

UWTSD

Research into cyber security attacks and Penetration testing for a virtualise simulated company Website

Ethical Hacking

Flore Paviot-Adet (2422827)
06/05/2025

Table of Content

Task 1 – Research and analysis of three cyber security attacks	2
MetLife attack:.....	2
MirrorFace attacks on Japan	4
Cyberattack against FranceTravail	5
Sources	6
Task 2 : Pentest report on the infrastructure of Cureton Pharmaceutical Company	10
Introduction.....	10
List of Figures.....	10
List of Tables	10
List of Acronyms	10
Contingency Policy	11
Penetration Testing Framework and Tools	12
Design Flaws	13
Attacks conducted	13
Recommended Solutions.....	18
Recommendation for improving infrastructure security	20
Cost of Solution	23
Timetable.....	24
Invoice for the prestation	24
References	25

Task 1 – Research and analysis of three cyber security attacks

MetLife attack:

At the end of last year, RansomHub, the most prolific group of hackers this year [1], claimed the attack of MetLife, an American insurance holding company. On their leak page, RansomHub displayed a countdown before releasing an alleged 1 TB of confidential data. This data included financial and investment paperwork, meeting documents, and a list of information about IP addresses and the OS of the systems of several nations, like Brazil, Colombia, and Chile. However, this worldwide insurance agency denies the cyber-attack and claims it only targets Fondo Genesis, which is a subsidiary, and the MetLife systems were not compromised [2]. Active since February 2024, RansomHub made hundreds of victims (600 are estimated) the same year [1], surpassing even the Lockbit group. Their modus operandi is based on Ransomware as a Service and double extortion tactics [2].

A ransomware is a type of malware designed to prevent access to data on a system and asks for a ransom in exchange. This ransom typically uses cryptocurrencies, which make it difficult to track the recipient. C. Beaman et al. identify 3 types of ransomware [3]:

- Scareware: Pop-ups will encourage the target to buy software that is doing nothing in the best case or malware that will perform malicious activities in worst cases.
- Locker: The malware will block primary computer functions like screen or keyboard. Those are often easy to overcome by rebooting the computer in safe mode or running an antivirus scanner.
- Crypto: The malware will encrypt the documents, and they are often irreversible as current encryption techniques are almost impossible to revert if they are well implemented. However, if the files are encrypted with a symmetric algorithm, reverse engineering on the malware can be used to retrieve the key. Unfortunately, those types of ransomware are often using hybrid encryption: A symmetric key is used to encrypt the data, then a public key generated previously by the attacker is used to encrypt the symmetric key. Asymmetric encryption is also rarely used on its own because it is way slower than the symmetric encryption.

Ransomware as a Service makes this attack accessible for everyone, whereas advanced knowledge was previously required to build such attacks. As A. Alwashali explains, cyber criminals create platforms giving the possibility for the customer to create their own custom ransomware and distribute it to the target. Once the victim made the payment, the platform took a fee, and the rest went to the customer. These kinds of platforms are available for anyone since they are cheap. It is possible to find \$39 licences for life for the platforms

Cerber, McRansom, Philadelphia... [4] key. Asymmetric encryption is also rarely used on its own because it is way slower than the symmetric encryption.

The CISA (Cybersecurity and Infrastructure Security Agency) of the United States [5] created a cybersecurity advisory about RansomHub, detailing how they perform their attacks. Firstly, to gain initial access, they will use phishing emails and known vulnerabilities [6, 7, 8, 9, 10, 11, 12, 13, 14] in Citrix, SMB, Confluence... Once in the network, RansomHub will perform network scanning with tools like NMAP or PowerShell-based ones. They will also exploit a vulnerability in the Veeam backup to extract credentials [15]. In order to evade defence systems, the malware will rename itself in an innocent file, delete log files and deactivate antivirus systems. The next step for RansomHub is to exfiltrate data. For this, they are using several methodologies like PuTTY, HTTP POST requests, WinSCP, Metasploit,... Then, the malware will encrypt all the user files using the Elliptic Curve Encryption Algorithm, also called Curve25519. This encryption algorithm is a particularly good implementation of an elliptic-curve Diffie-Hellman because the computational speed is high, as well as security, thanks to many choices made for its design, discussed by Daniel J. Bernstein [16].

At the end of the encryption process, RansomHub will delete all the shadow copies available and will create a text file containing all the necessary information to proceed with the payment [5].

As a response to this threat, the victim should quarantine or take the compromised host offline. Then, they could re-image the hosts and create credentials in order to collect any suspicious running services/processes and recent network connections.

To avoid such attacks, CISA proposes simple countermeasures that can be put in place, like [5]:

- Conserving encrypted backups of sensitive data in different geographical locations
- Implement a strong password policy.
- Keep all operating systems, firmware and software up to date.
- Segment networks
- Disable unused ports

The paper “Ransomware’s Early Mitigation Mechanisms” [17] discusses an interesting way to detect ransomware. Indeed, by using decoy folders (folders that are usually not manipulated by users or software and systems), an algorithm running in the background could identify and count each time a process accesses those folders. At the end, a score is calculated to evaluate if the process is malicious.

MirrorFace attacks on Japan

MirrorFace, also known as “Earth Kasha”, is a Chinese hackers group that has been targeting Japan since 2019 and has conducted over 200 attacks successfully. The journal “Republic World” [18] identifies 3 phases :

- Between 2019 and 2023, MirrorFace targeted government agencies and politicians by sending phishing emails and malware in the attachments.
- 2023: MirrorFace changes its target and begins exploiting vulnerabilities in industries like aerospace and semiconductors. One of their biggest hits was against JAXA (Japan Aerospace Exploration Agency). The attackers managed to gain unauthorised access to JAXA’s internal servers, compromising personal information of employees and information related to activities with external organisations [19].
- Since 2024, their new target is academics.

MirrorFace evolved over the years, targeting several critical infrastructures to gain unauthorised access and steal sensitive data. In order to gain that unauthorised access, the journal “Security Affair” and the Japanese National Police Agency identified different vectors of compromising [20-21]:

- Spread of the LODEINFO malware, which is a backdoor allowing remote execution [22].
- Visual Studio tunnel for remote execution and Windows Sandbox exploits.
- Exploits of vulnerabilities in networking equipment concerning Array Network [23], Fortinet [24] and Citrix [25].

After gaining initial access thanks to LODINFO hidden in the attachment of a phishing email, MirrorFace will enable Windows Sandbox in order to hide its activity. They will enable network connectivity to communicate with the command-and-control servers (attacker’s servers) and will establish shared folders with the host. While Windows Sandbox is the core of the tactic used by MirrorFace, they are also using a Visual Studio Code exploit. This IDE is one of the most popular among developers, and this group is using it to manage and execute payload scripts. Executing malicious scripts in trusted environments is also a technique to dissimulate their activities [21].

