Implementation of Security Controls for a Bank

Group-A Creditbanken

Petri Halla-aho
Tuomas Sillanaukee
Antti-Jussi Miettinen
Saad Malik
Arttu Reijonen
Eerik Snellman
Juan Laasonen
Miika Tuisku
Ville Karuaho

Master's Project: Cyber Security Implementation in Practice
April 2023
Master's Degree Programme in Cyber Security

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Figures

Tables

1 Introduction

1.1 Course management

Tasks were divided among team members in weekly status meetings. In the same meetings the progress of tasks was monitored, and the next set of assignments were decided.

1.2 Group roles & responsibilities

The course work was shared between team members. Team member responsibilities, roles and affected hosts are outlined in Table 1 (p. 1414). Each team member had a host to apply patches and mitigations for certain vulnerabilities or misconfigurations. Such tasks are compared to a task list found from *Appendix 1: Service Catalog creditbanken.vle.fi*. Each task is represented via *Risk id* number which can be compared to the task list. In addition to the patches, certain team members also had a task to write about different subjects around future work, implementation of additional security controls and other parts of the document like the chapter you are currently reading on. Those tasks are mentioned in *Future work*, *Implementation of additional Security Controls* and *Additional work* of the table. *Implementation of additional Security Controls* and *Future work* are evidenced in 5 and 7 respectively in the document.

To help the reader, mapping of given tasks to the *actual* work done should be straight forward. For example, the following Table 1 contains a subject called *AppLocker* (*Implementation of additional Security Controls* column) which can be found from chapter 5.1 AppLocker. In addition, Risk ids in the *Patching and mitigations (Risk id)* columns along with *Future work*, *Implementation of additional Security Controls* and *Additional work* columns follows the following color scheme and explanations: green (task is done and documented) and red (task is incomplete and not fully documented). Also keep in mind that it is the duty of the person responsible for the given task to complete the color scheme and is by default marked as incomplete (red).

Responsible	Hosts	Roles	Patching and mitigations (Risk id)	Future Work	Implementation of additional Security Controls	Additional work
Tuomas Sillanaukee	DC Files	Project Manager	14, 15, 24, 27, 64, 95	Update old Windows and Linux servers. Microsoft Defender for Endpoint & cloud SELinux & AppArmor	-	Project management Vulnerability testing (automation + manual) Technical security testing (chapter 3) Introduction (Group Roles & responsibilities refactoring, Company network diagram) Refactor report structure. Create template for Service updates and patches (extranet server)

Antti-Jussi Miettinen	Elasticsearch 1 Elasticsearch 2 Elasticsearch 3 FireEye Staff-remote-ws	Architect	12, 25, 26, 33, 34, 35, 36, 49, 80, 84			Run system updates. Run local privilege escalation checks with Linpeas and Winpeas Report and figure out data flows of the environment. (Done in chapters 4.2 and 4.5) Technical Security hardening (Project management) Verification and Analysis of Threat Exposure after Security Controls Implementation Service updates and patches (Intro for patches and fixes) Greenbone Scanner

						patches and fixes by server (intro)
Saad Malik	Firewall-ext Firewall-int Firewall-ISP-net SIEM SQL	Firewall Specialist	25, 29, 32, 54, 57, 58, 59, 60, 79, 82, 83, 85, 87	-	-	Run system updates. Firewall (Palo Alto) configurations (chapter 4) Host-based Firewalling Run local privilege escalation checks with Linpeas and Winpeas Description of Bank's Assets, Threats, and Risks Patching/Mitigating Assigned Vulns 5.6 CIS Benchmarks

						Report Structure & Finalization
Arttu Reijonen	PRTG NTP Ns1 Ns2 FireEye HR AD Staff-WS1 & 2	Project team member	42, 65, 66, 67, 72	-	-	Run system updates. Run local privilege escalation checks with Linpeas and Winpeas Service updates and patches (FireEye, install FireEye agent on workstations) Testing FireEye malware scans Patching/Mitigating Assigned Vulnerabilities
Eerik Snellman	DC Files Intra SQL	Project team member	16, 18, 19, 20, 39, 40, 61, 77, 78, 79, 81	-	AppLocker – AppLocker is enabled in Monitor and DC machine by using AaronLocker PowerShell scripts.	Run system updates – All Windows machines (PRTG, DC, Files, Dev-WS1, Legacy application and Staff-remote-ws) have been updated either by windows

	PRTG					update or WSUS offline tool. Run local privilege escalation checks with Linpeas and Winpeas. Refactor report structure. Spell checking, sentence structure checking, adding captions and cross-references. PRTG Service update.
Juan Laasonen	SimpleCA Proxy Dev-WS-1 Dev-WS2 HR	Project team member	43, 44, 45, 46, 86, 87, 88, 89, 90, 91, 92	SSH key authentication Tier level authentication model	Microsoft System Center Configuration Manager (SCCM) and Windows Server Update Services (WSUS)	Run system updates. Run local privilege escalation checks with Linpeas and Winpeas Vulnerability testing (automation) Introduction (Course management, Group

	Gitlab Legacy application Staff-WS1 & 2					roles & responsibilities (initial work)) Technical security hardening (System updates)
Miika Tuisku	Gitlab HR Legacy application Staff-ws	Project team member	28, 29, 30, 31, 32, 37, 60, 62, 73, 74, 82, 85	-	Center for Internet Security (CIS) Benchmark (level 1)	Run system updates. Run local privilege escalation checks with Linpeas and Winpeas Figure out what the Legacy application is for
Ville Karuaho	Extranet www Mail Helpdesk	Project team member	38, 47, 56, 63, 68, 69, 70, 71, 75, 76, 93, 94	Logging	Local Administrator Password Solution (LAPS) Sysmon	Run system updates. Run local privilege escalation checks with Linpeas and Winpeas Service updates and patches (Elastic 1-3

						(Configure beats for Elastic Search)

Table 1. Groups roles and responsibilities

1.3 Company network diagram

The Figure 1 outlines the company network structure:

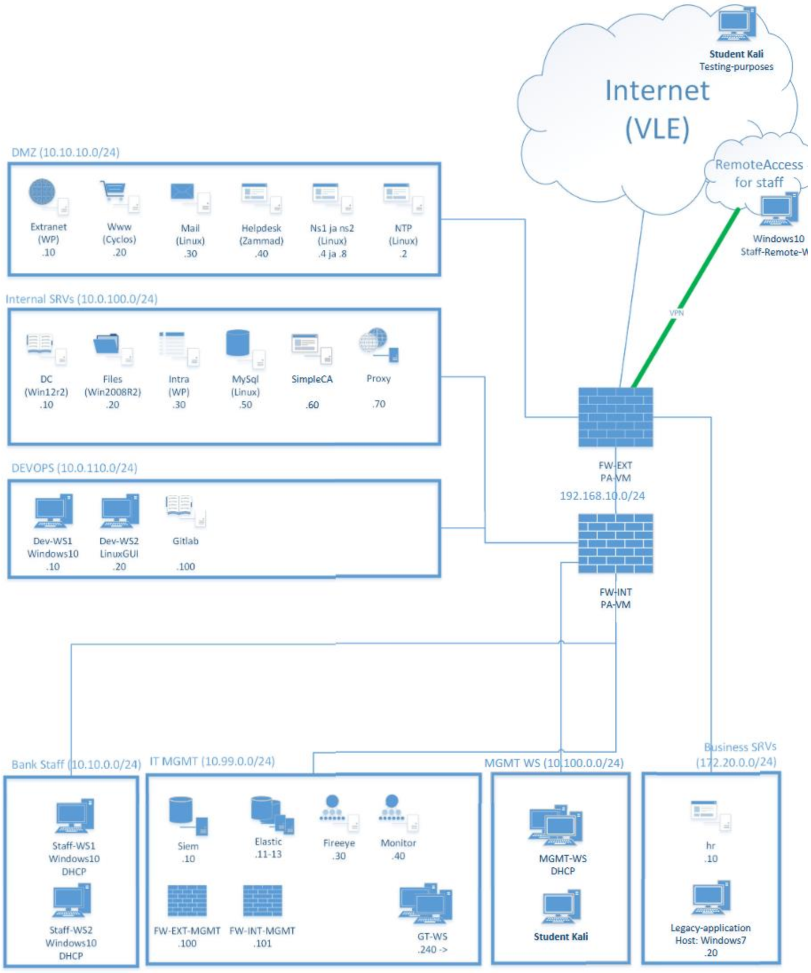


Figure 1. Network diagram

2 Description of Bank’s Assets, Threats, and Risks

In this chapter, we discuss the various assets that the Creditbanken bank possesses and how the network has been segmented. Moreover, we identify the various threats to these assets and the vulnerabilities which cause the threats. Finally, we assess the impact of vulnerability to the critical asset and calculate the risk. In the following chapter, we identify ways to reduce the risk to an acceptable level via implementation of various security controls.

The threats to any organization’s infrastructure include both outside and internal threats. The insider threats can be a company’s own disgruntled or poorly trained employees while the outside threats could include cyber criminals, competitors, or hacktivists. The threats faced could be spear phishing infection with malware. In this case the victims are sent an exploit document with enticing content and after the victim opens the file, the malware is installed into the victim’s computer. The other tactic could be webmail access via spearphish in which case a domain is registered spoofing a webmail service and email is sent to target to reset their passwords. When the recipient visits the fake login page and enters the credentials, they are stolen. Another tactic is the infection with malware via strategic web compromise and finally is the access through internet facing servers. In this case, Network Reconnaissance is performed to find vulnerable software and initial compromise is leveraged to access other systems and move deeper into the victim network. These are just some tactics that are employed by the attackers to gain access to your system by utilizing the known vulnerabilities.

2.1 Assets

The bank's assets include physical and hardware assets and the software assets. The network diagram in the previous section (chapter 1.3) shows the various assets that the IT Infrastructure of the bank possesses. These assets include information assets in the form of databases, software assets in the form of web applications and various security solutions, hardware assets in the form of Firewalls, services, and intangibles such as the bank’s reputation and intellectual property. The network has been segmented into various zones with each zone further comprising workstations, firewalls, and other security solutions.

DMZ

This zone consists of an Extranet, Cyclos, Mail server, Helpdesk, NS1 and NS2 and NTP server. The Extranet is a private, secure network aimed at sharing business information with partners, suppliers, and customers etc. It is implementation in DMZ (DeMilitarized Zone) gives streamlined business process management, high data security and increased customer satisfaction. Cyclos is banking software normally utilized by banks as a payment platform for mobile banking and enabling branchless banking. The Mail server in the said DMZ is CentOS Linux based. Zammad helpdesk software is a free helpdesk system which connects all your communication channels, email, chat, telephone and easily grant user rights and reporting. NS1 and NS2 and public master and slave Linux based DNS servers while NTP is the Network Time Protocol server that enables synchronization of system clocks from desktops to servers.

Internal SRVs

Internal services include DC, which is the Active Directory and DNS resolver, file service for employees, intranet for employees, MySQL database, Certificate Authority, and proxy server.

DevOps

The DevOps segment comprises of two Windows and Linux based Dev workstations and Linux based Git version control.

Bank Staff

The bank staff subnet contains two windows 10 based workstations which have been reserved for staff windows usage.

IT MGMT

The IT Management segment consists of a SIEM which is Security Incident and Event Management. SIEM allows us to perform real time monitoring of security events along with their analysis when doing the root cause analysis. It also allows us to collect logs and perform security data tracking. It automates many of the event detection and incident response processes. The SIEM implemented here is an Elastic search SIEM.

The IT Management section also contains three Elastic Search nodes. Elastic search is a distributed, NoSQL JSON database. The interaction with ELK is done via REST APIs and is known for its speed of search and scalability. Another important device in the IT Management section is the FireEye. FireEye Endpoint Security is an Endpoint protection platform which combines conventional anti-virus software with advanced real-time monitoring and detection. The PRTG is a network traffic monitoring solution also deployed in IT Management. Lastly, there are two External and Internal Firewalls at the Network edge for traffic filtering.

MGMT WS

The Management Workstations comprise of Student Kali workstation and DHCP workstation.

Business SRVs

Finally, the Business Services workstation comprises of HR workstations and Legacy application windows workstation.

2.2 Threats Confronting the Company

The Bank in question is a highly sought-after cyber target and thus demands strict policies to be put in place to preserve the user's information, bank's software assets, intellectual property, technical documentation along with the IT infrastructure that it possesses. In the present situation, with the rapid digitalization and cloud migration of all companies and banks assets, particularly in the post-COVID world, financial institutions such as banks are more prone to cyber-attacks and the threats and risks being faced by the bank are on the rise. Therefore, these risks and threats must be considered because in the banking sectors, significant sums of money are involved and in the event of compromise, the disruption to the financial institution and the economy itself can be considerable.

For the hardware-based assets, the threats can be building fire, theft, elevated temperature etc. while for the software-based assets including the databases and web applications, these threats include Ransomwares, security concerns with the remote work, Cloud based cyber-attacks, social engineering, and supply chain attacks, among others. A description of threats is detailed Table 2 found below.

Asset Type	**Asset**	**Threat**
Information Assets	Customer Accounts Database, Employee Accounts Database, Elastic Search, MySQL Database	Cyber criminals: Ransomware, Social Engineering, Phishing, Password Attack
Hardware Assets	Servers: NTP server, DNS Servers, Mail server, Proxy Server	DC Power Outage, Equipment theft, Data Center Fire
Hardware Assets	PA Firewalls and ISP Firewall	Hardware Device Failure I.e., SFP, Cable Cut, Electricity Outage

Human Resource	CISO, Bank’s Security Operations Team	Social Engineering, Spear-phishing, Disgruntled Employee Insider Attack
Software Assets	SIEM, Extranet, FireEye, Firewalls and device Configurations, Intra	Supply Chain attacks, Advanced Persistent Threats, Data Manipulation, Outdated Firewall Software
Software Assets	NTP, Mail server, PRTG, Proxy Server SQL, Cyclos, Gitlab, Management, HR and DevOps Workstations, Zammad Helpdesk, Certificate Authority	Malwares; Trojans, Worms, Viruses, Spyware, Spam
Software Assets	Bank’s Website, Mobile Application, Active Directory	Spoofing, Cross site scripting, SQL Injection, DDoS, Hijacking
Intangible Assets	Bank’s Reputation, Intellectual Property Trademark	Copy right breach by the Competitor

Table 2. Asset types, assets and threats

2.3 Vulnerabilities

Vulnerabilities are the weaknesses in the IT infrastructure that can be exploited by an attacker to conduct a successful cyber-attack. The vulnerabilities can be network vulnerabilities, operating system vulnerabilities, human and process vulnerabilities. To identify vulnerabilities in the network, we use various tools such as NMAP, Linpeas, Winpeas, Nessus and Green (see Table 4). We run scans on various network devices and these scans output the vulnerabilities in the network devices. The Table 3 illustrates the various vulnerabilities identified in the network based on the scans as well as the impact assessment of the threats posed by these vulnerabilities.

Sr. #	Asset (Device Name)	Vulnerability	CVE number	Short Description
1	Extranet, WWW, Mail	Polkit Out-of-Bounds Read and Write Vulnerability	CVE-2021-4034	Local privilege escalation in pkexec due to incorrect handling of argument vector
2	Helpdesk, Mail	Linux Kernel Race Condition Vulnerability	CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping
3	Extranet	Linux Kernel Privilege Escalation Vulnerability	CVE-2022-2588	A use-after-free flaw was found in route4_change in the net/sched/cls_route.c filter implementation in the Linux kernel. This flaw allows a local user to crash the sys-

				tem and possibly lead to a local privilege escalation problem.
4	NTP, NS1, NS2	Linux Kernel Race Condition Vulnerability	CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping
5	NTP, NS1, NS2	Polkit Out-of-Bounds Read and Write Vulnerability	CVE-2021-4034	Local privilege escalation in pkexec due to incorrect handling of argument vector
6	Mail, WWW	SSL Medium Strength Cipher Suites Supported (SWEET32)		The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

7	Mail	20007 - SSL Version 2 and 3 Protocol Detection		The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes.
8	Elasticsearch 1 & 2 & 3	dirtycow	CVE-2016-5195	A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings
9	Elasticsearch 1 & 2 & 3	dirtycow2	CVE-2016-5195	A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings

10	Elasticsearch 3		CVE-2021-4034	A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according to predefined policies. The current version of pkexec does not handle the calling parameters count correctly and ends up trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it will induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.
11	HR	dirtycow, dirtycow2, etc.	More than dozen	Ran yum update, linPEAS.sh
12	GitLab			yum / dnf upgrade not working (RHEL8)
13	legacy-app			

14	DC	SWEET32	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.
15	DC	Bar Mitzvah	CVE-2013-2566, CVE-2015-2808	The remote service supports the use of the RC4 cipher.
16	Files	BlueKeep	CVE-2019-0708	The remote host is affected by a remote code execution vulnerability.
17	Files	20007 - SSL Version 2 and 3 Protocol Detection		The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes.
18	Files	108797 - Unsupported Windows OS (remote)		The remote OS or service pack is no longer supported.
19	Files	58435 - MS12-020	CVE-2012-0002, CVE-2012-0152	The remote Windows host could allow arbitrary code execution.

20	Files	ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, ETERNALSYNERGY, WannaCry, EternalRocks, Petya, uncredentialed check	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148	The remote Windows host is affected by multiple vulnerabilities.
21	Files	35291	CVE-2004-2761	An SSL certificate in the certificate chain has been signed using a weak hash algorithm.
22	Files	SWEET32	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.
23	Files	18405	CVE-2005-1794	It may be possible to get access to the remote host.
24	Files	57608 - SMB Signing not required		Signing is not required on the remote SMB server.
25	SQL	PMASA-2019-1, PMASA-2019-2	CVE-2019-6798, CVE-2019-6799	The remote web server hosts a PHP application that is affected by multiple vulnerabilities.
26	SQL	PMASA-2019-3	CVE-2019-11768	The remote web server hosts a PHP application that is affected by SQLi vulnerability.

27	SimpleCA	20007 - SSL Version 2 and 3 Protocol Detection		The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes.
28	SimpleCA	2424 - CGI Generic SQL Injection (blind)		A CGI application hosted on the remote web server is potentially prone to SQL injection attack. An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.
29	SimpleCA	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.
30	Dev-WS1	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.

Table 3. Vulnerabilities

2.4 Risk Management

In risk management, Asset, Threat and Vulnerability management are brought together. In this exercise, all assets, threats and vulnerabilities are bound to cyber security area and issues with physical security (access control to facilities, natural disasters, et cetera and safety (employee safety like black mailing)) are out of scope.

The aim is to attach suitable threats to each asset. Each asset may have several threats and the same threat can occur in several different assets (Table 2. Asset types, assets and threats). Threats are associated with all appropriate vulnerabilities (Table 3. Vulnerabilities) in the same style as assets and threats. All matching vulnerabilities are added to each asset-threat combination, thus forming a matrix showing all combinations of asset, threat and vulnerability (combination of “Table 2. Asset types, assets and threats” and “Table 3. Vulnerabilities” is embedded to full list of vulnerabilities (Appendix 1). Measure of risk now reflects the overall effect of the risk on the company.

