Baltic Cyber Shield Cyber Defence Exercise 2010

After Action Report

Executive Summary

Baltic Cyber Shield (BCS) is an international technical cyber defence exercise (CDX). It was first time executed in May 2010 although a proof of concept exercise conducted in 2008 preceded the event.

The exercise was organized in collaboration with several organisations coordinated by Cooperative Cyber Defence Centre of Excellence (CCDCOE) and Swedish National Defence College (SNDC). Besides CCDCOE and SNDC the main contributors were Swedish Defence Research Agency (FOI), Estonian Cyber Defence League (ECDL), Swedish Civil Contingencies Agency (MSB), Swedish National Defence Radio Establishment (FRA), NATO Communication and Information Systems Services Agency Computer Incident Response Capability - Technical Centre (NCSA NCIRC - TC), and Clarified Networks.

During the exercise six Blue Teams, composed of public, private sector, and academic personnel had to defend virtual computer networks against hostile Red Team attacks. The game scenario described a volatile geopolitical environment in which a newly hired team of cyber security experts was asked to defend the IT systems of a power generation company in the face of increasingly sophisticated attacks by a group of hackers. The Blue Teams were competing with each other and their activities were measured by automatic and manual scoring.

The exercise was perceived as a great success by all the participants, especially by the Blue Teams. An overall objective of the exercise was to gather lessons identified for the future, something that was fulfilled and is reflected in the following. The purpose of this report is to identify what the lessons identified – later to be learned – were from planning and executing the Baltic Cyber Shield exercise.

Contents

1 Introduction 3

2 Objectives 4

3 Background 5

4 Execution 8

5 General Lessons Identified and Recommendations 16

6 Conclusions 18

7 Acknowledgements 19

8 ACRONYMS 20

1 Introduction

Baltic Cyber Shield (BCS) is an international technical cyber defence exercise (CDX). It was first time executed in May 2010 although a proof of concept exercise conducted in 2008 preceded the event.

The exercise was organized in collaboration with several organisations coordinated by Cooperative Cyber Defence Centre of Excellence (CCDCOE) and Swedish National Defence College (SNDC). Besides CCDCOE and SNDC the main contributors were Swedish Defence Research Agency (FOI), Estonian Cyber Defence League (ECDL), Swedish Civil Contingencies Agency (MSB), Swedish National Defence Radio Establishment (FRA), NATO Communication and Information Systems Services Agency Computer Incident Response Capability - Technical Centre (NCSA NCIRC - TC), and Clarified Networks.

During the exercise six Blue Teams, composed of public, private sector, and academic personnel had to defend virtual computer networks against hostile Red Team attacks. The game scenario described a volatile geopolitical environment in which a newly hired team of cyber security experts was asked to defend the IT systems of a power generation company in the face of increasingly sophisticated attacks by a group of hackers. The Blue Teams were competing with each other and their activities were measured by automatic and manual scoring.

2 Objectives

The BCS 2010 had the following objectives:

1) Increase the understanding of the international cyber environment (including legal aspects) and the need for cooperation. The objective was fulfilled through the bilateral work within the project team and via lessons learned.
2) Develop and increase international cooperation in handling technical cyber incidents through common training and sharing of best practice.
3) Increase cooperation between agencies at national level and increase the understanding of how to create cooperation. The objective was fulfilled by multi-agency participation and engagement.
4) Increase public-private cooperation by inviting the private sector to be a part of the Blue and Red teams and by cooperation between public sector and students.
5) Train IT-security students and professionals.

   Blue Teams were defined as the main training audience. Each Blue Team consisted of 6-10 members, either professionals or students. The CDX provided the Blue Teams an environment where operational aspects of administrating IT systems under large-scale cyber attacks could be exercised. Red Team's campaign was divided into phases with increasing intensity.
6) Improve the capability of conducting technical exercises. Research papers and after action report will be produced and issued through bilateral collaboration.
7) Study IT attacks and defence in CII/SCADA (Critical Information Infrastructure/Supervisory Control and Data Acquisition) environment. The aim of the CDX scenario and technical set up was to engage attacks against computer environment around CII/SCADA process- and control systems.
8) Exchange information and experiences through interaction within the project team and the training audience and as well through the final report.