MirrorFace could be linked to APT10, which is a Chinese state-sponsored cybergroup [26]. Indeed, some tactics and backdoors were considered exclusive to APT10, but we saw

MirrorFace using the same techniques, like the use of the backdoor “ANEL” [27]. But to this day, we don’t have sufficient evidence to make a definitive conclusion.

To counter MirrorFace campaigns, several measures could be taken [20]:

- Raise awareness and train the employees to recognise a phishing email and act accordingly.
- Keep Windows Sandbox disabled by default and limit administrative privileges.
- Put in place networking monitoring to detect unusual traffic.

Cyberattack against FranceTravail

8th March 2024, “France Travail”, the French unemployment platform, has undergone a data breach concerning registered persons on the job-seeker list or those who were on this list in the last 20 years [28]. This represents 43 million persons, almost 63% of the French population [29]. The information concerned by this breach is the first name, last name, social security number, “France Travail” ID, email addresses, postal address and phone numbers [28].

The leak of that personal data could lead to identity theft [30] but also to making large spear phishing campaigns.

Behind this massive data breach, 3 persons were able to find the login of an employee of “Cap Emploi”, which is linked to “France Travail” for disabled people. Once with this login, they asked the support to reset the password while impersonating the employee. With those credentials in hand, they were finally able to access all the sensitive data [31]. The CNIL decided to lead an investigation on France Travail to determine if they put in place enough security measures and if they were appropriate for the respect of the GDPR [28]. We can also wonder if this organisation respected GDPR, particularly on data minimisation and limitation of conservation of data principles. Indeed, they collected large amounts of data about the users that are maybe not useful, and they kept it for a long time (20 years) [32].

Unfortunately, the CNIL hasn’t published yet the report of the investigations but shared their concern as France Travail will soon collect more data which are sensitive (relatives to health) and highly personal (financial data) to better assist all the beneficiaries [33]. CNIL reminds us that they have already little time to secure massive amounts of data, including highly sensitive data, and that they have already undergone a massive data breach recently [33].

In this case, the entry point of the three suspects was the lack of a robust identification system. They were able to impersonate the employee only with his login to change his

password. Different methods are available to implement an identification system. Nilesch A. Lal.al [34] made a review of those authentication methods: passwords, smart cards, biometrics and digital certificates. Each of those have strengths and weaknesses and can be more adapted depending on the information system and the information it contains. Nevertheless, to ensure a strong authentication system, the best practice is to combine 2 or more authentication methods with something we know (passwords, PIN codes, etc.) and something we have or are (physical tokens, biometrics, etc.).

The second flaw that led to this breach is the privileges owned by the targeted employee. Indeed, he had access to the personal data of all the persons registered on France Travail, while he probably didn't need all this information to perform his job. The least privilege principles give to the people the minimal privileges to complete their tasks, even though they can ask for a temporary elevation of privileges to perform certain tasks. The benefit of this principle is it can reduce drastically the surface of attacks. [35]

Sources

- [1] Cybernews, *Ransomlooker Tool*, Cybernews. [Online]. Available: <https://cybernews.com/ransomlooker/>
- [2] S. Schappert., "MetLife claimed by RansomHub, insurance giant says 'no incident'", *Cybernews*, Dec. 31, 2024. [Online]. Available: <https://cybernews.com/news/metlife-latin-america-claimed-by-ransomhub-group/>
- [3] C. Beaman et al., "Ransomware: Recent advances, analysis, challenges and future research directions," *Computers & Security*, vol. 111, Dec. 2021, doi: 10.1016/j.cose.2021.102516.
- [4] A.Alwashali et al., "A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack", *IEEE* Mar. 1, 2022. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9719456>
- [5] CISA, "#StopRansomware: RansomHub Ransomware", CISA Aug. 29, 2024. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
- [6] NIST, "CVE-2023-3519 Detail", NVD Mar. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2023-3519>
- [7] NIST, "CVE-2023-27997 Detail", NVD Mar. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2023-27997>
- [8] NIST, "CVE-2023-46604 Detail", NVD Mar. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2023-46604>

- [9] NIST, "CVE-2023-22515 Detail", NVD Feb. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2023-22515>
- [10] NIST, "CVE-2023-46747 Detail", NVD Apr. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2023-46747>
- [11] NIST, "CVE-2023-48788 Detail", NVD Jan. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2023-48788>
- [12] NIST, "CVE-2023-0144 Detail", NVD Apr. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2017-0144>
- [13] NIST, "CVE-2023-1472Detail", NVD Mar. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2020-1472>
- [14] NIST, "CVE-2023-0787 Detail", NVD Apr. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2020-0787>
- [15] Trend Micro, "Ransomware Spotlight: RansomHub," Dec. 20, 2024. [Online]. Available: <https://www.trendmicro.com/vinfo/gb/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub>
- [16] D. J. Bernstein, "Curve25519: New Diffie-Hellman Speed Records," in *Public Key Cryptography - PKC 2006*, Lecture Notes in Computer Science, vol. 3958, M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, Eds. Springer, 2006, pp. 207–228. [Online]. Available: https://link.springer.com/chapter/10.1007/11745853_14
- [17] R. Moussaileb et al. "Ransomware's Early Mitigation Mechanisms" ACM Digital Library, Aug. 27, 2018. [Online]. Available: <https://dl.acm.org/doi/pdf/10.1145/3230833.3234691>
- [18] Republic World, "200 Breaches & Counting: China's 'Mirror Face' Hackers Now Hunting European Intelligence," Mar. 24, 2025. [Online]. Available: <https://www.republicworld.com/defence/global-defence-news/200-breaches-countingchinas-mirror-face-hackers-now-hunting-european-intelligence>
- [19] Japan Aerospace Exploration Agency (JAXA), "Report on Unauthorized Access at JAXA," July 5, 2024. [Online]. Available: https://global.jaxa.jp/press/2024/07/20240705-2_e.html
- [20] P. Paganini, "China-linked APT group MirrorFace targets Japan," *Security Affairs*, Jan. 10, 2025. [Online]. Available: <https://securityaffairs.com/172890/apt/china-linked-apt-mirrorface-targets-japan.html>
- [21] National Police Agency (NPA), "Alert: Cyberattacks by MirrorFace," Feb. 4, 2025. [Online]. Available: https://www.npa.go.jp/bureau/cyber/pdf/20250204_mf.pdf
- [22] Trend Micro, "Spot the Difference: Earth Kasha's New LODEINFO Campaign and the Correlation Analysis With the APT10 Umbrella," Nov. 19, 2024. [Online]. Available: https://www.trendmicro.com/en_gb/research/24/k/lodeinfo-campaign-of-earth-kasha.html

