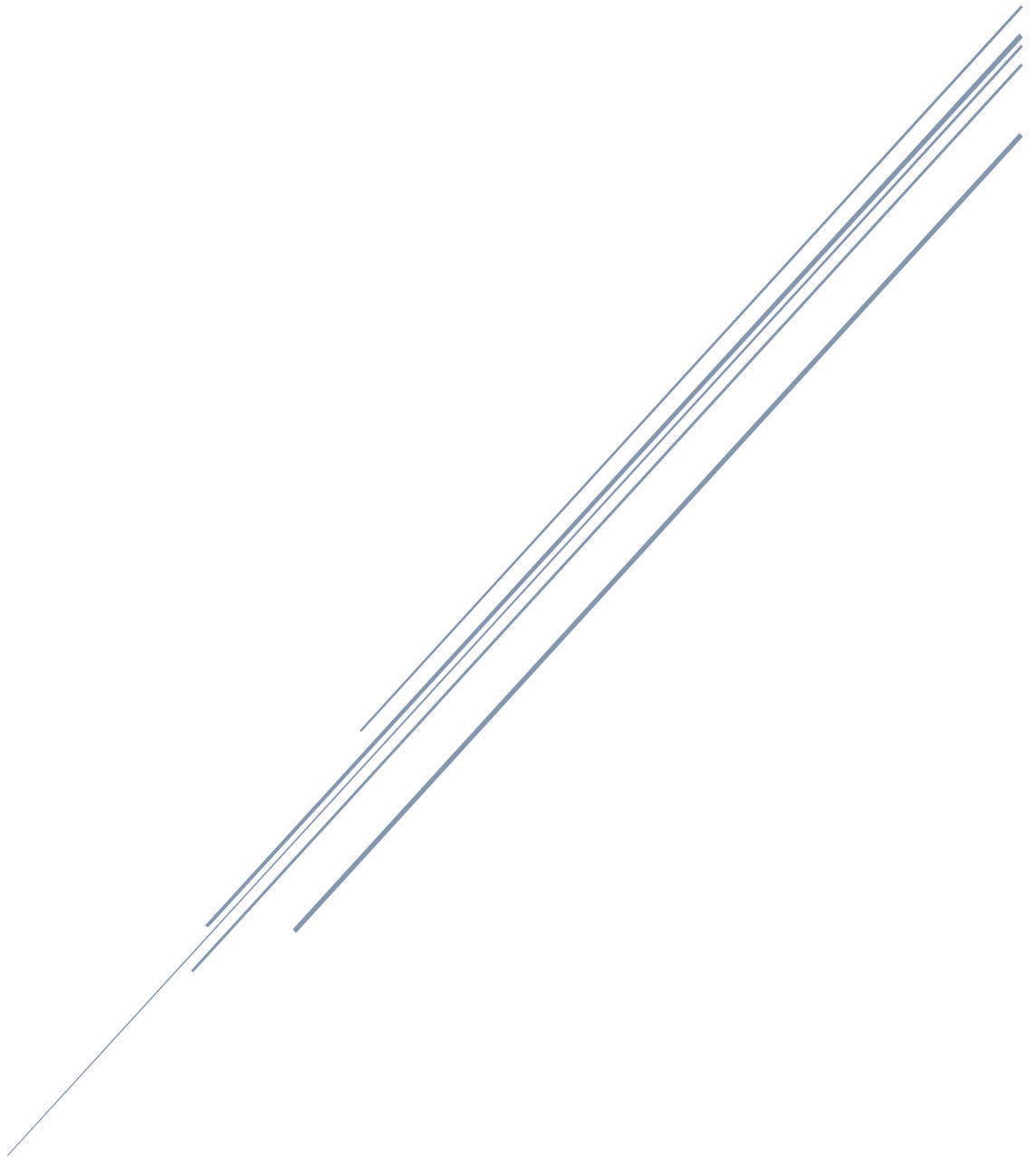


CYBERSECURITY RESEARCH AND SIMULATION



UWTSD Swansea
Ethical Hacking

Contents

Research and documentation	2
Cyberattack on Université Paris-Saclay	2
Context of the attack.....	2
Analysis of the attack	2
Preventive measures.....	2
Contec CMS800 Patient monitor – Insecure design issue.....	4
Context and discovery.....	4
Technical analysis	4
Potential impacts	4
Recommendations for mitigation	4
Cyberattack on Free – Data breach targeting Freebox and Free Mobile subscribers	6
Context of the attack.....	6
Analysis of the attack	6
Preventive measures.....	6
References.....	8
Security testing simulation.....	0
Design of the infrastructure	0
Assumptions.....	0

Research and documentation

In this part, we will focus on two cyberattacks, and one cybersecurity issue. The following case will allow us to analyse the strategies that can be used by cybercriminals, the possible consequences of these attacks, and to formulate recommendations for better defence in the future.

