



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA7033 Ethical Hacking Assessment

**Research into cyber security attacks and
Penetration testing for a virtualised
simulated company website**

Author:

Quentin LAURENT

Lecturer:

Assoc. Professor Carlene Campbell

May 6, 2025

Table of contents

Abstract.....	3
Introduction	3
1. Analysis of three recent cyberattacks	4
1.1. Change Healthcare breach (2024).....	4
1.1.1. Overview and analysis.....	4
1.1.2. Attack details and identified security flaws.....	5
1.1.3. Recommendations to prevent future attacks	6
1.2. LastPass Data Breaches (2022).....	7
1.2.1. Overview and analysis.....	7
1.2.2. Attack details and identified security flaws.....	8
1.2.3. Recommendations to prevent future attacks	9
1.3. SolarWinds Supply Chain Attack (2020)	10
1.3.1. Overview and analysis.....	10
1.3.2. Attack details and identified security flaws.....	11
1.3.3. Recommendations to prevent future attacks	12
2. Designing a server infrastructure and simulating an attack against it	14
2.1. Contingency policy	14
2.2. Chosen penetration testing framework and penetration testing tools	15
2.3. Overview of Cureton Pharmaceutical Company's (CPC) critical server infrastructure	15
2.4. Detailed walkthrough of the simulated attack.....	18
2.4.1. Initial reconnaissance and scanning.....	19
2.4.2. Accessing CPC's staging website server via a Remote Code Execution (RCE)	20
2.4.3. Privilege escalation on the server running CPC's staging website	22
2.4.4. Accessing the production database by inspecting the users bash histories	23
2.5. Attack simulation results and summary	25
2.6. Remediation summary	25
2.6.1. Execution timetable	25
2.6.2. Total cost	27
3. Conclusion.....	28
4. Table of figures.....	28
5. References.....	29

Abstract

This document presents a comprehensive analysis of contemporary cybersecurity challenges through two distinct yet interconnected topics. The first part of this document examines and analyses three recent cyberattacks that targeted large companies and government agencies, detailing the root cause of each attack, its impacts as well as the remediation measures that should be put in place in order to prevent these from happening in the future.

The second part of this document transitions to a practical simulation of an attack against a deliberately insecure enterprise network infrastructure. The simulated penetration test identifies security flaws and oversights, demonstrates how they can be exploited from a technical point of view and proposes various remediation actions to be taken to strengthen the security of the infrastructure.

The findings of this document emphasize the importance of proactive security assessments and the need for continuous implementation of security controls to protect against increasingly sophisticated threats.

Introduction

The evolving landscape of cyber security threats necessitates a comprehensive understanding of real-world attacks and underlying vulnerabilities. This document addresses this need through a two-part analysis.

The first part focuses on analysing three recent cyberattacks that have specifically targeted large companies and government agencies. Each attack is presented in a way that allows us to understand its magnitude. Moreover, we also dive into the details of the root cause of each attack (when available) to get a better understanding of the specific flaws that were exploited. Finally, recommendations are made to prevent such attacks from happening in the future.

The second part of this document designs a purposefully vulnerable enterprise infrastructure through a practical example and simulates an attack against that infrastructure by leveraging multiple flaws found in its design and its configuration. The attack is explained in technical details to get a better understanding of the underlying flaws as well as to provide technical details on how to remediate uncovered weaknesses. An estimated cost is also established in order to implement a secure infrastructure that would not have been impacted by the simulated attack.

The objective of this document is to bridge theoretical knowledge with a practical application, providing insights into enhancing organizational cybersecurity practices.

1. Analysis of three recent cyberattacks

1.1. Change Healthcare breach (2024)

1.1.1. Overview and analysis

Change Healthcare is a subsidiary of UnitedHealth Group Incorporated, an American company specializing in health insurance. Change Healthcare primarily acts as a payment processor that connects payers, providers, and patients within the U.S. healthcare system. It is estimated that Change Healthcare “processes approximately half of all medical claims in the United States for around 900 000 physicians, 67 000 pharmacies, 5500 hospitals and 600 laboratories” [5].

On February 21, 2024, Change Healthcare detected that ransomware was being deployed in its internal computer infrastructure, leaving the latter in an unusable condition. As a result, Change Healthcare decided to shut down most of the systems in order to prevent the attack from spreading further [1].

Following an internal investigation conducted by Change Healthcare’s security team and assisted by external investigators, it was confirmed on March 7, 2024, that a large quantity of data was exfiltrated from Change Healthcare’s internal infrastructure between February 17, 2024 and February 20, 2024 [1]. This implies that prior to the initial detection of the intrusion in their systems on February 21, 2024, Change Healthcare was not aware of such activity. This legitimately raises questions regarding the ability of the company to monitor the confidentiality of their systems.

Although specific details have not been released nor confirmed officially by Change Healthcare, it was reported by multiple news sources that the volume of stolen data is around 6TB¹ and affects roughly one third of the American population [2, 3].

Following the attack, Change Healthcare decided to pay a ransom of \$22 million in Bitcoin to the attacker, as confirmed by UnitedHealth Group CEO² Andrew Witty in a hearing conducted by the Oversight and Investigations Subcommittee of the House Committee on Energy and Commerce of the United States [4].

Although ransomware-based attacks are quite common, the nature of the target spread outrage considering that a substantial amount of sensitive (medical) data was exfiltrated from Change Healthcare’s systems. Moreover, due to the fact that Change Healthcare had to shut its systems down (and due to the ransomware itself making the systems unavailable), the entire payment processing chain managed by the company was put out of order, impacting millions of people that depend on it.

¹ Terabytes

² Chief Executive Officer

According to a survey done by the American Medical Association (published on April 29, 2024) [21]:

- 60% of physician practices faced challenges in verifying patient eligibility
- 75% faced barriers with claim submission
- 79% could not receive electronic remittance advice
- 85% experienced disruptions in claim payments
- 80% lost revenue from the inability to submit claims
- An overwhelming 91% have had to commit additional staff time and resources to complete revenue cycle tasks

1.1.2. Attack details and identified security flaws

Although specific details have not been revealed by Change Healthcare, it was confirmed by UnitedHealth Group CEO Andrew Witty in a testimony published before a hearing conducted by the American House Committee on Energy and Commerce that “on February 12, 2024, criminals used compromised credentials to remotely access a Change Healthcare Citrix portal, [...]. Once the threat actor gained access, they moved laterally within the systems in more sophisticated ways and exfiltrated data. Ransomware was deployed nine days later” [6].