- [23] NIST, "CVE-2023-28461" Mar. 14, 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2023-28461>
- [24] NIST, "CVE-2023-27997 " Mar. 10, 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2023-27997>
- [25] NIST, "CVE-2023-3519 " Mar. 10, 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2023-3519>
- [26] F. Yuzon, "Military Operations and Law (MILOPS)," July 15, 2019. [Online]. Available: https://stiececmsdusgva001.blob.core.usgovcloudapi.net/public/documents/Bengoshi_Vol_I_V_Issue_I.pdf
- [27] D. Breitenbacher, "Operation AkaiRyū: MirrorFace invites Europe to Expo 2025 and revives ANEL backdoor," *ESET Research*, Mar. 18, 2025. [Online]. Available: <https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/>
- [28] CNIL, "France Travail : la CNIL enquête sur la fuite de données et donne des conseils pour se protéger," Mar. 13, 2024. [Online]. Available: <https://www.cnil.fr/fr/france-travail-la-cnil-enquete-sur-la-fuite-de-donnees-et-donne-des-conseils-pour-se-protger>
- [29] INSEE, "Population au 1er janvier : Données annuelles de 1990 à 2025," Jan. 14, 2025. [Online]. Available: <https://www.insee.fr/fr/statistiques/5225246>
- [30] France Info, "France Travail : 43 millions de fichiers ont été piratés lors d'une cyberattaque," Mar. 14, 2024. [Online]. Available: https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/france-travail-43-millions-de-fichiers-ont-ete-pirates-lors-d-une-cyberattaque_6424123.html
- [31] RTL, "Cyberattaque à France Travail : comment les trois suspects ont réussi à hacker le site," Mar. 20, 2024. [Online]. Available: <https://www.rtl.fr/actu/justice-faits-divers/cyberattaque-a-france-travail-comment-les-trois-suspects-ont-reussi-a-hacker-le-site-7900365714>
- [32] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," May 4, 2016. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434>
- [33] T. Engrand, "Trop d'informations sensibles pas assez protégées : la CNIL s'inquiète de la collecte de données par France Travail," *Le Figaro*, Jan. 14, 2025. [Online]. Available: <https://www.lefigaro.fr/social/trop-d-informations-sensibles-pas-assez-protgees-la-cnil-s-inquiete-de-la-collecte-de-donnees-par-france-travail-20250114>

[34] M. Farik, N. A. Lal, et S. Prasad, "A Review of Authentication Methods," *International Journal of Scientific & Technology Research*, vol. 5, no. 11, pp. 1–10, Nov. 2016. [Online]. Available: https://www.researchgate.net/profile/Mohammed-Farik/publication/311514269_A_Review_Of_Authentication_Methods/links/584fbed808aed95c250b4915/A-Review-Of-Authentication-Methods.pdf

[35] South Asian Academic Research Journal, *An International Multidisciplinary Research Journal*, July 7, 2022. [Online]. Available : <https://saarj.com/wp-content/uploads/special-issue/2022/ACADEMICIA-JULY-2022-SPECIAL-ISSUE.pdf>

Task 2 : Pentest report on the infrastructure of Cureton Pharmaceutical Company

Introduction

The pentest was conducted with the goal to detect potential vulnerabilities, misconfigurations and security weaknesses within CPC's infrastructure and website. To achieve these objectives, we simulated real attack scenarios to assess the resilience of the systems. This report outlines all the methodologies, tools and techniques used to perform the pentest and will also bring recommendations and solutions to improve security and patch vulnerabilities.

List of Figures

Figure 1 - CPC's critical infrastructure	12
Figure 2 - Port Security configuration.....	15
Figure 3 - Recommended CPC's infrastructure.....	21
Figure 4 - Gantt Diagram for the implementation of the solution	24

List of Tables

Table 1 - Recommended solution for each vulnerability and security weaknesses.....	18
Table 2 - Cost and duration to implement security patches proposed in Table 1.....	23
Table 3 - Cost of the hardware to securise the infrastructure	23
Table 4 - Cost of the implementation of the hardwares in the network.....	23
Table 5 - Cost and duration of pentesters' work	24

List of Acronyms

- ACL : Access Control List
- CPC : Cureton Pharmaceutical Company
- DHCP : Dynamic Host Configuration Protocol
- DNS : Domain Name System
- FTP : File Transfer Protocol
- FTPS : File Transfer Protocol over SSL/TLS

- HDD : Hard Disk Drive
- IDS : Intrusion Detection System
- IPS : Intrusion Prevention System
- RAM : Random Access Memory
- SFTP : Secure File Transfer Protocol
- SQL : Structured Query Language
- SUID : Set owner User ID
- TCP : Transmission Control Protocol
- UDP : User Datagram Protocol
- VLAN : Virtual LAN
- XSS : Cross-Site Scripting

Contingency Policy

During penetration testing, some incidents may occur even though all the efforts are made to minimise the risk of disruption of services. The pentesting operations will be performed on a replica of CPC's internal infrastructure; the risk of exposure to sensitive data and disruption of services is low. In the case such incidents happen, escalation procedures are in place to contact immediately stakeholders. Backups and recovery mechanisms must be managed by the client.

If a critical vulnerability is found during the pentest, we are committed to informing the stakeholders immediately.

We will provide, at the end of the report, a list of modifications to do in order to patch the vulnerabilities. These are recommendations, and you are free to apply them or not, but we cannot be put liable if an incident occurs where the vulnerabilities found are exploited.

Penetration Testing Framework and Tools

To conduct this pentest on CPC's infrastructure, we used the Mitre Att&ck Framework [1], which allows us to perform a complete and comprehensive pentest. This framework covers all the principal areas, such as reconnaissance, initial access, persistence, privilege escalation, ...

The tools used to perform this pentest are :

- Nmap : Tool for network discovery. It can detect open ports, services running and operating systems.
- Hydra : Login cracker by brute force. Supports a large variety of protocols.
- Metasploit: A pentesting tool helping with the exploitation of vulnerabilities.
- Social Engineering Toolkit: Create multiple believable social engineering attacks using different vectors.
- BurpSuite: Intercepts requests, allowing us to modify them and automate the attacks.
- Sqlmap : SQL injection scanner for web applications.
- Gobuster : Directory discovery for web applications by brute force.
- Netcat : Opens network connections in UDP or TCP.
- Hashcat : Password cracker.

