

Assessment Ethical Hacking ACCA7033

Amine Laimeche



Table of content

Table of content	1
Task 1	2
1 : 2011 Playstation Network hack, one of the biggest gaming hacking in history	2
2 : 2021 Microsoft Exchange Attack by the Hafnium Group	4
3 : 2022 Ransomware attack on Corbeil-Essonnes Hospital	6
Task 2	8
1. Introduction and network architecture	8
2. List of Acronyms	10
3. Contingency Policy	10
4. Penetration Testing Framework	11
5. Penetration Testing Tools	11
6. Attack Simulation	11
Simulation 1: CPC Web Portal	11
Simulation 2: CPC Mail Server	13
7. Recommendations & Countermeasures	15
For PSN-type Attacks	15
For Hafnium-style Zero-days	15
8. Cost Analysis	16
References	20

Task 1

1 : 2011 Playstation Network¹ hack, one of the biggest gaming hacking in history

In early 2011, George Hotz, a hacker, published on his website an exploit to run a custom firmware on PS3, from a Linux installation disk.

A custom firmware gives a lot of liberty to users, allowing them a root and debug access, running homebrews (unofficial apps) and games from a backup (basically playing them for free), customizing systems with new themes, running emulators.

This is totally illegal and Sony can block consoles if they detect a custom firmware installed on it.

In January of 2011, Sony filed a court order against George Hotz, for violation of DMCA and Computer Fraud.

In a form of protest, on April 4, the famous Anonymous group attacked the Playstation Network with a DDOS attack. Their goal was to persuade Sony to cancel the lawsuits against George Hotz. This attack lasted for 3 days, but Anonymous realized that it was harming the consumers rather than Sony, so they decided to stop this attack. Sony eventually settled the lawsuit with Hotz by April 11

Between April 17 2011 and April 19 2011, Sony's Playstation Network was a victim of an "external intrusion". Sony suspected another Anonymous attack but nothing can confirm this. This attack led to one of the **largest data breaches** in the video game industry.

Sony has not released all the technical details of the intrusion, but post-incident analyses have allowed for a partial reconstruction of the method used. The attack is believed to have involved a mix of classic but effective techniques :

Phishing: The attackers were able to obtain administrator or employee credentials through phishing campaigns, allowing them to access internal systems.

SQL injection: SQL injection vulnerabilities were exploited on PSN's web servers. This allowed the attackers to execute unauthorized queries to databases, bypassing authentication mechanisms.

Privilege Escalation and Data Exfiltration: Once initial access was gained, the hackers were able to escalate their privileges on Sony's internal systems and then extract massive amounts of sensitive data. The exfiltration was reportedly made possible by a network segmentation flaw between public servers and user databases.

The PSN infrastructure at the time also included several outdated software components, some of which were no longer regularly updated. This facilitated the exploitation of known vulnerabilities.

¹ Playstation Network (PSN) : Service provided by Sony that allows to buy, download and play online games on PS3 and PSP at the time (PSN still exist nowadays for PS4 and PS5)

The consequences were **catastrophic**:

77 million accounts were compromised. Hackers got names, emails, postal addresses, dates of birth, hashed passwords, purchase history, and potentially credit card data (which Sony has never confirmed).

Sony was forced to shut down PSN for 24 days, from April 20 to May 14, 2011. This prevented users worldwide from accessing their online games, downloading content, or using connected services, leading to immense frustration

Sony estimated the total cost of the attack at **over 170 million dollars** : incident response costs, legal proceedings, security system overhauls, and the “Welcome Back” program. This program gave free games and subscriptions to PSN users, as a compensation.

Several class action lawsuits were filed against Sony, notably in the US and Canada. Sony **was also heard by the U.S. Congress**. The case contributed to a global awareness of the need to protect personal data in digital services, at a time before the GDPR.

Sony's image has been seriously tarnished. Gamers criticized the slowness of communication (it took Sony nearly a week to acknowledge the extent of the leak), the lack of transparency about the causes, and the internal security flaws.

The weaknesses exploited in this attack demonstrate **insufficient** security :

- Lack of clear network segmentation between web services and databases.
- Non-updated server software, exposed to known vulnerabilities (notably SQL injection).
- Lack of strong password encryption (weak hashing algorithm, no salting).
- Lack of proactive monitoring (absence of a SIEM system, detection of network anomalies or unusual activity).
- Late communication, revealing a lack of a crisis management plan.

Here are the main **countermeasures** that **could have prevented**, or limited, this attack :

- Regularly updating web servers and immediately patching known vulnerabilities.
- Systematic application of Web Application Firewalls to intercept SQL injections.
- Use of salted and hashed passwords with a robust algorithm.
- Implementation of strong authentication and logging.
- Deployment of a clear incident response plan, with trained teams, regular testing, and emergency communication channels.
- Adopting a DevSecOps approach, and integrate security into the core of the development cycle

2 : 2021 Microsoft Exchange Attack by the Hafnium Group

In January 2021, a global cyberattack and data theft campaign began by **exploiting critical zero-day vulnerabilities** in on-premises Microsoft Exchange email servers.

The group initially behind the attack, dubbed Hafnium by Microsoft, is an advanced nation-state actor operating out of China.

