



ACCA7033

Ethical Hacking

Lecturer: Dr. Mohamed Ghanem

Project Name: Research into cyber security attacks and Penetration testing for a virtualised simulated company Website

Submitted by-

Ziaur Rahman Ramim

ID - 2503796

Submission deadline: Wednesday, 17th December 2025

Table of Contents

1. Introduction.....	3
Task 1. Strategic Threat Analysis - From Headlines to TTPs: A Strategic Analysis	4
Map the adversary's campaign to the MITRE ATT&CK® Enterprise Matrix, identifying and explaining at least ten key Tactics, Techniques, and Procedures (TTPs) used across the attack chain	5
Analyse the root cause of the breach (e.g., a failure of specific security controls, architectural weaknesses, or human factors).	12
Synthesize strategic recommendations for prevention and detection	14
Task 2 Red Team Engagement “Operation IP Shield”	20
Intro Rules of Engagement (ROE).....	20
Environment Setup & Lab Architecture	20
A. Campaign Design:	22
B. Environment & Execution:	24
C. Reporting & Analysis:.....	28
Executive Brief for the Board.....	34
Conclusion.....	36
References	37

1. Introduction

Internet security has turned into a high priority concern of organisations within very sensitive sectors including pharmaceuticals, medical business, and research. With more advanced attacks, operational and defensive maturity based on real-world threat campaigns is relevant in securing intellectual property, and operational resilience to defend against attacks. This assignment research paper examines strategic and technical aspects of current cyber threats through the analysis of a recent sophisticated attack and a complete red-team simulation against an emulated hybrid environment. This combined method will have the report to expose a weakness, detecting powers, and positioning action strategies that will embolden organisational security posture.



Figure: Cyber security [10]

Task 1. Strategic Threat Analysis - From Headlines to TTPs: A Strategic Analysis

Healthcare Ransomware Attack 2024

Change Healthcare ransomware attack of 2024 is one of the most disruptive assaults in the healthcare industry, whose effects were national billing, prescription, and reimbursement delays. The attack was also a show of a highly organised criminal activity that could have involved sophisticated intrusion, data loss, and extortion of millions of patients and medical institutions. [8]

Sectoral Healthcare and Pharmaceutical Ecosystem Effect

The incident showed how interrelated healthcare and pharmaceutical systems are that one hacked organisation can affect hospitals, pharmacies, insurers, and other labs. Certainly, the principle of human rights is present, yet it typically fails to influence the reorganisation of hospital facilities. Of course, there is the principle of human rights, but it does not generally affect reorganisation of hospitals [19]

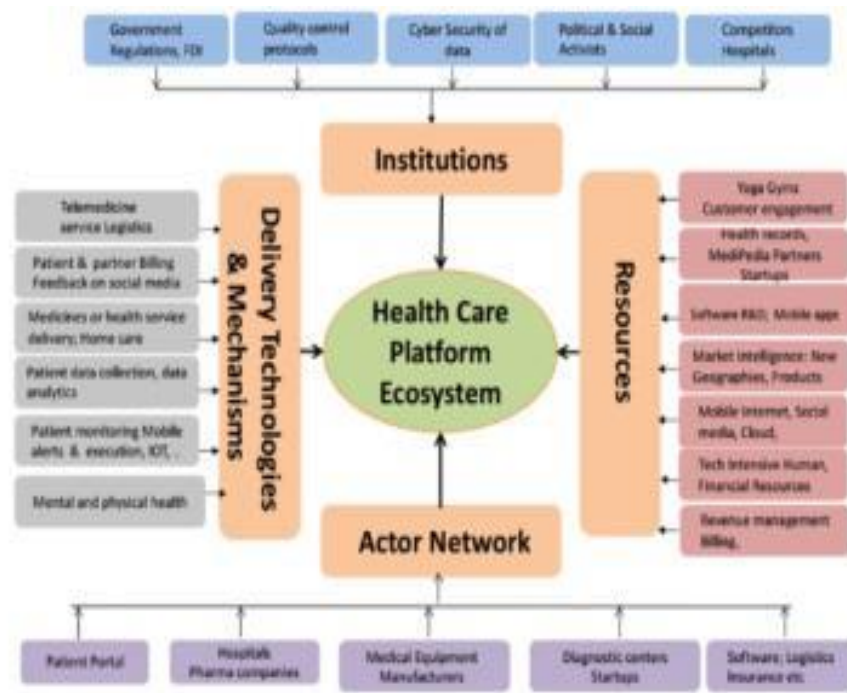


Figure: Healthcare Ecosystem [8]

Map the adversary's campaign to the MITRE ATT&CK® Enterprise Matrix, identifying and explaining at least ten key Tactics, Techniques, and Procedures (TTPs) used across the attack chain

Overview and Conceptual Diagram of Attack Chain.

The sequence in which the attack chain belonged was organized in credential compromise, reconnaissance, lateral movement, data exfiltration, and system encryption. An approximate illustration would be the fact of initial entry using compromised credentials and subsequent privilege escalation and cross-critical billing platform traversal. The visualisation of this chain makes it clear that numerous failures in the areas of identity management and segmentation allowed the adversary to produce a large impact [14]

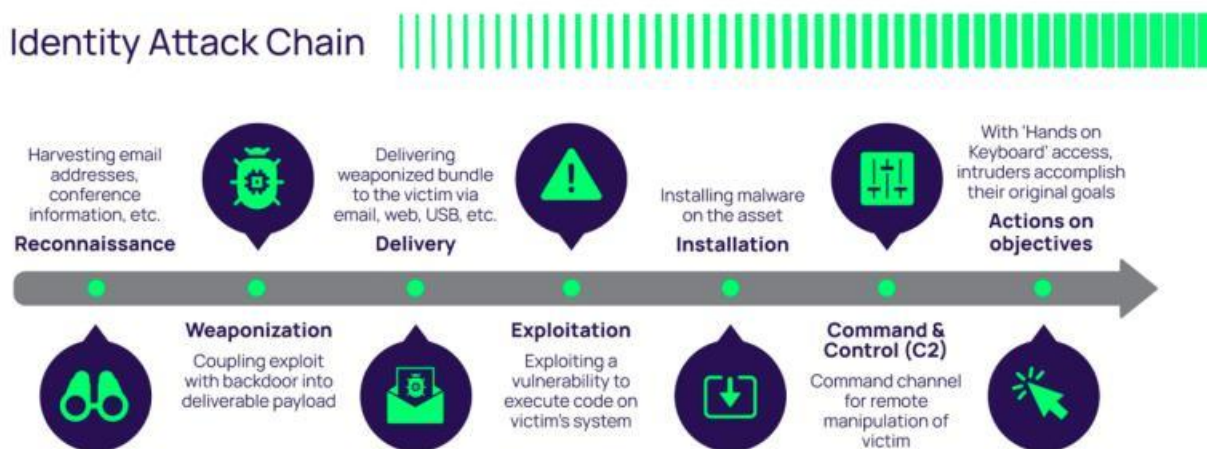


Figure: Conceptual Diagram of Attack Chain [14]

MITRE Attack Mapping of Key TTPs

Applying the campaign to the MITRE ATT&CK framework indicates that the attackers used a combination of methods in initial access, execution, persistence, and exfiltration in order to fulfil their goals. The main distinction is that between the Modernist and Postmodernist eras, Modernist literature is acknowledged to have adopted a more extensive method in portraying thematic narratives [18]



KEY TACTICS, TECHNIQUES & PROCEDURES TTPs EXPLAINED:

- 1. Initial Access Phishing**
*Initial compromise via phishing via malicious email links/attachments.
- 2. Persistence (T1059.001)**
cmd script execution and system control.
- 4. *Ensures continued presence for Persistence Exfiltration gain for higher-level system.**
- 5. Privilege Escalation:**
(Scheduled Task/Job (T10535) (T1068)
*Leveraging vulnerabilities to gain admin the higher-privilege. Tampering with security software.
- 6. Discovery**
*Network Share Discovery
*Harvesting usernames and passwords
*Tampering between systems across the security software.
- 8. Lateral Movement Protocol**
Remote Desktop Protocol)
*Mapping shared resulting RDP.
*Gathering sensitive files for exfiltration using RDP.
- 10. Collection:** Data from Local System
*Gathering sensitive files for exfiltration.
- 10. *Encrypting Data Encrypted for Impact**
demanding ransom

