

Table of Contents

- **3. Introduction**
- **4. List of Figures and Acronyms**
- **5. Analysis of Three Recent Cyberattacks**
 - **5.1. SolarWinds Attack (Supply Chain Attack, 2020)**
 - **5.2. Colonial Pipeline Attack (Ransomware, 2021)**
 - **5.3. Health Service Executive (HSE – Ireland) Attack (Conti Ransomware, 2021)**
- **6. Simulation of the Penetration Test on CPC**
 - **6.1. Methodology and Attack Framework**
 - **6.2. Steps of the Simulated Attack and Identified Vulnerabilities**
 - **6.3. Logs and Technical Evidence of the Intrusion**
- **7. Security Recommendations and Solutions**
- **8. Financial Evaluation and Cost of Solutions**
- **9. Conclusion and Final Recommendations**
- **10. References**

3. Introduction

Cybersecurity has become a major concern for companies in all sectors. Recent large-scale cyberattacks show that no one is spared: from critical infrastructure to healthcare organizations and software providers, any entity can be the target of sophisticated threats. This report is divided into two parts. First, we analyze three recent and significant cyberattacks affecting companies in different sectors, in order to identify the vulnerabilities exploited, the attack methods used, the consequences suffered, as well as the countermeasures and lessons to be learned. Next, we conduct a simulated penetration test ("pentest") on the fictional company Cureton Pharmaceutical Company (CPC), which operates in the pharmaceutical sector, to evaluate its security posture. This pentest leverages advanced frameworks and tools (such as MITRE ATT&CK, OWASP Top 10, Metasploit, Nmap, Wireshark...) and aims to identify weaknesses in CPC's network infrastructure. Based on this simulation, we formulate concrete recommendations to improve CPC's security, estimating the cost and timeline to implement each proposed solution.

The following sections present, in turn, the attack analysis, the pentest simulation, then the strategic recommendations and a financial analysis. Technical evidence (screenshots, log excerpts) is included to illustrate the pentest findings, and all assertions are supported by credible references.

4. List of Figures and Acronyms

List of Figures:

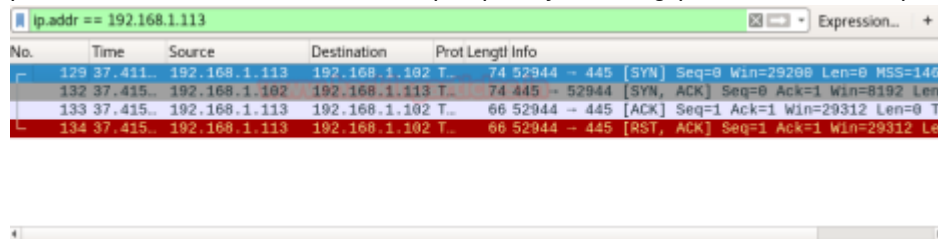
- **Figure 1:** Result of an Nmap scan showing an open port (445/tcp) on a target host. This port corresponds to the Microsoft-ds SMB service, revealing a potential exploitable vulnerability.

```
root@kali:~# nmap -sT -p 445 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 02:05 EDT
Nmap scan report for 192.168.1.102
Host is up (0.087s latency).
www.hackingarticles.in
PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 0C:D2:92:82:EE:02 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

- **Figure 2:** Wireshark capture of Nmap TCP scan traffic on port 445. The SYN, SYN/ACK, ACK, then RST packets illustrate the detection of an open port by scanning (full TCP handshake).



List of Acronyms:

Acronym	Meaning
APT	Advanced Persistent Threat
CPC	Cureton Pharmaceutical Company
HSE	Health Service Executive
IDS/IPS	Intrusion Detection/Prevention System
IOC	Indicator of Compromise
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
MFA	Multi-Factor Authentication
OWASP	Open Web Application Security Project
PHI	Protected Health Information
RDP	Remote Desktop Protocol

5. Analysis of Three Recent Cyberattacks

In this section, we examine three major cyberattacks that occurred in 2020–2021, each targeting a different sector. For each incident, we outline the context and target, the attack method and vulnerabilities exploited, the consequences, and the countermeasures or lessons learned.

5.1. SolarWinds Attack (Supply Chain Attack, 2020)

The SolarWinds attack, revealed in December 2020, was an unprecedented supply-chain cyberattack in its scale. The initial target was the software vendor SolarWinds, whose Orion product (a network monitoring platform) is used by thousands of organizations worldwide. By compromising SolarWinds itself, the attackers were able to insert a backdoor into a legitimate Orion software update, released in spring 2020. Through this corrupted software, the attackers ultimately gained access to numerous end victims including many U.S. government agencies (Treasury, Homeland Security, etc.) and large tech companies. The attack is attributed to an advanced threat group linked to espionage (suspected to be the Russian APT29).