3 Background

3.1 Participants

3.1.1 Management Team

The Management Team was responsible for planning and setting up the exercise, and writing after action review. For the execution the members of the Management Team were divided between Green, White and Red Team.

3.1.2 White Team

The White Team was responsible for developing the rules, including scoring rules. During the execution the White Team acted as exercise controllers' cell by assigning manual scores and evaluating the progress of the Blue Teams. The core of the White Team consisted of 3 persons: 1 in Tallinn scoring successful attacks and 2 in Stockholm being part of a configuration control board (CCB), and a computer emergency response team (CERT) collecting and evaluating incident reports, etc. However, more persons where part of the White Team during preparation.

3.1.3 Blue Teams

The task of the Blue Teams was to secure a pre-built IT infrastructure of a small company and defend it against the Red Team's attacks. Blue Teams had to maintain services listed in the requirements document assuring availability, confidentiality and integrity of the systems. The size of the Blue Team was limited to 10 members.

The following teams participated in BCS 2010:

1) NCSA - NCIRC TC Blue Team – located in Mons, Belgium
2) Lithuanian Blue Team of IT specialists from governmental agencies – located in Kaunas
3) Latvian Blue Team of IT specialists from governmental agencies – located in Riga
4) Swedish Team of technicians from different agencies – located in Stockholm
5) Swedish Team of IT experts – located in Stockholm
6) Swedish Team of students – undergraduate and graduate students from KTH Royal Institute of Technology, located in Stockholm

3.1.4 Red Team

Red Team's mission was to compromise or degrade the performance of the systems that were protected by Blue Teams. Red Team had to ensure a balanced and sustained pressure on all six Blue Teams.

As the focus of BCS 2010 was to train the Blue Teams, Red Team used a white-box approach. They were provided all the documentation and access to the Blue Teams systems 3 weeks beforehand.

Red Team was composed of 20 voluntary participants working for private sector and governmental agencies from Estonia, Finland, Sweden, Latvia and NCSA - NCIRC TC.

3.1.5 Green Team

Green Team (also called Technical Team) was responsible for preparing the technical infrastructure in the lab. This included the VPN access to the pre-built Blue Team's systems, visualization solutions, communication, recording and logging facilities, etc.

3.2 Scenario

According to the CDX scenario a "cyber warfare division" of the extreme environmentalist movement called Klimate Kaos Krew (K3) threatened to attack six power companies located in Belgium, Latvia, Lithuania and Sweden, unless they agree to convert to green power alternatives. Coincidentally, the power companies in questions had just failed a cyber security inspection and had fired most of their IT staff. There were fears about insider threat.

Blue Teams were tasked to assemble a Rapid Reaction Team to take over the responsibilities of administration and protection of the IT systems of the power company. Red Team's role was to play the angry environmentalists.

3.3 Technical Environment

3.3.1 General Infrastructure

Technical infrastructure for the CDX was set up in lab located at FOI in Linköping. It consisted of 9 racks each of which contained 20 older servers (2x 2.2GHz Xeon processors, 2 GB RAM, 80 GB HDD, 2 10/100Mbit Ethernet interfaces). The servers were running VMware Server 2.0.2 on Gentoo Linux. In general the network was divided into 2 segments: management network and game network.

The teams accessed the lab environment remotely from their home countries over OpenVPN.

3.3.2 Blue Team Systems

Blue Team's infrastructure represented a typical company network including additionally some SCADA components. The network consisted of 28 different Windows and Linux based VMs (VM) divided between 4 segments:

- DMZ: publicly available services such as website based on old version of Joomla CMS; custom-made PHP web application acting as customer portal; a news site set up using WordPress; MS-SQL database server collecting reports from SCADA systems; DNS; NTP and e-mail (SMTP, POP3, IMAP, SquirrelMail) servers
- INTERNAL: domain controller, fileserver, intranet server, back-end database server running MySQL, Windows workstations
- HMI and PLC hosting lab SCADA systems: remote factories, and systems simulating power production, distribution and consumption and monitoring of those systems. This setup consisted of Programmable Logic Controllers (PLC); small steam engines, models of solar power plant, power distribution grid, industry and village; software called Cimplicity acting as Human-Machine-Interface (HMI)

Network segments were separated by 3 Netfilter firewalls.