Cyberattack on Université Paris-Saclay

Context of the attack

In August 2024, the ANSSI was notified by Université Paris-Saclay that it had been targeted by a cyberattack. The attack was carried out using the “White Rabbit” ransomware. Additionally, one terabyte of data was stolen. In October 2024, the RansomHouse group claimed the attack.

It impacted the university's operations, disrupting administrative services, research systems, and internal communications. The cost of expenses related to the cyberattack was estimated at €2.6 million in December 2024, according to AEF info. This estimate was confirmed by the president of Université Paris-Saclay, Camille Galap.

Analysis of the attack

After extensive research, no official report detailing the specifics of the attack has been found as of today. Consequently, we will draw from similar attacks to gain insights into the probable methods and strategies employed.

The attackers likely gained initial access to the university's systems through targeted phishing campaigns or by exploiting unpatched vulnerabilities. Following this initial compromise, traces of Cobalt Strike commands found in other White Rabbit attacks suggest that the attackers used this tool for post-exploitation activities, such as reconnaissance and lateral movement within the network.

Once inside the network, the attackers would have deployed the White Rabbit ransomware payload, a small (approximately 100 KB) and discreet binary file. This payload remains inactive without a specific command-line password, allowing it to avoid early detection while enabling malicious actions once activated.

When activated, White Rabbit first terminates several processes and services, particularly those related to antivirus and security programs, to minimize the chances of detection and interruption. With system defences weakened, the ransomware proceeds to encrypt files across fixed, removable, and network drives. It deliberately avoids critical system paths and specific file types to prevent system instability and ensure its ransom notes are preserved. Encrypted files are appended with the ".script" extension, while each affected file is accompanied by a ransom note named after the original file with the ".script.txt" extension.

Following the encryption, White Rabbit employs a double extortion strategy. In addition to encrypting the data, the attackers threaten to publish or sell the stolen information if the ransom is not paid, thereby increasing the pressure on the victims to comply.

Preventive measures

To reduce the risk of these incidents, public university should consider the following actions:

- Providing training sessions or self-paced modules — like the Phishing Quiz created by Jigsaw in partnership with Google — can help users develop their ability to analyse emails. Additionally, conducting regular simulated phishing campaigns would help maintain user vigilance and reinforce their reflexes when confronted with attack attempts. These measures would significantly reduce the risk of phishing attacks.

- To minimize the impact of a potential breach, enforcing strict access controls based on the principle of least privilege is essential. This principle restricts users' access to only the resources necessary for their roles, thereby limiting the potential damage from compromised accounts. If access controls are not properly enforced, attackers can move laterally within the network, escalating privileges and gaining access to sensitive information. By applying least privilege, organizations reduce the chances of an attacker exploiting excessive permissions to escalate their actions.
- Deploying Intrusion Detection Systems (IDS) is another critical recommendation to identify malicious activities early on. IDS continuously monitors network traffic in real time, detecting suspicious patterns or potential intrusions. Early detection allows organizations to respond quickly and contain threats before they escalate. Without an IDS, malicious activities may go unnoticed, giving attackers ample time to inflict damage or exfiltrate sensitive data. By using IDS, organizations can detect and respond to threats in a timely manner, minimizing the potential impact.
- Finally, to ensure data availability and support rapid recovery in the event of an attack, it is crucial to perform regular backups of critical data and securely store them off-site. In case of a ransomware attack or system compromise, having secure, up-to-date backups ensures that critical information can be restored quickly, minimizing downtime. Without reliable backups, organizations risk losing important data, which could result in severe operational disruptions or permanent data loss. By implementing a robust backup strategy, organizations can ensure continuity of operations even after a security incident.

Contec CMS800 Patient monitor – Insecure design issue

Context and discovery

In January 2025, the Cybersecurity Infrastructure and Security Agency (CISA), with the Food and Drug Administration (FDA), issued an alert concerning the CONTEC CMS8000 patient monitor and its variants. The devices were suspected of containing a hidden backdoor communicating with a Chinese IP address, raising concerns about potential security risks.

Further research conducted by Team82, a cybersecurity group from Claroty, revealed that the situation was more nuanced. Their findings suggested that the flaw was not a malicious backdoor but rather an insecure design choice, introducing significant vulnerabilities into hospital networks.

Technical analysis

Team82 acquired a CMS8000 device and analysed its firmware. Their investigation revealed that the patient monitor was preconfigured to communicate with a specific IP address over the network for central management operations and firmware updates. This address is publicly routable, meaning anyone can usurp it.

Key findings include:

- The device's manual explicitly instructs users to configure the monitor to use the hardcoded IP, implying no attempt at concealment.
- Firmware updates involve connecting to this IP via the NFS (Network File System) protocol, an inherently insecure method if exposed to external networks.
- The update mechanism can only be triggered manually at boot by pressing a physical button, reducing remote exploitation risks but not eliminating them.
- Despite the apparent lack of malicious intent, this design flaw opens pathways for man-in-the-middle attacks and potential compromise of patient data or system functionality.