Risks are assessed based on the following rules. Machines are valued with the impact level from 1 to 4 (1 = low, 4 = critical) based on how critical the machine is for the company’s network and operations. The impact level (this can be seen in each machines chapter), and risk criticality give us the threat level. Threat level tells us how crucial it is to mitigate or fix the issue in the environment.

3 Technical security testing

This section describes methods the internal security team used to find flaws in the company's technical security posture. The purpose of technical security testing was to figure out the company's current technical issues, vulnerabilities, and misconfigurations across different hosts. Such findings were then managed accordingly, namely patched, mitigated, classified as a future work, or marked as an accepted risk. Also, such findings and the person responsible for acting accordingly were documented to an Excel sheet (see *Appendix 1: Service Catalog creditbanken.vle.fi*.) on the columns *Vulnerability* and *Responsible person,* respectively.

The network diagram which outlines hosts in the company network can be evidenced from Figure 1 (page 15).

3.1 Summary

Serious and numerous flaws were identified in the company's technical security posture. Such flaws required immediate attention to be fixed and are outlined in the document's sections 2 and 4. Such flaws included but were not limited to remote code execution on numerous hosts due to such hosts missing critical system and service updates. For example, Files server was vulnerable to Eternal Blue (CVE-2017-0143) and Gitlab server to CVE-2021-22205 which both allowed executing code in the machine from an unauthenticated standpoint. In addition to flaws that were due to missing security patches, there were also several ones found that were derived from poor application misconfigurations. Namely, HR server was exposing its database credentials in publicly and easily available file in its web server. In addition, there were guessable credentials in the *creditbanken.vle.fi* domain in the Windows Active Directory for a user *at* that belongs to domain admins group, a group that controls the whole domain.

In addition to more severe security flaws, several minor misconfigurations were identified. For example, the company's authoritative DNS server (ns2) was allowing unauthorized DNS Zone Transfers (see Nidecki 2019) to public parties. In addition, several hosts were exposing its service names and corresponding version numbers.

3.2 Approach

The approach to find security flaws on the company hosts was to combine both automation and manual testing. The security team was provided with information about hosts in the company network (see Figure 1 (p. 15)). Such information included things like what services are running on what hosts. However, some key information such as which ports were open on which hosts was yet to be discovered. Therefore, the team decided to port scan every IP subnet to generate a list of open ports associated with the hosts in the network. After this, the hosts and their corresponding ports were scanned with a vulnerability scanner and then, found vulnerabilities were technically validated.

In addition to using purely automation, manual security testing was also applied depending on the host and corresponding services offered. For example, Windows Active Directory environment was reviewed for common misconfigurations like users with excessive privileges or bad practice security hardenings through querying LDAP. In addition, for example hosts that were offering a web service were manually scanned for publicly available files through a technique called directory brute forcing. Indeed, many bad practice configurations and vulnerabilities were discovered manually.

To summarize the approach outlined above:

Automation

1. Scan and map every subnet for hosts to discover which ports are open on the host.
2. Run a vulnerability scanner against the before generated list.
3. Verify findings.

Manual testing

1. Scan and map every subnet for hosts to discover which ports are open on the host.
2. Apply manual security testing approach for given services.

3.3 Tooling

To achieve the forementioned results, certain security testing tooling was used. The Table 4 specifies used tooling, more specifically tool's name, purpose, and source:

Name	Purpose	Source
Rustscan	Portscanner	GitHub (see Rustscan the modern port scanner 2022)
Nessus Essentials	Vulnerability Scanner	Tenable web site (see Tenable for Education n.d.)
Impacket's tool suite	Includes several tools to test Windows Active Directory	GitHub (see Impacket 2022)
ffuf	Directory Bruteforcing	GitHub (see ffuf - Fuzz Faster U Fool 2023)
PywerView	Query LDAP protocol for Windows Active Directory misconfigurations	GitHub (see PywerView 2023)
Metasploit Framework	Validate vulnerabilities	Metasploit web site (see Get Metasploit n.d.)
LinPEAS	Linux Privilege Escalation enumeration	GitHub (see LinPEAS - Linux Privilege Escalation Awesome Script 2023)

WinPEAS	Windows Privilege Escalation enumeration	GitHub (see Windows Privilege Escalation Awesome Scripts 2023)
CrackMapExec	Query LDAP and SMB protocols for Windows Active Directory misconfigurations	GitHub (see CrackMapExec 2022)
hashcat	Password hash brute-force tool	Hashcat web site (see hashcat advanced password recovery 2022)
GreenBone Security Assistant	The Greenbone Security Assistant (GSA) is the web interface that a user controls scans and accesses vulnerability information with. It is the main contact point for a user.	GreenBone (see *Greenbone,* 2021)

Table 4. Tooling

3.4 Findings

This section specifies the most notable security findings. The Table 5 outlines the name of the vulnerability (or misconfiguration) and corresponding host, severity, description, and the tool that was used to find the vulnerability. Please note that all the findings can be evidenced from Appendix 1: Service Catalog creditbanken.vle.fi.

Vulnerability & misconfiguration name	**Host**	**Severity**	**Description**	**Tool**
Multiple RCE's (e.g., CVE-2021-22205)	GitLab	Critical	A source control application running on the remote web server is affected by an RCE vulnerability.	Nessus
Eternalblue, Eternalchampion, Eternalromance, Bluekeep	Files	Critical	The remote host is affected by a remote code execution vulnerability.	Nessus
PMASA-2019-1, PMASA-2019-2	SQL	Critical	The remote web server hosts a PHP application that is affected by multiple vulnerabilities. (Arbitrary File Read Vulnerability)	Nessus
PMASA-2019-3	SQL	Critical	The remote web server hosts a PHP application that is affected by SQLi vulnerability.	Nessus

Database creds exposed	HR	Critical	DB creds found at: https://hr.credit-banken.vle.fi/lib/confs/Conf.php-distribution	ffuf
One can issue and revoke certificates without authentication	SimpleCA	High	N/A	Web browser
Dirtycow & Dirtycow 2	Elasticsearch 1 & 2 & 3, HR, SimpleCA	High	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."	LinPEAS
SNMP Agent Default Community Name (public)	Firewall-int	High	The name of the community in remote SNMP server can be guessed. An attacker may use this information to gain more knowledge about the remote host, or to change the	Nessus

			configuration of the remote system (if the default community allows such modifications).	
Default password policy	AD	High	N/A	CrackMapExec
Same password for local admin account (User).	Staff-ws1 & 2	High	Since the workstations are probably derived from the same golden image, they have the same local admin user account (User: RID 1000) and password. If any of the machines is compromised, it is possible to perform lateral movement between the machines with the NTLM hash of the user, without having to crack the password.	Impacket
Redundant domain admin credentials with a weak guessable password	AD	High	User account gt which belongs to domain admins group and has a guessable password Yamk-gt.	hashcat
DNS Server Zone Transfer Information Disclosure (AXFR)	Ns2	Medium	The remote name server allows zone transfers. A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that	Nessus

			can give hints as to a server's primary application (for instance, proxy.example.com, payroll.example.com, b2b.example.com, etc.).	
MachineAccountQuota attribute is 10 (default)	AD	Medium	Users can create up to 10 machine account objects to the domain.	CrackMapExec
Login panel not restricted	SQL, Extranet, Intra, SIEM	Low	Login panel is exposed everywhere in the company estate.	Web browser

Table 5. Summary of security findings

4 Technical security hardening

This section describes what methods the company used to patch and remediate found technical security flaws to ensure feasible security posture.

4.1 Project management

An Excel workbook has been used as the project management tool for the updating and patching phase, which serves as a basis for defining the criticality of the work, dividing responsibility and controlling the workflow.

Basic server information such as IP address, name, IDs and passwords, etc. has been recorded in Excel on the computer tab (see *Appendix 2: Network Catalog creditbanken.vle.fi*). In addition to the basic information, the computer tab has an assessment of the criticality of the machine to the company's operation in the "impact level" column. At the beginning of the work, we ran operating system updates to machines where it was possible, that is, the machine's operating system is not in EoF status, the status of the update is marked in the Updated column.

During the web scan, we collected a list of vulnerabilities in project management Excel on the Vulnerability tab. Vulnerabilities were collected e.g., Nessus reports, linPEAS and winPEAS checks and other tools mentioned earlier in the Tool section. We also calculated the severity of the vulnerability in the criticality column. For each vulnerability found, a responsible person was named whose task it was to patch or mitigate that vulnerability.

In the last step, a person was assigned responsibility for the machines, whose task was to examine the installation of the machine in more detail and to correct possible installation errors and vulnerabilities. The person responsible is named in the Assigned to column. The duties of the person responsible also included recording the descriptions of the chapter Service updates and patches.

The urgency of the patch is determined by the criticality of the machine and the severity of the vulnerability. The most critical servers with high vulnerabilities are patched or mitigated first.

Patching urgency is determined based on the severity of the machine and the vulnerability. The most critical servers with major vulnerabilities are patched or controlled first.

4.2 General Workflow

At the beginning we ran through scans on every machine, by using winpeas/linpeas script inside the machine and Nessus from the network against each machine. After the preliminary scanning, we updated all the systems we could.

Some of the Linux systems are updated nicely to the latest possible build for that release path like CentOS7, as it is still on support. Then there are other Linux machines with CentOS 6 or 8. support for those operating systems ended some time ago. These systems we were able to update only partially. Some components installed on these machines are no longer updated to support these discontinued operating systems.

After updating all the systems as far as possible we ran those scans again and got the listing of the weaknesses that cannot be mitigated easily just by updating operating systems.

Some of these old operating systems can still be updated by installing packages manually. But then there are those old Windows operating systems. All of them cannot be updated at all, as the operating system is not activated and even the activated system would need long term support agreement with Microsoft to get any kind of updates for these. This problem concerns Windows 7 and Windows Server 2008R2 systems, but also Windows Server 2012R2 is old enough to be difficult to update without support agreements with Microsoft. Windows machines also suffer from poorly configured Group Policies that prevent all connection to Microsoft’s Update services to get updates there. And there has not been any installation of local repository or cache to offer Windows updates to machines connected to the company’s network.

Updated Servers and status

All the CentOS 7 machines were updated to the latest version. CentOS 8 is already in the End-of-Life state, so there we faced some difficulties to update operating system. Some of the OS components are not What servers were updated and what are not and why...

4.3 Service updates and patches

Many of the services/applications were installed to the machines as a separate package and could not be a general update process.

All Linux servers have been tried to patch the common security holes found by the Greenbone scanner (*Greenbone,* 2021). Repairs have been made to the servers, which includes repairs, among other things:

- removing old kernels
- SSL/TLS secure configuration
- Verifying SSH and ensuring sufficient encryption strength.
- removed TLSv1.0 and TLSv1.1

Using a configuration management tool like Ansible (see Ansible, 2023), Puppet (See Puppet, 2023) or Chef (see Chef, 2023) could have made sense to centralize Linux patching. These tools provide a centralized and automated approach to managing configurations and updates across multiple Linux servers. By utilizing these tools, we would have been able to install patches and updates more easily to all Linux servers in a controlled and coordinated manner, while ensuring that all servers are constantly patched and up to date. In addition, these tools provide auditing and reporting capabilities that facilitate tracking and monitoring of the repair status of the server base and quickly fix any anomalies or vulnerabilities.

4.4 Patches and fixes by server

Because automatic scanners such as Nessus and Greenbone (*Greenbone,* 2021) are not able to effectively find mistakes made during installation, such as bad and repeated passwords and forgotten files. We also try to examine the files and configurations related to the services of the servers and report and fix them. The problems found were reported and mitigated as much as possible.

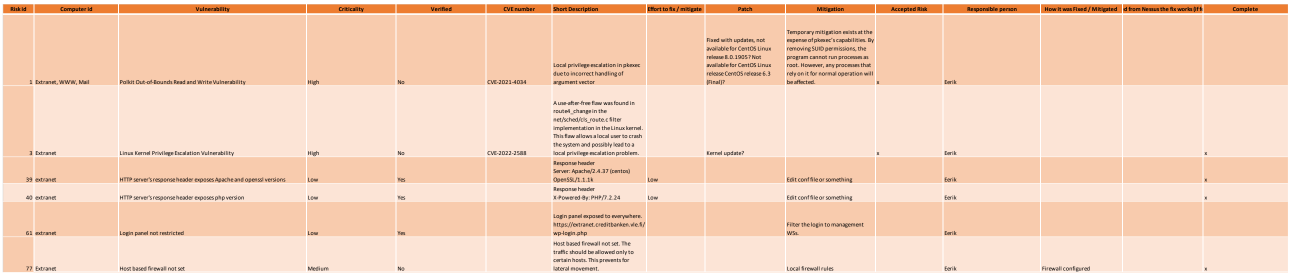
4.4.1 Extranet Server

Impact: Estimated impact medium 2: Possible Loss of same sensitive customer data.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
OS Linux release 8.5.2111	Apache 2.4.37 PHP 7.2.24 MariaDB 10.3.28-1 WordPress 5.3	Server provides “consulting services” to customers for external use.	**Inbound** 0.0.0.0/0 (HTTP (80), HTTPS (443)) Management VLANs (SSH (22)) MySQL-server (10.0.100.50/32 (TCP, 3306))	WordPress Management connections MariaDB
			Outbound (allowed to) Elastic nodes (TCP, 9200) FireEye EDR (TCP, 80)	Auditbeat agent, Filebeat agent FireEye agent

Patching & mitigations

The following Figure 2 specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigated	d from Nessus the fix works (if f	Complete
1	Extranet, WWW, Mail	Polkit Out-of-Bounds Read and Write Vulnerability	High	No	CVE-2021-4034	Local privilege escalation in pkexec due to incorrect handling of argument vector		Fixed with updates, not available for CentOS Linux release 8.0.1905? Not available for CentOS Linux release CentOS release 6.3 (Final)?	Temporary mitigation exists at the expense of pkexec's capabilities. By removing SUID permissions, the program cannot run processes as root. However, any processes that rely on it for normal operation will be affected.	x	Eerik			
3	Extranet	Linux Kernel Privilege Escalation Vulnerability	High	No	CVE-2022-2588	A use-after-free flaw was found in route4_change in the net/sched/cls_route.c filter implementation in the Linux kernel. This flaw allows a local user to crash the system and possibly lead to a local privilege escalation problem.		Kernel update?		x	Eerik			x
39	extranet	HTTP server's response header exposes Apache and openssl versions	Low	Yes		Response header Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k	Low		Edit conf file or something		Eerik			x
40	extranet	HTTP server's response header exposes php version	Low	Yes		Response header X-Powered-By: PHP/7.2.24	Low		Edit conf file or something		Eerik			x
61	extranet	Login panel not restricted	Low	Yes		Login panel exposed to everywhere. https://extranet.creditbanken.vle.fi/wp-login.php			Filter the login to management WSs.		Eerik			
77	Extranet	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Eerik	Firewall configured		x

Figure 2. Extranet patching and remediations

Notes regarding the server

Since CentOS 8 is End of Life, mirrors were changed to vault.centos.org where they will be archived permanently the server has been updated to the last possible version. The vulnerabilities mentioned in the project Excel have been fixed.

The server's firewall is enabled. In the firewall, traffic to the internet is allowed only for http and https services. Subnets IT MGMT and MGMT WS connected to trusted networks, so ssh, SIEM and FireEye services work. In the Palo Alto firewall, the traffic of the management networks is more precisely restricted per service and port. Access to the servers is blocked from other servers in the same subnet.

Since CentOS 8 is no longer supported, automatic update cannot be enabled.

Unnecessary packages have been cleaned from the server.

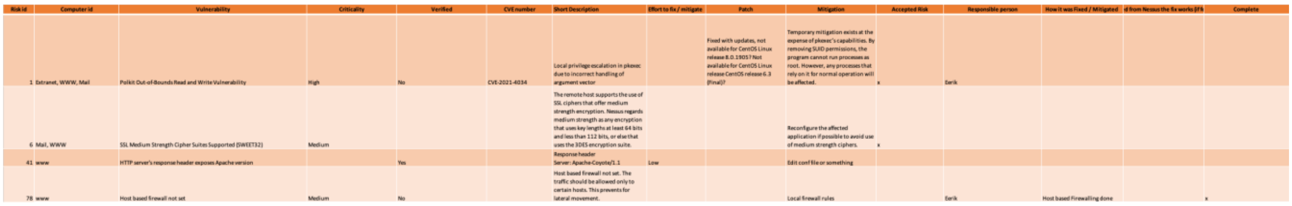
4.4.2 WWW Server

Impact: Estimated impact Critical 4: A critical service for the bank's operation, significantly affects the bank's ability to operate and contains highly confidential data. High risk of misuse.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
OS Linux release CentOS release 6.10 (Final)	Tomcat 6.0.24-115.el6_10 MySQL 5.1.73-8.el6_8 Cyclos 3.7.3 java version 1.6.0_41	Server provides Banks main network banking application	**Inbound** 0.0.0.0/0 (HTTP (80) HTTPS (443) Management VLANs (SSH (22)) MySQL-server (127.0.0.1 (TCP, 3306)) localhost (25) localhost (1733)	Tomcat running Cyclos banking software redirect to local 8443 redirect to local 8443 Management connections. MySQL Sendmail Cupsd printing srv
			Outbound (allowed to) Elastic nodes (TCP, 9200)	Auditbeat agent, Filebeat agent

Patching & mitigations

The following Figure 3. WWW Server patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigated	d from Nessus the fix works (if fi	Complete
1	Extranet, WWW, Mail	Polkit Out-of-Bounds Read and Write Vulnerability	High	No	CVE-2021-4034	Local privilege escalation in pkexec due to incorrect handling of argument vector		Fixed with updates, not available for CentOS Linux release 8.0.1905? Not available for CentOS Linux release CentOS release 6.3 (Final)?	Temporary mitigation exists at the expense of pkexec's capabilities. By removing SUID permissions, the program cannot run processes as root. However, any processes that rely on it for normal operation will be affected.	x	Eerik			
6	Mail, WWW	SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium			The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.			Reconfigure the affected application if possible to avoid use of medium strength ciphers.	x				
41	www	HTTP server's response header exposes Apache version		Yes		Response header Server: Apache-Coyote/1.1	Low		Edit conf file or something					
78	www	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Eerik	Host based Firewalling done		x

Figure 3. WWW Server patching and remediations

Notes regarding the server

As CentOS 6 is in End of life, it should be updated Immediately. All the most important services are out of date (Tomcat, Java, MySQL) also due to the aging of the operating system, i.e., the services are no longer updated according to the normal update process. The services must be updated manually from the packages. There is a considerable risk of the service breaking down, which may be too big a risk because there is no more detailed information about installing the service.