The critical part to note here is that the Citrix portal that was remotely accessed by threat actors offered the possibility to the user to initiate remote access to desktops located inside Change Healthcare’s infrastructure. The key weakness that was outlined during the investigations is that, according to CEO Andre Willy’s testimony, “The portal did not have multi-factor authentication”, which means that, once in possession of the credentials, the threat actor could effectively infiltrate Change Healthcare’s internal infrastructure.

By looking at the different dates, it appears that the attackers were able to navigate inside Change Healthcare’s systems for nine days before being detected, during which they have successfully exfiltrated data and launched a ransomware attack.

Because of the lack of publicly available information on the “lateral movements” made by the attackers while inside Change Healthcare’s systems, it is not possible to pinpoint the exact vulnerabilities and security oversights that allowed the exfiltration of a large quantity of sensitive data. However, we can note two major flaws that allowed the attack to occur in the first place:

- The lack of Multi Factor Authentication (MFA) on the Citrix instance that the attackers logged into using stolen credentials
- The lack of monitoring inside Change Healthcare’s systems which allowed the threat actors to operate undetected for nine days

1.1.3. Recommendations to prevent future attacks

From the information exhibited in the previous part, we can make several recommendations to prevent such an attack from occurring in the future.

First, by strengthening the authentication on systems that have access to critical parts of Change Healthcare's infrastructure, such as the Citrix instance that was accessed by the attackers. Several options are available to reinforce the authentication on critical systems:

- Applying a strict and strong password policy, by setting minimal length requirements (e.g. a minimum of 20 characters with the use of lowercase and uppercase letters, numbers and special characters), prohibiting the reuse of identical passwords between different systems. The use of randomly generated passwords should be heavily encouraged.
- Implementing a password rotation policy, based on the criticality of the system (e.g. forcing passwords to be changed every 6 or 12 months)
- Enforcing Multi Factor Authentication (MFA) for all user accounts on critical systems. Nowadays, MFA offers more secure options than SMS-based One-Time Passwords (OTPs) such as authenticator mobile applications that use biometrics or face recognition

Secondly, by implementing a robust monitoring system that would allow the detection of suspicious behaviour inside Change Healthcare's critical infrastructure. More specifically, it appears critical to strictly monitor access to sensitive data on databases considering the sensitive nature of the data stored and managed by Change Healthcare.

1.2. LastPass Data Breaches (2022)

1.2.1. Overview and analysis

LastPass is a company that provides password management as a service. As such, LastPass develops and maintains a web application accessible by users and develops and distributes web browsers plugins and mobile applications that integrate with their web service. The core service of LastPass allows users to store their usernames and passwords for different services on a centralized encrypted vault that is maintained by LastPass.

Before analysing the attack, it is important to note that, at the time of the incident, LastPass only did encrypt usernames and passwords for each service, and did not encrypt other metadata such as the service name, the service URL (if it is a website), etc. Encrypted data stored and managed by LastPass is encrypted using a “master password” created and only known by the LastPass user.

In August 2022, LastPass CEO Karim Toubba published a notice informing users that an unauthorized party gained access to LastPass development environment and exfiltrated portions of their source code as well as other proprietary information. It was also indicated that LastPass was still operating as usual.

On December 22, 2022, LastPass releases a notice with updates on that prior security incident [17] stating that the security breach that occurred in August 2022 was more severe than it initially appeared to be. It was revealed by LastPass that credentials allowing to access and decrypt storage volumes stored on cloud-based storages services were stolen. As a result, the unauthorized third party was able to exfiltrate and decrypt volumes containing “basic customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service”. Moreover, the threat actor also managed to exfiltrate a backup of customer vault data which contains a mix of encrypted and unencrypted data (as described previously).

While LastPass clearly states that extremely sensitive data, such as usernames and passwords used by users for their different services, are fully encrypted with 256-bit AES³ encryption, it is important to note that the safety of users’ data is dependent on the strength of the “master password” they used when creating their storage vault. As a result, LastPass clearly explained what distinguishes a weak password from a strong password and encouraged customers who used a weak master password to immediately change their stored passwords as those would be at risk of being decrypted.

It can also be noted that, since 2018, LastPass enforces a minimum password length policy of 12 characters to its customers, which reduces the risk of user data being decrypted in such attacks.

³ Advanced Encryption Standard

1.2.2. Attack details and identified security flaws

On March 1, 2023, LastPass published an additional document detailing the breach that occurred in 2022 [18]. In this document, LastPass differentiates two incidents:

- The initial August 2022 incident
- A second incident spanning from August 12, 2022, to October 26, 2022

According to LastPass, the threat actor leveraged information acquired during the first incident to launch a second attack on the course of several months where most of the data was exfiltrated. The notice published in December 2022 did not differentiate between both incidents as LastPass did not yet grasp the perspective of the attack.

Reading through the investigation report published by LastPass, it appears that this attack was not the result of a usual mistake such as the use of a weak password or the stealing of credentials through social engineering. In fact, according to LastPass, the threat actor was able to obtain valid credentials to the cloud storage environment by specifically targeting one of the four DevOps engineers that had access to said storage.

Additionally, it is indicated that the threat actor specifically targeted the home computer of the DevOps engineer and exploited a “vulnerable third-party media software package” (which, according to a news article citing an anonymous source [19], was Plex, a media server software) to install keylogger malware on the engineer’s computer. The threat actor was then able to obtain the engineer corporate LastPass vault’s master password and use it once the employee had authenticated using MFA, ultimately gaining access to the cloud storage environment credentials.

In this case, even though multiple security measures were already put in place by LastPass, such as the use of encryption on their cloud storage environment and the requirement for employees to use MFA to access LastPass’ systems, the key weakness seems to lie in the fact that the targeted DevOps engineer was able to access LastPass’ critical infrastructure from his personal home computer. This indicates that there is a lack of oversight of the devices that are allowed to access LastPass’ internal systems.

1.2.3. Recommendations to prevent future attacks

One critical piece of information regarding this attack is the fact that the threat actor was able to obtain credentials to LastPass systems by targeting the personal computer of one of LastPass's engineers. This highlights one primordial issue: the use of a personal device to access LastPass's critical infrastructure.

An important security measure to put in place would be to restrict the ability for remote workers to access LastPass' systems using their personal devices. Good security practices include using devices provided by the company, which often include security software such as endpoint protection applications as well as a VPN⁴ client that allows the owner of the company device to securely access the company network remotely. In such a case, it would be way harder for a threat actor to exploit vulnerabilities in third party applications as the installation of such applications is often prohibited on company devices.

In the case of this specific attack, LastPass was already implementing several good security measures and did enforce relatively strong password policies to its customers, thus limiting the amount of data that can be decrypted by the attackers.

