

Name: Md. Mashrurul Haque

ID: 2435257

Programme: MSc Cybersecurity and Digital Forensics

Module: Ethical Hacking (ACCA7033)

Lecturer: Dr Mohamed Ghanem

Date of Submission: 17/12/2025

Table of Contents

1. Introduction.....	3
2. List of Figures and Tables.....	4
3. List of Acronyms.....	5
4. Strategic Threat Analysis: Change Healthcare Ransomware Attack.....	7
4.1 Case Overview.....	7
4.2 Attack Timeline.....	8
4.3 MITRE ATT&CK TTP Mapping.....	9
4.4 Root Cause Analysis.....	10
4.4.1 Control Failures.....	10
4.4.2 Architectural and Third-Party Weaknesses.....	10
4.4.3 Organisational and Sectoral Factors.....	11
4.5 Strategic Recommendations.....	11
4.5.1 Strengthen Initial Access and Authentication.....	11
4.5.2 Implement Zero-Trust Segmentation and Privilege Management.....	11
4.5.3 ATT&CK-Aligned Monitoring and Detection.....	11
4.5.4 Resilience, Third-Party Governance and Economic Justification.....	12
5. Red Team Engagement (Operation IP Shield).....	13
5.1 Rules of Engagement (RoE).....	13
5.1.1 Purpose and Objectives.....	13
5.1.2 Scope.....	13
5.1.3 Authorised Techniques and Tools.....	13
5.2 Threat Emulation Plan (MITRE ATT&CK TTP Mapping).....	14
5.3 Lab Environment Setup & Network Design.....	16
5.4 Attack Narrative (Reconnaissance - Exfiltration).....	17
5.4.1 Reconnaissance.....	18
5.4.2 Initial Access to CPC-CT-WEB01.....	20
5.4.3 Internal Reconnaissance from CPC-CT-WEB01.....	23
5.4.4 Compromise of Dev/CI Server CPC-DEV-CICD01.....	23
5.4.5 R&D Server and Workstation Data Access and Exfiltration.....	25
5.5 Detection Gap Analysis.....	29
5.5.1 Web Layer (CPC-CT-WEB01).....	30
5.5.2 Dev/CI Infrastructure (CPC-DEV-CICD01).....	30
5.5.3 Workstation and R&D Environment.....	30
5.5.4 Active Directory Reconnaissance.....	30
5.5.5 Logging, Monitoring and Correlation.....	31
5.6 Strategic Recommendations.....	31
5.6.1 Web Application Security (CPC-CT-WEB01).....	31
5.6.2 Dev/CI Server Hardening (CPC-DEV-CICD01).....	31
5.6.3 Workstation and R&D Environment.....	31
5.6.4 Workstation and Active Directory Reconnaissance.....	32
5.6.5 Logging, Monitoring and Detection.....	32
5.7 Cost-Benefit Analysis.....	32
6. Conclusion).....	34

7. References)	35
----------------	----

1. Introduction

The healthcare sector and the pharmaceutical industry keep facing more attacks from advanced cyber threats. These areas hold valuable data along with complicated digital setups. They also rely heavily on constant operations without any breaks. Studies from recent years point out that healthcare groups deal with the biggest costs from data breaches on average. According to IBM's report from 2024, that cost sits at about 9.8 million USD. This figure comes out to more than twice the average across all industries [1]. Ransomware stands out as a major issue these days. Attackers often use double-extortion tricks. They steal information first and then lock it up to gain more power. They aim at key systems for patient care and billing processes [2].

This report splits into two key parts. Task 1 looks at the strategic risks from the ransomware hit on Change Healthcare in February 2024. That company falls under UnitedHealth Group. People call it the biggest healthcare data leak ever recorded [4], [5]. The review places the attacker's actions onto the MITRE ATT&CK Enterprise grid. It spots main problems in tech areas and management practices. Then it pulls together suggestions for stopping and spotting such threats early. Task 2 designs a red-team engagement, “Operation IP Shield”, for the fictional Cureton Pharmaceutical Company (CPC). In Task 2, Threat campaign is planned and emulated in a lab environment that mirrors CPC’s hybrid.

2. List of Figures and Tables

List of figures:

Figure 1: Change Healthcare Ransomware Attack Lifecycle Overview

Figure 2: CPC Lab Network Topology and Host Addressing

Figure-3: CPC Lab Network IP Pinging

Figure-4: CPC Attack Flow Diagram

Figure-5: CPC Web Portal Scanning Using Nmap

Figure-6: CPC CI-CD/Development Scanning Using Nmap

Figure-7: CPC Workstation Scanning Using Nmap

Figure-8: CPC R&D Domain Server Scanning Using Nmap

Figure-9: DVWA SQL Injection Normal Query Response

Figure-10: DVWA SQL Injection Exploitation via Burp Suite

Figure- 11: DVWA Reflected XSS Payload Execution

Figure-12: DVWA Reflected XSS Payload Execution Using Burp Suite

Figure-13: Internal Host Discovery from Compromised Web Server

Figure-14: Root Shell Access on CPC-DEV-CICD01

Figure-15: Nmap Service Scan of CPC-DEV-CICD01

Figure-16: Metasploit UnrealIRCd Backdoor Exploit Execution

Figure-17: SMB Share Enumeration on CPC-RD-Server

Figure-18: Research Data Access via SMB

Figure-19: SMB Access to Workstation Notes Using Valid Credentials

Figure-20: Workstation Research Data Access via SMB

Figure-21: Nmap Enumeration of R&D Domain Controller

Figure-22: Password Policy of R&D Domain Controller

Figure-23: Nessus Vulnerability Scan Configuration

Figure-24: Nessus Vulnerability Scan Results for CPC-DEV-CICD01

List of Tables:

Table-1: Selected MITRE ATT&CK TTPs in the Change Healthcare Campaign

Table-2: MITRE ATT&CK Mapping of Red Team Techniques Used in Operation IP Shield

Table-3: Cost–Benefit Summary for CPC Security Controls

3. List of Acronyms

1. **AD:** Active Directory
2. **APT:** Advanced Persistent Threat
3. **AV:** Antivirus
4. **AWS:** Amazon Web Services
5. **C2:** Command and Control
6. **CISA:** Cybersecurity and Infrastructure Security Agency (US)
7. **CPC:** Cureton Pharmaceutical Company
8. **CSP:** Content Security Policy
9. **CI/CD:** Continuous Integration / Continuous Deployment
10. **DC:** Domain Controller
11. **DLP:** Data Loss Prevention
12. **DVWA:** Damn Vulnerable Web Application
13. **EDR:** Endpoint Detection and Response
14. **FTP:** File Transfer Protocol
15. **FIDO2:** Fast Identity Online 2
16. **HC3:** Health Sector Cybersecurity Coordination Center (US HHS)
17. **HTTP:** Hypertext Transfer Protocol
18. **HTTPS:** Hypertext Transfer Protocol Secure
19. **IAM:** Identity and Access Management
20. **ICMP:** Internet Control Message Protocol
21. **IDS/IPS:** Intrusion Detection System / Intrusion Prevention System
22. **IEEE:** Institute of Electrical and Electronics Engineers
23. **IP:** Internet Protocol
24. **IRC:** Internet Relay Chat
25. **LSASS:** Local Security Authority Subsystem Service
26. **MFA:** Multi-Factor Authentication
27. **NLA:** Network Level Authentication
28. **Nmap:** Network Mapper
29. **OS:** Operating System
30. **OSINT:** Open-Source Intelligence
31. **PHI:** Protected Health Information
32. **RaaS:** Ransomware-as-a-Service
33. **R&D:** Research and Development
34. **RDP:** Remote Desktop Protocol
35. **RoE:** Rules of Engagement
36. **RPC:** Remote Procedure Call
37. **SANS:** SysAdmin, Audit, Network, and Security
38. **SIEM:** Security Information and Event Management
39. **SMB:** Server Message Block
40. **SQLi:** SQL Injection
41. **TTP:** Tactics, Techniques, and Procedures
42. **URL:** Uniform Resource Locator
43. **VM:** Virtual Machine

- 44. **VPC:** Virtual Private Cloud
- 45. **WAF:** Web Application Firewall
- 46. **WMI:** Windows Management Instrumentation
- 47. **XDR:** Extended Detection and Response
- 48. **XSS:** Cross-Site Scripting

4. Strategic Threat Analysis: Change Healthcare Ransomware Attack

4.1 Case Overview

Change Healthcare runs essential payment and revenue cycle services for a big part of the United States healthcare system. These services cover pharmacy benefit management along with claims processing and eligibility checks. The organization faced a serious ransomware attack on 21 February 2024. Experts link this incident to the ALPHV/BlackCat ransomware as a service (RaaS) operation [4], [6]. UnitedHealth Group reacted by isolating Change Healthcare's data centres from the broader network. This action triggered major disruptions in pharmacy claims, prescription handling, and payments to providers across the nation [4].

During testimony before the U.S. Senate Finance Committee, UnitedHealth's CEO explained that attackers first entered through a Citrix remote access portal. They used stolen credentials for this entry. The portal lacked multi factor authentication, which made it easier for them [4]. After gaining access, the attackers spread through the systems in advanced ways. This movement lasted about nine days. Then they released the ransomware on 21 February 2024 [4].

Later reports and official notifications indicate that the attackers stole large amounts of protected health information and other sensitive data before the encryption started [5], [7]. The breach likely affected around 190 million people. That makes it the biggest healthcare data incident ever based on the number of affected individuals [5]. UnitedHealth expects direct costs of about USD 1.4 to 1.6 billion just in 2024. These costs include recovery efforts, response measures, and aid to impacted providers [6].

4.2 Attack Timeline

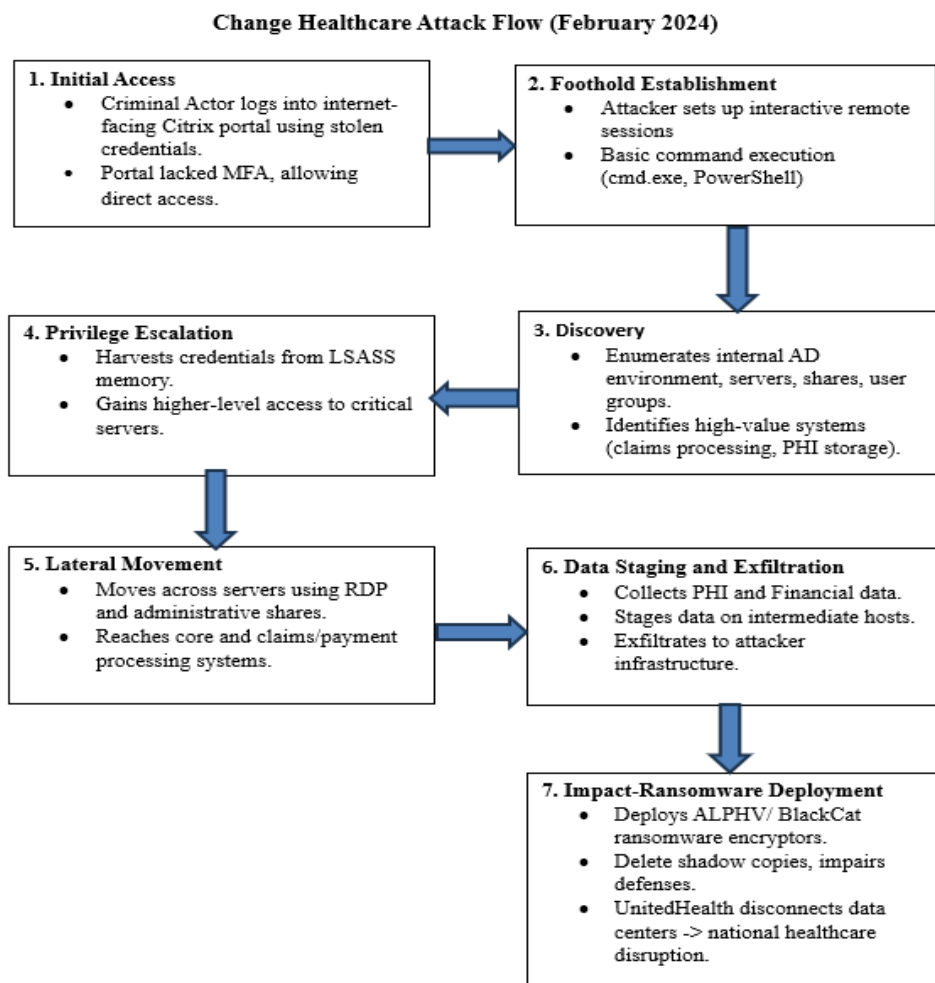


Figure 1: Change Healthcare Ransomware Attack Lifecycle Overview

Open sources material does not provide a complete forensic timeline. Still, blending public testimony with intelligence on ALPHV/BlackCat gives a solid outline of events [4, 7, 8, 9].