On February 25, 2025, CISA updated its advisory, assigning the vulnerability CVE-2025-1204, categorizing it as a hidden function vulnerability in the update mechanism of the affected devices.

Potential impacts

Although there is no direct evidence of malicious exploitation, the design flaw presents critical risks:

- Unauthorized modification of firmware could lead to inaccurate monitoring or device malfunction, endangering patient safety.
- Leakage of sensitive health information (PHI) to unauthorized external servers.
- Compromise of hospital internal networks if the device is connected without proper segmentation.

Recommendations for mitigation

To mitigate the identified risks, healthcare organizations using CONTEC CMS8000 monitors should consider the following actions:

- Isolate medical devices like patient monitors on dedicated network segments, preventing lateral movement in case of compromise.
- Block all outbound traffic from the device to public IP addresses unless explicitly necessary and approved.

- Regularly inspect and, if possible, replace firmware with versions that do not use hardcoded external IPs.
- Pressure vendors to redesign the network communication features, adhering to secure update mechanisms and proper use of private network addresses.
- Since triggering the update requires physical access, ensuring physical security controls in sensitive areas can prevent unauthorized firmware tampering.

This case highlights the importance of rigorous cybersecurity evaluation for medical devices, even when the risk stems from poor engineering practices rather than deliberate malicious intent.

Cyberattack on Free – Data breach targeting Freebox and Free Mobile subscribers

Context of the attack

In late October 2024, the French telecom operator Free, the second-largest Internet Service Provider (ISP) in France, publicly confirmed it had fallen victim to a cyberattack targeting its customer data systems. The breach affected both Freebox and Free Mobile subscribers. On October 26, Free filed a formal complaint with the French judiciary and notified relevant regulatory authorities, including the CNIL.

The scope of the attack remains uncertain, but a hacker using the alias “Drussellx” posted a sample of the stolen database on BreachForums, claiming to possess data on more than 19.2 million users. The leaked data quickly circulated on cybercriminal forums, raising significant privacy and security concerns for millions of French citizens.

Analysis of the attack

At the time of writing, Free has not disclosed detailed technical information about the method of intrusion. However, independent cybersecurity researchers and news outlets suggest the breach may have been enabled by a vulnerability in a back-office tool used to manage customer information.

The hacker did not encrypt systems or use ransomware, but instead exfiltrated a large volume of customer data. No passwords, banking information, or communication content (SMS, calls, emails) were part of the breach, according to Free’s initial findings.

This incident does not follow the traditional ransomware double-extortion model, but rather a data leak with extortion potential, as the attacker offered the data for sale and implied potential consequences for Free if they failed to respond. Despite the absence of direct service disruption, the exposure of sensitive personal data represents a severe threat to customer privacy and trust.

Preventive measures

To reduce the risk of similar incidents in the future, organizations handling large volumes of customer data should consider the following measures:

- Ensure all internal tools, particularly those handling customer records, are developed following secure coding practices and are regularly audited for vulnerabilities. Failure to do so allows attackers to exploit outdated systems or misconfigured access rights.
- Sensitive customer information should be encrypted both at rest and in transit. Furthermore, organizations should adopt a data minimization approach, retaining only the information necessary for operations. This reduces the attractiveness of targets and mitigates impact in case of a breach.
- Advanced Security Information and Event Management (SIEM) systems can monitor access patterns to sensitive databases. Unusual data export behaviour, such as large queries by non-administrators or off-hour access attempts, should trigger alerts and investigations.
- Implementing Zero Trust principles can prevent lateral movement and privilege escalation within the network. Access to critical systems should require multi-factor authentication and be tightly controlled with role-based permissions.
- In the event of a breach, prompt and transparent communication with affected users is critical. Free’s response included a legal complaint and communication with regulators, but offering identity monitoring or credit protection to customers could help mitigate the consequences and restore trust.

By combining strong technical controls, real-time monitoring, and clear communication protocols, organizations can significantly reduce both the likelihood and impact of large-scale data breaches like the one experienced by Free.