Finally, it has been legitimately highlighted on user forums [20] that LastPass does not encrypt everything in customers' vaults. Even though critical information such as usernames and passwords are encrypted, other information is not and could be used by threat actors to launch different types of attacks that involve social engineering or the use of thought-to-be private information to gain the trust of unsuspecting customers. It would then be preferable for LastPass to encrypt such apparently non-sensitive data in the future.

⁴ Virtual Private Network

1.3. SolarWinds Supply Chain Attack (2020)

1.3.1. Overview and analysis

SolarWinds is an American company that provides network monitoring software to several companies and institutions, including the United States federal government. As a result, SolarWinds is considered to be part of the supply chain of these companies as they install and use software produced and distributed by SolarWinds onto their systems.

On December 12, 2020, the company FireEye reported that in November 2020, it detected an intrusion into its systems and identified that the source came from a compromise in the Orion platform, which is a software developed and distributed by SolarWinds. It was also later confirmed by the company Microsoft that several of its cloud platforms were also affected by this kind of intrusion [7]. Because SolarWinds is used by several United States government agencies, the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) releases an emergency directive on December 13, 2020, containing instructions on required mitigations [8] to protect US federal agencies from further exploitation of the vulnerability. Three days later, White House's National Security Council activated the Cyber Unified Coordination Group (UGC) which coordinates the government-wide response with the help of officials from the Federal Bureau of Investigation (FBI), CISA and the National Security Agency (NSA).

According to the timeline consolidated by the United States Government Accountability Office (GAO), the following happened following the discovery exposed by FireEye:

- On December 16, 2020, CISA stated that all impacted federal agencies had disabled the SolarWinds Orion software
- On January 5, 2021, UGC claimed that the breach likely originated from a Russian state-sponsored threat agent
- On February 8, 2021, CISA released two malware analysis reports, exposing the inner working of the malware that was included in the SolarWinds Orion software: *SUNBURST* and *TEARDROP* [9, 10]
- On April 15, 2021, it is confirmed by multiple government agencies (CISA, NSA, FBI, NCSC) that the threat actor was identified as the Russian Foreign Intelligence Service (SVR) [11]. The same day, an executive order is released to issue sanctions targeting the harmful foreign activities of the Russian Government [12].
- On April 19, 2021, the UGC is deactivated, and the investigation comes to an end

This type of attack is called a supply chain attack and can have a broad area of effect considering that, by definition, the attack is distributed through the supply chain of multiple entities. In this specific case, the attack affected all customers of SolarWinds, including multiple agencies of the United States federal government, which explains the large incident response that was initiated as a result.

By looking at the more technical details of this attack, we find that the *SUNBURST* malware was designed to sleep on infected systems for around two weeks following its installation, before starting to perform any kind of malicious activity [9]. Moreover, the malware monitors the processes running on the infected system and will refuse to perform any kind of malicious activity if specific processes are running, such as antivirus software components (e.g. Avast or AVG) or network traffic analysers (such as Wireshark) [9]. The use of such methods corroborates the claims made by US and UK agencies that this attack was performed by a state sponsored threat-agent.

1.3.2. Attack details and identified security flaws

It has been reported by several news sources [13, 14, 15] that the root cause of this supply chain attack might have originated from a password leaked on a GitHub repository, effectively granting access to one of SolarWinds FTP⁵ servers. It is important to note that SolarWinds never confirmed these claims and that there is no effective proof that this specific FTP server would allow anyone to compromise software distributed by SolarWinds.

However, it was reported that these credentials (including the famous “solarwinds123” password) did give access to a SolarWinds FTP server, which highlights a blatant lack of a strong password policy for that specific system. Such practices might indicate that the company does not enforce strong password policies on all its systems.

Other sources also reported that multiple criminals were offering selling access to SolarWinds systems back in 2017 [16], once again indicating potential weaknesses in SolarWinds infrastructure.

Even though the specific details on how the attackers gained access to SolarWinds internal systems were never disclosed, it was uncovered during the investigations conducted by US agencies that threat actors initially gained access to SolarWinds systems back in September 2019. The attackers then began distributing malicious software updates from February 2020 unnoticed until they were discovered by the company FireEye in November 2020 [7].

Once again this illustrates the inability of SolarWinds to, for a period of several months, detect that there was an intrusion in its systems but also to detect that malicious software updates were being crafted and sent out to customers while being digitally signed by the company.

⁵ File Transfer Protocol

We can then identify the major flaws in SolarWinds systems that allowed the attackers to perform this supply chain attack:

- The apparent lack of strong authentication mechanisms
- The apparent lack of policies enforcing various security practices
- The lack of monitoring systems allowing SolarWinds to detect:
 - Intrusions in its systems
 - Malicious modifications being made to their software

1.3.3. Recommendations to prevent future attacks

Although supply chain attacks appear sophisticated, many measures can be put in place to reduce the risk of being affected by such an attack.

First, reinforcing the security of authentication-based systems seems essential, and relies on measures such as:

- Designing and enforcing strict and strong passwords policies. Those policies should define minimal length requirements (e.g. a minimum of 20 characters with the use of lowercase and uppercase letters, numbers and special characters) and prohibit the reuse of identical passwords between different systems. The use of randomly generated passwords should be heavily encouraged.
- Implementing a password rotation policy, based on the criticality of the system (e.g. forcing passwords to be changed every 6 or 12 months). This would, for instance, circumvent issues where passwords have been leaked accidentally on public websites.
- Enforcing Multi Factor Authentication (MFA) for all user accounts on critical systems.

Moreover, considering that SolarWinds' core business is software development and distribution, several measures should be put in place in order to ensure that software that is distributed to clients has not been altered in any way by a malicious third party:

- Securing the build environment where software is packaged and signed prior to distribution: this can be done by isolating build environments and granting minimal access to it, enforcing integrity checks on all the files that are part of the distributed software (e.g. comparing the hashes of the files at each stage of the build process against known trustable hashes) and performing regular audits to make sure that the security level of the build environment is still satisfying.
- Securing the software signing process: this can be done by, for instance, enforcing multi-person authorization to sign software releases and by implementing a regular key rotation policy, where digital keys used for signing software releases are frequently rotated (e.g. every 6 or 12 months).

Finally, it would be crucial to implement a complete monitoring infrastructure designed to detect, log and trace access to different systems that are part of SolarWinds' infrastructure. This part is critical as one the main issue in this supply chain attack was the fact that attackers were able to sit inside SolarWinds' system for several months, allowing them to carefully craft an attack that would be even harder to detect.