The first known intrusions were observed as early as January 2021, and the attack compromised the email systems of **approximately 30,000 organizations** in the United States alone and at **least 7,000 entities** in the United Kingdom, including the European Banking Authority, the Norwegian Parliament, and the Chilean Financial Services Commission. In total, it is estimated that as of March 2021, no fewer than 250,000 Exchange servers worldwide had been compromised. Microsoft revealed that the exploited flaws had existed latently in the Exchange code for nearly 10 years. The Hafnium campaign thus highlighted the systemic vulnerability of a critical component, corporate email, in many sectors.

Hafnium exploited a **chain of four major zero-day vulnerabilities** in Microsoft Exchange Server :

- Initial Exploit – CVE-2021-26855: This is a **Server-Side Request Forgery** vulnerability that allows arbitrary HTTP requests to be sent to the Exchange server while impersonating it. Specifically, the attacker could, without prior authentication, **send HTTP commands that were accepted as legitimate** by the Exchange server. This step allowed them to authenticate as if they were the server itself, bypassing normal access controls.
- Server Compromise – CVE-2021-26857: This vulnerability resided in the Exchange Unified Messaging service and involved insecure deserialization. By leveraging **untrusted data injected into a deserialization process**, Hafnium was able to **execute arbitrary code with system privileges** on the server. However, exploiting this vulnerability required already having administrative privileges on the server or the prior use of another vulnerability. In practice, the attacker obtained these privileges by combining it with the CVE-2021-26855
- Backdoor Installation (Web Shell) – CVE-2021-26858 / CVE-2021-27065: These two vulnerabilities allowed **post-authentication arbitrary file writing** on the Exchange server. Once authenticated (via CVE-2021-26855), the attacker could write files to any location on the server. Hafnium used this to **drop a malicious web shell**, a web script (often in ASPX) installed in the Exchange web server directory, providing **persistent remote access**. For example, a China Chopper-like web shell was implanted, allowing the attacker to send system commands via simple HTTP requests. Once the web shell was in place, the server remained compromised even after patches were applied, acting as a persistent backdoor.
- Post-exploitation actions: With full administrator access to the mail server, Hafnium operators performed various actions to further escalate their access and steal sensitive data. Some of the techniques observed included: using the ProcDump tool to extract the contents of LSASS process memory (containing cleartext or hashed credentials), installing tools like 7-Zip to compress stolen data for exfiltration, using

Exchange PowerShell cmdlets to export full user mailboxes, deploying additional backdoors via PowerShell reverse shells (e.g. Nishang script) or using PowerCat (netcat-like implant) to establish connections to external servers

Many organizations suffered **sensitive data theft** (confidential emails, attachments, internal address books) as a result of this attack. For some, strategic or personal information may have been leaked. The sudden need to urgently patch thousands of servers also disrupted corporate IT services. Many organizations had to mobilize incident response resources to detect and remove installed web shells, which generated an unforeseen workload and potentially email service interruptions during remediation. Furthermore, the attack eroded confidence in the security of communications: knowing that internal emails could have been read by an unauthorized actor had a destabilizing effect on the internal governance of certain entities (need to notify partners of the leak, etc.)

The overall financial cost is difficult to estimate but **likely very high**. Affected companies have had to incur significant expenses for security consultants, forensics, and system restoration. Some may have been forced to replace compromised servers or accelerate their migration to cloud solutions, resulting in unforeseen costs. According to CNBC, the losses include not only technical response costs, but also the economic damage related to stolen information that could be exploited by competitors or nation-states.

The Hafnium attack sparked reactions at the highest levels of government. The United States and its allies publicly attributed the attack to China and denounced this campaign internationally in July 2021. Investigations were opened in several countries to assess the extent of the compromises of government organizations. Legally, victim companies may have been required to notify affected individuals if personal data appeared in the stolen emails (an obligation under the GDPR in Europe, for example). Microsoft also came under criticism and had to collaborate with authorities to facilitate crisis management. It should be noted that this attack prompted the FBI to carry out an unprecedented action: a remote deletion operation of web shells on Exchange servers in the United States (under court order) to help organizations that had not eliminated the post-patch backdoor. This intervention raised legal questions about "hack-back" by authorities to protect victims.

Several technical and organizational countermeasures could have limited, or even prevented, the compromise of Exchange servers:

The most obvious preventative measure is **rigorous patching**. Microsoft released patches for the exploits used (ProxyLogon) on March 2, 2021, but many organizations had not updated their Exchange servers promptly. Had the patches been applied as soon as they became available, the attack would have been stopped before it could cause such widespread damage. Furthermore, Microsoft had announced the end of support for Exchange 2010, but had to release a one-off patch for it—which underscores the importance of updating end-of-life software or migrating to supported versions. Maintaining a tight update cycle (including emergency patches outside of "Patch Tuesday") is a key lesson from this incident.

Many on-premises Exchange servers were directly exposed to the internet for web access or EWS services. Countermeasures such as implementing a mandatory VPN to access the administration interface or Exchange services could have prevented anonymous SSRF exploitation.

An upstream countermeasure is to conduct regular audits of exposed systems. Companies could fund more bug bounty programs for their critical applications.

