be further developed and participants better trained to increase the frequency and accuracy of reports provided by human experts.

5. CDX should be run multiple times on the same (refined) setup to improve return on investment. The focus should be on improving the learning experience and measuring.

6. A lot of effort and resources are required to design the technical environment such that technical problems do not affect the learning experience. A centralised storage system could easily become a bottleneck if not carefully planned.

7. Locked Shields should continue to be a live-fire exercise. Detailed forensic analysis tasks could be conducted on the attacked systems after the exercise.

8 Acknowledgements

NATO CCD COE would like to thank all institutions and individuals who were part of the organising team for LS12 for their significant contributions, and all Legal and Blue Team members for making the exercise a remarkable experience. In particular, we wish to thank the Swiss Armed Forces Command Support Organisation, Finnish Defence Forces, Estonian Cyber Defence League, Kapsi Internet-käyttäjät, CERT-EE, CERT-FI and CERT-LV, Finnish Communications Regulatory Authority, NATO Computer Incident Response Capability – Technical Centre, Swedish National Defence College, RUAG Defence, Swisscom, Clarified Networks, Clarified Security, IT Centrs, and Jussi Jaakonaho.

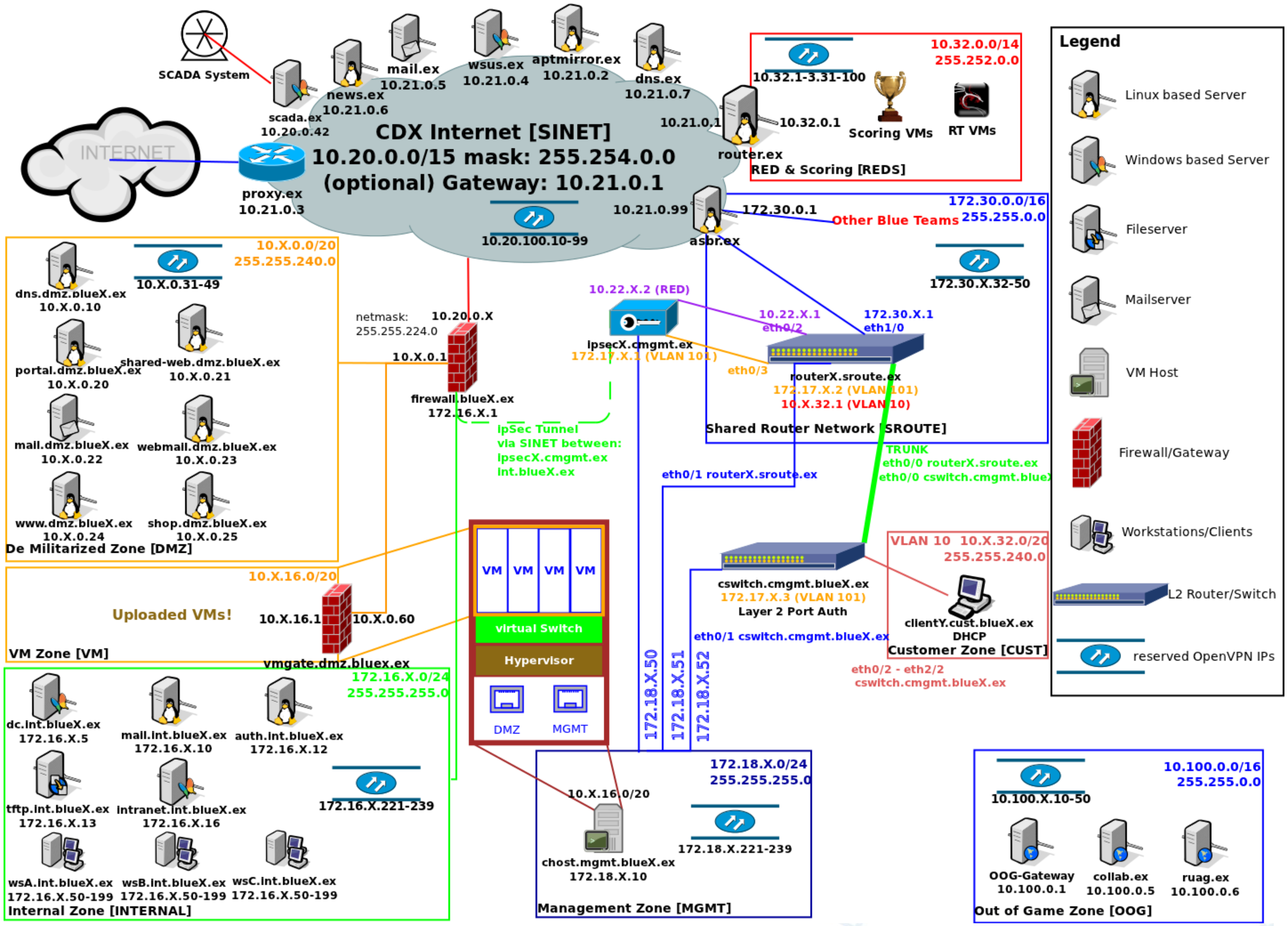
9 Acronyms

BCS	Baltic Cyber Shield
BT	Blue Team
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
CDX	Cyber Defence Exercise
CND	Computer Network Defence
ECDL	Estonian Cyber Defence League
FDF	Finnish Defence Forces
FPC	Final Planning Conference
GT	Green Team
HMI	Human-Man Interface
IPC	Initial Planning Conference
LS	Locked Shields
LT	Legal Team
MNE	Multinational Experiment
MNE7 SA	Multinational Experiment 7 CDX12 Situational Awareness Team
MPC	Main Planning Conference
POC	Point of Contact
RDP	Remote Desktop Protocol
RT	Red Team
SA	Situational Awareness
SAF	Swiss Armed Forces
SOP	Standard Operating Procedure
VM	Virtual Machine
WAF	Web Application Firewall
WT	White Team
YT	Yellow Team

Appendices

Appendix A: Blue Team Systems

A.1 Network Scheme



SCADA System

scada.ex
10.20.0.42

news.ex
10.21.0.6

mail.ex
10.21.0.5

wsus.ex
10.21.0.4

aptmirror.ex
10.21.0.2

dns.ex
10.21.0.7

INTERNET

proxy.ex
10.21.0.3

CDX Internet [SINET]
10.20.0.0/15 mask: 255.254.0.0
(optional) Gateway: 10.21.0.1

10.20.100.10-99

10.21.0.1

router.ex

10.32.0.1

10.32.1-3.31-100

Scoring VMs

RT VMs

10.32.0.0/14
255.252.0.0

RED & Scoring [REDS]