2. Designing a server infrastructure and simulating an attack against it

2.1. Contingency policy

The following part outlines the actions that should be taken in case the simulated attack (penetration testing) unintentionally affects systems. This includes, but is not limited to:

- **Unexpected System Instability or Failure:** If the simulated attack inadvertently causes a system (e.g. a server, a firewall or a workstation) to become unstable, unresponsive or crash
- **Data Corruption or Loss:** If the simulated attack results in corruption or loss of data within or outside the tested environment
- **Unintended Access or Privilege Escalation:** If the simulated attack is able to escalate privileges into an environment that was defined as out of scope for the penetration test

Before beginning the simulated attack, ensure that backups are created for all systems that are in and out of the scope of the penetration test. This includes, but is not limited to, configuration backups, databases backups and backups of all other data considered important. Moreover, ensure that these backups are working (i.e. ensure that restoration from the backups works as intended).

In case any of the aforementioned scenarios occur, the following steps should be taken:

- **Unexpected System Instability or Failure:** Stop the simulated attack. Attempt to restart the affected systems. If the restart is unsuccessful, use prior-made backups to restore the affected systems to a previously known working state. Identify and document the root cause of the failure to prevent it from reoccurring.
- **Data Corruption or Loss:** Stop the simulated attack. Assess the situation and determine the extent of the impact. Use prior-made backups to restore the data to its previous state. Identify and document the root cause of the failure to prevent it from reoccurring.
- **Unintended Access or Privilege Escalation:** Stop the simulated attack. Assess the situation and determine the extent of the impact. If any damage has been caused in the out-of-scope environment, restore affected systems to a previously known working state using backups. Identify and document the root cause to ensure that future penetration testing will not go out-of-scope.

2.2. Chosen penetration testing framework and penetration testing tools

In order to perform the simulated attack against CPC's critical infrastructure, the following penetration methodology, adapted from the OWASP penetration testing framework [21], will be used:

- **Reconnaissance:** this phase will be dedicated to gathering as much information as possible about systems that make up CPC's critical infrastructure
- **Scanning:** this phase will be dedicated to scan for entry points into CPC's infrastructure through the detection of open ports and the analysis of network traffic
- **Vulnerability assessment:** the phase will be dedicated to identifying potentially exploitable vulnerabilities in CPC's systems using the information gathered in the previous steps
- **Exploitation:** this phase will be dedicated to exploiting found vulnerabilities to gain access to CPC's critical infrastructure and point out flows in it
- **Reporting:** this phase will be dedicated to detailing the found weaknesses in CPC's critical infrastructure, and providing remediations to strengthen its security

As a result, the following tools will be used for the different phases of the simulated attack:

- **Reconnaissance:** Internet search, DNS lookups
- **Scanning:** [nmap](#), [wireshark](#)
- **Vulnerability assessment:** [National Vulnerability Database \(NVD\)](#)
- **Exploitation:** [Metasploit](#)
- **Reporting:** Manual

2.3. Overview of Cureton Pharmaceutical Company's (CPC) critical server infrastructure

Before describing the simulated attack launched against CPC's critical server infrastructure, we will describe the latter in this part and detail its components.

The figure below contains a diagram of the architecture of CPC's critical server infrastructure:

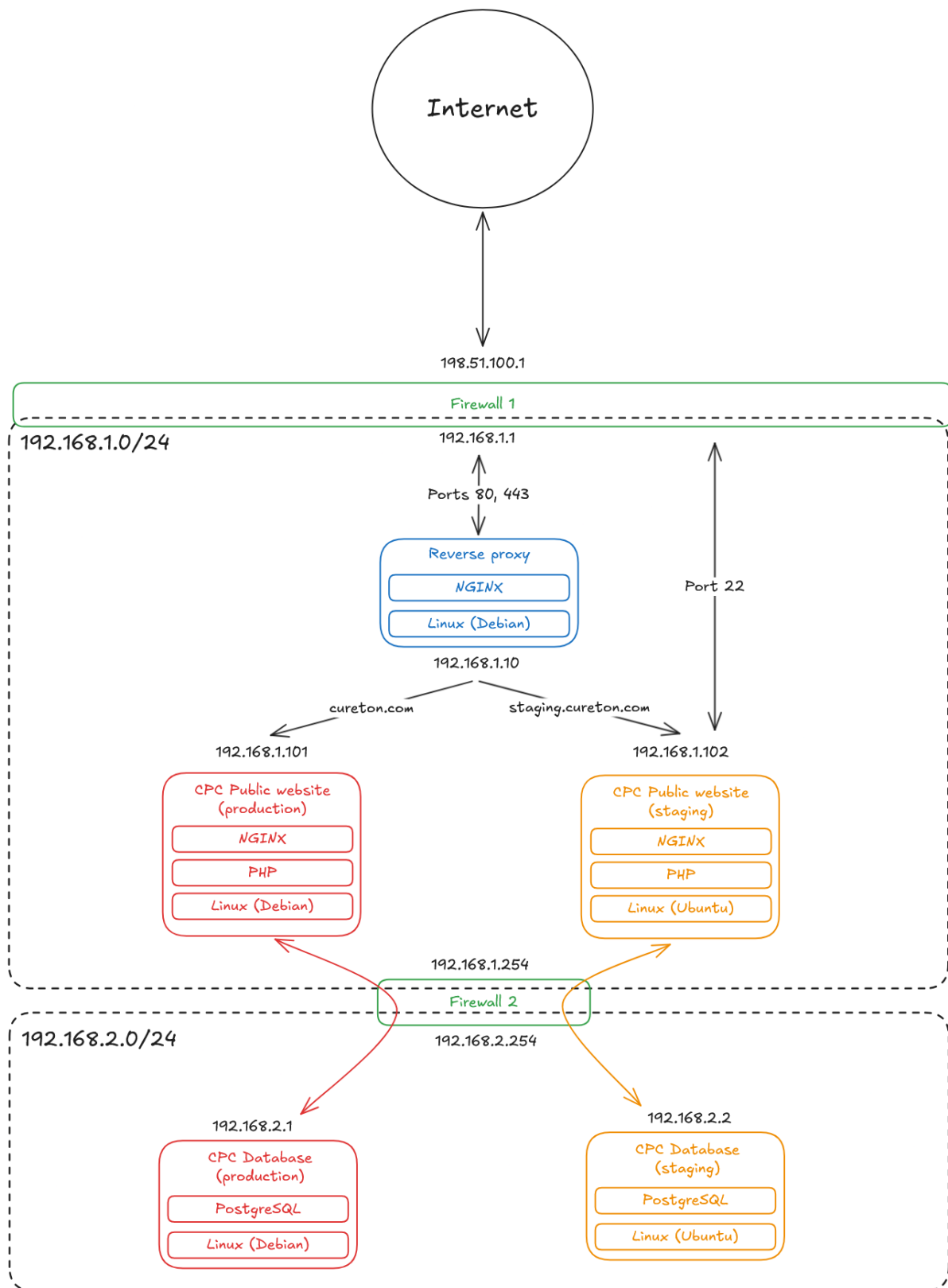


Figure 1: Diagram of CPC's critical server infrastructure

As shown in the diagram, the network architecture is made up of two separate networks:

- The **192.168.2.0/24** network, which contains two separate servers hosting CPC's databases for its staging and production environments
- The **192.168.1.0/24** network, which contains:
 - two separate servers hosting CPC's staging and production websites
 - a reverse proxy used to redirect HTTP/S traffic to both servers depending on the domain in HTTP requests
 - a firewall exposed on the Internet that forwards HTTP/S traffic to the reverse proxy and SSH traffic to the server running CPC's staging website

Both networks are separated by a firewall that allows traffic only coming from those two networks.