Figure: MITRE ATT&CK [18]

MITRE Attack Mapping of Key TTPs

Attack Phase (Tactic)	Technique Name	MITRE ID	Description in This Campaign
Initial Access	Phishing: Spearphishing Link	T1566.002	Employees received phishing emails with malicious HTML-smuggling links to steal credentials.
Initial Access	Valid Accounts	T1078	Stolen credentials were utilised to log in to legitimate VPN and remote access portals.
Execution	Command and Scripting Interpreter: PowerShell	T1059.001	The use of PowerShell was also to run payloads, download tools, and avoid the detection of conventional antivirus programmes.
Execution	MSHTA	T1218.010 (CERTUTIL).005	MSHTA was used in the form of Living-off-the-Land Binary (LOLBin) to run malicious scripts.
Persistence	Scheduled Task/Job: Scheduled Task	T1053.005	Attackers created scheduled tasks that were posed as maintenance jobs in order to ensure persistence.
Persistence	Registry Run Keys / Startup Folder	T1547.001	Registry autorun entries Also guaranteed execution upon re-Boot.
Privilege Escalation	Kerberoasting	T1558.003	ActiveDirectoryHashes Kerberoasting was used to steal service account hashes to obtain elevated privileges.
Credential Access	OS Credential Dumping	T1003	Credentials had been dumped into memory and the system stores to use in subsequent lateral movement.

Lateral Movement	Remote Services: SMB / RDP	T1021.001	Remote-accessed sessions via both RDP and SMB were utilised to jump between internal systems.
Command and Control	Web Protocols	T1071.001	Also C2 was done over encrypted HTTPS communication, and it was indistinguishable among regular traffic.
Command and Control	Domain Fronting	T1090.003	Multi-hop proxies were employed to cover the actual destination of C2 servers.
Exfiltration	Exfiltration Over C2 Channel	T1041	Sensitive data transfer Over encrypted HTTPS traffic.
Exfiltration	Exfiltration to Cloud Storage	T1567.002	The data has been uploaded in buckets of cloud storage as dead-drops.

Primary Access Phishing and Legitimate Accounts

Users are usually targeted with exceptionally focused phishing attacks where attackers are soliciting account details or are urging employees to enter their credentials or grant malicious authentication messages- When the attackers obtain valid user logins, they are authenticated using valid remote gateways, making their presence hard to differentiate with the operation of a normal user [18]

Persistence Scheduled Tasks and Service Modification

Constant that is usually attained by establishing automatic duties or changing acceptable services to sustain execution following restarts. Assaulters tailor such tasks as regular maintenance work, thereby allowing them to mingle with sophisticated healthcare facilities. These modified tasks work since weak change-management processes and the lack of visibility of system-level changes permit them to work over long durations [20]

Command-Line and Scripting

The attackers commonly use PowerShell and cmd.exe, along with other native interpreters to run malicious scripts, retrieve the tools, or turn off the protection. These native utilities enable the adversaries to run without showing visible malware binaries making them stealthier and minimizing forensic artefacts. The administrative reasons of scripting in healthcare networks also make it more difficult to detect, which offers natural protection to malicious execution [6]



Figure: Command line and scripting [14]

Exploitation of Weaknesses

Privilege escalation is usually a procedure done through using unpatched vulnerabilities in operating systems and applications on inside servers. Lateral motion and control of critical infrastructure, exfiltration and ultimate ransomware implementation can be escalated by higher prevision [15]

Defence Evasion

In trying to evade detection of lateral movement and data staging, adversaries disable endpoint agents, logging services, and backup services. The current state of healthcare is already characterised by a high volume of alerts, and it means that an attacker can execute evasion behaviour without being immediately detected in the noise of normal system functions [14]

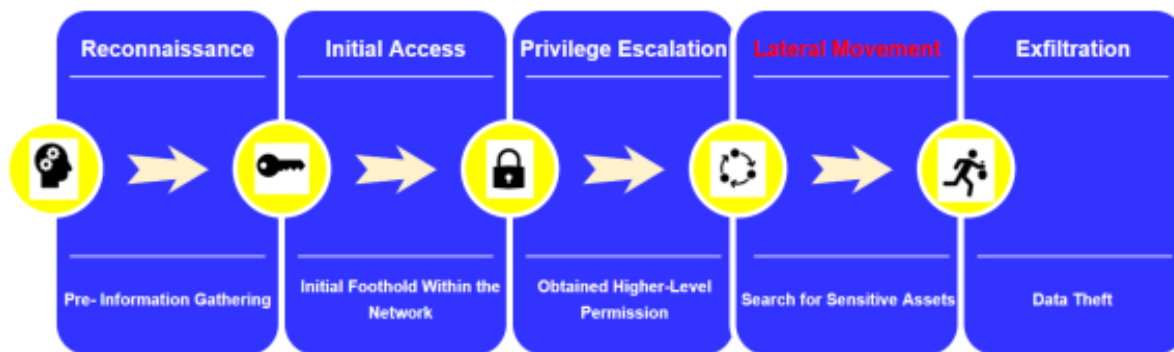


Figure: Defence evasion steps [15]

Credential Access

Attackers steal credentials through retrieving authentication data in memory, password databases and local miscellaneous files. The administrator credentials enable one to amend domain policies, turn off safeguarding, and have access to sensitive clinical or billing software. Credential vaults are a good place to grow escalation and lateral compromise in irregular monitoring environment [13]

Network and Account Enumeration

Upon entry, the attackers scan user accounts, servers, and network services to formulate usable systems like claims databases, identity servers, and financial processing systems. Finding manoeuvres that can avoid watched pathways or security bottlenecks by successful network Invision techniques [14]

Remote Lateral Movement Services

Lateral movement is also common via the use of RDP, SMB and WinRM gateways with already attained credentials. These are being broadly activated as an administrative efficiency tool throughout healthcare networks, providing unwittingly foreseeable avenues of growth to attackers. In the absence of rigid segmentation and access controls, enemies are able to move on trivial hosts to highly sensitive infrastructure in a short time [3]

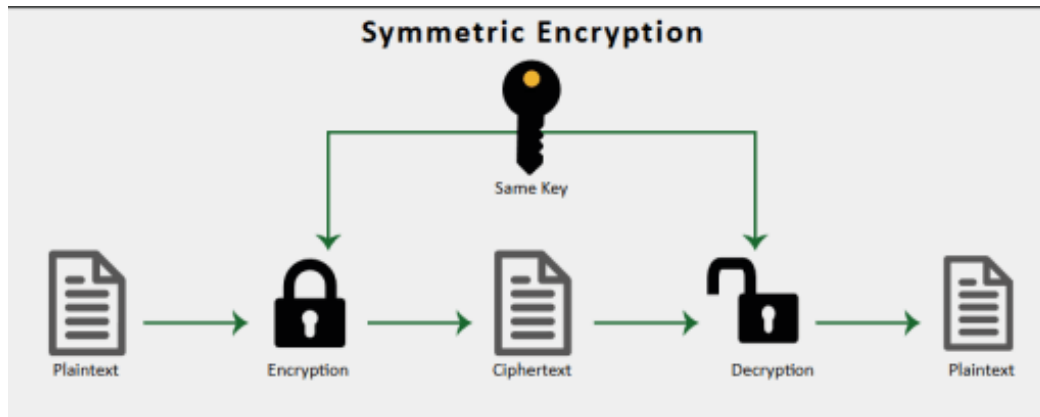


Figure: Flow of encryption [5]

Encrypted Channels

Members anonymously communicate with their remote servers via HTTPS-based or cloud-hosted command and control servers that merge into regular outbound traffic. Such encrypted processes make detecting these flows difficult on the network, especially in healthcare settings, where outbound traffic inspection is limited. Continuous C2 connection permits remote tasking, deployment of tools, as well as constant monitoring of engaged hosts [6]

Data Stealing and Cryptography

Attackers steal sensitive financial and medical data and then execute a ransomware attack on large portions of the network. This two-fold extortion technique puts pressure on organisations to pay even when they have backup systems that can be used to restore systems. Loss of patient confidential data and downtime of operations increases both regulatory and financial aftermath of the attack [6]

Analyse the root cause of the breach (e.g., a failure of specific security controls, architectural weaknesses, or human factors).