10.21.0.99

asbr.ex

172.30.0.1

Other Blue Teams

172.30.0.0/16
255.255.0.0

172.30.X.32-50

10.22.X.2 (RED)

ipsecX.cmgmt.ex
172.17.X.1 (VLAN 101)

10.22.X.1
eth0/2

172.30.X.1
eth1/0

eth0/3

routerX.sroute.ex
172.17.X.2 (VLAN 101)
10.X.32.1 (VLAN 10)

Shared Router Network [SROUTE]

TRUNK
eth0/0 routerX.sroute.ex
eth0/0 cswitch.cmgmt.blueX

IpSec Tunnel
via SINET between:
ipsecX.cmgmt.ex
int.blueX.ex

eth0/1 routerX.sroute.ex

netmask:
255.255.224.0

10.20.0.X

10.X.0.1

firewall.blueX.ex
172.16.X.1

dns.dmz.blueX.ex
10.X.0.10

10.X.0.31-49

10.X.0.0/20
255.255.240.0

portal.dmz.blueX.ex
10.X.0.20

shared-web.dmz.blueX.ex
10.X.0.21

mail.dmz.blueX.ex
10.X.0.22

webmail.dmz.blueX.ex
10.X.0.23

www.dmz.blueX.ex
10.X.0.24

shop.dmz.blueX.ex
10.X.0.25

De Militarized Zone [DMZ]

10.X.16.0/20

Uploaded VMs!

10.X.16.1

10.X.0.60

vmgate.dmz.bluex.ex

VM Zone [VM]

VM VM VM VM

virtual Switch

Hypervisor

DMZ

MGMT

cswitch.cmgmt.blueX.ex
172.17.X.3 (VLAN 101)
Layer 2 Port Auth

eth0/1 cswitch.cmgmt.blueX.ex

VLAN 10 10.X.32.0/20
255.255.240.0

clientY.cust.blueX.ex
DHCP

Customer Zone [CUST]

eth0/2 - eth2/2
cswitch.cmgmt.blueX.ex

172.18.X.50

172.18.X.51

172.18.X.52

172.16.X.0/24
255.255.255.0

dc.int.blueX.ex
172.16.X.5

mail.int.blueX.ex
172.16.X.10

auth.int.blueX.ex
172.16.X.12

tftp.int.blueX.ex
172.16.X.13

intranet.int.blueX.ex
172.16.X.16

172.16.X.221-239

wsA.int.blueX.ex
172.16.X.50-199

wsB.int.blueX.ex
172.16.X.50-199

wsC.int.blueX.ex
172.16.X.50-199

Internal Zone [INTERNAL]

10.X.16.0/20

172.18.X.0/24
255.255.255.0

chost.mgmt.blueX.ex
172.18.X.10

172.18.X.221-239

Management Zone [MGMT]

10.100.X.10-50

10.100.0.0/16
255.255.0.0

OOG-Gateway
10.100.0.1

collab.ex
10.100.0.5

ruag.ex
10.100.0.6

Out of Game Zone [OOG]

Legend

Linux based Server

Windows based Server

Fileserver

Mailserver

VM Host

Firewall/Gateway

Workstations/Clients

L2 Router/Switch

reserved OpenVPN IPs

A.2 Zones

The network the Blue Teams had to secure and manage during LS12 consisted of several Zones which are described in the following table:

Zones			
Name	**Abbreviation**	**IP Range**	**Description**
Simulated Internet	SINET, REDS	10.20.0.0/15	Network simulating internet. It contains the Green Team servers providing services such as root DNS, software repositories for updates, and ensures connectivity between public systems of all the Players. Customer traffic (scoring, White Team members, traffic generation) and systems of malicious parties will be also located in this Zone.
Demilitarised Zone	DMZ	10.X.0.0/20	Network segment for BlueX public services that should be accessible for everyone from SINET.
Virtual Machine Zone	VM	10.X.16.0/20	Virtual Machines for BlueX cloud hosting services.
Customer Zone	CUST	10.X.32.0/20	Zone for customer computers using (simulated) DSL connection provided by BlueX. These computers are not under the control of BTs but could be secured at some level by using firewall rules and content filtering.
Internal Zone	INTERNAL	172.16.X.0/24	Desktops for BlueX employees and servers for Back-Office.
Customer Management Zone	CMGMT	172.17.X.0/24	Zone for devices required to provide ‘internet’ connectivity to systems in CUST Zone
Management Zone	MGMT	172.18.X.0/24	Zone for management interfaces of VPS hosting machine, virtual switch and router
Shared Routing	SROUTE	172.30.X.0/16	Shared routing infrastructure between all Blue Teams based on OSPF.
Out-of-Game Zone	OOG	10.100.0.0/16	Collaboration environment used during the game. VM Management Interface

A.3 Generic Requirements for Systems

Blue Teams had to conform to the following requirements:

1. The description of each individual system defines the general functionality of the host and what services have to be provided. These services could be used for automatic availability checks.
2. Services running on VMs in DMZ and VM Zone are considered public and have to be accessible from SINET, REDS and INTERNAL, and CUST Zones of all Blue Teams.
   - Note that the administrators of the Blue Team primary IT team have been used to administering the DMZ hosts remotely from arbitrary IPs in the 'internet' (SSH, RDP, VNC, web interfaces). The primary IT team may need instant access from South Africa and you are not allowed to block access to remote administration services in the firewall.
3. Services running on VMs in INTERNAL, MGMT and CMGMT Zone have to be accessible for hosts in the same subnet and to all other hosts which are required to guarantee the functionality of services specified under system descriptions. Blue Teams have to work out the dependencies themselves.
4. Blue Team employees using the workstations in INTERNAL must be allowed to browse the web (HTTP, HTTPS) in the whole Game Internet. Game Internet consists of all subnets inside the address space of 10.0.0.0/8. Content may be filtered and access blocked to sites that are used for malicious purposes (e.g., for hosting malware or running an attacker's C&C server).
5. Clients in the CUST segment have to be provided with an unfiltered connection to the Game Internet. All incoming and outgoing TCP/UDP ports and ICMP protocol must be allowed. The only exception is SMTP which could be limited in case spamming activity is detected.
6. Blue Team employees have priority using their workstations. Administrators cannot distract the employees without prior agreement. Maintenance of workstations has to be requested by sending an email to white@mail.ex.
7. White Team members simulating employees may use scripts and browser add-ons for making actions automatic. Also, scripts for making scoring checks will be running inside workstation. Blue Teams are not allowed to remove or stop those scripts.
8. Only White and Green Team members have VPN access to Blue Team Zones. This access may not be blocked by the Blue Teams. White Team is using VPN to access workstations in the INTERNAL Zone and Green Team may need access to verify technical problems.
9. Discrepancies from these rules and specific requirements could be stated in the description of the specific system.