Technical details about each machine that is part of CPC's infrastructure can be found in the following table:

Machine	IP addresses	Open ports	Details
Firewall 1	198.51.100.1 192.168.1.1	22, 80, 443	Forwards traffic with destination ports 80/443 to the reverse proxy Forwards traffic with destination port 22 to CPC website server (staging)
Reverse proxy	192.168.1.10	80, 443	Forwards HTTP traffic to port 443 on CPC website server depending on the domain requested
CPC website server (production)	192.168.1.101	22, 443	
CPC website server (staging)	192.168.1.102	22, 443	Can be accessed remotely via SSH from the Internet using an SSH key
Firewall 2	192.168.1.254	22, 5432	Allows traffic from 192.168.1.0/24 to destination ports 22 and 5432 in 192.168.2.0/24 Allows traffic from 192.168.2.0/24 to 192.168.1.0/24 when traffic originated from the latter

CPC database server (production)	192.168.2.2	22, 5432	
CPC database server (staging)	192.168.2.2	22, 5432	

Additionally, the following information relevant to the simulated attack is available:

- CPC's production website server is running up-to-date software with no known vulnerabilities
- CPC's staging website server is part of a staging environment and does not implement security measures as strong as the production server. As a result, this server hosts an older version of CPC's website which uses a vulnerable WordPress plugin "WordPress Popular Posts" version 5.3.2 which is vulnerable to CVE-2021-42362
- CPC's staging website server is used by multiple employees at CPC which use different user accounts with root privileges
- CPC's staging website server runs a daily cronjob under the root user to launch a custom script located in **/opt/export_logs.sh** with permissions set to **766** (rwx-rw-rw-). This cronjob is registered in the **/etc/crontab** file which has its permissions set to **744** (rwxr--r--).

2.4. Detailed walkthrough of the simulated attack

The simulated attack will go through three major steps for the attacker to access secure data stored in CPC's production database server, as shown on the diagram below:

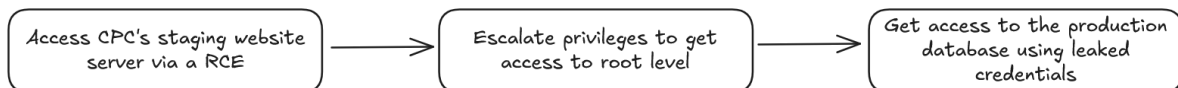


Figure 2: Attack path used in the simulated attack

Each phase is detailed in the following parts.

2.4.1. Initial reconnaissance and scanning

In this phase, we will gather as much information as possible on CPC's infrastructure from the perspective of an attacker that has no prior knowledge of CPC's internal infrastructure. The only information known to the attacker is that CPC owns a publicly available website under the domain name **cureton.com**.

The first step is to get the IP address of the machine associated with that domain name. This can be done by simply doing a DNS query to publicly available DNS servers such as 1.1.1.1 or 8.8.8.8. For instance, the command below would return the IP address associated with the domain **cureton.com**:

```
nslookup cureton.com 1.1.1.1
```

The command above then returns the IP address of CPC's first firewall: **198.51.100.1**. Having gathered this IP address, it is now possible to verify if other domain names are registered with this address by doing a reverse DNS lookup. For instance, the following command would return the domain names associated with the IP address **198.51.100.1** providing that PTR records are correctly set up:

```
nslookup 198.51.100.1
```

The command above then returns the two following domain names:

```
cureton.com  
staging.cureton.com
```

This reveals the existence of CPC's staging website which is indeed available at **staging.cureton.com**.

Upon visiting both websites, by looking at the HTTP requests header, we can notice that the "Server" header is different for each website:

- The header of CPC's production website is **Server: nginx**
- The header of CPC's staging website is **Server: nginx/1.22.1 (Ubuntu)**

This provides valuable information as it indicates that both websites are probably not hosted on the same machine as the web server configuration for populating the "Server" HTTP header is different. This also reveals the presence of the reverse proxy as both websites are accessible through the same IP address.

Knowing this information, it seems preferable to try to find weaknesses in CPC's staging website as development and staging environments are often less secure than production ones.

Before targeting CPC's staging website server, we will run a **nmap** scan to list the open ports on the IP address **198.51.100.1** using the following command:

```
$ nmap -sS 198.51.100.1

Starting Nmap 7.92 ( https://nmap.org )
Nmap scan report for 198.51.100.1
Host is up (0.020s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 54.57 seconds
```

This scan reveals that three ports are open: 80, 443 and 22 and exposes the fact that CPC probably uses an internet-facing firewall that forwards ports 80, 443 and 22.

2.4.2. Accessing CPC's staging website server via a Remote Code Execution (RCE)

2.4.2.1. Attack walkthrough

We will now focus on trying to get access to CPC's staging website server by leveraging a weakness on the publicly available staging website.

Upon visiting the website, we can easily guess that the website is using WordPress as its Content Management System (CMS). One common source of vulnerability in WordPress-based websites is the use of out-of-date vulnerable plugins. We will then try to enumerate the website's WordPress plugins using **wpscan**:

```
wpscan --url https://staging.cureton.com --enumerate p

<REDACTED FOR CLARITY>

[INFO] Enumerating plugins (via Aggressive Detection) ...
| wordpress-popular-posts (5.3.2) - Detected (Aggressive Detection) -
[https://wpscan.com/plugin/wordpress-popular-posts]
|   Location: https://staging.cureton.com/wp-content/plugins/wordpress-popular-posts/
|   Readme: https://staging.cureton.com/wp-content/plugins/wordpress-popular-
posts/readme.txt
|   Style URL: https://staging.cureton.com/wp-content/plugins/wordpress-popular-
posts/style.css?ver=5.3.2
|   Version: 5.3.2 (Detected) - [Vulnerability Database]
|   Title: WordPress Popular Posts < 5.3.3 - Authenticated Code Injection
|   References:
|     * https://wpscan.com/vulnerability/e54d204b-5416-4664-9e61-295758631a1d
|     * https://patchstack.com/database/vulnerability/wordpress-popular-posts/wordpress-
popular-posts-plugin-5-3-2-authenticated-code-injection-vulnerability-leading-to-remote-
code-execution-rce
|   Fixed in: 5.3.3

<REDACTED FOR CLARITY>

[INFO] Vulnerabilities found: 1
```

Here, we find that a vulnerable WordPress plugin is used (WordPress Popular Posts version 5.3.2), which is affected by vulnerability CVE-2021-42362 [26], which allows an authenticated user to perform Remote Code Execution (RCE) on the server running the web application.