Following the Hafnium attack, organizations running Microsoft Exchange on-premise should strengthen their cybersecurity posture through the following key measures:

- Migrate to secure cloud services: Move to Exchange Online or trusted managed email services that offer automatic updates and centralized monitoring, reducing exposure to 0-day vulnerabilities.
- Implement a strong vulnerability management program: Continuously monitor vendor security bulletins and apply critical patches immediately. Use automated tools to detect vulnerabilities and plan maintenance accordingly.
- Enhance threat detection and incident response: Leverage a SOC service to monitor logs 24/7. Utilize indicators of compromise IOCs shared by vendors and maintain tailored response playbooks for critical assets.
- Ensure reliable backups and business continuity: Maintain encrypted, offline backups of Exchange servers and test them regularly.
- Train and raise awareness: Educate IT staff to detect signs of compromise and brief executives on cybersecurity risks to secure appropriate funding. Share lessons learned and participate in community feedback to continuously improve resilience.

3 : 2022 Ransomware attack on Corbeil-Essonnes Hospital

In August 2022, the Centre Hospitalier Sud Francilien (CHSF), a **major hospital** in the Paris region, was hit by a large-scale **ransomware attack** that paralyzed its entire IT infrastructure. The ransomware, **LockBit² 3.0**, encrypted critical systems : medical records, imaging tools, and laboratory software. This forced the hospital to switch to paper-based procedures. Emergency services were rerouted, and many appointments were canceled. Attackers demanded a 10 million dollars ransom, which the hospital refused to pay.

The attack followed a **classic ransomware kill chain**: an initial compromise, likely through a phishing email or an exposed Remote Desktop or VPN service, followed by lateral movement using tools like Cobalt Strike and Mimikatz. The attackers escalated privileges, reached critical infrastructure, and **launched the ransomware** during off-hours for maximum impact. As a form of double extortion, they **also exfiltrated sensitive data**, including medical reports and staff payrolls, and leaked them online after the ransom was refused.

Technically, the success of the attack stemmed from **several weaknesses**: outdated systems, poor segmentation, lack of endpoint detection, and weak backup strategies. Organizationally, the hospital lacked real-time detection capabilities and likely did not have a structured incident response plan. **Human error** also played a role, as phishing remains a

² **LockBit** is a cybercriminal group proposing [ransomware as a service](#)

common entry point, especially in environments where staff are not aware of cyber menaces.

The consequences were significant. Operationally, the hospital's **core services were disrupted for weeks**. Financially, the cost of recovery (new hardware, cybersecurity experts, system rebuilds) likely **reached millions**. Legally, the hospital had to report the incident to regulatory authorities, and patient **data exposure** raised privacy concerns. Psychologically, both patients and staff experienced stress, uncertainty, and a loss of trust in the institution.

Several countermeasures could have reduced the risk or impact of the attack:

- Network segmentation: **Isolating** medical, administrative, and backup systems would have contained the spread of ransomware.
- Up-to-date systems: **Regular patching** of exposed services and removal of unsupported devices would have closed many attack vectors.
- Robust backup strategies: Offline and encrypted **backups** could have enabled faster recovery without needing to pay ransom.
- EDR and monitoring: Deploying **endpoint detection** and response tools, coupled with network anomaly detection, might have caught the attack earlier.
- Access control and least privilege: Limiting admin rights and using MFA could have blocked lateral movement and privilege escalation.
- Staff training: Phishing simulations **before** a real attack occurs and basic cybersecurity awareness for all employees would reduce the risk of human error.

Hospitals must treat cybersecurity as a **core component** of patient safety. This means investing in secure infrastructure (Zero Trust models, updated hardware), and deploying advanced defenses (EDR, SOC, threat intelligence). Regular incident simulations, clear communication plans, and psychological support for staff after incidents are also crucial.

The CHSF attack was a **wake-up call** : in today's healthcare landscape, cyber threats can have real, life-threatening consequences. Prevention requires not just technical tools, but a culture of vigilance, preparation, and continuous improvement.

Task 2

1. Introduction and network architecture

In the wake of persistent cyber threats affecting industries worldwide, Cureton Pharmaceutical Company has mobilized a Red Team to **simulate multi-layered attacks** on its systems. The objective is to **evaluate and reinforce** the company's infrastructure before its imminent release of critical respiratory virus vaccines.

This report draws from **real-world cyberattacks** to simulate similar threats in CPC's virtual environment. Each simulation is critically analysed, and tailored countermeasures are proposed to reinforce the resilience of CPC's infrastructure.