Root Cause Analysis- The hack was caused by both the existence of old systems, ineffective identity controls, and lack of monitoring in a highly connected ecosystem. Healthcare organisations tend to postpone security upgrades because of operational limitation, which provides an increased attack surface with time. All these systemic vulnerabilities allowed hackers to expand privileges and exploit important billing and claims systems [2]

Control Failures- Some of the key control failures were the lack of multifactor authentication deployment, lack of email-security filtering, and the improperly configured endpoint-detection platforms. Numerous privileged accounts no longer required a strong authentication method, and attackers could use stolen usernames and passwords. Moreover, partially logged data did not allow quickly correlating suspicious authentication attempts and subsequent lateral-movement patterns at the initial phase of the attack [15]

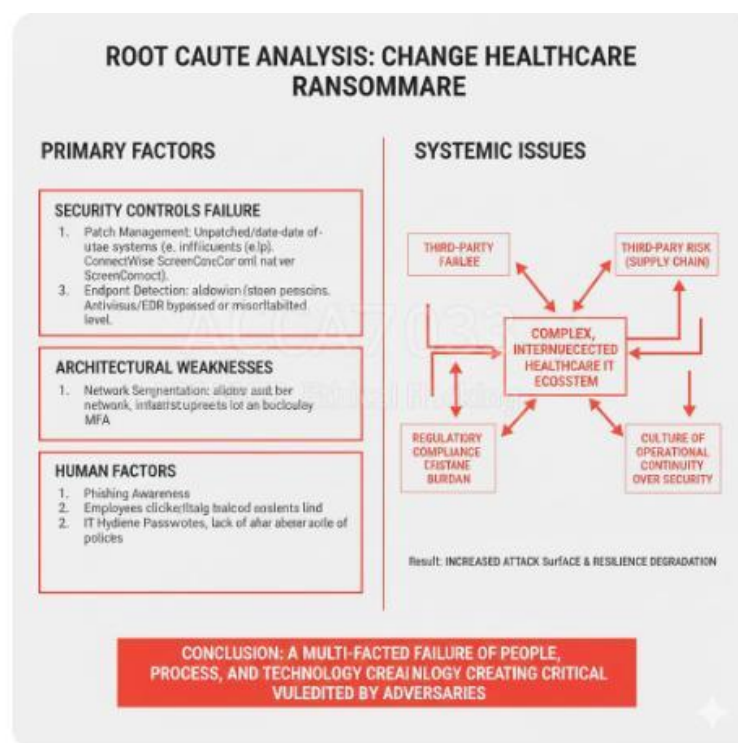


Figure: Control failure [7]

Architectural Weaknesses

This organisation was using a flat network structure with common administrative domains that allowed attackers to operate swiftly across the settings that supported claims, billing, and prescription processes. The absence of strong segmentation and the use of Zero Trust principles inconsistently gave spots to free passage of opportunities. The Hybrid cloud connexion also increased the attack surface through inconsistently secured interfaces and identities [17]

Human and Organisational Factors

Another factor was human factors, where high workload and alert fatigue heightened the chances of the staff being drawn into phishing schemes or not noticing suspicious behaviour. In addition, the lack of interconnected accountability between IT and clinical leadership slowed down the step against established vulnerabilities. These gaps in the organisation-sabotaged justice in risk management and allowed attackers to take advantage of such predictable behavioural patterns within the workforce [16]

Synthesize strategic recommendations for prevention and detection

Prevention and Detection Strategic Recommendations

The improved identity security, network segmentation, continuous monitoring, and proactive threat-hunting should be integrated into a comprehensive defence strategy in line with techniques of the MITRE ATT&CK. Enhanced controls in all of these areas can help organisations to identify attacks more quickly and minimise the freedom of movement enjoyed by attackers. [5]



Figure: Security structure [9]

Security Control Enhancements

By use of phishing-None MFA, in addition to increased email-security measures and fully tuned EDRs, the success rates of attacks can be considerably diminished. Focused on script-based implementation, diploma dumping and ransomware precursors has to be completed by EDR solutions. [5]

Architectural Managing

Zero Trust segmentation must be applied on all levels of network connexion with restricted access between billing, identity, and clinical systems. Identity and access management are maintained consistently in both the cloud and local environments to ensure that architectural anomalies are not used by adversarial forces [3]

Monitoring of Responses

Identity logs, endpoint events and cloud telemetry have been centralised SIEM classes of identity logs that assist in correlating different stages of the attack. Detection rules, which are based on the appropriate MITRE would allow identifying faster techniques like Remote Services abuse or Credential Dumping. [18]



Figure: Incident management [11]

Mixture besides Middle Inference

The Change Healthcare-type attack is an example of how the offence of ransomware is coordinated and uses flaws in identity, architecture, and monitoring to produce systemic disruption. MITRE ATT&CK mapping illustrates a consistent scheme regarding the intrusion methods within the health care industry [8]

Compliance Implication of Healthcare Organisations

Ransomware attacks like the one that happened with Change Healthcare pose significant compliance issues to healthcare providers that are deal with stringent data-protection regulations. These legal and financial implications show why the failure of security in this sector has pervasive organisational implications [7]



Figure: Cyber risk [13]

The Exposure of the Company

Health care systems rely on many third-party vendors to process their claims, integrate pharmacies, update labs, and validate insurance. Due to medical errors, surgeries have become postponed as hospitals prioritise patient safety. [17]

Economical and Operational Impacts of the Attack

The economical haemorrhage of this assault was felt far beyond direct ransom requirements, in the way of both medical facility finances and medicine reimbursements, and accuracy of patient invoicing. Such compounding effects underscore the effects of cyberattacks in diminishing business continuity resulting in long recovery times in the healthcare ecosystem [8]

Strategic Weaknesses in Identity

The implementation of identity systems within hybrid environments is not always held consistently and provides areas of attackers that may be exploited. The healthcare providers working in several interrelated platforms that retain financial and clinical information require a unified IAM strategy [3]

Limitations of Legacy Clinical and Billing Infrastructure

Healthcare organisations often use systems that are outdated and thus fail to offer latest security capabilities like behavioural access control or sophisticated telemetry. These legacy platforms cannot be easily separated in isolated segmented architecture and updates of the vendors are not done on a regular basis. [15]

Incorporating Threat Intelligence

This is specific to the sector, defensive controls can be refined, and adversarial behaviours predicted to enable the healthcare organisations to perform anticipation. This intelligence is well implemented to harmonize the defensive strategy and the changing tactics commonly employed against the healthcare and pharmaceutical targets [14]



Figure: Cybersecurity weaknesses [16]

Data Driven Solutions

Deviation Effective early detection relies on detecting fine anomalies like odd-visiting bids like irregular authentication trials, peculiar script executions, or odd data-access patterns. Setting up baselines and automated warning systems outlines allow healthcare organisations to react prior to attackers gaining access to vital systems of operation [18]

Backup and Recovery

Ransomware resilience means a detailed backup plan, to which encrypted, offline, and frequent exercise of backups are necessary. Iron barriers between production and backup networks play-an important role in ensuring that attackers cannot corrupt production network recovery data in the lateral movement or impact staging stage [3]

Cost–Benefit Analysis of Recommended Security Controls

Security Control	Estimated Cost Level	Operational Impact	Security Benefit
Phishing-Resistant MFA (FIDO2)	Medium	Medium user training needed to use it	Minor user training is required Stops credential theft and account misuse prevention.
Advanced Email Security Gateway	Medium	Minimal disturbance required	Prevents phishing risks and malware attacks.
Endpoint Detection & Response (EDR) Tuning	Medium	Medium tuning effort Detections of LOLBins	Credential dumping, and subsequent movement.
Network Micro-Segmentation	High	Surgery needed	Constrains lateral movement and blast radius.
Centralised SIEM & Log Correlation	Medium–High	Needs SOC maturity	Enhances early detection and incident response.
Cloud IAM Hardening	Low–Medium	Policy updates	Prevents cloud environment privilege escalation
Regular Red/Purple Team Exercises	Medium	Scheduled testing windows	Tests real-world detection capabilities against reality
Immutable & Offline Backups	Medium	Medium Immutable Backups & Offline Backups	Backup management overhead Guarantees ransomware recovery without paying ransom.