Initially, all the Blue Teams had identical setup that was significantly insecure. Operating system components, network services and applications were unpatched and vulnerable. The systems were full of configuration errors, weak passwords and SSH keys generated on vulnerable Debian

installation were used, unneeded services were enabled, personal firewalls and anti-virus was turned off on some hosts. Red Team was allowed to use even pre-planted backdoors and malware.

3.4 Rules

Blue Teams and the Red team had to comply with a long list of regulations. For instance the size of the Blue Teams was limited to 10 persons, the Blue Teams had to follow quite complex change management rules – for some changes like patching operating system permission had to asked from configuration control board (CCB) played by the White Team. They also had to stay in the legal framework of their home country which essentially prohibited counter attacks.

Red Team was supposed to do a close cooperation with the White Team, they were not allowed to attack the systems part of the general infrastructure like core routers or scoring system, social engineering and VM escapes were also prohibited. However, Red Team still had relatively free-hands to choose specific tools or attack methods to achieve their goals.

3.5 Communication and Information Sharing

Many different environments and tools were used for information sharing and communication among the organisers and participants:

- Wiki-based collaboration environment: different instances for Green, Red and Blue Teams. Wiki was most actively used for planning the work by the Green and Red Team. Green Team also documented the technical infrastructure in wiki. Red Team used it to map the skills of the people, develop attack scenarios, track the successful attacks during the execution, etc.
- XMPP based chat
- MS Groove mostly for sharing files and developing documents such as the Blue Team packet, project plan, writings covering data collection.
- VTC, WebEx, Gotomeeting, Skype for virtual meetings and web conferences. During the execution VTC was established between Linköping (Green Team), Stockholm (White Team) and Tallinn (White and Red Teams)
- Website for hosting specific tools required for the observers
- Scoreboard – a custom PHP application displaying both automatic and manual scores

3.6 Data Collection

A group of persons was specifically focusing on collecting all relevant data from the CDX that could be beneficial for post-exercise analysis. An observer was sent to five out of six Blue Teams and also to the Red Team.

4 Execution

Baltic Cyber Shield was executed on 10-11 May 2010. Blue Teams were given only limited access to the CDX environment beforehand for connectivity testing.

4.1 Planned Phases

The White Team decided to divide exercise into four phases each lasting approximately 3.5 hours:

1) **Phase I - Border skirmishes**

   Red Team objective during this phase was to deface public website with a "war declaration" from K3. They were also allowed to map target systems, gain control over not more than one server in DMZ in addition to the public websites and compromise not more than one workstation in INTERNAL network via a client side attack.

2) **Phase II - Perimeter breach**

   The objectives of the second phase were to compromise (confidentiality, integrity and/or availability lost) all "scored" systems in DMZ and in INTERNAL.

3) **Phase III - Crown jewels**

   During third phase Red Team was tasked to gain access to all "scored" systems in HMI (Human-Man-Interface) segment where the monitoring and controlling stations of the SCADA systems were located.

4) **Phase IV - Berserker rage**

   This phase was meant for causing maximum disruption and damage to all target systems.

4.2 Overview of the Events

4.2.1 Phase I

The first exercise day begun at **07:00Z**[1] with opening announcements from Lars Nicander, director of the Center for Asymmetric Threat Studies (CATS) in SNDC, and Col Ilmar Tamm, director of the CCDCOE.

Before the exercise all the Blue Teams had VPN access to the lab environment but they were not provided any user accounts and passwords for the VMware Consoles and VMs. Passwords were delivered at **07:40Z** and the official STARTEX was announced.

The start was slow because of different technical issues. For example administering the exercise environment and using Internet facing communication channels simultaneously proved rather complicated. There were also VPN connectivity issues and trouble with accessing the VMware Server Console.

Red Teams actions were kept back until majority of the technical issues were solved. The Red Team was given permission to start achieving phase I objectives at **8:50Z**. After an hour and an half 5 out of

[1] Coordinated Universal Time, i.e. UTC/GMT/Zulu time was used for the exercise . The time was 09:00 in Mons and Stockholm, and 10:00 in Tallinn, Riga, Kaunas and Helsinki.