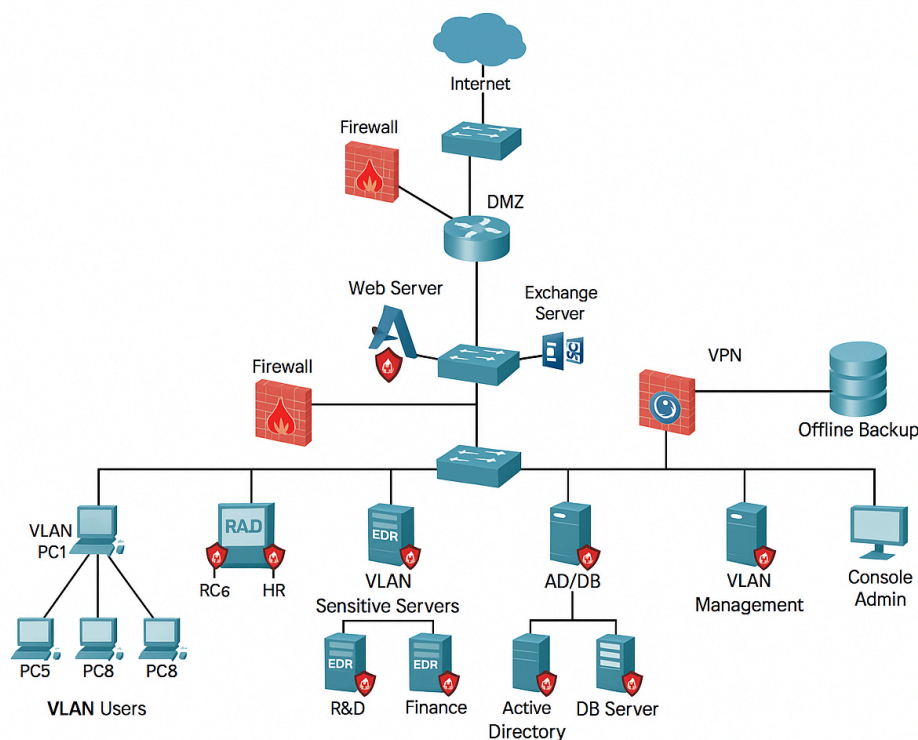


Figure 1: CPC's Simulated Network Architecture

This diagram illustrates the simulated network architecture of **CPC**, designed in response to the cyber threats detailed in **Task 2** of this report. The architecture follows principles of defense-in-depth, strict network segmentation, and incorporates key security components aligned with the attack scenarios simulated.

Perimeter Firewall: This device filters all incoming traffic from the Internet, only allowing necessary ports (ex : HTTPS for the web portal and OWA access to Exchange).

DMZ (Demilitarized Zone): This intermediary zone hosts the externally exposed services:

- **Web Server (Apache):** Entry point of Simulation 1, vulnerable to SQL injection.
- **Exchange Server:** Target of Simulation 2, exposed to the Internet for Outlook Web Access. A **Web Application Firewall** is deployed in front of the Web Server to block application-layer attacks such as SQL injection and XSS.

Internal Firewall: This firewall separates the DMZ from the internal network, preventing direct lateral movement from compromised public-facing services to critical internal systems.

User VLAN: This segment contains employee workstations. In the diagram, three user PCs represent a group of approximately 100 users. These machines are restricted to accessing authorized services only and are protected with **Endpoint Detection and Response** agents.

Sensitive Servers VLAN: This segment includes critical business servers such as R&D, finance and HR.

These servers are monitored by EDR and are protected through strict access control rules. They are key targets during lateral movement phases in advanced attacks.

Infrastructure VLAN (AD/Database): This zone hosts:

- The **AD domain controller**, a critical target in privilege escalation attempts.
- The **User Database Server**, exploited in Simulation 1 for credential extraction. Both servers are monitored with EDR and are isolated from general network access.

Management VLAN: Reserved for administrative and monitoring functions, this segment includes:

- The **Administration Console**
- The **Security Information and Event Management (SIEM)** system, which collects and correlates logs to detect anomalies such as unexpected connections or privilege escalations.

Secure VPN Access: All remote administrative access must go through a secure VPN tunnel with strong authentication. This measure eliminates the risk of exposing administrative interfaces to the Internet.

Offline Backup System: Critical data is regularly backed up to a storage system that is physically or logically disconnected from the active network. This ensures recovery capabilities in the event of destructive attacks such as ransomware.

Red Shield Icons (EDR): These indicate systems protected by EDR agents. EDR provides real-time detection of suspicious behavior (e.g., privilege escalation attempts, credential

dumping, unusual PowerShell activity) and can either block malicious actions or trigger alerts to the SOC team.

2. List of Acronyms

- CPC – Cureton Pharmaceutical Company
- PSN – PlayStation Network
- EDR – Endpoint Detection and Response
- MFA – Multi-Factor Authentication
- IOC – Indicator of Compromise
- SIEM – Security Information and Event Management
- VPN – Virtual Private Network
- MITRE – MITRE ATT&CK Framework
- OWASP – Open Web Application Security Project

3. Contingency Policy

Before initiating the Red Team simulation, the following contingency measures were implemented:

- **System Backups:** Secure snapshots of all virtual machines and critical systems stored offline.
- **Legal & Compliance Readiness:** Internal legal team on standby in case of critical exposure.
- **Incident Response Team :** A parallel Blue Team assigned to monitor and isolate test anomalies.
- **Communication Protocol:** Defined channels to alert stakeholders during the test if production systems are impacted.
- **Scope Definition:** Attack simulation is strictly confined to the replicated virtual environment with no impact on production.

4. Penetration Testing Framework

We adopted the **OWASP TOP TEN** and **MITRE ATT&CK** frameworks to guide the simulation lifecycle. Each step followed the reconnaissance, enumeration, exploitation, and post-exploitation structure.