References

- [1] D. Leloup and S. Le Nevé, "La cyberattaque de Paris-Saclay revendiquée par le groupe RansomHouse," *Le Monde*, 15 10 2024. [Online]. Available: https://www.lemonde.fr/pixels/article/2024/10/15/la-cyberattaque-de-paris-saclay-revendiquee-par-le-groupe-ransomhouse_6352459_4408996.html. [Accessed 20 March 2025].
- [2] A. Dela Cruz, B. M. Ebriega, D. O. Ladores and M. Yambao, "New Ransomware Spotted: White Rabbit and Its Evasion Tactics," 18 January 2022. [Online]. Available: https://www.trendmicro.com/fr_fr/research/22/a/new-ransomware-spotted-white-rabbit-and-its-evasion-tactics.html. [Accessed 20 April 2025].
- [3] ANSSI, "CYBER THREAT OVERVIEW 2024," February 2025. [Online]. Available: <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-004.pdf>. [Accessed 19 March 2025].
- [4] CISA, "Contec CMS8000 Contains a Backdoor," 30 January 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/2025-02/fact-sheet-contec-cms8000-contains-a-backdoor-508c_0.pdf. [Accessed 27 April 2025].
- [5] MITRE, "CVE-2025-1204," 10 February 2025. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-1204>. [Accessed 27 April 2025].
- [6] Université Paris Saclay, "FAQ piratage," [Online]. Available: <https://www.universite-paris-saclay.fr/piratage>. [Accessed 12 April 2025].
- [7] S. Piovezan, "Cyberattaque à Saclay : "Dans la période actuelle, il faut sécuriser nos données, notamment scientifiques"," *AEF Info*, 6 March 2025. [Online]. Available: <https://www.aefinfo.fr/depeche/726755-cyberattaque-a-saclay-dans-la-periode-actuelle-il-faut-securiser-nos-donnees-notamment-scientifiques-c-galap>. [Accessed 20 April 2025].
- [8] D. Bancal, "Fuite de données pour FREE mobile et FreeBox ?," *ZATAZ*, 22 October 2024. [Online]. Available: <https://www.zataz.com/fuite-de-donnees-pour-free-mobile-et-freebox/>. [Accessed 23 April 2025].
- [9] S. Gatlan, "Free, France's second largest ISP, confirms data breach after leak," *Bleeping Computer*, 28 October 2024. [Online]. Available: <https://www.bleepingcomputer.com/news/security/free-frances-second-largest-isp-confirms-data-breach-after-leak/>. [Accessed 23 April 2025].
- [10] Team82, "Do the CONTEC CMS8000 Patient Monitors Contain a Chinese Backdoor? The Reality is More Complicated...," *Claroty*, 2 February 2025. [Online]. Available: <https://claroty.com/team82/research/are-contec-cms8000-patient-monitors-infected-with-a-chinese-backdoor-the-reality-is-more-complicated>. [Accessed 27 April 2025].
- [11] S. Jain, "France's Free Cyberattack Exposes User Data," *The Cyber Express*, 29 October 2024. [Online]. Available: <https://thecyberexpress.com/free-cyberattack-confirmed/>. [Accessed 24 April 2025].
- [12] Le Monde with AFP, "Free porte plainte après une cyberattaque sur les données personnelles de ses abonnés, dont l'ampleur reste inconnue," *Le Monde*, 26 October 2024. [Online]. Available: <https://www.lemonde.fr/pixels/article/2024/10/26/free-porte-plainte-apres-une->

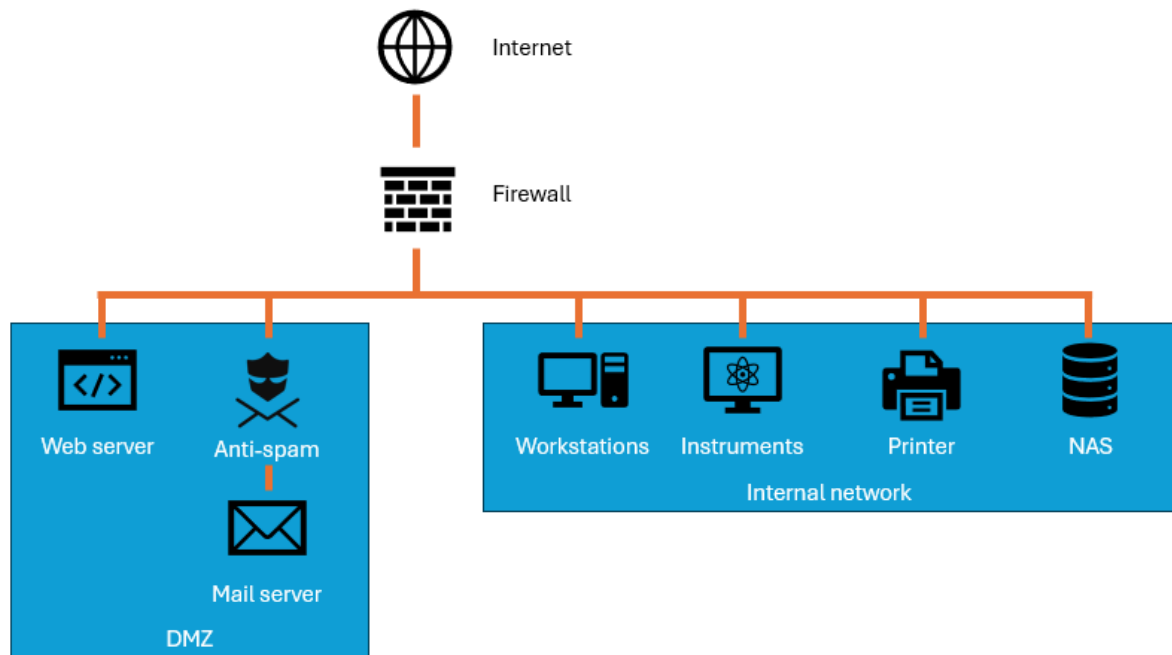
cyberattaque-sur-les-donnees-personnelles-de-ses-abonnes-dont-l-ampleur-reste-inconnue_6360440_4408996.html. [Accessed 23 April 2025].