6 Blue Teams had one of their web site defaced with a declarations like „STOP USING NUCLEAR POWER. HACKED BY K3“ and „K3: nu:kz R b4d“.

The scores for automatic availability checks were reset at **10:25Z** such that the initial connectivity problems would not have so much impact on the final results.

4.2.2 Phase II

During the second phase (start was announced at **12:15Z**) Red Team kept increasing pressure on the DMZ systems. They were able to gain access to more web servers and deface the sites, compromise MS-SQL server collecting the reports from SCADA systems, exploit vulnerability in the e-mail server giving them root access and also take some services down with denial of service exploits.

In some cases the job was really easy for the Red Team. For instance the Windows based database server was initially running a VNC[2] which firstly did not require any authentication and secondly was remotely exploitable. Few Blue Teams did not even reconfigure the service such that it would ask for a username and a password.

One of the Blue Teams had only 4 members. They were all Windows administrators without real experiences with Unix-like operating systems. As all the firewalls were based on Linux Netfilter they had real difficulties with managing the firewall rules and closing down access from the external gamenet to their internal network segments. The initial configuration of the external firewall was purposely insecure leaving access to internal segments wide open. Therefore Red Team was able to gain access to a workstation inside that Blue Team's internal network directly without client-side exploit.

Red Team finished their business for the first day at **14:45Z** and then Blue Teams had about half an hour to fill in feedback forms and to complete any on-going administrative activities.

4.2.3 Phase III and IV

The second exercise day started with SQL injection (SQLi) attacks against Windows based web-server hosting the public website of the company at **07:30Z**. Although the Blue Teams had now somewhat patched or hardened servers and it was not possible to gain administrative shell access, SQLi still worked against 4 teams. Red Team did not try to deface anything this time but just dropped the databases.

According to the plan, client-side exploits should have been used already during the first day. Unfortunately White Team was facing serious lack of staffing to simulate the users and "do the clicking". There was also no automatic system which would simulate the actions of security ignorant users such as opening carelessly e-mail attachments or clicking on suspicious links. Another problem was again VMware console. White Team was not prepared to use RDP or VNC to access Blue Teams office workstations. The VMware console on the other hand was tremendously slow and unresponsive. As a consequence:

1) White Team was only able to click on links provided by the Red Team from few Windows computers in each Blue Team network. One of the browser exploits did not work and the other was successful only on one Blue Team machine (**09:45Z**).

[2] Virtual Network Computing – a remote control software with graphical user interface

2) Red Team had limited possibilities to gain access to the Blue Teams' internal network segments where many of the most important targets (SCADA control and monitoring hosts) were located. In fact, Red Team possessed a 0-day exploit taking advantage of vulnerabilities in Internet Explorer 6 and 7 and Firefox, tested to be working on Windows XP, Ubuntu Linux and Mac OS X[3]. The effective client-side attack was in fact conducted using this 0-day exploit.

An effective method of gaining access to the INTERNAL, HMI and PLC segments was to use the default passwords on the firewalls. Half of the Blue Teams had not changed those accounts. Therefore Red Team members were able to use machines with backdoors in the DMZ to get into the external firewall and jump from that to the next. This resulted in giving the Red Team access to the critical PLC interfaces in case of few Blue Teams[4].

According to the reports 2 out of 6 Blue Teams basically managed to keep Red Team out of their internal networks. Red Team was capable of conducting remarkable damage against one Blue Team by "autopwning" 9 internal office workstations simultaneously.

Two Blue Teams also had the back-end MySQL database compromised which was located in the INTERNAL segment. Public client portal in DMZ needed to communicate with it and thus there was connection allowed from DMZ to INTERNAL segment. However, as far as we know, Red Team did not succeed to use those hosts as a platform for further attacks in internal networks.

During the third phase Red Team continued attacking DMZ hosts, as the client-side exploitation did not work as expected. Note that Red Team was allowed to attack the same host exploiting the same vulnerability again after 60 minutes had passed from publishing the previous incident on the scoreboard.

Attacks affecting the availability of the services were intensified step-by-step. In the end Red Team started to purposely shutting down the hosts they could access and use different denial of service methods.