In order to avoid any disruption in services, we created a copy of the critical infrastructure represented by this schema:

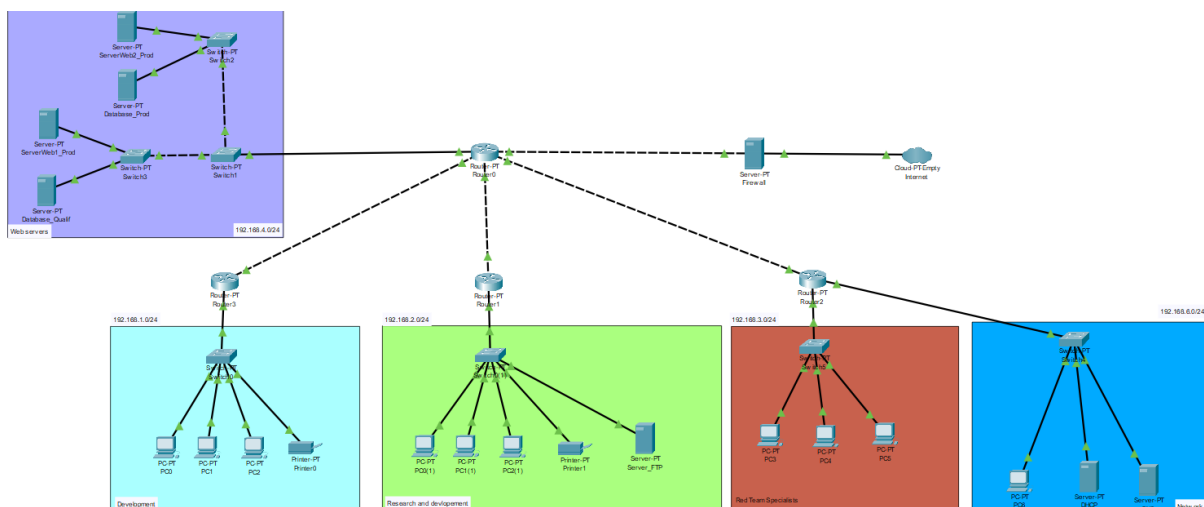


Figure 1 - CPC's critical infrastructure

Design Flaws

Based on the topological network plan provided, we can notice that there is only one firewall separating the internal network and the Internet. Ideally internal firewalls should be present in order to restrict traffic between zones. ACLs and VLANs can be put in place to achieve this goal.

Furthermore, for the web servers, the development and production are located in the same network. Test traffic and production traffic follow the same route, which could lead to a potential leak of sensitive data.

The FTP server, which is used to store all the sensitive data, is vulnerable. SFTP or FTPS should be used instead.

Lastly, in this topology there is no IDS/IPS or logging infrastructure like a SYSLOG server.

Attacks conducted

First of all, we will perform a general enumeration with « `nmap -sV -p- <network>` » for each network of the company. This will allow us to list the active hosts on the network and enumerate open ports and services associated.

To have further information about the firewall, we will execute the command « `nmap --script=firewalk --traceroute <host ip>` ». This command will allow us to see the firewalls on the route leading to the host and what the blocked ports are.

FTP - Credentials brute force

We know that there is an FTP server in the network. We can try to bruteforce usernames and passwords to gain access. We will use the command « `hydra -L /usr/share/wordlist/usernames.txt -P /usr/share/wordlist/rockyou.txt ftp://<IP of the FTP Server>` »

No login attempts were successful. This means that all the employees having an FTP account didn't use a too "easy" password to guess.

FTP - Anonymous access

The Metasploit module “auxiliary/scanner/ftp/anonymous” will help us determine if the FTP server allows anonymous access and determine the permissions. The output showed that anonymous access was disabled, which prevents anyone from accessing all the sensitive files.

FTP - VSFTP backdoor

On the nmap scan, we saw on the FTP server the service “vsftp 2.3.4” running. According to the CVE-2011-2523 [2], this version of vsftp contains a backdoor which opens a shell on port 6200. We can exploit this vulnerability thanks to Metasploit and the module “exploit/unix/ftp/vstpd_234_backdoor”. After configuring the target IP and the target port in the options, we can launch the exploit to gain root access on the server.

FTP - FTP Admin 0.1.0

FTP Admin is an administration tool often used with vsftp. This tool is used to modify users or generate users’ passwords. The version 0.1.0 is vulnerable to Cross-Site Scripting (CVE-2007-6232 [3]) via the “error” parameter in the URL. With this vulnerability we can execute arbitrary JavaScript code. We can also exploit the “page” parameter and insert the name of the file we are interested in [4].

FTP - SUID files

On Linux, we can find SUID permission on certain files. It means that the user could execute it with root permission. We can leverage those permissions on some executable to gain root access. To find all the files with SUID permissions, we will use the command :

```
find / -perm -u=s -type f 2>/dev/null
```

We notice that cat has SUID permissions ; we can read every file on the system [5].

DHCP - Spoofing

An attacker in the internal network could intercept the DHCP Discover and Request messages and answers to those requests by impersonating a DHCP server. The goal of the attacker is to replace the default gateway IP address with its own IP. With this technique called “man in the middle”, the attacker will be able to intercept all the traffic and forward it to the real gateway.

Here, in this network, the DHCP server needs to provide IP addresses to several sub-networks. The option 82, also known as the DHCP relay agent information, must be activated on the routers. Its role is to redirect all the DHCP requests towards the DHCP server. The activation of this option can make it harder for an attacker to perform DHCP Spoofing, but to mitigate this attack, DHCP Snooping must be activated on the switches. DHCP Snooping will block all the DHCP offers coming from “untrusted” ports, which are the ports where a user can be connected.

In the schema below, the trusted ports are marked with blue dots and untrusted ports with orange dots.