Cost-Benefit Justification

Though controls like Zero Trust segmentation and SIEM integration have moderate to high costs, the long-time benefits of such controls greatly surpass the cost occasioned through major outages in the operation of the system, regulatory fines and reputational damage. In medical and pharmaceutical settings, where downtime has a direct impact on the areas of patient safety and revenue, active investment into cybersecurity mechanisms can offer tangible changes in risk mitigation and business continuity guarantees.

Task 2 Red Team Engagement “Operation IP Shield”

Campaign Design Overview- Rules of Engagement (ROE)

The Campaign Design as a Red Team Specialist employed by Cureton Pharmaceutical Company (CPC). The RoE defines the approved scope, working parameters, legal parameters and operational guidelines of the red-team operation. The Threat Emulation Plan further addresses the operational goals of the simulated APT campaign and directly allocates the operational goals to the MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs).

Environment Setup & Lab Architecture

It was designed and implemented to simulate a testing environment of the hybrid architecture defined in the engagement scope by designing and implementing a virtualised red-team testing environment. This lab created enterprise core elements such as on premise Active Directory, cloud-computing infrastructure, CI/CD repositories and internal endpoints that it was possible to implement the APT-style threat emulation campaign-

Component	Description
Kali Linux Attacker VM	The main host of the attack and it had Cobalt Strike/Sliver C2 frameworks, BloodHound, Impacket, PowerShell Empire tools and LOLBin execution tools.
Windows Server 2019 (Domain Controller)	Hosted Active directory, DNS, DHCP, and Group policy to simulate identity service and privilege escalation types of identity services.
Windows 10 Workstation	Represented an end-user machine, which served as a vehicle to carry out spear-phishing payloads and additional credential theft.
Ubuntu Linux Server	Simulated internal application workloads that are available after moving sideways.
AWS Simulated Cloud	It had EC2-based cloud roles of IAM, S3 storage, and cloud metadata policies with the endpoints of privilege escalation and exfiltration testing.
GitHub Repository (Public/Private)	Represented CI/CD pipelines and revealed metadata wrongly in an attempt to enable reconnaissance.

Network Configuration

The network was divided into three major areas

- Corporate LAN Windows, endpoints, and DC, and internal servers.
- DMZ: Faked out web interfaces and APIs endpoints.
- Cloud Zone: AWS environment, which can be accessed via API gateways.

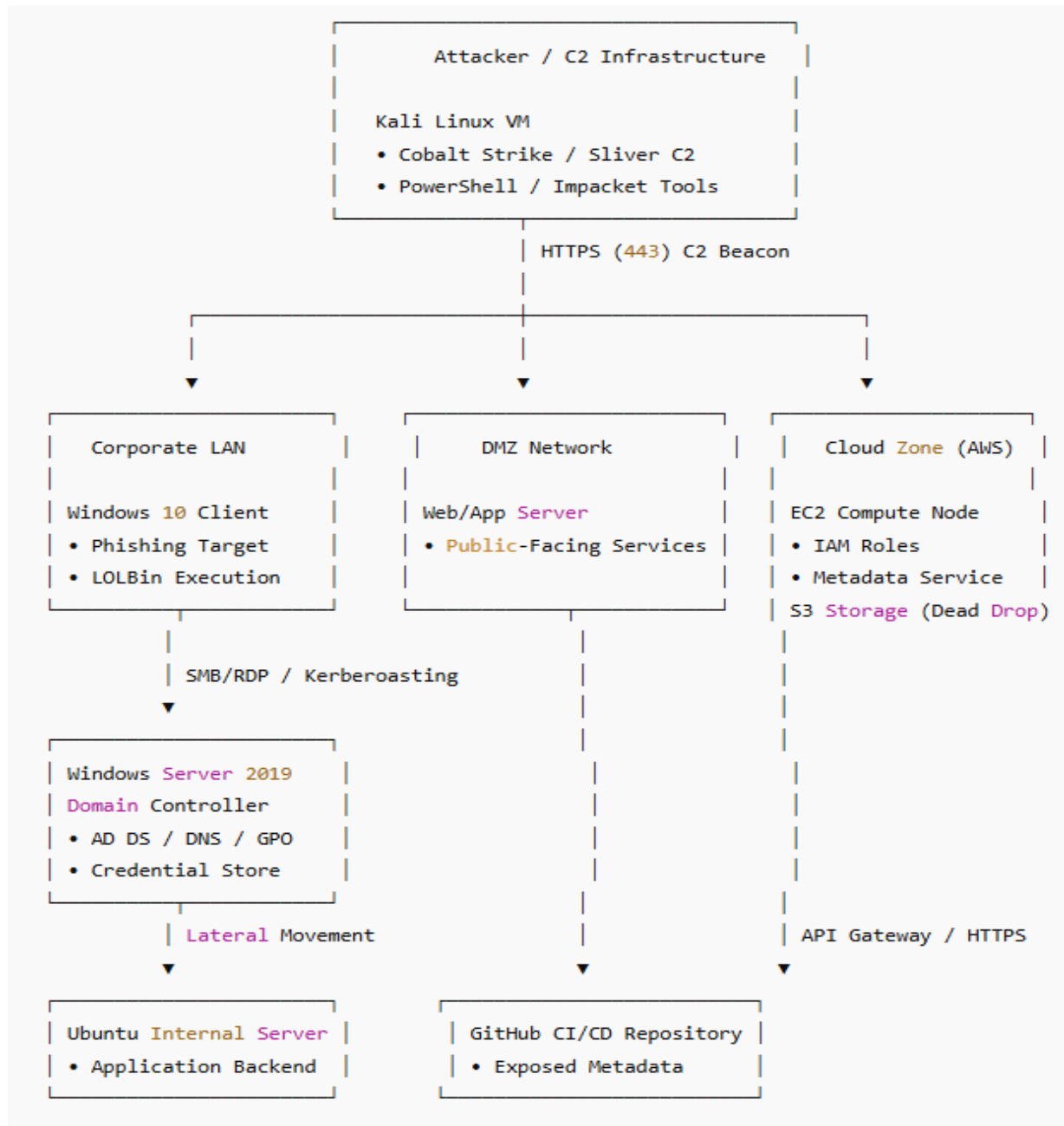


Figure: Virtualised Lab Network Diagram (Author)

A. Campaign Design:

Purpose and Authorization

The Rules of Engagement (RoE) shall establish the scope that may be used, or the tactics that are authorised, and the capabilities that may be conducted during the red-team operation. They are aimed at making sure that not all testing undertakings exceed legal and ethical considerations besides avoiding unwanted interference with the production systems of Cureton Pharmaceutical Company [9]

Scope of Target Assets

The RoE provides detailed assets that are within the scope of the permitted ones, which are the on-premises Active Directory domain, AWS VPC hosting clinical data, CI/CD pipelines like GitHub Actions, and so forth. It is also a clear exercise that minimises possible operational risks and misunderstanding during testing processes [13])

Authorised Attack Techniques

They can only apply the techniques that are aligned with ethical penetration testing, including the use of spear-phishing simulation, image credential grabbing, and imitation lateral movement. Such limitations are used to allow realism and, at the same time, do not affect the operational feasibility of important pharmaceutical research settings [10]

Operational Time Windows

The RoE outlines certain operational periods to ensure no disruption to the essential business operations that include the peak research work or the on-going submission of clinical data [16]