At **12:00Z** The automatic scoring was stopped, Blue Teams were still required to keep all their services up but they were allowed to patch all their systems without asking permission from the CCB. Red Team was given a permission to cause as much as damage they could[5]. Green Team revealed to the Red Team details about kernel level rootkit that had been planted on specific hosts (2 out of 6 Blue teams were still vulnerable). The reasoning behind stopping availability checks was that White Team could not be sure how much impact Red Team's activities could have on the general network infrastructure. In reality, this was not a good decision because many of Blue Teams were not motivated to continue protecting their systems.

The only factory was blown up approximately at **13:00Z**. One of the reasons why Red Team did not succeed with the attacks against SCADA components was miscommunication with the Green Team.

[3] The vulnerability was reported to the vendors. One month later no patch had been still released.

[4] Compromising a firewall was not taken into account by the White Team when assigning manual scores. Unfortunately the Red Team did not document all successful attacks from which the Blue Teams was not penalized. The focus was writing down events that the White Team used for assigning manual points. Therefore also the attacks against availability were poorly documented.

[5] Multiple Linux machines were destroyed by executing „rm –rf /"

Red Team did not know how the process in the factory actually worked and respectively how to set the fireworks attached to the logic controller on fire. There is a hypothesis that the factory was burned down because of an effective fuzzing attack against the Modbus protocol.

The end of the exercise was announced 30 minutes before the initial plan at **13:30Z.** Rest of the day was spent on hot wash-up, collecting feedback and announcing the final scores.

It is interesting to note that after dropping the databases of MS-SQL server in the very beginning of the second exercise day, Red Team did not have any successful scored attack against confidentiality or integrity of the systems administered by Blue Team 5, who was declared as the winner of the CDX.

4.3 Red Team Activities

Red Team consisted of approximately 20 volunteers with different skill set and background in penetration testing. Although the team was international with members from different organisations they were very good at internal collaboration. Red Team used a wiki-based collaboration environment to plan the work, map the skills, write down scenarios, document Blue Team networks, find interesting targets and track successful attacks during the execution. At the preparation period chat was mostly used for internal communication. Red Team had 2 collaborative exercises where they were able to access the first Blue network set up by the Green Team and test out some of the attacks.

For the execution of CDX Red Team was divided into 4 smaller sub groups – web application testers, fuzzing, client-side, and remote exploitation team. After successful attack against one team the same method had to be repeated on all the other Blue Teams. However, it was not easy to keep the pressure balanced. Therefore sometimes Red Team members focused too much on particular Blue Team.

Initially, the Blue Teams network was significantly insecure and it was not hard to achieve the first objective to deface a public website. The following lists some of the Red Team's tactics:

- Exploiting publicly-known vulnerabilities in Windows operating system such as MS03-026, MS04-011, MS06-040, MS08-067, MS10-025; and in other network services like Icecast or SQUID3.
- Using VNC without authentication – on some machines the initial configuration of VNC even did not require password and username. In case the Blue Teams had set the password, there was still a NULL authentication vulnerability in RealVNC 4.1.1.
- Taking down mail servers because sendmail used vulnerable clamav-milter plugin.
- Hacking web applications which were based on older versions of content management systems such as Joomla and Wordpress and a custom made PHP client portal:
    - Initially, administrative interfaces for web applications had a default, weak or no password at all (e.g. Joomla management interface, phpMyAdmin). Note that the Webmin installed into the firewalls also had the same issues.
    - Common web application vulnerabilities were exploited such as SQL injection, local and remote file inclusion (LFI and RFI respectively), path traversal, and cross-site scripting.

  - The custom web application was firstly exploited using RFI vulnerability. Red Team uploaded “Emp3ror Undetectable” PHP shell to the server which allowed them to read the contents of the files. Source code and database connection passwords were stolen using this method. Soon, many Blue Teams reconfigured their servers to disallow remote file inclusions. Still, the Red Team was able to exploit the same vulnerability with local file inclusion using PHP Protocol input wrapper method.