Before February 2024, the setup involved interconnected platforms at Change Healthcare. These handle a huge portion of U.S. healthcare payments. Such a central role means a wide internal network with many third-party links [4], [5].

On 12 February 2024, attackers gained initial entry. They used valid but compromised credentials to log into an internet exposed Citrix remote access portal. Since multi factor authentication was not in place, the username and password alone allowed full interactive access [4].

From 12 to 21 February 2024, the attackers built their position after entry. They spent roughly nine days on discovery of systems and network shares. They also raised privileges and shifted to machines tied to claims and payment functions [4], [7], [8]. Drawing from known ALPHV tactics, this phase probably relied heavily on standard Windows admin tools. It included credential extraction and remote-control methods [7, 8, 9].

Before 21 February 2024, the group prepared data for theft. They spotted sensitive files like protected health information (PHI) and financial details. Then they gathered these on intermediate servers and sent them out to their own setups. This matches BlackCat's approach of double extortion [5, 7, 8, 9].

On 21 February 2024, the ransomware went live on various systems. It locked data and halted many services [4], [7]. UnitedHealth then disconnected the data centres to limit spread. Service failures spread far and wide as a result.

After 21 February 2024, the attackers pushed for ransom. They leveraged both the encrypted systems and the stolen data. UnitedHealth launched a major recovery push. This covered system rebuilds and new security steps. At the same time, they informed regulators and partners about the breach [5], [6].

4.3 MITRE ATT&CK TTP Mapping

The MITRE ATT&CK Enterprise matrix gives a clear framework for mapping out the tactics and techniques that played a role in the Change Healthcare breach [3], [10].

Tactic	Technique (ID)	Case manifestation (Procedure)
Initial Access	Valid Accounts (T1078)	Use of compromised Change Healthcare credentials to authenticate to Citrix without MFA [4], [7].
Initial Access	External Remote Services (T1133)	Abuse of an internet-facing Citrix remote access portal to gain interactive access into internal networks [4], [7].
Execution	Command and Scripting Interpreter (T1059)	Use of cmd.exe and PowerShell for discovery, tooling and later ransomware deployment, a standard BlackCat pattern [7, 8, 9].
Credential Access	OS Credential Dumping (T1003.001)	Dumping of LSASS memory to harvest additional credentials, as documented in multiple ALPHV intrusions [7, 8, 9].
Discovery	Remote System Discovery (T1018)	Enumeration of servers and services to identify claims and payment systems during the nine-day period [4], [7], [8].
Discovery	Network Share Discovery (T1135)	Identification of network shares hosting PHI and financial data prior to staging [7, 8, 9].
Discovery	File and Directory Discovery (T1083)	Local file-system enumeration to locate data repositories and configuration files [7, 8, 9].
Lateral Movement	Remote Services: Remote Desktop Protocol (T1021.001)	Lateral movement between servers via RDP or similar remote-administration protocols, as widely observed in BlackCat campaigns [7, 8, 9].
Collection	Data Staged (T1074)	Aggregation of selected datasets on staging hosts before exfiltration as part of the double-extortion model [5, 7, 8, 9].
Exfiltration	Exfiltration Over C2 Channel (T1041) / Exfiltration to Cloud Storage (T1567)	Transfer of staged data over encrypted channels or to cloud storage controlled by the attacker, prior to public leak threats [5, 7, 8, 9].
Defense Evasion	Defenses Disable or Modify Tools (T1562.001)	Disabling or tampering with security tools, clearing logs and deleting shadow copies to hinder detection and recovery [7, 8, 9].

Impact	Data Encrypted for Impact (T1486)	Deployment of ALPHV ransomware payloads to encrypt data and disrupt services across Change Healthcare's environment [4, 7, 8, 9].
--------	-----------------------------------	---

Table-1: Selected MITRE ATT&CK TTPs in the Change Healthcare Campaign

Not every one of these techniques shows up in official reports. Still, the choices line up well with known ALPHV practices [7], [8], [9]. They also fit the pattern seen in the long time the attackers stayed inside, the data they took out before encrypting things, and the huge effects across the board.

4.4 Root Cause Analysis

The Change Healthcare incident cannot be explained by a single exploited vulnerability. Instead, it reflects multiple interacting root causes across control, architectural and governance domains.

4.4.1 Control Failures

The lack of MFA on a key remote access portal exposed to the internet. With how common credential theft and password reuse have become, it is hard to defend using only usernames and passwords for a vital healthcare hub in 2024 [1], [2], [4]. This gap let in ATT&CK techniques T1078 and T1133 right away.

A second problem showed up in early detection efforts. The attackers held access for about nine days before the ransomware hit [4]. In that time, standard ALPHV moves like credential dumping, checking network shares, and moving sideways through RDP would have set off alerts in a solid EDR or SIEM setup [7], [8], [9]. The lack of intervention suggests that either such tools were not deployed consistently and effectively monitored.

Third, controls on pulling out data seemed limited. Big moves of protected health info and financial details from main systems to unusual spots should have raised alerts. This holds especially true for a group dealing with tightly regulated data [5]. That points to gaps in data loss prevention or checks on network behaviour.

4.4.2 Architectural and Third-Party Weaknesses

On the architecture side, Change Healthcare acted as a single weak spot for much of the billing and pharmacy work in U.S. healthcare. The downtime made it clear that hitting one vendor could affect and disrupt thousands of separate groups [4], [5]. This setup shows a need for more spread-out options and backup plans across the system.

Inside Change Healthcare's own setup, attackers shifted easily from the remote portal to core areas. That suggests network splits around top priority assets were not strong enough. MITRE's guidance for healthcare emphasises identification and isolation of those key systems. It calls for layers of security between them and outside entry points [3].

Lastly, the breach highlighted issues in managing third-party governance. Many affected hospitals and providers had little direct control over Change Healthcare's internal security posture as depended on its availability and integrity. Existing regulatory frameworks and contractual arrangements had not ensured that a vendor in such a critical position applied contemporary baseline controls such as MFA, zero-trust design and continuous security validation.

4.4.3 Organisational and Sectoral Factors

Within the organization, skipping basic controls like MFA on key services shows a mismatch between what risks seemed like and the real threats out there. Studies from academics and industry point out that healthcare groups often spend too little on security compared to ransomware dangers and data leaks. They focus more on keeping things running short-term and holding down costs [1], [2].

4.5 Strategic Recommendations

The Change Healthcare example shows the attack path was not new trick rather a standard ransomware script that hit known weak spots. So, strategic recommendations can be grounded in existing best practice and ATT&CK-informed defence principles [2], [3], [10], [11].

4.5.1 Strengthen Initial Access and Authentication

1. **Mandatory phishing-resistant MFA for all remote access.**

Every outside remote access tool like Citrix, VPN, RDP gateways, or cloud portals needs phishing-resistant MFA. Things like FIDO2 or hardware keys work for this. It blocks T1078 and T1133 by making sure stolen logins alone are insufficient.

2. **Risk-based and device-aware access control.**

Set up access policies that consider device health, location, time, and risk flags. Block or limit logins from unmanaged or risky devices.

3. **Credential hygiene and rapid revocation.**

Push for strong password policies, minimise shared accounts, and revoke logins quickly for ex-employees or partners.

4.5.2 Implement Zero-Trust Segmentation and Privilege Management

1. **Segmentation around intellectual systems.**

Do a full check on intellectual properties to find systems where a breach would hit hard, like claims switches or pharmacy approvals. Put them in tight network zones with few links and strict entry rules. This follows zero-trust principles [3].

2. **Least-privilege and just-in-time admin.**

Replace standing administrative privileges with just-in-time elevation controlled by privileged access management workflows. It limits moves like T1069 and T1021 by narrowing privileged routes.

3. **Harden lateral movement pathways.**

Limit RDP and admin shares to special management networks, turn off unnecessary remote protocols, and use tough host firewalls.

4.5.3 ATT&CK Monitoring and Detection

1. **EDR/XDR tuned to ransomware TTPs.**

Deployment of endpoint detection and response on all servers and workstations. Tune it to catch ransomware signs like odd PowerShell runs (T1059), credential pulls (T1003.001), heavy share scans (T1135), and shadow copy wipes or antivirus tweaks (T1562.001, T1490) [7], [8], [9].

2. **Network-level exfiltration analytics.**

Put in network behaviour checks and data loss tools aimed at sensitive areas. Sudden increase in data shifting to new spots, especially from PHI or payment servers, need to trigger alerts and auto responses.

3. Continuous ATT&CK-based security validation.

Run tools that mimic attackers and map to ATT&CK to see if controls really stop full attack flows [10], [11]. Do regular simulation that copy ALPHV attacks. They can uncover hidden gaps in detection logic and push for continuous improvement.

4.5.4 Resilience, Third-Party Governance and Economic Justification

1. Architect for graceful degradation and failover.

For key areas like claims and payments, build in switches to other vendors or offline setups.

2. Strengthen third-party minimums and oversight.

Regulators and big payers need to set and require baseline rules for vital vendors in the sector including MFA, segmentation, EDR, tested response plans, and duties to report issues.

3. Frame security investment as risk reduction, not pure cost.

The Change Healthcare hit cost around USD 1.4 to 1.6 billion [6]. Weigh that against the price of adding MFA, segmentation, EDR, and security validation checks. It shows a strong cost-benefit ratio. IBM's data on average healthcare breach costs further supports the argument that proactive investment is economically rational, reducing both expected loss and tail risk [1].

5. Red Team Engagement (Operation IP Shield)

5.1 Rules of Engagement (RoE)

5.1.1 Purpose and Objectives

The main goal involves simulating a targeted attack in the style of an advanced persistent threat against Cureton Pharmaceutical Company. This simulation aims to evaluate how straightforward it would be to steal dummy research data from a hybrid research and development setup. The focus stays on techniques that feel realistic yet remain under control. These techniques include web exploitation along with internal reconnaissance. They also cover exploitation of services that have vulnerabilities. Further aspects involve abuse related to Windows and SMB systems. The process ends with data exfiltration. From this exercise, technical findings emerge for the blue team at CPC. Business level insights appear for the management there as well.

5.1.2 Scope

In-scope lab systems:

- CPC-CT-WEB01
OWASP/Kali web host running DVWA (clinical trial portal simulation).
- CPC-DEV-CICD01
Metasploit Linux host simulating a vulnerable Dev/CI server.
- CPC-RD-WKS01
Windows 7 R&D workstation.
- CPC-RD-Server
Windows Server acting as research and development server (ResearchShare, clients note share etc).
- Attacker hosts
Kali Linux used for Nmap, Burp Suite, Metasploit, enum4linux, rpcclient, smbclient.
- Windows host for running Nessus Essentials.

Out of scope:

- Home router and ISP equipment.
- Personal mobile devices and laptops.
- Any systems outside of local lab setup.

5.1.3 Authorised Techniques and Tools

Authorised techniques:

- Reconnaissance & Discovery
 - Nmap host and service scanning on 192.168.0.61-64.
 - Internal host discovery via ICMP and simple ping loops from compromised web server.
- Initial Access (Portal)

- SQL injection reflected XSS and command injection against DVWA on CPC-CT-WEB01.
- Use of Burp Suite Community for intercepting and modifying DVWA requests.
- Dev/CI Exploitation
 - Exploitation of known services on CPC-DEV-CICD01, specifically UnrealIRCd (exploit/unix/irc/unreal_ircd_3281_backdoor).
- Windows Domain Controller Reconnaissance
 - Nmap of Windows ports (135/139/445, optionally 88/389) on 192.168.0.64.
 - enum4linux and rpcclient against 192.168.0.64 for account, group, share and policy discovery.
- Lateral Movement & Data Access
 - SMB share enumeration and access using valid lab accounts (CPC_RESEARCH, CPC_RD_WKSS01) on 192.168.0.64.
 - Optional SMB access to workstation-style data hosted on the R&D server.
- Exfiltration
 - Copying dummy research files (CPC_RESEARCH_CONFIDENTIAL_DATA.txt, workstation notes) from Windows server shares to the attacker machine over SMB.
- Vulnerability Assessment
 - Nessus Essentials scans from the Windows host, primarily against 192.168.0.61-64.

Authorised tools:

- Nmap, Burp Suite Community, Metasploit, enum4linux, rpcclient, smbclient, standard Linux/Windows CLI tools, Nessus Essentials.