A.4 Systems

The following table lists the systems deployed for Execution of the CDX12.

Name	Zone	OS	Description
auth.int.bluex.ee	INTERNAL	Linux Ubuntu 11.04 i686	Authentication Server for Customer Zone [CUST]
chost.mgmt.bluex.ex	DMZ, MGMT	Linux Ubuntu 11.04 x86_64	(Nested) KVM system for hosting virtual private servers
cswitch.cmgmt.bluex.ex	CMGMT, MGMT	IOS	Switch connecting elements of CUST Zone
dc.int.bluex.ex	INTERNAL	Windows 2003 Server	Domain Controller for INTERNAL Zone
dns.dmz.bluex.ex	DMZ	Linux Ubuntu 11.04 i686	External DNS server hosting BT domains
firewall.bluex.ex	DMZ, INTERNAL, SINET	Linux Endian	Firewall / default gateway between SINET and BT Networks
intranet.int.bluex.ex	INTERNAL	Windows 2003 Server	Intranet Web Server
ipsecx.cmgmt.ex	CMGMT, MGMT	Linux Endian	Endian IPsec gateway to INTERNAL
mail.dmz.bluex.ex	DMZ	Linux Debian i686	SMTP/POP3/IMAP & Relay server
mail.int.bluex.ex	INTERNAL	Linux Ubuntu 11.04 32 Bit	Mail Server for ‘corporate’ Email
out-of-game vpn server for DMZ	DMZ		IPs reserved for BT's VPN client
out-of-game vpn server for Internal	INTERNAL		IP reserved for out-of-game VPN server and clients
portal.dmz.bluex.ex	DMZ	Linux Ubuntu 11.04 i686	Blue Team Customer Portal
routerx.sroute.ex	CMGMT, MGMT, SROUTE	IOS	Blue Team customer gateway
scada.ex	SINET	Multiple	Shared small SCADA installation to control cooling system of server room
sensor.oog.bluex.ex	oog	Ubuntu 11.4 server i386	This VM is in Yellow network and get a copy of the traffic of team's DMZ, internal, mgmt and cisco switch.
shared-web.dmz.bluex.ex	DMZ	Linux Ubuntu 11.04 i686	Shared Webhost, with several virtual Hosts serving different clients of the ISP.
shop.dmz.bluex.ex	DMZ	Windows 2003 Server	E-shop application for Blue Teams to sell phones, TV-sets, network

			equipment, etc
tftp.int.bluex.ex	INTERNAL	Windows XP	TFTP Server for making configuration backups of switches and routers
webmail.dmz.bluex.ex	DMZ	Linux Debian i686	Web interface for Blue Team customers to access mail
wsA.int.bluex.ex	INTERNAL	Windows XP SP3 (32bit)	Windows workstation for employees. Configuration A.
wsB.int.bluex.ex	INTERNAL	Windows 7 Ult (32bit)	Windows workstation for employees. Configuration B.
wsC.int.bluex.ex	INTERNAL	Linux Ubuntu 10.04 i686	Linux Workstation for Employees
www.dmz.bluex.ex	DMZ	Linux Ubuntu 11.04 i686	Information portal where the Blue Team provides news to the clients about network failures, advertises new products, etc

Appendix B: Red Team Campaign Plan Prior to Execution

This appendix provides an overview of the Red Team's campaign as it was agreed before the execution of LS12. There were no major changes to the objectives after STARTEX except for the timing control. It was most challenging to execute tasks that had to be preceded by activities from other teams, such as Blue Teams to accomplish a business task or White Team Blondes to carry out some clicking and email transfers.

B.1 Objectives and Tasks

Note that activities to achieve objective O4 were never conducted in reality.

1. **O1: Deface a website in DMZ**
    a. TASK 1 (O1-T1): Deface one of the following targets in DMZ:
        - www.dmz.bluex.ex
        - portal.dmz.bluex.ex
        - shop.dmz.bluex.ex

    b. Rationale: Defacement using 'the Janitors' signature. Since the Blue Teams only know about RBN at this point, it will confuse them. Media reports about the Janitors about an hour later.
2. **O2: Steal a customer's database from DMZ**
    a. TASK 1 (O2-T1): Steal database from shop.dmz.bluex.ex in DMZ.
    b. TASK 2 (O2-T2): Steal database from portal.dmz.blue.ex in DMZ.
    c. Rationale: Opening move of RBN. They steal the database to blackmail the ISP later, when ISP threatens to take down (or actually takes down) a Red Team C&C server or malware server.
    d. Comments: Keep silent about the fact that the data has been leaked. CERT/media informs/asks BT about possible data thefts and WT asks if data has been leaked and for the details as to how it was done.
3. **O3: Steal confidential documents and emails**
    a. TASK 1 (O3-T1): Steal a confidential memo 'MemoBx.rtf' from Documents folder in wsB.int.bluex.ex
        - Rationale: The Janitors are trying to gain access to incriminating information about ISP 'illegal' practices. Try to download documents.

    b. TASK 2 (O3-T2): Steal a confidential message from al.bundy@cust.bluex.ex account by compromising webmail.dmz.bluex.ex (email is sent by White Team Blondes from big.boss@int.bluex.ex account on mail.int.bluex.ex).
4. **O4: Conduct faked data leakage campaigns/PR** (was never conducted)
    a. Comments:
        - Send email from INTERNAL workstation to media.
        - Upload fake documents to public servers in DMZ and leak the URLs to media.

5. **O5: Conduct hostile activities in Virtual Private Server hosting infrastructure**

    a. TASK 1 (O5-T1): As if playing a (bad) Blue Team customer, upload a vulnerable/infected web host. After that CERT demands takedown. If Blue Team contacts Red Team to inform about takedown, then Red Team blackmails (Red Team has the leaked a database). Red Team complies with the first takedown request with no retaliation. After the second takedown request, Red Team will blackmail.
    b. TASK 2 (O5-T2): Register an account through vmgate.dmz.bluex.ex, create new VM from existing templates and break out of that VM using KVM; exploit and own all the VMs running on chost.mgmt.bluex.ex
        - This task was never accomplished. Due to limited disk space on chost, it was not easy to get all Blue Teams to clean some of the VMs to make room for new (bad) customers. In addition, Red Team could not develop reliable exploit specific to used platform to break out from the VM.