Key references include:

- MITRE ATT&CK
- OWASP Top 10 vulnerabilities

5. Penetration Testing Tools

Tool	Purpose
Kali Linux	Base pentesting environment
Metasploit	Exploit development & delivery
Burp Suite	Web application analysis
SQLmap	Automated SQL injection scanning
Nmap	Network scanning and enumeration
Mimikatz	Credential dumping
Cobalt Strike	Simulated adversarial command & control
Wireshark	Network traffic inspection
PowerShell Empire	Post-exploitation and lateral movement
Splunk	Log analysis and SIEM

6. Attack Simulation

Simulation 1: CPC Web Portal

Reconnaissance: The red team attacker begins by scanning CPC's external footprint for weak points. Using Nmap, they identify an outdated web server hosting CPC's customer portal : an Apache server with missing patches and no web application firewall. This corresponds to OWASP Top 10 **issue A06: Vulnerable and Outdated Components**, since the server software had known flaws. The attacker also maps subdomains and open ports (HTTP, HTTPS) to find any entry point

Initial Access (Exploitation): The attacker discovers a **SQL injection** vulnerability in the web portal login page. By crafting malicious input in a login field, they trick the application into executing unintended SQL queries. Using **SQLmap**, the attacker dumps user credentials and even executes system commands via the database. This corresponds to OWASP **A01: Injection** and MITRE technique **T1190: Exploit Public-Facing Application** for initial compromise. Here, the injected SQL spawns a shell on the web server with the privileges of the web application for persistent access.

Privilege Escalation: The attacker now seeks higher privileges. The web server account may be limited, so they exploit a local vulnerability (misconfigured sudo) to become root. If the server is Windows, they might use **Metasploit** exploits to escalate (MITRE **T1068: Exploitation for Privilege Escalation**). They could also harvest credentials from memory using **Mimikatz** if the server is domain-joined (ATT&CK **T1003**). In our simulation, the web server had a database connection account with reuse of an Active Directory credential : **OWASP A07: Identification and Authentication Failure**. Using this, the attacker now has a foothold in the internal network under a valid user context.

Persistence: To ensure continued access, the attacker installs persistence mechanisms on the compromised server. They add a new admin user and schedule a hidden task to re open a reverse shell. The webshell planted earlier also serves as persistence (MITRE **T1505.003**). This means even if the server is rebooted or the initial vulnerability patched, the attacker can come back. The attacker may also maintain access by **backdooring database accounts** or leaving a rogue VPN account.

Lateral Movement: Now the attacker pivots deeper into CPC's internal network. From the DMZ web server, they connect to the **User Database** via SMB using the stolen credentials. This is similar to how the PSN hackers accessed databases with millions of user records. The attacker uses **SMB, and its port 445** to move laterally (MITRE **T1021** for remote services).

Active Directory is also targeted – the attacker uses the foothold to query AD for other servers (file shares, HR systems). This step correlates with MITRE's **Discovery and Lateral Movement** phases. Every new system compromised is leveraged to reach the next, eventually reaching critical data stores. In a real 2011-style breach, lack of network segmentation allowed an attacker who owned a single server to roam freely across Sony's network

Exfiltration & Impact: After collecting sensitive data, the attacker exfiltrates it out of CPC's network. The attacker dumping database tables to CSV files and compresses it to ZIP for exfiltration. They then use HTTP to send the files to an external server under their control (MITRE **T1041: Exfiltration Over C2 Channel**). To avoid detection, the data might be sent in chunks or over an encrypted tunnel. Finally, as an impact, the attacker should delete logs. In our simulation, the breach results in a major data leak of customer info

Detection & Response: This attack highlights multiple opportunities for a Blue Team to detect or block the intrusion. In the Recon stage, a web application firewall could block the SQL injection payloads, preventing exploitation. During exploitation, the sudden massive SQL data extraction should trigger an alert (unusual volume or use of system tables). Likewise, the web server spawning a command shell process is a red flag an EDR agent

could catch. As per OWASP best practices, proper input sanitization or use of prepared statements would have mitigated the injection entirely.

Once the attacker is on a server, monitoring for **privilege escalation** behaviors is crucial – these can be detected by host-based intrusion detection. Lateral movement might be caught by the anomaly of a DMZ server initiating connections deep into the internal network (which is unusual in a properly segmented network).

Finally, large outbound data transfers of sensitive data outside normal business hours could be spotted by Data Loss Prevention systems. In the PSN breach, Sony was criticized for failing to detect the intrusion for days. A well-prepared Blue Team at CPC would correlate these signals and respond rapidly – isolating affected servers and expelling the attacker before the **exfiltration** stage. Robust logging and an incident response plan are key to limiting damage.

Simulation 2: CPC Mail Server

Reconnaissance: The attacker (APT **Hafnium** simulation) scans for CPC's email server. CPC's infrastructure includes an on-premises Exchange server (ex : mail.cpc.com) exposed to the internet for Outlook Web Access. Using **Shodan**, the attacker finds an Exchange server running a version vulnerable to the *ProxyLogon* exploit. They perform reconnaissance on DNS records to discover the OWA endpoint and use HTTPS probes to confirm the Exchange version. This aligns with MITRE **T1595: Active Scanning** of external services.