By once again using **wpscan**, we can also try to find valid WordPress credentials by supplying a list of commonly used unsecure/defaults credentials:

```
[1] User(s) Identified:

[+] admin
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Author Id Brute Forcing Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

[+] Editor
| Found By: Author Id Brute Forcing Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 2 user/s

[SUCCESS] Editor / editor
Trying Editor / editor Time : 00:18:01 <

[!] Valid Combinations Found:
| Username: Editor , Password: editor

<REDACTED FOR CLARITY>
```

As a result, we obtain the credentials of the “Editor” account, which has sufficient privileges to exploit CVE-2021-42362.

Exploitation of CVE-2021-42362 is rather lengthy and not straightforward and won’t be detailed here but can be used through the help of **Metasploit** [27]. An exploit is also detailed on exploit-db [28].

Such a setup allows the attacker to create a web shell on the server, effectively allowing the user to run arbitrary command on CPC’s staging website server.

2.4.2.2. Recommended solutions

In this specific scenario, two different weaknesses allowed the attacker to gain access to the server remotely:

- The use of weak credentials for the WordPress user account “Editor”
- The use of an outdated and vulnerable WordPress plugin (WordPress Popular Posts) that is affected by a critical vulnerability (Remote Code Execution)

To remedy those issues, it is necessary to:

- Use strong credentials for all WordPress user accounts, even on the staging website. The exploitation of CVE-2021-42362 would not have been possible without the attacker having access to a user’s account
- The patching of vulnerable software running on the server, such as the “WordPress Popular Posts” plugin which was subject to a critical vulnerability. Generally, it is capital to keep software components up to date and to monitor published vulnerabilities that affect the software installed on the server.

2.4.2.3. Cost of recommended solutions

Fortunately, these solutions are both quick and practically costless to implement, Remediation can be done immediately without any additional costs.

2.4.3. Privilege escalation on the server running CPC’s staging website

2.4.3.1. Attack walkthrough

Now that we can execute commands on CPC’s staging website server, we need to escalate our privileges to be able to run commands with root privileges. By inspecting the configuration of the server, we are able to find that the file **/etc/crontab** contains the line:

```
0 0 * * * /opt/export_logs.sh
```

By inspecting the file **/opt/export_logs.sh**, we notice that this file, although executed by the user **root** (via a cronjob) has its permissions set to **766** making it editable by all users on the server.

This enables a privilege escalation by, for instance, adding the public key of an SSH key of the attacker in **/root/.ssh/authorized_keys**, effectively granting the attacker SSH access as the **root** user directly to CPC’s staging website server (as CPC’s first firewall forwards SSH traffic to the staging server).

The privilege escalation can then be done by adding the line **echo “SSH_KEY” >> /root/.ssh/authorized_keys** to the file **/opt/export_logs.sh** by replacing SSH_KEY with the attacker’s public SSH key. On the next run of the cronjob at midnight, the server will allow the attacker’s SSH key to be used when connecting remotely to the server.

2.4.3.2. Recommended solutions

In this specific scenario, a configuration mistake as well as bad security practices resulted in the attacker being able to escalate its privileges after gaining access to CPC's staging website server:

- The use of **/etc/crontab** to run system-wide crontabs as the **root** user is generally considered bad practice and is often discouraged
- The fact that the **root** user was executing a script which was not **exclusively** writable by the **root** user resulted in the attacker being able to effectively execute commands as the **root** user

To remedy those issues, it is necessary to:

- Refrain from using **/etc/crontab** to run system-wide regular tasks. Prefer the use of cronjobs executed by an unprivileged user to reduce the risk of privilege escalation.
- If running system-wide cronjobs cannot be avoided, make sure that those cronjobs are executing scripts that are **only** accessible to the **root** user, both in reading and writing

2.4.3.3. Cost of recommended solutions

Once again, these solutions are quick and costless to implement, as they entirely consist of configuration changes. However, in such a scenario, it would be advised to ensure that system administrators are up to date on the best security practices when administering servers.

The cost for specific training for system administrators is hard to estimate and could range from as low as £500 to a couple of thousands of pounds for more advanced training (for a 3-day training session).

2.4.4. Accessing the production database by inspecting the users bash histories

2.4.4.1. Attack walkthrough

Now, we effectively have root access on CPC's staging website server, which allows us to look for any kind of valuable information on that specific server.

By looking at the **/home** directory, we notice that this server is used by multiple users that all have dedicated user accounts. Having root privileges, we can inspect each user's bash history by simply looking at the content of the file **/home/user/.bash_history** where **user** is the username of the specific user.

Looking at all the users' histories, we find the following command:

```
psql -h 192.168.2.1 -p 5432 -U postgres -W 'fgaG4$fMCt4ewc$!'
```

This effectively gives us access to CPC's production database with the **postgres** user account, which is the superuser of the PostgreSQL instance running on that server.

2.4.4.2. Recommended solutions

In this specific scenario, the lack of proper network segmentation as well as bad practices allowed the attacker to gain access to CPC's production database with a privileged user account:

- A system administrator's account was used to directly connect to CPC's production database using the credentials of the most privileged account available (**postgres**). This is not good practice as the server is part of CPC's staging environment and should use the dedicated staging database server under all circumstances. Moreover, passwords should never be supplied directly in commands as those are susceptible to being logged in multiple places without the user knowing.
- The lack of network segmentation allowed the attacker to connect to a server that is part of the production environment directly from the staging environment.

To remedy those issues, it is necessary to:

- Make sure that system administrators follow good security practices
- Implementing proper network segmentation to ensure that logical environments (production, staging, development, testing, etc.) are properly separated. This can be done virtually (e.g. using VLANs) or physically (e.g. using different physical equipment). Generally, it is crucial to at least keep the production environment separated from all other environments.