Weak password in MySQL is changed. Cyclos and Sendmail configured to use authentication. Cyclos password requirements are updated.

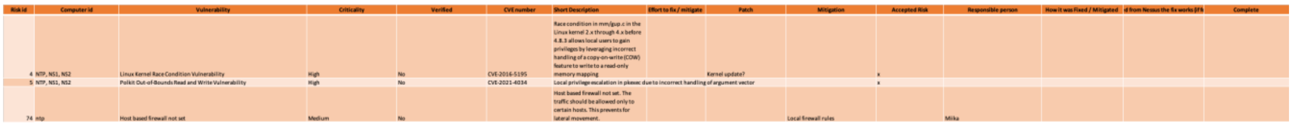
4.4.3 NTP Server

Impact: Estimated impact medium 2: Possible attack vector for several other servers.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
CentOS Linux release 7.9.2009 (Core)	chrony 3.4-1.el7	Server provides time synchronization to network	**Inbound** Management VLANs (SSH (22))	Management connections
			Outbound (allowed to) Elastic nodes (TCP, 9200)) Chronyd (UDP,123)	Auditbeat agent, Filebeat agent NTP service

Patching & mitigations

The following Figure 4. NTP server patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigated	d from Nessus the fix works (ff	Complete
4	NTP, NS1, NS2	Linux Kernel Race Condition Vulnerability	High	No	CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping		Kernel update?		x				
5	NTP, NS1, NS2	Polkit Out-of-Bounds Read and Write Vulnerability	High	No	CVE-2021-4034	Local privilege escalation in pkexec due to incorrect handling of argument vector				x				
74	ntp	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Miika			

Figure 4. NTP server patching and remediations

Notes regarding the server

The server's firewall is enabled. In the firewall, Subnets IT MGMT and MGMT WS connected to trusted networks, so ssh, SIEM and FireEye services work. In the Palo Alto firewall, the traffic of the management networks is more precisely restricted per service and port. Access to the servers is blocked from other servers in the same subnet, except ntp-protocol is allowed. Unnecessary packages have been cleaned from the server.

Vulnerabilities ID 4 and ID 5 were marked as accepted risks because these would require OS update to mitigate.

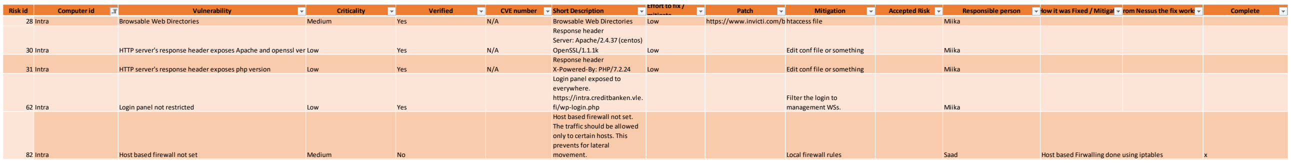
4.4.4 Intranet Server

Impact: Estimated impact High 3: Possible Loss of sensitive customer data and banks internal documentation.

OS versioning	Service numbering (after updates)	Service description	Firewalling (Source hosts, Protocol + Port)	More details about connections
OS Linux release 8.5.2111	Apache 2.4.37 PHP 7.2.24 MariaDB 10.3.28-1 WordPress 5.3	Server provides Intranet platform for staffs interna use	**Inbound** 0.0.0.0/0 (HTTP (80), HTTPS (443)) Management VLANs (SSH (22)) MySQL-server (10.0.100.50/32 (TCP, 3306))	WordPress Management connections MariaDB
			Outbound (allowed to) Elastic nodes (TCP, 9200)	Auditbeat agent, Filebeat agent

Patching & mitigations

The following Figure 5. Intranet patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigat	rom Nessus the fix works	Complete
28	Intra	Browsable Web Directories	Medium	Yes	N/A	Browsable Web Directories	Low	https://www.invicti.com/b	htaccess file		Miika			
30	Intra	HTTP server's response header exposes Apache and openssl ver	Low	Yes	N/A	Response header Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k	Low		Edit conf file or something		Miika			
31	Intra	HTTP server's response header exposes php version	Low	Yes	N/A	Response header X-Powered-By: PHP/7.2.24	Low		Edit conf file or something		Miika			
62	Intra	Login panel not restricted	Low	Yes		Login panel exposed to everywhere. https://intra.creditbanken.vle.fi/wp-login.php			Filter the login to management WSs.		Miika			
82	Intra	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Saad	Host based Firwalling done using iptables		x

Figure 5. Intranet patching and remediations

Notes regarding the server

Since CentOS 8 is End of Life, mirrors were changed to vault.centos.org where they will be archived permanently the server has been updated to the last possible version. The vulnerabilities mentioned in the project Excel have been fixed.

The server's firewall is enabled. In the firewall, traffic to the internet is allowed only for http and https services. Subnets IT MGMT and MGMT WS connected to trusted networks, so ssh, SIEM and FireEye services work. In the Palo Alto firewall, the traffic of the management networks is more precisely restricted per service and port. Access to the servers is blocked from other servers in the same subnet.

Since CentOS 8 is no longer supported, automatic update cannot be enabled.

Unnecessary packages have been cleaned from the server.

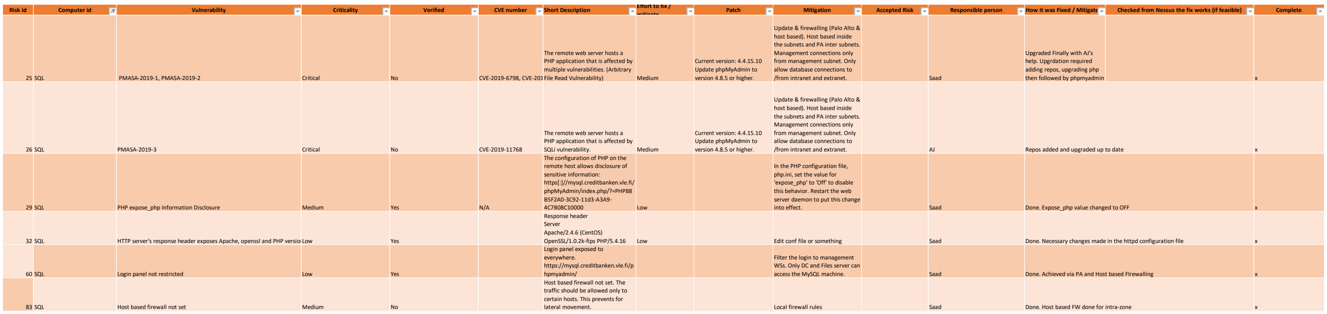
4.4.5 MySQL Server

Impact: Estimated impact Critical. Loss of customer's data, bank's employee's data.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
OS Linux release 7	Database Server Version: 5.5.68-MariaDB PHPMyAdmin: 5.2.1 PHP Version: 8.2.4	MySQL serves as the Database of users and devices.	**Inbound** 10.100.0.0/24 Ports 80, 443 for HTTP, HTTPS Port 22 for SSH	For web access to the MySQL server Management connections
			Outbound (allowed to)	

Patching and Mitigations:

The Figure 6 specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigate	Checked from Nessus the fix works (if feasible)	Complete
25	SQL	PMASA-2019-1, PMASA-2019-2	Critical	No	CVE-2019-6798, CVE-201	The remote web server hosts a PHP application that is affected by multiple vulnerabilities. (Arbitrary File Read Vulnerability)	Medium	Current version: 4.4.15.10 Update phpMyAdmin to version 4.8.5 or higher.	Update & firewalling (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet. Only allow database connections to /from intranet and extranet.		Saad	Upgraded Finally with AJ's help. Upgrdation required adding repos, upgrading php then followed by phpmyadmin		x
26	SQL	PMASA-2019-3	Critical	No	CVE-2019-11768	The remote web server hosts a PHP application that is affected by SQLi vulnerability.	Medium	Current version: 4.4.15.10 Update phpMyAdmin to version 4.8.5 or higher.	Update & firewalling (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet. Only allow database connections to /from intranet and extranet.		AJ	Repos added and upgraded up to date		x
29	SQL	PHP expose_php Information Disclosure	Medium	Yes	N/A	The configuration of PHP on the remote host allows disclosure of sensitive information: https[:]//mysql.creditbanken.vle.fi/phpMyAdmin/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000	Low		In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.		Saad	Done. Expose_php value changed to OFF		x
32	SQL	HTTP server's response header exposes Apache, openssl and PHP versio	Low	Yes		Response header Server Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16	Low		Edit conf file or something		Saad	Done. Necessary changes made in the httpd configuration file		x
60	SQL	Login panel not restricted	Low	Yes		Login panel exposed to everywhere. https://mysql.creditbanken.vle.fi/phpmyadmin/			Filter the login to management WSs. Only DC and Files server can access the MySQL machine.		Saad	Done. Achieved via PA and Host based FIrewalling		x
83	SQL	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Saad	Done. Host based FW done for intra-zone		x

Figure 6. SQL patching and remediations

Notes Regarding the Server:

Since CentOS 7 is End of Life, mirrors were changed to vault.centos.org where they will be archived permanently the server has been updated to the last possible version. The vulnerabilities mentioned in the project Excel have been fixed. The server's firewall is enabled.

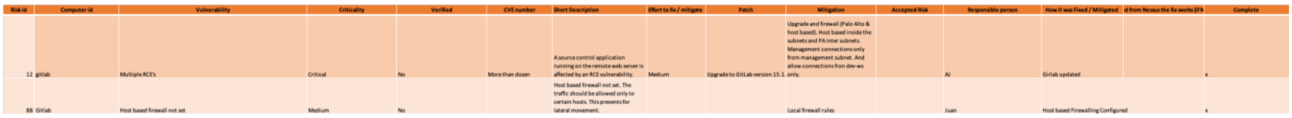
4.4.6 Gitlab Server

Impact: Estimated impact Critical 4: the server contains the codes of the bank's critical systems.

OS versioning	Service numbering (after updates)	Service description	Firewalling (Source hosts, Protocol + Port)	More details about connections
OS Linux release 8.5.2111	Apache 2.4.37 gitlab-ee 15.10.1	Server provides code repository and collaborative software development platform	**Inbound** Management VLANs (SSH (22)) 10.0.110.10 & 20(SSH (22))	Management connections Gitlab ssh connection
			Outbound (allowed to) Elastic nodes (TCP, 9200)	Auditbeat agent, Filebeat agent

Patching & mitigations

The Figure 77. Gitlab patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigated	d from Nessus the fix works (if fi	Complete
12	gitlab	Multiple RCE's	Critical	No	More than dozen	A source control application running on the remote web server is affected by an RCE vulnerability.	Medium	Upgrade to GitLab version 15.1.	Upgrade and firewall (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet. And allow connections fron dev-ws only.		AJ	Girlab updated		x
88	Gitlab	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan	Host based Firewalling Configured		x

Figure 77. Gitlab patching and remediations

Notes regarding the server

Since CentOS 8 is End of Life, mirrors were changed to vault.centos.org where they will be archived permanently the server has been updated to the last possible version. The vulnerabilities mentioned in the project Excel have been fixed.

The server's firewall is enabled. In the firewall, traffic to the internet is not allowed. Subnets IT MGMT and MGMT WS connected to trusted networks, so ssh, SIEM and FireEye services work. In the Palo Alto firewall, the traffic of the management networks is more precisely restricted per service and port. Access to the servers is blocked from other servers in the same subnet, except ssh connection from 10.0.110.10 and 20 are allowed connect to Gitlab via SSH.

Since CentOS 8 is no longer supported, automatic update cannot be enabled.

Unnecessary packages have been cleaned from the server.

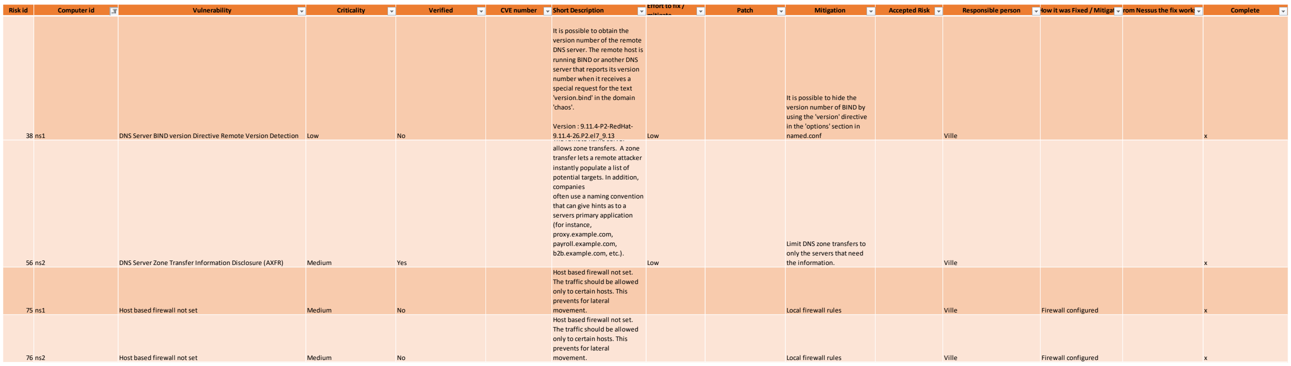
4.4.7 NS1-2

Impact: Estimated impact medium 2: Name services are important for everyday operations of the organization, but loss of them does not deny accessibility of resources via IP-address. Configuration files on many of the organization's servers contain either IP-based or name-based addresses making assessment of the impact difficult should the name services be lost.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
CentOS Linux release 7.9.2009 (Core)	Apache 2.4.37	Server stores and manages domain names and their corresponding IP addresses	**Inbound** Management VLANs (SSH (22)) DNS	Management connections Name services
			Outbound (allowed to)	

Patching & mitigations

The Figure 88. NS1-2 patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigat	rom Nessus the fix work	Complete
38	ns1	DNS Server BIND version Directive Remote Version Detection	Low	No		It is possible to obtain the version number of the remote DNS server. The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'. Version : 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.13	Low		It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf		Ville			x
56	ns2	DNS Server Zone Transfer Information Disclosure (AXFR)	Medium	Yes		allows zone transfers. A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that can give hints as to a servers primary application (for instance, proxy.example.com, payroll.example.com, b2b.example.com, etc.).	Low		Limit DNS zone transfers to only the servers that need the information.		Ville			x
75	ns1	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x
76	ns2	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x

Figure 88. NS1-2 patching and remediations

Notes regarding the server

Since CentOS 7 is End of Life, mirrors were changed to vault.centos.org where they will be archived permanently the server has been updated to the last possible version. The vulnerabilities mentioned in the project Excel have been fixed. The server's firewall is enabled. Since CentOS 8 is no longer supported, automatic update cannot be enabled. Unnecessary packages have been cleaned from the server.

Vulnerabilities

Service: Bind9

Details

Updated conf files to prevent zone transfer.

Service: Named Bind version number was hidden from name server configuration files. Mitigation was confirmed by querying the version number. NS2 DNS zone transfer was limited to only NS1 by creating a list of trusted servers. Confirmed by testing DNS query from NS1 which works but fails from student Kali.

Firewalling

Host based firewalling was configured to only allow SSH from management network. DNS services were allowed for all hosts in the environment.

4.4.8 FireEye

Service: FireEye EDR, Appliance image was updated from 5.1.1.953432 -> 5.3.1.982205.

Description: FireEye Endpoint Security (HX) is an endpoint security solution that combines antivirus (EPP), next-generation antivirus (NGAV), and EDR.

Agents: Agents were installed on Staff-WS2 (10.10.0.101) and Extranet-server (10.10.10.10)

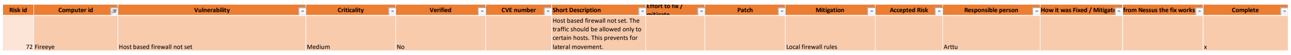
OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
FireEye v.5.3.1.982205	N/A	Endpoint security solution	**Inbound** 0.0.0.0/0 (HTTP (80), HTTPS (443)) Management VLANs (SSH (22)) FireEye EDR (TCP, 80)	WordPress Management connections FireEye Agent
			Outbound (allowed to)	

Verification

Tested FireEye malware scan by installing EICAR test virus file to Extranet-server. Initiated scan to extranet, but scan failed for some reason. Logs did not provide any valuable information about why the scan failed. After multiple failed scans, EICAR was installed to Staff-WS2 server. Then executed malware scan to staff server, scan was completed successfully but it did not find vulnerabilities. It seems that servers have some protection that detected EICAR test file and made it not function properly.

Patching & mitigations

The Figure 9. FireEye patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigate	from Nessus the fix works	Complete
72	Fireeye	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Arttu			x

Figure 9. FireEye patching and remediations

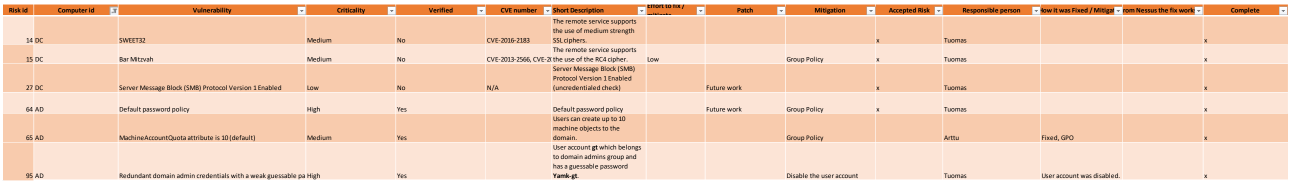
4.4.9 Windows Active Directory (DC01)

Impact: Estimated impact Critical 4: Possible Loss of sensitive customer or employee data.

OS versioning	Service numbering (after updates)	Service description	Firewalling (Source hosts, Protocol + Port)	More details about connections
Windows Server 2012R2	N/A	Server provides Windows Active Directory Domain Services (ADDS)	**Inbound** Files, Bank Staff subnet, MGMT WS subnet (SMB, RPC interfaces (135, 139 and 445), Kerberos (88), DNS (53)	Allowed to all AD related services from Files server and from subnets Bank Staff and MGMT WS.
			Outbound (allowed to) Elastic nodes (TCP, 9200)	Auditbeat agent, Filebeat agent

Patching & mitigations

The Figure 910 specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix /	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigat	rom Nessus the fix works	Complete
14	DC	SWEET32	Medium	No	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.				x	Tuomas			x
15	DC	Bar Mitzvah	Medium	No	CVE-2013-2566, CVE-2(	The remote service supports the use of the RC4 cipher.	Low		Group Policy	x	Tuomas			x
27	DC	Server Message Block (SMB) Protocol Version 1 Enabled	Low	No	N/A	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)		Future work		x	Tuomas			x
64	AD	Default password policy	High	Yes		Default password policy		Future work	Group Policy	x	Tuomas			x
65	AD	MachineAccountQuota attribute is 10 (default)	Medium	Yes		Users can create up to 10 machine objects to the domain.			Group Policy		Arttu	Fixed, GPO		x
95	AD	Redundant domain admin credentials with a weak guessable pa	High	Yes		User account **gt** which belongs to domain admins group and has a guessable password **Yamk-gt**.			Disable the user account		Tuomas	User account was disabled.		x

Figure 910. AD patching and remediations

Notes regarding the server

Firewalling

Server should be allowing only inbound traffic to Windows Active Directory specific services. Server should allow outbound Elastic Beat connections to the Elastic server.