5.2 Threat Emulation Plan (MITRE ATT&CK TTP Mapping)

Phase	Lab Activity	ATT&CK Tactic	Technique ID & Name
Initial web foothold	Exploited DVWA SQL injection, reflected XSS and command injection on CPC-CT-WEB01	Initial Access	T1190 Exploit Public-Facing Application; T1059 Command & Scripting Interpreter; T1059.007 JavaScript

Web to OS foothold	Used DVWA command injection to run whoami, uname -a, ping sweep from the web server	Execution / Discovery	T1059 Command & Scripting Interpreter; T1082 System Information Discovery; T1018 Remote System Discovery
Internal host & service discovery	Nmap scans of 192.168.0.61–64; identification of UnrealIRCd, SMB, RPC, etc.	Discovery	T1046 Network Service Scanning; T1018 Remote System Discovery
Dev/CI compromise (CPC-DEV-CICD01, 62)	Metasploit exploit/unix/irc/unreal_ircd_3281_backdoor against TCP/6667; obtained root shell	Initial Access / Execution	T1190 Exploit Public-Facing Application/Service; T1059 Command & Scripting Interpreter
Windows reconnaissance on R&D server	Nmap on 192.168.0.64 ports; enum4linux -a and rpcclient (srvinfo, enumdomusers, enumdomgroups)	Discovery	T1087 Account Discovery; T1069.001 Permission Groups Discovery (Domain/Local Groups); T1201 Password Policy Discovery
SMB share discovery	smbclient -L 192.168.0.64 -U <user> to enumerate ResearchShare, CPC_RESEARCH, CPC_RD_WKS01_NOTES	Discovery	T1135 Network Share Discovery
Abuse of research file and workstation	Used CPC_RESEARCH and CPC_RD_WKSS01 credentials to access SMB shares on 192.168.0.64	Credential Access / Lateral Movement	T1078 Valid Accounts
Lateral-style access to workstation data	Used workstation-style account to access CPC_RD_WKS01_NOTES share and download notes	Lateral Movement	T1021.002 Remote Services: SMB/Windows Admin Shares
Research data exfiltration	Downloaded CPC_RESEARCH_CONFIDENTIAL_DATA.txt from \\192.168.0.64\ResearchShare to Kali over SMB	Exfiltration	T1041 Exfiltration Over C2/Command Channel (SMB used as the exfil path)

Vulnerability assessment (dev server)	Ran Nessus Essentials against 192.168.0.62 and reviewed high-risk findings (Samba, NFS, DNS, SMB issues)	Discovery	T1046 Network Service Scanning (automated scanner)
---------------------------------------	--	-----------	--

Table-2: MITRE ATT&CK Mapping of Red Team Techniques Used in Operation IP Shield

5.3 Lab Environment Setup & Network Design

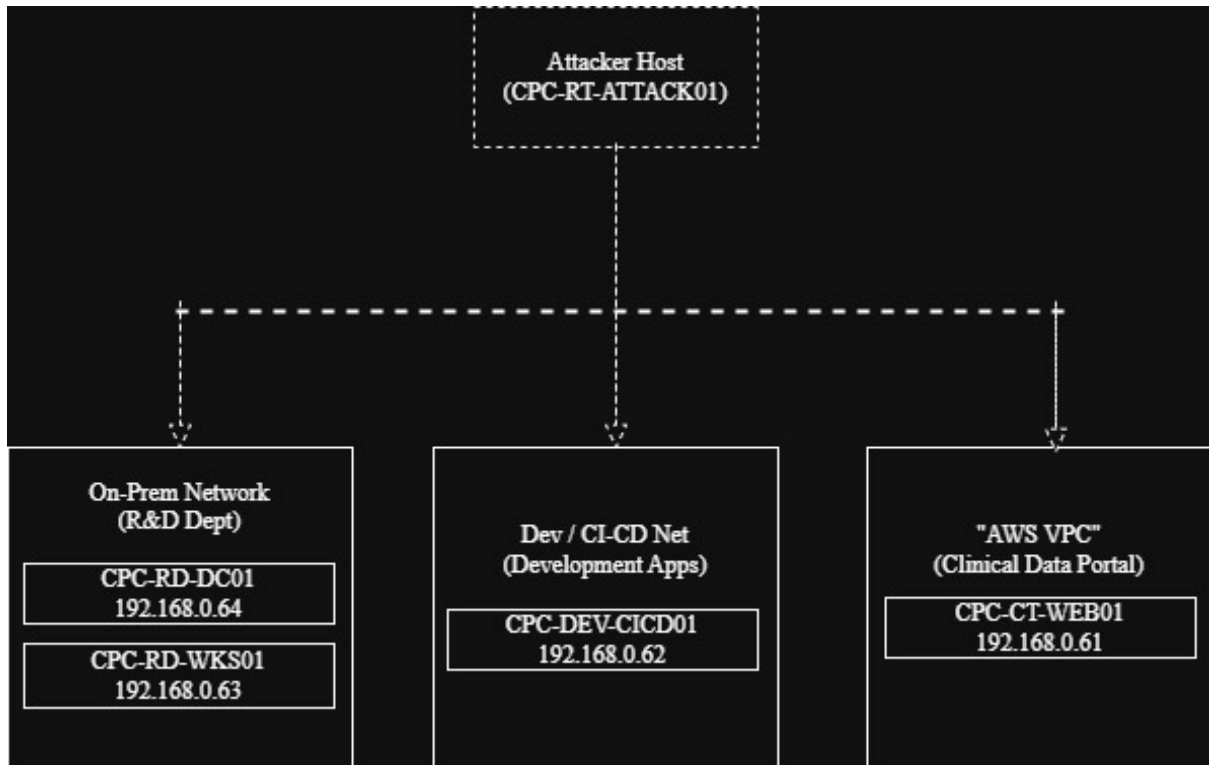


Figure 2: CPC Lab Network Topology and Host Addressing

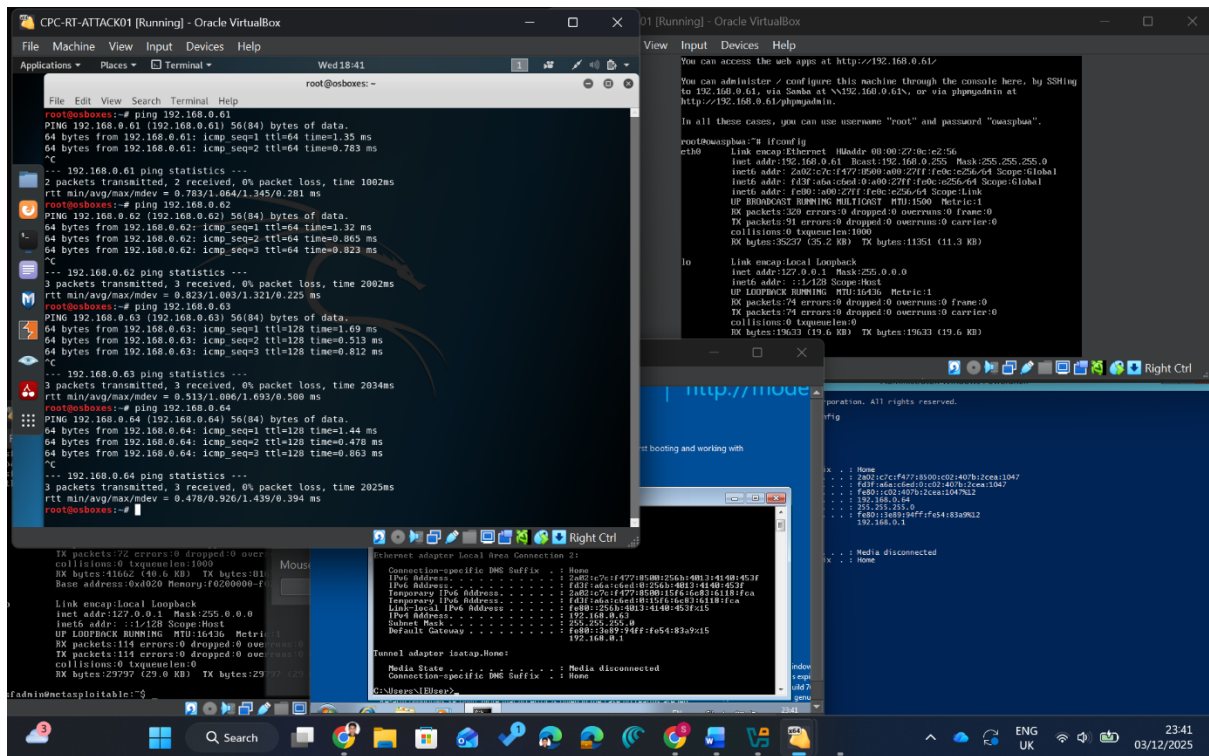


Figure-3: CPC Lab Network IP Pinging

5.4 Attack Narrative (Reconnaissance - Exfiltration)

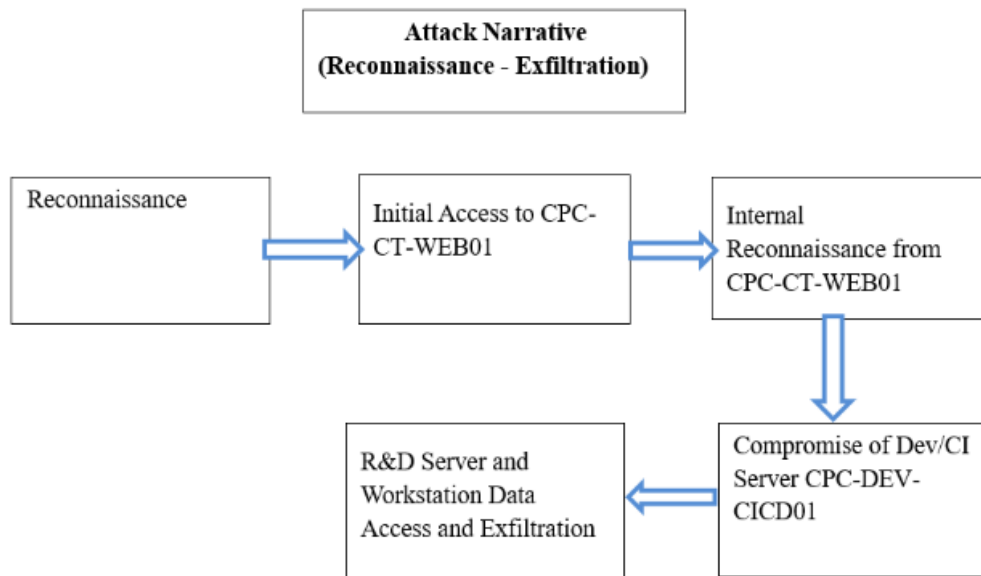


Figure-4: CPC Attack Flow Diagram

5.4.1 Reconnaissance

Nmap service enumeration was used to identify active hosts and exposed services within the lab environments. Four target systems were discovered.

- CPC-CT-WEB01 – Clinical trial web server hosting Apache, Tomcat, Jetty and Samba services, proving multiple potential web exploitation vectors.
- CPC-DEV-CICD01 – Development server exposing numerous insecure and outdated services, including VSFTPD 2.3.4, Telnet, Samba, MySQL, PostgreSQL, NFS and an open bindshell, representing a highly vulnerable asset.
- CPC-RD-WKS01 – R&D workstation exposing SMB and RPC services typical of a user endpoint, presenting opportunities for lateral movement and credential access.
- CPC-RD-DC01 – Windows server domain controller exposing active directory related services, including SMB and multiple RPC endpoints domain. It is confirmed that it works as the primary authentication and directory service for the lab domain.

The results from this recon shaped the rest of the attack path. The CPC-CT-WEB01 was chosen as the way to get initial access. From there, the plan involved lateral movement inside to CPC-DEV-CICD01, CPC-RD-WKS01, and CPC-RD-DC01 which became the key points for pulling out data.