- Metasploit framework was one of the most popular attacking tools for exploiting publicly known vulnerabilities, generating malicious payloads, and deploying reverse backdoors.
- Escalating privileges in Linux systems after initial compromise using local root exploits in the kernel. For instance, a particular vulnerability in vmsplice() system call was exploited. Similar methods were applied on Windows – using local privilege escalation to gain SYSTEM privileges.
- After gaining sufficient privileges, taking the user accounts and password hashes from already compromised systems, cracking weak passwords and trying to use those on other systems. In case of some Windows systems Red Team was able to use attack method called pass-the-hash because many machines had the same administrative account with the same password on them.
- Disrupting the availability with fuzzing tools, Slowloris against Apache web server, exploiting denial of service vulnerabilities in NTP daemon and Squid3 web proxy, SYN flooding or just shutting down the hosts.
- Modifying compromised systems in various ways:
  - Fortification of machines to make the attacks persistent. Usually Poison Ivy, Zeus bot, Optix and netcat were installed as backdoors, the functionalities built into Metasploit were utilized (persistent meterpreter), new administrative accounts were added, PHP shells dropped, etc
  - Altering the victim’s crontab file to continuously drop firewall rules
- Using pre-installed malware and backdoors:
  - Zeus
  - Kernel loadable module rootkit called eNYe LKM
  - ICMP bindshell which XORed the traffic with static key (some blue teams blocked ICMP traffic in their firewalls so it was then not working anymore)
  - A backdoor that continuously searched for the commands from Apache web server access.log

Red Team possessed a zero-day client-side exploit for Internet Explorer 6 and 7 and Firefox. It was confirmed to be working on Windows XP, Mac OS X and Ubuntu Linux. As the White Team did not manage to properly simulate users the client side exploits were not widely used. However, the successful client-side attack was conducted using this zero-day exploit. Firstly the Red Team gained user privileges to the hacked system and then used local privilege escalation vulnerability to gain SYSTEM privileges and dump password hashes.

4.4 Blue Team Activities

4.4.1 Blue Teams in General

Naturally, every Blue Team was different when comparing the background of the team members, their skills and motivation. This resulted in different strategies and tactics used to defend their networks. For instance, One of the blue teams firstly closed all incoming and outgoing traffic on their external firewall and started to patch the systems. By following this strategy they lost a great deal of availability points but naturally the Red Team managed to conduct only few successful attacks against this team. This blue team was also the only team who replaced vulnerable PHP application with simple static page with a press release describing the situation.

We will cover in detail the Blue Team 5 strategy and tactics – Blue Team 5 was declared as the winner of the BCS 2010.

4.4.2 Blue Team 5

Blue Team 5 was composed of persons who replied to an e-mail sent by the team leader to an e-mail list of security community in Sweden. Initially, the plan was to assemble completely distributed team physically located in different places. In the end there was only one remote participant. The roles in the team were divided as follows:

- 1 person for administrating VMware Console
- 2 persons to administer the firewalls (infrastructure)
- 3 persons to administer Windows machines
- 2 persons to administer Linux machines
- a leader for coordinating the work inside the team, communicating with the White Team and compiling incident reports

The following list provides an overview of some of the activities and decisions made by Blue Team 5:

- A hardened VM was prepared and essential services (NTP, DNS, Webmail) were moved to that server:
    - According to the scenario all the servers could have been completely compromised and it would be extremely difficult to find all pre-planted backdoors and rootkits.
    - The team members knew that SquirrelMail application could have serious vulnerabilities and thus has to be replaced.
    - The hardening of team's own server included mandatory access controls in form of AppArmor-profiles. Everything/All was done to lock down unsecure programs.
- Patching was not used at all. It was a conscious choice since the team did not believe this would have changed the situation. For instance patching does not help if there are backdoors already in the systems.
- White Team was proposed to use OOB communication channel in the beginning of the exercise as the mail server could have been compromised.
- Before the exercise a list of tools that could be used was compiled. Also some planning was done in the wiki.
- Team decided not to use reverting of the VMs as that would have cost points.