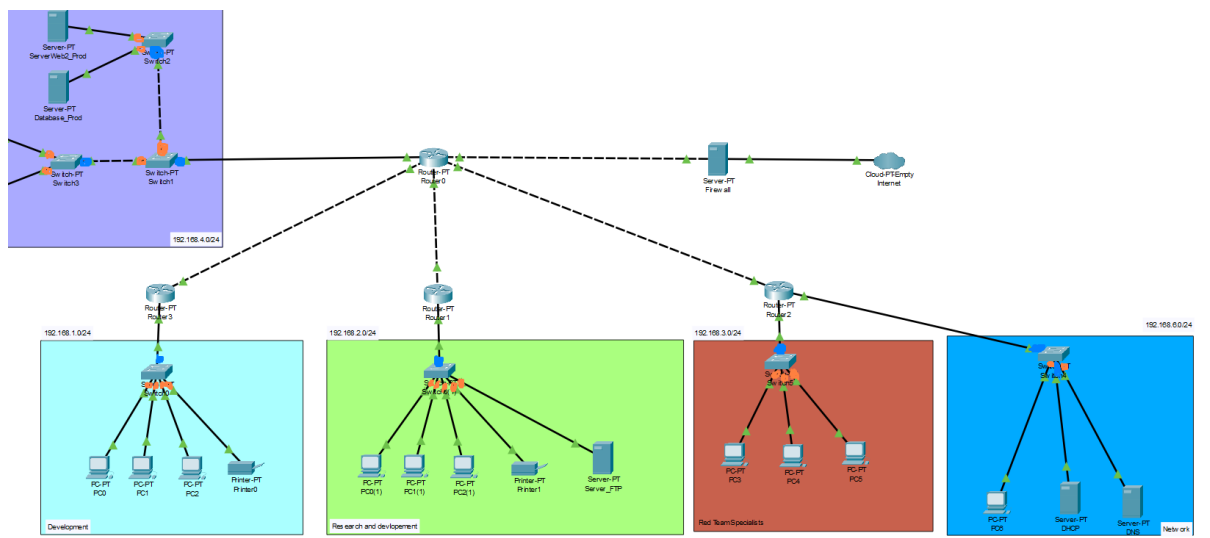


Figure 2 - Port Security configuration

DHCP - Starvation

In order to paralyse the network, an attacker could flood the DHCP server with DHCP requests using spoofed MAC addresses to empty the pool of IP addresses. As a result, the legitimate users would be unable to obtain an IP address.

To mitigate this attack, we could configure port security on switches to limit the number of source MACs allowed on a port. If the limit is exceeded, the port will shut down until the administrator performs the “no shut” command.

DNS - Spoofing

Thanks to the Nmap scan, we know that Telnet is listening on port 23. This unsecured protocol can be used to connect remotely to the server and modify the DNS entry. In order to

log on to the DNS server, we will use the Metasploit module “auxiliary/scanner/telnet/telnet_login” to brute force credentials and try to connect with Telnet. In order to run this module, we need to configure the IP of the DNS and the wordlists for the usernames and the password.

We were able to connect to the DNS server with the credentials admin/dns1234. With now all the access to the configuration files, we can add a static entry pointing to an IP we own and link to a domain name often used, like Gmail or Facebook. We can clone one of these websites thanks to the Social-Engineering Toolkit.

Once the users try to go on the website, the forged one will load, and the attacker will be able to retrieve their credentials.

Web - Apache vulnerability

In the Nmap scan, we saw that the Apache version was 2.4.50. For this version, we found 2 vulnerabilities documented (CVE-2021-44790 [6] and CVE-2021-44224 [7]). The first one is the possibility to cause a buffer overflow in the mod_lua parser. This extension allows the addition of Lua scripts for multiple purposes (authentication, authorisation, access control, ...) [8]. The second vulnerability can be used to perform server-side request forgery or DoS if the proxy is not well configured. Once again, this vulnerability can be exploited only if the mod_proxy is activated, which it is not, because there is only 1 web server. Even though the 2 vulnerabilities concerning this Apache version can't be applied on this server, it is best practice to upgrade to the latest version to receive all the security patches.

Web - SQL Injection

Thanks to SQL injection, it is possible to gain unauthorised access. On the connection form of the CPC website, we can try to enter some credentials. We don't see the login or the password in the URL, so we know that POST requests are used. We also notice that the website indicated an error: “Invalid username”. This error can be useful to determine if the user exists or not. Using Burpsuite, we can intercept the POST request, send it to Repeater to automate the sending of the connection request and modify each time the username by an entry we configure in Burpsuite. For the user “Admin”, we notice that now the error is “Invalid password”, so we can deduce that “Admin” is a valid user. To test the SQL injection with this username, we will save the POST request sent in a file. To test if SQL injections are possible, we will use sqlmap : « `sqlmap -r post_request.txt -p Pass` » where “Pass” is the name of the parameter in the request containing the password.

Sqlmap found a “time delays SQL injection”. It means that we can test a boolean condition and trigger a time delay if the condition is true. With this technique, we could enumerate each letter of the wanted information (name of the database, passwords, ...).

To validate the sqlmap finding, we will insert in the password field of the form : ‘ SELECT IF (1=1, SLEEP(10),’a’)

The page loaded for 10 seconds before displaying the error. The website is vulnerable to time-based SQL injections. Even though this type of SQL injection is complicated to exploit, all the information contained in the database could be extracted.

Web - XSS

On the website, there is a form to contact the company. To test if this form is vulnerable to cross-site scripting, we can enter in the field : `<script> alert("Hello") </script>`. Once the form is validated, we see a pop-up saying “Hello”. This confirms that the website is vulnerable to XSS attacks. We could, for example, steal the cookie of the administrators of the website or at least the users that receive the contact forms. It can be achieved with something like : `[?cookie=document.cookie]>` The “onerror” will be executed because the source of the image will not be found, the website will redirect towards our interceptor and will include the cookie.

Web - File Upload

In the “Profile” section, it is possible to upload a profile picture. The website asks for a PNG or a JPG, and all the other extensions are rejected. By looking at the JavaScript file, we know that the verifications are based on the extensions and the magic numbers (the first byte in a file used to identify the type of file). At the same time we execute : « `gobuster dir -u <URL> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt` » to enumerate the directories. We also used the web extension Wappalyzer to determine that the website is using Javascript as a back end. In the output of the Gobuster command, we see the directory ‘content/profile_pictures’. We can access it directly in the browser, so there is a directory indexing vulnerability. We can notice that all the pictures have the name “image” followed by a number going from 1 to 485.

We will try to gain access to the web webserver from the website with a reverse shell. First of all, we will reload the page while the “Intercept” mode of BurpSuite is on to catch the answer and delete the link toward the JavaScript file. Then, we can use the code to create a reverse shell on the Floppywiggler GitHub repository [9] and upload it as a profile picture. The upload was successful; there were no filters on server side. Before executing the code we sent to the server, we need to set up a listener with netcat : « `nc -lvp <port>` ». We can now access the “content/profile_pictures” and find the “image486” file and click on it. On the listener, we saw that we obtained a shell, and we can navigate through the server.

MySQL - Access to database

To access the database, we will use Metasploit's module "auxiliary/scanner/mysql/mysql_login" to brute force the credentials. We found that the credentials "debian-sys-maint" and "FcT5YjU6LunnuHZD" worked. This is the default credentials for MySQL on Linux servers. With that access, we can extract all the data, but we also could modify or delete it.