Initial Exploitation (ProxyLogon): The attacker launches the **ProxyLogon exploit chain** against CPC's Exchange server, taking advantage of multiple CVEs. First, an **SSRF** vulnerability (CVE-2021-26855) is used to bypass authentication and impersonate an admin on the Exchange **ECP** web panel. This OWASP Top 10 issue (**A10:2021 – SSRF**) allows the attacker to send specially crafted HTTP requests that the Exchange server treats as internal, granting the attacker privileged access without valid credentials. Next, the attacker leverages a **post-authentication file write** vulnerability (CVE-2021-27065) to upload a web shell onto the Exchange server's www directory. This effectively gives remote code execution as SYSTEM on the Exchange box (**T1190: Exploit Public-Facing Application** and **T1505.003: Webshell on server**). The tool for this step is a **Metasploit module** automating the exploit chain. In real Hafnium attacks, once the webshell was planted, attackers had full control of Exchange and thus a beachhead in the network

Persistence: With a webshell installed, the attacker attains persistent access to the Exchange server. Even if CPC applies emergency patches after that, the webshell remains on disk ready to be used. The attacker may also create new user accounts or add a hidden Exchange admin. Because the Exchange server is now effectively under attacker control, they could utilize built-in services for persistence – for example, registering a malicious **Service** or backdooring an Exchange transport agent (malicious DLL). However, the webshell itself is sufficient: it allows the attacker to issue commands at will. In our simulation, the attacker created a new domain user "exchhelp" added to the Exchange Organization Management role, which provides an alternative login path if the webshell gets removed

Privilege Escalation: Compromising Exchange often means **instant SYSTEM privileges** on that server (since the web service runs as high-privilege). The next goal is to become Domain Admin. Exchange servers have high privileges in AD by design, and the attacker exploits this. One approach: use **LSASS dumping** to grab credentials. The attacker runs **Mimikatz** via the webshell to dump the memory of the LSASS process (MITRE **T1003.001: LSASS Memory**). This yields password hashes and Kerberos tickets. Suppose they extract the hash of a domain admin who recently logged into the Exchange (or the machine account of Exchange, which might be part of Exchange Trusted Subsystem group). They can then perform a **Pass-the-Hash** or use the `sekurlsa::logonpasswords` output from Mimikatz to get cleartext creds. At this point, the attacker obtains Domain Admin privileges.

Lateral Movement: Using the newly gained credentials, the attacker moves laterally through CPC's network. The Exchange server itself is in the internal network segment, so from there the attacker can reach file servers, the domain controller, etc. They may deploy a full **Cobalt Strike** beacon or another C2 agent for more flexible control (MITRE **C2** tactic). Using **SMB** to execute commands on other servers (MITRE **T1021.002**). For instance, the attacker might run `psexec` with Domain Admin rights to push a payload into an HR application server. They enumerate sensitive systems: perhaps CPC's internal research database or financial records server. In the hypothetical worst case, the adversary could even deploy **ransomware** across the environment once domain admin is obtained. In our simulation, after escalating, the attacker quietly installed **backdoors on the domain controller**.

Exfiltration & Impact: The primary objective observed in the real Hafnium attacks was **data theft** – specifically stealing email contents. In CPC's simulation, the attacker uses Exchange's own management shell to export mailboxes. They run PowerShell cmdlets (via the webshell or a remote PowerShell session) to export mailbox data to PST files. For example, they might use the **New-MailboxExportRequest** cmdlets, which dump users' emails to files on the server. These files are then compressed, and archives (containing executive emails or R&D data) are then exfiltrated. The attacker could exfil via the webshell (downloading the files through an HTTPS session) or use a tool like **PowerCat** to transfer data to a remote host. (In our case, they opened a connection to a cloud server controlled by them, tunneling the data out.) All of this happens over **HTTPS**, blending in with normal traffic (MITRE **T1041**). The impact is a major **data breach** – intellectual property and confidential communications are now in adversaries' hands. Additionally, having Domain Admin, the attacker could have deployed destructive malware. We simulate that the red team stops short of actual ransomware deployment, but notes that this access could enable a **ransomware event** or further sabotage. This dual possibility is noted by security researchers: an Exchange breach can escalate to full domain ransomware deployment if not caught.

Detection & Mitigation: Detecting the Exchange attack requires monitoring both the application layer and post-exploitation behavior. Early on, one clue is unusual log entries in Exchange HTTP logs (ex : an admin session to ECP with no corresponding login). A WAF could also have mitigated the SSRF by blocking unexpected headers or internal server requests. Once the webshell is dropped, defenders could catch it by **file integrity monitoring** on Exchange directories (an unknown .aspx file appearing in `/owa/` directory). If the attacker attempts to dump LSASS, EDR systems can detect this. Network-wise, the

Blue Team might notice the Exchange server making unusual external connections (it normally shouldn't send data to random IPs).

To **block** this attack in the first place, **patching** is critical (ProxyLogon was a known bug by March 2021, so applying updates would stop the exploit). Short of patching, Microsoft's one-click mitigation tool or a proxy rule to block `/ecp` requests would dramatically reduce risk. From an OWASP perspective, the root cause was running vulnerable software (OWASP 2017 A9 and 2021 A06). A robust patch management and virtual patching approach (WAF rules for example) would align with best practices. Blue Teams should also perform threat hunting: after patches, look for created webshells or new accounts. In summary, network defenders can detect this attack at multiple stages – but only if logging and monitoring are in place. Defense-in-depth (with network detection, host EDR, and identity monitoring) is crucial because zero-day exploitation is hard to prevent at the door. Once an Exchange is breached, catching the attacker's **post-exploitation** actions (credential dumping, lateral movement, mailbox exports) is the last line of defense to prevent full domain compromise.