Security testing simulation

In this part, we will assume that we are performing a penetration testing on a replicated environment, as a Red Team Specialist employed by Cureton Pharmaceutical Company (CPC)

Disclaimer: Due to limited resources on my computer, I will not be able to run virtual machines.

Design of the infrastructure



Assumptions

1. The firewall is well configured, with integrated IDS
2. The NAS contains the vaccine
3. No segmentation in the internal network
4. Workstation are on Windows 11
5. An employee will open the reverse shell file which is in a trapped email

Cureton Pharmaceutical Company (CPC)

Pentest report

Ethical Hacking

Nicolas Hing (2422991)
03/05/2025

Table of content

Table of content	1
Introduction	2
List of acronyms	3
Detailed contingency policy	4
Purpose	4
Scope	4
Pre-test measures.....	4
Emergency protocols	5
Ethical considerations.....	5
Selection of penetration testing framework	6
Reasons for choosing PTES	6
PTES phases utilized on this mission	6
Selection of penetration testing tools.....	7
Explanation of simulated attacks.....	7
Recommended solutions for discovered threats.....	11
Solution cost.....	14
Cost of replacing software and hardware	14
Solution implementation cost.....	14
Execution schedule and professional services invoice	16
Solution execution schedule.....	16
References	18

Introduction

Cureton Pharmaceutical Company (CPC) is actively developing a new vaccine for respiratory viruses. The competition in this field is intense, and as CPC gets closer to a breakthrough, any data breach or loss could have serious consequences.

Nowadays, cyberattacks are rising rapidly, often aiming to steal sensitive data or demand ransom. In response to these growing threats, CPC has tasked its internal Red Team with simulating a cyberattack to identify vulnerabilities and strengthen system security before real-world attackers can exploit them.

List of acronyms

DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MFA	Multi-Factor Authentication
NAC	Network Access Control
NAS	Network Attached Storage
OSINT	Open-Source Intelligence
PTES	Penetration Testing Execution Standard
SMB	Server Message Block
SPF	Sender Policy Framework
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network

Detailed contingency policy

As this penetration test is conducted entirely within a simulated environment, hosted theoretically on a virtualized infrastructure, there are no direct risks to a production environment, user data, or operational continuity. Nevertheless, to uphold best practices and simulate real-world operational standards, the following contingency policy is defined.

Purpose

This contingency policy aims to outline precautionary measures and response procedures that would typically be followed in a real-world penetration testing scenario. Although the current test is purely simulated, this framework demonstrates responsible planning and professional methodology.

Scope

The penetration test focuses on a virtual replica of Cureton Pharmaceutical Company's (CPC) network architecture, including:

- Mail server in the DMZ
- Internal network with workstations and NAS
- Simulated user behaviour (e.g., email interactions)

No actual hardware, employees, or production data are involved.

Pre-test measures

Item	Description
Data protection	No real data is used; no backups are necessary.
Stakeholder notification	No real stakeholders involved; this is a solo simulation.
System stability	All test environments are isolated; no real impact possible.
Logging and monitoring	Actions during the simulated penetration testing will be logged for reporting and traceability.
Attack scope and limits	The test will simulate attacks including phishing, reverse shells, and internal file access without privilege escalation. No actions targeting availability (DoS) or persistent threats will be performed.

Emergency protocols

Given the theoretical nature of the simulation:

- No real-time response team is required
- No rollback plans are necessary
- No alerts will be triggered.

However, all attack steps will be documented, and hypothetical response procedures will be discussed in the final report.

Ethical considerations

Although no live systems are affected, ethical standards are followed:

- No data exfiltration of real content.
- No unapproved persistence or privilege escalation simulated.
- The scenario remains educational and demonstrative.

Selection of penetration testing framework

In the penetration testing of Cureton Pharmaceutical Company's (CPC) infrastructure, the Penetration Testing Execution Standard (PTES) framework was selected. This standardized framework provides a structured and methodical approach for vulnerability assessment and attack simulation.

Reasons for choosing PTES

The PTES framework was chosen for the following reasons:

- Comprehensive methodology: PTES cover all the necessary phases of a penetration test-from an initial reconnaissance to final report writing.
- Adaptability: This approach can be customized to CPC's particular constraints and requirements.
- Professional recognition: PTES is recognized in the cybersecurity sector as a quality measure.
- Detailed documentation: The framework encourages rigorous documentation throughout, which is essential in a penetration test report.