6. **O6: Compromise shared SCADA installation**
    a. TASK 1 (O6-T1): Compromise the shared SCADA installation scada.ex through some Blue Team's INTERNAL Zone.
    b. Comments:
        - VNC consoles of the SCADA system components could be accessed only from the INTERNAL segment of Blue Team networks. Therefore compromising client's workstation is a prerequisite.
        - White Team demands Blue Teams to constantly monitor (every full hour) the temperature in the server rooms (credentials sent over plaintext).
    c. Rationale: 'The Janitors' want to shut down the cooling and fire-alarm systems in the ISP server room.
7. **O7: Conduct a phishing campaign and play a bad web hosting customer**
    a. TASK 1 (O7-T1): Sends a phishing email (Simple Phishing Toolkit) to big.boss@int.bluex.ex and many other email addresses. White Team Blondes will click on the link (from wsA or wsB) that leads to 'Outlook Web Access' page. Task is accomplished when Red Team gets the credentials: phishing spam was not detected and clicking on suspicious links was not prevented by the Blue Teams.
    b. TASK 2 (O7-T2): After providing credentials in TASK 1, user is offered chance to download OutlookClient_NEW.exe (executing it creates Meterpreter session). Task is accomplished when Red Team gets the Meterpreter session: Blue Teams did not detect and block malware.
    c. TASK 3 (O7-T3): Play a (bad) customer and host malicious content (EICAR.com test virus inside a zip bomb) on shared-web.dmz.bluex.ex. Accomplishing this task will not be directly scored. Instead, abuse handling inject will be scored by White Team. CERT will request Blue Teams to initiate takedown of the hosting.
    d. Rationale: regular RBN business. If confronted (take down malware), send a blackmail demand threatening to publish customer database in a carder's forum.
8. **O8: Steal the configuration of routers and switches**
    a. TASK 1 (O8-T1): Steal the configuration of routers and switches which are part of the infrastructure providing internet access to the customers. Mess with the OSPF.
9. **Conduct activities that will be not automatically scored**

a. Preparations: compromising machines to pivot into main targets, placing backdoors, etc.
b. Attacks against availability - these will affect automatic availability checks.

B.2 Campaign Timetable

Note that the timetable was somewhat changed during the Execution.

Time	Janitors	RBN	White Team
DAY I			
07:30Z	O1-R0: Defacement in DMZ.		Blondes start logging in to ALL workstations in INTERNAL Zone.
08:15Z	O3-T1: Steal a confidential memo 'MemoBx' from folder 'My Documents' on wsB.int.bluex.ex. Title contains unique string per BT!		Blondes are ready to start clicking on client-side attack links from wsB.int.bluex.ex
08:30Z	O8: OSPF and routers/switches configuration stealing. (manually not scored option is to mess with services)		
09:00Z		O2-T1: Steal database from shop.dmz.bluex.ex. O2-T2: Steal database from portal.dmz.bluex.ex	
10:30Z		O5-T1: Start deploying vulnerable VPS to every BT hosting to host malware (EICAR).	CERT sends out question to BTs asking if their DMZ DB data has been stolen.
10:45Z			Blondes send out confidential email from big.boss@int.bluex.ex to al.bundy@cust.bluex.ex with a UNIQUE string (that RT can use as evidence).
11:00Z	O1-R1: Defacement Repeat 1 in DMZ.		O9: WT sends sensitive emails to customer mailboxes.

11:30Z	O3-T2: Steal a confidential message from al.bundy@cust.bluex.ex account by compromising webmail.dmz.bluex.ex (email is sent by Blondes from big.boss@int.bluex.ex account on mail.int.BlueX.ex)		
12:00Z		O7-T1: Phishing campaign email and link. O7-T2: Phishing campaign: malware from link executed.	Blondes will click on the links on phishing email sent to big.boss@int.bluex.ex , enter their credentials and run the exe file (OutlookClient_NEW.exe) that the web server offers to download automatically.
12:15Z		O7-T3: Malware placed on shared-web hosting.	CERT demands takedown.
13:00Z	O1-R2: Defacement Repeat 2 in DMZ.		GT or WT deploys a legitimate machine to VPS hosting, that RT will attack O5-T2.
15:00Z	Automatic Scoring will be stopped		
DAY II			
08:00Z	O4: Fake compra sent to media from ’insiders’ in INT to journalist2@mail.ex (basically we need to break into internal network and send some compromising looking media to that journalist address)	O5-T2: KVM attack to degrade services and take down legitimate hosts in VPS hosting.	WT sends message to BT team leads a management demand to report SCADA readings every 30 minutes.
08:30Z	O9: Customer emails stolen and published O1-R3: Defacement Repeat 3 in DMZ.		Contractor's laptop plugged into INT
09:00Z		O6: SCADA attack - blow up.	
11:00Z	O1-R4: Defacement Repeat 4 in DMZ.		
11:00Z	SHOCK & AWE starts - all attacks are allowed		

13:00Z	Automatic scoring will be stopped

Appendix C: Legislation

C.1 Definitions

For the purposes of this Act:

1. **message** means any data transmitted between parties or to unspecified recipients in a communications network.
2. **identification data** means data which can be associated with a subscriber or user and which is processed in communications networks for the purposes of transmitting, distributing or providing messages. IP addresses are considered to be identification data if they are gathered from relayed network traffic.
3. **critical information infrastructure** means information infrastructure which is used by critical infrastructure (like air traffic control) and or to provide critical services to people (like emergency call centres).
4. **CERT** means a national CERT team (WT-CERT).

C.2 Processing messages and identification data

1. All messages, identification data and personal information are confidential.
2. The sender and intended recipient of a message are entitled to process their own messages and the identification data.
3. Messages and identification data can be processed with the consent of the sender or intended recipient.
4. Messages and identification data may be processed by the operator to the extent necessary for:
    - providing a service.
    - the purpose of ensuring information security of a service as provided in section 3.
    - the purpose of detecting a technical fault or error.
    - the purpose of exchanging traffic data between operators in order to ensure information security or to detect technical fault or error.
    - the purpose of providing information about information security incidents to CERT.
    - the purpose of fulfilling the requirements of national legislation.
5. Processing is only allowed to the extent necessary for the purpose of such processing.

C.3 Measures taken to implement information security

1. A telecommunications operator or any party acting on its behalf has the right to undertake necessary measures referred to in Section 2 for ensuring information security in order to:
    - detect, prevent and investigate disruptions to the information security of communications networks.
    - safeguard the communications ability of the sender or the recipient of the message.
2. The Measures referred to in Subsection 1 above may include:

    - automatic analysis of message content.
    - automatic prevention or limitation of message conveyance or reception.
    - automatic removal from messages of malicious software that pose a threat to information security.
    - using of darknets, honeynets and honeypots to detect information security incidents.
    - any other comparable technical measure.
3. If there is reason to believe that the message contains a malicious software or command, and automatic content analysis of the message cannot ensure the attainment of the goals referred to in Subsection 1, the contents of a single message may be processed manually.