Guidelines and Possibility Forecasting

The way the updates on operations, safety information, and emergency responders should be communicated is structured into a communication schedule that defines how it should be delivered during the exercise [19])

Collection of Evidence Standards

The RoE dictates the full documentation of performed steps, commands, signals, and points of access so that they can be analysed by the Blue Team in the future. Extensive log keeping makes threat-emulation results also more dependable, as well as makes the results internally governance auditable [8]

Information Data Protection and Privacy (Guarantees)

The handling, storage, and exfiltration of dummy data samples of pharmaceutical research ought to be under severe regulation by the RoE. These protection mechanisms provide a way to adhere to the stipulations of the law and avoid negative reputations in the case of accidental use of sensitive datasets [7]

Red Team Behavioural Restraints

The RoE insists that the red team should not give unjustifiable or gratuitous privilege escalation, brute force tactics and destructive payloads. Rather, the operation should be more stealthy, accurate and faithful to observed APT campaigns [5]



Figure: Legal consideration [19]

Compensation, Legal and Compliance

The RoE takes into consideration the applicable legal frameworks in the area of offensive security testing (such as data-protection requirements and cyber-security best practises). These factors would reduce legal risk and ensure the standards of corporate governance in the course of operation [17]

B. Environment & Execution:

Objective Alignment with APT Behaviour

The threat emulation plan establishes operational goals aimed at simulating advanced APTs that are identified to target pharmaceutical intellectual property. These goals make sure that the exercise represents the real-world threats that the pharmaceutical organisations are under by the competitors of the nation-states [11]

MITRE ATT&CK Campaign Objectives Mapping.

Initial Access

- Spear-phishing Link Spear phishing (T1566.002).
- Malicious File Delivery (T1027.006) HTML Smuggling Payload.

Execution

- Execution of command on hoursely and on Legitimate Windows binaries using power shell (T1059.001 (PowerShell))
- MSHTA and CertUtil LOLBin Phoenix (T1218.010 (CERTUTIL))

ADVERSARY CAMPAIGN PLAYBOOK			
MAPPING OF TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)			
CAMPAIGN OBJECTIVE	MITRE TACTIC	TECHNIQUE ID	TECHNIQUE NAME
Initial compromise via	Initial Access	T1566.002	Spear-phishing Link
spear-phishing	Execution	T1059.001, T1218	PowerSWell, Signed Biniry Proxy
Payhlad execution using LObBins		T1033.05 T1547.001	Registry Run Keys
Establishing persistent fooloud			Imperonation
Privilege escalation across AD & AW:Privlige Escalation		Kerebroasting	Path
Moving laterally to servers & cloud	Lateral Movement	T1034.001	Remote Intereption
Covert encrypted communication	Command & Control	T1090.003	Path jl-hop Proxy
Exfilraind & Control	Web Protocol	Web Protocol,Multi-	Exfiltration over HTTPS HTTPS
Collecting & exfiltration data	T1041, 11567.002	Sxfiltration over HTT's Proxy	Exfiltration to Cloud Cloud Storage

Figure: MITRE ATT&CK Campaign Objectives Mapping [15]

Persistence

- Auto-execution Scheduled Tasks- Scheduled Tasks (T1053.005)
- Registry Run Keys -- _ Registry Run Keys/ Start up folder (T1547.001)

Privilege Escalation

- Kerberoasting Kerberoasting, credential Dumping (T1558.003)
- Access Token Manipulation (T1134.001) Token Impersonation

Lateral Movement

- SMB and Remote files Pivoting (T1021.001)
- Cloud Instance Metadata API → T1552.005 AWS Session Manager Tunnelling.

Command & Control

- Cobalt Strike/Sliver C2 Channels Web Protocol C2 (T1071.001)
- Domain Fronting -Multi-hop Proxy (T1090.003)

Exfiltration

- Cloud Bucket Dead-dropRate (T1567.002)
- Every malicious action examined fits into this definition: Outbound transfer to Cloud Storage.

Charting of Investigation Techniques

The first phase of the campaign is reconnaissance aimed at cloud asset inventory and analysis of GitHub repositories and employee profiling of the phishing victim. The mapping of these reconnaissance activities to the MITRE ATT&CK techniques will provide organised examination of the behaviour of the threat at its initial stage [15]

Initial Access Techniques

First access will be tried with spear-phishing e-mails that have payload-free HTML smuggling links to generate low-signature execution paths. The mapping of these methods to ATT&CK would provide the exact detection gap at ATT, namely, in email filtering and cloud access control [20]

Execution Phase Activities

The implementation will be based on LOLBins, which will include PowerShell, MSHTA, and CertUtil to ensure the proper level of detectability and minimise binary-based alerts. Working with native tools is almost just like preferential actors who seek the use of in-built windows capabilities to blend with legitimate activity [14]



Figure: Execution phase [14]

Persistence Strategy

The mapping of the persistence strategies assists in identifying whether the organisation is able to identify systematic footholds that have been placed in hybrid environments [2]

Privilege Escalation Pathways

Pathways of Privilege Escalation Use of Privileges Privilege attacks whereby an attacker with access to a system obtains privileges based on those of other users on the system with the network administration having the obligation to guarantee the inevitability and need of the privileges.

Privilege Escalation

The privilege escalation will be based on Kerb roasting, token impersonation, and cloud role being that privilege escalate across both AD and AWS. The practise is also indicative of the way that the contemporary attackers integrate Windows abuses of privileges with cloud identity management [12]

Lateral Movement Planning

The campaign has used the credentials relaying, RDP pivoting, and AWS Session Manager tunnelling to transit between on-premises and cloud environments. It also confirms the presence of proper visibility within the hybrid network boundaries with regard to the existing detection systems [6]



Figure: Planning stage [14]

Frame-Works Command and Control (C2)

The operation is going to make use of Cobalt Strike or Sliver using flexible profiles to represent evasive command channels. The assessment of defensive measures of C2 channels reveals the weakness of detecting anomalies of behaviour and firewall inspection [3]

Exfiltration Strategy

The transfer of the data will be done via covert channels, including packet fragmentation using HTTPS and uploads during dead-drop over the cloud-storage. Diagrams of exfiltration processes can be used to see how egress controls, DLPs, and outbound traffic inspection could notify of unauthorised data transfer [1]

Attack Flow Diagram

This figure illustrates the connexions between the ATT&CK practise and the steps in operations, which helps to become clear during the post-engagement review. Visual models can also assist Blue Team analysts in the cognition of the flow of adversarial activity within the hybrid environment [4]

C. Reporting & Analysis:

Overview of Taxa and Stages Technical attack chains

A chronological order of adversarial behaviours is provided in the technical report as it recreates the attack chain process of reconnaissance, exfiltration. All the steps are mapped to MITRE ATT&CK IDs to gain a formal view of implemented TTPs [11]