PTES phases utilized on this mission

Information gathering: Passive reconnaissance using DNSRecon and Google/LinkedIn searches to uncover employee domains and email addresses.

- Threat analysis: Determination of likely attack vectors.
- Vulnerability analysis: Port scanning and detection of possible vulnerabilities.
- Exploitation: Attempts to send emails with malicious payloads.
- Post-exploitation: Attempts to create reverse shell connections.
- Reporting: Detailed documentation of results and recommendations.

Selection of penetration testing tools

To carry out this attack simulation on CPC's virtual infrastructure, several specialized tools were selected depending on the test phases and the objectives targeted.

Recognition tools

- DNSrecon: DNS enumeration tool
Identify sub-domains and information exposed publicly

Scanning tools

- Nmap: Port scanner
Mapping the network infrastructure
- Shodan: Passive port scanner
Find open port from outside

Explanation of simulated attacks

A. List of targeted vulnerabilities

1. Exposure of sensitive Information: Attempt to extract information via DNS and open lookups
2. Firewall configuration weaknesses: Scanning for open or poorly protected ports
3. Lack of employee awareness: Targeting by phishing to gain initial access
4. Lack of network segmentation: Potential exploitation to access sensitive data on the NAS

B. Attack tools used

Attack phase	Tools used	Objective
Reconnaissance	DNSrecon	Discover domains and subdomains associated with CPC
Scanning	Nmap (ICMP scan, SYN scan, stealth scan)	Identify open ports and accessible services
OSINT research	Google, LinkedIn	Collect employee email addresses
Payload creation	Metasploit framework	Generate a reverse shell to establish access
Antivirus evasion	Veil-Evasion	Encrypt the payload to bypass security protections

C. Protocols involved in the attack

Protocol	Usage in the attack
DNS	Reconnaissance of domains and subdomains
ICMP	Scanning to detect active hosts
TCP	SYN scan to identify open ports

D. Attack launching

Phase 1: Reconnaissance

1. DNS Analysis using DNSrecon

```
'dnsrecon -d cureton-pharma.com -t std'
```

Result: Limited information obtained, mainly the company's public-facing website.

2. Employee Information Gathering

Used LinkedIn to identify CPC employees.

Email format discovered: firstname.lastname@cureton-pharma.com

Phase 2: Network scanning

1. Passive port scanning with Shodan

2. ICMP scan

```
'nmap -sn -PE cureton-pharma.com'
```

Result: Fail – The firewall blocks ICMP requests

3. SYN scan

```
'nmap -sS -p 1-65535 cureton-pharma.com'
```

Result: Fail – The firewall blocks ports scanning

4. Stealth scan

```
'nmap -sS -T2 -f -p 1-65535 cureton-pharma.com'
```

Result: Fail – Even with a slow and fragmented scan, no ports were detected

Phase 3: Malware sending

1. Creation of a malicious file

Payload: Standard reverse shell integrated in a PDF attachment

Method: Direct file sending for testing

Result: Failed - The integrated antivirus blocked the file before execution.

2. More sophisticated malicious file

Payload: Reverse shell encrypted with Veil-Evasion

Method: The file disguised as a legitimate document related to vaccine development

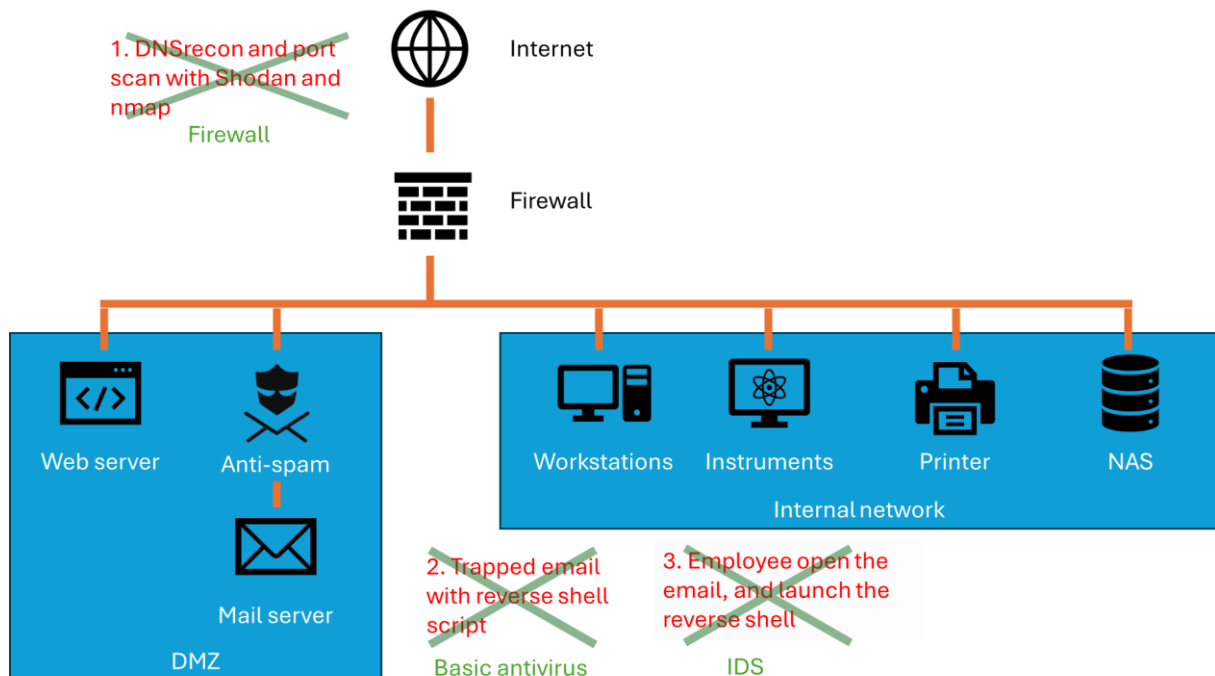
Result: Partial failure - The file was opened, but when the payload attempted to establish a connection, the firewall's IDS detected and blocked the suspicious communication.