2.4.4.3. Cost of recommended solutions

As stated before, the cost of personnel training is hard to estimate. It is also not straightforward to estimate the cost of implementing network segmentation as it depends on lots of different factors such as:

- The size of the network
- The amount of different environments
- The preferred approach for segmenting the network (physical or virtual segmentation)

Depending on these parameters, the cost of implementing proper network segmentation could greatly vary.

2.5. Attack simulation results and summary

During this attack simulation, major flaws were discovered in CPC's critical server infrastructure, which would allow an external based attacker to effectively exfiltrate the content of CPC's production database without prior knowledge of CPC's internal infrastructure.

The following flaws have been identified during the attack simulation:

- Misconfiguration of several servers: misconfigured web servers leaked information (such as "Server" HTTP headers) that could allow attackers to have a better understanding of CPC's internal network
- The lack of maintenance on CPC's staging website: several software components were not up to date and were subject to critical vulnerabilities
- The lack of good practice among system administrators, which led to CPC's staging website server being misconfigured, allowing a potential attacker to escalate its privileges upon gaining access to the server
- The lack of network segmentation, which allows servers in the staging environment to communicate with servers in the production environment

2.6. Remediation summary

2.6.1. Execution timetable

Below is a proposed timeline for execution the various remediation actions to strengthen the security of CPC's critical infrastructure:

- **Step 1:** Immediately apply patches to outdated and vulnerable software components, especially those that are installed on servers hosting internet-facing applications such as CPC's production and staging websites
- **Step 2:** Review CPC servers' configuration and apply changes to not give away technical information to potential threat actors. For instance, NGINX web servers should be configured with the **server_tokens** configuration option set to **off** to not expose the version number in the "Server" header in HTTP requests sent by the servers
- **Step 3:** Schedule, if deemed necessary, additional training for system administrators to reinforce the use of good practice when administering critical servers
- **Step 4:** Redesign CPC's server infrastructure to make use of proper network segmentation by ensuring that the production environment is separated from other environments such as CPC's staging environment. A proposed segmented architecture is shown on the diagram below.

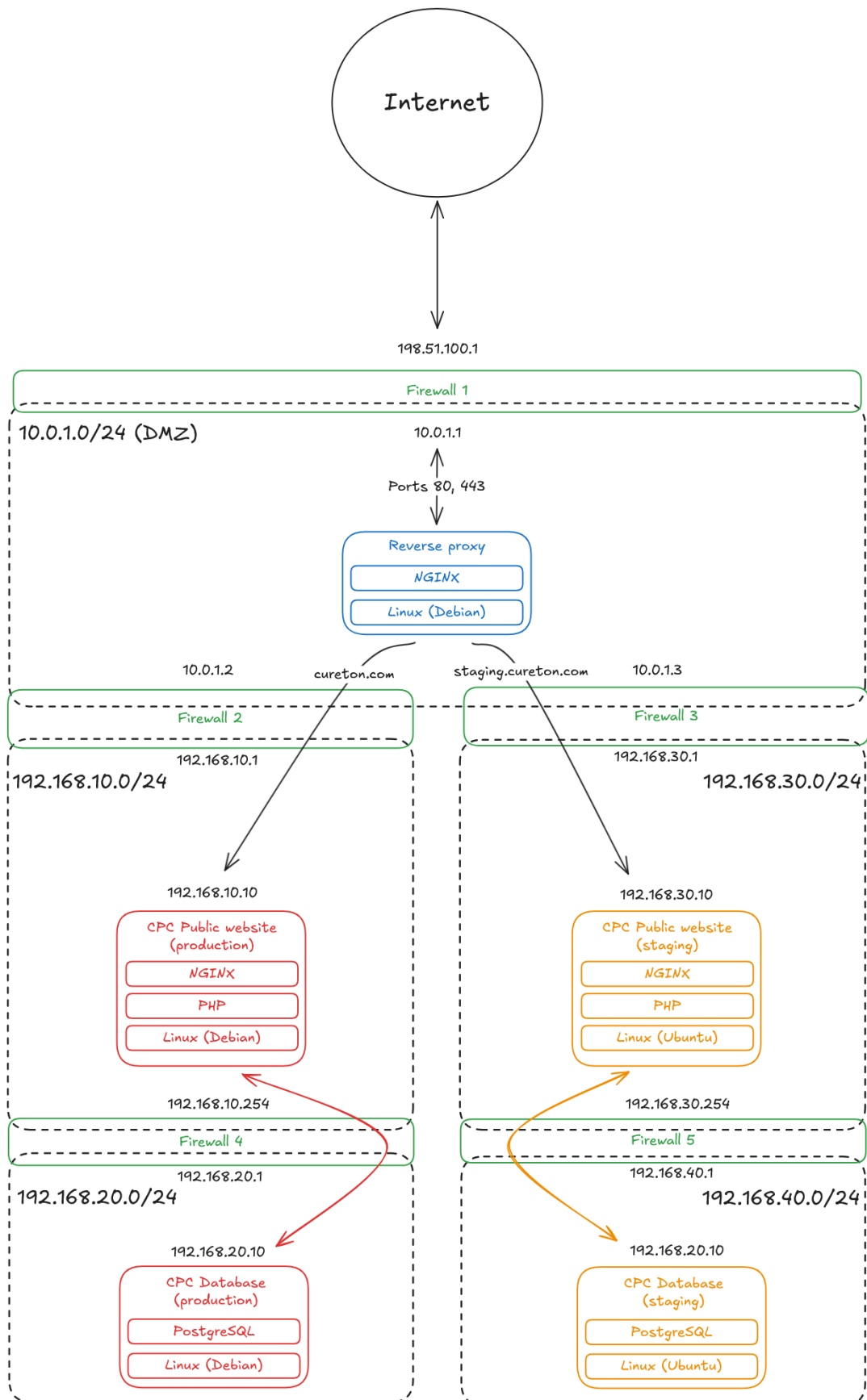


Figure 3: Proposed segmented network architecture for CPC

2.6.2. Total cost

As discussed before, most of the remediation actions do not require additional costs, except for potential employee training. However, the implementation of network segmentation requires investment in network equipment to properly separate CPC's production and staging environments.

In the case of choosing to separate both environments physically, as shown on the diagram above, it would be necessary for CPC to acquire multiple firewalls to filter network traffic entering and leaving the separated networks. Prices for firewalls that would satisfy CPC's needs in terms of network segmentation can range from £1,000 to £10,000. Additionally, the hourly rate of a specialist that would implement the required fixes as well as setting up a segmented network architecture would range from £60 to £200 an hour.