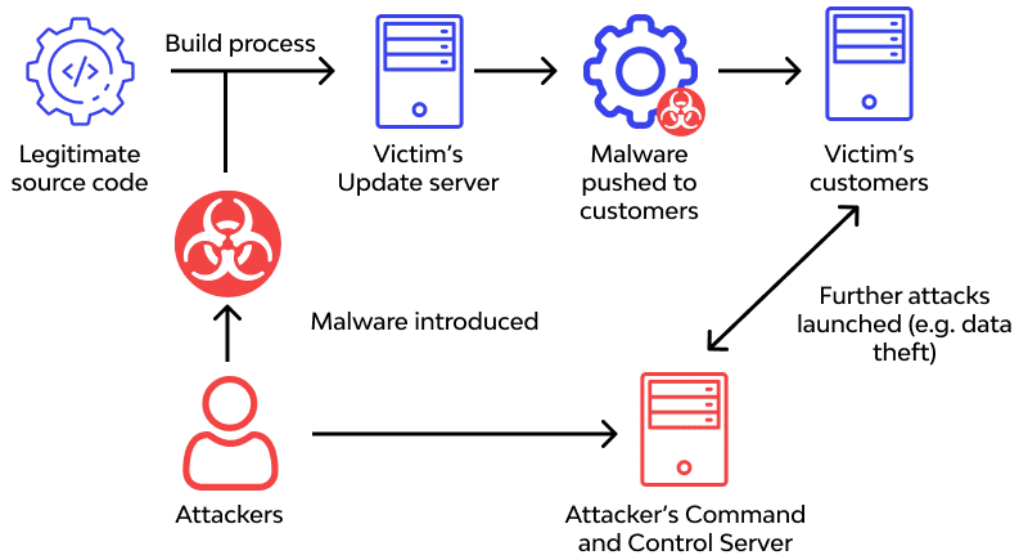


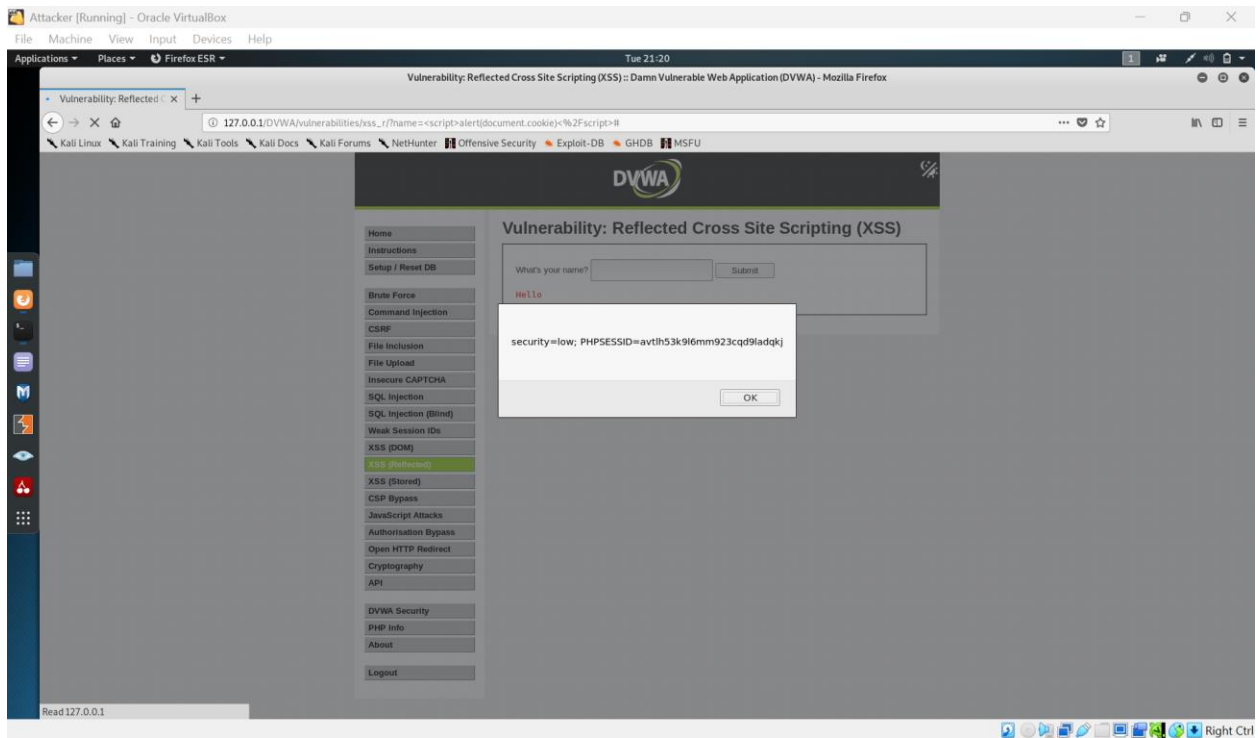
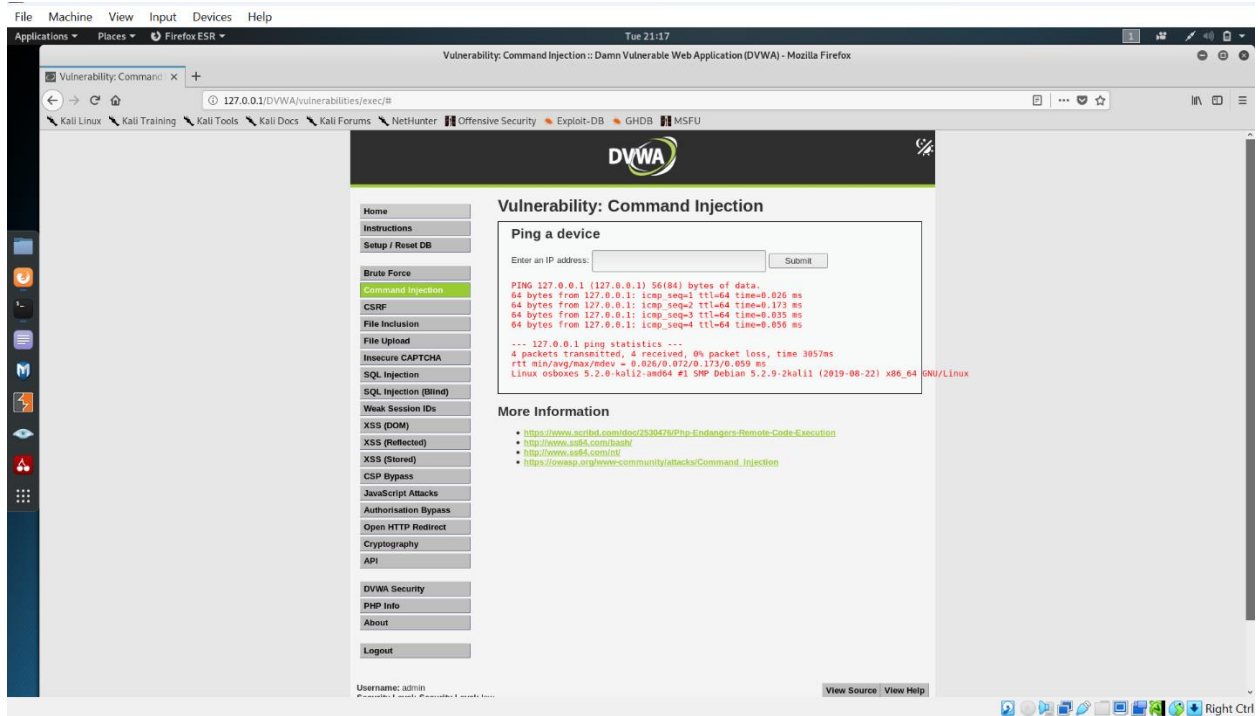
Figure: Attack chain [6]