C.4 Responsibilities of a telecommunications operator

1. A telecommunications operator must:
    - handle abuse if notified;
    - protect the critical information infrastructure;
    - notify the CERT without undue delay of all violations of information security;
    - provide to CERT additional information about the violations of information security (detected vulnerabilities, etc.); and
    - have the following email addresses:
        - Abuse (abuse@int.bluex.ex)
        - Service (service@int.bluex.ex)
        - Sales (sales@int.bluex.ex)
        - Info (info@int.bluex.ex).

C.5 Operator's right to disconnect customers

1. A telecommunications operator may disconnect customer if the customer is:
    - Spreading malware.
    - Sending spam.
    - Maintaining command and control server.
    - Conducting other kind of cyber attacks (e.g., exploiting vulnerabilities, hijacking traffic, causing disruptions and denial of service).
2. The customer must be notified and given 30 minutes to comply before disconnection.
    - You have to send the notification by email to white@mail.ex. Notification has to include the name of your company (team number).
3. If the customer conducts actions defined in Paragraph 1 repeatedly, he can be disconnected without notification.

C.6 CERT role

1. CERT can give additional regulation.
2. CERT can request additional information from the operator. The requested information must be provided without delay.
3. CERT can provide legal support to the telecommunications operator.

Appendix D:Blue Team Company Policy

Out-game remark: *The present company policy is a mandatory document of which Blue Teams must take notice. It provides generic guidance on the expected role-game behaviour of each team and reflects the scoring categories (type of scored activities) and priorities. A detailed scoring table will not be provided to the Blue Teams.*

You are the IT security team of a fictional ISP in an imaginary European country. Your company is an established actor on the local ISP market, having a well-formed corporate identity. The following is an excerpt of your company's policy regarding its IT services.

1. The company always complies with present law (see in-game Legislation and Rules) and does not tolerate any unlawful actions taken by its staff.
   The company will comply with all lawful requests of national authorities without delay.
2. The continuous availability of the IT services is of crucial importance for the well-being of the company and requires the highest attention. Integrity and confidentiality must be guaranteed all the time.
3. In case of an IT security incident, appropriate steps must be taken immediately and it needs to be ensured that similar incidents do not happen again.
4. Acknowledging the competitive ISP market, our company also understands its central role as part of the national critical infrastructure. As such, we want to promote and support cooperation in the ISP community and, in particular, with the national CERT, sharing crucial information where possible.
   For communication with the national CERT, a wiki-based reporting format was agreed upon in the past and shall be primarily used.
5. Our company aims for high customer satisfaction. All requests shall be managed in a timely manner.
6. Proactive cooperation with the media is important to prevent rumours and panic during an incident, also to raise awareness about safe behaviour and give instructions to users. Media relations shape the public image of the company. Every media inquiry requires an adequate and timely response. A short overview of incidents with the media needs to be marked down in the situation report to the management.
7. The management expects a situation report on regular basis (all 4h), informing them of the current situation and any important events as well as their current status (Appendix H: Executive Reporting).
8. The company expects all its departments to be managed in an organised way. Clear role allocation, proper documentation and efficient incident handling are expected.
9. The company uses an external service to host its systems in a virtualised environment. They provide 'restore from snapshot' service for an additional but expensive fee.
10. In case a situation requires that a customer (identified as the source of a security incident and in accordance with the legislation) is disconnected from the services provided to him, a dedicated email summarizing the reasons for this action **must** be set to white@mail.ex to inform the legal department of the circumstances.

Appendix E: Rules

E.1 Execution

1. Execution times will be the following:
    - **Day 0** 2011-03-26 10:00 - 17:00 GMT+3h (pre-exercise day).
    - **Day 1** 2011-03-27 10:00 - 18:00 GMT+3h (exercise day 1).
    - **Day 2** 2011-03-28 10:00 - 18:00 GMT+3h (exercise day 2).

E.2 Red Team Rules of Engagement

1. The objective of the Red Team is to conduct cyber attacks equally balanced against all Blue Teams participating in the exercise.
    - For this, Red Team follows a pre-defined campaign but is allowed to re-exploit earlier identified vulnerabilities in the Blue Teams' defence.
    - Successful attacks by the Red Team lead to negative score points assigned to the Blue Teams.
2. Red Team and White Team must work in close cooperation. While acting independently, the Red Team always has to follow the instructions given by the White Team.
3. In case of doubt about a certain action, or in case of introducing new attacks not initially planned for, the Red Team will consult the White Team first, seeking its permission.
4. All the attacks must stay inside the exercise environment. This includes social engineering attacks which will be not made outside the Gamenet.
5. If Red Team finds and/or exploits vulnerability in one Blue Team system, it must check for the same in all other Blue Teams' systems, also attempting to exploit it.
6. Red Team is not allowed to attack the core CDX infrastructure. This includes the services administered by Green Team such as Root DNS on dns.ex, mail server on mail.ex, Gamenet router router.ex, news site news.ex and scoring system.
    - In case of doubt, White Team is to be consulted first.
7. Red Team is not allowed to use self-propagating malware without the consent of and agreement from Green Team.
8. Red Team is not allowed to target Blue Team-owned machines used by its members to access the Gamenet.
    - Red Team is not to be held responsible if Blue Team members download some content to their own machines from the Gamenet and execute it.
    - After noticing that Red Team accidentally attacks a computer used by Blue Team members to access the Gamenet, Red Team will immediately stop all actions on this computer and inform White Team about this. No further claims may be raised against Red Team.
9. All Denial of Service (DoS) or brute-forcing actions which result in increased consumption of resources (e.g., CPU cycles, network bandwidth) have to be coordinated with Green Team. The purpose is to avoid DoS'ed VMs influencing all other systems.
10. High-traffic DoS attacks are not allowed. Still, RT is allowed to generate artificial traffic to cover other actions.

E.3 Rules for Blue Teams

E.3.1 Introduction

Blue Teams will play the role of an ISP in a fictional, European nation-state. This environment is described in the following documents:

a. Legislation providing a legal framework applicable to the ISP played by the Blue Teams.
b. A Company Policy which reflects aspects that will result in being scored. Blue Teams will not be provided with a detailed scoring table before the end of the exercise.
c. A Communications Plan defining the communication channels within the game environment as well as the call signs to be used.
d. A set of rules defining limitations of the use of the game environment and to ensure fair play between teams.