MySQL - Passwords

The passwords in the database are hashed with Bcrypt (recognisable with the "\$2y\$" suffix). Those hashes are salted, which makes them more resistant against rainbow table attacks.

However, we can try to crack them using Hashcat: `hashcat -m 3200 -a 0 password_hashes.txt /usr/share/wordlists/rockyou.txt -r OneRuleToRuleThemAll.rule`

Thanks to Hashcat, we were able to retrieve 20% of the passwords. Some of them had fewer than 8 characters and didn't have at least one number or special character.

Recommended Solutions

Based on what we found, you will need to make modifications to your infrastructure, software and configurations to protect your data. You will find in the table below the list of the vulnerabilities discovered, their criticality and the solution proposed. The criticality is calculated for each vulnerability depending on the likelihood and the effects of the exploit.

Table 1 - Recommended solution for each vulnerability and security weaknesses

Vulnerability	Criticality	Solution
CVE-2011-2523 : Possibility to exploit a backdoor and obtain a shell. Concerning vsftpd 2.3.4 on the FTP server	Very High	Upgrade vsftpd to the latest stable version which is 3.0.3

Vulnerability	Criticality	Solution
CVE-2007-6232 : Cross-site scripting vulnerability found on FTP Admin 0.1.0	Medium	Change for another administration tool. FTP Admin is not maintained anymore. An alternative could be adminvsftpd.
Files with SUID permissions could be use for privilege escalation.	High	Limit the number of files with the SUID permissions.
DHCP Spoofing : an attacker could impersonate a DHCP server, responding to DHCP request and perform a Man-in-the-middle attack. All the traffic would be sent to him before forwarding it to the real gateway.	Medium	Configure DHCP Snooping on the switches.
DHCP Starvation : An attacker could empty the pool of IP address available in the DHCP, resulting in paralyzing the network	High	Configure port security on the switches.
Insecure credentials on the DNS server	Very High	Implement a strong password policy
CVE-2021-44790 : Possibility to exploit a buffer overflow in the mod_lua parser for apache 2.4.50	Low	Upgrade Apache to the latest stable release which is 2.4.63
CVE-2021-44224 : Possibility to cause a DoS or to perform a Server-Side Request Forgery if the proxy is not well configured for apache 2.4.50	Low	Upgrade Apache to the latest stable release which is 2.4.63
Time-based SQL Injection found in the login form. Possibility to extract all the information from the database even though it is unlikely because of the difficulty to exploit.	High	Always sanitize users entries and use prepared queries.
The errors on the website give too much information. The attacker can know for example if the username exists and try to bruteforce the password	Low	Use generic errors and try to give the least information possible.

Vulnerability	Criticality	Solution
Cross-site-scripting is possible in the contact form of the website. It allows the attacker to execute scripts	Very High	Sanitize user entries.
Directory indexing : It is possible to see all the files of the directories in the browser	High	Configure the .htaccess file and add the line "Options - Indexes" to disable it.
Malicious files upload : It is possible to bypass the filters and send on the server other files than png or jpg	Very High	Add filters and verification also in the backend.
Default credentials on the MySQL server	Very High	Modify the password of the default user.
No password policy when an account is created on the website	High	Create a strong password policy when a user wants to create an account : At least 12 characters, one number and one special character

Recommendation for improving infrastructure security

As it is, the only protection is the firewall filtering the traffic between the internal and the external network. Internal networks should also be filtered to avoid the compromise of all the network if one PC gets infected, for example. Internal firewalls and ACLs can perform this task. In case of attack or incident, a logging system (represented below by the SYSLOG server) could be very useful to backtrack the attacker and evaluate the area affected. Rsyslog could be a good solution for CPC, as it is light and can support numerous log sources, transform them and generate multiple formats to read and analyse the logs (files, MySQL, Elasticsearch, etc.).

Finally, adding IPS is recommended to detect and prevent attacks. They can detect network scans and bruteforce attempts and block the IP who is responsible. No additional hardware will be necessary for IPS, as they can be embedded in firewalls. We recommend installing IPS

in the firewalls protecting sensitive data : the firewall protecting the web servers, the firewall protecting the FTP server and the firewall filtering external networks.

You will find below a schema of a more secure infrastructure based on existing.