7. Recommendations & Countermeasures

For PSN-type Attacks

- Enforce WAF to mitigate SQLi
- Salted + hashed passwords (bcrypt/Argon2)
- Strict access control between databases and public servers
- DevSecOps with static code analysis (like SonarQube)

For Hafnium-style Zero-days

- Mandatory VPN before Exchange web access
- Enforce patch management policies
- Implement anomaly detection for webshell behavior (Defender for Endpoint)
- Consider migrating to cloud-based email (O365 with Defender ATP)

8. Cost Analysis

Implementing the above recommendations will require investments in technology, services, and time. Below is a breakdown of the estimated costs and a suggested timeline for execution. All costs are approximate, in USD, and should be refined with quotes from vendors and consultation with CPC's finance department.

8.1 Replacement & Implementation Costs: *(Hardware/Software procurement and deployment)*

- **Web Application Firewall** : ~\$20,000/year (including license and support) for an enterprise-grade WAF appliance or cloud service. Initial deployment professional service: \$5,000.
- **Next-Gen Firewall Upgrade**: If replacing or upgrading firewall devices, estimated \$15,000 per firewall appliance (mid-sized enterprise model) – likely two devices for high availability = \$30,000. Plus \$5,000 for installation services.
- **Endpoint Detection & Response Solution**: Approximately \$60 per endpoint/year. For ~500 endpoints (including servers and PCs) = \$30,000/year. Plus one-time setup fee \$5,000 (vendor or integrator assistance).
- **Email Security Gateway/ATP**: If cloud-based (e.g., Microsoft 365 Defender or Proofpoint), approx \$3/user/month. For 500 users ~ \$18,000/year.
- **Privileged Access Management System**: Can range widely. A baseline PAM for 50 privileged accounts might be ~\$25,000 for software and deployment. Alternatively, using cloud PAM services could be subscription (e.g., \$10,000/year).
- **Multi-Factor Authentication** : If CPC uses something like Duo or a built-in Microsoft Azure AD MFA: Duo approx \$3/user/month = \$18,000/year for 500 users. Hardware tokens (if needed for some) ~\$50 each. We budget \$5,000 for token purchases and \$15,000/year for the MFA service.
- **SIEM Solution**: If on-prem Splunk: license ~\$1500 per ingest GB/day. Assuming CPC logs would be ~5 GB/day, that's ~\$7,500/year plus infrastructure. Cloud SIEM like Azure Sentinel might be ~\$4,000/month for similar volume = \$48,000/year. We estimate initial SIEM setup (including maybe a SIEM engineer contract) \$10,000.
- **Network Segmentation Hardware**: Possibly additional switches or firewall modules for segmentation: allocate \$10,000 for network re-architecture (VLAN setups, perhaps new switch for DMZ).
- **Backup System Upgrade**: Implementing immutable backup storage – e.g., a cloud backup subscription or new appliance: \$15,000 (could be a one-time for an appliance or yearly for cloud storage depending on approach). Tapes and tape drive if chosen: \$8,000 initial plus offsite storage service \$2,000/year.

- **Misc Software (Vulnerability scanner license, upgraded anti-malware, etc.):** \$10,000/year combined.

8.2 Professional Services Costs:

- **Red Team Engagement (this simulation):** *If this were an external service:* typically ~4 weeks of work for a team of 2-3. At an average rate of \$200/hour, and ~400 hours total = **\$80,000**
- **Incident Response Readiness Service:** We recommend a one-time engagement with a security firm to refine CPC's incident response plan and playbooks (with focus on ransomware). Estimated at 40 hours at \$250/hour = **\$10,000**.
- **Security Awareness Training Provider:** If using an external platform for phishing simulations and training modules, ~\$5,000/year.
- **Implementation Services:**
 - *Network Segmentation Project:* Hiring a network engineer consultant for design and config – e.g., 80 hours at \$150/hour = **\$12,000**.
 - *EDR Deployment Assistance:* Vendor or MSP could assist 40 hours at \$200/hr = **\$8,000** (if needed, or internal IT can handle if trained).
 - *SIEM Use Case Development:* 60 hours of a security analyst at \$150/hr = **\$9,000** to set up initial correlation rules and dashboard.
 - *Zero Trust Architecture Advisory:* Possibly engage a consultancy to roadmap Zero Trust implementation (could be part of existing security partner services). Budget a workshop + design at **\$15,000**.
- **Penetration Testing (annual going forward):** To ensure continued security, budget for annual red team or pentest at ~\$50,000 each year

8.3 Execution Timeline:

- **Immediate (0-1 month):**
 - Patch all critical systems (Exchange, web server) – within days.
 - Implement emergency MFA on VPN/RDP (can do in weeks).
 - Deploy critical EDR sensors on key servers (even if full rollout takes longer).