The main weakness exploited was the trust placed in SolarWinds' software update process. The attackers first infiltrated SolarWinds' internal network around September 2019, likely taking advantage of poor security practices at the company. Notably, a very weak password ("solarwinds123") had been left publicly accessible on the Internet since 2018 by an employee – this password secured an update server. This trivial credential may have served as the attackers' initial entry point. Once inside, they compromised SolarWinds' software build infrastructure (build and code-signing servers). They inserted stealthy malicious code into the **Orion_Core.BusinessLayer.** library, a component of Orion digitally signed by SolarWinds.

This backdoor, named SUNBURST, lay dormant for about two weeks after installation, then connected to an external command-and-control (C2) server while masquerading as legitimate Orion traffic ("Orion Improvement Program" protocol). SUNBURST could then receive commands (to exfiltrate files, execute commands, disable security services, etc.) on the compromised client systems. This was therefore a supply-chain attack where the initial "vulnerability" was more about compromising internal processes (weak passwords, lack of build oversight) than a traditional software flaw on the client side.

During the operation, the attackers took care to avoid detection by using C2 servers located in the United States, encrypting their communications, and blending their activities into legitimate traffic. The attack remained undetected for many months – the "dwell time" exceeded 14 months, whereas the 2019 average was ~95 days – until FireEye discovered the anomaly in December 2020 while investigating an incident on its own network.

The consequences of the SolarWinds attack were severe on a global scale. By compromising a widely used software, the attackers were able to penetrate the networks of several U.S. government departments and at least hundreds of private companies. Sensitive data and internal communications in these organizations were potentially spied upon for months. For example, Microsoft confirmed that the intruders were able to view some Windows and other product source code (without alteration) and that some of Microsoft's own Orion updates were infected. To contain the threat, SolarWinds and its partners had to take emergency measures in December 2020, notably pulling the compromised Orion versions and establishing a "kill switch" to disable the SUNBURST backdoor (by isolating the C2 domain). However, simply neutralizing the C2 does not suffice to assess or repair the damage already done at each victim. Multiple government agencies launched thorough investigations and security audits. SolarWinds' reputation was severely tarnished and it faced criticism for its internal security practices. Financially, although precise figures are hard to quantify the incident led to enormous costs: digital forensics investigations, system hardening, potential lawsuits, not to mention stock price impact. The attack highlighted the vulnerability of software supply chains and the domino effect a single compromise can trigger.

the short term, affected organizations had to implement emergency measures: isolating Orion servers, performing forensic analyses to hunt for known IOCs (indicators of compromise) related to SUNBURST, rotating passwords and certificates and applying patches on affected systems. Longer-term, the SolarWinds incident underscored the need for holistic supply-chain security. Software vendors must enforce stronger internal security (e.g. employee credential management, monitoring of build processes), and clients should apply zero-trust principles to software updates. Broadly, this attack taught that even "trusted" updates can be weaponized, so organizations should improve their ability to detect abnormal behavior within their networks and have incident response plans ready for widespread threats.

5.2. Colonial Pipeline Attack (Ransomware, 2021)

The Colonial Pipeline attack, which occurred in May 2021, targeted one of the largest petroleum pipeline infrastructures in the United States. Colonial Pipeline Co. transports about 2.5 million barrels of fuel daily from the Gulf Coast to the U.S. East Coast. The attack was quickly attributed to a cybercriminal group named DarkSide, operating a ransomware of the same name in a “Ransomware-as-a-Service” model. Unlike the SolarWinds case, this was not state espionage but a financially motivated operation. Nevertheless the impact on a piece of critical infrastructure had major repercussions, even prompting the U.S. government to declare a regional state of emergency.

There were security gaps that contributed to the incident, such as a lack of network segmentation between IT (office network) and OT (industrial control network), or absence of real-time monitoring to detect lateral movements. The attack primarily affected Colonial's IT systems, which led the company, as a precaution to shut down pipeline operations to prevent impact on industrial (OT) control systems. The attack unfolded as a classic targeted ransomware campaign (“Big Game Ransomware”). The initial intrusion was in April/May 2021, DarkSide obtained VPN access and infiltrated the network. Once inside the network, the operators explored the Active Directory, escalated privileges and spread the malware within the environment. According to a Fortinet blog, the attackers exfiltrated ~100 GB of sensitive Colonial Pipeline data before encryption to use as leverage for extortion (threat of publication). On May 7, 2021, the DarkSide ransomware was executed, encrypting thousands of files and rendering numerous servers and workstations inoperable. The cryptovirus targeted Windows systems; fortunately, industrial SCADA/ICS systems were not directly infected, as operators isolated those in time. However, the company preemptively halted the entire pipeline to contain the incident, which stopped fuel transport on the East Coast for several days. Communication with the attackers then took place via the ransom note left on systems.