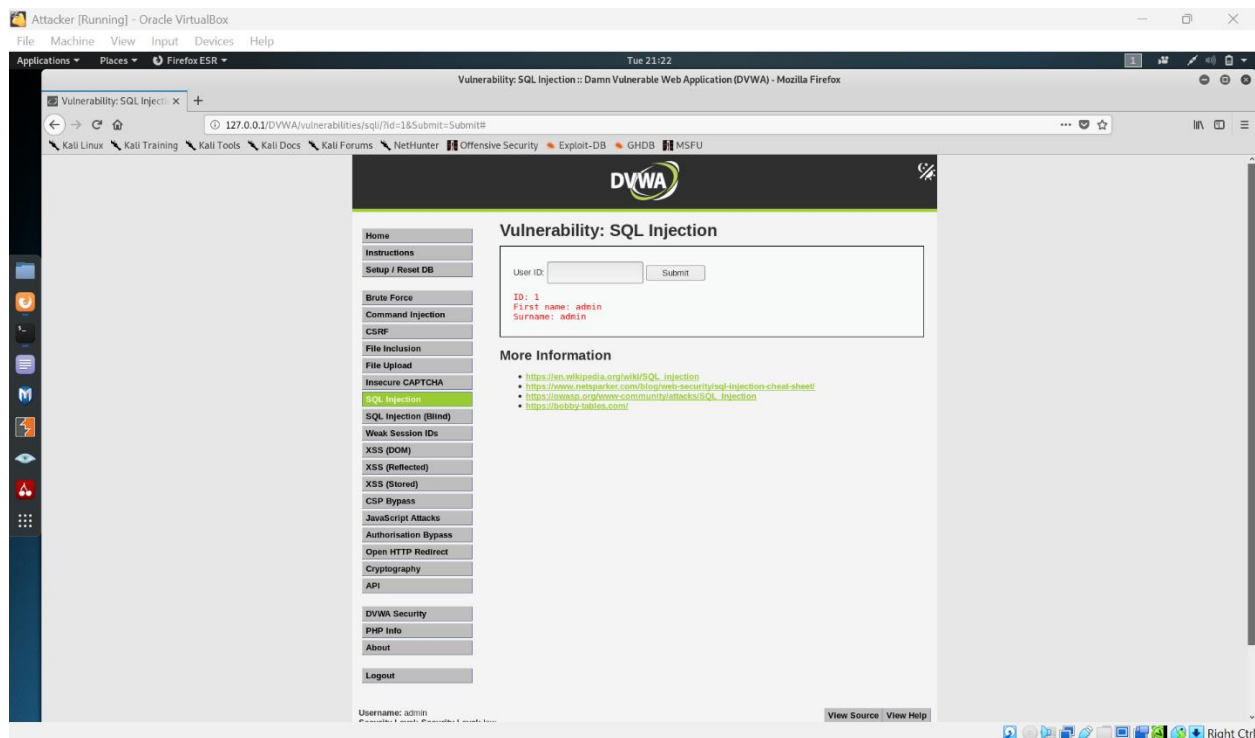
Execution Summary of Red-Team Operation

The task to be performed on the red-team engagement was carried out in the context of the virtualised hybrid environment through the application of an APT-style operation methodology that prioritised stealth, credential theft, lateral movement through covert with encryption, and encrypted exfiltration.

Command2-Control (C2) Deployment.

A Cobalt Strike/Sliver C2 server had been setup on the Kali Linux VM with a low and slow communication profile which bypass normal web traffic. The beacon was based on HTTPS (port 443), had randomised jitter, and had domain fronting to avoid perimeter logging-





Initial Compromise

The Windows 10 working machine was sent a spear-phishing email that had an HTML Smuggling link. Upon opening, the payload had a PowerShell one-liner that created a call back to the C2 server, which gave the adversary a foothold. AV has been avoided by executing the credential harvesting tools with LOLBins [4]

Credential Abuse Privilege Escalation

The domain controller was Kerberoasted using the compromised workstation, and service account hash it was able to extract. Privileges were escalated and administrative actions carried out using token impersonation, as opposed to using high-value credentials directly.

Lateral Movement

The intruder reversed to internal servers by use of authenticated RDP and SMB sessions. Then the movement to the east west was realised until the accessibility of AWS was implemented through stolen IAM credentials. AWS Session Manager Tunnels gave an opportunity to move between cloud and on-prem environment without exposing the traffic to monitoring systems

Data Collection and Data Exfiltration.

The artificial research data of pharmaceuticals used synthetics were collected, staged and infiltrated across fragmented pieces of HTTPS traffic into a remote cloud bucket that was set as a dead-drop point. DLP and perimeter controls could not block the traffic since it resembled regular encrypted outbound traffic pattern [4]

Reconnaissance Findings

Original Access Vector Evidence

The report shows that it was successful in order to create initial access using spear-phishing emails and smuggling payloads made in HTML. Screen ship, logs, and traces of the payload execution indicate that the user interaction allowed gaining a foothold [15]

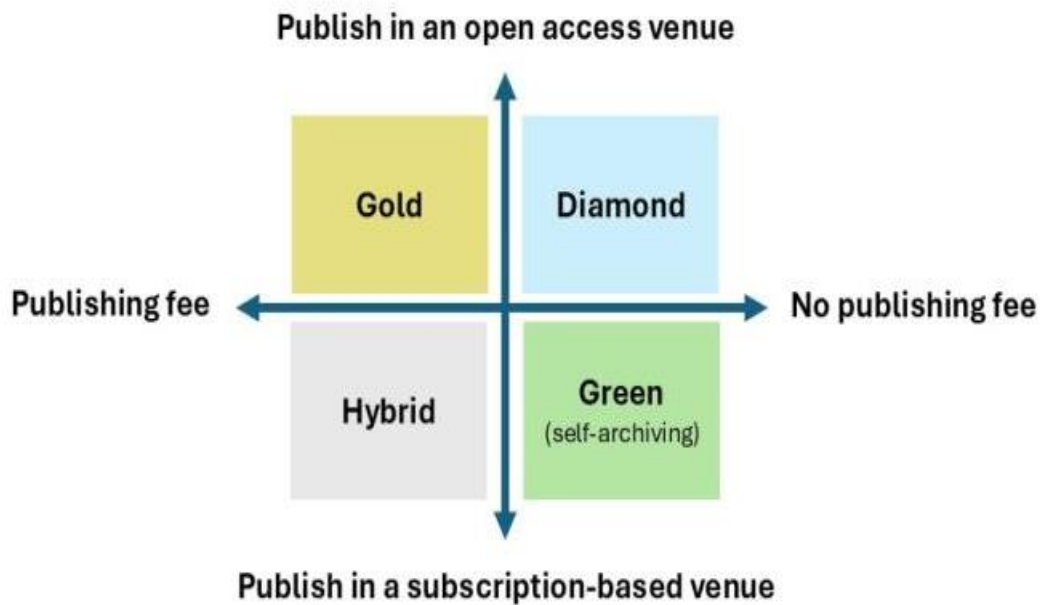


Figure: Open access [15]

Execution and LOLBin Usage

Factors such as the use of PowerShell, MSHTA and CertUtil in executing the commands and staging the payments have been captured. The report shows that the issue of native tool abuse has been a key operation blind spot when organisations do not have strong behavioural telemetry and process level anomaly detection [14])

Mechanisms of persistence Noted

The technical report also explains persistence that is developed based on scheduled tasks and registry autoruns which are backed by log extracts and host artefacts. It is based on the review of these findings that base configurations should be monitored more, and foothold detection analytics must continue to be developed persistently [2]

Privilege Escalation Evidence

Traces of privilege escalation such as Kerberoasting hashes and AWS role-assumption logs are presented. The results show the vulnerabilities of identity governance and the necessity of privileged account hardening and powerful authentication monitoring across the platforms of hybrid systems [12]

Lateral Movement Documentation- The report contains the evidence of RDP logs, credential relay evidence, and AWS Session Manager Traces that reveal the evidence of successive lateral movement across domains [6]

The Military and the Government

It is indicated by beacon logs that have been captured and encrypted network packets that Cobalt Strike or Sliver created stealthy communication routes. The report showed us how sophisticated C2 systems are not detected by traditional network monitoring systems, it is crucial that anomaly-based detection and DNS-layer behavioural analysis are required [3]

Da Vinci Data Exfiltration Cheque

Screen-hots, packet captures and cloud upload logs attest to the successful exfiltration of synthetic research data through HTTPS fragmentation. The results provide an insight into the ways in which the opponents might actually steal intellectual property through the hidden pathways in the real-world scenario, particularly in the situation when egress traffic is not well-controlled [1]

Detection Gap Analysis

As the analysis of the detection gap shows, some malicious activities were not detected because of incomplete log coverage, low-fidelity alerting and inappropriate EDR set up. As this analysis reveals, organisational interrelations are based on signature-based detection instead of behavioural analytics that could be used to detect subtle anomalies [19]

Root Cause Evaluation

The report provides root causes as poor identity governance, improperly configured cloud roles, obsolete policies on logging and the lack of SOC correlation functions. The concept of root causes enables an organisational leader to forsake tactical band-aid solutions in favour of strategic long-term structural changes that are in a position to mitigate the underlying security deficiencies [8]