Vulnerabilities

Server suffers from certain non-critical vulnerabilities or misconfigurations as seen in the before Figure. Risk with ID 95 was deemed the highest severity misconfiguration due to the ease to obtain Domain Admin equivalent credentials in the domain. Risks with ID 14 and 15 are deemed as accepted risks since they are unlikely to be exploited (ID 14) or the actual business impact is not high (ID 15). Namely risk 14 requires that attacker has obtained *man-in-the-middle* type of position in the network. On the other hand, risk 15 allows obtaining a Kerberos ticket with RC4 encryption as opposed to AES. Risk id 65 was fixed in order to prevent several attacks from working that require a control of service account (an AD account with an SPN). Since computer accounts satisfy this requirement, the *Machine Account Quota* AD attribute was set to 0.

MachineAccountQuota

MachineAccountQuota setting was changed from 10 to 0. By default, In the Microsoft Active Directory, members of the authenticated user group can join up to 10 computer accounts in the domain. This value is defined in the attribute *ms-DS-MachineAccountQuota* on the domain-DNS object for a domain. After changing value to 0, users must have explicit permissions in Active Directory to join computers to a domain.

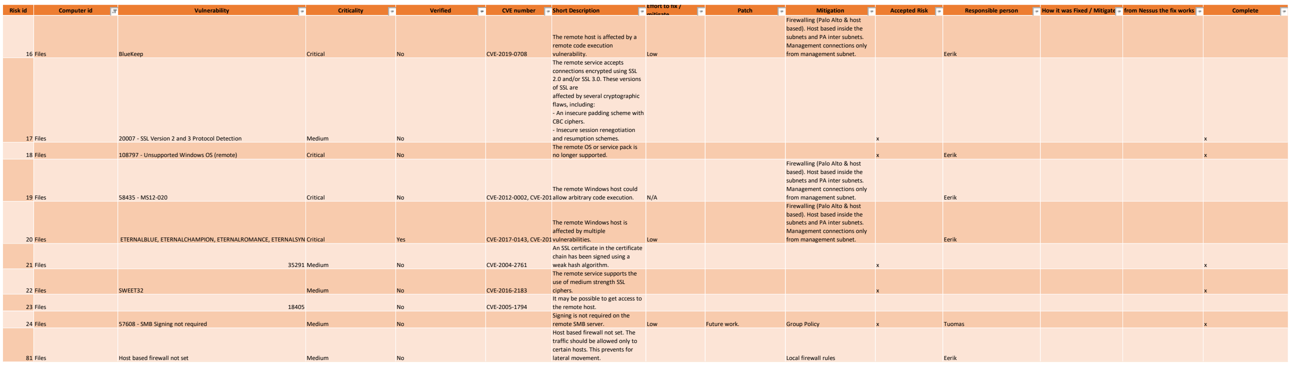
4.4.10 File and Storage services (Files)

Impact: Estimated impact medium 2: Possible Loss of sensitive customer or employee data.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
Windows Server 2008R2	N/A	Server provides Windows File and Storage Services.	**Inbound** Files, Bank Staff subnet, MGMT WS subnet (SMB, RPC interfaces (135, 139 and 445)	Allowed to all AD related services from subnets Bank Staff and MGMT WS.
			Outbound (allowed to) Elastic nodes (TCP, 9200)	Auditbeat agent, Filebeat agent

Patching & mitigations

The Figure 1011 specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigate	from Nessus the fix works	Complete
16	Files	BlueKeep	Critical	No	CVE-2019-0708	The remote host is affected by a remote code execution vulnerability.	Low		Firewalling (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet.		Eerik			
17	Files	20007 - SSL Version 2 and 3 Protocol Detection	Medium	No		The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes.				x				x
18	Files	108797 - Unsupported Windows OS (remote)	Critical	No		The remote OS or service pack is no longer supported.				x	Eerik			x
19	Files	58435 - MS12-020	Critical	No	CVE-2012-0002, CVE-201	The remote Windows host could allow arbitrary code execution.	N/A		Firewalling (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet.		Eerik			
20	Files	ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, ETERNALSYN	Critical	Yes	CVE-2017-0143, CVE-201	The remote Windows host is affected by multiple vulnerabilities.	Low		Firewalling (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet.		Eerik			
21	Files	35291	Medium	No	CVE-2004-2761	An SSL certificate in the certificate chain has been signed using a weak hash algorithm.				x				x
22	Files	SWEET32	Medium	No	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.				x				x
23	Files	18405		No	CVE-2005-1794	It may be possible to get access to the remote host.								
24	Files	57608 - SMB Signing not required	Medium	No		Signing is not required on the remote SMB server.	Low	Future work.	Group Policy	x	Tuomas			x
81	Files	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Eerik			

Figure 1011. Files patching and remediations

Notes regarding the server

Firewalling

Server should be allowing only inbound traffic to File and Storage specific services. Server should allow outbound Elastic Beat connections to the Elastic server.

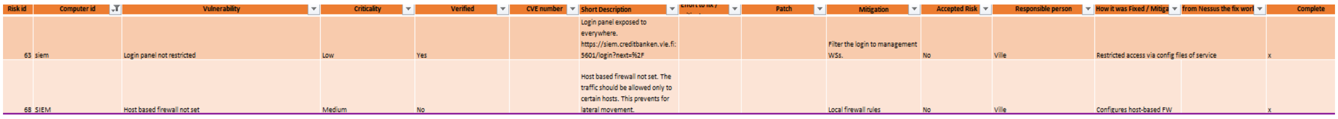
4.4.11 SIEM (security information and event management)

Impact: 4 – critical, SIEM-server is critical for organizational operations to detect unusual activity from logs.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
CentOS Linux release 7.7.1908 (Core).	Kibana version: 7.14.2 Nginx version: 1.16.1 OpenSSH version: 7.4p1	Kibana provides search and data visualization capabilities for data indexed in Elasticsearch nodes. The server provides a portal for authenticated users to search logs indexed on Elasticsearch. Server uses nginx to proxy local Kibana services.	**Inbound** Https TCP 5601 SSH	Kibana portal: https://siem.credit-banken.vle.fi Beats connect to Kibana via HTTPS which is proxied to port 5601. Kibana portal is served the same way. SSH connection allowed from management network
			Outbound (allowed to) 9200	Kibana connects to Elastic nodes on port 9200

Patching & mitigations

The Figure 1112. SIEM patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix /	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitiga	from Nessus the fix worl	Complete
63	siem	Login panel not restricted	Low	Yes		Login panel exposed to everywhere. https://siem.creditbanken.vle.fi:5601/login?next=%2F			Filter the login to management WSs.	No	Ville	Restricted access via config files of service		x
68	SIEM	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules	No	Ville	Configures host-based FW		x

Figure 1112. SIEM patching and remediations

Notes regarding the server

Login panel access was restricted by applying access only to authenticated users via nginx configuration. Access to portal was further restricted to only connections coming from management network via host-based firewall rules. Kibana, Nginx, SSH services are outdated.

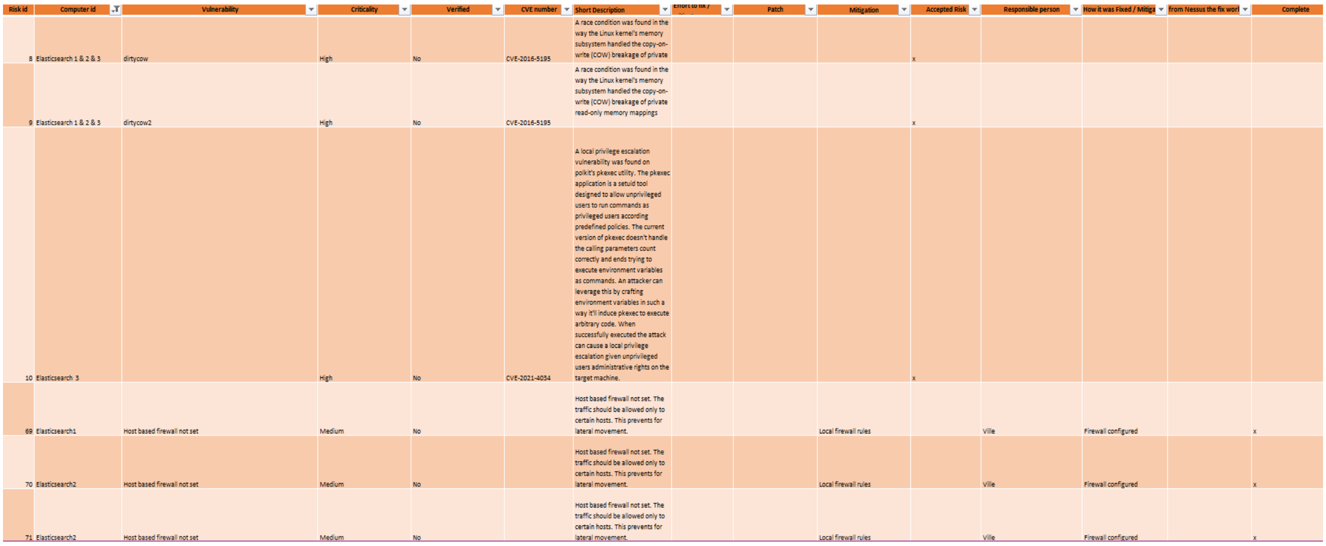
4.4.12 Elastic 1-3

Impact: 4 – critical, Elasticsearch is critical for SIEM-server to function properly.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
CentOS Linux release 7.9.2009 (Core).	Filebeat version: 7.9.2, latest 8.6.2 Elasticsearch version: 7.14.2, latest 8.6.2 OpenSSH version: 7.4p1	Elasticsearch indexes log data from Beat-agents. It provides indexed logs to Kibana. In the organization's environment, three Elasticsearch nodes are set up as a cluster.	**Inbound** Ports: 9200, 9300 Beats connect to Elastic via port 9200. ssh – Connection allowed from management VLAN	SSH connection allowed from management network. Kibana connects to Elastic nodes on port 9200.
			Outbound (allowed to) Elastic connects to other Elastic nodes on port 9200 and 9300	Auditbeat, Filebeat and Metricbeat agents on Elastic nodes.

Patching & mitigations

The Figure 1213. Elastic 1-3 patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix /	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitiga	from Nessus the fix worl	Complete
8	Elasticsearch 1 & 2 & 3	dirtycow	High	No	CVE-2016-5195	A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private				x				
9	Elasticsearch 1 & 2 & 3	dirtycow2	High	No	CVE-2016-5195	A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings				x				
10	Elasticsearch 3		High	No	CVE-2021-4034	A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.				x				
69	Elasticsearch1	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x
70	Elasticsearch2	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x
71	Elasticsearch2	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x

Figure 1213. Elastic 1-3 patching and remediations

Notes regarding the server

Host based firewall set so that SSH is only allowed from management network. Ports 9200 and 9300 are allowed publicly and all other traffic is dropped. Filebeat, Elasticsearch and SSH services are outdated.

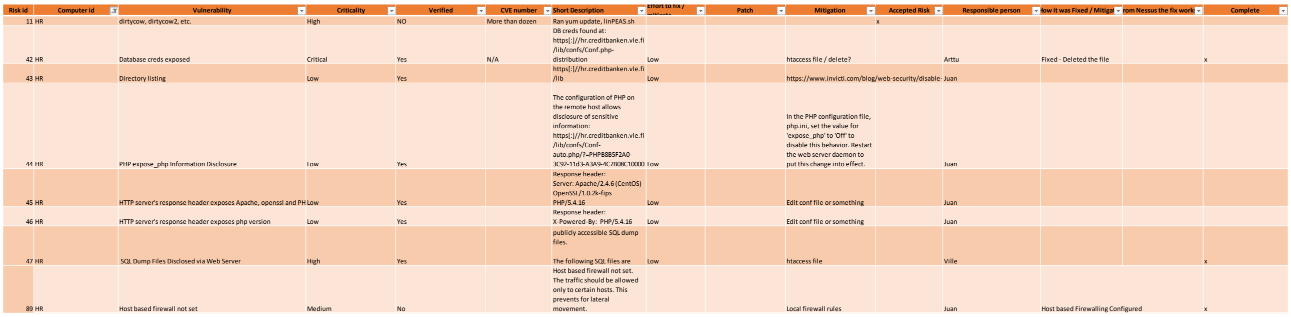
4.4.13 HR Management

Impact: 3 – high, HR services are valued high for organizations operations.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
CentOS Linux release 7.9.2009 (Core)	Apache v2.4.6	Apache v2.4.6, hosts the HR-website. MySQL - provides DB for HR	**Inbound** SSH and HTTPS – allowed from management network. HTTPS allowed from Bank staff subnet (10.10.0.0/24) MySQL-server (10.0.100.50/32 (TCP, 3306))	
			Outbound (allowed to)	

Patching & mitigations

The Figure 1314. HR management patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix /	Patch	Mitigation	Accepted Risk	Responsible person	ow it was Fixed / Mitigat	rom Nessus the fix work	Complete
11	HR	dirtycow, dirtycow2, etc.	High	NO	More than dozen	Ran yum update, linPEAS.sh				x				
42	HR	Database creds exposed	Critical	Yes	N/A	DB creds found at: https[:]//hr.creditbanken.vle.fi /lib/confs/Conf.php- distribution	Low		htaccess file / delete?		Arttu	Fixed - Deleted the file		x
43	HR	Directory listing	Low	Yes		https[:]//hr.creditbanken.vle.fi /lib	Low		https://www.invicti.com/blog/web-security/disable-		Juan			
44	HR	PHP expose_php Information Disclosure	Low	Yes		The configuration of PHP on the remote host allows disclosure of sensitive information: https[:]//hr.creditbanken.vle.fi /lib/confs/Conf- auto.php/?=PHPB8B5F2A0- 3C92-11d3-A3A9-4C7B08C10000	Low		In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.		Juan			
45	HR	HTTP server's response header exposes Apache, openssl and PH	Low	Yes		Response header: Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16	Low		Edit conf file or something		Juan			
46	HR	HTTP server's response header exposes php version	Low	Yes		Response header: X-Powered-By: PHP/5.4.16	Low		Edit conf file or something		Juan			
47	HR	SQL Dump Files Disclosed via Web Server	High	Yes		publicly accessible SQL dump files. The following SQL files are	Low		htaccess file		Ville			x
89	HR	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan	Host based Firewalling Configured		x

Figure 1314. HR management patching and remediations

Vulnerabilities: Lines 11,42,43,44,45,46,47,89 from excel.

Hardening:

Database credentials were found in configuration file and were exposed to public access. These credentials were not in use, so they were deleted. Httpd.conf was edited so that htaccess-files could be used. Availability of SQL dump files was restricted to require authentication. Currently only 'testuser:test123321' can access the files via browser.

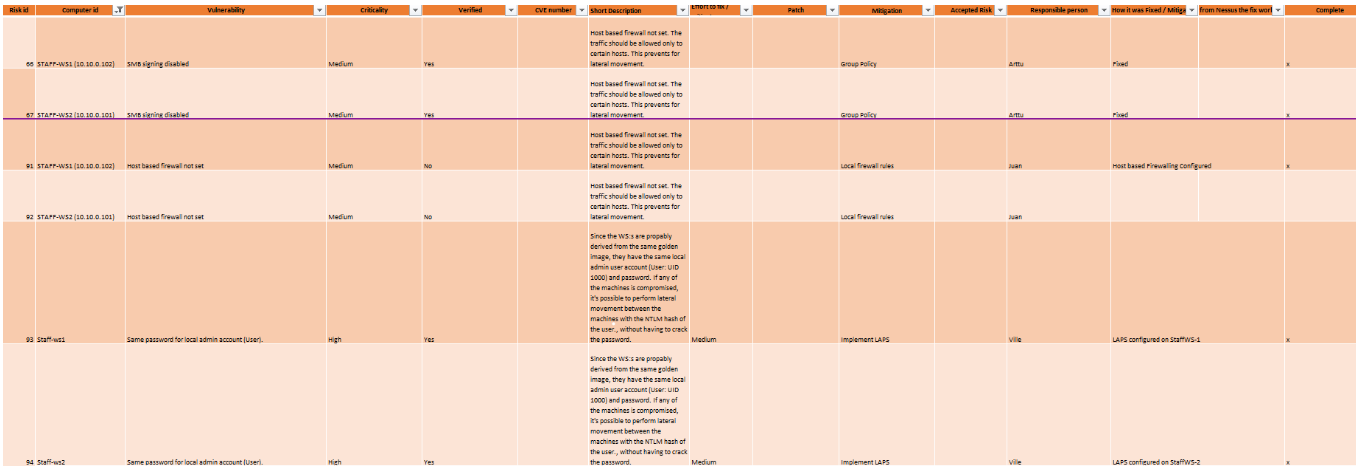
4.4.14 STAFF-WS1 & STAFF-WS2

Impact: 1 – Low, Provides basic workstation capabilities for bank staff.

OS versioning	Service numbering (after updates)	Service description	Firewalling (Source, hosts, Protocol + Port)	More details about connection
Windows 10		Staff workstation. Provides basic workstation capabilities for bank staff.	**Inbound** RDP connection allowed from management network.	
			Outbound (allowed to) Http Https Port 9200 Elastic nodes	

Patching & mitigations

The Figure 1415. Staff-WS1 patching and specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix /	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitiga	from Nessus the fix worl	Complete
66	STAFF-WS1 (10.10.0.102)	SMB signing disabled	Medium	Yes		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Group Policy		Arttu	Fixed		x
67	STAFF-WS2 (10.10.0.101)	SMB signing disabled	Medium	Yes		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Group Policy		Arttu	Fixed		x
91	STAFF-WS1 (10.10.0.102)	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan	Host based Firewalling Configured		x
92	STAFF-WS2 (10.10.0.101)	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan			
93	Staff-ws1	Same password for local admin account (User).	High	Yes		Since the WS:s are propably derived from the same golden image, they have the same local admin user account (User: UID 1000) and password. If any of the machines is compromised, it's possible to perform lateral movement between the machines with the NTLM hash of the user., without having to crack the password.	Medium		Implement LAPS		Ville	LAPS configured on StaffWS-1		x
94	Staff-ws2	Same password for local admin account (User).	High	Yes		Since the WS:s are propably derived from the same golden image, they have the same local admin user account (User: UID 1000) and password. If any of the machines is compromised, it's possible to perform lateral movement between the machines with the NTLM hash of the user., without having to crack the password.	Medium		Implement LAPS		Ville	LAPS configured on StaffWS-2		x

Figure 1415. Staff-WS1 patching and remediations

Notes regarding the server

General

FireEye agent was deployed to workstation. Sysmon and Winlogbeat installed.