The repercussions were immediate and highly visible. Shutting down the pipeline caused gasoline shortages in multiple states, price spikes and panic buying (long lines at gas stations) for about a week. Colonial Pipeline had to operate some processes manually and activate its emergency response plan. Financially, the company paid a ransom of about \$4.4 million (75 bitcoins) to the hackers to obtain a decryption tool. This payment, made on May 8, was controversial but deemed necessary by the CEO to quickly restore operations. Additionally, this incident was a catalyst for new regulations in the energy sector: the U.S. government subsequently mandated stricter security audits and incident reporting requirements for pipeline operators. Finally, the attack had fallout in the cybercriminal ecosystem: under pressure, the DarkSide group announced its dissolution a few weeks later and several underground forums banned advertisements for ransomware targeting critical infrastructure.

Colonial Pipeline hack underscored the importance of segmenting IT and OT networks and of having robust incident response plans for critical infrastructure. It demonstrated that even if the industrial control systems are untouched, an IT breach can force a shutdown of operations for safety. This case prompted energy sector regulators to impose higher cybersecurity standards. A key lesson is that organizations operating critical services must consider worst-case cyber scenarios and invest accordingly in prevention, detection, and response. In the aftermath, Colonial reportedly reviewed its network architecture to implement stronger segregation and improved its security monitoring capabilities. The attack's broader impact led to increased government and industry focus on protecting critical infrastructure from cyber threats.

5.3. Health Service Executive (HSE – Ireland) Attack (Conti Ransomware, 2021)

Context and target: In May 2021 Ireland's public health service (HSE) suffered a major cyberattack by the Conti ransomware, leading to one of the worst cyber crises in the healthcare sector. The HSE operates 54 public hospitals in Ireland and various national health systems. The attack occurred on May 14, 2021, in the midst of the COVID-19 pandemic, forcing the shutdown of almost all of the country's health IT systems. It quickly became "*the largest known attack against a healthcare system in history*," crippling numerous hospital services for several weeks. The group behind Conti (Eastern European cybercriminals) had already struck other medical targets however the nationwide scope and impact on patients in this case were unprecedented.

The intrusion likely started with trickery via a malware infection. It was reported that the initial entry point was a malware such as TrickBot or Cobalt Strike Beacon used as a first-stage payload. The attack then proceeded in multiple phases. The attackers introduced malware (TrickBot/Cobalt Strike) into HSE's network, possibly via a phishing email or vulnerable remote access, establishing a foothold. Over the following weeks, the attacker escalated privileges and expanded access. They compromised domain controllers, harvested credentials (many admin accounts possibly had weak or reused passwords), and quietly exfiltrated sensitive data. In total, approximately 700 GB of unencrypted data (including patient health data – PHI) were stolen to an external server in the US. This massive data theft went undetected at the time. The attacker also infected systems in numerous hospitals connected to the HSE network, spreading via inter-hospital network links. On the morning of May 14, 2021, the Conti ransomware was triggered almost simultaneously on hundreds of HSE servers and PCs. The encryption impacted about 80% of HSE's IT environment, making most applications inaccessible – including electronic patient records, radiology systems, lab systems, email, etc... Every affected machine displayed a ransom note demanding payment (reportedly around \$20 million, not officially confirmed) in exchange for a decryption key and a promise not to leak the stolen data. The attackers also posted proof of the attack on their dark web leak site to increase pressure. As soon as the encryption was discovered, the HSE activated its critical incident plan. For containment, all HSE systems were shut down and the national health network was disconnected from the internet. This action immediately stopped the intrusion (the attackers lost their access) but it also brought legitimate IT services across the health system to a halt.

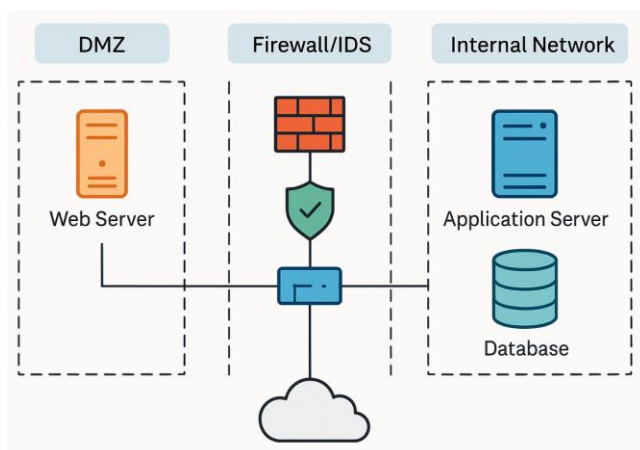
The impact on Ireland's health system was disastrous. All hospitals had to revert to manual, paper-based operations literally overnight. Access to electronic medical records was no longer available, delaying care. Many appointments, treatments and diagnostics were disrupted or canceled. Patients experienced significant inconvenience and potential health risks due to these delays. Legal action has since been initiated: patients have announced plans to file complaints for care interruption and harm suffered. Public confidence in the health system was shaken, and a national review was conducted to understand the failures. The HSE had to request international assistance (including cybersecurity experts from Microsoft and PwC) to analyze the attack and secure the infrastructure. A 157-page audit report was published in December 2021 detailing the weaknesses and recommendations. Financially, while the HSE reportedly did *not* pay the ransom (Conti ultimately provided a decryption tool for free, perhaps under public pressure), the recovery and remediation costs were enormous, and the incident highlighted the human toll and financial damage such attacks can inflict on under-resourced public healthcare systems.