E. Reasons for success of failure

Failures observed

1. Limited reconnaissance
 - The company's website discloses little usable information
 - The DNS configuration is minimalist, limiting infrastructure exposure
2. Effective firewall
 - Robust configuration blocking port scans
3. Effective malware protection
 - Integrated antivirus detects standard payloads
 - Malicious files are blocked before execution
4. Malicious communication detection
 - Even with an encrypted payload, the IDS detected the reverse shell communication

Summary chart of the attempted attacks



Positive security points

The simulation demonstrated that primary security controls (firewall, antivirus, IDS) are working effectively to protect against basic external attacks.

Identified weaknesses

The lack of segmentation in the internal network. If an attacker was able to penetrate the external defences, they could potentially directly access the NAS containing sensitive vaccine data.

Recommended solutions for discovered threats

Following the attack simulation on the CPC virtual environment, several recommendations can be made to further strengthen system security, particularly regarding the major weakness identified: the lack of network segmentation.

A. Recommended configuration changes

Internal network segmentation

The main recommended improvement is the implementation of robust network segmentation:

1. Create separate VLANs to logically separate:
 - Administrative network
 - Research and development network
 - Scientific instrument network
 - Storage area network (NAS)
2. Configure internal firewalls between network segments:
 - Implement filtering rules between VLANs
 - Limit inter-segment communications to only necessary protocols and ports
 - Apply the principle of least privilege for inter-segment communications
3. Strengthen authentication for NAS access:
 - Implement multi-factor authentication (MFA) for access to sensitive data
 - Implement role-based access controls
 - Log all access to sensitive data

Optimize existing systems

1. External firewall:
 - Maintain the current configuration, which has proven effective
 - Implement more efficient inspection in-depth analysis of outgoing packets (to block data in case of exfiltration)
2. Anti-spam system:
 - Keep definitions up to date
 - Consider adding a sandboxing system for dynamic attachment analysis
3. Mail server:
 - Implement DMARC, SPF, and DKIM policies to reduce the risk of identity theft

- Configure stricter filtering rules for emails containing executable attachments

B. Recommended new software and hardware

Hardware

1. Internal Next-Generation Firewall (NGFW):
 - FortiGate 100F or equivalent for internal segmentation
 - Deep Packet Inspection capabilities
 - Integrated IPS/IDS features
2. Managed switches supporting VLANs:
 - Cisco Catalyst 9200 or equivalent
 - 802.1Q support for VLAN management
 - Advanced security features (port security, DHCP snooping)

Software

1. Host-Based Intrusion Detection System (HIDS) for workstations and servers:
 - Wazuh or OSSEC for file monitoring and anomaly detection
 - Deployment on all critical systems, especially servers with NAS access
3. NAC (Network Access Control) solution:
 - Cisco ISE or ForeScout CounterACT
 - Control of devices that can connect to the Network
 - Automatic quarantine of non-compliant devices
4. EDR (Endpoint Detection and Response) solution:
 - CrowdStrike Falcon or SentinelOne
 - Advanced detection of malicious behaviour
 - Automated incident response
5. Security Information and Event Management (SIEM) system:
 - Splunk Enterprise Security or ELK Stack
 - Centralization and correlation of security logs
 - Detection of abnormal network behaviour

C. Defence strategy to prevent these attacks in the future

Defence in depth

1. Layered architecture:
 - Deployment of complementary security controls at each network layer
 - Application of the defence in depth principle
2. Implementation of the principle of least privilege:
 - Restriction of access to only necessary resources
 - Periodic review of access rights
3. Security awareness program:
 - Regular employee training on phishing risks