Vulnerabilities

Server suffers from certain non-critical vulnerabilities or misconfigurations as seen in the before Figure.

SMB Signing disabled

(ID 66) Server message block signing, or SMB signing for short, is a Windows feature that allows you to digitally sign at the packet level. SMB signing is needed because digital signing helps recipients to confirm the origin and authenticity of the incoming packet. SMB signing was disabled in Staff-ws2, and we enabled the setting.

Same password for local admin account

Since the workstations are probably derived from the same golden image, they have the same local admin user account (User: RID 1000) and password. If any of the machines is compromised, it is possible to perform lateral movement between the machines with the NTLM hash of the user, without having to crack the password. LAPS was configured on Staff-ws1 server to mitigate.

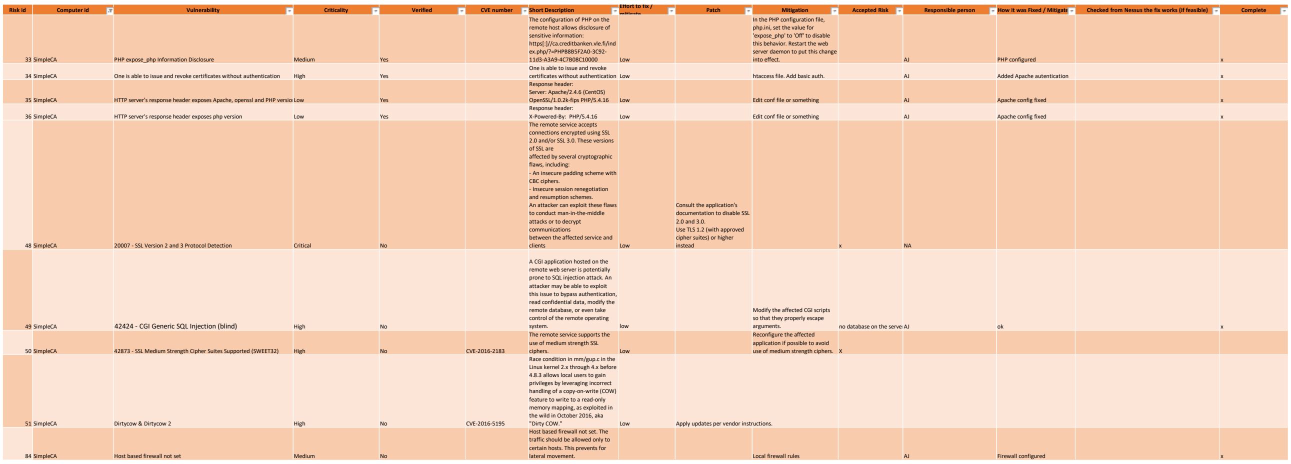
4.4.15 SimpleCa

Impact: Estimated impact critical 4: Possible Loss of certification. Affects availability of services and integrity of data.

OS versioning	**Service numbering (after updates)**	**Service description**	**Firewalling (Source hosts, Protocol + Port)**	**More details about connections**
CentOS Linux release 7.9.2009 (Core)	Custom	Service provides certification management	**Inbound** 0.0.0.0/0 HTTPS (443) Management VLANs (SSH (22))	
			Outbound (allowed to)	

Patching & mitigations

The Figure 1516. SimpleCA patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigate	Checked from Nessus the fix works (if feasible)	Complete
33	SimpleCA	PHP expose_php Information Disclosure	Medium	Yes		The configuration of PHP on the remote host allows disclosure of sensitive information: https[:]//ca.creditbanken.vle.fi/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000	Low		In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.		AJ	PHP configured		x
34	SimpleCA	One is able to issue and revoke certificates without authentication	High	Yes		One is able to issue and revoke certificates without authentication	Low		htaccess file. Add basic auth.		AJ	Added Apache autentication		x
35	SimpleCA	HTTP server's response header exposes Apache, openssl and PHP versio	Low	Yes		Response header: Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16	Low		Edit conf file or something		AJ	Apache config fixed		x
36	SimpleCA	HTTP server's response header exposes php version	Low	Yes		Response header: X-Powered-By: PHP/5.4.16	Low		Edit conf file or something		AJ	Apache config fixed		x
48	SimpleCA	20007 - SSL Version 2 and 3 Protocol Detection	Critical	No		The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients	Low	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead		x	NA			
49	SimpleCA	42424 - CGI Generic SQL Injection (blind)	High	No		A CGI application hosted on the remote web server is potentially prone to SQL injection attack. An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.	low		Modify the affected CGI scripts so that they properly escape arguments.	no database on the serve	AJ	ok		x
50	SimpleCA	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	High	No	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.	Low		Reconfigure the affected application if possible to avoid use of medium strength ciphers.	X				
51	SimpleCA	Dirtycow & Dirtycow 2	High	No	CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."	Low	Apply updates per vendor instructions.						
84	SimpleCA	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		AJ	Firewall configured		x

Figure 1516. SimpleCA patching and remediations

Notes regarding the server

Since CentOS 7 is End of Life, mirrors were changed to vault.centos.org where they will be archived permanently the server has been updated to the last possible version. The vulnerabilities mentioned in the project Excel have been fixed.

The server's firewall is enabled. In the firewall, traffic to the internet is allowed only for http and https services.

Since CentOS 8 is no longer supported, automatic update cannot be enabled.

Unnecessary packages have been cleaned from the server.

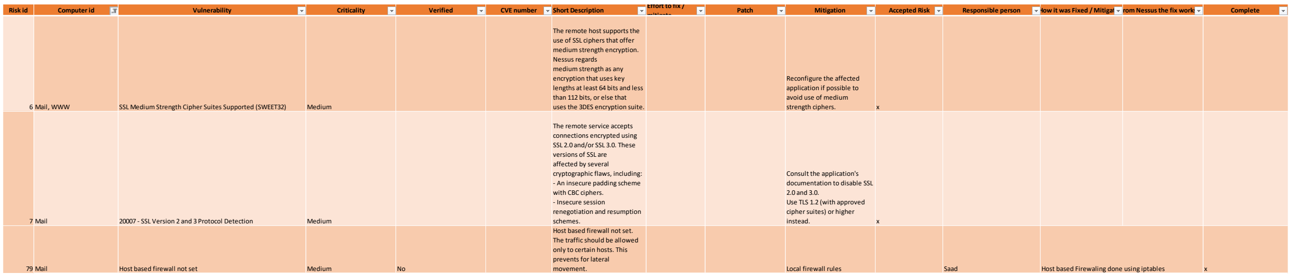
4.4.16 Mail Server

Impact: Estimated impact medium 3: Loss of data could have significant impact on business operations, including delays in communication, missed opportunities, and potential loss of revenue.

OS versioning	Service numbering (after updates)	Service description	Firewalling (Source hosts, Protocol + Port)	More details about connections
CentOS Linux release 7.9.2009 (Core)	Postfix Dovecot Roundcubemail	Service provides mail for users	**Inbound** 0.0.0.0/0 HTTPS (443) Management VLANs (SSH (22))	
			Outbound (allowed to)	

Patching & mitigations

The Figure 1617. Mail Server patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix /	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigat	rom Nessus the fix work	Complete
6	Mail, WWW	SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium			The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.			Reconfigure the affected application if possible to avoid use of medium strength ciphers.	x				
7	Mail	20007 - SSL Version 2 and 3 Protocol Detection	Medium			The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes.			Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.	x				
79	Mail	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Saad	Host based Firewaling done using iptables		x

Figure 1617. Mail Server patching and remediations

Notes regarding the server

Since CentOS 7 is End of Life, mirrors were changed to vault.centos.org where they will be archived permanently the server has been updated to the latest possible version. The vulnerabilities mentioned in the project Excel have been fixed.

The server's firewall is enabled. In the firewall, traffic to the internet is allowed only for http and https services.

Since CentOS 8 is no longer supported, automatic update cannot be enabled.

Unnecessary packages have been cleaned from the server.

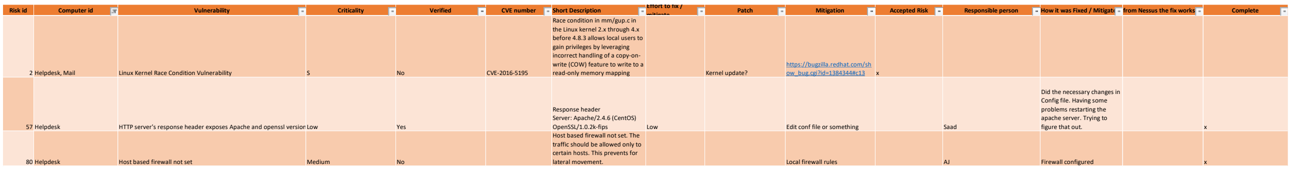
4.4.17 Helpdesk

Impact: Estimated impact critical 4: The helpdesk server is a critical component of IT support operations within the organization, including delays in resolving IT issues, reduced productivity, and potential loss of revenue.

OS versioning	Service numbering (after updates)	Service description	Firewalling (Source hosts, Protocol + Port)	More details about connections
CentOS Linux release 7.9.2009 (Core)	Zammad	Helpdesk for users	**Inbound** 0.0.0.0/0 HTTPS (443) Management VLANs (SSH (22))	
			Outbound (allowed to)	

Patching & mitigations

The Figure 1718. Helpdesk patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigate	from Nessus the fix works	Complete
2	Helpdesk, Mail	Linux Kernel Race Condition Vulnerability	S	No	CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping		Kernel update?	https://bugzilla.redhat.com/show_bug.cgi?id=1384344#c13	x				
57	Helpdesk	HTTP server's response header exposes Apache and openssl version	Low	Yes		Response header Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips	Low		Edit conf file or something		Saad	Did the necessary changes in Config file. Having some problems restarting the apache server. Trying to figure that out.		x
80	Helpdesk	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		AJ	Firewall configured		x

Figure 1718. Helpdesk patching and remediations

Notes regarding the server

Since CentOS 7 is End of Life, mirrors were changed to vault.centos.org where they will be archived permanently the server has been updated to the latest possible version. The vulnerabilities mentioned in the project Excel have been fixed.

The server's firewall is enabled. In the firewall, traffic to the internet is allowed only for http and https services.

Since CentOS 8 is no longer supported, automatic update cannot be enabled.

Unnecessary packages have been cleaned from the server.

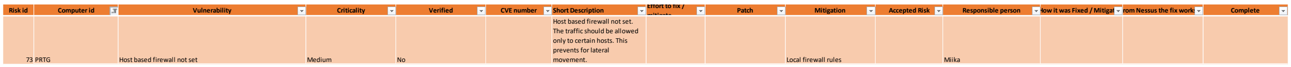
4.4.18 PRTG

Impact: Estimated impact high 3: Network monitoring and management server. Used to monitor IT infrastructure, including servers, routers, switches and other network devices.

OS versioning	Service numbering (after updates)	Service description	Firewalling (Source hosts, Protocol + Port)	More details about connections
Windows Server 2012R2	N/A	Network monitoring and management service	**Inbound** 0.0.0.0/0 (HTTP (80), HTTPS (443)) Management VLANs (SSH (22))	WordPress Management connections
			Outbound (allowed to) Elastic nodes (TCP, 9200)	

Patching & mitigations

The Figure 1819. PRTG patching and remediations specifies e.g., vulnerabilities and corresponding criticality, description, patch, mitigation and whether it is specified as accepted risk.



Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix /	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigat	rom Nessus the fix works	Complete
73	PRTG	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Miika			

Figure 1819. PRTG patching and remediations

Notes regarding the server

Firewalling

Server should be allowing only inbound traffic to Windows Active Directory specific services. Server should not initiate any connections and are therefore blocked.

4.5 Firewalling

Firewalling is done to prevent the Bank's network from unauthorized access to the servers and rest of the network devices. It further segments the network into trusted, untrusted and semi-trusted zones and monitors and logs all connections. Therefore, the primary function of a firewall will be to create a border and inspect the packets that enter and leave the network. The inspection is done through creation of firewall rules based on source IP addresses, destination IP addresses and application.

Types of Firewalls:

Firewalls can be either hardware or software based. The major types of firewalls are Packet Filtering, Proxy, Stateful, Next Generation and Unified Threat Management Firewalls. For our network, we have used the Palo Alto Networks Next Generation Firewalls that can perform packet inspection at the application level. Further, in our Bank's network, there are two Firewalls; the first one is the External Firewall and the second one is the Internal Firewall. Each of these firewalls are explained in the section below: -

Firewall External:

The External Firewall acts as the Perimeter Firewall and prevents Private networks' access to known malicious sites. It also prevents unwanted traffic from entering the network. There is also a Demilitarized Zone (DMZ) associated with the External Firewall that is intended to be an additional layer of security for an organization's internal network. The bank's external and customer facing servers and services such as DNS, mail, proxy, NTP and bank's website are in the DMZ. The DMZ provides a buffer between the internet and bank's internal private network. The main benefits of a DMZ include Enabling Access Control, Preventing Network Reconnaissance and Blocking IP Spoofing.

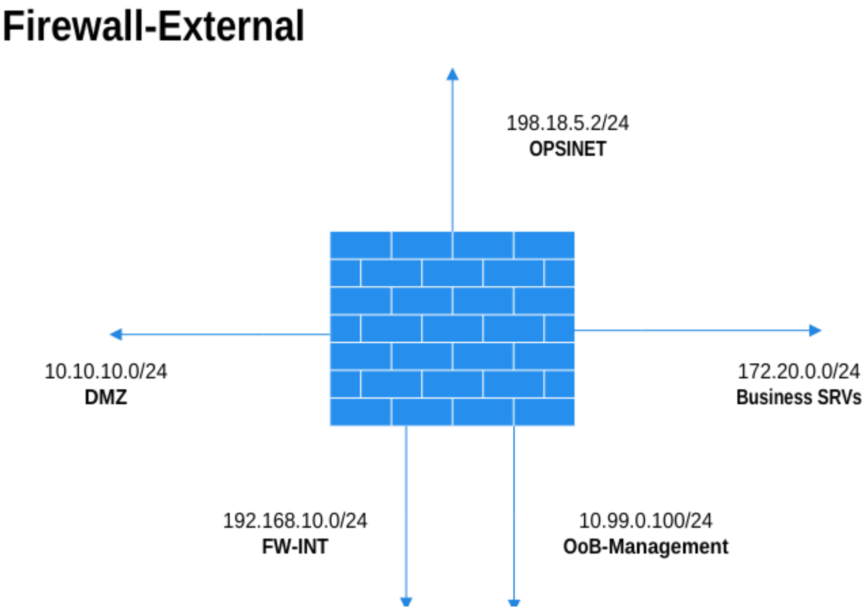


Figure 1920. External firewall

The network diagram for the External Firewall is given above (Figure 19). The first interface named OPSINET is the one connected to the internet. This interface is the one that is visible to the outside world. The second interface is the Management interface that is assigned the Management IP. This IP is the one that is used by machines in the network for accessing the Firewall. The third interface is named Firewall Internal which connects the External Firewall to the Internal Firewall. The remaining two zones are named the DMZ and Business Servers. The purpose of DMZ has been explained above. In the case of our Bank's network, it contains the Extranet Server, the Web Server, the Mail Server, the Helpdesk, the DNS servers and the NTP server. The Business Servers contain the HR machine and the Legacy Windows Application.

The Palo Alto Firewall is accessible via both command line SSH and web HTTPS. The setting of Firewall policies and configuration changes can be done via both CLI and GUI. The first step we took towards hardening Palo Alto firewall was that we upgraded the current firewall version from 9.0.5 to 11.0.0. Version upgradation serves to automatically take care of any old misconfiguration and vulnerabilities. The upgradation of PA Firewall just follows a series of commands from the command line and is also possible from the web interface.

Firewall Configurations:

The first step in configuring the firewall for necessary control over the traversing traffic is that the various interfaces of the firewall are assigned IP addresses and then these interfaces are assigned to specific zones which in our case are DMZ, BUSINESS SRVs, FW-INT, OPSINET and FW-EXT. The next step is the creation of Address Groups and Addresses which is done in the Objects section of PA Firewall configurations.

Afterwards comes the creation of Security Profiles. Before starting out to create the security policies, it is essential to create at least one security profile to be used in all your security rules. The first Security Profile to be created is The Antivirus Profile in which various protocols such as SMTP, POP3, IMAP, HTTP2 and FTP have various actions associated with them. These actions include allow, drop, alert, reset-client, reset-server and reset-both. This profile can also perform Packet Capture. The next is the Anti-Spyware Profile which operates based on the severity level of the threat. If the threats are Critical, Medium or High we can associate packet capture and either reset client, server or both. Similar actions can be taken for Low or Informational level threats. Similarly, relevant actions can be taken for DNS policies. The next profile is Vulnerability Protection, more commonly known as IPS/IDS. Here the threats can be classified based on their severity level as Critical, Medium, High or Low and Informational.

Afterwards, there is URL Filtering Profile in which the filtering is done based on URL categories which can be Ransomware, Phishing sites, adult sites, religious sites and Gambling sites. Then comes the File Blocking Profile in which the PA Firewall can block files based on their extensions. The last is the WildFire Analysis Profile in which based on the file name, file type and application, the file is forwarded to the Public Cloud. Finally, we create the Security Profile Group in which all these security profiles are merged, and default is named for the Security Profile Group.

NAT:

Network Address Translation or more commonly known as NAT / PAT is an essential part of Firewall configurations that is required by hosts in the network to reach the internet and vice versa. In our network, NAT is performed from OPSINET to DMZ as an Inbound NAT and from DMZ to OPSINET as an outbound NAT. The private IP Addresses being used are both class-A, class-B and class-C. While configuring NAT, we give the NAT policy a necessary name, the source zone, the destination zone, the source address, destination address and the type of translation that can be either NAT, PAT or dynamic IP and Port. There is also one-to-many NAT done for traffic originating from FW-INT and going to the Internet but primarily it is the one-to-one NAT that has been performed for flow of traffic between the firewall interfaces.

Security Policies:

Next is the creation of Security Policies. Two Security Policies, i.e., Intrazone and Interzone have been created by default. We have created the following rules for our External Palo Alto Firewall.