E.3.2 Team Composition

1. Each Blue Team may consist of up to 10 members who can be professionals or students.
2. Each team must appoint a Team Leader and Deputy Team Leader who are responsible for the overall management of team's activities and serve as a Point of Contacts (POC) to the exercise controllers.

E.3.3 Technical Environment

1. Blue Teams will get full access to their systems one week before the final execution for four days. Immediately before Day 1, all systems will be **reverted back** to the initial snapshots. Therefore Blue Teams will lose all changes made in the meanwhile and start the exercise from the original stage.
2. Blue Teams will get VPN access at Layer 2 into their network segments. Although Red Team is not allowed to attack the IP range reserved for VPN, it is up to the Blue Teams to ensure access even if attacked accidentally.
3. Blue Teams, acknowledging the very nature of this exercise, shall not have any confidential or valuable data on the equipment they use to connect with the game environment.
   - While not foreseen in this exercise, it cannot be guaranteed that hardware, introduced by the Blue Teams and connected to the Gamenet, will not become accidentally subject to attacks by the Red Team (including take notice and logical destruction of data) or get infected with malware.
   - The exercise organisers and especially the Red Team shall be free from liability for any damages or data loss caused as a result of participating in this exercise.
4. At the end of the first exercise day, the automatic scoring engine will be stopped and access to the game environment will be closed. Blue Team virtual machines may stay running and the Blue Teams will be allowed to finalise their activities in a 30 minute time window after the end of the exercise. Then the VPN connection will be cut.
5. Blue Teams will receive the final documentation one week before the Execution. It will include essential documents such as Legislation, Rules, Technical Documentation, instructions for Reporting, etc.

    - Draft versions will be made available beforehand and are accessible in the Blue Team collaboration wiki (starting from 15 February with the Test Run). Feedback and comments are welcome.

6. Technical documentation will be provided, but does not include specific details on patch levels or version numbers of systems deployed. The documentation includes:
    - Network scheme (being on purpose ‘outdated’ to reflect poor IT documentation practices in the given company).
    - List of systems and services Blue Teams have to maintain during the exercise.
7. As part of the initial configuration the Blue Teams are provided with, there will be ‘orphan’ systems and services running which are not required to be maintained. Blue Teams are allowed to disable any service or system that is not required (Blue Team Systems), but are responsible for figuring out and considering any dependencies between services.
    - If a Blue Team is unsure about the necessity of a particular system or service, they can consult with White Team. Points lost for accidentally disabled services that were required to be maintained will not be reimbursed.
8. All software products pre-installed on the VMs are covered by licences provided by Green Team.
9. Blue Teams are allowed to use own tools and software products but are required to guarantee proper license coverage where applicable.
10. Inside Gamenet, two repositories are deployed for providing a software updates service for Windows operating systems (wsus.ex) and Ubuntu 11.04 (aptmirror.ex).
    - Blue Teams are required to use these repositories only and not to download updates directly from the internet.
    - Blue Teams can assume these repositories to be current and not manipulated.
11. Access to the internet from within the Gamenet is only permitted via the (transparent) HTTP proxy.
    - The proxy is only meant for downloading patches, software updates or additional software which cannot be obtained from Gamenet repositories.
    - The usage of this proxy will be monitored by the Green Team.
12. Blue Teams are free to make any changes to, for example, the firewall and IPS rules, and to take defensive actions as they see appropriate, but will be held accountable for these. If the modifications interfere with the functionality of the scoring engine, resulting in not being granted availability scores for required services, there will be no reimbursement.
13. Blue Teams are permitted to replace originally deployed applications and services with new ones, providing that they deliver exactly the same content, data, and functionality as the original service. The user interface for employees and customers have to remain the same. All original user accounts for employees and customers must remain functional.
14. Changing the DNS names of systems providing required services is not permitted (the scoring engine relies on the initial DNS names).
15. Blue Teams can prepare up to two virtual machines to be deployed into their network with their own tools and services.
16. Reverting VMs to snapshot will be possible through the BT VM management interface, but it will result in a penalty.

E.3.4 Changing the Passwords

1. An administrative account ‘greenteam’ is present in many systems deployed for the Blue Teams.
    - Blue Teams are not allowed to disable, restrict, reset, replace, modify or use this account by any means throughout the entire exercise.
    - Red Team is not permitted to compromise ‘greenteam’ account.
2. Company employees are working all the time and are expect to experience as little inconvenience in their work as possible. This especially includes the ability to log into their workstations whenever necessary.
    - Only in case of a security incident connected with one of these employee user accounts it is permitted to reset their password.
    - If a password reset is deemed necessary, Blue Teams are required to document *user name*, *new password* and *brief reasoning* on the **Passwords** page of the team-specific Collab instance.
    - If an employee is not able to log in using the default password or the new one specified in that wiki-page, a penalty will be applied.
3. Blue Teams are not permitted to change passwords on behalf of the company customers at any time. This can only carried out by the customer. If this is seen as necessary, Blue Teams are requested to contact white@mail.ex, stating a short reason and requesting a password change.
    - This applies to all customer passwords such as portal accounts, email accounts, web hosting accounts, etc., as found present by the Blue Teams.

E.3.5 Complain and Appeal Process

If Blue Teams want to challenge a scoring decision or suspect a rules violation by other Blue Teams or the Red Team, they are free to bring it to White Team's attention by contacting white@mail.ex presenting briefly their argument.

- A complaint must be presented no later than two hours after the event in question took place.
- White Team will look into the complaint and provide a decision no later than two hours after reception.
- White Team decisions are final.

Blue Teams can formulate an appeal against the final scoring and submit it to the White Team leader no later than four hours after the end of the exercise.

- White Team will consider the appeal and provide the appealing party with an answer no more than 24 hours later.
- If the appeal is justified, the final scoring will be adjusted and communicated to the exercise participants.

Appendix F: Scoring Principles

1. Only Blue Teams’ performance will be scored, the actions of the Red Team will not.
2. All Blue Teams will be equally challenged, based on a pre-defined list of injects or attacks.
3. Blue Teams have the continuous task of keeping a set of services up and running, the availability of which is measured automatically and, if needed, verified manually by the White Team.
4. There six groups of scores, one measured automatically. These are:
   a. Service uptime and availability of services provided.
   b. Successful Red Team attack.
   c. Reporting and cooperation.
   d. ‘Common Business Cases’.
   e. Green Team requests, such as a VM reset.
   f. Special scoring such as rule violations.
5. Consistency of scoring is checked at a central point in the White Team.
6. Given scores are made visible to the Blue Teams after a short delay depending on the type of score.
7. Blue Teams can challenge a scoring decision by bringing their claims to the White Team’s attention – White Team will look into the matter and communicate their decision.

Appendix G:Situational Awareness Solutions

G.1 Finnish Yellow Team Solution

G.1.1 The Challenge

In BCS10, while different technical mechanisms were in place to establish situational awareness, one aspect was lacking. Human actions and observations were not collected and, as a result, it is likely that insights into human actions were lost. In turn, in the real world defending information systems may need collaboration between several distributed, even cross-organisational teams. Traditional reporting methods are cumbersome, and they lack the element of speed and machine readability for establishing proper situation awareness.

G.1.2 The Solution

The Finnish Yellow Team Solution is two-fold:

1. Provide a Lightweight method for humans to report their activities.
2. Provide the network traffic-based visualisations and drill-down capability to inspect game network's traffic.

The main focus will be on human reporting. The goal of the solution is to test whether an informal and Lightweight method for sharing operational information between stakeholders can be used for establishing situation awareness over incidents. Promptness is established by allowing teams to submit microblog-style reports from their observations and actions.

We will provide two reporting interfaces for the teams:

1. An instant messaging-based room for quickly submitting new information.
2. A wiki-based environment for updating and fixing submitted information.

As an intended side-effect of this method, we should be able to establish situation awareness just with a small modification to the workflows of different teams.

G.1.3 Promoting the Collaboration

Motivation is done in two ways:

- By following real-world processes to protect national critical information infrastructure:
  - ISPs (Blue Teams) will report their findings and actions to a CERT team, which in turn shares the information to help other ISPs (Blue Teams) to protect themselves.
- By scoring:
  - Reported observations and actions will be scored by two senior CERT team members, based on the quality of the reports. Blue Teams will be informed what kinds of reports are usable in protecting the critical infrastructure.

- Teams may also get extra points for providing valuable information to other teams.

G.1.4 Expected Result

- Team observations and actions are more visible to after-action analysis and thus will benefit the participants by providing better analysis results.
- Experience is gained as to how information sharing could be done more promptly, and without burdening the operational staff too heavily.
- As a result of more effective collaboration, observers, such as MNE7 participants in the White Team, can extract and report more high-level information more easily.
- Other observers, such as the Legal Team are better able to take notice of what happens at the ground level, and are thus better able to see the practical issues in cyberspace.

G.2 Swiss Yellow Team Solution

Life has become digital and many applications in the digital world improve quality of life in the real world (e.g., office@home, online banking, video telephony, etc.). However, these new technologies can also be used to perform criminal or illegal activities. Unlike in the past, a person and his/her activities often cannot be tracked without violating the privacy of others. An example is *internet data retention*: To track and observe the activities of *possible* criminal persons, the data/connection information of all users have to be saved. Moreover, criminals use more and more obfuscation techniques like *data encryption* or *hidden channels* to cover their activities.

We believe that maximisation of security can only be accomplished when everyone contributes. For surveillance, this means that everyone must accept a certain likelihood that his conversation might be recorded for future investigation, if it stands out of standard communication patterns. However, the data recorded about an individual must be kept to a minimum. Therefore we actively research methods to distinguish communications that are likely to have an implication for security from those which do not.

To make this distinction, we classify data streams using *Data Mining* algorithms and *Artificial Intelligence*. Our solution is very efficient in collecting and pre-processing data streams. The pre-processing step prepares the data such that reasonable information processing can take place. This includes feature extraction and normalisation of datasets. In the next step, we explore the streams to classify a flow into either interesting or uninteresting. After classification, the result is once more verified using mathematical reasoning. If after that, the data is still considered interesting, the data can be stored allowing further investigation when needed.

During the CDX, we plan to observe the data using *Emergent Self-Organising Maps* (ESOM). In short, these maps are a projection method based on an *unsupervised artificial neural net*, projecting high-dimensional data vectors into a two-dimensional data space. Thus, the underlying structure of a data set is not only analysable by computer algorithms but also by human eyes. Unlike other dimension reduction algorithms, which try to minimise a global projection error and often favour great distances, the ESOM *training algorithm* preserves the *local topology*, which means that local distances are almost correctly projected while ’far’ distances are still far but their real distances are biased in favour of the local distances. In the field of classification, this effect is welcome, because far distances denote different classes, while, for short distances, classification criteria like distances between data points and density of local structures can be accurately used for class membership decisions. Furthermore, additional projections on top of the map show 'natural' cluster borders based on local distance and/or density information and therefore can reveal structures in data sets which may be undetected else.

To sniff packets from the network layer, we use our self-developed software, called *Tranalyzer*. This tool is responsible for combining the packets to Layer 3 or 4 flows and extracting/calculating features. After this step, a single flow is now represented as high-dimensional vector, where every feature represents one dimension of the vector. Useful features determined before are then pre-processed and projected on an ESOM specially trained for the specific type of network data. The significance of a feature is based on a specific question to the data. In our case, the question could be 'Differentiate between normal internet traffic and attacks from the Red Team, furthermore differentiate between the types of attacks.' In the ideal case, all vectors and therefore flows describing an attack are located in a map's region completely different from the ones which describe 'normal' traffic.

The use of statistics has the advantage that our system is able to assign variations of the same application source to the same class. For example if a malicious software construction kit produces various instances of a specific prototype code (e.g., the Zeus Botnet construction kit), where every instance has a different signature (because of different naming, hard-coded IP addresses, etc.), our system would classify correctly all these instances as members of this construction kit. This is because the underlying principal behaviour of the prototype code will be still the same. Furthermore, we can avoid analysing the payload in depth (for example looking for specific keywords) which also makes us able to deal with obfuscated and even encrypted data streams. Last but not least, without the need of deep packet analysis we can anonymise the payload before processing it without any disadvantages to our solution and thus are able to preserve most of the privacy of the users.

A critical part of this approach, when it is used in live systems, is the trade-off between the number of packets collected per flow – in the following called N – and the accuracy of a classification decision – called A. If N is too low, then A is also low which can lead to high false positive or false negative rates. If N is too high, an attack might be over before the ESOM is able to take a decision. Therefore an important part is to determine an appropriate N for every specific question and network data.

Appendix H:Executive Reporting

This Appendix provides information on how the Blue Teams were expected to report to their management.

H.1 Reporting Instructions

You are expected to write a report directed to your company's senior management in a language suitable for them. This report is required at 13:00 and 17:00 on both days. It must be compiled on your team-based collaboration site and link to the page has to be sent to boss@mail.ex

- The very last report is expected to be more comprehensive and to summarise the two exercise days. It will be scored higher than the others. The first three reports shall not exceed 400 words, the last one 600 words.
- The report should consist of four core items following the structure below.
- The sub-items are to provide you with more information on what you could consider to touch upon.