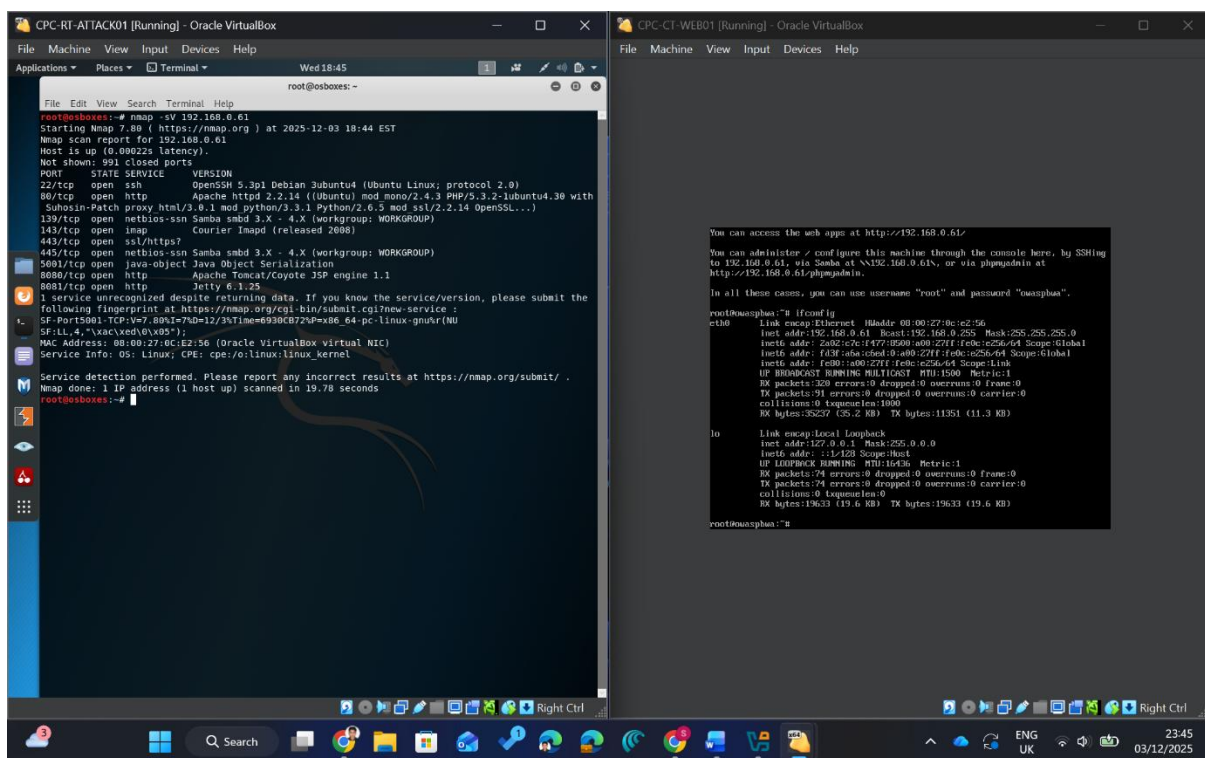


Figure-5: CPC Web Portal Scanning Using Nmap

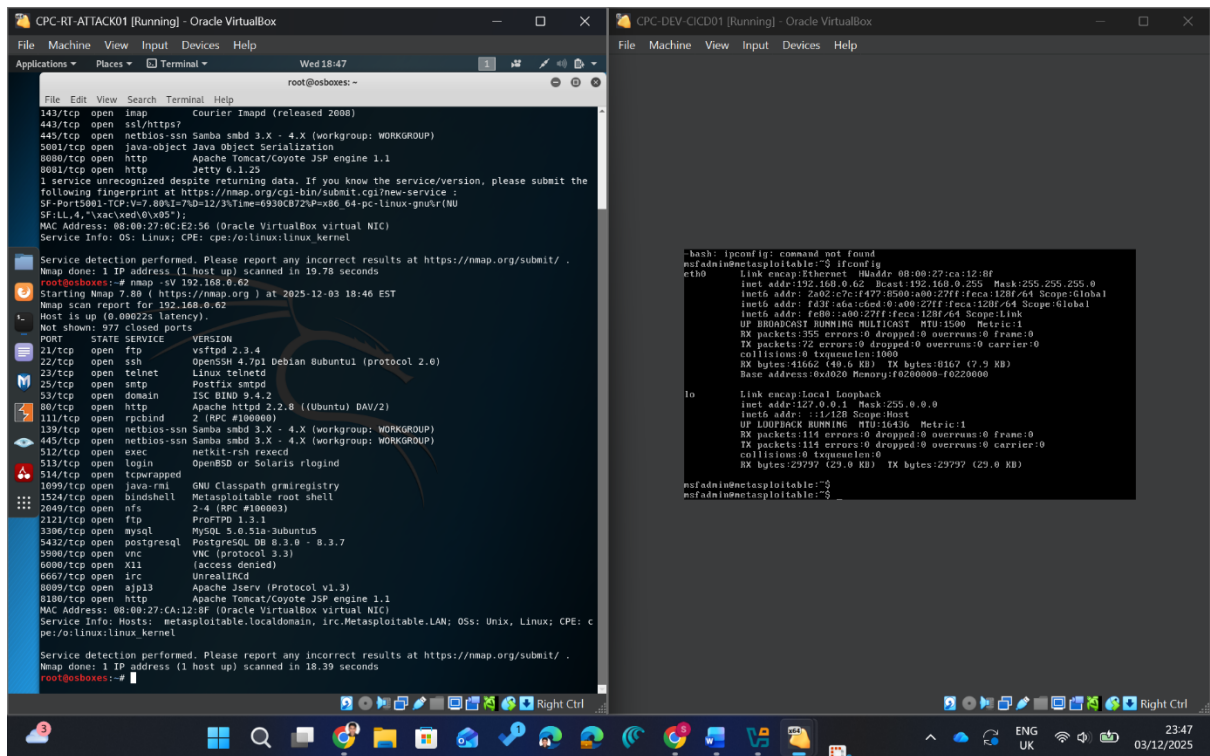


Figure-6: CPC CI-CD/Development Scanning Using Nmap

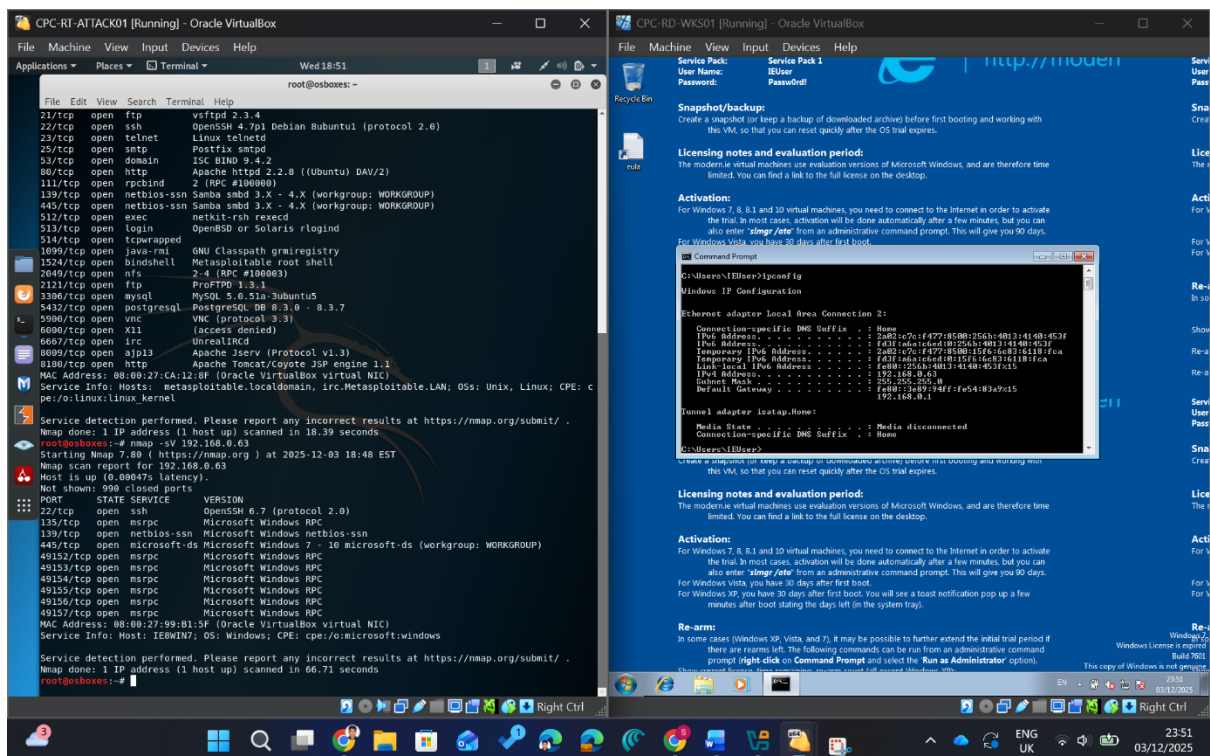


Figure-7: CPC Workstation Scanning Using Nmap

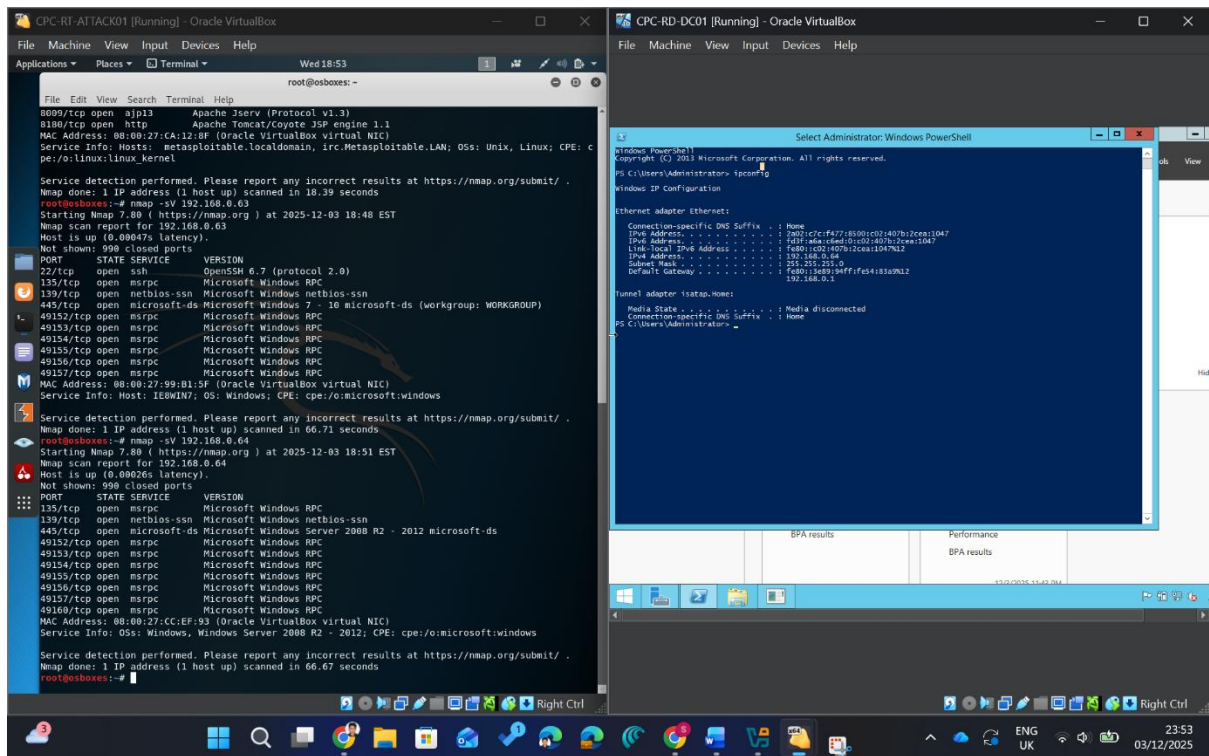


Figure-8: CPC R&D Domain Server Scanning Using Nmap

5.4.2 Initial Access to CPC-CT-WEB01

- On DVWA SQL injection page, id = 1 returned a single “admin” record (Fig. 9). Then, the parameter was set to 1' OR '1'='1 in Burp Suite repeater returned multiple users.
- The XSS (Reflected) inputting <script>alert('Md.Mashrurul Haque');</script> triggered an alert in browser. (Fig. 11).