- Remove known malware/web shells from systems, change all admin passwords (remediation from simulation).
- Begin network isolation of high-value assets (as a stop-gap, even manual ACLs).
- Hire necessary contractors/partners for upcoming projects.
- **Short-Term (1-3 months):**
 - Deploy EDR to all endpoints and servers (month 1-2).
 - Install and tune WAF for the web portal (month 1).
 - Set up new NGFWs and reconfigure network into VLANs/DMZ segments (month 1-3, phased by segments).
 - Enforce MFA for all users (roll out by month 2).
 - Implement enhanced email filtering solution (month 2).
 - Conduct staff training refresher, especially on phishing and incident reporting (month 2).
 - Kick off SIEM deployment: start log collection by the end of month 3.
 - Establish offline backups for critical data (month 2).
 - Address easy config fixes: lock down PowerShell, apply GPO hardening, disable unnecessary services (continuous through month 1-3).
- **Medium-Term (4-6 months):**
 - Fully implement Privileged Access Management and separate admin workstations (by month 4).
 - Complete SIEM use-case tuning and have SOC monitoring (month 4-5, perhaps using managed service if needed).
 - Zero Trust pilot: implement ZTNA for remote access as a pilot (month 4-6).
 - Microsegmentation solution evaluation and possibly pilot in one environment (month 5-6).
 - Perform a follow-up penetration test or at least a vulnerability scan to verify improvements (month 6).

- Fine-tune incident response plan with a simulation exercise (like a tabletop for ransomware scenario).
- **Long-Term (6-12 months):**
 - Gradually enforce network segmentation down to finer levels (this can take time to adjust applications).
 - Expand Zero Trust principles across more applications and infrastructure (e.g., implement device compliance enforcement).
 - Continue migrating any legacy on-prem services to more secure cloud options if feasible (for instance, consider moving Exchange to Microsoft 365 which could have prevented the ProxyLogon scenario entirely).
 - Achieve a mature steady state where all recommended security controls are in operation and monitored.
 - Plan for continuous improvement: schedule regular (at least annual) security assessments, and maintain an ongoing security awareness program.

Total Estimated Costs (Year 1): The first-year investment could be on the order of **\$200,000 - \$250,000**. Yearly recurring costs (licenses, subscriptions, maintenance) might be around **\$100,000**. This is a significant investment, but considering the potential cost of a breach or ransomware incident (which can run into **millions**, not counting reputational damage), it is justified. For perspective, the Sony breach cost was enormous in customer fallout and fines, and CHSF likely incurred heavy recovery costs and government aid for cybersecurity upgrades. Investing proactively is **far cheaper than suffering a successful attack**.

References

Sony Data Breach: What Happened and How to Prevent It

<https://www.strongdm.com/what-is/sony-data-breach>

The 2011 PlayStation Network Hack – What Actually Happened?

<https://wsswired.com/4837/entertainment-3/the-2011-playstation-network-hack-what-actually-happened/>

Sony PlayStation Network Data Breach: What & How It Happened?

<https://www.twingate.com/blog/tips/Sony%20PlayStation%20Network-data-breach>

2011 PSN Hack Documentary: How Sony Failed Their Customers

<https://www.youtube.com/watch?v=oBflgU5ComI&t=287s>

wsswired.com (2021) The 2011 PlayStation Network Hack – What Actually Happened?

<https://wsswired.com/4837/entertainment-3/the-2011-playstation-network-hack-what-actually-happened/>

BBC News. (2011). *Sony's PlayStation Network hacked.*

<https://www.bbc.com/news/technology-13192359>

CISA. (2021). *Joint Cybersecurity Advisory: Microsoft Exchange Server Vulnerabilities.*

<https://www.cisa.gov/>

Le Parisien. (2022). *Corbeil-Essonnes: une attaque informatique paralyse le CHSF.*

<https://www.leparisien.fr/recherche/?query=attaque+informatique+CHSF>

Microsoft. (2021). *HAFNIUM targeting Exchange Servers with 0-day exploits.*

<https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/>

MITRE. (2024). *MITRE ATT&CK® for Enterprise – Tactics and Techniques.*

<https://attack.mitre.org/>

Numerama. (2022). *Ce que l'on sait de l'attaque contre l'hôpital de Corbeil-Essonnes.*

<https://www.numerama.com/cyberguerre/1109782-hopital-pirate-de-corbeil-essonnes-on-connaît-le-nom-du-coupable.html>

OWASP. (2023). *Top 10 Web Application Security Risks.* Retrieved from

<https://owasp.org/www-project-top-ten/>

US-CERT. (2021). *Microsoft Exchange Server Vulnerabilities - Alert AA21-062A.*

<https://us-cert.cisa.gov/ncas/alerts/AA21-062A>

Wikipedia. *PlayStation Network outage*

https://en.wikipedia.org/wiki/PlayStation_Network_outage

Wikipedia (2023). *Cyberattaque du Centre hospitalier Sud Francilien*
https://fr.wikipedia.org/wiki/Centre_hospitalier_sud_francilien#Cyberattaque

Zataz. (2022). *LockBit revendique l'attaque contre l'hôpital de Corbeil-Essonnes*.
<https://www.zataz.com/>

Microsoft Exchange ProxyLogon Remote Code Execution Exploit
vulners.com