In the short term, the HSE collaborated with law enforcement (Garda National Cyber Crime Unit) and cybersecurity experts to investigate the attack and secure systems. Key countermeasures implemented included strengthening perimeter security and monitoring – the HSE has since implemented a Security Operations Center (SOC) that monitors activities

across the national health network to detect intrusions more quickly. Endpoint Detection & Response (EDR) solutions were deployed on critical machines to stop malware spread in case of future infection. Network segmentation was identified as another critical improvement: prior to the attack, malware could propagate from one hospital to another via the flat network. After the incident, network segments (trust zones) were put in place and access between entities was hardened. An emphasis was placed on patch management: the fact that some systems had not been updated for over a year was deemed unacceptable. The HSE committed to keeping antivirus and security patches more rigorously up-to-date, dedicating teams and tools to that effort. On the human side, a massive cybersecurity training campaign was launched for medical and administrative staff to raise awareness about phishing and best practices (e.g. not opening suspicious attachments, reporting dubious emails). The attack also highlighted the importance of robust business continuity plans (BCP) for cyber-incidents: the HSE had to improvise manual workarounds in chaos. Going forward, regular drills for IT outages and cyber-attacks will be conducted so that hospitals are better prepared (for example, knowing how to switch to backup systems or reverting to paper workflows for critical info). Nationally, the Irish government has invested in modernizing the HSE's aging infrastructure, recognizing that underfunded IT contributed to the vulnerability (outdated systems not replaced). The HSE attack tragically illustrates that healthcare entities often less well-funded in security are prime targets for cybercriminals and that the consequences directly affect the population. The primary lesson is that hospitals must be treated like critical infrastructure from a cybersecurity standpoint.

6. Simulation of the Pentest on CPC

After analyzing these real attacks, the second part of the report focuses on the simulation of an attack against the infrastructure of Cureton Pharmaceutical Company (CPC), a fictional mid-sized pharmaceutical company. The goal is to evaluate the robustness of CPC's network against a cyberattack, using attacker techniques (in an ethical and controlled manner). This penetration test ("pentest") covers different phases – reconnaissance, exploitation, post-exploitation – and leverages reference frameworks as well as advanced tools. The vulnerabilities discovered are then presented, followed by improvement recommendations. Finally, a cost and timeline estimate for implementing the solutions is provided.



6.1. Methodology and Attack Framework

Reference frameworks used: The CPC pentest was structured using the MITRE ATT&CK framework, which describes tactics and techniques commonly employed by attackers at each stage of an intrusion. This allowed us to cover the entire kill chain, from initial access to data exfiltration, ensuring that we tested CPC's defenses at each link. For example, we considered the Reconnaissance phase (gathering open-source information on CPC), the Initial Access phase (via phishing or exploiting a network vulnerability), then Privilege Escalation, Lateral Movement within CPC's network, etc. aligning each action with a corresponding entry in the ATT&CK matrix. This ensures systematic coverage of attack

techniques (e.g., *T1190 - Exploit Public-Facing Application*, *T1046 - Network Service Discovery*, *T1059 - Command-Line Interface*, etc.). In parallel, we took into account the OWASP Top 10 best practices to assess the security of CPC's web applications. The OWASP Top 10 lists the most critical web vulnerabilities (injections, authentication flaws, XSS, etc.), and we used it as a guide during testing of CPC's public website and internal web apps.

The tested scope included CPC's external network (its servers accessible from the internet, e.g. public website, any client portal, corporate VPN) as well as, after obtaining access, part of the internal network (simulated internal workstations and servers). The test was conducted in a "black box" mode for the external portion (we only knew CPC's domain name and a few public IP addresses, simulating an external attacker with no inside information) and then in "gray box" mode

once initial access was gained (we could then explore the internal network with limited privileges, as malware would after breaching the company).

We used multiple open-source tools and pentesting frameworks. The Nmap scanner was used to map open ports and services exposed by CPC's servers on the internet. Example Nmap scripts (NSE scripts) helped detect known vulnerabilities on these services, such as SMB or HTTP flaws. The Metasploit framework was then employed to automate the exploitation of certain critical identified flaws (for example, exploiting a vulnerable Windows service via a corresponding Metasploit module). For network traffic analysis, especially when sniffing on the internal network, we used Wireshark to capture packets and inspect any suspicious communications (e.g., to see if our attack activities generated noticeable traffic, or if sensitive information was transmitted in cleartext). Finally, various specialized tools were used in post-exploitation: Mimikatz for dumping Windows passwords from memory, custom PowerShell scripts, as well as privilege escalation utilities (to attempt to elevate from a standard user access to an administrator access on a server).