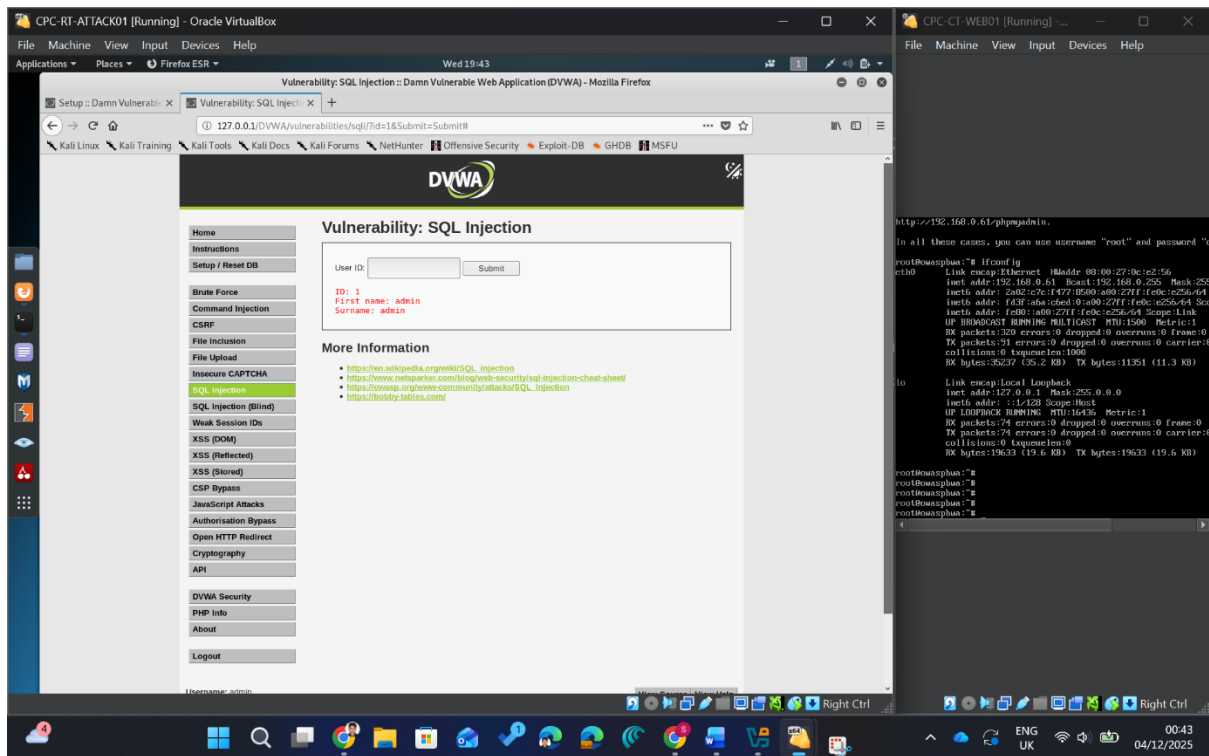


Figure-9: DVWA SQL Injection Normal Query Response

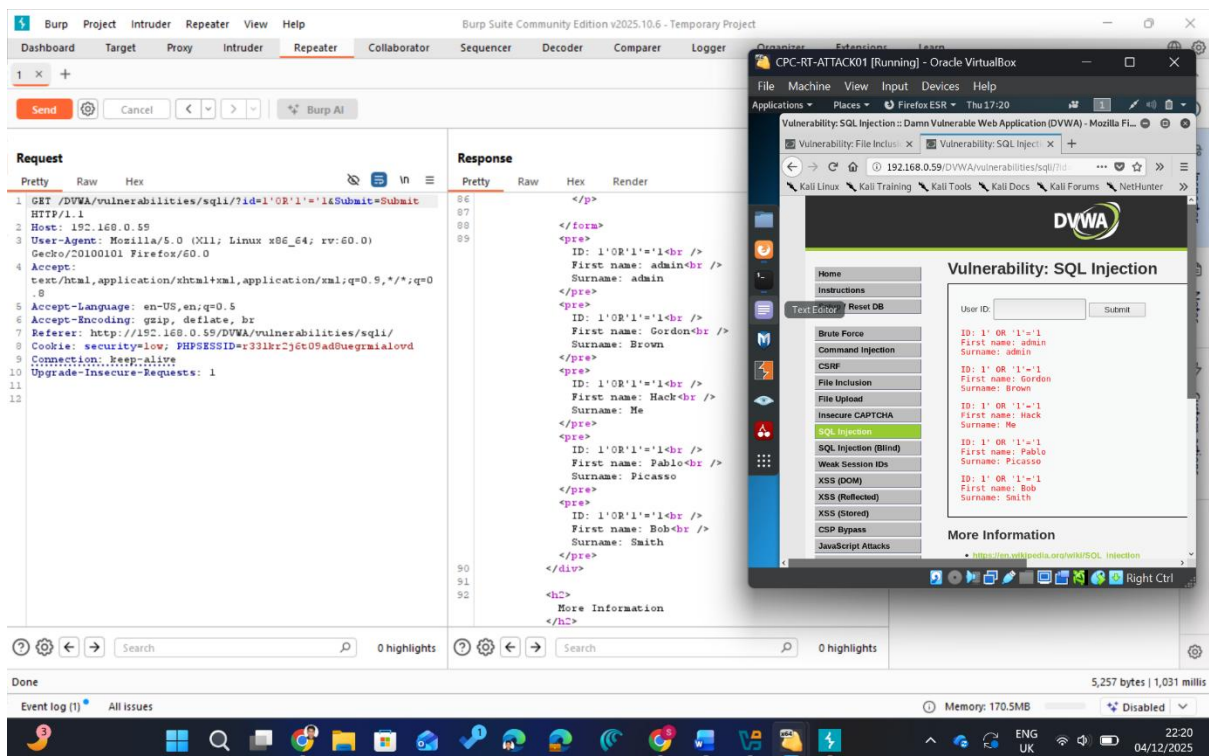


Figure-10: DVWA SQL Injection Exploitation via Burp Suite

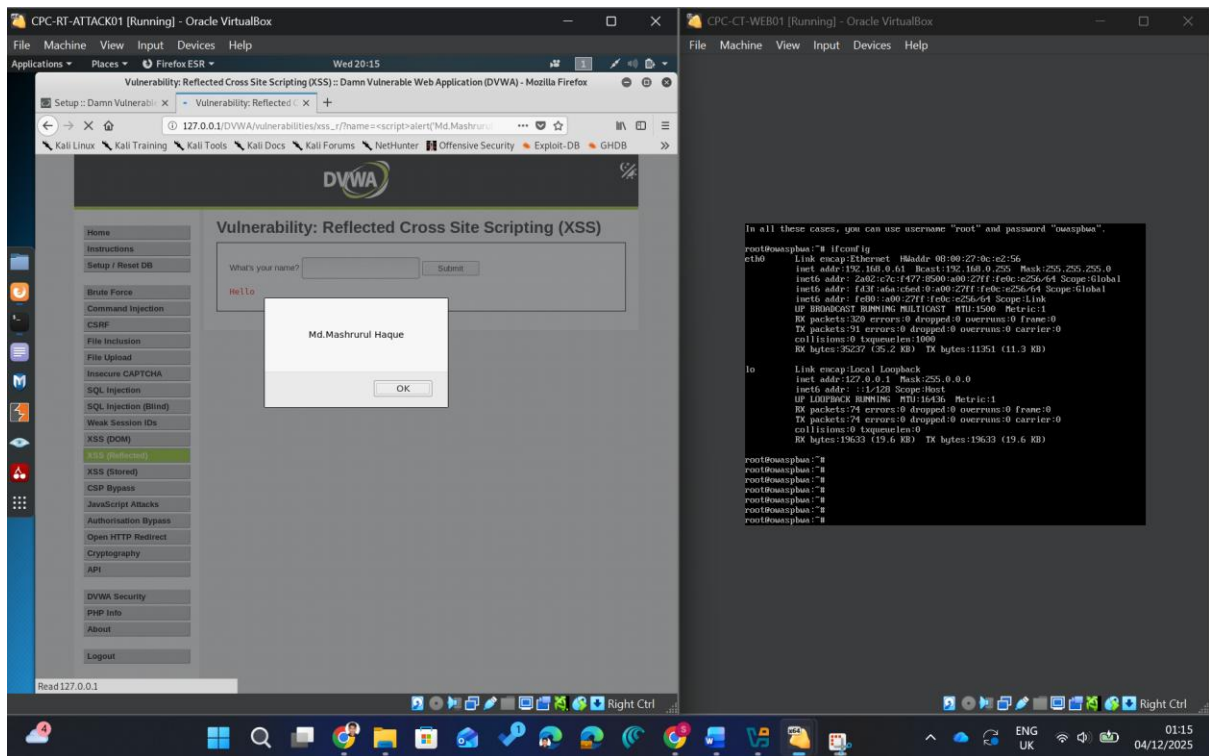


Figure- 11: DVWA Reflected XSS Payload Execution

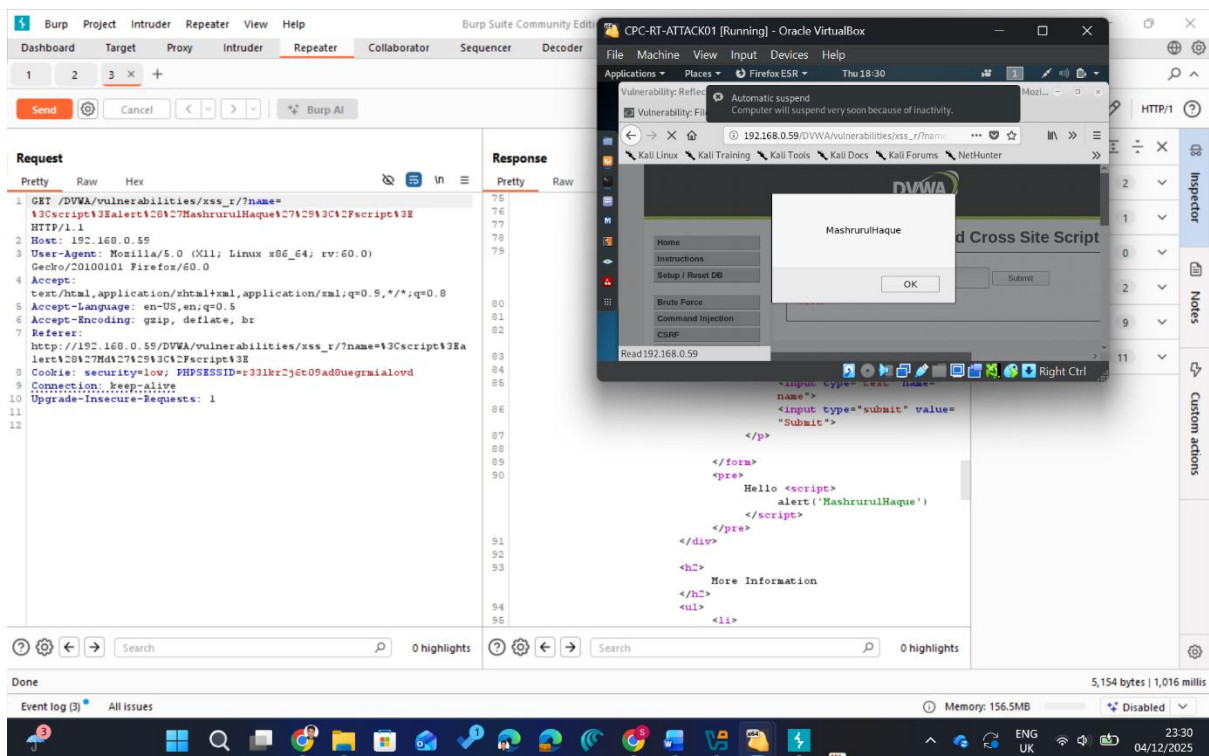


Figure-12: DVWA Reflected XSS Payload Execution Using Burp Suite

5.4.3 Internal Reconnaissance from CPC-CT-WEB01

Again, in DVWA Command Injection page, the input “127.0.0.1; for i in \$(seq 61 64); do ping -c 1 192.168.0.\$i; done” was sent (Fig. 13) which showed successful replies from hosts.

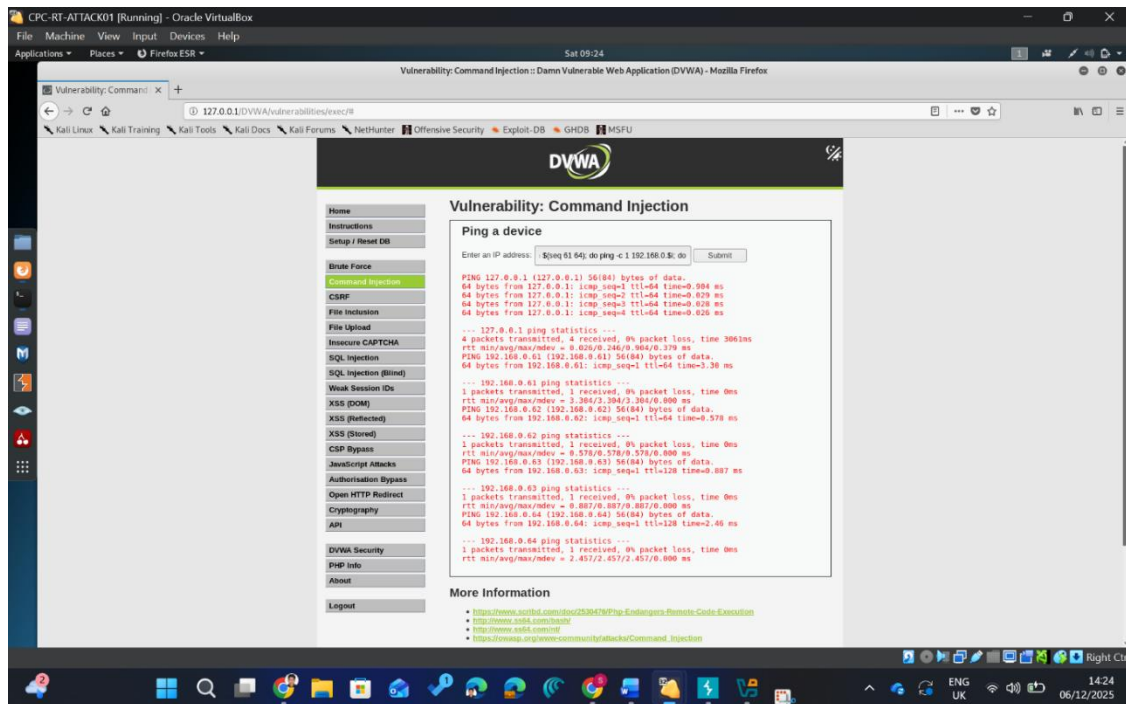


Figure-13: Internal Host Discovery from Compromised Web Server

5.4.4 Compromise of Dev/CI Server CPC-DEV-CICD01

- Nmap showed that 192.168.0.62 exposed many insecure services, including UnrealIRCd on TCP/6667.
- In Metasploit, the module exploit/unix/irc/unreal_ircd_3281_backdoor was run against 192.168.0.62:6667 (Fig. 16).
- The exploit opened a remote shell session. Commands such as id, uname -a, hostname and ifconfig confirmed root access on the Metasploitable dev/CI host.