- Phishing simulation exercises to assess training effectiveness

Monitoring and response

1. Establishment of a Security Operations Centre (SOC) team:
 - Continuous network monitoring
 - Incident response protocols
2. Regular penetration testing:
 - Quarterly security assessments
 - Targeted testing of new systems before they are put into production
3. Vulnerability management program:
 - Regular scans to identify vulnerabilities
 - Formalized process for patch deployment

Solution cost

Cost of replacing software and hardware

Hardware

Element	Quantity	Unit price	Total
FortiGate 100F (Internal NGFW)	1	€3,500	€3,500
Cisco Catalyst 9200-24P	3	€2,800	€8,400
Server for SIEM	1	€5,200	€5,200
Hardware subtotal			€17,100

Software and licenses (annual)

Element	Quantity	Unit price	Total
EDR solution (50 workstations)	50	€65	€3,250
Splunk enterprise licenses (SIEM)	1	€12,000	€12,000
NAC solution (50 workstations)	50	€55	€2,750
Annual software subtotal			€18,000

Solution implementation cost

Professional services

Service	Estimated hours	Hourly rate	Total
Detailed architecture design	40	€120	€4,800
NGFW installation and configuration	16	€120	€1,920
Switch deployment and VLAN configuration	24	€120	€2,880
SIEM implementation	40	€120	€4,800
EDR agent deployment	16	€120	€1,920
NAC configuration	24	€120	€2,880

Testing and validation	32	€120	€3,840
Administrator training	16	€120	€1,920
Documentation	24	€120	€2,880
Services subtotal	232		€27,840

Cost summary

Category	Cost
Hardware	€17,100
Software and licenses (First Year)	€18,000
Professional services	€27,840
Total implementation cost	€62,940

Execution schedule and professional services invoice

Solution execution schedule

Phase	Activity	Duration	Start week	End week
Phase 1: Preparation	Final requirements validation	1 week	W1	W1
	Detailed design	1 week	W1	W1
	Hardware and software acquisition	2 weeks	W2	W3
Phase 2: Network segmentation implementation	New switch installation	1 week	W4	W4
	VLAN configuration	1 week	W4	W4
	Internal NGFW deployment	1 week	W5	W5
	Filtering rules configuration	1 week	W5	W5
Phase 3: Endpoint security reinforcement	EDR solution deployment	1 week	W6	W6
	NAC implementation	2 weeks	W6	W7
Phase 4: Monitoring and detection	SIEM installation	1 week	W8	W8
	Log sources configuration	1 week	W9	W9
	Alert rules creation	1 week	W9	W9
Phase 5: Testing and validation	Functionality testing	1 week	W10	W10
	Post-implementation penetration testing	1 week	W10	W10
	Identified issues remediation	1 week	W11	W11

Phase 6: Training and documentation	Administrator training	1 week	W12	W12
	Documentation finalization	1 week	W12	W12
	Knowledge transfer	1 week	W13	W13

Total project duration: 13 weeks (approximately 3 months)

References

- [1] Fortinet, “Qu’est-ce que l’EDR (Endpoint Detection and Response) ? Fonctionnement,” *Fortinet*. [Online]. Available: <https://www.fortinet.com/fr/resources/cyberglossary/what-is-edr>
- [2] N. Sas, “Le Pentesting et le Standard PTES,” *Nomios France*, Jul. 26, 2024. [Online]. Available: <https://www.nomios.fr/actualite/le-pentesting-et-le-standard-ptes/>
- [3] “The Penetration Testing Execution Standard,” *PTES*. [Online]. Available: http://www.pentest-standard.org/index.php/Main_Page
- [4] Juniper Networks, “What is IDS and IPS?,” *Juniper Networks*. [Online]. Available: <https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html>
- [5] F. Habte, “What is SOC (Security Operation Center)?,” *Check Point Software*, May 11, 2022. [Online]. Available: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/>
- [6] Wazuh, “Wazuh - Open source XDR. Open Source SIEM.,” *Wazuh*, Jan. 17, 2024. [Online]. Available: <https://wazuh.com/>
- [7] OSSEC, “OSSEC - world’s most widely used Host Intrusion Detection System - HIDS,” *OSSEC*, Mar. 05, 2025. [Online]. Available: <https://www.ossec.net/>
- [8] Cloudflare, “What are DMARC, DKIM, and SPF?,” *Cloudflare*. [Online]. Available: <https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/>
- [9] HackerSploit, “Veil-Evasion complete tutorial,” *YouTube*, May 05, 2018. [Online]. Available: <https://www.youtube.com/watch?v=iz1twCSJZyo>
- [10] Rapid7, “Home,” *Metasploit Documentation Penetration Testing Software, Pen Testing Security*. [Online]. Available: <https://docs.metasploit.com/>
- [11] Kali Linux, “dnsrecon | Kali Linux Tools,” *Kali Linux*. [Online]. Available: <https://www.kali.org/tools/dnsrecon/>