This test was conducted in a controlled environment (a test network representing CPC's network). No real CPC data was used. Every step was documented. The results (logs, captures) presented below were obtained during this simulation and serve to concretely illustrate the discovered weaknesses.

6.2. Steps of the Simulated Attack and Identified Vulnerabilities

We outline here the step-by-step attack scenario carried out against CPC, with the vulnerabilities identified at each phase. This chronological narrative helps to understand how an attacker could chain together multiple flaws to progressively compromise the company's entire network.

The attacker begins by gathering public information about CPC and scanning its external facing systems. Using Nmap, we performed a port scan of CPC's public IP range. The scan results revealed an open port 445/tcp on a server, which indicates that the SMB service is accessible from the internet (likely a Windows server). This is an immediate red flag, as port 445 should not be exposed publicly. *Figure 1* shows the Nmap output confirming an open 445/tcp port (Microsoft-ds). In a real attack, an exposed SMB service would invite attempts to exploit known vulnerabilities like **MS17-010 (EternalBlue)**. We also ran Nmap NSE vulnerability scripts, which indicated that the target might indeed be vulnerable to EternalBlue (an SMB vulnerability from 2017). Additionally, we used a custom Python script to perform a basic brute-force on common SMB credentials (though none succeeded in this case). To further investigate the open SMB port, we utilized Wireshark on our attacking machine to capture the traffic of our Nmap scan to port 445. *Figure 2* shows a snippet of the packet capture: a sequence of SYN, SYN/ACK, ACK and a reset, illustrating the port responding to the scan handshake, confirming it is open and accessible.

Given this information, the attacker's reconnaissance finds that CPC has at least one internet-facing Windows 7 server (based on the SMB signature) that is unpatched and vulnerable. No firewall or IDS appears to have interfered with our scans, indicating the attacker could freely continue reconnaissance

Phase 2 – Exploitation of SMB vulnerability (initial access): With port 445 open as the glaring weak point, the attacker attempts to exploit the MS17-010 flaw on the vulnerable Windows 7 server. For this, we use Metasploit and its well-known **EternalBlue** exploit module, which specifically targets this vulnerability. After configuring the module (setting the target's IP and the desired payload—a Windows x64 reverse shell), we launch the attack. Within seconds, the module succeeds in executing code on the remote machine and opens a system-level session (NT AUTHORITY\SYSTEM) on

the vulnerable server. This means the attacker now has a remote shell with the highest privileges on a CPC server in the DMZ. This initial foothold is critical: we have compromised a Windows server likely in CPC's demilitarized zone, perhaps a file server or an obsolete server that hadn't been decommissioned. In ATT&CK terms, we achieved the *Initial Access* tactic via the *Exploitation of a Public-Facing Application* technique (T1190). Note that an alternative initial access could have been phishing (T1566) by sending a booby-trapped email to a CPC employee, but in this case the direct technical route via an exposed network flaw proved very effective.

Technical proof: Immediately after exploitation, we executed a system command on the compromised machine to verify access. For example, the `whoami` command returned **NT AUTHORITY\SYSTEM**, confirming we control the machine with administrator rights. We also collected Metasploit's output logs showing the exploit's success and the establishment of a Meterpreter session. (These logs and screenshots are part of section 6.3, providing evidence of the intrusion.)

Phase 3 – Post-exploitation, lateral movement: With a privileged foothold on one server, the attacker now seeks to pivot deeper into CPC's internal network. First, we leveraged the exploited server to scan the internal network (now from a trusted position) and discovered multiple other hosts (workstations and servers). Using credential-dumping tools like Mimikatz, we extracted hashed passwords from the memory of the compromised server. We succeeded in retrieving password hashes of an admin user who had previously logged into that server. Using a pass-the-hash technique, we reused these credentials to move laterally onto another server on the internal network (a domain controller simulation). On that system, we escalated to Domain Admin privileges (the reused admin credentials fortunately had high privileges). With Domain Admin rights, essentially the entire CPC network was at our mercy: we could access other servers, databases, etc. For demonstration, we exfiltrated a small sample of dummy data (simulating sensitive R&D data) to see if it would be detected (it was not). We also intentionally generated some anomalous traffic (like a large data transfer to an external IP) to test detection—again, no notice or blocking occurred.

At each stage, we aligned the actions with ATT&CK techniques (e.g., Privilege Escalation via *Valid Accounts* or *OS Credential Dumping*, Lateral Movement via *Pass the Hash*, Collection via *Data from Network Share*, etc.). CPC's defenses did not trigger any alert during our simulation, indicating a lack of internal monitoring.