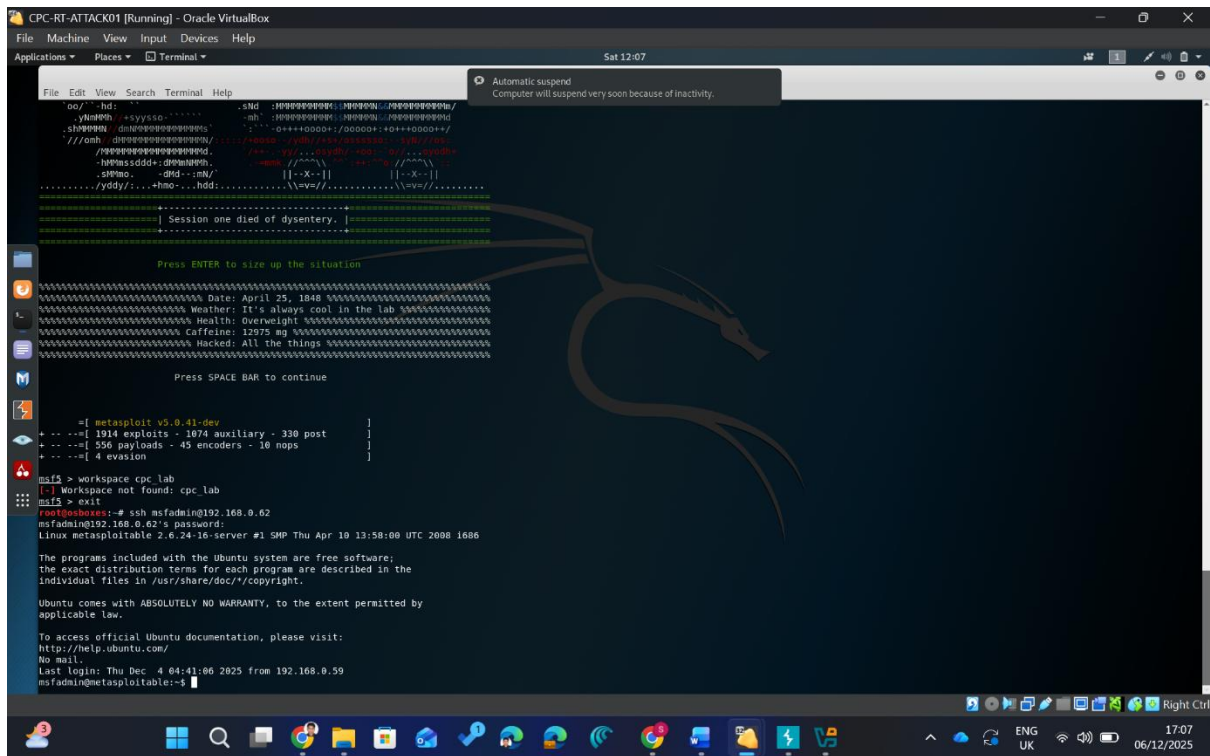


Figure-14: Root Shell Access on CPC-DEV-CICD01

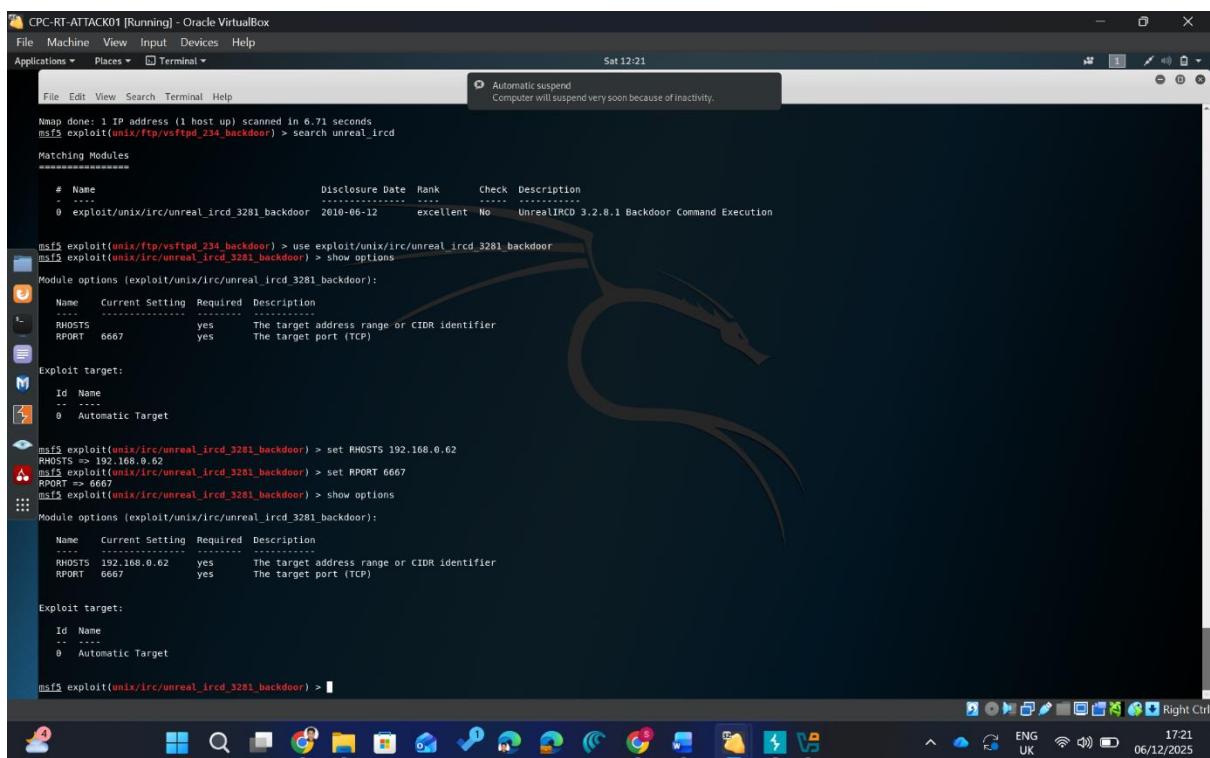


Figure-15: Nmap Service Scan of CPC-DEV-CICD01

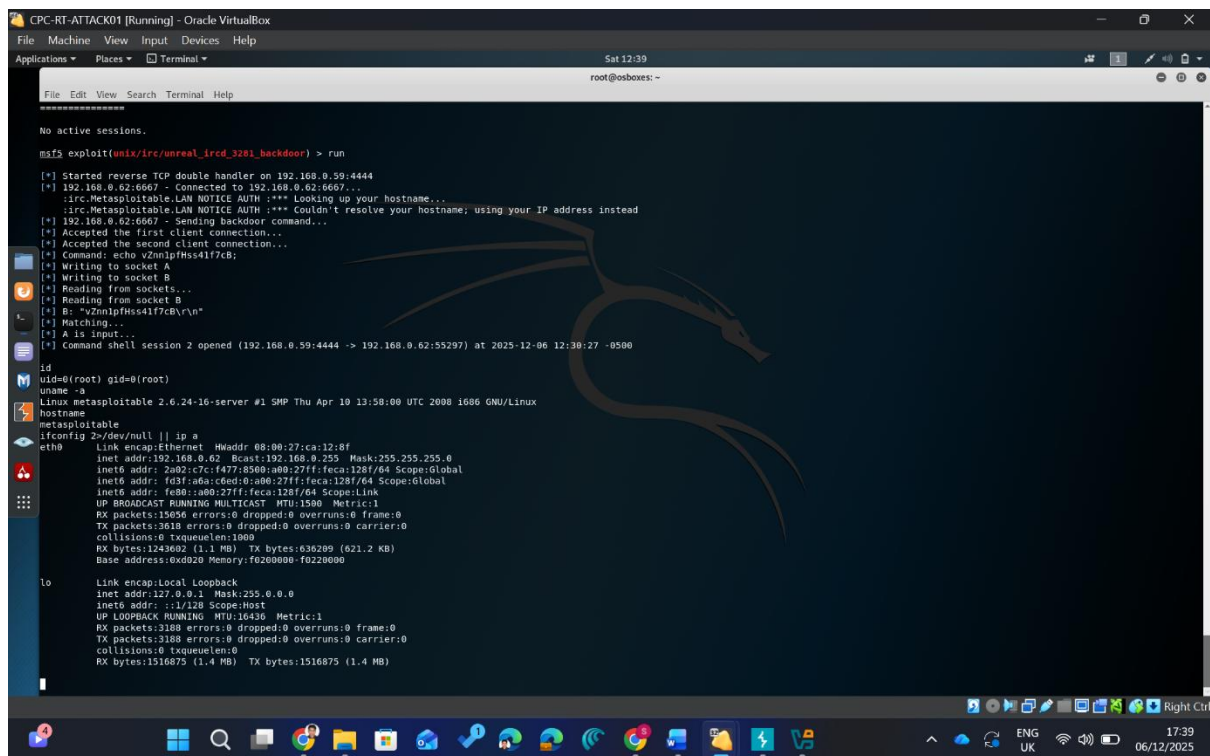


Figure-16: Metasploit UnrealIRCD Backdoor Exploit Execution

5.4.5 R&D Server and Workstation Data Access and Exfiltration

- From Kali, smbclient -L 192.168.0.64 -U CPC_RESEARCH was used to enumerate SMB shares on the R&D server. The output showed ResearchShare, CPC_RESEARCH and CPC_RD_WKS01_NOTES as available shares (Fig. 17).
- The attacker then connected to the research share with smbclient 192.168.0.64/ResearchShare -U 'WIN-P29CAIVMQGQ\CPC_RESEARCH'. Then Running ls revealed the file CPC_RESEARCH_CONFIDENTIAL_DATA.txt. After that, file was downloaded with get CPC_RESEARCH_CONFIDENTIAL_DATA.txt and later viewed on Kali with cat, confirming successful extraction of the dummy research data (Fig. 18)
- A scan was run on 192.168.0.64 using nmap -sV -p 88,135,139,389,445 192.168.0.64 which confirmed exposed Windows RPC and SMB services and consistent with an R&D file server.
- A “workstation” account (CPC_RD_WKSS01) was then used to authenticate to the same R&D server smbclient -L 192.168.0.64 -U 'WIN P29CAIVMQGQ\CPC_RD_WKSS01'. This account could see and access the CPC_RD_WKS01_NOTES share and download its note file via get. This demonstrate that the workstation credentials could also read stored workstation data on the R&D server, supporting lateral movement and data exposure from a client context.
- Nessus Essentials was run from the Windows host against the CPC lab range. Due to network and routing constraints, only the dev/CI server at 192.168.0.62 returned full

scan results (Fig. 24). The report for 192.168.0.62 showed many medium and high-risk findings. It showed outdated services (e.g. Samba, NFS, DNS and SMB-related issues).