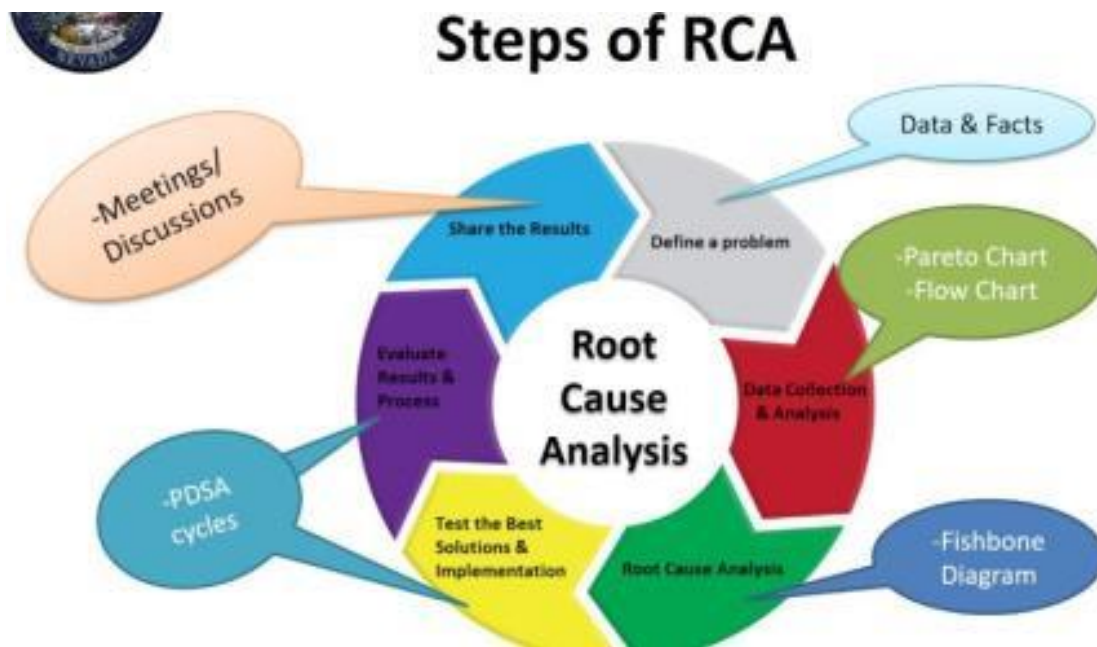


Figure: Root cause [17]

Strategic Security Recommendations

Some of the suggested recommendations are the use of phishing-resistant MFA, the refinement of EDR behavioural rules, micro-segmentation, and cloud identity governance. The suggestions include practical changes that can make their infrastructure more resilient to APT-style campaigns to compromise the intellectual property of pharmaceutical companies [5]

Priority of Architectural Improvements

The report suggests the redesign of the network boundaries, implementation of the least-privilege access models, and deployment of the zero-trust segmentation in the hybrid settings. Such underlying shifts are the ones that add a lot of complexity to the cross-domain intrusion and the preservation of C2 channels in subsequent assaults [17]

Executive Brief for the Board

This involvement indicates that the organisation confronts material strategic risks that emerge because of more sophisticated cyber threats against pharmaceutical intellectual property. Simulated APT campaign was able to penetrate on-premises and cloud environments, indicating structural weaknesses in the identity governance, network segmentation, log coverage as well as

readiness to respond to attack incidents. Some of the priority enhancements comprise adopting phishing-resistant MFA, enhancing EDR behavioural analytics, adopting Zero Trust network segmentation, and implementing cloud identity governance

Conclusion

The presence of this kind of involvement and research by the red team indicates that proactive cybersecurity measures are extremely necessary as a proactive measure of the protection of sensitive pharmaceutical research and the protection of intellectual property. It was found that when the strategic threat analysis and simulation of APT campaigns were carried out, there were vulnerabilities in the identity governance, network segmentation and monitoring which indicates gaps that higher sophistication adversaries can exploit. Lastly, the resilience would be enhanced by the availability of organisational policy and security culture grounded on the lessons learnt in the attack simulations, the reduction of potential financial and reputational losses, and avoiding the exposure of important digital assets.

References

- [1] American Hospital Association, Ransomware Attacks on Hospitals Have Changed. AHA Cybersecurity Advisory, 2024.
- [2] L. Albright, T. Murphy, and P. Chen, “Cyber-attacks on hospital systems: A narrative review,” *Journal of Healthcare Cybersecurity*, vol. 4, no. 1, pp. 12–28, 2025.
- [3] M. Brown and R. Patel, “Implementing Zero Trust and micro-segmentation in healthcare networks,” *International Journal of Health Informatics & Security*, vol. 7, no. 1, pp. 66–82, 2021.
- [4] S. Halleman, “Major healthcare cyberattack and breach incidents of 2024,” *Health Systems Security Review*, vol. 18, no. 2, pp. 140–152, 2024.
- [5] Health-ISAC, 2025 Health Sector Cyber Threat Landscape Report. Health-ISAC Annual Sector Briefing, 2024.
- [6] S. Herath, H. Gelman, J. Hastings, and Y. Wang, “Safeguarding virtual healthcare: An attacker-centric model for security and privacy,” *Cybersecurity and Privacy Journal*, vol. 10, no. 2, pp. 99–115, 2024.
- [7] HIPAA Journal Editorial Board, “Ransomware trends in healthcare: 2024 annual review,” *HIPAA Compliance and Security Review*, vol. 9, no. 1, pp. 30–47, 2025.
- [8] IBM Security, Healthcare Industry Cyberattack Trends Report 2024, IBM Security Intelligence Report, 2024.
- [9] G. Kirubavathi, W. Regis Anne, and U. K. Sridevi, “A recent review of ransomware attacks on healthcare industries,” *International Journal of System Assurance Engineering and Management*, vol. 15, no. 3, pp. 455–469, 2024.
- [10] The Lancet Digital Health, “Cyberattacks on healthcare: A growing threat,” *The Lancet Digital Health*, vol. 6, no. 9, pp. 789–790, 2024.
- [11] Microsoft Threat Intelligence, US Healthcare at Risk: Strengthening Resiliency Against Ransomware Attacks, Microsoft Security Report, 2024.

- [12] D. C. Pircalaboiu, “Cyber risk assessment in the pharmaceutical industry: Vulnerabilities and mitigation strategies,” *Journal of Global Security Studies*, vol. 9, no. 2, pp. 200–214, 2024.
- [13] B. Pranggono and A. Arabo, “Ransomware: Recent advances, analysis, challenges and future research,” *Computers & Security*, vol. 111, pp. 1–23, 2021.
- [14] M. R. Rahman, S. K. Basak, R. M. Hezaveh, and L. Williams, “Attackers reveal their arsenal: An investigation of adversarial techniques in CTI reports,” *Journal of Cyber Threat Intelligence*, vol. 3, no. 1, pp. 1–17, 2024.
- [15] J. Reed, “When ransomware kills: Attacks on healthcare facilities,” *Journal of Critical Infrastructure Security*, vol. 14, no. 3, pp. 220–234, 2023.
- [16] S. A. Rongala, “Applying cybersecurity best practices in pharmaceutical IT: A focus on data integrity and compliance,” *International Journal of Finance, Management and Regulatory Issues*, vol. 12, no. 2, pp. 50–66, 2024.
- [17] A. Smith and B. Jones, “Securing clinical trial data in cloud environments: Challenges and best practices,” *Journal of Pharmaceutical Cybersecurity*, vol. 5, no. 2, pp. 88–101, 2022.
- [18] S. Thomas, J. Mathew, P. George, and L. Roy, “Ransomware attacks on healthcare systems: Case studies and mitigation strategies,” *Medical Informatics & Engineering*, vol. 8, no. 4, pp. 34–48, 2022.
- [19] U.S. Department of Health & Human Services, *Healthcare Ransomware Threat Advisory 2023*, HHS Cybersecurity Division, 2023.
- [20] L. Zhang, C. Williams, and J. Smith, “Towards insighting cybersecurity for healthcare domains: A framework analysis,” *Healthcare Cybersecurity Review*, vol. 2, no. 1, pp. 55–76, 2023.