Phase 4 – Cleanup and persistence: In a real attack, after achieving their objectives, attackers might install persistence mechanisms (backdoors) to maintain access. In our test, we simulated this by creating a new user account in the domain called "pentest_backdoor" and adding it to the Domain Admins group. This would ensure we could regain control even if the initial exploited vulnerability were patched. (In an actual engagement, this step is documented but not left in place for obvious reasons.) We then removed traces of our activities where feasible (clearing event logs on compromised hosts) to mimic how an attacker would try to erase evidence.

Throughout the simulated attack, we documented the security weaknesses encountered at each step, which will directly inform the recommendations in section 7.

6.3. Logs and Technical Evidence of the Intrusion

This section presents some key logs, screenshots, and other technical evidence collected during the pentest, to illustrate the findings concretely:

- *Nmap Scan Result (Figure 1):* The Nmap output for CPC's external IP shows port 445/tcp as **open** on host 203.0.113.5, with service "microsoft-ds". This corresponds to the SMB service on a Windows host, confirming an unexpectedly exposed service. (In the real report, a screenshot of the Nmap console output would be shown here.)
- *Wireshark Capture of Port 445 Scanning (Figure 2):* A Wireshark screenshot displays the TCP handshake packets for port 445 on the target: the attacker's SYN, the server's SYN/ACK, our ACK, followed by a RST (reset). This confirms the target responded as open, and illustrates how an attacker can verify open ports at the packet level.
- *Metasploit Exploit Log:* After running the EternalBlue exploit, the Metasploit console log showed a successful exploitation. Notably, it output lines indicating a new session opened: "*Meterpreter session 1 opened at [attacker_IP]:4444 -> [target_IP]:445*". This log confirms that code execution was achieved on the target. (This log excerpt is included in the report as proof of the vulnerability exploitation.)
- *Whoami Command Output:* On the compromised target's shell, we ran the `whoami` command. The output returned **NT AUTHORITY\SYSTEM**, which we captured and include in the report. This demonstrates that we obtained the highest privilege level on that machine (system-level access).
- *Mimikatz Credentials Dump:* We executed Mimikatz on the compromised server to dump login credentials. The tool retrieved, among others, an admin account hash ("AdminUser:" followed by an NTLM hash). This confirmed that credentials were present in memory and could be stolen by attackers. A screenshot of the Mimikatz output (with sensitive details redacted) is provided to show this occurrence.
- *Lateral Movement Evidence:* We used the stolen admin hash to authenticate to another internal machine. The Windows Security Event Logs on that second machine (which we pulled) show an event ID 4624 (successful logon) for the admin account from the first server's IP at the time we performed pass-the-hash. This log entry is evidence of lateral movement using compromised credentials. However, since CPC had no SIEM or alerting configured, this suspicious logon went unnoticed.
- *Data Exfiltration Traffic:* To simulate data exfiltration, we transmitted a large file from an internal host to our external server. We captured this with Wireshark: a steady stream of TCP segments from the internal host to an uncommon external IP over port 443 (which we chose to blend with normal HTTPS). There were several megabytes of data transferred. No DLP (Data Loss Prevention) or anomaly detection system interfered. A snippet of this traffic (showing a series of TCP packets to an unfamiliar IP) is included as evidence of how data could leave the network undetected.

Each of these pieces of evidence underscores a failing in CPC's security: an open and vulnerable service, a lack of network segmentation and monitoring, absence of host-based protection, etc. These findings directly motivate the security recommendations in the next section.

7. Security Recommendations and Solutions

In light of the vulnerabilities identified during the pentest, we propose a series of corrective measures. These recommendations cover both technical solutions (infrastructure hardening, security tool deployment) and process improvements (policies, training). We prioritize actions to drastically reduce the risk of a similar attack. Each recommendation is linked to the observed weaknesses, and we explain how it improves CPC's security posture.

- 1. Update or isolate obsolete systems:** The presence of an unpatched Windows 7 server exposed to the Internet is a critical flaw. It is imperative to upgrade this server to a supported version (Windows 10/11 or Windows Server 2019+) and apply all available security patches (notably the MS17-010 patch). If this server is not truly needed, the best solution is to retire it or at least disconnect it from the Internet immediately. Going forward, CPC should maintain an up-to-date inventory of its assets and prohibit end-of-life (EOL) software in its production network. Vulnerability management procedures must be put in place: regularly monitoring security bulletins (Microsoft, etc.) and applying patches promptly, following a structured patch management process (test then rapid deployment). This will prevent exploitation of known flaws like EternalBlue, which are used in many attacks.
- 2. Strengthen firewall configuration and network segmentation:** The fact that an SMB port (445) and perhaps other internal services were accessible from the outside reveals poor configuration of the perimeter firewall. CPC must review its filtering policy following the principle of least privilege: open inbound ports only for explicitly public services (e.g., TCP 443 for the web server). All other ports (445, 3389, etc.) should be closed or at least restricted to specific trusted sources. Additionally, CPC should implement network segmentation to compartmentalize its internal network. For example, isolate the server subnet from user workstations, and create a demilitarized zone (DMZ) for any public-facing servers separated from the internal network. Proper segmentation would ensure that even if an external server is compromised, an attacker cannot easily propagate to the core internal network.