- The known Malicious, High-risk and Bulletproof IP addresses have been blocked from Untrust to Inside Network. Similarly, their access from inside Network to Outside has also been blocked.
- The Management interface of the External Firewall has been granted access from the Management Workstations subnet inside the Internal Firewall via SSH, HTTP and HTTPS.
- The Direct Access from Internet to Firewall Internal Zone has been blocked by any IP address.
- The access from Internet to DMZ has been allowed.
- The access from DMZ to Internet has also been allowed.
- The traffic between the DMZ and Business Servers has been restricted.
- Some specific Management Applications have been granted the access

Monitoring:

The traffic that flows across the various Firewall interfaces can be monitored with the help of Palo Alto Firewall. In the policies section of the PA-Firewall, there is a possibility to count the hits that the Firewall experiences for a certain policy rule. Furthermore, in the Monitor section, there are logs for data traffic between zones with the time stamp, packet-size, port, source IP and destination IP. There are similar logs for threats, URL filtering, wildfire submissions along with the report generation capability.

Zero-Trust:

Overall, with the help of this Firewall, we have implemented a zero-trust architecture in the Bank's enterprise network. Zero-trust refers to a Cybersecurity approach in which every stage of the digital interaction is validated and the principle of "Never Trust, Always Verify" is adopted using the policy of least access. We have implemented Zero-trust in our architecture using deny-all as the default policy and then allowing the traffic flow for specific applications and between certain zones and network devices.

Firewall Internal:

The Internal Firewall performs the Inter-zone traffic flow control between the zones in the internal network. The diagram (Figure 20) for the Internal Firewall indicates how the interfaces have been assigned to various zones.

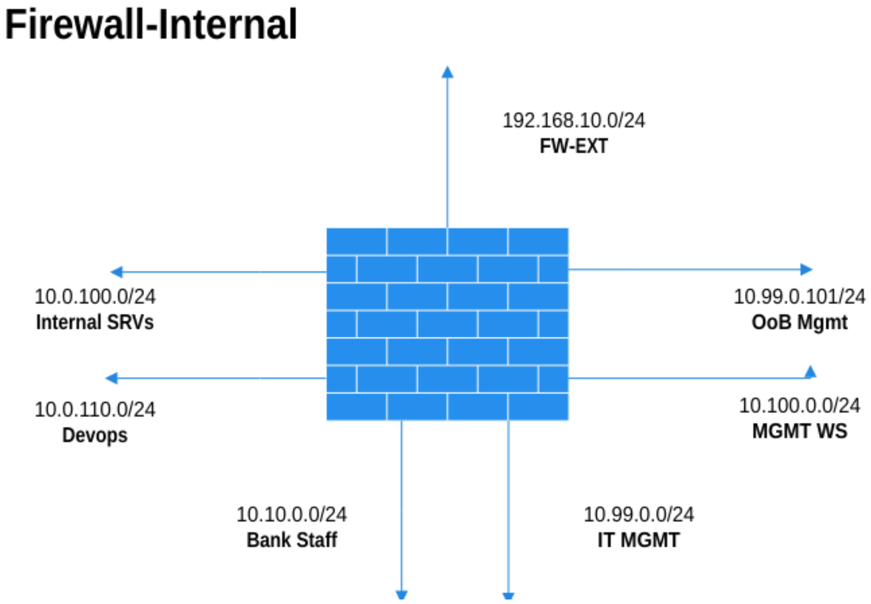


Figure 2021. Internal firewall

The first interface is connected to the External Firewall which receives the traffic from the Internet, the DMZ and Business Servers. The second interface is the OoB Management which refers to

10.99.0.101 IP address for accessing the Internal Firewall from the Management Workstations. The third zone is the Internal Servers which contains Active Directory. Active Directory is the directory service for windows-based machines. The Active Directory serves as the role of Domain Controller. It performs the authentication and authorization of all users in Windows domain network. In other words, it performs the system administration of windows-based machines. This zone also contains the Files Server which is a windows machine and is based on the ftp protocol and provides a shared disk space for storing files that can be accessed via workstations. There is also an Intranet server for sharing information, tools and collaboration within the organization. MySQL Server is a Linux based CentOS-7 operating system machine that serves as database for the whole network. There is also Simple CA which is the Certificate Authority for storing, signing and issuing Digital Certificates. The last is the proxy server which provides as intermediary between the client requesting the service and the server providing that resource.

The next zone is Devops which contains a Windows based machine, a Linux based machine and Gitlab. The Bank Staff zone contains two DHCP machines which are both windows based. The Management Workstation contains the student kali which is the machine for accessing the rest of the network along with a DHCP server for assigning the users dynamic IP addresses. Lastly, the most important is the IT Management subnet which comprises of the Firewall Management IPs, the Elastic SIEM for logs monitoring, the Fireeye, the Monitor machine which is the PRTG and three Elastic Search storage nodes.

Firewall Configurations and Security Policies:

Similar to the FW-EXT, the Internal Firewall configuration begins with creating the network interfaces and assigning them the IP addresses. It then assigns these interfaces to various zones, each of which has been explained above. Network Address Translation is not required for the Internal Firewall since the NAT has already been performed for the External Firewall. The Security Profiles for Anti-virus, Anti-spyware, Vulnerability Protection, URL Filtering, File Blocking and Wildfire area created just like previously.

Using the Internal Firewall, inter-zone access has been restricted except for specific applications and machines on need-basis. The following security policies have been created using the Internal Firewall: -

- The Management Workstation zone is allowed access to every other zone since the student kali desktop needs to access every machine in the Bank's network.
- Two-way access between the Devops zone and Bank Staff zone is restricted.
- The access between Internal Servers and Devops is restricted.
- The access between Internal Servers and Bank Staff is restricted.
- All the machines in the Internal Servers subnet are allowed to access every other machine in the IT Management subnet except for Firewalls.
- The Devops machines subnet and the IT Management zone are also restricted in access.
- The IT Management zone has restricted access for all other zones in the network.

The logs for the relevant security policies can be monitored through the hit counts and from the monitoring section of the Palo Alto Firewall.

5 Implementation of additional Security Controls

This section defines what additional security controls the company implemented.

5.1 AppLocker

Theory

AppLocker is a tool/feature of Windows that limits the applications and files user can run in Windows installation. These include executable files, scripts Windows installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers (Microsoft, 2023).

Information is the only and the most precious thing (asset) to secure in many companies and organizations. That is why we must ensure that only approved users can access that information. Access control technologies like Active Directory Rights Management Services (AD RMS) and access control lists (ACLs), eases the control user accesses.

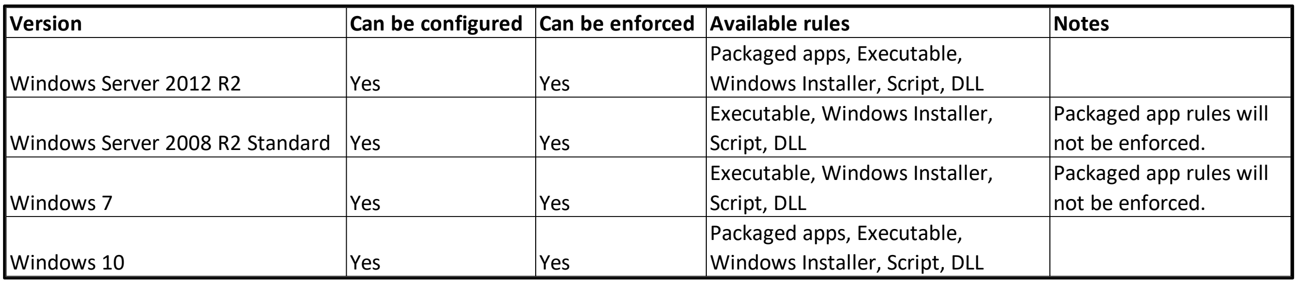
AppLocker is made to help control user or groups to delete or transmit sensitive information out of organization if user intentionally or unintentionally runs malicious software. AppLocker mitigates this risk of security breaches caused by malicious software execution by restricting the file4s that users can run.

AaronLocker

AaronLocker is a toolset for helping AppLocker and Windows Defender Application Control (WDAC) (Microsoft, 2023) creation and maintenance of a strict and robust application control. The toolset uses a small number of PowerShell scripts to do the job (Margosis, 2023).

Technical implementation

Environments where we can use AppLocker/AaronLocker functionality can be found in Table 6.



Version	Can be configured	Can be enforced	Available rules	Notes
Windows Server 2012 R2	Yes	Yes	Packaged apps, Executable, Windows Installer, Script, DLL	
Windows Server 2008 R2 Standard	Yes	Yes	Executable, Windows Installer, Script, DLL	Packaged app rules will not be enforced.
Windows 7	Yes	Yes	Executable, Windows Installer, Script, DLL	Packaged app rules will not be enforced.
Windows 10	Yes	Yes	Packaged apps, Executable, Windows Installer, Script, DLL	

Table 6. Windows system where to use AppLocker.

5.2 Local Administrator Password Solution (LAPS)

Microsoft provides a solution for managing local administrator passwords called Local Administrator Password Solution (LAPS). LAPS provides a secure method for automatically generating and managing unique passwords for local administrator accounts on Windows computers and storing them securely in Active Directory. LAPS also allows for password policy enforcement and auditing of password changes (Microsoft, n.d.).

5.3 Sysmon

Sysmon is a Windows system service and device driver that provides advanced system monitoring capabilities. It can be used to collect detailed information about various system activities, such as process creation, file creation, network connections, and registry modifications, and then log this information to the Windows event log. Sysmon can be configured to generate highly customizable event logs that provide detailed information about system events, and can be used for various use cases, such as intrusion detection, malware analysis, and forensic investigations (Microsoft, 2021).

Sysmon was installed in combination with Winlogbeat to StaffWS-2 to send Windows system logs to Kibana.

5.4 Microsoft System Center Configuration Manager (SCCM) and Windows Server Update Services (WSUS)

WSUS and SCCM are both IT management products by Microsoft. Both have their own unique capabilities to ensure endpoints are in optimal condition and compliant to policy. Both products are considered legacy products and are designed for Windows OS and Microsoft products.

WSUS stands for Windows Server Update Service (Microsoft, 2023). It is a default role that can be installed on a Windows server. WSUS is also free to use. WSUS is used to distribute patches and updates to endpoints on the network. WSUS uses push-style patching. One of the limitations with WSUS is that there is no way of knowing if the endpoint is missing a patch. Determining if a patch is missing from and endpoint is the IT administrator's responsibility. WSUS can be deployed on-prem or through Azure.

SCCM stands for System Center Configuration Manager (Microsoft, 2023), and it is included in the Microsoft Endpoint Configuration Manager (MECM) SCCM offers more feature for endpoint management like health monitoring, remote access, OS deployment, endpoint discovery, protection, and reporting. SCCM is more valuable when combined with WSUS. Unlike WSUS, SCCM is not free to use but requires a license.

WSUS and SCCM are capable effectively of managing and monitoring Microsoft environments when they are used together. Non-Windows OS management and monitoring is an issue however for these products. SCCM can patch Mac OS with add-ons, but for Linux it is not a valid option.

5.5 SCCM / WSUS in target company for assignment

1. WSUS will be used for Windows updates: WSUS is primarily designed to manage Windows updates, so it is best to use it for this purpose. This can include critical security patches, non-security updates, and service packs.
2. SCCM will be used for third-party updates: While WSUS is designed for Windows updates, SCCM can manage both Windows and third-party updates.
3. Each update will be tested in a controlled environment to ensure that they do not cause any issues.
4. Updates and compliance will be monitored. It is important to monitor the status of updates and ensure that devices are compliant with the organization's policies. This can include running regular compliance reports and tracking failed updates.
5. WSUS and SCCM maintenance: To ensure that WSUS and SCCM function effectively, it is essential to perform regular maintenance tasks like backup and recovery, database optimization, and security updates.

5.6 Center for Internet Security (CIS) Benchmark (level 1)

While performing the vulnerability scanning for the Bank’s network and followed by the security testing and technical security hardening, we have tried to implement the CIS Security Controls. CIS controls are a list of high-priority and very effective defensive actions that provide a first do starting point for every enterprise looking to improve its cyber defense. By adopting these controls, organizations can prevent a major chunk of cyber-attacks. The latest version 8 of these security controls is enumerated below:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protection
10. Malware Defenses
11. Data Recovery

12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

During the course of our technical security hardening, we performed some of these controls. These include Inventory and Control of Enterprise Assets, Software Assets, Secure Configuration of Enterprise Assets and Software, Access Control Management, Continuous Vulnerability Management, Email and Web Browser Protection, Malware Defenses, Network Monitoring and Defense and Incident Response Management.

6 Verification and Analysis of Threat Exposure after Security Controls Implementation

In this chapter, we look at verifying and analyzing exposure to a threat after security controls have been implemented in systems.

Based on the vulnerabilities collected in Excel (see Appendix 1) and the Nessus reports, we had created a list of vulnerabilities. Based on this list and reports, selected patches were implemented to patch the vulnerabilities. After the implementation of the security control measures, the Nessus scanner was run again, which was used to evaluate the effectiveness of the implemented control measures in mitigating the detected vulnerabilities. When doing each patch, we always try to ensure the reliability of the patch, either with a scanner or by checking manually. The patching method is usually recorded in the Excel workbook as well. At this point, it must be stated that some of the vulnerability fixes were possibly not recorded in the Excel workbook, especially at the point when we went through the servers manually. The final scan and analysis results revealed the following findings:

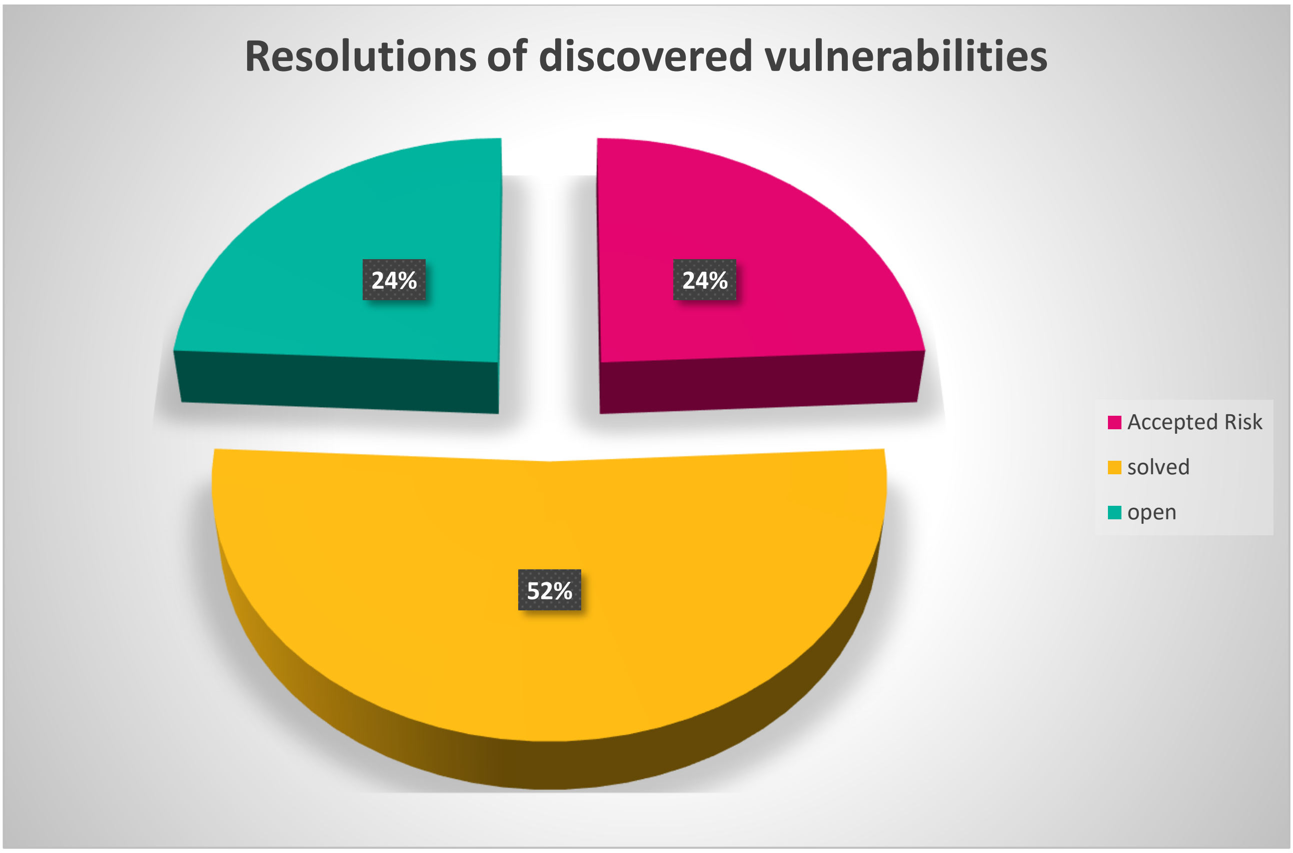


Figure 2122. Resolutions of discovered vulnerabilities

52% of vulnerabilities fixed: This indicates that more than half of the vulnerabilities identified in the vulnerability assessment were successfully fixed and the associated risks have been reduced. Patching means installing software updates or vendor-supplied patches to fix known vulnerabilities in software applications or operating systems.

24% of vulnerabilities were considered acceptable: This means that a quarter of the identified vulnerabilities were considered acceptable based on the risk assessment. Acceptable vulnerabilities are vulnerabilities that cannot be fixed or mitigated for several reasons, such as technical limitations, operational effects or lack of expertise. The aim is to monitor these systems with the help of Elastic SIEM and FireEye systems.

24% of vulnerabilities were still open: This suggests that a sizable portion of identified vulnerabilities remained unpatched and related security holes still exist. This is partly due to the fact that not all members of the group participated fully in the exercise and the servers assigned to them were partially or completely not processed.

Out of all the vulnerabilities found by Nessus (see Figure 2223), the priority was to fix Critical and High vulnerabilities. Other classifications such as medium and low were discussed within the framework of the sufficiency of time and expertise.