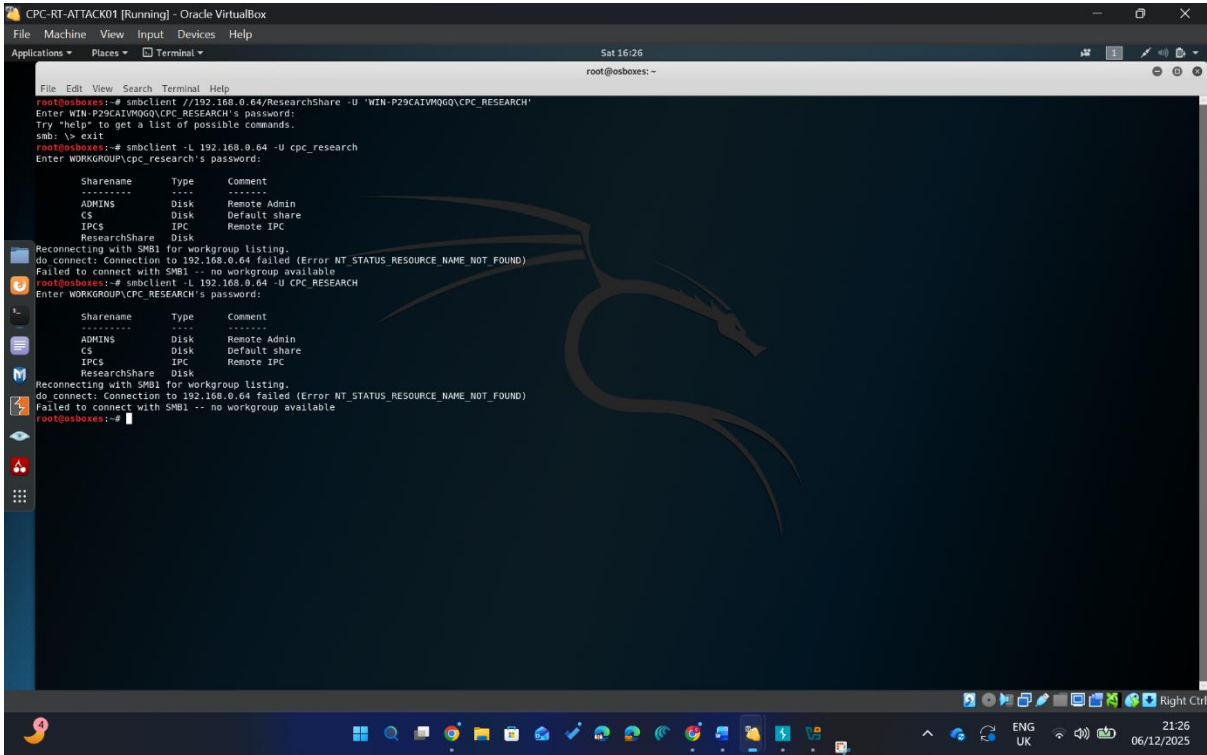


Figure-17: SMB Share Enumeration on CPC-RD-Server

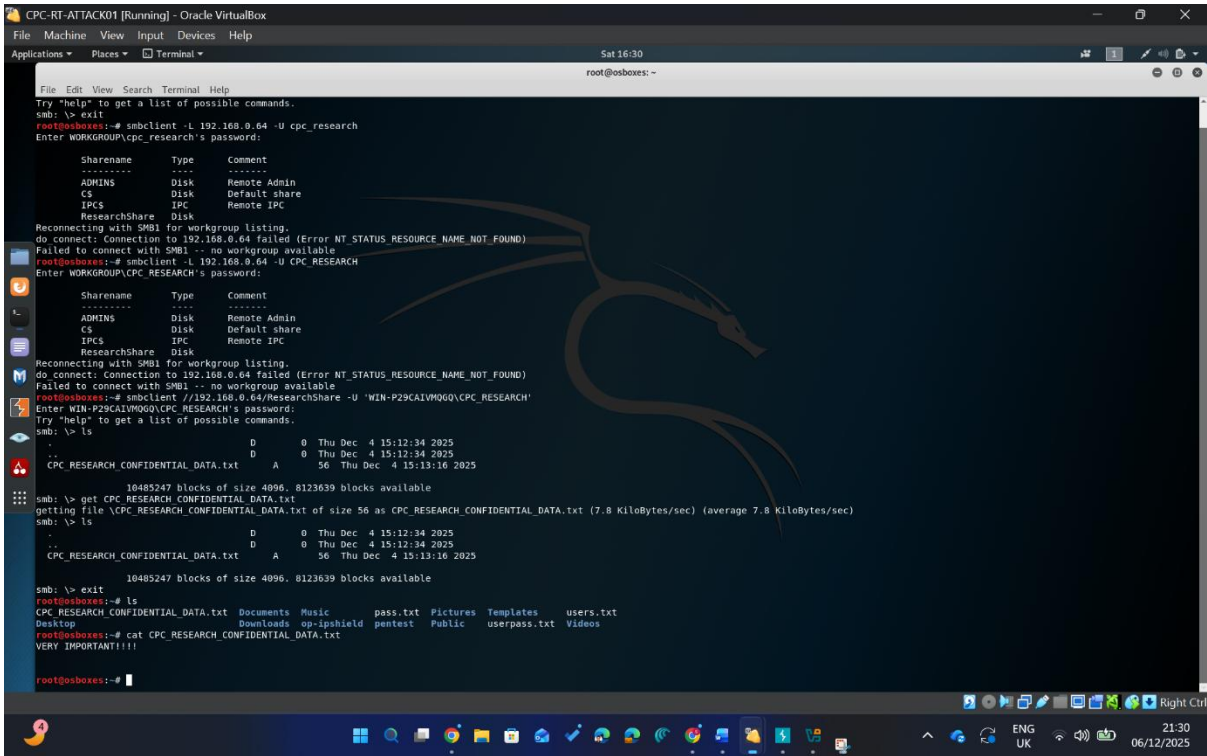


Figure-18: Research Data Access via SMB

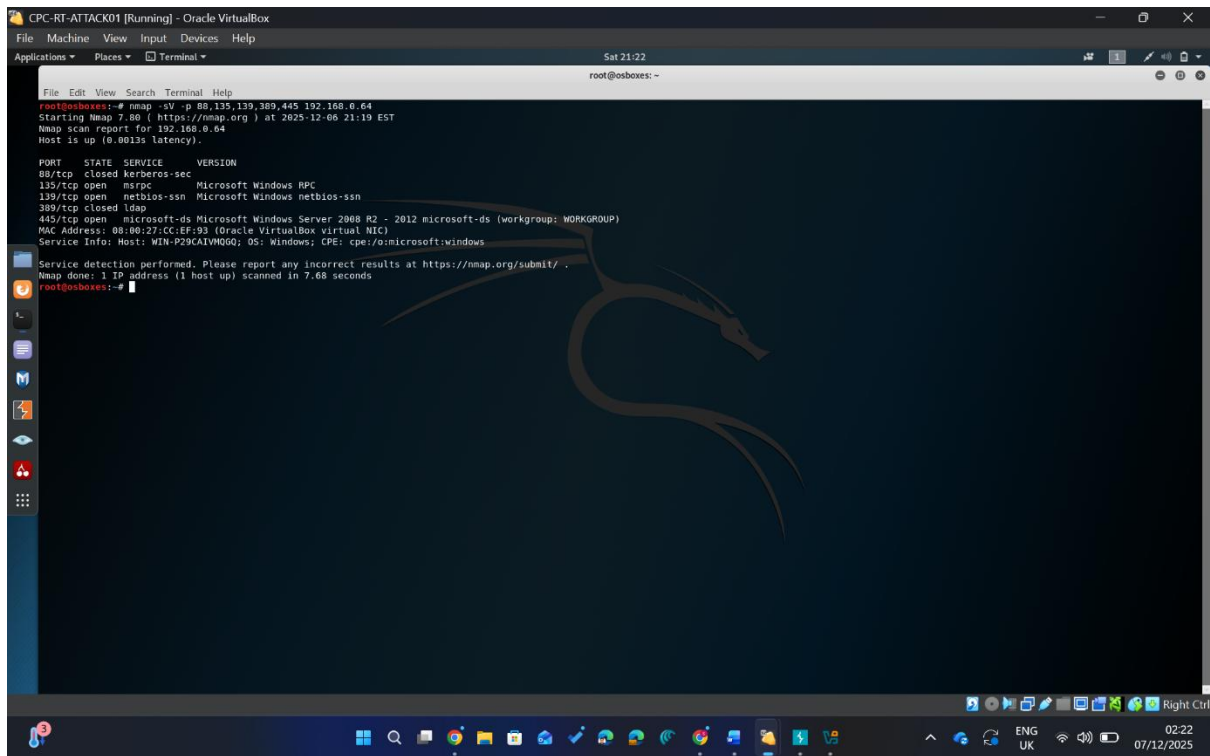


Figure-21: Nmap Enumeration of R&D Domain Controller

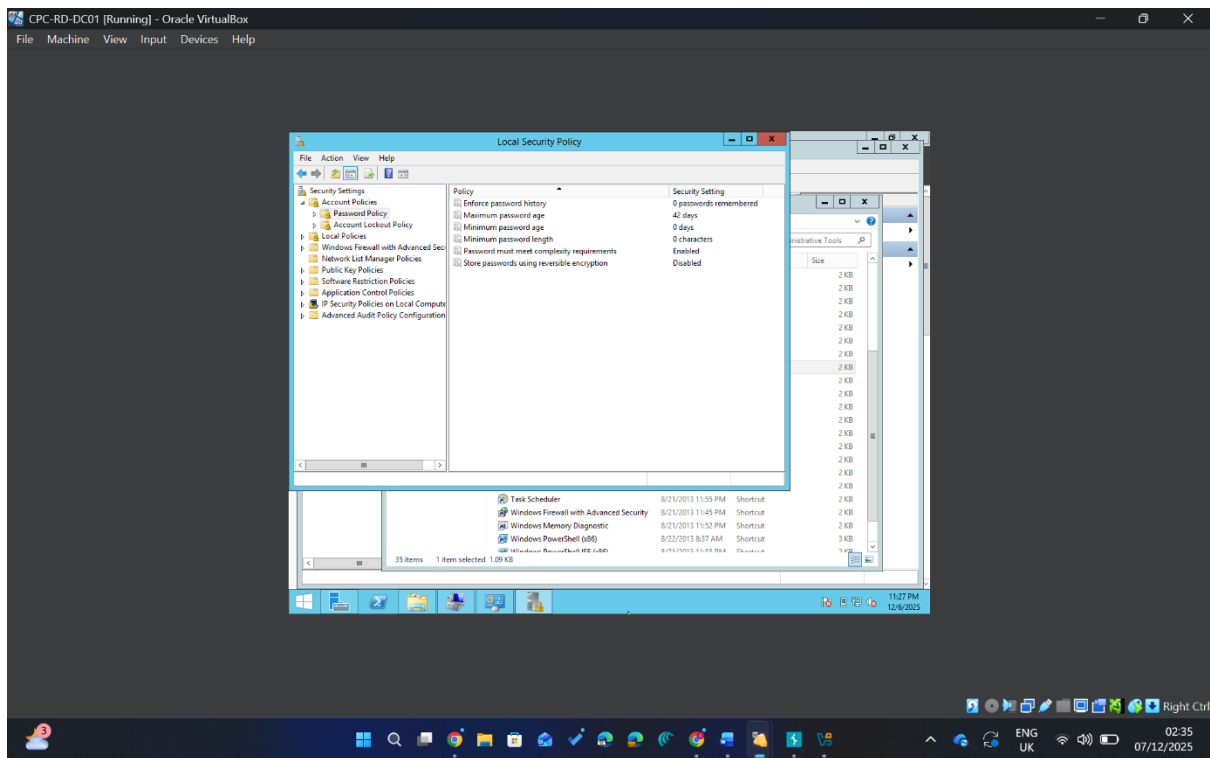


Figure-22: Password Policy of R&D Domain Controller

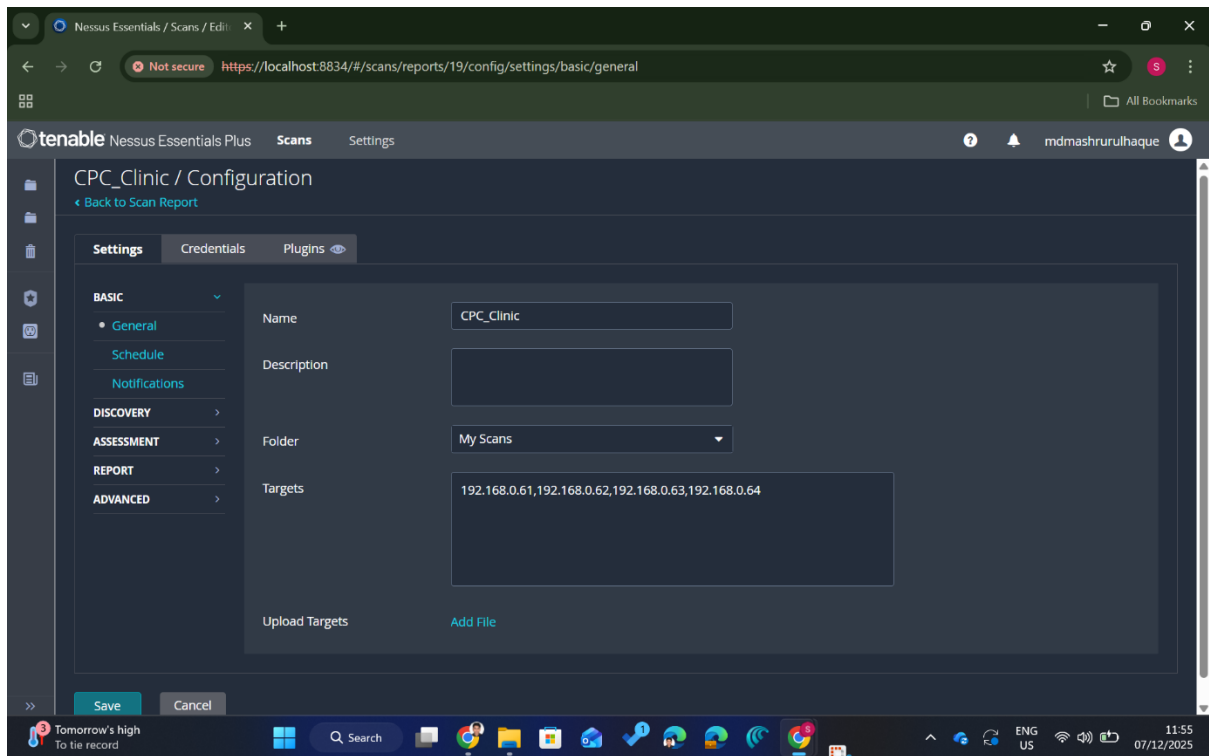


Figure-23: Nessus Vulnerability Scan Configuration

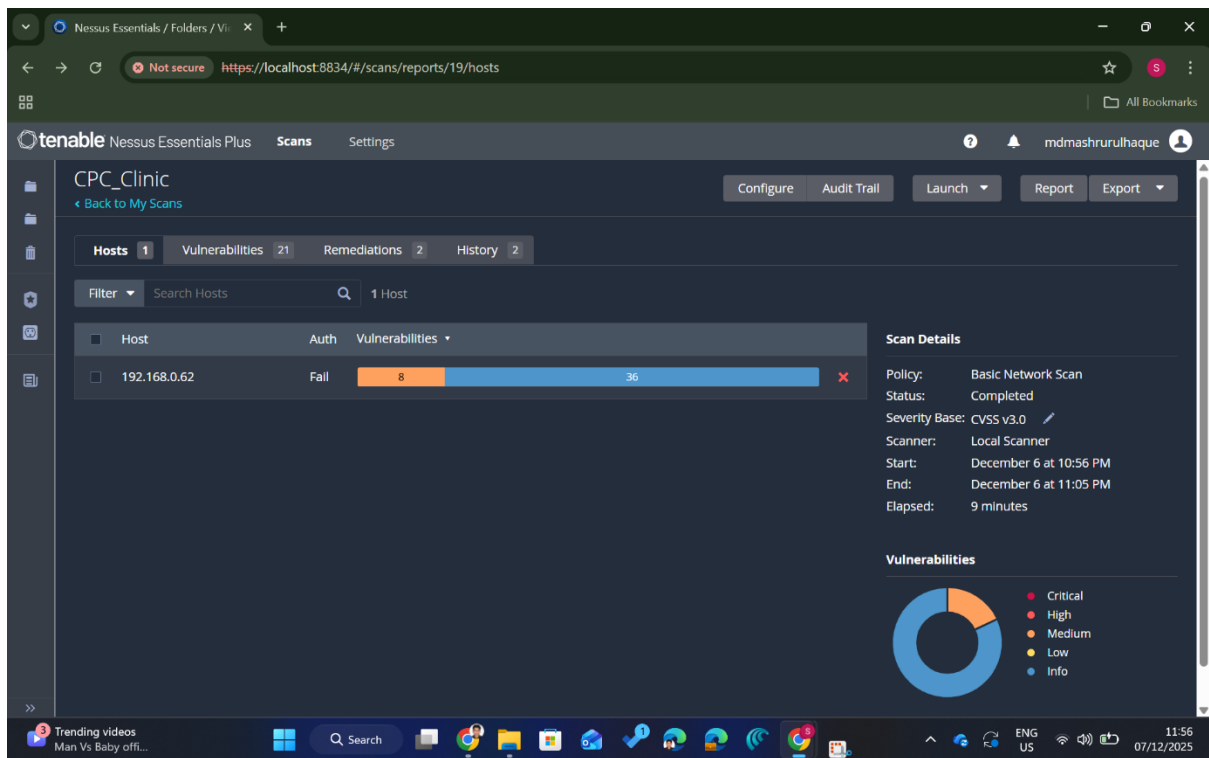


Figure-24: Nessus Vulnerability Scan Results for CPC-DEV-CICD01

5.5 Detection Gap Analysis

This section demonstrates where CPC's defences failed to detect or restrain the simulated APT campaign across each phase.

5.5.1 Web Layer (CPC-CT-WEB01)

- **No input validation or WAF:**
SQL injection, reflected XSS and command injection all worked with basic payloads. There was no evidence of filtering, blocking or rate-limiting on the DVWA pages.
- **No monitoring of suspicious OS commands:**
Command injection allowed direct shell commands from the web front-end, but there were no host-based alerts for www-data running unexpected commands such as ping sweeps.

5.5.2 Dev/CI Infrastructure (CPC-DEV-CICD01)

- **Legacy services exposed and unpatched:**
Services such as UnrealIRCd, Telnet, NFS, old Samba and FTP were discoverable and exploitable. The UnrealIRCd backdoor exploit worked immediately, indicating missing patching and hardening.
- **Lack of intrusion detection on remote services:**
The Metasploit exploitation of UnrealIRCd opened a root shell without any simulated alarms, connection throttling or account lockouts.
- **Vulnerability management gaps:**
Nessus reported multiple medium/high issues on 192.168.0.62, suggesting that even a basic vulnerability management programme would have highlighted this host as high risk before the attack.

5.5.3 Workstation And R&D Environment (CPC-RD-WKS01 & CPC-RD-DC01)

- **Overly permissive SMB share configuration:**
Research and workstation-style accounts (e.g. CPC_RESEARCH, CPC_RD_WKSS01) could list and access shares such as ResearchShare and CPC_RD_WKS01_NOTES with no additional controls. There was no clear separation between research data and workstation notes.
- **No effective access control on sensitive files:**
The dummy “confidential” file (CPC_RESEARCH_CONFIDENTIAL_DATA.txt) was readable by a low-privileged research account over SMB. There was no encryption, classification or approval step before access.
- **Insufficient monitoring of SMB activity and exfiltration:**
Multiple SMB connections from Kali (smbclient sessions, file listings, file downloads) were performed, but there was no evidence of alerting on unusual source IPs, user behaviour or file transfer volumes.

5.5.4 Active Directory Reconnaissance

- **Unrestricted account and share enumeration:**
Tools such as enum4linux and rpcclient could query password policy, users, groups and share information from 192.168.0.64 using low-privileged credentials. There were no signs of throttling or detection of repeated enumeration.

5.5.5 Logging, Monitoring and Correlation

- **Limited or no central logging:**
The engagement did not surface any centralised logging or SIEM capability. Web logs, Linux logs and Windows event logs were not aggregated or correlated, creating blind spots between layers.
- **No obvious alerting on key attack stages:**
High-risk actions such as web command injection, Metasploit exploitation, SMB share enumeration, and file exfiltration all completed without visible alerts, blocks or account lockouts in the lab.

5.6 Strategic Recommendations

5.6.1 Web Application Security (CPC-CT-WEB01)

- **Eliminate injection flaws (SQLi, command injection)**
 - Implement server-side input validation and parameterised queries.
 - Disable direct OS command execution from web inputs; use safe wrappers/whitelists instead.
- **Harden against XSS**
 - Apply output encoding for all user-controlled data.
 - Set security headers (Content-Security-Policy, X-XSS-Protection, etc.) on the portal.
- **Secure SDLC and code review**
 - Integrate basic security checks into the CI/CD pipeline (linting, SAST for SQLi/XSS).
 - Make security tests part of pull requests for web code.

5.6.2 Dev/CI Server Hardening (CPC-DEV-CICD01)

- **Remove or isolate legacy services**
 - Retire Metasploitable-like services (UnrealIRCd, Telnet, older FTP, NFS) from production-style builds.
 - If needed for training, move them to a clearly isolated lab segment.
- **Baseline patching and configuration management**
 - Apply OS and service patches regularly.
 - Use configuration management (e.g. Ansible/Puppet) to enforce hardened templates for dev/CI hosts.
- **Limit attack surface on CI/CD**
 - Restrict inbound ports to only what the pipeline needs (SSH, HTTPS).
 - Enforce strong auth for CI/CD admins; avoid shared accounts.

5.6.3 Workstation and R&D Environment (CPC-RD-WKS01 & CPC-RD-DC01)

- **Tighten SMB share permissions**
 - Apply least-privilege on shares like ResearchShare and CPC_RD_WKS01_NOTES.
 - Restrict access to specific R&D groups, not generic or workstation accounts.
- **Protect sensitive research data**
 - Store research data in dedicated, access-controlled locations.