H.2 Contents of the Report

Team:

(add name of your team)

Report time period:

e.g. 2012-03-05 13:00 – 17:00

H.2.1 Current Situation

- Executive summary describing briefly the current situation of operations.
- Summary of issues of major importance or impact on operations. Focus on the ones in the given time-frame, and those from earlier still having an impact or relevance. In your summary consider:
  a. What happened: a brief description of what, when, how?
  b. Who did it: if you have reasons to believe you know who caused the incident, provide identity and short reasoning.
  c. Impact or damage on operations: briefly describe the impact this incident had on your services. Consider downtimes, damage to customer basis, negative PR, potential legal actions taken against you, etc.
  d. Actions taken: describe the major steps taken by you to mitigate the issue; has the source/vulnerability of the incident been discovered - if so which was it?
  e. Current status.

H.2.2 Any other business

- (If you have further information or recommendations for management's attention).

H.3 Example Report

Team: Blue 1

Report time period: 2012-03-05 1300 - 1700

H.3.1 Current Situation

Two hours ago we faced a successful web defacement of our corporate web page, where a hacker calling himself ‘XXX’ placed a message stating ‘STOP SPYING ON PEOPLE’. The original condition of our website was restored after 35 min. We are still investigating the reasons for the successful defacement. The website functionality and other dependent services were not interrupted over this time-frame.

This incident got noticed by the media and we were confronted with an unpleasant media inquiry by Hackers Daily Magazine.

We also noticed a couple of unsuccessful attempts to get unauthorized access to our email server.

The malware infection, reported earlier this day, has been successfully stemmed. The cause of it has been identified (a customer’s service got hacked via a plugin having an unpatched but known vulnerability used for further spreading) and the customer was supported in enhancing his security. Furthermore, we have introduced additional means to detect and respond more quickly to similar cases in the future.

H.3.2 Any Other Business

Regarding the malware infection, the management should consider communicating the reasons for this incident and the actions taken to the other business clients in an appropriate way.

Appendix I: Lightweight Human Reporting

I.1 Introduction

In the following we describe the Lightweight Human Reporting system from a Blue Team's perspective. These reports are meant to be sent to the CERT team by using one of the following ways:

1. Form-based wiki reporting.
2. Chat-based wiki reporting which is done via the TweetBot lurking on Blue Team chat channel.

I.2 What to Report

Most important details for the CERT team are answers to these questions:

- **what**: a free-form description of what has happened. The most important aspect to report!
- **where**: which network segment has been attacked? E.g., DMZ or INTERNAL.
- **when**: when this event took place? This information is added automatically by the reporting system.
- **who**: who handled this incident?
- **why**: what was the motivation of the attackers (if known)?
- **attackerip**: the IP for the attackers used to perform the attack (can be several).
- **victimip**: the IP of the attacked system (can be several).
- **status**: once you are satisfied with your incident report, you can submit it to the CERT team for review by changing the...
- **status**: to review. Once the CERT Team has scored the incident, you will see it in the table below. Please note that creating your own scores for incidents will lead to automatic disqualification.

I.3 Creating Incident

The easiest way to report a new incident is to use the TweetBot on Blue Team channel, e.g. with the following message:

Message
#simplereport what='Our website was defaced' @svimes

This will cause the TweetBot to create a new incident with the name 'simplereport' on your Incident Tracking page as follows.

	what	when	where	who	why	attacker ip	victim ip
simplereport	Our website was defaced	2012-02-08T12:01:33.748328		svimes			

The incident reporting relies on the aforementioned 5Ws (WHAT, WHERE, WHEN, WHO, WHY) and a number of IPs belonging either to an attacker or your system(s) that have been attacked.

I.4 Updating an Incident

This information can be filled in iteratively as the situation develops through a number of tweets related to your incident. Here's a more complex example of incident reporting conducted through a number of tweets:

- Again first the incident is created as follows with the example incident name ‘fullreport’:

Message

#fullreport what=’Our webserver was compromised through a SQL injection and defaced as a result.’ @svimes

- Then as the situation develops, the incident is updated as follows with the compromised system details of network segment and IP:

Message

#fullreport where=DMZ ‘victim ip’=1.2.3.4

- As more information becomes available the incident is again updated with the IP of the attacker:

Message

#fullreport ‘attacker ip’=6.6.6.6

- And finally the Blue Team is able to discern an inkling as to why the attacker did what they did:

message«

#fullreport why=’Based on the defaced website analysis, the attack seems to be the work of hacktivists.’

- And presto, we have filled in the best available details for the CERT team to assess and score our incident report, which is as follows:

	What	When	Where	Who	Why	attacker ip	victim ip
fullreport	Our webserver was compromised through an SQL injection and defaced as a result.	2012-02-10T11:48:22.997114	DMZ	jani, svimes	Based on the defaced website analysis, the attack seems to be the work of hacktivists.	4.5.6.7, 8.5.4.3	1.2.3.4

- Later on it is discovered that our initial analysis was faulty and @jani tweets the following correction:

message«

#fullreport @janianalyzed the logs again that the attacker ips were actually ‘attacker ip’=4.5.6.7 and ‘attacker ip’=8.5.4.3

- This results in an updated situation awareness of the incident as follows:

	What	When	Where	Who	Why	attacker ip	victim ip
fullreport	Our webserver was compromised through an SQL injection and defaced as a result.	2012-02-10T11:48:22.997114	DMZ	jani, svimes	Based on the defaced website analysis, the attack seems to be the work of hacktivists.	4.5.6.7, 8.5.4.3	1.2.3.4

I.5 Submitting an Incident for Review

- Once you are satisfied with your incident report, you can submit it to the CERT team for review. This is done by setting the value of the **status** key to **review** as follows:

message
#fullreport status=review

- This will signal the CERT team that your incident report is ready for review. They in turn will changed the status to **scored** once they have reviewed your incident report with the appropriate score, justification and name of the CERT team member who gave the score. Please note that Blue Teams scoring their own incidents will be automatically disqualified.

	What	**When**	**Where**	**Who**	**Why**	**attacker ip**	**victim ip**	**status**
fullreport	Our webserver was compromised through an SQL injection and defaced as a result.	2012-02-10T11:48:22.997114	DMZ	jani, svimes	Based on the defaced website analysis, the attack seems to be the work of hacktivists.	4.5.6.7, 8.5.4.3	1.2.3.4	review