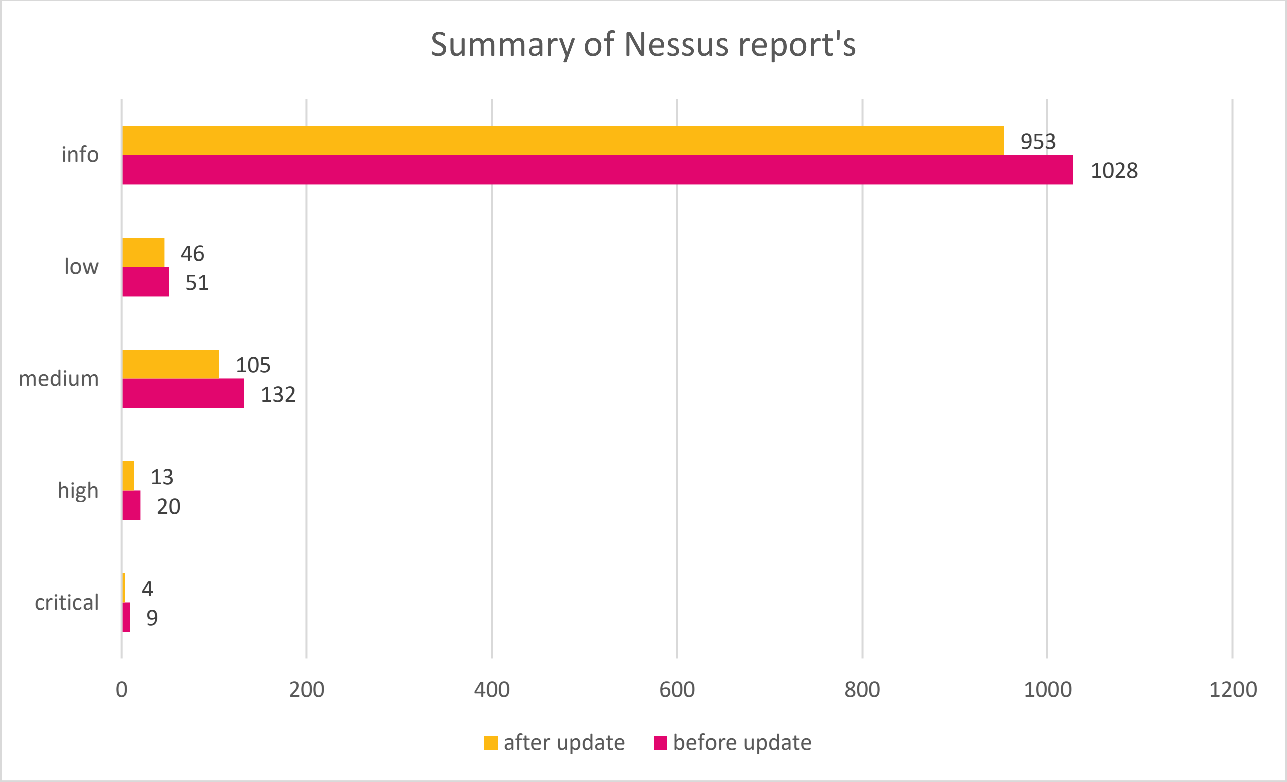


Figure 2223. Summary of Nessus reports

Based on the findings, although a significant part of the vulnerabilities was successfully fixed and were considered acceptable, there is room for improvement in fixing the remaining open vulnerabilities.

In summary, verification and analysis of threat exposure following the deployment of security controls revealed that while progress has been made in remediating and remediating acceptable vulnerabilities, additional efforts are needed to mitigate remaining open vulnerabilities.

7 Future work

The following section defines the future work to be done to enhance the company's security posture.

7.1 Update old Windows and Linux servers.

The company employs some End of Life (EOL) servers or servers that will soon drop the support for system updates. Since such systems do not receive security updates, they are prone to have critical security vulnerabilities. The possibility of updating the following servers should be examined and upgrading them if possible. In the same note, such servers should employ the newest service updates as when the servers are updated. The upgrades should be done before May 2023. The following Table 7. Operating System upgrades outlines the hosts that should be upgraded:

Host	**OS**	**EOL**	**Notes**
PRTG	2012R2	10.10.2023	Update to Windows Server 2019
www	CentOS6	30.11.2020	Update to Centos 8.5
DC	2012R2	10.10.2023	Update to Windows Server 2019
Files	2008R2	14.1.2020	Update to Windows Server 2019
Dev-WS2	Xubuntu 20.04	29.4.2023	Update to Xubuntu 22.10

Legacy application	Windows 7	14.1.2020	Update to Windows Server 2019 or Windows 10

Table 7. Operating System upgrades

In addition, the following hosts seen in Table 8 should have the service packages updated if deemed possible. Such updates should be done due to May 2023.

Host	**OS**	**Service to be updated**
Firewall-ext	PANOS	Firewall
Firewall-int	PANOS	Firewall
SIEM	CentOS7	ElasticSIEM
Elasticsearch1	CentOS7	Elasticsearch
Elasticsearch2	CentOS7	Elasticsearch
Elasticsearch3	CentOS7	Elasticsearch
ntp	CentOS7	Chrony
ns1 & ns2	CentOS7	Bind
Extranet	CentOS8	WordPress

Mail	CentOS7	Postfix + Dovecot + Roundcubemail
Helpdesk	CentOS7	Zammad
Intra	CentOS8	WordPress
SQL	CentOS7	MySQL
SimpleCA	CentOS7	Custom
Proxy	CentOS7	Squid
Gitlab	CentOS8	Gitlab
HR	CentOS7	OrangeHRM

Table 8. Service updates

7.2 Microsoft Defender for Endpoint & cloud

The company has ongoing negotiations with Microsoft to update the endpoint detection and response system from FireEye to Microsoft Defender for Endpoint. In addition, the company is moving from local hosted services to cloud and is choosing to use Microsoft as the provider. The company is going to move to *Office 365* to use Office tools suite and Exchange. For hosting other services, the company is currently choosing between Azure and AWS. The upgrades should be done before June 2023.

7.3 SELinux & AppArmor

The company is going to enable SELinux and AppArmor security controls for the *nix systems. Such security controls could prevent escalating privileges on such systems if the attacker has a foothold on them. The upgrades should be done before October 2023.

7.4 SSH key authentication

SSH public key authentication (SSH, 2023) is based on an algorithm. Two of the most common that are being used are RSA and DSA. Public key encryption algorithms work with two separate keys. These two keys form a pair called public key and private key.

The motivation for using public key authentication and not passwords is security. SSH key authentication provides cryptographic strength that even extremely complicated passwords cannot offer. SSH public key authentication allows the implementation of single sign-on across SSH servers.

SSH key authentication prevents brute-force attacks and if the server that uses SSH key authentication is compromised. There are no credentials at risk.

SSH key authentication will be used for every Linux endpoint in the company network. In addition to SSH key authentication, the Root access for all Linux endpoints will be configured to go through a PAM (Privileged Access Management) solution. The PAM solution will also rotate the SSH keys after every launched session.

7.5 Tier level authentication model

MSFT Red Forest vs PAM

Privileged Access Management (PAM) (Microsoft, 2023) and Microsoft's Red Forest (Microsoft, 2023) are two distinct concepts related to cybersecurity, specifically in the domain of identity and access management. Red Forest architecture became popular to combat rising cyber-attacks. However, while the Red Forest approach was promising in theory, it was a complex and costly solution. For this reason, Microsoft is not recommending Red Forest approach anymore and has instead recommending the use of PAM.

Red Forest overview

The Red Forest or ESAE (Enhanced Security Admin Environment) (Microsoft, 2023) idea is based on tiering and limiting exposure of Administrative or highly privileged credentials in a case of a credential theft attack. The purpose of the tiers is to protect systems with a set of buffer zones between full control (Tier 0) and the high-risk workstations that are being compromised regularly. The tier model is composed of three levels. Each level includes only administrative accounts and not any standard user accounts.

Tier levels

Tier 0 has direct administrative access to the Active Directory or Domain controllers and all the assets they have. Tier 0 is the most critical and sensitive tier as it can control all the other assets.

Tier 1 has control of server operating systems, cloud services and enterprise applications. The tier 1 administrative accounts have high privileged access as they can control servers and cloud services. By compromising a tier 1 administrative account, the attacker gains access to the servers and cloud services and can control enterprise services.

Tier 2 has control of user workstations and devices. Tier 2 administrator accounts have control of business assets like Help desk and support administrator. For this reason, they have access to user data across the enterprise.

PAM (Privileged Access Management)

Microsoft has recently (Year?) retired the Red Forest approach to addressing privileged access and privileged access escalation. The recommendation is to use PAM instead (Microsoft, 2023) PAM is Privileged access management, and its aim is to implement least privileged and zero trust in enterprise environments. PAM can be implemented to cover most if not all modern enterprise use cases and most PAM products offer a wide variety of functionalities that cover everything from credential management to sessions launching, monitoring, and auditing.

PAM in target company for assignment

A PAM solution will be implemented in the environment, and it will be used for all access that can be considered privileged access. The PAM solution will be used for RDP and SSH connections for accessing administrative and root accounts on Windows and Linux servers. A password and SSH key rotation will be implemented to maximize security in the endpoints. HTTPS connections to services with administrative accounts will also be included in the PAM solution.

7.6 Logging

Company uses Elasticsearch and Kibana from ELK stack to apply logging to environment activities. Elasticsearch is a search and analytics engine used for storing and indexing logs. Kibana is a visualization tool used for querying and analyzing log data through a web interface. The ELK stack is commonly used for various use cases, such as troubleshooting, security analysis, and business intelligence (Elasticsearch B.V., n.d.).

Log collecting and shipping is implemented via Beats. Beats is an open-source platform for collecting, shipping, and processing data in real-time. It is composed of lightweight data shippers that can be installed on various sources, such as servers, containers, and IoT devices, to collect and forward data to a centralized location. The data can then be processed and analyzed by various backends, such as Elasticsearch, Logstash, or Kibana. Beats include various modules, such as Filebeat for collecting log files, Metricbeat for collecting system metrics, and Packetbeat for analyzing network traffic. The platform is commonly used for various use cases, such as monitoring, security, and application performance management (Elasticsearch B.V., n.d.).

The company will expand its current logging policies to affect all systems within its network. Current logging status can be reviewed in this report’s attachment which includes information about what Beat-agents are used, in which systems those are installed and what modules are enabled within them.

During the review of the environment, it was observed that in all the configuration files of the ELK-stack the master credentials for the log system were stored in clear text. The Company can either implement API-key authentication or change the authentication credentials to some less privileged ones. The credentials being used are suitable for setting up the environment but should not be used in production. Kibana will also be configured with additional credentials for viewing log data instead of using the master credentials.

In addition, it was observed that Beat-agent configurations were not using SSL-verification when connecting to Elasticsearch nodes. The company will change the configurations of installed agents and enable SSL.

References

Ansible -Automation tool. Accessed on 1 April 2023. Accessed from https://www.ansible.com

Chef -Automation tool. Accessed on 1 April 2023. https://www.chef.io

CrackMapExec. (2022, November 14). GitHub page for the tool. Accessed on 1 April 2023. Retrieved from https://github.com/Porchetta-Industries/CrackMapExec.

Elasticsearch B.V. (n.d.). What is the ELK stack? Retrieved from https://www.elastic.co/what-is/elk-stack

Elasticsearch B.V. (n.d.). Beats. Retrieved from https://www.elastic.co/beats/

ffuf - Fuzz Faster U Fool. (2023, February 6). GitHub page for the tool. Accessed on 1 April 2023. Retrieved from https://github.com/ffuf/ffuf.

Get Metasploit. (n.d.). Page to download the tool. Accessed on 1 April 2023. Retrieved from https://www.metasploit.com/download.

GreenBone - The Greenbone Security Assistant (GSA). (2021). GitHub page for the tool. Accessed on 10 January 2023. Retrieved from https://github.com/greenbone/

hashcat advanced password recovery. (2022 September 2). Accessed on 1 April 2023. Page to download the tool. Retrieved from https://hashcat.net/hashcat/.

Impacket. (2022, May 4). GitHub page for the tool. Accessed on 1 April 2023. Retrieved from https://github.com/fortra/impacket.

LinPEAS - Linux Privilege Escalation Awesome Script. (2023, March 29). GitHub page for the tool. Accessed on 1 April 2023. Retrieved from https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS.

Microsoft. (n.d.). Local Administrator Password Solution (LAPS). Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=46899

Microsoft. (2021). Sysmon. Retrieved from https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Microsoft. (2023,0403). Enhanced Security Admin Environment https://learn.microsoft.com/en-us/security/privileged-access-workstations/esae-retirement

Microsoft .(2023) What is privileged access management (PAM) https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam

Nidecki, T.A. (2019, September 26). *What Are DNS Zone Transfers (AXFR)*. Article on Acunetix's website. Accessed on 1 April 2023. Retrieved from https://www.acunetix.com/blog/articles/dns-zone-transfers-axfr/.

Puppet -Automation tool. Accessed on 1 April 2023. Accessed from https://www.puppet.com/

PywerView. (2023, January 26). GitHub page for the tool. Accessed on 1 April 2023. Retrieved from https://github.com/the-useless-one/pywerview.

Rustscan the modern port scanner. (2022, November 7). GitHub page for the tool. Accessed on 1 April 2023. Retrieved from https://github.com/RustScan/RustScan.

SSH. (2023). What is SSH Public Key Authentication? https://www.ssh.com/academy/ssh/public-key-authentication

Tenable for Education. (n.d.). Page to download the tool. Accessed on 1 April 2023. Retrieved from https://www.tenable.com/tenable-for-education/nessus-essentials.

Windows Privilege Escalation Awesome Scripts. (2022, December 23). GitHub page for the tool. Accessed on 1 April 2023. Retrieved from https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

Wikipedia. (2020). *File Server.* Retrieved from https://en.wikipedia.org/wiki/File_server

Wikipedia. (2021). *Active Directory.* Retrieved from https://en.wikipedia.org/wiki/Active_Directory

Wikipedia. (2019). *Intranet.* Retrieved from https://en.wikipedia.org/wiki/Intranet

Palo Alto Networks. (n.d.) *What is Zero-Trust Architecture.* Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

Fireeye (2017, January). *APT 28: At the Center of the Storm.* Retrieved from

https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

Sans Institute (2021, May 18). *CIS Controls v8.* Retrieved from https://www.sans.org/blog/cis-controls-v8/

Appendix 1. Service Catalog creditbanken.vle.fi

Risk id	Computer id	Vulnerability	Criticality	Verified	CVE number	Short Description	Effort to fix / mitigate	Patch	Mitigation	Accepted Risk	Responsible person	How it was Fixed / Mitigat	rom Nessus the fix works	Complete
1	Extranet, WWW, Mail	Polkit Out-of-Bounds Read and Write Vulnerability	High	No	CVE-2021-4034	Local privilege escalation in pkexec due to incorrect handling of argument vector		Fixed with updates, not available for CentOS Linux release 8.0.1905? Not available for CentOS Linux release CentOS release 6.3 (Final)?	Temporary mitigation exists at the expense of pkexec's capabilities. By removing SUID permissions, the program cannot run processes as root. However, any processes that rely on it for normal operation will be affected.	x	Eerik			
2	Helpdesk, Mail	Linux Kernel Race Condition Vulnerability	S	No	CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping		Kernel update?	https://bugzilla.redhat.com/show_bug.cgi?id=1384344#c13	x				
3	Extranet	Linux Kernel Privilege Escalation Vulnerability	High	No	CVE-2022-2588	A use-after-free flaw was found in route4_change in the net/sched/cls_route.c filter implementation in the Linux kernel. This flaw allows a local user to crash the system and possibly lead to a local privilege escalation problem.		Kernel update?		x	Eerik			
4	NTP, NS1, NS2	Linux Kernel Race Condition Vulnerability	High	No	CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping		Kernel update?		x				
5	NTP, NS1, NS2	Polkit Out-of-Bounds Read and Write Vulnerability	High	No	CVE-2021-4034	Local privilege escalation in pkexec due to incorrect handling of argument vector				x				
6	Mail, WWW	SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium			The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.			Reconfigure the affected application if possible to avoid use of medium strength ciphers.	x				
7	Mail	20007 - SSL Version 2 and 3 Protocol Detection	Medium			The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes.			Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.	x				
8	Elasticsearch 1 & 2 & 3	dirtycow	High	No	CVE-2016-5195	A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW)				x				
9	Elasticsearch 1 & 2 & 3	dirtycow2	High	No	CVE-2016-5195	A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings				x				

10	Elasticsearch 3		High	No	CVE-2021-4034	A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.				x				
11	HR	dirtycow, dirtycow2, etc.	High	NO	More than dozen	Ran yum update, linPEAS.sh				x				
12	gitlab	Multiple RCE's	Critical	No	More than dozen	A source control application running on the remote web server is affected by an RCE vulnerability.	Medium	Upgrade to GitLab version 1	Upgrade and firewall (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet. And allow connections fron dev-ws only.		AJ	Girlab updated		x
13	legacy-app													
14	DC	SWEET32	Medium	No	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.				x	Tuomas			x
15	DC	Bar Mitzvah	Medium	No	CVE-2013-2566, CVE-2(	The remote service supports the use of the RC4 cipher.	Low		Group Policy	x	Tuomas			x
16	Files	BlueKeep	Critical	No	CVE-2019-0708	The remote host is affected by a remote code execution vulnerability.	Low		Firewalling (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet.		Eerik			
17	Files	20007 - SSL Version 2 and 3 Protocol Detection	Medium	No		The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes.				x				
18	Files	108797 - Unsupported Windows OS (remote)	Critical	No		The remote OS or service pack is no longer supported.				x	Eerik			
19	Files	58435 - MS12-020	Critical	No	CVE-2012-0002, CVE-2(	The remote Windows host could allow arbitrary code execution.	N/A		Firewalling (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet.		Eerik			
20	Files	ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, ETERN/	Critical	Yes	CVE-2017-0143, CVE-2(	The remote Windows host is affected by multiple vulnerabilities.	Low		Firewalling (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet.		Eerik			
21	Files	35291	Medium	No	CVE-2004-2761	An SSL certificate in the certificate chain has been signed using a weak hash algorithm.				x				
22	Files	SWEET32	Medium	No	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.				x				
23	Files	18405		No	CVE-2005-1794	It may be possible to get access to the remote host.								
24	Files	57608 - SMB Signing not required	Medium	No		Signing is not required on the remote SMB server.	Low	Future work.	Group Policy	x	Tuomas			x
25	SQL	PMASA-2019-1, PMASA-2019-2	Critical	No	CVE-2019-6798, CVE-2(	The remote web server hosts a PHP application that is affected by multiple vulnerabilities. (Arbitrary File Read Vulnerability)	Medium	Current version: 4.4.15.10 Update phpMyAdmin to version 4.8.5 or higher.	Update & firewalling (Palo Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet. Only allow database connections to /from intranet and extranet.		Saad	Upgraded Finally with AJ's help. Upgrdation required adding repos, upgrading php then followed by phpmyadmin		x
26	SQL	PMASA-2019-3	Critical	No	CVE-2019-11768	The remote web server hosts a PHP application that is affected by SQLi vulnerability.	Medium	Current version: 4.4.15.10 Update phpMyAdmin to version 4.8.5 or higher.	Alto & host based). Host based inside the subnets and PA inter subnets. Management connections only from management subnet. Only allow database connections to /from intranet and extranet.		AJ	Repos added and upgraded up to date		x
27	DC	Server Message Block (SMB) Protocol Version 1 Enabled	Low	No	N/A	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)		Future work		x	Tuomas			x
28	Intra	Browsable Web Directories	Medium	Yes	N/A	Browsable Web Directories	Low	https://www.invicti.com/b	htaccess file		Miika			
29	SQL	PHP expose_php Information Disclosure	Medium	Yes	N/A	The configuration of PHP on the remote host allows disclosure of sensitive information: https[:]//mysql.creditbanken.vle.fi/phpMyAdmin/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000	Low		In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.		Saad	Done. Expose_php value changed to OFF		x
30	Intra	HTTP server's response header exposes Apache and openssl ver	Low	Yes	N/A	Response header Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k	Low		Edit conf file or something		Miika			
31	Intra	HTTP server's response header exposes php version	Low	Yes	N/A	Response header X-Powered-By: PHP/7.2.24	Low		Edit conf file or something		Miika			
32	SQL	HTTP server's response header exposes Apache, openssl and PH	Low	Yes		Response header Server Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16	Low		Edit conf file or something		Saad	Done. Necessary changes made in the httpd configuration file		x
33	SimpleCA	PHP expose_php Information Disclosure	Medium	Yes		The configuration of PHP on the remote host allows disclosure of sensitive information: https[:]//ca.creditbanken.vle.fi/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000	Low		In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.		AJ	PHP configured		x