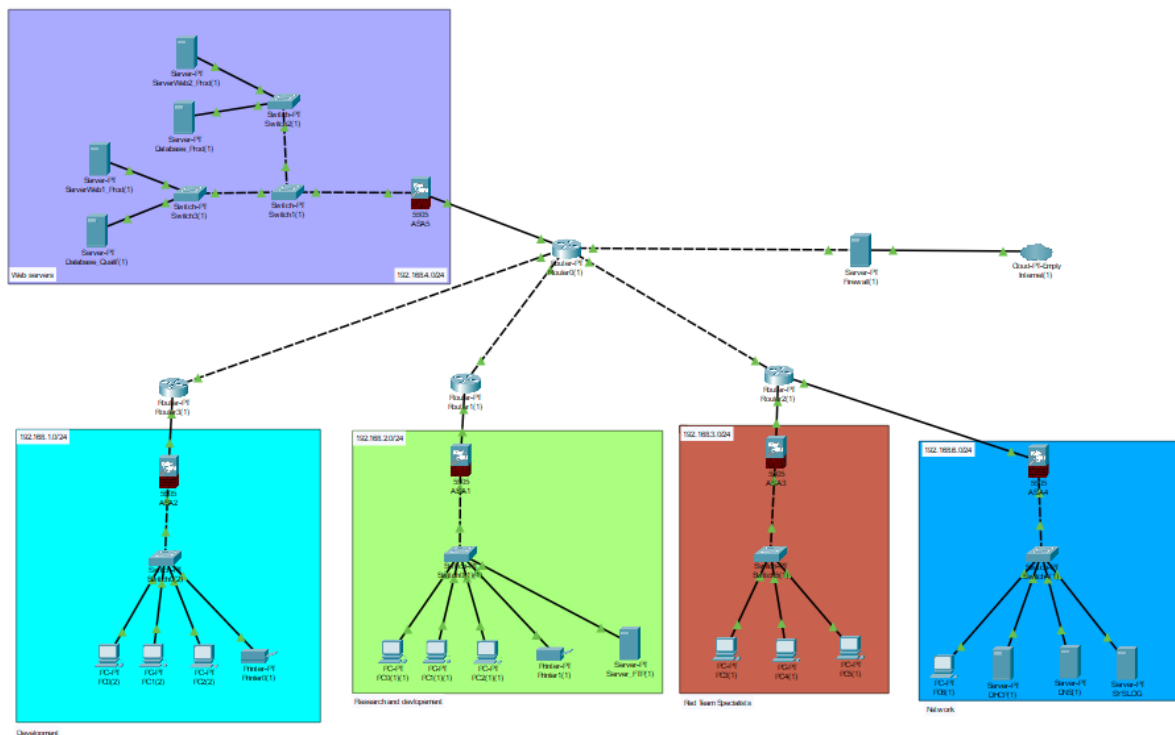


Figure 3 - Recommended CPC's infrastructure

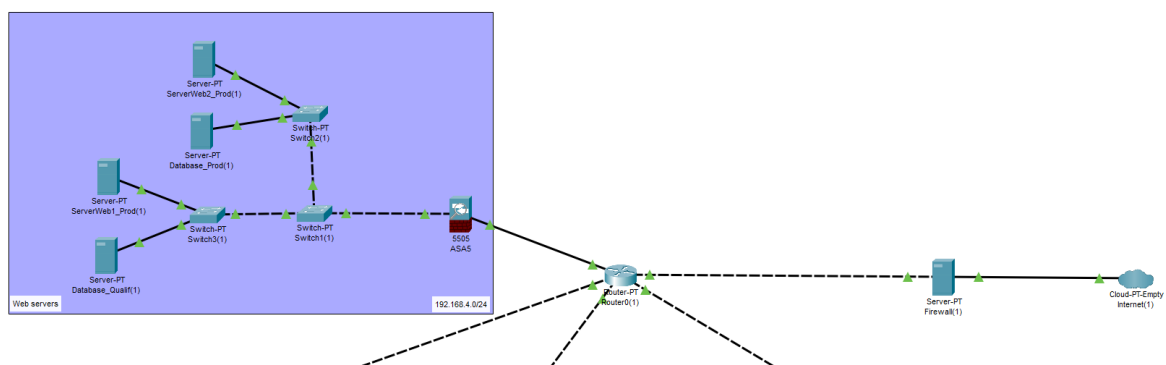


Figure 3.1 - Focus on web servers

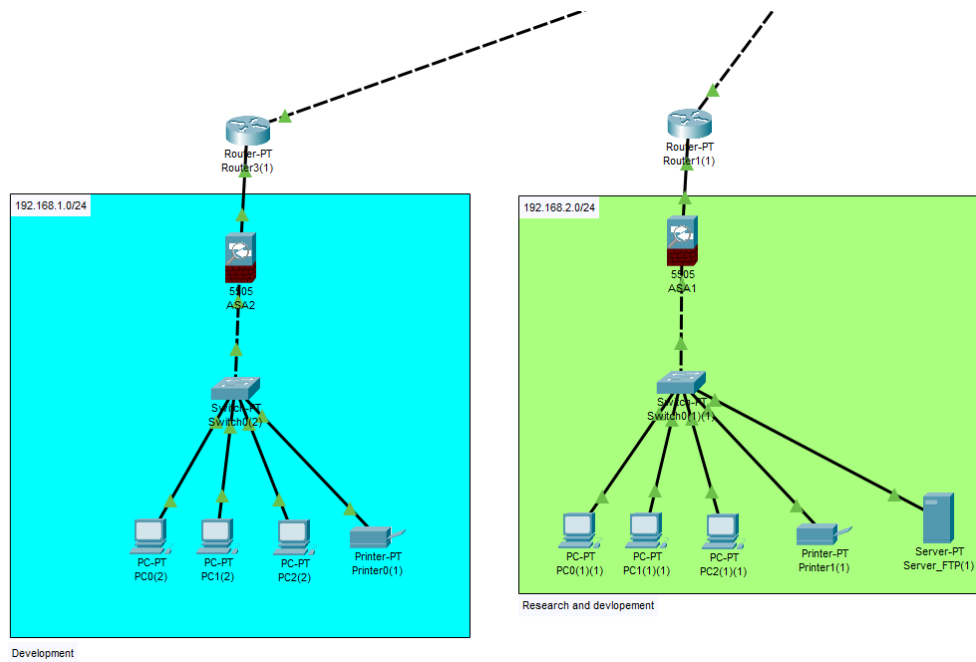


Figure 3.2 - Focus on Development and R&D

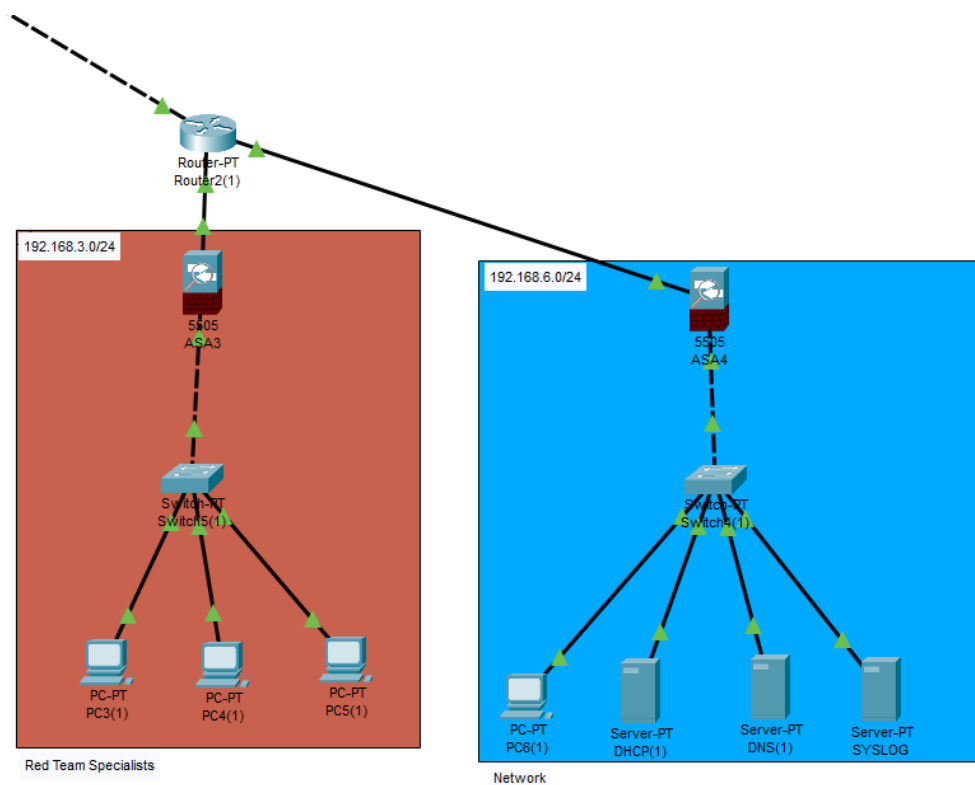


Figure 3.3 - Focus on RedTeam and Network team

Cost of Solution

To implement all the modifications, CPC will need a system administrator and a developer. We assume that one day of work is equivalent to seven hours [10][11].