- For remote administration SSH, RDP and VNC were utilized. VNC was locked down as one of the first actions.
- On firewalls, Webmin was configured not to run as root. Actually, this could be seen as violation of the requirements. It was not possible to administer the server anymore over the Webmin. Unfortunately White Team did not verify if the functionality of the services has been preserved.
- All existing firewall rules were dropped and written from the scratch.
- For protecting Linux systems, the initial idea was use Samhain host-based IDS and compile it to be working in stealth mode. As someone was afraid that it would be complicated due to dependencies the idea was dropped. In reality, compiling Samhain would have been simple - so it was pity that the idea was dropped. Instead, AppArmor was used extensively and custom small shell scripts also proved to be very useful.
- Computer Integrity System CIS SE46[6], kernelGuard and small special tools were used to protect Windows servers. This made it more or less impossible for the Red Team to install new software without the consent of Blue Team members. Central syslog server was set up and the logs from Windows machines were sent that system. However, no log correlation was done.
- The team was capable of finding most of the backdoors installed on Windows hosts.
- For fighting against SYN flooding, SYN cookies proved to be helpful.
- Packet sniffer called *tcpdump* was constantly running on the external firewall. The team tried to analyse traffic patterns and use rate limiting based on expectedly normal user behaviour. DNS traffic was also monitored. Unfortunately, Clarified Analyzer was not used due to lack of experiences and previous knowledge of this tool.
- The attacker's IP addresses were blocked case-by case. Traffic from hostile machines was either black-hole routed or redirected.

4.5 White Team Activities

White Team injected a legal business task in the morning of the first day. The Blue Teams where requested to send incident reports twice per day. White team also served as a substitute for the power generation company's management to which Blue Teams e-mailed their own requests. For instance, requests were for management policy decisions on contacting the CERT as well as law enforcement and security services. The management was also advised to draft press releases describing the situation at hand, having its legal advisors updated and ready to deal with various civil and criminal suites, etc.

4.6 Green Team Activities

Green team activities during the exercise concerned monitoring the technical infrastructure, managing data collection and decide about approval or denial of those of blue team requests that concerned changes in technical infrastructure. The technical environment remained relatively stable during the exercise which led to that most of the work in the green team was focused on the data collection. A lot of time was spent during the first day with debugging the Blue team 1 connection

[6] http://www.se46.se/produkter/eng_cis.shtml

problems and a number of other small issues as well. Most of the technical issues were of types that would have been solved during a pre-exercise before the real event.

A data collection manager in the green team was point of contact with the observers in Blue, White and Red Teams. The observers in Blue and Red teams reported events based on a predefined scheme. This was helpful in order for Green and White Team to have a situation overview of what was happening in the game. The data collection manager in Green Team provided situation the observers in Blue Teams with situation updates based mainly on reports from observers in White and Red Team, concerning critical events that were expected to affect Blue Teams. In this way, the Blue Team observers had a better chance to understand what was going on in the team they observed. Green Team also monitored the web camera and sound recordings in the teams.

Blue Team requests to make changes in their technical system were to be approved by Green Team to make sure that these changes were in line with the rules and would not affect the exercise negatively. All Blue Team requests were approved.

5 General Lessons Identified and Recommendations

1) The exercise was interesting to all teams from the trained Blue Teams to the Red, White and Green Team. The attackers were quite successful – they managed to keep a continuous pressure on the Blue Teams, there were no longer periods without any events happening.

2) Complex CDX environment lead to a high number of lessons identified and therefore gave a lot of learning benefit both to the organizers and participants.

3) Organising technical CDX is work intensive and requires considerable amount of resources. There are lot of aspects considering overall management that have to be improved:

    - communication and information sharing
    - project planning and meeting the deadlines
    - assigning devoted team leaders in the beginning of the preparation period
    - prioritizing – technical environment could have been simplified and more focus should have been on other issues such as staffing the White Team

4) Meetings – at least three real planning meetings bringing together all the relevant stakeholders would be required. Future exercises would also need more staffing than BCS 2010 had for organizing the event. This includes having a Management Team that stays somewhat intact from planning/preparation and during the execution, as well as and more persons to the Green, Red and White Team. The Red Team mainly consisted of voluntary supporters which helped to keep the budget of the CDX low. One has to take into account that this kind of voluntary support may not be always available. Outsourcing similar service from professional penetration testing team would be remarkably expensive.

    Also, the visualisation and situational awareness solutions were mainly sponsored by Clarified Networks.

5) International large-scale cyber exercises have usually high interest by the media. There should be specific person in the White, Red and Green team other than the team leader who is responsible for describing the progress of the exercise to the media and visitors. A special time should be scheduled for the visits and key messages agreed between all the parties.