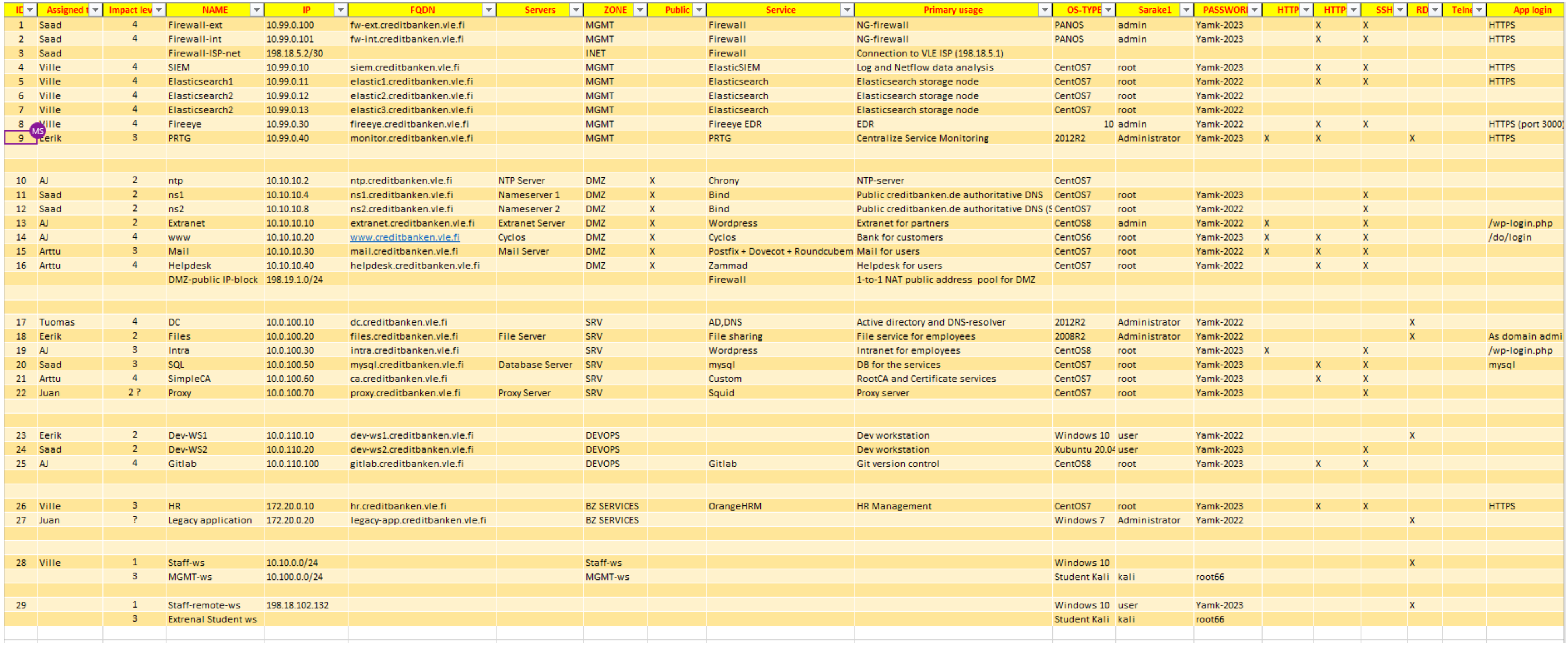
34	SimpleCA	One is able to issue and revoke certificates without authenticati	High	Yes		One is able to issue and revoke certificates without authentication	Low		htaccess file. Add basic auth.		AJ	Added Apache autentication		x
35	SimpleCA	HTTP server's response header exposes Apache, openssl and PH	Low	Yes		Response header: Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16	Low		Edit conf file or something		AJ	Apache config fixed		x
36	SimpleCA	HTTP server's response header exposes php version	Low	Yes		Response header: X-Powered-By: PHP/5.4.16	Low		Edit conf file or something		AJ	Apache config fixed		x
37	Proxy	HTTP server's response header exposes squid proxy version	Low	Yes		Response header: Server: squid/3.5.28 http[:]//proxy.creditbanken.vle.fi:3128/	Low		Edit conf file or something		Miika			
38	ns1	DNS Server BIND version Directive Remote Version Detection	Low	No		It is possible to obtain the version number of the remote DNS server. The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'. Version : 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.13	Low		It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf		Ville			x
39	extranet	HTTP server's response header exposes Apache and openssl ver	Low	Yes		Response header Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k	Low		Edit conf file or something		Eerik			
40	extranet	HTTP server's response header exposes php version	Low	Yes		Response header X-Powered-By: PHP/7.2.24	Low		Edit conf file or something		Eerik			
41	www	HTTP server's response header exposes Apache version		Yes		Response header Server: Apache-Coyote/1.1	Low		Edit conf file or something					
42	HR	Database creds exposed	Critical	Yes	N/A	DB creds found at: https[:]//hr.creditbanken.vle.fi/lib/confs/Conf.php-distribution	Low		htaccess file / delete?		Arttu	Fixed - Deleted the file		x
43	HR	Directory listing	Low	Yes		https[:]//hr.creditbanken.vle.fi/lib	Low		https://www.invicti.com/blog/web-security/disable-		Juan			
44	HR	PHP expose_php Information Disclosure	Low	Yes		The configuration of PHP on the remote host allows disclosure of sensitive information: https[:]//hr.creditbanken.vle.fi/lib/confs/Conf-auto.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000	Low		In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.		Juan			
45	HR	HTTP server's response header exposes Apache, openssl and PH	Low	Yes		Response header: Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16	Low		Edit conf file or something		Juan			
46	HR	HTTP server's response header exposes php version	Low	Yes		Response header: X-Powered-By: PHP/5.4.16	Low		Edit conf file or something		Juan			
47	HR	SQL Dump Files Disclosed via Web Server	High	Yes		publicly accessible SQL dump files. The following SQL files are	Low		htaccess file		Ville			x
48	SimpleCA	20007 - SSL Version 2 and 3 Protocol Detection	Critical	No		The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients	Low	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead		x	NA			
49	SimpleCA	42424 - CGI Generic SQL Injection (blind)	High	No		A CGI application hosted on the remote web server is potentially prone to SQL injection attack. An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.	low		Modify the affected CGI scripts so that they properly escape arguments.	no database on the ser	AJ	ok		x
50	SimpleCA	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32	High	No	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.	Low		Reconfigure the affected application if possible to avoid use of medium strength ciphers.	X				
51	SimpleCA	Dirtycow & Dirtycow 2	High	No	CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."	Low	Apply updates per vendor instructions.						
52														

53	Dev-WS1	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32	High	No	CVE-2016-2183	The remote service supports the use of medium strength SSL ciphers.	Low		Reconfigure the affected application if possible to avoid use of medium strength ciphers.	X				
54	Dev-WS2	privileged escalation polkit root on linux with bug	High	No	CVE-2021-3560	It was found that polkit could be tricked into bypassing the credential checks for D-Bus requests, elevating the privileges of the requestor to the root user. This flaw could be used by an unprivileged local attacker to, for example, create a new local administrator. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	high		Red Hat has investigated whether a possible mitigation exists for this issue, and has not been able to identify a practical example. Please update as soon as possible. Update/fix might not exist		Saad			
56	ns2	DNS Server Zone Transfer Information Disclosure (AXFR)	Medium	Yes		The remote name server allows zone transfers. A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that can give hints as to a servers primary application (for instance, proxy.example.com, payroll.example.com, b2b.example.com, etc.).	Low		Limit DNS zone transfers to only the servers that need the information.		Ville			x
57	Helpdesk	HTTP server's response header exposes Apache and openssl ver	Low	Yes		Response header Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips	Low		Edit conf file or something		Saad	Did the necessary changes in Config file. Having some problems restarting the apache server. Trying to figure that out.		x
58	Firewall-ext	SNMP Agent Default Community Name (public)	High	No		The community name of the remote SNMP server can be guessed. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications). The remote SNMP server replies to the following default community string : public	Low		Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.		Saad	Fixed - Changed the default Community String		x
59	Firewall-int	SNMP Agent Default Community Name (public)	High	No	CVE-1999-0517	The community name of the remote SNMP server can be guessed. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications). The remote SNMP server replies to the following default community string : public	Low		Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.		Saad	Fixed - Changed the default Community String		x
60	SQL	Login panel not restricted	Low	Yes		Login panel exposed to everywhere. https://mysql.creditbanken.vle.fi/phpmyadmin/			Filter the login to management WSs. Only DC and Files server can access the MySQL machine.		Saad	Done. Achieved via PA and Host based FIrewalling		x
61	extranet	Login panel not restricted	Low	Yes		Login panel exposed to everywhere. https://extranet.creditbanken.vle.fi/wp-login.php			Filter the login to management WSs.		Eerik			
62	Intra	Login panel not restricted	Low	Yes		Login panel exposed to everywhere. https://intra.creditbanken.vle.fi/wp-login.php			Filter the login to management WSs.		Miika			
63	siem	Login panel not restricted	Low	Yes		Login panel exposed to everywhere. https://siem.creditbanken.vle.fi:5601/login?next=%2F			Filter the login to management WSs.	No	Ville	Restricted access via config files of service		x
64	AD	Default password policy	High	Yes		Default password policy		Future work	Group Policy	x	Tuomas			x

65	AD	MachineAccountQuota attribute is 10 (default)	Medium	Yes		Users can create up to 10 machine objects to the domain.			Group Policy		Arttu	Fixed, GPO		x
66	STAFF-WS1 (10.10.0.102)	SMB signing disabled	Medium	Yes		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Group Policy		Arttu	Fixed		x
67	STAFF-WS2 (10.10.0.101)	SMB signing disabled	Medium	Yes		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Group Policy		Arttu	Fixed		x
68	SIEM	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules	No	Ville	Configures host-based FW		x
69	Elasticsearch1	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x
70	Elasticsearch2	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x
71	Elasticsearch2	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x
72	Fireeye	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Arttu			x
73	PRTG	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Miika			
74	ntp	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Miika			
75	ns1	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x
76	ns2	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Ville	Firewall configured		x
77	Extranet	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Eerik	Firewall configured		x
78	www	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Eerik	Host based Firewalling done		x
79	Mail	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Saad	Host based Firewaling done using iptables		x
80	Helpdesk	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		AJ	Firewall configured		x
81	Files	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Eerik			

82	Intra	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Saad	Host based Firwalling done using iptables	x
83	SQL	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Saad	Done. Host based FW done for intra-zone	x
84	SimpleCA	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		AJ	Firewall configured	x
85	Proxy	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Saad	Host based Firewalling done using ip tables	x
86	Dev-WS1	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan		
87	Dev-WS2	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Saad	Done. Host based FW done for intra-zone	x
88	Gitlab	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan	Host based Firewalling Configured	x
89	HR	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan	Host based Firewalling Configured	x
90	Legacy application	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan		
91	STAFF-WS1 (10.10.0.102)	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan	Host based Firewalling Configured	x
92	STAFF-WS2 (10.10.0.101)	Host based firewall not set	Medium	No		Host based firewall not set. The traffic should be allowed only to certain hosts. This prevents for lateral movement.			Local firewall rules		Juan		
93	Staff-ws1	Same password for local admin account (User).	High	Yes		Since the WS:s are propably derived from the same golden image, they have the same local admin user account (User: UID 1000) and password. If any of the machines is compromised, it's possible to perform lateral movement between the machines with the NTLM hash of the user., without having to crack the password.	Medium		Implement LAPS		Ville	LAPS configured on StaffWS-1	x
94	Staff-ws2	Same password for local admin account (User).	High	Yes		Since the WS:s are propably derived from the same golden image, they have the same local admin user account (User: UID 1000) and password. If any of the machines is compromised, it's possible to perform lateral movement between the machines with the NTLM hash of the user., without having to crack the password.	Medium		Implement LAPS		Ville	LAPS configured on StaffWS-2	x
95	AD	Redundant domain admin credentials with a weak guessable pa	High	Yes		User account **gt** which belongs to domain admins group and has a guessable password **Yamk-gt**.			Disable the user account		Tuomas	User account was disabled.	x

Appendix 2. Network Catalog creditbanken.vle.fi



ID	Assigned t	Impact lev	NAME	IP	FQDN	Servers	ZONE	Public	Service	Primary usage	OS-TYPE	Sarake1	PASSWORI	HTTP	HTTP:	SSH	RD	Telne	App login
1	Saad	4	Firewall-ext	10.99.0.100	fw-ext.creditbanken.vle.fi		MGMT		Firewall	NG-firewall	PANOS	admin	Yamk-2023		X	X			HTTPS
2	Saad	4	Firewall-int	10.99.0.101	fw-int.creditbanken.vle.fi		MGMT		Firewall	NG-firewall	PANOS	admin	Yamk-2023		X	X			HTTPS
3	Saad		Firewall-ISP-net	198.18.5.2/30			INET		Firewall	Connection to VLE ISP (198.18.5.1)									
4	Ville	4	SIEM	10.99.0.10	siem.creditbanken.vle.fi		MGMT		ElasticSIEM	Log and Netflow data analysis	CentOS7	root	Yamk-2023		X	X			HTTPS
5	Ville	4	Elasticsearch1	10.99.0.11	elastic1.creditbanken.vle.fi		MGMT		Elasticsearch	Elasticsearch storage node	CentOS7	root	Yamk-2022		X	X			HTTPS
6	Ville	4	Elasticsearch2	10.99.0.12	elastic2.creditbanken.vle.fi		MGMT		Elasticsearch	Elasticsearch storage node	CentOS7	root	Yamk-2022						
7	Ville	4	Elasticsearch2	10.99.0.13	elastic3.creditbanken.vle.fi		MGMT		Elasticsearch	Elasticsearch storage node	CentOS7	root	Yamk-2022						
8	Ville	4	Fireeye	10.99.0.30	fireeye.creditbanken.vle.fi		MGMT		Fireeye EDR	EDR	10	admin	Yamk-2022		X	X			HTTPS (port 3000)
9	Eerik	3	PRTG	10.99.0.40	monitor.creditbanken.vle.fi		MGMT		PRTG	Centralize Service Monitoring	2012R2	Administrator	Yamk-2023	X	X		X		HTTPS
10	AJ	2	ntp	10.10.10.2	ntp.creditbanken.vle.fi	NTP Server	DMZ	X	Chrony	NTP-server	CentOS7								
11	Saad	2	ns1	10.10.10.4	ns1.creditbanken.vle.fi	Nameserver 1	DMZ	X	Bind	Public creditbanken.de authoritative DNS	CentOS7	root	Yamk-2023			X			
12	Saad	2	ns2	10.10.10.8	ns2.creditbanken.vle.fi	Nameserver 2	DMZ	X	Bind	Public creditbanken.de authoritative DNS (S	CentOS7	root	Yamk-2022			X			
13	AJ	2	Extranet	10.10.10.10	extranet.creditbanken.vle.fi	Extranet Server	DMZ	X	Wordpress	Extranet for partners	CentOS8	admin	Yamk-2022	X		X			/wp-login.php
14	AJ	4	www	10.10.10.20	www.creditbanken.vle.fi	Cyclos	DMZ	X	Cyclos	Bank for customers	CentOS6	root	Yamk-2023	X	X	X			/do/login
15	Arttu	3	Mail	10.10.10.30	mail.creditbanken.vle.fi	Mail Server	DMZ	X	Postfix + Dovecot + Roundcubem	Mail for users	CentOS7	root	Yamk-2022	X	X	X			
16	Arttu	4	Helpdesk	10.10.10.40	helpdesk.creditbanken.vle.fi		DMZ	X	Zammad	Helpdesk for users	CentOS7	root	Yamk-2022		X	X			
			DMZ-public IP-block	198.19.1.0/24					Firewall	1-to-1 NAT public address pool for DMZ									
17	Tuomas	4	DC	10.0.100.10	dc.creditbanken.vle.fi		SRV		AD,DNS	Active directory and DNS-resolver	2012R2	Administrator	Yamk-2022				X		
18	Eerik	2	Files	10.0.100.20	files.creditbanken.vle.fi	File Server	SRV		File sharing	File service for employees	2008R2	Administrator	Yamk-2022				X		As domain admi
19	AJ	3	Intra	10.0.100.30	intra.creditbanken.vle.fi		SRV		Wordpress	Intranet for employees	CentOS8	root	Yamk-2023	X		X			/wp-login.php
20	Saad	3	SQL	10.0.100.50	mysql.creditbanken.vle.fi	Database Server	SRV		mysql	DB for the services	CentOS7	root	Yamk-2023		X	X			mysql
21	Arttu	4	SimpleCA	10.0.100.60	ca.creditbanken.vle.fi		SRV		Custom	RootCA and Certificate services	CentOS7	root	Yamk-2023		X	X			
22	Juan	2 ?	Proxy	10.0.100.70	proxy.creditbanken.vle.fi	Proxy Server	SRV		Squid	Proxy server	CentOS7	root	Yamk-2023			X			
23	Eerik	2	Dev-WS1	10.0.110.10	dev-ws1.creditbanken.vle.fi		DEVOPS			Dev workstation	Windows 10	user	Yamk-2022				X		
24	Saad	2	Dev-WS2	10.0.110.20	dev-ws2.creditbanken.vle.fi		DEVOPS			Dev workstation	Xubuntu 20.04	user	Yamk-2023			X			
25	AJ	4	Gitlab	10.0.110.100	gitlab.creditbanken.vle.fi		DEVOPS		Gitlab	Git version control	CentOS8	root	Yamk-2023		X	X			
26	Ville	3	HR	172.20.0.10	hr.creditbanken.vle.fi		BZ SERVICES		OrangeHRM	HR Management	CentOS7	root	Yamk-2023		X	X			HTTPS
27	Juan	?	Legacy application	172.20.0.20	legacy-app.creditbanken.vle.fi		BZ SERVICES				Windows 7	Administrator	Yamk-2022				X		
28	Ville	1	Staff-ws	10.10.0.0/24			Staff-ws				Windows 10						X		
		3	MGMT-ws	10.100.0.0/24			MGMT-ws				Student Kali	kali	root66						
29		1	Staff-remote-ws	198.18.102.132							Windows 10	user	Yamk-2023				X		
		3	Extrenal Student ws								Student Kali	kali	root66						