- Consider file-level encryption and labelling/classification (e.g. “Confidential R&D”).
- **Improve account and credential hygiene**
 - Avoid using the same credentials across server and workstation contexts.
 - Enforce strong password policy and basic lockout for repeated failures.

5.6.4 Workstation and Active Directory Reconnaissance Defence

- **Reduce information disclosure**
 - Harden SMB and RPC so that only authorised admins can run detailed enumeration tools.
 - Limit what low-privileged accounts can see via enumdomusers/share listing.
- **Segment R&D and dev networks**
 - Introduce basic network segmentation between web, Dev/CI and R&D file services.
 - Use firewall rules so that only required flows are allowed (e.g. web to app, not web to SMB).

5.6.5 Logging, Monitoring and Detection

- **Centralise logs**
 - Forward web server, Linux and Windows logs into a single SIEM or log platform.
 - Enable logging for authentication events, share access and process execution.
- **Baseline and alert on key behaviours**
 - Detect repeated SQL errors, command injection patterns and suspicious HTTP payloads.
 - Alert on unusual SMB access (new source IPs, sudden bulk file reads, out-of-hours access).
- **Deploy endpoint detection on critical hosts**
 - Use EDR/AV on R&D servers and dev/CI systems to flag Metasploit-style shells, reverse connections, or unexpected command execution.

5.7 Cost–Benefit Analysis

Security Investment Area	Indicative Annual Cost (USD)	Primary Business Benefit
Web Application Hardening (secure coding, input validation, basic WAF rules)	5,000 – 8,000	Reduces risk of SQL injection, XSS, and web-based initial access
Dev/CI Server Hardening & Patching	3,000 – 6,000	Eliminates high-risk legacy services and prevents trivial exploits
Endpoint Protection (EDR/AV for servers & workstations)	10,000 – 15,000	Improves detection of lateral movement, shells, and ransomware activity

Centralised Logging & Basic SIEM	8,000 – 12,000	Enables early detection, correlation, and incident response
Vulnerability Scanning (e.g., Nessus/OpenVAS)	4,000 – 6,000	Identifies exposed services and misconfigurations before exploitation
Estimated Total Annual Cost	≈ 35,000 – 60,000	Significant reduction in breach likelihood and impact

Table-3: Cost–Benefit Summary for CPC Security Controls

An estimated annual spend of USD 35,000-60,000 would directly address the attack paths used in the simulation, including web exploitation, insecure development services, and unmonitored access to research data. From a business perspective, this investment represents a high-return risk-reduction measure that protects intellectual property, ensures operational continuity, and demonstrates due diligence to regulators and partners.

6. Conclusion

This report shows that major healthcare and pharmaceutical cyber incidents are often driven by basic security gaps especially weak remote access controls, limited internal visibility, and insufficient monitoring. The Change Healthcare case demonstrates the scale of operational and financial impact when these weaknesses are exploited. In the CPC “Operation IP Shield” lab, the same types of gaps enabled a realistic attack path from initial access to data extraction. The key takeaway is clear: targeted investment in strong authentication, hardened services, tighter access to sensitive data, and centralised logging would significantly reduce both the likelihood and impact of a real breach.

7. References

- [1] IBM Security, Cost of a Data Breach Report 2024, IBM Corp., 2024.
- [2] G. Kirubavathi, W. R. Anne, and U. K. Sridevi, "A recent review of ransomware attacks on healthcare industries," *International Journal of System Assurance Engineering and Management*, vol. 15, no. 11, pp. 5078–5096, Nov. 2024, doi: 10.1007/s13198-024-02496-4.
- [3] MITRE, "MITRE cyber experts take on ransomware threats against health systems," MITRE, Mar. 9, 2021. [Online]. Available: <https://www.mitre.org>
- [4] A. Witty, "Testimony of Andrew Witty, Chief Executive Officer, UnitedHealth Group, before the Senate Finance Committee: 'Hacking America's Health Care: Assessing the Change Healthcare cyber attack and what's next'," U.S. Senate Committee on Finance, Washington, DC, USA, May 1, 2024.
- [5] S. Alder, "Healthcare data breach statistics," *HIPAA Journal*, Oct. 26, 2025. [Online]. Available: <https://www.hipaajournal.com>
- [6] Reuters, "UnitedHealth hikes 2024 cost hit from Change Healthcare hack to \$1.6 billion," 2024. [Online]. Available: <https://www.reuters.com>
- [7] U.S. Department of Health and Human Services, Health Sector Cybersecurity Coordination Center (HC3), BlackCat ransomware: Analyst note, 2022.
- [8] Trend Micro, Ransomware Spotlight: BlackCat, Threat Research Article, 2023.
- [9] Group-IB, Uncovering the BlackCat ransomware affiliate program, Threat Intelligence Report, 2021.
- [10] MITRE, MITRE ATT&CK® Enterprise Matrix, 2020–2024. [Online]. Available: <https://attack.mitre.org>
- [11] AttackIQ, Countering ransomware with MITRE ATT&CK 101: How CISOs can build a bulkhead of threat-informed defense, White Paper, 2024.
- [12] Mandiant, "Ransomware rebounds: Extortion threat surges in 2023 as attackers rely on publicly available and legitimate tools," Threat Intelligence Report, 2024.