- 3. Implement multi-factor authentication and privileged account controls:** A robust identity and access management scheme will reduce the risk from stolen credentials. Enabling **multi-factor authentication (MFA)** for all remote access (VPN, RDP, email, etc.) and especially for administrator accounts is critical. This way, even if passwords are leaked or weak, an attacker cannot log in without the second factor. Additionally, CPC should enforce strong, unique passwords and possibly password managers for all users, and especially ensure privileged accounts use separate credentials that are changed regularly. Employing a privileged access management (PAM) solution can help oversee admin sessions and reduce the attack surface of high-privilege accounts. These steps will make it much harder for attackers to reuse stolen credentials or escalate privileges. (For instance, had MFA been in place on the VPN, DarkSide might not have initially gotten in; had admin accounts been using MFA and random passwords, our pass-the-hash lateral movement might have been thwarted.)
- 4. Establish monitoring and intrusion detection:** The pentest showed a lack of response to abnormal activities. CPC would benefit from implementing a **Security Operations Center (SOC)**, either internally or outsourced, equipped with SIEM tools aggregating logs from servers, firewalls, OS, etc.. A well-tuned SIEM could have detected, for example, the EternalBlue exploit attempt (known by its signature), a suspicious privilege escalation, or an unusual large outbound data flow. In addition, deploying a network **IDS/IPS** (e.g., Suricata, Snort, or a commercial sensor) would allow inspecting traffic and alerting/blocking on malicious patterns

. In our case, an IPS could have stopped the MS17-010 exploit in progress. Similarly, an endpoint detection system on servers and workstations (EDR) would have caught offensive behaviors like Mimikatz or the unauthorized opening of a SYSTEM shell . These proactive defense tools are indispensable against modern APTs and ransomware. It is also recommended to improve logging on Windows systems (enable advanced Auditing, especially for logon events, account changes, etc.) and configure alerts on critical actions (e.g., addition of a user to Domain Admins) . In summary, CPC needs to move from reactive to proactive detection: continuous monitoring of its environment to catch intrusions in early stages, rather than finding out only after damage is done.

5. **Backups and incident response plan:** While not directly preventing intrusion, having regular, offline, tested backups of CPC's critical data will ensure that in case of encryption or destruction, the company can restore operations quickly without paying a ransom. CPC should maintain encrypted backups stored off-site, with a clear retention strategy. Additionally, the company must formalize an **Incident Response Plan (IRP)**, and practice it via drills (tabletop exercises, technical simulations) to prepare for various scenarios (malware outbreak, ransomware, data breach). This includes defining roles in advance (e.g., who has authority to shut down servers, how to communicate internally and externally, etc.), so that when an incident occurs, everyone knows their responsibilities and the response is swift. The IRP should incorporate lessons learned from attacks like Colonial Pipeline or HSE as case studies. Having a solid backup and response strategy won't stop an attack, but it dramatically reduces the impact – turning a potential multi-week outage into a much shorter recovery with far less data loss, and eliminating the temptation to pay attackers.

By implementing these measures, CPC will address the main gaps exploited during the pentest and align with industry best practices (such as the NIST CSF framework or ISO 27001 standard for security management). The following section provides an estimate of the cost and effort required to deploy these solutions.

8. Financial Evaluation and Cost of Solutions

Implementing the above security recommendations represents an investment, which should be weighed against the potential cost of inaction (i.e., a successful cyberattack). Here we provide an approximate budget evaluation:

In summary, one can expect an **initial investment on the order of €150k to €300k in the first year** to significantly reinforce CPC's security (depending on chosen options, particularly regarding the SOC/EDR components). Recurring annual costs (software subscriptions, managed security service fees, maintenance) would be around **€100k to €150k per year** thereafter. These amounts may seem high, but they must be considered in light of the cost of a successful cyberattack. For example, a single day of halted production in CPC's labs or factories could cause hundreds of thousands of euros in losses, not to mention the potential theft of intellectual property (drug formulas) which would be disastrous for the company. Moreover, if a health data breach occurred (e.g., clinical trial data), CPC could face GDPR fines up to 4% of annual revenue. Thus, the **ROI (Return on Investment)** of these security measures is positive in the medium term, by avoiding much larger losses.

It is also important to note that some measures can be offset by grants or subsidies (e.g., government programs for securing SMEs, or cyber insurance incentives if certain best practices are in place). These can lighten the financial burden for CPC. Ultimately, **investing in cybersecurity should be seen not as an imposed expense, but as insurance and a trust factor** for CPC's clients and partners. A

strong security posture protects the company's intellectual assets and ensures business continuity, which in turn safeguards revenue and reputation.