Table 2 - Cost and duration to implement security patches proposed in Table 1

Profession	Hourly Rate	Days of works	Total
System Administrator	£20	9	£1260
Developer	£23	2	£322

To change the infrastructure, you will need five firewalls [12] and one server [13] and eight hard drives [14] for the server. A network technician [15] will be necessary to install the hardware and a system administrator [10] to configure them.

Table 3 - Cost of the hardware to securise the infrastructure

Hardware	Cost	Number	Total
Fortinet Fortigate 40F	£596,65	5	£2983,25
Server HP DL380 GEN10 8SFF	£885,73	1	£885,73
HPE Enterprise - hard drive - 2.4 To - SAS 12Gb/s	£732,24	8	£5857,92

Table 4 - Cost of the implementation of the hardwares in the network

Profession	Hourly Rate	Days of works	Total
System Administrator	£20	6	£840
Network technician	£16	1	£112

In total, to realize all the modification recommended, CPC will have to pay : **£12 260,90**

Timetable

You will find below the timetable proposed to implement the solution :

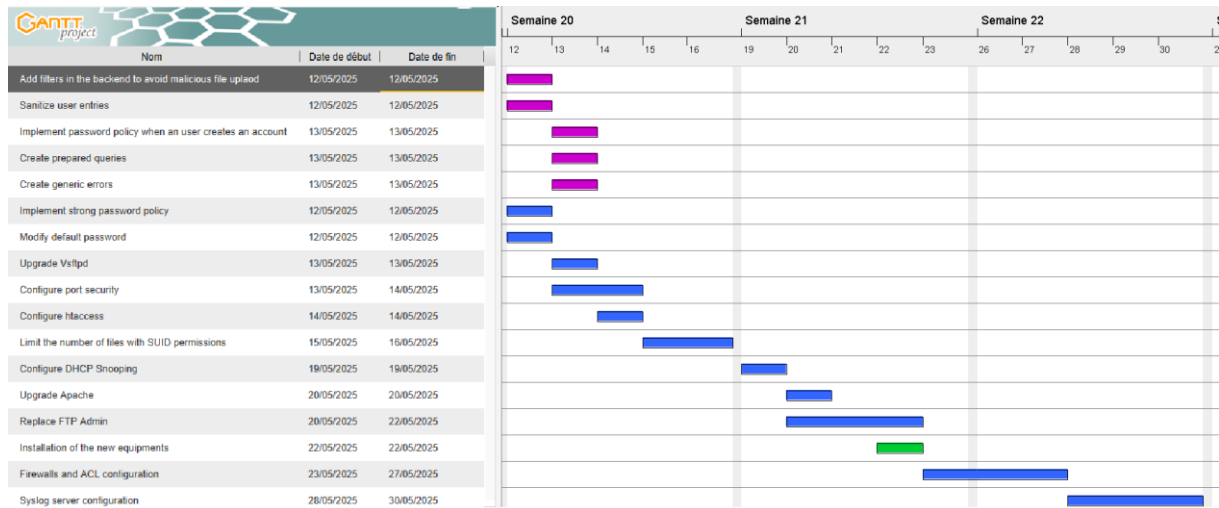


Figure 4 - Gantt Diagram for the implementation of the solution

Invoice for the prestation

To conclude this pentest and redact the report, we took 1 month as a team of three. Our team is composed of one junior pentester [16] and two senior pentesters [17].

Table 5 - Cost and duration of pentesters' work

Profession	Hourly rate	Days of work	Total
Pentester Junior	£18	25	£3150
Pentester Senior	£36	25	£6300
Pentester Senior	£36	25	£6300

In total, this pentest cost to CPC £15 750.

References

- [1] MITRE, "MITRE ATT&CK®" [Online]. Available: <https://attack.mitre.org>
- [2] NIST, "CVE-2011-2523 Detail", NVD Nov. 2024. [Online]. Available: <https://nvd.nist.gov/vuln/detail/cve-2011-2523>
- [3] NIST, "CVE-2007-6232 Detail", NVD Apr. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2007-6232>
- [4] OMNI, "ftp Admin 0.1.0 - Local File Inclusion / Cross-Site Scripting / Authentication Bypass," Exploit Database, EDB-ID: 4681, Nov. 2007. Available: <https://www.exploit-db.com/exploits/4681>
- [5] E. Pinna and A. Cardaci, "cat," GTF0Bins. Available: <https://gtfobins.github.io/gtfobins/cat/>
- [6] NIST, "CVE-2021-44790 Detail", NVD May. 2025. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2021-44790>
- [7] NIST, "CVE-2021-44224 Detail", NVD Nov. 2024. [Online]. Available : <https://nvd.nist.gov/vuln/detail/CVE-2021-44224>
- [8] The Apache Software Foundation, "mod_lua - Apache HTTP Server Version 2.5," Apache HTTP Server Documentation. Available: https://httpd.apache.org/docs/trunk/mod/mod_lua.html
- [9] floppywiggler, "reverse-shell.js," GitHub, 2025. Available: <https://github.com/floppywiggler/javascript-reverse-shell/blob/master/reverse-shell.js>
- [10] Talent, "System Administrator average salary in United Kingdom, 2025." Available: <https://uk.talent.com/salary?job=system+administrator>
- [11] Talent, "Developer average salary in United Kingdom, 2025." Available: <https://uk.talent.com/salary?job=developer>
- [12] LDLC, "Fortinet FortiGate 40F (FG-40F)", LDLC. Available: <https://www.ldlc.pro/fiche/PB00405073.html>
- [13] Servermall, « Serveur HPE ProLiant DL380 Gen10 », Servermall. Available: <https://servermall.com/fr/catalog/servers/server-hpe-proliant-dl380-gen10/>
- [14] Inmac Wstore, « HPE Enterprise - disque dur - 2.4 To - SAS 12Gb/s », Inmac Wstore. Available: <https://www.inmac-wstore.com/hpe-enterprise-disque-dur-2-4-to-sas-12gb-s/p7258263.htm>.

[15] Talent, "Network Technician average salary in United Kingdom, 2025." Available:
<https://uk.talent.com/salary?job=network+technician>

[16] Talent, "Pentester Junior average salary in United Kingdom, 2025." Available:
<https://uk.talent.com/salary?job=penetration+tester+junior>

[17] Talent, "Pentester Senior average salary in United Kingdom, 2025." Available:
<https://uk.talent.com/salary?job=penetration+tester+senior>