6) Training objectives should be more concrete identifying clearly the training audience and what aspects the exercise should focus on.

7) There should be one pre-exercise day dedicated for testing the environment under the same conditions as it is during the execution. Pre-exercise should directly precede the main exercise day because all the teams and observers have to be present. Pre-CDX day should be devoted to:

    - test all communication channels and also all backup communication channels.
    - test VPN connectivity to the exercise environment by all team members together.
    - test all VMs and access to them.

- test if automatic scoring is working and if the Blue Teams understand how it is working.
- test the recording solutions and if all systems have the synchronized the time simultaneously to UTC (GMT/Zulu) before the exercise starts.
- helping the Blue Teams to install their own VMs if they have not managed to do it yet.
- introduce the rules and objectives.

8) There were proposals to have a 48 hour exercise. Although we consider this an interesting idea it would be problematic to find sufficient number of persons, especially for the Red Team, to keep events happening during the whole CDX.

   A two-day CDX conducted during working hours with one additional day for testing is a good solution. Still, Blue Teams could be given more time on analysis and preparation for the next phases. This could be scheduled between the main exercise phases and potentially during the night if agreed by the Blue Teams.

9) The Rules were too complicated and have to be redesigned and simplified:
   - Even the Green and White Team members were not sure about all the rules and lot of them were not strictly followed.
   - Change Management is one example for which the Configuration Control Board did not have a sufficient number of persons and competence. Often the Blue Teams had to ask several times if they are allowed to carry out requested actions

10) The rule allowing each team to bring in own tools was good and this approach should be continued.

11) There was a lot of documentation about the technical environment, communication, rules, data collection, etc. The teams should be provided a summary with the most important information.

12) With some exceptions, the Blue Team members were not particularly active before the CDX. This is another argument supporting the idea of having a special day for testing.

13) There should be clear rule indicating when the VPN access will be closed after the first exercise day. The Blue Teams would require some time to finish ongoing activities such as installing updates or new software. Still, it should be their own responsibility to finish ongoing activities before the fixed closing time.

14) It was difficult to enforce the teams to fill in the surveys in the end of the exercise days. More attention is needed to figure out how to motivate the teams to give a better feedback.

15) Common media package has to be prepared and shared with interested parties.

6 Conclusions

In general, the objectives were met and the exercise was a great success. Still, a lot of lessons were identified.

1) There were too many objectives and they were not clearly measurable. The objectives should be defined better.
2) The ambition and available resources were not in accordance. More dedicated staff would be required for conducting international technical CDX.
3) Real complexity of conducing BCS was not foreseen (technical environment, management team involvement, international participation).
4) Project management, information sharing and keeping to deadlines has to be improved.
5) Better solutions for real-time situational awareness have to be developed.
6) Physical meetings are necessary and the execution also benefits from close proximity. At least three planning conferences in addition to virtual meetings would be required.
7) A pre-exercise is required to test systems and connectivity, explain the objectives and rules.
8) Clearer and fewer rules are needed.
9) The core technical platform has to be upgraded or replaced.

7 Acknowledgements

The CCD COE and the SNDC would like to thank FOI, ECDL, MSB, FRA, NCIRC, Clarified Networks, the voluntary participants of the Red Team for their significant contribution and all the Blue Team members for making BCS 2010 a great experience.

8 ACRONYMS

BCS Baltic Cyber Shield
CCB Configuration Control Board
CCDCOE Cooperative Cyber Defence Centre of Excellence
CDX Cyber Defence Exercise
CERT Computer Emergency Response Team
CII Critical Information Infrastructure
ECDL Estonian Cyber Defence League
FOI Swedish Defence Research Agency
FRA Swedish National Defence Radio Establishment
IDS Intrusion Detection System
LFI Local File Inclusion
MSB Swedish Civil Contingencies Agency
NCSA NCIRC TC NATO Communication and Information Systems Services Agency / NATO Computer Incident Response Capability – Technical Centre
OOB Out-of-band
RFI Remote File Inclusion
SCADA Supervisory Control and Data Acquisition
SNDC Swedish National Defence College
VM Virtual Machine