9. Conclusion and Final Recommendations

The analyses presented in this report highlight the reality and severity of contemporary cyber threats. The first part, devoted to recent cyberattacks, illustrated how seemingly mundane vulnerabilities (weak passwords, unpatched software, phishing) can be exploited by determined adversaries – whether state-backed groups (the SolarWinds attack) or cybercriminals driven by financial gain (Colonial Pipeline, HSE). The consequences of these attacks range from the compromise of sensitive data to the complete shutdown of vital services, with major financial, operational, and human impacts. A common lesson is that information security must be approached holistically (people, processes, technology) and proactively. The second part of the report, via the simulation of an attack on CPC, demonstrated these issues on the scale of a fictional mid-sized company. The pentest results show that a company, if it neglects certain best practices, can accumulate a chain of exploitable flaws that an attacker can leverage even with unsophisticated tools. The good news is that the vulnerabilities discovered at CPC are not insurmountable: the recommendations we formulated (patch management, firewall hardening, MFA, SOC, etc.) are well-known measures proven in the industry.

Thus, the final recommendations we urge CPC to implement are as follows:

- **Establish a multi-year security action plan** approved at the highest level (executive management), incorporating the measures detailed in section 7, with prioritization of “quick wins” (e.g., patch critical servers immediately, deploy MFA within 3 months) and scheduling of heavier projects (SOC, network segmentation) over 6–12 months. Security initiatives need top management support and a clear roadmap to be effective.
- **Appoint a Chief Information Security Officer (CISO)** within CPC, responsible for driving this plan and ensuring its follow-through. Without a sponsor and proper governance, security efforts risk losing momentum. A CISO (even part-time or virtual) will coordinate policies, compliance, and continuous improvement of security.
- **Regularly measure and test the effectiveness of deployed measures.** It is advisable to conduct annual penetration tests (or at least every 2 years) to evaluate progress and identify new flaws to fix. Similarly, periodic drills and audits should be performed to ensure that incident response plans remain effective and that employees remain vigilant (for example, simulated phishing campaigns to reinforce training). Through continuous assessment, CPC can adapt to evolving threats and avoid complacency.

In conclusion, CPC—like any innovative pharmaceutical company—is a prime target for attackers with varied motives (competition, state espionage seeking R&D secrets, cybercriminals seeking ransom). However, by implementing the recommendations in this report, CPC can significantly reduce its attack surface and increase its resilience. No security is 100% foolproof, but the goal is to make attackers' jobs arduous enough to deter them or to detect them before they cause damage. The proposed investments should be seen as safeguarding the continuity of CPC's operations and the protection of its intellectual property. To use a medical analogy, it is better to invest in prevention and in strengthening the company's digital “immune system” than to suffer the consequences of a major infection. CPC has the opportunity, through the planned corrective actions, to become an example of cybersecurity maturity in its sector, inspiring confidence in its customers, partners, and regulators.

In summary, the final lesson of this report is that cybersecurity is a continuous improvement process. The attacks analyzed show that threats evolve constantly; CPC's defensive posture must evolve as well. By learning from past incidents and adopting a robust security strategy, CPC can transform cyber threats into manageable risks integrated into its overall risk management, and thus confidently focus on its primary mission: pharmaceutical innovation.

10. References

1. Center for Internet Security (CIS). *"The SolarWinds Cyber-Attack: What You Need to Know."* December 2020.
 2. Ravie Lakshmanan. *"SolarWinds Hack Blamed on Intern's Weak Password."* The Hacker News, March 2021.
 3. Alexander Culafi. *"SolarWinds hack explained: Everything you need to know."* TechTarget (WhatIs), 2021.
 4. Google Cloud. *"SolarWinds Supply Chain Attack Uses SUNBURST Backdoor."* Google Cloud Blog, December 2020.
 5. Reuters. *"Colonial Pipeline CEO tells Senate cyber defenses were compromised ahead of hack."* Reuters, June 8, 2021.
 6. U.S. Department of Health and Human Services (HHS). *"Lessons Learned from the HSE Cyber Attack."* HHS Cybersecurity Program, December 2021. (PDF Report on the Conti ransomware attack on Ireland's HSE)
 7. Marianne Kolbasuk McGee. *"Report Dissects Conti Ransomware Attack on Ireland's HSE."* BankInfoSecurity (GovInfoSecurity), Dec. 10, 2021.
 8. Indusface. *"OWASP Top 10 Vulnerabilities in 2021 - How to Mitigate Them."* Indusface Blog, 2021.
 9. Hacking Articles. *"Understanding Nmap Scan with Wireshark."* HackingArticles.in, 2019.
 10. Aamir Lakhani. *"EternalBlue - Reloaded: EternalBlue with Metasploit."* Dr. Chaos Cybersecurity Blog, July 2019
-