Below is an invoice for CPC's particular case:

Invoice

BALANCE DUE

£ 20,167.00

Debit To:

Cureton Phamarceutical Company

Kings Rd, Swansea SA1 8EW

Debit Date:

06/05/2025

Debit No.:

123456

Invoice No.:

123456

#

Item name

Description

Quantity

Unit Price

Amount

1

Hourly rate

Hired expert

35

£ 80.00

£ 2,800.00

2

Medium Enterprise Firwall

3

£ 5,789.00

£ 17,367.00

Note

Subtotal

£ 20,167.00

Shipping

£ 0.0

Total

£ 20,167.00

Figure 4: Proposed invoice for CPC

05/06/2025

27

3. Conclusion

This document has provided a dual perspective on the modern landscape of cybersecurity. The analysis of recent cyberattacks against large companies and government agencies highlights the important and evolving nature of threats, focusing on consequences of security vulnerabilities. Understanding the root causes behind such attacks allows us to often prevent such attacks from happening in the future by strengthening security practices.

Complementarily, the simulated attack against CPC's critical server infrastructure demonstrated how common flaws could be exploited by threat actors to gain unauthorized access to sensitive data, thus highlighting the need for strong security measures and practices. The remediations proposed in this document offer a starting point to fortify network defences and mitigate identified risks.

Ultimately, this document highlights the continuous nature of cybersecurity, which requires permanent vigilance, regular security assessments and constant implementation of robust security measures to effectively protect against an ever-increasing list of sophisticated threats.

4. Table of figures

Figure 1: Diagram of CPC's critical server infrastructure	16
Figure 2: Attack path used in the simulated attack.....	18
Figure 3: Proposed segmented network architecture for CPC.....	26
Figure 4: Proposed invoice for CPC	27

5. References

- [1] Change Healthcare. "Change Healthcare Cyberattack Support." <https://www.unitedhealthgroup.com/https://www.unitedhealthgroup.com/ns/health-data-breach.html>
- [2] Ionut Arghire, "Change Healthcare Confirms BlackCat Ransomware Attack," Feb 29 2024. Accessed: 2025. [Online]. Available: <https://www.securityweek.com/blackcat-ransomware-gang-claims-attack-on-change-healthcare/#:~:text=claiming%20the%20theft%20of%206%20Tb%20of%20data>
- [3] Steve Alder, "Judge Sets Deadline for Motions to Dismiss Claims in Change Healthcare Data Breach Lawsuits," *The HIPAA Journal*, Feb 19 2025. Accessed: 2025, [Online]. Available: <https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/#:~:text=a%20data%20breach%20involving%20the%20theft%20of%206%20TB%20of%20data>
- [4] "What We Learned: Change Healthcare Cyber Attack," May 03 2024. Accessed: 2025. [Online]. Available: [https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack/#:~:text=\\$22 million in Bitcoin](https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack/#:~:text=$22 million in Bitcoin)
- [5] U.S. Government Accountability Office. "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)." <https://www.gao.gov/https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic>
- [6] U.S. Cybersecurity and Infrastructure Security Agency. "ED 21-01: Mitigate SolarWinds Orion Code Compromise." <https://www.cisa.gov/https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise>
- [7] U.S. Cybersecurity and Infrastructure Security Agency, "MAR-10318845-1.v1 - SUNBURST," U.S. Cybersecurity and Infrastructure Security Agency (CISA), Accessed: 2025. [Online]. <https://www.cisa.gov/news-events/analysis-reports/ar21-039a>
- [8] U.S. Cybersecurity and Infrastructure Security Agency, "MAR-10320115-1.v1 - TEARDROP," U.S. Cybersecurity and Infrastructure Security Agency (CISA), Accessed: 2025. [Online]. <https://www.cisa.gov/news-events/analysis-reports/ar21-039b>
- [9] UK National Cyber Security Centre. "UK and US call out Russia for SolarWinds compromise." <https://www.ncsc.gov.uk/https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise>
- [10] Keumars Afifi-Sabet, "SolarWinds blames intern for weak 'solarwinds123' password," Mar 1 2021. Accessed: 2025. [Online]. Available: <https://www.itpro.com/security/cyber-attacks/358738/intern-blamed-for-weak-password-that-may-have-sparked-solarwinds>
- [11] Brian Fung and Geneva Sangs, "Former SolarWinds CEO blames intern for 'solarwinds123' password leak," Feb 26 2021. Accessed: 2025. [Online]. Available: <https://edition.cnn.com/2021/02/26/politics/solarwinds123-password-intern/index.html>

- [12] Raphael Satter, Christopher Bing and Joseph Menn, "Hackers used SolarWinds' dominance against it in sprawling spy campaign," Dec 16 2020. Accessed: 2025. [Online]. Available: <https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8/>
- [13] LastPass. "12-22-2022: Notice of Security Incident." <https://blog.lastpass.com>. <https://blog.lastpass.com/posts/notice-of-recent-security-incident>
- [14] LastPass Support. "Incident 2 – Additional details of the attack." <https://support.lastpass.com>. https://support.lastpass.com/s/document-item?nocache=https%3A%2F%2Fsupport.lastpass.com%2Fs%2Fdocument-item%3Flanguage%3Den_US%26bundleId%3Dlastpass%26topicId%3DLastPass%252Fincident-2-details.html%26_LANG%3Ditit
- [15] Dan Goodin, "LastPass says employee's home computer was hacked and corporate vault taken," Feb 28 2023. Accessed: 2025. [Online]. Available: <https://arstechnica.com/information-technology/2023/02/lastpass-hackers-infected-employees-home-computer-and-stole-corporate-vault/>
- [16] "PSA: LastPass Does Not Encrypt Everything In Your Vault", *Hackernoon*, <https://hackernoon.com/psa-lastpass-does-not-encrypt-everything-in-your-vault-8722d69b2032>
- [17] "The OWASP Testing Framework." <https://owasp.org>. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies#penetration-testing-framework
- [18] NIST. "CVE-2021-42362 Detail." <https://nvd.nist.gov>. <https://nvd.nist.gov/vuln/detail/CVE-2021-42362>
- [19] h00die, Simone Cristofaro and Jerome Bruandet, "Wordpress Popular Posts Authenticated RCE." <https://www.rapid7.com>. https://www.rapid7.com/db/modules/exploit/multi/http/wp_popular_posts_rce/
- [20] Simone Cristofaro. "WordPress Plugin Popular Posts 5.3.2 - Remote Code Execution (RCE) (Authenticated)." <https://www.exploit-db.com>. <https://www.exploit-db.com/exploits/50129>
- [21] American Healthcare Association, "Change Healthcare cyberattack impact," American Healthcare Association, 2024. Accessed: 2025. [Online]. <https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf>