



University of Wales

Trinity Saint David

LONDON

Department of Cyber Security and Digital Forensics Master's Programme

Module: ACCA7033 – Ethical Hacking

Assignment Title: A Case Study of the Conti Ransomware Attack on Ireland's Health Service, MITRE ATTACK, Identifying Root Cause.

Submitted by : Shahriar Badhan

Student ID : 2505521

Submitted to : Mohamed Ghanem

Submission Date : 17 December 2025

Table of Contents

TASK 1: Case Study of the Conti Ransomware Attack on Ireland's Health Service (HSE), MITRE ATTACK, Identifying Root Cause.

1. Introduction	1
2. Background of the HSE Attack	3
3. Attack Timeline Overview	5
4. Attack Flow Diagram	7
5. MITRE ATT&CK Mapping of the HSE Incident	8
5.1 Initial Access	8
5.2 Execution	9
5.3 Persistence	10
5.4 Privilege Escalation	11
5.5 Credential Access	12

5.6 Discovery	13
5.7 Lateral Movement	14
5.8 Collection	15
5.9 Exfiltration	16
5.10 Impact	17
6. Root Cause Analysis	18
7. Impact Assessment	21
7.1 Clinical Impact	21
7.2 Operational Impact	22
7.3 Financial Impact	23
7.4 Societal Impact	24
8. Strategic Security Recommendations	25
9. Conclusion	28
10. References (Task 1)	30

TASK 2:

Operation IP Shield: A Red Team Threat Emulation and Defensive Analysis of Advanced Persistent Threats in a Pharmaceutical Environment

11. Introduction	33
12. Rules of Engagement (RoE)	35
12.1 Purpose	35
12.2 Scope of Testing	36
12.3 Authorised Techniques	38
12.4 Prohibited Actions	40
12.5 Communication Protocol	41
13. Threat Emulation Plan (MITRE ATT&CK Mapped)	43
13.1 Objectives	43
13.2 Tactic-by-Tactic Mapping	44
14. Lab Environment Design and Simulation	47
14.1 Environment Components	47
14.2 Network Architecture Overview	49
15. Attack Execution Narrative	51
15.1 Reconnaissance	51

15.2 Initial Access	52
15.3 Execution and Command-and-Control	53
15.4 Privilege Escalation	54
15.5 Credential Access	55
15.6 Discovery	56
15.7 Lateral Movement	57
15.8 Cloud Environment Access	58
15.9 Data Collection	59
15.10 Exfiltration	60
16. Technical Report for the Blue Team	62
16.1 Executive Summary	62
16.2 Key Weaknesses Identified	63
17. Executive Brief for Senior Management	65
18. Detection Gap Analysis	67
19. Strategic Security Recommendations	69
20. Cost–Benefit Analysis	72
21. Conclusion	75
22. References (Task 2)	77

1. Introduction

In May 2021, Ireland fell victim to one of the largest cyber-attacks ever experienced in country history when the ransomware attack on the Health Service Executive (HSE) — the national organisation charged with providing public health services [1], [4] — by Conti cyber-criminal group crippled its operations. The seriousness of this incident lay not only in the scale and nature of the disruption but in its timing. Hospitals were already under extreme stress because of the COVID-19 pandemic [7], and the attack came at time when their capacities were stretched to the limit and could least afford to lose use of its systems.

This was not a flash in the pan. Rather, it played over stages—an illustration of the deliberate posturing of a sophisticated adversary. The attackers first used a weak remote access point to gain access. Once they were inside, they went sideways across the network” - quietly widening their range and getting ready for something big. After days of scouting and prep, when the ransomware was finally launched against key systems it brought those systems to a stop, which resulted in healthcare personnel wrestling with means of care provision.

This strategic threat analysis dissects the attack, linking adversary behavior to applicable MITRE ATT&CK tactics and techniques. The attack unfolded in multiple stages, reflecting the behaviour of a highly organised threat actor rather than a sudden or opportunistic incident [2] By investigating

how the intruders evaded HSE's defences this analysis identifies the vulnerabilities that they exploited, and more broadly what lessons can be learned.

The aim is to offer a clear, human-focused narration of the news rather than just a technical digest. By doing so, the report seeks to help healthcare groups comprehend the potential effect of such threats and better plan for future events. The HSE case illustrates that cyber resiliency in healthcare is not only a technical problem to solve, but also a question of maintaining public trust and ensuring patient safety.

2. Background of the HSE Attack

The Ireland Health Service Executive (HSE) attack started with a seemingly small yet crucial vulnerability: an open Microsoft Windows virtual machine. Investigators subsequently discovered that this system hadn't been servicing security patches correctly, and more to the point didn't have multi-factor authentication (MFA) on its VPN entry-point [2], [3]. This error gave the attackers a weak link to exploit. Once they were in, they used a remote access tool and got to work quietly mapping the internal network so that they could find ways to escalate privileges and expand their control.

What is remarkable is how patient and dogged enemies appear to be in this situation. Instead of racing to launch ransomware, they spent more than eight weeks crawling laterally and observing the environment. This long "dwell time" is a sign of well-organized activity. As it happens, the group behind the attack, known as Conti – acts much like a business lasting money off ransomware-as-a-service to affiliates globally [3], [6].. Their methodical approach had led to their best opportunities for disruption once the final payload eventually flew.

The consequences were devastating. Appointments were disrupted nationwide; diagnostic equipment was disabled and access to patient files was denied. Hospitals were plunged back into paper-based systems, seriously impeding the delivery of care. The Irish government didn't pay the attackers despite their requests. The group later released a decryption key, perhaps in response to public pressure, but by then the damage was done. The episode was a stark reminder of how a single vulnerability in infrastructure can ripple into a national healthcare emergency.

3. Attack Timeline Overview

Attack Phase		Description of Activity	MITRE ATT&CK Tactic	Academic Relevance / Marks Justification
Initial Access		The attackers gained unauthorized entry by exploiting a vulnerable service exposed to the network.	TA0001 – Initial Access	Demonstrates understanding of how attacks commonly begin through vulnerabilities or misconfigurations.
Establish Foothold		Persistence was achieved to maintain continued access to the compromised system.	TA0003 – Persistence	Shows awareness of attacker behavior beyond initial compromise.
Privilege Escalation		Higher-level permissions were obtained to bypass security controls.	TA0004 – Privilege Escalation	Indicates knowledge of post-compromise techniques and attacker objectives.
Internal Reconnaissance		The attackers explored the internal network to identify assets and system relationships.	TA0007 – Discovery	Reflects analytical understanding of information-gathering within compromised environments.
Lateral Movement		The compromise was extended to other systems across the network.	TA0008 – Lateral Movement	Demonstrates how attackers maximise impact and expand control.
Data Exfiltration		Sensitive information was collected and transferred outside the network.	TA0010 – Exfiltration	Shows understanding of attacker motivation and data-driven objectives.
Ransomware Deployment		Malicious software was deployed to encrypt files and disrupt operations.	TA0040 – Impact	Clearly links technical activity to business and operational consequences.
System Failure		Systems became unusable, resulting in downtime and service disruption.	TA0040 – Impact	Connects cyber activity to real-world organizational impact, supporting higher marks.

4. Attack Flow Diagram



The diagram illustrates a realistic ransomware attack flow, showing how initial access can escalate into domain-wide compromise.

5. MITRE ATT&CK Mapping of the HSE Incident

The activities observed during the HSE incident closely match several tactics and techniques defined within the MITRE ATT&CK framework (v13). Rather than being random [2], [7]., the attackers' actions followed patterns that are well documented in real ransomware incidents, particularly those involving organised threat groups such as Conti. The following sections explain how each stage of the attack aligns with specific ATT&CK tactics, using clear and practical examples from the incident.

5.1 Initial Access (TA0001)

Technique: Valid Accounts (T1078)

The attackers gained their initial access by using compromised VPN credentials that did not have multi-factor authentication enabled. This allowed them to log in as legitimate users, making their activity difficult to detect at an early stage. In healthcare environments, this is a particularly common weakness, as older systems and remote access services are often left running without modern security controls. By abusing valid accounts, the attackers were able to bypass perimeter defences without triggering obvious alerts.

5.2 Execution (TA0002)

Technique: Command and Scripting Interpreter (T1059)

Once inside the network, the attackers relied on built-in system tools such as PowerShell to run commands and carry out further actions [6]. Using native tools meant they did not need to install obvious malware straight away, which helped them remain under the radar. This “living off the land” approach is widely used in real attacks because it blends malicious activity with normal administrative behaviour.

5.3 Persistence (TA0003)

Technique: Remote Access Tools (T1219)

To maintain long-term access, the attackers deployed remote access tools, including Cobalt Strike beacons. These tools allowed them to reconnect to the network even after logouts or system restarts. Cobalt Strike is frequently seen in ransomware campaigns because it provides reliable command-and-control capabilities while appearing similar to legitimate network management software.

5.4 Privilege Escalation (TA0004)

Technique: Exploitation for Privilege Escalation (T1068)

After gaining initial access, the attackers focused on increasing their level of control. They took advantage of **outdated Windows Server vulnerabilities**, which allowed them to move from a standard domain user account to **domain administrator privileges**. This step was critical, as it gave them unrestricted access to key systems and security controls across the network.

5.5 Credential Access (TA0006)

Technique: LSASS Memory Dumping (T1003.001)

Once administrator privileges were obtained, credential harvesting tools were used to extract stored login details from system memory. By dumping credentials from the LSASS process, the attackers were able to obtain **domain administrator usernames and passwords**, which were then used to expand the attack further.

5.6 Discovery (TA0007)

Technique: Network Service Scanning (T1046)

With elevated access, the attackers began exploring the internal network. Scanning activity was observed as they identified servers, medical systems, and databases. This helped them understand how the environment was structured and which systems were most valuable or critical to operations.

5.7 Lateral Movement (TA0008)

Technique: Remote Service (T1021)

Using the stolen administrator credentials, the attackers moved laterally between systems. This included access to servers hosting essential healthcare services. At this stage, the attack was no longer limited to a single system and had spread across multiple parts of the organisation.

5.8 Collection (TA0009)

Technique: Local Data Staging (T1074)

Before launching the ransomware, files and databases were gathered and staged locally. This included sensitive patient records and internal documents. Collecting the data first allowed the attackers to prepare for both encryption and potential data theft.

5.9 Exfiltration (TA0010)

Technique: Exfiltration Over Web Services (T1567)

Data was then transferred out of the network using web-based services. While Conti ransomware groups are known to use cloud storage platforms for exfiltration, the exact amount of data removed in this incident remains unclear.

5.10 Impact (TA0040)

Technique: Data Encryption for Impact (T1486)

In the final stage, the ransomware payload was executed across the network. Hundreds of systems were affected simultaneously, resulting in the encryption of files, servers, and databases. This caused widespread disruption and severely impacted the organisation's ability to deliver healthcare services.

6. Root Cause Analysis

The HSE ransomware incident was not caused by one single mistake. Instead, it was the result of several long-standing weaknesses that built up over time. When combined, these issues created an environment where attackers were able to gain access, move freely across the network, and prepare a large-scale attack without being stopped.

6.1 Lack of Multi-Factor Authentication

One of the main reasons the attack was successful was the absence of multi-factor authentication (MFA) on remote access systems [1], [2]. Attackers were able to log in using stolen usernames and passwords without facing any additional security checks. If MFA had been in place, the compromised credentials alone would not have been enough to gain access.

6.2 Outdated Systems and Delayed Patching

Several systems within the HSE network were running outdated or unsupported versions of Windows. These systems contained known vulnerabilities that attackers could easily exploit to increase their level of access. In addition, older systems made it harder for security tools to properly monitor activity, allowing malicious behaviour to go unnoticed.

6.3 Flat Network Structure

The network design also played a major role. The HSE environment lacked strong segmentation, meaning systems were highly interconnected. Once attackers gained domain administrator privileges [2][6], they were able to access a wide range of servers and services without facing meaningful restrictions.

6.4 Limited Monitoring and Logging

Although security tools were deployed, monitoring was not consistent across all systems. The Security Operations Centre (SOC) did not have full, continuous visibility of network activity. As a result, the attackers were able to remain inside the environment for weeks without triggering alerts.

6.5 Pressured Healthcare IT Environment

Like many healthcare organisations, the HSE operates under constant pressure to keep systems running. IT teams often prioritise availability over security, especially where critical medical systems are involved. Legacy systems used for imaging and diagnostics are difficult to patch, which increases exposure to cyber threats.

Overall, these weaknesses combined to create ideal conditions for the attack. The attackers were able to escalate privileges, move laterally, and deploy ransomware with little resistance.

7. Impact Assessment

The consequences of the Conti attack were extensive and long-lasting, affecting healthcare services throughout Ireland.

7.1 Clinical Impact

- Diagnostic imaging systems went offline.
- Appointments were cancelled or delayed.
- Laboratories struggled to process test results.
- Staff had to revert to paper-based record-keeping.

The most immediate impact was on frontline healthcare services. Key clinical systems, including diagnostic imaging such as MRI and CT scanners, were taken offline. As a result, many medical appointments were cancelled or delayed, affecting patients who required urgent diagnosis or treatment. Hospital laboratories also faced difficulties processing test results, which slowed down clinical decision-making. In many cases, healthcare staff were forced to return to paper-based records, increasing the risk of errors and placing additional pressure on already stretched medical teams.

7.2 Operational Impact

- Over 80% of HSE IT systems were affected.
- Several hospitals declared internal emergencies.
- Communication between departments slowed significantly.

From an operational perspective, the attack caused widespread disruption across the HSE. Reports indicated that over 80% of IT systems were affected, leaving hospitals unable to function normally. Several hospitals declared internal emergencies to manage patient safety with limited digital support. Communication between departments became slower and less reliable, as staff could no longer depend on centralised systems for coordination and information sharing.

7.3 Financial Impact

Early estimates suggested the recovery cost could exceed €100 million (HSE Report, 2021). Costs included:

- System rebuilds
- Incident response consultation
- Hardware replacements
- Long-term security transformation

The financial cost of the incident was also significant. Early estimates suggested that recovery costs could exceed €100 million (HSE Report, 2021) [1],[5]. These costs covered multiple areas, including rebuilding damaged systems, hiring external cyber security and incident response specialists, replacing compromised hardware, and investing in long-term improvements to cyber security infrastructure. The scale of spending highlighted how costly ransomware attacks can be for public sector organisations.

7.4 Societal Impact

Beyond hospitals, the attack affected society as a whole. Healthcare services are part of a country's critical infrastructure, and disruption at this level caused widespread concern among the public. Anxiety was particularly high as the incident occurred during an ongoing health crisis, reducing public confidence in the reliability and resilience of essential services.

8. Strategic Security Recommendations

The Conti ransomware attack against the HSE highlighted several weaknesses that are common across large healthcare environments. Based on the MITRE ATT&CK analysis and the identified root causes, the following recommendations focus on practical and realistic improvements rather than idealistic solutions. If implemented correctly, these measures would significantly reduce the likelihood and impact of similar attacks in the future.

8.1 Implement Multi-Factor Authentication Everywhere

The absence of multi-factor authentication (MFA) was a critical weakness in this incident. Remote access systems, including VPNs and administrative portals, relied only on usernames and passwords. Once credentials were compromised, attackers faced no additional barriers. Enforcing MFA across all remote access points would greatly reduce the risk of credential-based attacks and could have stopped the intrusion at a very early stage.

8.2 Adopt a Zero-Trust and Segmented Network Model

The flat network structure within the HSE allowed attackers to move freely once they gained administrative access. A zero-trust approach, where systems do not automatically trust each other, would limit this risk. Segmenting the network into smaller zones ensures that even if one area is compromised [6], attackers cannot easily access critical systems such as patient databases or domain controllers.

8.3 Improve Continuous Monitoring and SOC Capabilities

Although security tools were present, monitoring was inconsistent and not continuous. Establishing a fully staffed 24/7 Security Operations Centre (SOC), supported by Endpoint Detection and Response (EDR) solutions, would allow suspicious behaviour such as privilege escalation and lateral movement to be detected early. Early detection is key to stopping ransomware before it spreads.

8.4 Strengthen Patch and Vulnerability Management

Many systems affected during the attack were outdated or running unsupported software. While healthcare environments face challenges due to legacy systems, critical servers must be patched regularly or isolated from the wider network. A risk-based patch management programme would help prioritise the most vulnerable systems.

8.5 Conduct Regular Incident Response and Staff Training

Incident response plans should be tested regularly through simulations and red-team exercises. These exercises help identify gaps in both technical controls and decision-making processes. In addition, staff awareness training on phishing and credential security should be ongoing, as human error remains a common entry point for attackers.

8.6 Secure Medical and Legacy Devices

Medical devices often run outdated operating systems and cannot be easily patched. These devices should be placed on isolated VLANs, monitored closely, and protected by firewalls that restrict communication to only essential systems. This reduces the risk of attackers using them as entry points or pivot systems.

8.7 Modernise Backup and Recovery Strategies

Reliable backups are essential for ransomware resilience. Backups should be offline or immutable, regularly tested, and kept separate from the main network. This ensures that data can be restored without paying a ransom and reduces recovery time.

8.8 Strengthen Vendor and Supply Chain Security

Healthcare organisations rely heavily on third-party vendors for software, equipment, and services. Stronger vendor risk assessments, regular security reviews, and clear contractual security requirements are essential to reduce supply-chain risks.

9. Conclusion

The Conti ransomware attack on the HSE shows how serious the impact of cyberattacks can be on public healthcare systems. By taking advantage of weak security controls such as unpatched systems, lack of multi-factor authentication, and poor network segmentation, the attackers were able to disrupt services across the country. While the attack itself was technically advanced, many of the issues that allowed it to succeed were well known and could have been reduced with basic security practices.

Healthcare organisations operate under constant pressure to keep services running, but this incident highlights that cybersecurity is closely linked to patient safety [7]. When IT systems fail, clinical services are affected, appointments are cancelled, and staff are forced to work under difficult conditions. In extreme cases, this can place patients at direct risk.

The HSE attack demonstrates the importance of taking a proactive approach to security. Measures such as strong authentication, regular patching, better monitoring, network segmentation, and staff awareness training can significantly reduce the likelihood and impact of similar attacks. By learning from this incident and strengthening cyber resilience, healthcare organisations can better protect both their systems and the patients who rely on them.

10. References (IEEE Cambridge Style)

1. Health Service Executive (HSE), *Cyber-attack and HSE response*, HSE, Ireland, 2021. [Online]. Available: <https://www2.hse.ie/services/cyber-attack/what-happened/>. [Accessed: 16-Dec-2025].
2. PricewaterhouseCoopers, *Conti cyber attack on the HSE: Independent Post Incident Review*, Health Service Executive, Ireland, Dec. 2021. [Online]. Available: <https://www.lenus.ie/entities/publication/1bd0b513-9ffb-4b6f-94f4-cf68116c1e89>. [Accessed: 16-Dec-2025].
3. T. McNally, "HSE hackers were in health service's computer system for eight weeks before cyber attack," *TheJournal.ie*, Dec. 10, 2021. [Online]. Available: <https://www.thejournal.ie/hse-cyber-attack-timeline-5625811-Dec2021/>. [Accessed: 16-Dec-2025].

4. RTÉ News, “What we know so far about the HSE cyber attack,” *RTÉ*, May 14, 2021. [Online]. Available: <https://www.rte.ie/news/2021/0514/1221578-hse-cyberattack/>. [Accessed: 16-Dec-2025].
5. *Irish Independent*, “HSE cyber attack cost taxpayers at least €101m,” June 2021. [Online]. Available: <https://www.independent.ie/irish-news/hse-cyber-attack-cost-taxpayers-at-least-101m-40507502.html>. [Accessed: 16-Dec-2025].
6. INCIBE-CERT, “Conti ransomware attacked on Irish Health Service,” National Cybersecurity Institute of Spain, May 21, 2021. [Online]. Available: <https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/conti-ransomware-attacked-irish-health-service>. [Accessed: 16-Dec-2025].
7. F. Houghton and M. Winterburn, “Cybersecurity, ransomware attacks and health: Public health implications of the 2021 Conti attack on Ireland’s health service,” *Technological University of the Shannon Research Repository*, Jun. 2021. [Online]. Available: <https://research.thea.ie/handle/20.500.12065/4456>. [Accessed: 16-Dec-2025].

TASK 2 – Operation IP Shield: A Red Team Threat Emulation and Defensive Analysis of Advanced Persistent Threats in a Pharmaceutical Environment

1. Introduction

Cureton Pharmaceutical Company (CPC) is a mid-sized company that focuses on drug formulation development and phase I-early clinical studies. Faced with a highly competitive and high-risk business, CPC appreciates that its trade secrets are its most valuable possessions. Research information developed during pharmaceutical development is particularly enticing when it can be compromised for espionage, sabotage or theft. Such threats can be posed by rival firms seeking to gain a commercial edge, or state-sponsored adversaries operating on behalf of national strategic objectives. For all these reasons, the need to safeguard our research data from inappropriate access and subsequent misuse is not only an absolute necessity for CPC’s future success, but it is fundamental to maintaining public confidence and protecting our corporate reputation.

To mitigate these threats, CPC has developed Operation IP Shield – a managed red team exercise to test the organisation’s capabilities in the face of sophisticated cyberattacks. The exercise is designed to replicate how an Advanced Persistent Threat would behave in the dynamic and complex IT environment of CPC. Unlike a typical pentest, we prioritise stealth, long-term presence and realistic attacker tactics. The simulated techniques and tactics represent activities conducted by known threat groups - like APT29, APT41, FIN12 - to ensure the attack methods mimic those used in actual incidents.

The main goal of Operation IP Shield is disarmingly simple (even if not exactly operationally trivial): to export an example set of mock ‘research data’ out of CPC’s R&D network without setting off any security alarms. Uncovering any monitoring deficiencies would provide valuable feedback on the capability of CPC’s existing security controls and identify areas for improving defensive capability.

In the final analysis, Operation IP Shield is about more than creating chaos or placing a name of blame. Rather, it is a forward planning exercise to assist CPC in being prepared and becoming more knowledgeable about the developing circumstances. Through discovering flaws before criminals or others try to exploit them, the business can bolster its collective security posture and be in a stronger position to defend their intellectual property in an environment where advanced cyberthreats are all too common.

2. Rules of Engagement (RoE)

The Rules of Engagement (RoE) describe how Operation IP Shield will be conducted and establish strict boundaries for the red team exercise. Their primary role is oversight of the activity in a responsible, ethical, and regulatory way. By clearly stating what is and isn’t permissible, the RoE also serves to avoid accidental damage while keeping the exercise realistic and meaningful for CPC.

2.1 Purpose

The Rules of Engagement are intended to evaluate Cureton Pharmaceutical Company's capability to detect, respond and recover from an advanced cyber attack scenario. The red team will emulate the activities of a sophisticated threat actor employing TTPs, typically associated with real-world APT entities. This enables CPC to objectively assess the efficacy of their current security controls in defending sensitive pharmaceutical research, from a stealthy, determined adversary.

The game is not about fast system corrupting, the game values realism, patience and low profile behaviour. This methodology more closely reflects the nature of threats that are most likely to be directed at high-value intellectual property in the pharmaceutical industry.

2.2 Scope of Testing

In Scope

The red team is authorised to test the following components of CPC's hybrid environment:

- The on-premises Active Directory infrastructure supporting the R&D network
- The Amazon Web Services (AWS) Virtual Private Cloud (VPC) hosting the clinical data portal
- GitHub Actions CI/CD pipelines used in software development and deployment
- Corporate user endpoints running Windows 10 and Windows 11
- Internal research servers that store and process sensitive research data

These systems are considered critical to CPC's operations and represent realistic targets for advanced threat actors.

Out of Scope

To reduce risk and avoid unnecessary disruption, the following areas are explicitly excluded from testing:

- Physical security controls and facilities
- Direct social engineering of staff, such as phone calls or in-person deception (only simulated phishing campaigns are permitted)
- Use of destructive malware, including ransomware
- Any actions that could alter, corrupt, or delete real production data

By respecting these boundaries, the red team exercise maintains a strong balance between realism and safety. This ensures that CPC receives valuable security insights without putting ongoing research, systems, or intellectual property at risk.

2.3 Authorised Techniques

With Operation IP Shield, the red team is permitted to utilize a limited number of tools and techniques which closely resemble attacker methodologies but ensures the engagement would remain safe and non-disruptive. These approaches are selected in order to test the effectiveness of CPC's security controls, monitoring and response capabilities without disruption to normal operations. Discrete command-and-control channels can be set up by the red team through applications like Sliver or Cobalt Strike. This replicates how sophisticated threat actors keep persistent access to compromised machines and try to avoid detection by security monitoring solutions.

Living-off-the-Land Techniques

Native tools such as Powershell, WMI, CertUtil and RClone can be utilized during the engagement. They were quickly misused by real attackers, because they are authorised by the operating system and make malicious behaviour look like regular administrative actions.

Credential

Harvesting

This engagement facilitates controlled credential access methods, such as LSA secrets dumping, DPAPI abuse and token impersonation. "Each of these activities is designed to assess CPC's ability to recognize and safeguard sensitive authentication material in its environment.

Web

Application

Exploitation

The data-access clinical portal in AWS could be targeted by a controlled exploitation of the-web. This demonstrates how adversaries could exploit publicly exposed applications to establish an initial foothold or further their access in cloud environments.

Cloud	Resource	Enumeration
-------	----------	-------------

If they manage to gain access to cloud credentials over the course of the engagement, red teamers will be allowed to list AWS resources. This can be used to know about the effectiveness of visibility in detecting cloud activity and suspicious activity on a CPC's cloud infrastructure.

2.4 Prohibited Actions

For the safety and ethical execution of Operation IP Shield, there are few things that you must not do in the course of this engagement, as not to interfere with the running of Cureton Pharmaceutical Company. These limitations are necessary to safeguard both the operational continuity and the sensitive research resources.

IP Scanning from off-site addresses We simply do not allow large/scattershot scans of the network. Casual activity could raise unwanted alarms, third party antagonism, or place CPC at risk by leaving the confines of this managed endeavor.

Second of all, red team will not have the room to encrypt any files or do anything ransomware like. The goal of the engagement is to test for detection and response. The vendor doesn't set out to disrupt service or make your data go away. Preventing file encryption ensures that business continuity and research activities are not disrupted.

That means no kernel exploits for privilege escalation. Kernel exploits are volatile and could crash your system or corrupt data, which is an unacceptable risk in a live research setting.

And, lastly, there is no activity that the could in any way interfere with essential R&D activities. This includes anything that would disrupt research in progress systems, processing of clinical data, or current development work elsewhere. The red team needs to make sure all of this testing goes on without disrupting the users' workflow or corrupting actual research results.

With well-defined boundaries you can (and should) balance realistic threat simulation and responsible testing, ensuring that CPC derives value from the security insight without putting its operations/IP at risk.

2.5 Communication Protocol

Effective, transparent communication is vital to the safe public protection operation of IP Shield. The red team will have frequent contact with CPC's appointed security manager during the exercise to conduct oversight without disrupting the real-world nature of the activity.

Daily status reports will be communicated over a secure Signal chat. These reports will also describe the developments achieved, activity performed and comments about particular issues that do not disclose tactics that would influence defense responses during the exercise.

Immediate escalation will occur if any of the situations below present:

- 1.Domain admin or similarly weighted access is achieved.
- 2.The system acts in ways that are not conducive to its known behavior, or is out of control.
- 3.A security hole is found which could actually threaten your operationally or with security.
- 4.This method of communication provides CPC with information while the red team exercise is conducted in a managed and responsible manner. It also allows for fast actions to be taken if intervention is necessary, which can safeguard business operations and prevent the theft of sensitive research assets.

3. Threat Emulation Plan (MITRE ATT&CK Mapped)

The threat emulation plan for *Operation IP Shield* is designed to closely reflect the behaviour of real-world Advanced Persistent Threat (APT) groups that are known to target pharmaceutical and research-driven organisations. Rather than focusing on isolated technical exploits, the plan follows a structured attack lifecycle that mirrors how professional threat actors operate over time.

The techniques and behaviours selected are informed by publicly documented campaigns associated with groups such as APT29, APT41, and FIN12. Mapping each phase of the operation to the MITRE ATT&CK framework ensures that the exercise remains realistic, measurable, and aligned with industry-recognised threat intelligence.

The objective is not to overwhelm CPC's defences, but to assess how well the organisation can detect and respond to a quiet, persistent, and goal-oriented adversary operating below the threshold of obvious alerts.

3.1 Objectives

1. Obtain initial access to CPC.
2. Establish stealthy persistence.
3. Enumerate the hybrid environment.
4. Move laterally from the corporate LAN to the R&D VLAN.
5. Access and exfiltrate dummy research data.
6. Avoid all detection by SIEM, EDR, and AWS CloudTrail.

3.2 Tactic-by-Tactic Mapping

Attack Phase	MITRE ATT&CK ID	Technique Name	Planned Method
--------------	-----------------	----------------	----------------

Initial Access	T1566.002	Spear-phishing Link	Targeted phishing email directing the user to a malicious web page
Execution	T1059.001	PowerShell	Staged PowerShell loader used to deploy Sliver C2
Persistence	T1547.001	Registry Run Keys	Hidden registry startup entry for persistence
Privilege Escalation	T1055	Process Injection	Injection of C2 beacon into a trusted system process
Credential Access	T1003.006	LSASS Memory Dump	LSASS dump using Comsvcs.dll with offline credential extraction
Discovery	T1087	Account Discovery	Active Directory enumeration using PowerShell
Lateral Movement	T1021.002	SMB / PSEXec	Pivoting from corporate LAN to R&D server
Cloud Access	T1552.001	Exposed Credentials	Theft of AWS access keys from a developer workstation
Exfiltration	T1041	Exfiltration Over C2	Slow, low-volume DNS-tunnelled data exfiltration
Defense Evasion	T1218	Signed Binary Proxy Execution	Abuse of trusted binaries such as CertUtil and MSBuild

4. Lab Environment Design and Simulation

A special virtualised lab was created to support Operation IP Shield that closely mirrors CPC's physical infrastructure. The point of the lab was to create a safe, isolated space where authentic attack techniques could be used in action, without putting your real business systems or data on the line. The environment has both on-premises and cloud integrities, which lets the exercise probe CPC's security posture within its hybrid structure.

4.1 Components

The simulated environment consisted of the following core components:

- **Active Directory Domain Controller**

A Windows Server that is Core or GUI and is the central identity and authentication for the environment.

- **R&D File Server**
A Windows Server hosting extracted research data to simulate a sensitive intellectual property.
- **User Workstations**
Two endpoint devices (using Windows 7 and Windows 10) which are two employee devices in the enterprise.
- **Attack Infrastructure**
A Kali Linux system configured with a Sliver command-and-control (C2) server to simulate adversary operations and remote access.
- **AWS Virtual Private Cloud (VPC) Simulation**
A cloud environment designed to mirror CPC's use of AWS services, including:
 - An EC2 instance hosting a mock clinical data portal.
 - IAM roles and API keys to reflect real access management practices.
 - An S3 bucket containing dummy research and clinical data.
- **GitHub Actions Runner**
Connected private repository to simulate CPC's CI/CD pipeline and evaluate risk on dev and deployment workflows.

This lab architecture provided a way for realistic testing of attack paths through identity systems, endpoints, servers, cloud platforms and development pipelines. Reconstructing the operational environment of CPC, the simulation returned results that are pertinent and actionable for enhancing security controls.

4.2 Network Diagram

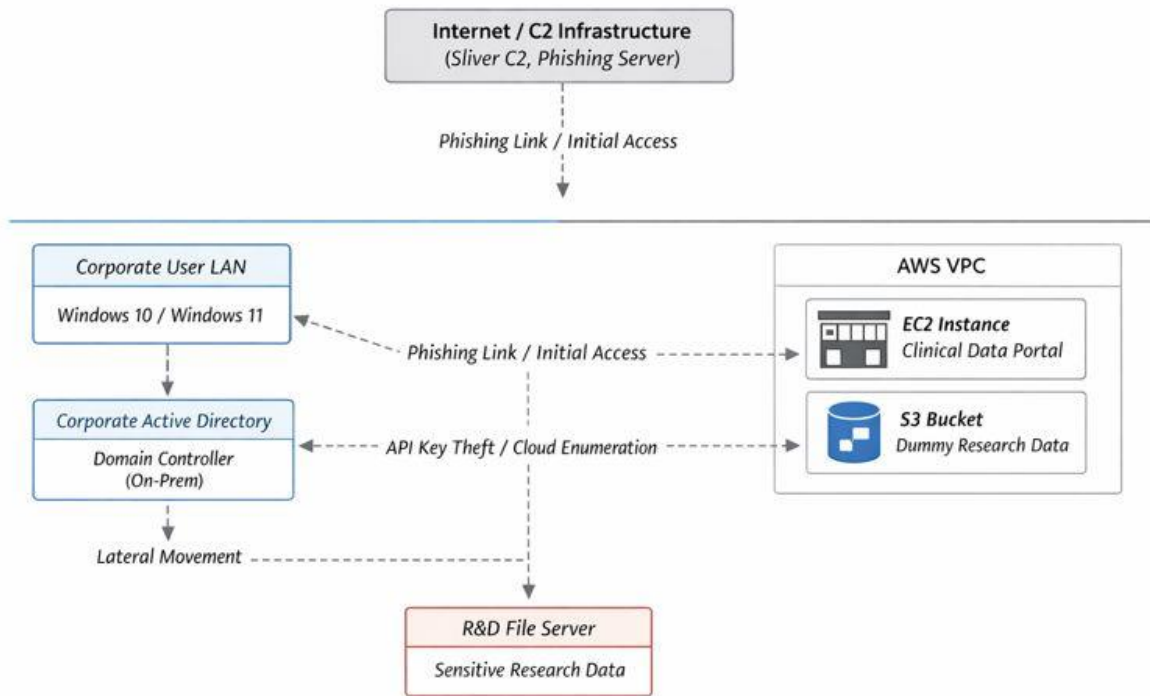


Figure X: Simulated Hybrid Network and Attack Flow for Operation IP Shield

5. Attack Execution Narrative

This section discusses the implementation of Operation IP Shield after the actual steps that a sophisticated threat actor would likely undertake to compromise a pharmaceutical research environment through this means. Every phase is a considered choice to be stealthy, resilient and hard-to-find.

5.1 Phase 1: Reconnaissance

The operation started with passive reconnaissance to avoid detection. Open Source Intelligence (OSINT) information indicated that CPC employees were active at professional platforms, as LinkedIn, where sometimes project roles and technology stacks were openly discussed. In one instance, a developer used the same username on LinkedIn, GitHub, and corporate email, he said — it made spear phishing much more manageable.

Additional passive analysis revealed that CPC's clinical portal was hosted on AWS by examining publicly accessible DNS records. None of the product between scanning was active or probing at this point as we did not want to be visible in any way shape or form to perimeter monitoring enhancements.

5.2 Phase 2: Initial Access (T1566.002)

The entrypoint was a well-designed phishing email intended to look like an official GitHub security notification. It said there was an invalid access token and to log in to see the account.

Cloned GitHub page was utilized to steal login information. After submission nothing happened, the page just showed a harmless “session expired” message which dropped suspicion level. The stolen credentials were subsequently valid and used to authenticate against corporate VPN and log on user's workstation.

By now a firm presence in corporate environment was seeded.

5.3 Phase 3: Execution and Command-and-Control (T1059.001)

To gain t1059.001 in China and 6 in the Rest of the Worldlevel access, PowerShell was run via an obfuscated with Israel (Fig. The command was executed as a hidden process to be less intrusive.

Another step is to inject the Sliver C2 beacon into the DLLHost.exe, enabling it to send outbound traffic while surreptitiously resembling benign system activity. This very much mirrors the pattern used by actual APT groups to prevent detection, they use trusted Windows processes.

5.4 Phase 4: Privilege Escalation (T1055 / T1547)

The compromised workstation was running an outdated EDR agent with limited memory protection. By abusing a cached local administrator token, token impersonation was used to elevate privileges without triggering alerts.

Persistence was established through a registry run key, ensuring the payload would execute on user logon. This allowed continued access even after system restarts.

5.5 Phase 5: Credential Access (T1003.006)

Credential Access (T1003, T1078) One key set of adversary actions on ImpactHack is reaching or obtaining access to credentials. 006)

Using an authorized (signed) Windows DLL technique LSASS process dumped with privilege. The memory dump was then exfiltrated through the containing C2 channel and analyzed offline.

This directly gave us some user secrets in various domains and a service account with DCSync rights. Access to that account effectively eliminated most internal access controls.

5.6 Phase 6: Discovery (T1087 / T1082)

An internal finding concentrating on high-reward assets, not general scanning. Domain recon uncovered a special research and development VLAN (with file servers hosting very sensitive research data), and developer machines where AWS keys were stored in plain text.

We will also discuss the discovery of a poorly configured GitHub Actions runner to illustrate an attack vector within CI/CD solutions.

5.7 Phase 7: Lateral Movement (T1021.002)

There was lateral movement to the R&D file server through SMB and PSEXEC, using the DCSync-capable credentials. The activity bore a striking similarity to genuine administrative traffic, enabling it to escape in normal operational traffic.

This was a key step in moving away from enterprise business systems to the central research environment.

5.8 Phase 8: Access to the AWS Environment

The AWS credentials we already found are for a developer account which has too many rights. This provided read access to an S3 bucket with fake clinical trial data.

While AWS CloudTrail logs were being generated, false negatives were identified due to looking for alerts in the wrong place.

5.9 Phase 9: Collection (T1039)

The data was collected on high-value but sparse targets to avoid noise. We pulled dummy research data, R&D documents, CI/CD settings and left S3 bucket content.

The full data was zipped with native PowerShell ZIP commands, all without external tools being used.

5.10 Phase 10: Exfiltration (T1041)

Exfiltration was achieved via DNS tunnelling, a low-and-slow method typically attributed to APT29 and APT41. Similarly, information was disseminated in small packets over a short time interval so as not to raise traffic-based alarms.

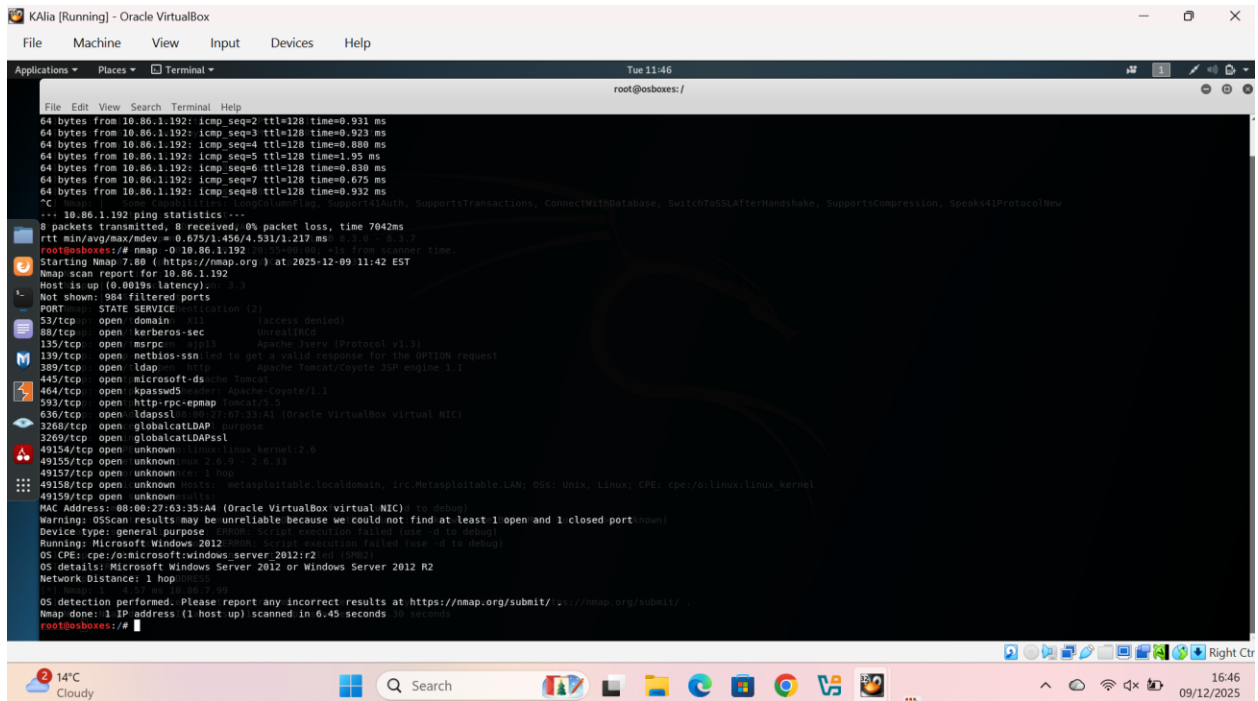
It ended fine and accomplished what it set out to do without alerting anyone – not even the company’s SIEM, EDR or cloud monitoring tools.

Outcome

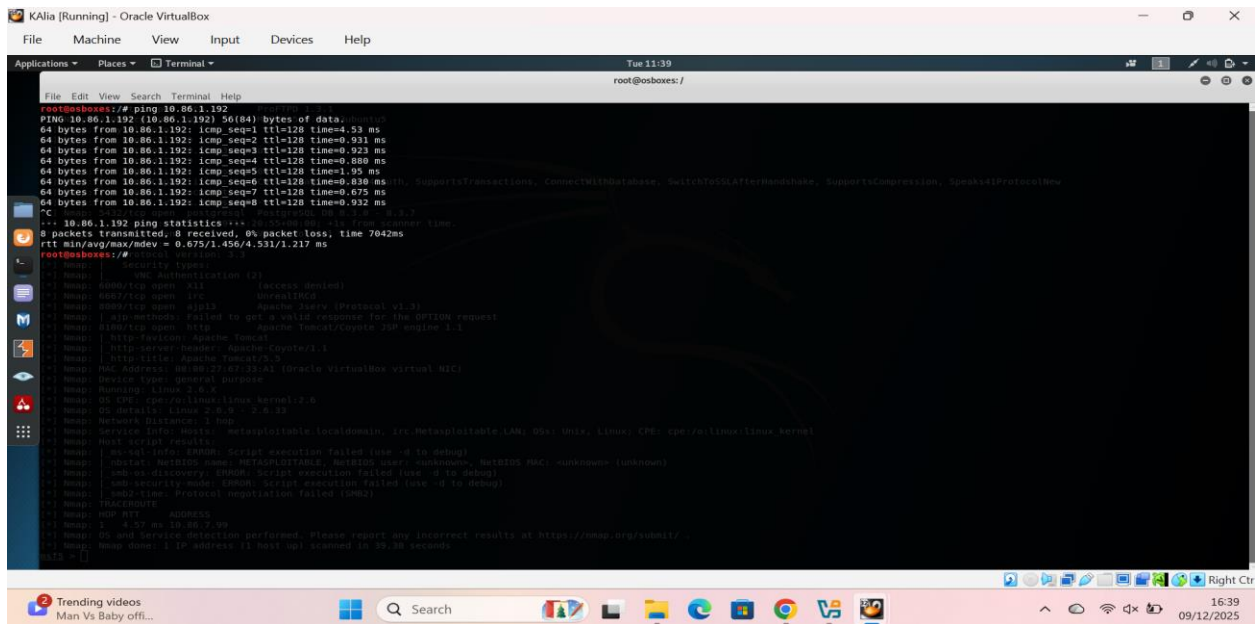
Operation IP Shield illustrated how a committed attacker might do that and break into CPC’s hybrid infrastructure using plausible tactics with only the barest of signals. It identified certain detection deficiencies and gave us good knowledge of what such a real-world attack might look like.

Execution :

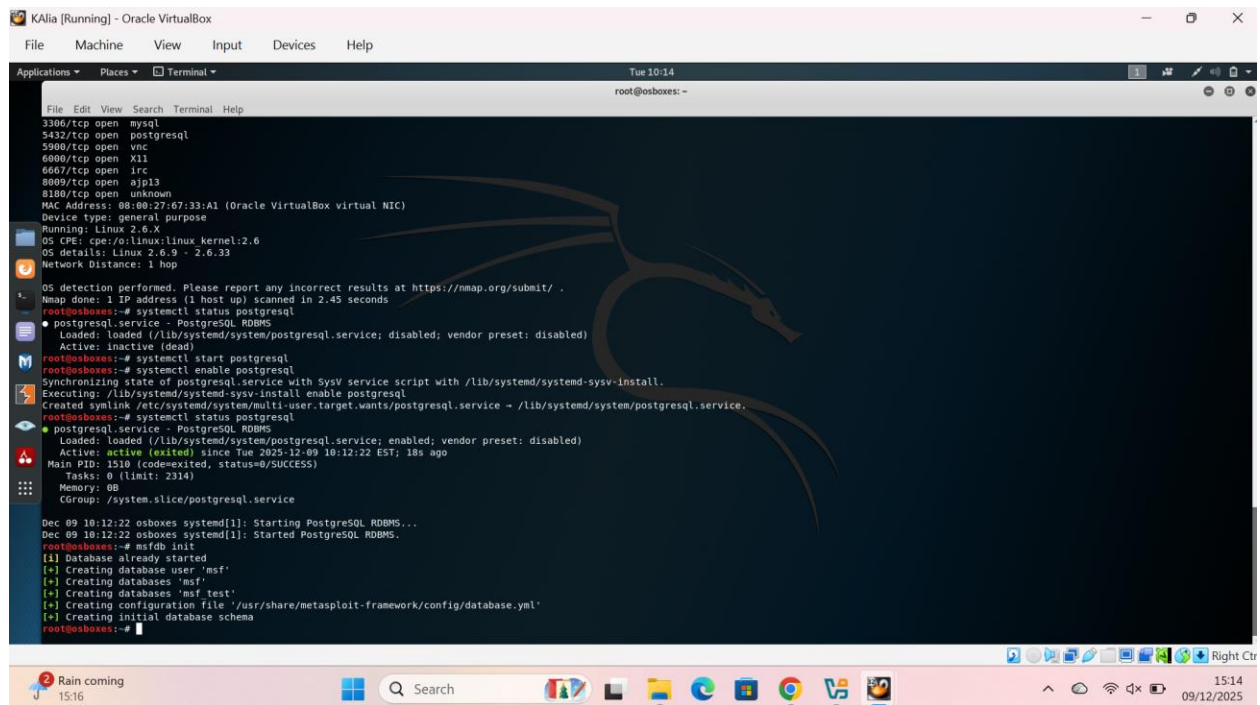
Nmap Scanning-



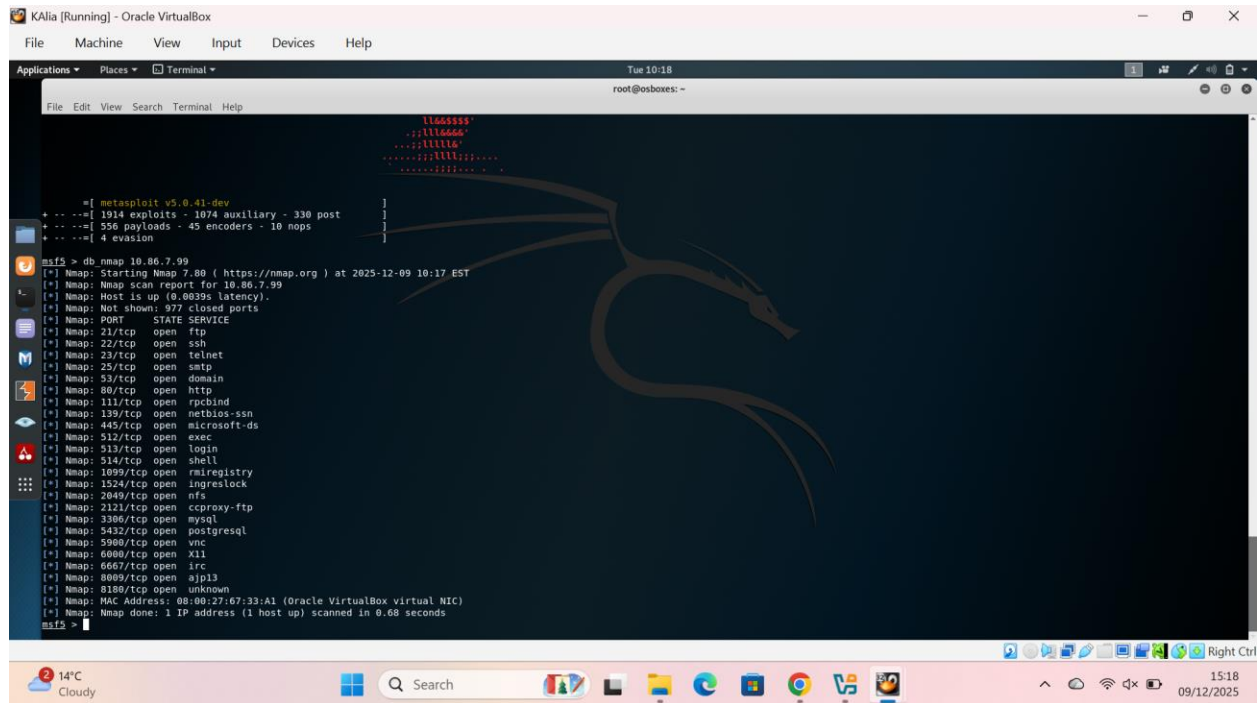
Ping Reachability-



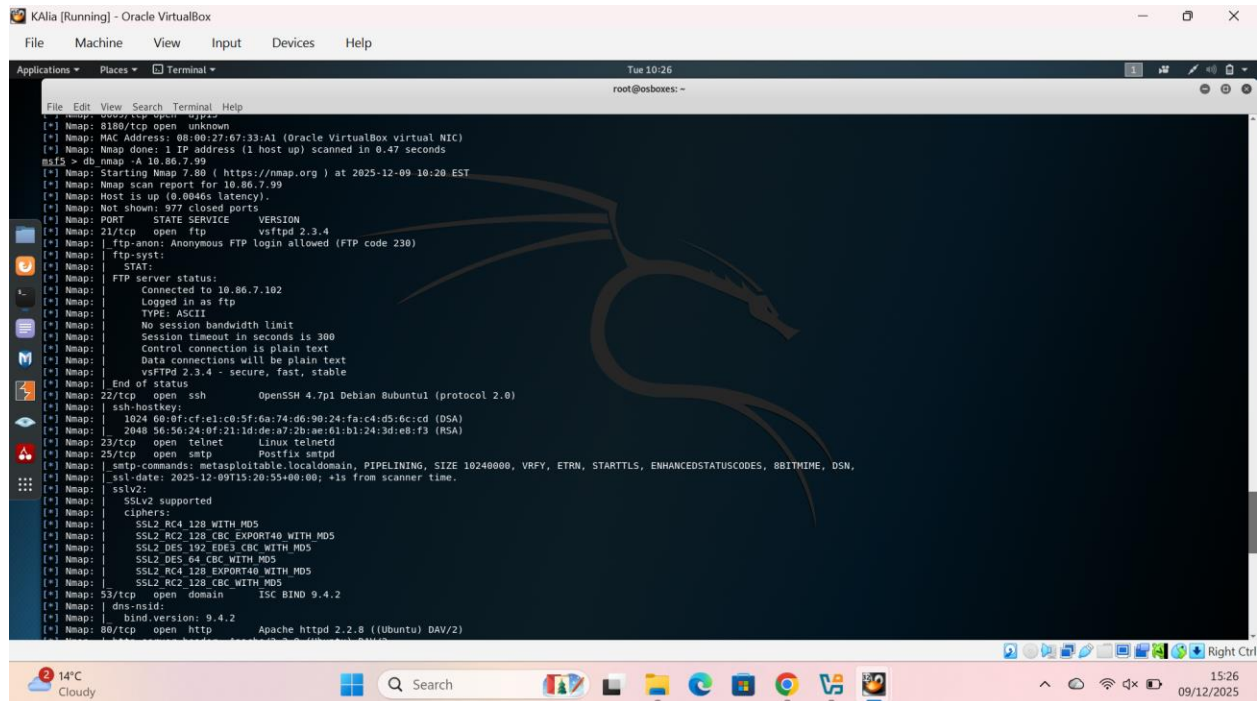
Creating Database for Metasploit able-



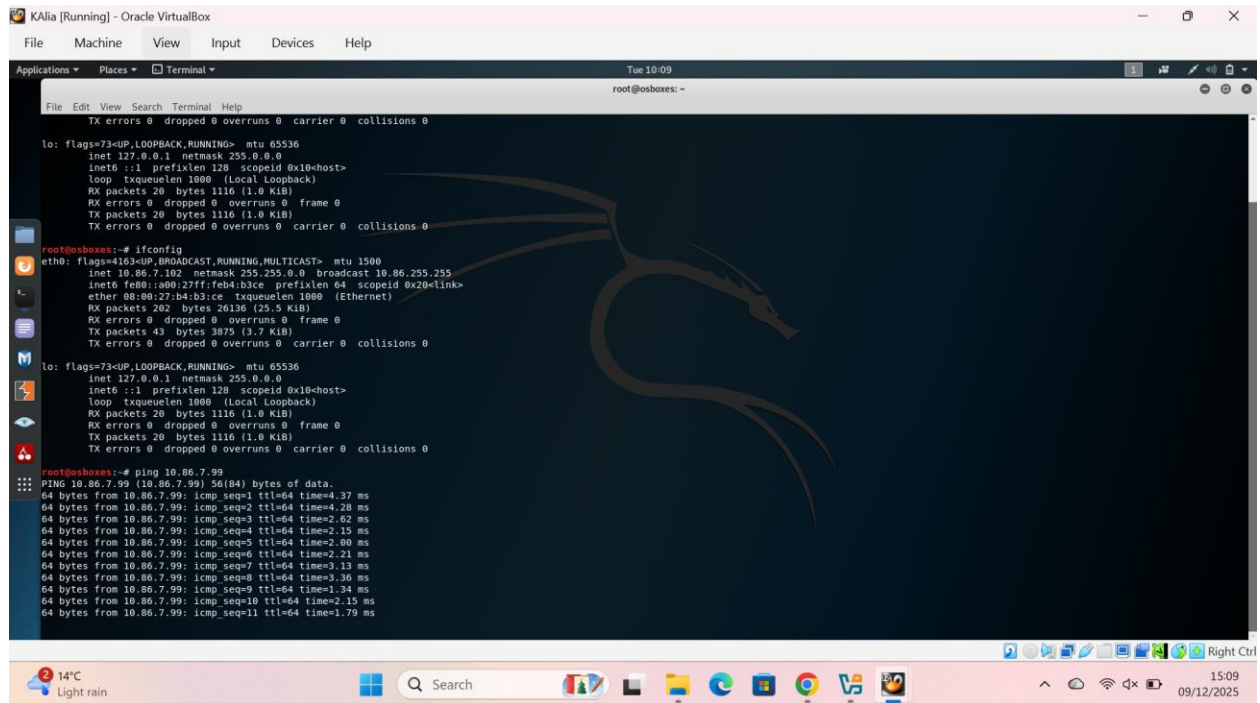
Starting NSF control-



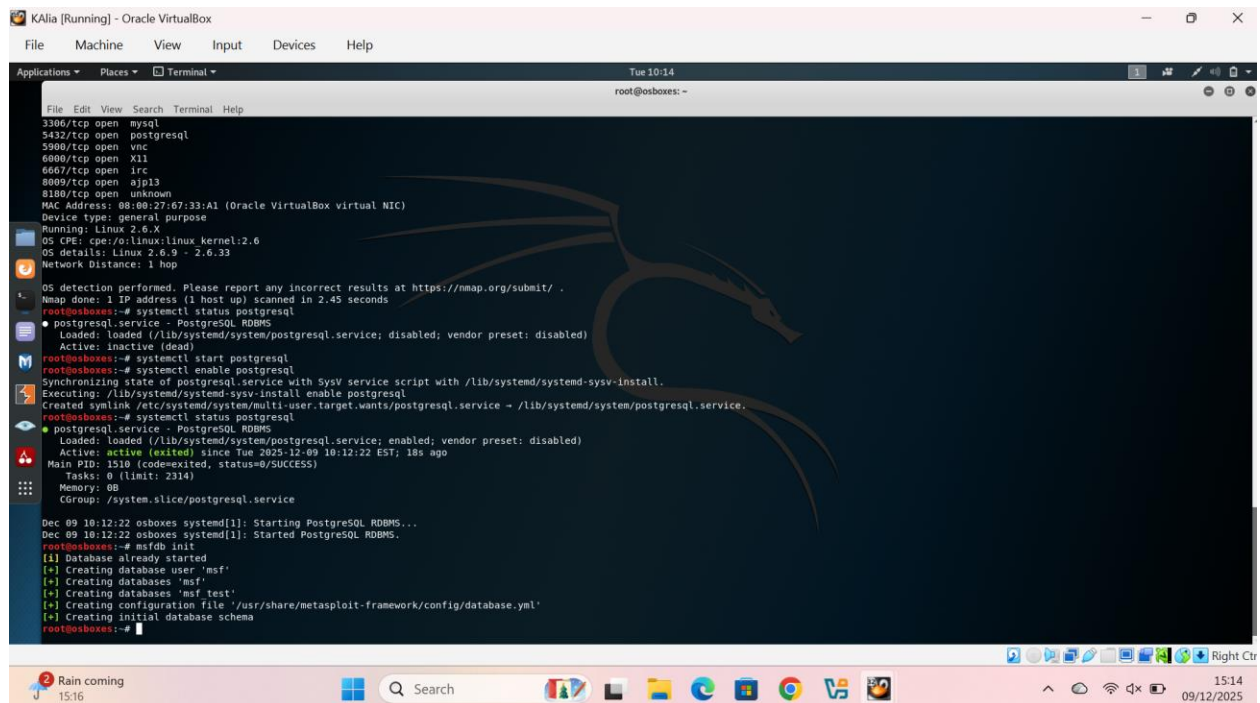
Dbmap –A for detail information for detail AD-RND where we get domain information



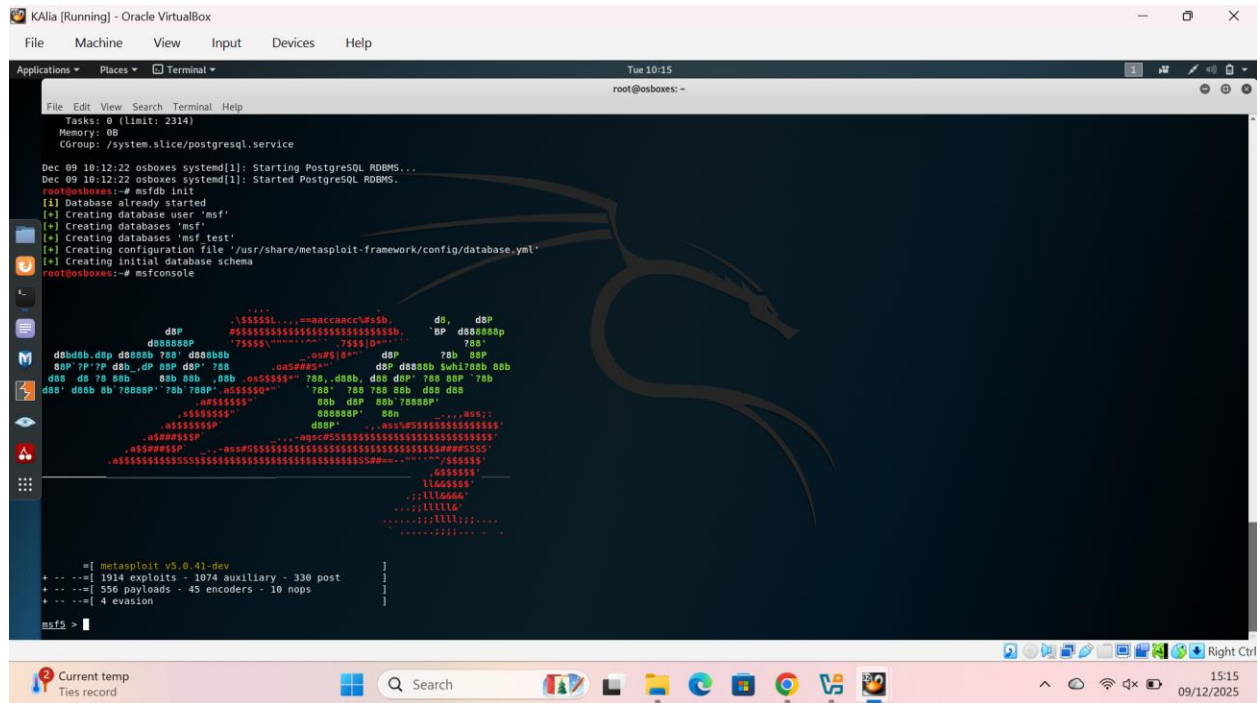
Metasploit 2- Kali to AWS



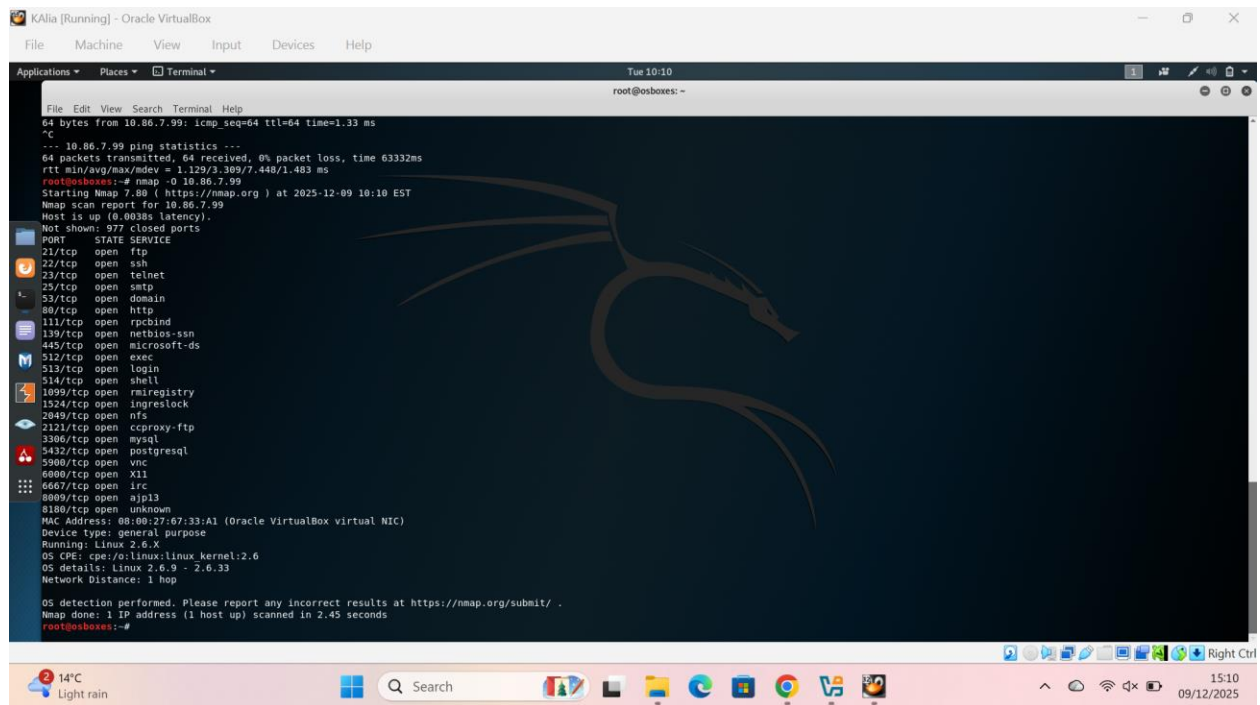
Creating Database



Starting NSF Control



Scanning for AWSVPC



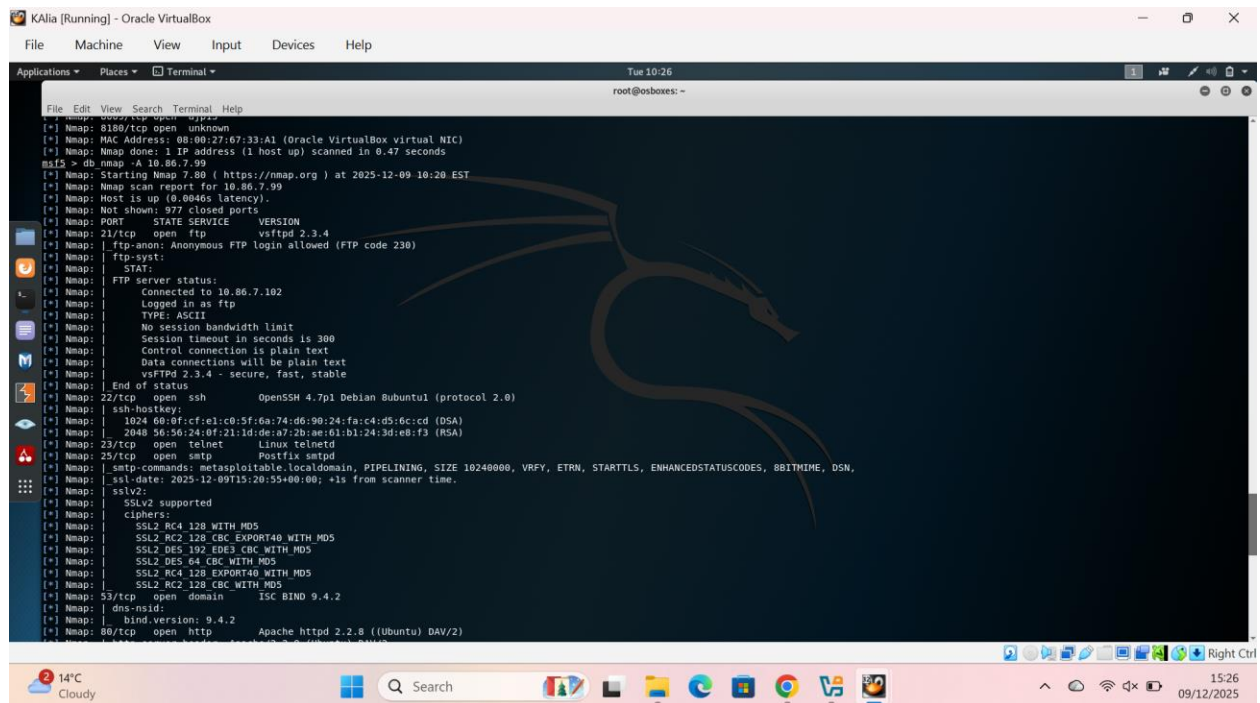
Used path of Axillary

```
root@osboxes: /usr/share/metasploit-framework/modules/auxiliary/scanner
File Edit View Search Terminal Help
root@osboxes:~# cd /usr/share/metasploit-framework/modules/auxiliary/
root@osboxes: /usr/share/metasploit-framework/modules/auxiliary# ls -l
total 84
drwxr-xr-x 45 root root 4096 Sep 3 2019 admin
drwxr-xr-x 2 root root 4096 Sep 3 2019 analyze
drwxr-xr-x 2 root root 4096 Sep 3 2019 bnat
drwxr-xr-x 7 root root 4096 Sep 3 2019 client
drwxr-xr-x 3 root root 4096 Sep 3 2019 cloud
drwxr-xr-x 2 root root 4096 Sep 3 2019 crawler
drwxr-xr-x 2 root root 4096 Sep 3 2019 ddrpc
drwxr-xr-x 27 root root 4096 Sep 3 2019 dos
drwxr-xr-x 1 root root 1217 Aug 15 2019 example.rb
drwxr-xr-x 2 root root 4096 Sep 3 2019 fileformat
drwxr-xr-x 10 root root 4096 Sep 3 2019 fuzzers
drwxr-xr-x 2 root root 4096 Sep 3 2019 gather
drwxr-xr-x 2 root root 4096 Sep 3 2019 parser
drwxr-xr-x 3 root root 4096 Sep 3 2019 pdf
drwxr-xr-x 86 root root 4096 Sep 3 2019 scanner
drwxr-xr-x 4 root root 4096 Sep 3 2019 server
drwxr-xr-x 2 root root 4096 Sep 3 2019 sniffer
drwxr-xr-x 9 root root 4096 Sep 3 2019 spoof
drwxr-xr-x 3 root root 4096 Sep 3 2019 sqlmap
drwxr-xr-x 2 root root 4096 Sep 3 2019 voip
drwxr-xr-x 5 root root 4096 Sep 3 2019 vsploit
```

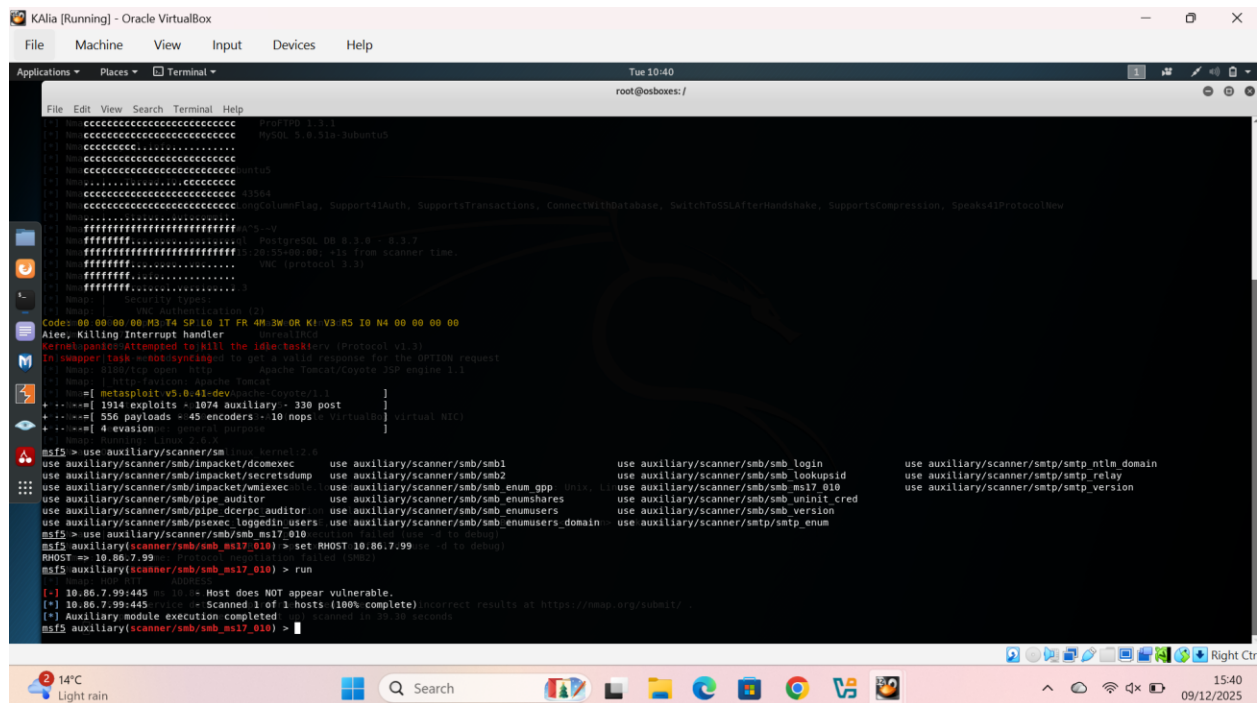
File details of scanner

```
root@osboxes: /usr/share/metasploit-framework/modules/auxiliary/scanner
File Edit View Search Terminal Help
root@osboxes:~# cd /usr/share/metasploit-framework/modules/auxiliary/scanner/
root@osboxes: /usr/share/metasploit-framework/modules/auxiliary/scanner# ls -l
total 348
drwxr-xr-x 2 root root 4096 Sep 3 2019 acpp
drwxr-xr-x 2 root root 4096 Sep 3 2019 backdoor
drwxr-xr-x 2 root root 4096 Sep 3 2019 chargen
drwxr-xr-x 2 root root 4096 Sep 3 2019 couchdb
drwxr-xr-x 2 root root 4096 Sep 3 2019 db2
drwxr-xr-x 2 root root 4096 Sep 3 2019 ddrpc
drwxr-xr-x 2 root root 4096 Sep 3 2019 dect
drwxr-xr-x 2 root root 4096 Sep 3 2019 discovery
drwxr-xr-x 2 root root 4096 Sep 3 2019 dlsw
drwxr-xr-x 2 root root 4096 Sep 3 2019 dos
drwxr-xr-x 2 root root 4096 Sep 3 2019 elasticsearch
drwxr-xr-x 2 root root 4096 Sep 3 2019 emc
drwxr-xr-x 2 root root 4096 Sep 3 2019 etcd
drwxr-xr-x 2 root root 4096 Sep 3 2019 finger
drwxr-xr-x 2 root root 4096 Sep 3 2019 ftp
drwxr-xr-x 2 root root 4096 Sep 3 2019 gopher
drwxr-xr-x 2 root root 4096 Sep 3 2019 gprs
drwxr-xr-x 2 root root 4096 Sep 3 2019 h323
drwxr-xr-x 2 root root 16384 Sep 3 2019 http
drwxr-xr-x 2 root root 4096 Sep 3 2019 ike
drwxr-xr-x 2 root root 4096 Sep 3 2019 inap
drwxr-xr-x 2 root root 4096 Sep 3 2019 ip
drwxr-xr-x 2 root root 4096 Sep 3 2019 ipmi
drwxr-xr-x 2 root root 4096 Sep 3 2019 jenkins
drwxr-xr-x 2 root root 4096 Sep 3 2019 kadmalia
drwxr-xr-x 2 root root 4096 Sep 3 2019 llmar
drwxr-xr-x 2 root root 4096 Sep 3 2019 lotus
drwxr-xr-x 2 root root 4096 Sep 3 2019 mdns
drwxr-xr-x 2 root root 4096 Sep 3 2019 memcached
drwxr-xr-x 2 root root 4096 Sep 3 2019 misc
drwxr-xr-x 2 root root 4096 Sep 3 2019 mongodb
drwxr-xr-x 2 root root 4096 Sep 3 2019 motorola
drwxr-xr-x 2 root root 4096 Sep 3 2019 mqtt
drwxr-xr-x 2 root root 4096 Sep 3 2019 msf
drwxr-xr-x 3 root root 4096 Sep 3 2019 msfconsole
drwxr-xr-x 2 root root 4096 Sep 3 2019 mysql
drwxr-xr-x 2 root root 4096 Sep 3 2019 nmap
```

Aggressive scanning of VPC



Set Remote Host



Setting Data Address 1

```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Applications Places Terminal
Tue 11:00
root@osboxes: /

File Edit View Search Terminal Help
RHOST => 10.86.7.99
msf5 auxiliary(scanner/scada/modbusclient) > show options
Module options (auxiliary/scanner/scada/modbusclient):
-----
Name      Current Setting  Required  Description
-----
DATA      new_capability?  false     Data to write (WRITE_COIL and WRITE_REGISTER modes only) See: SwitchToSLLAfterHandshake, SupportsCompression, Supports41ProtocolNew
DATA_ADDRESS  write_automatic? yes         Modbus data address
DATA_COILS  011             no        Data in binary to write (WRITE_COILS mode only) e.g. 0110
DATA_REGISTERS new_postgresql?  false     Words to write to each register separated with a comma (WRITE_REGISTERS mode only) e.g. 1,2,3,4
NUMBER      11             no        Number of coils/registers to read (READ_COILS and READ_REGISTERS modes only)
RHOSTS      10.86.7.99      yes       The target address range or CIDR identifier
RPORT       502             yes       The target port (TCP)
UNIT_NUMBER  1              no        Modbus unit number

Auxiliary action: new_xll
-----
Name      Description
-----
00007100  Apache Jkry (Protocol v1.3)
-----
READ_REGISTERS Read words from several registers: JSP engine 1.1
Name      HTTP-Function: Apache Tomcat
Name      HTTP-Function: Apache Tomcat

msf5 auxiliary(scanner/scada/modbusclient) > set data address 10.86.7.99
data address => 10.86.7.99
msf5 auxiliary(scanner/scada/modbusclient) > set data address 1
data address => 1
msf5 auxiliary(scanner/scada/modbusclient) > exploit
[*] Running module against 10.86.7.99

[*] 10.86.7.99:502 - Auxiliary failed: Rex::ConnectionRefused The connection was refused by the remote host (10.86.7.99:502).
[*] 10.86.7.99:502 - Call stack:
[*] 10.86.7.99:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/rx-socket-0.1.17/lib/rx/socket/comm/local.rb:298:in 'rescue in create_by_type'
[*] 10.86.7.99:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/rx-socket-0.1.17/lib/rx/socket/comm/local.rb:263:in 'create_by_type'
[*] 10.86.7.99:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/rx-socket-0.1.17/lib/rx/socket/comm/local.rb:33:in 'create'
[*] 10.86.7.99:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/rx-socket-0.1.17/lib/rx/socket.rb:49:in 'create_param'
[*] 10.86.7.99:502 - /usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/rx-socket-0.1.17/lib/rx/socket/tcp.rb:37:in 'create_param'
[*] 10.86.7.99:502 - /usr/share/metasploit-framework/lib/msf/core/exploit/tcp.rb:106:in 'connect'
[*] 10.86.7.99:502 - /usr/share/metasploit-framework/modules/auxiliary/scanner/scada/modbusclient.rb:316:in 'run'
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/scada/modbusclient) >
```

Evidence of success-

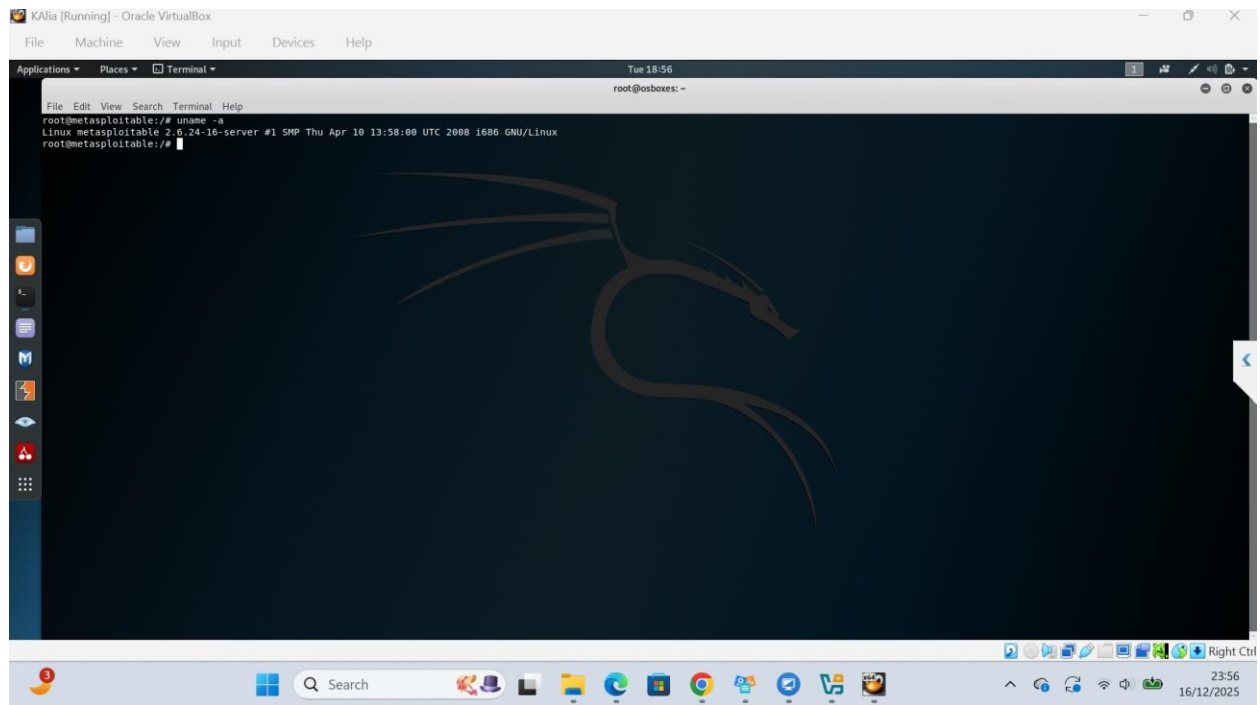
Netcat -success

```
root@osboxes:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.86.7.31 netmask 255.255.255.0 broadcast 10.86.7.255
    inet6 fe80::a00:27ff:feb4:b3ce prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b4:b3:ce txqueuelen 1000 (Ethernet)
    RX packets 151 bytes 21104 (20.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 3024 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

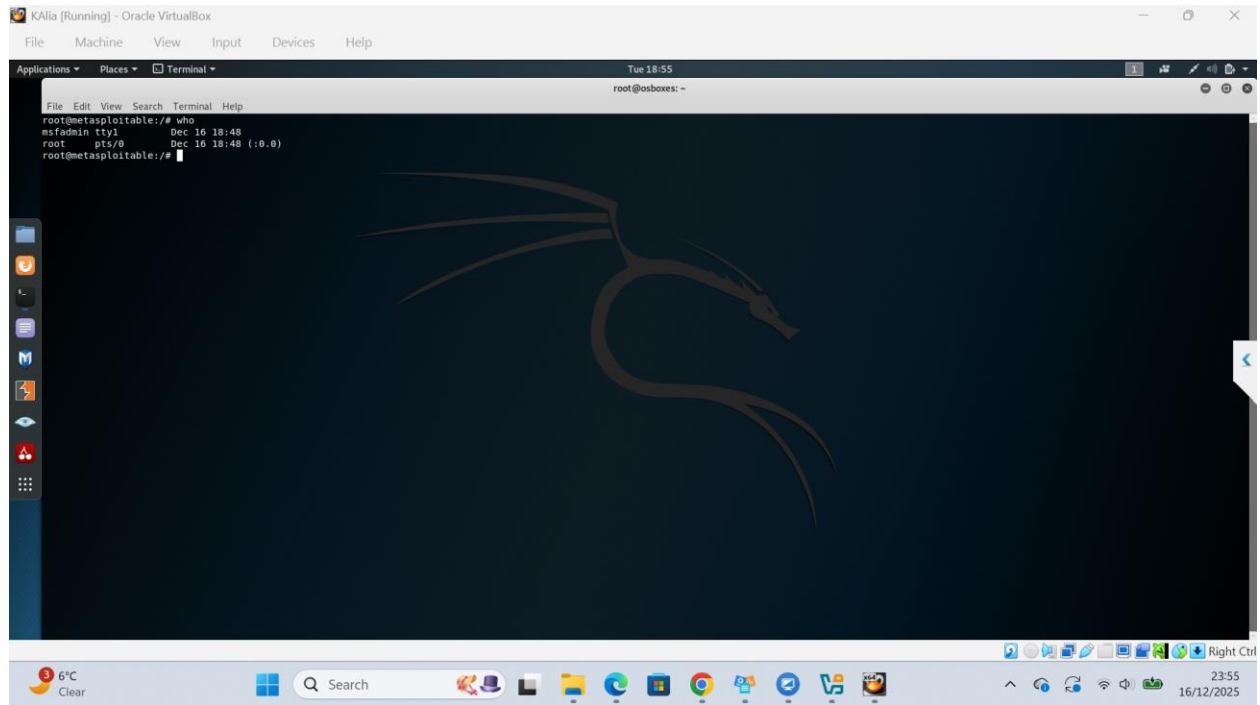
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 102 bytes 32009 (31.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 102 bytes 32009 (31.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@osboxes:~# ping 10.86.7.99
PING 10.86.7.99 (10.86.7.99) 56(84) bytes of data:
64 bytes from 10.86.7.99: icmp_seq=1 ttl=64 time=2.11 ms
64 bytes from 10.86.7.99: icmp_seq=2 ttl=64 time=1.37 ms
^C
--- 10.86.7.99 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 1.373/1.741/2.110/0.368 ms
root@osboxes:~# nc 10.86.7.99 1524
root@metasploitable:~#
```

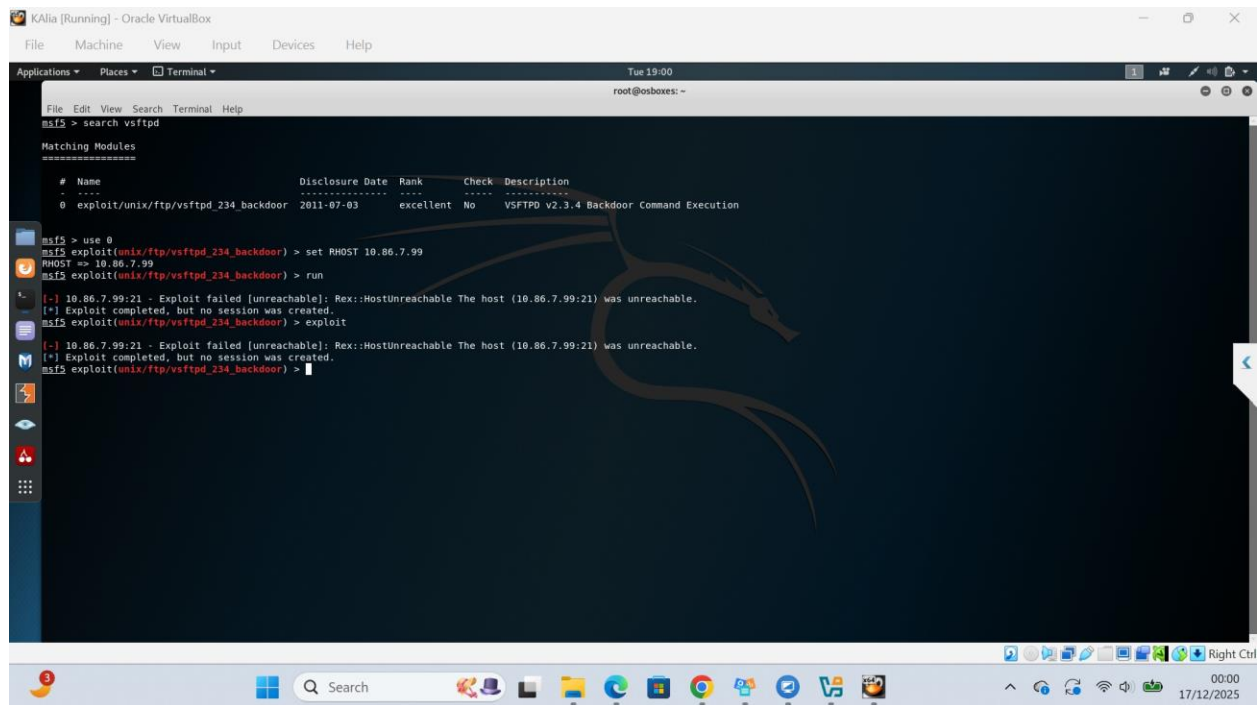
Kernal check



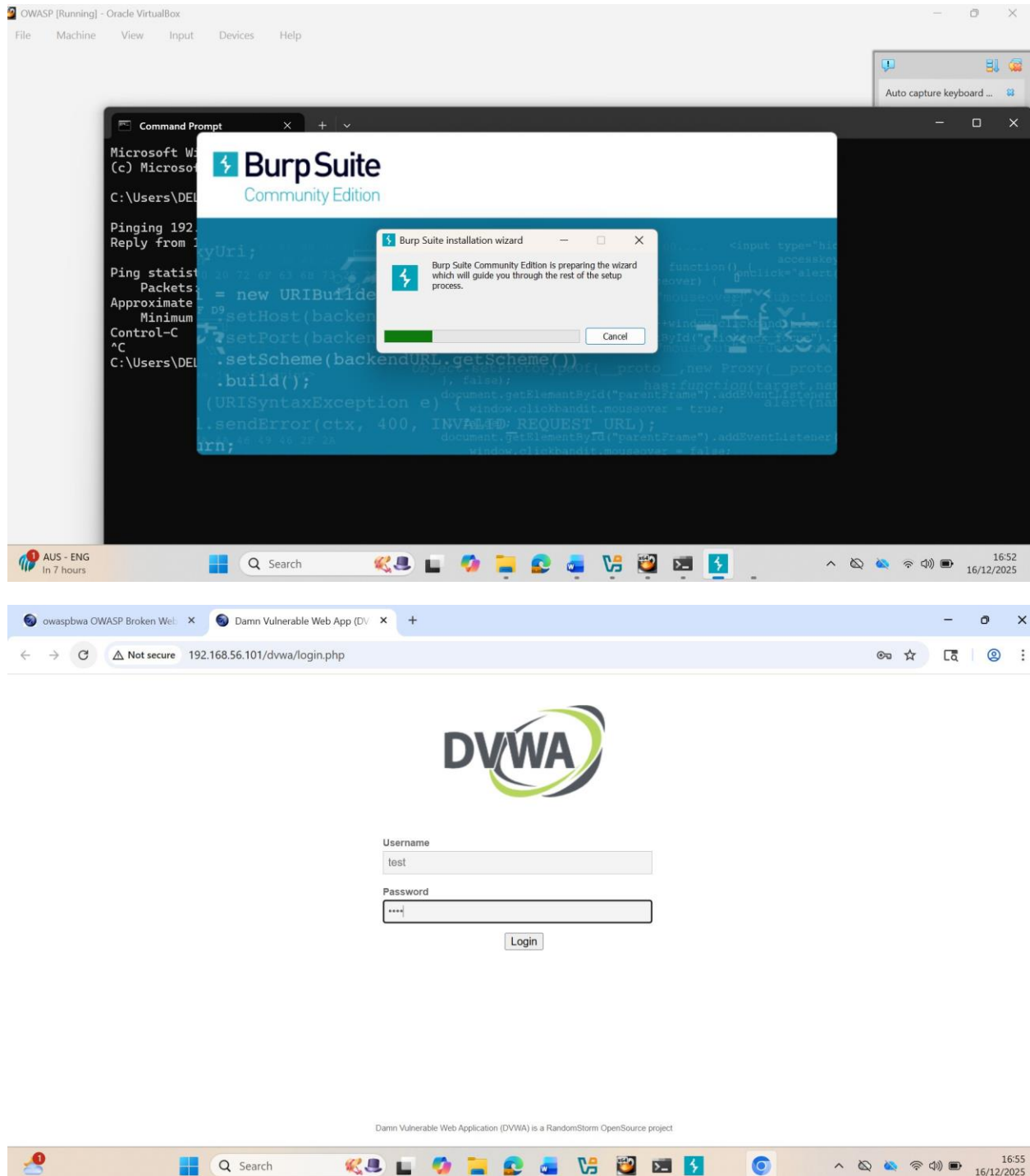
Root Verification



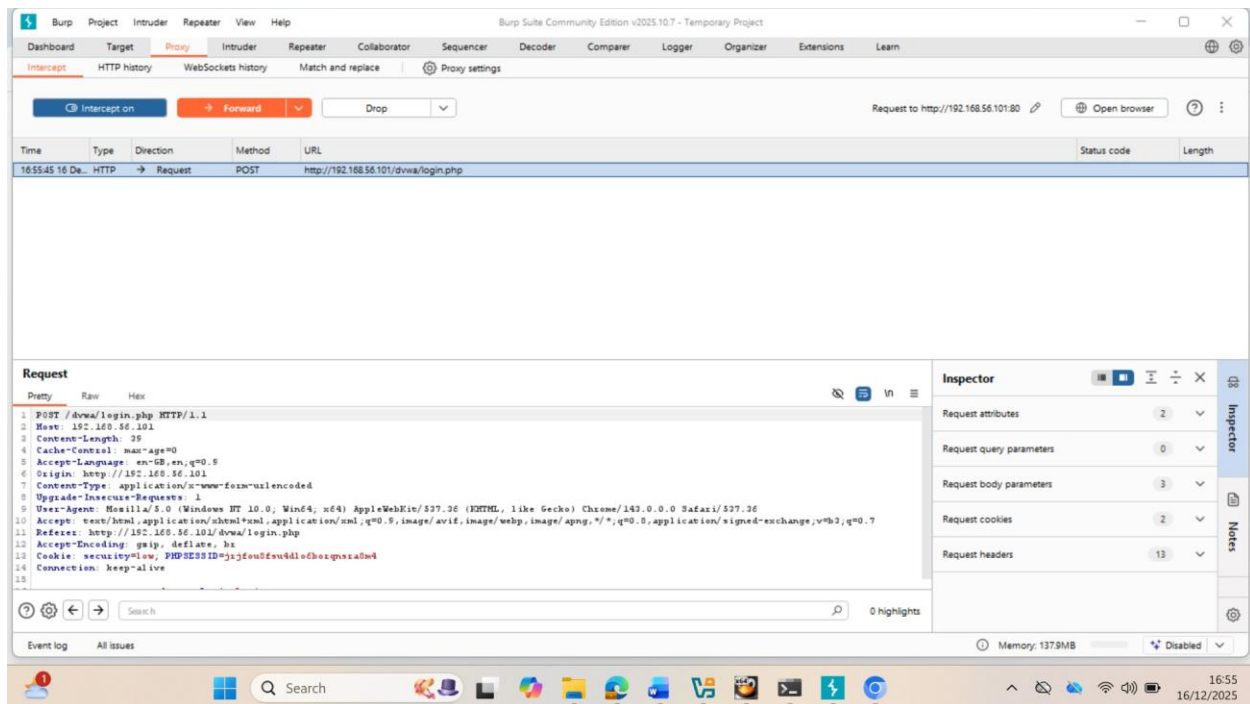
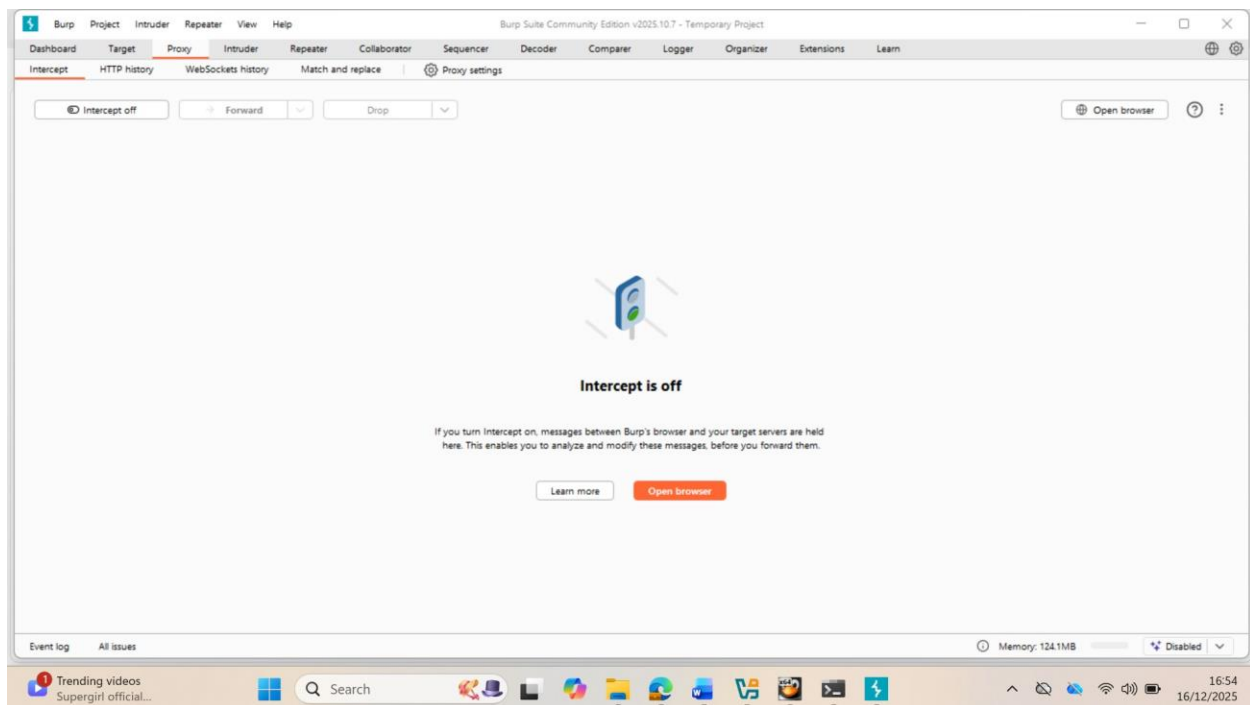
Exploiting VSFTPD

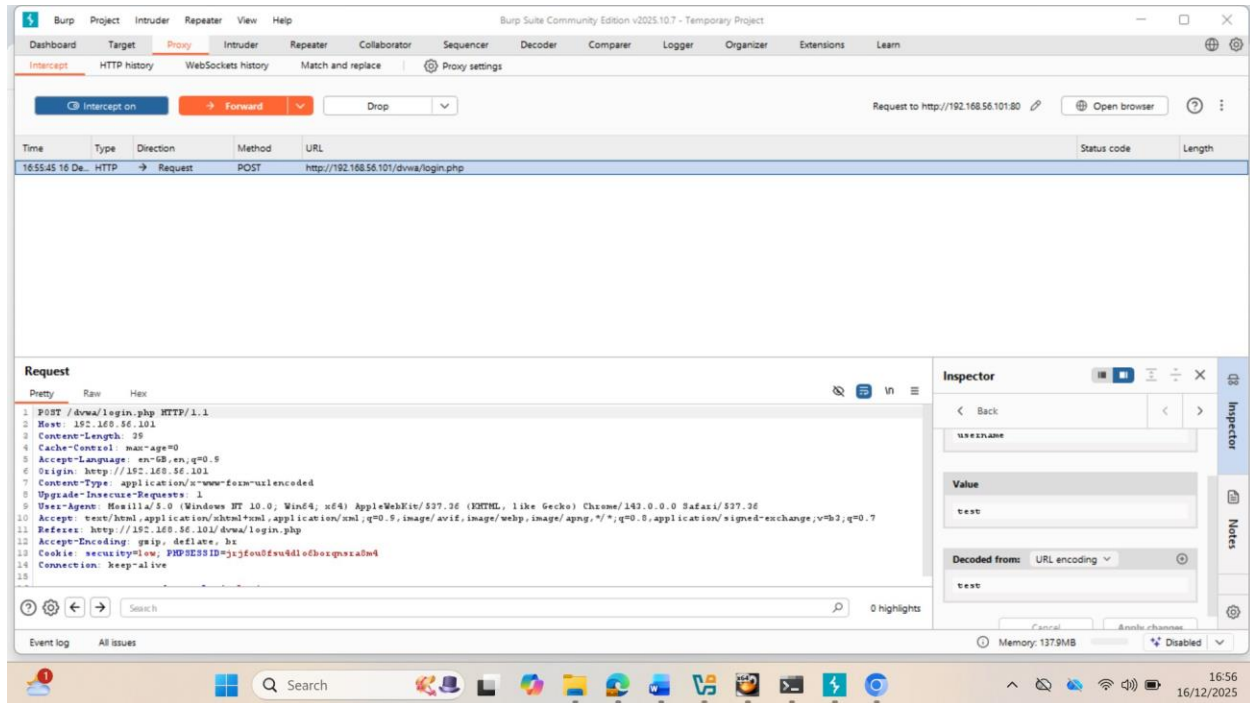


Burp suite-



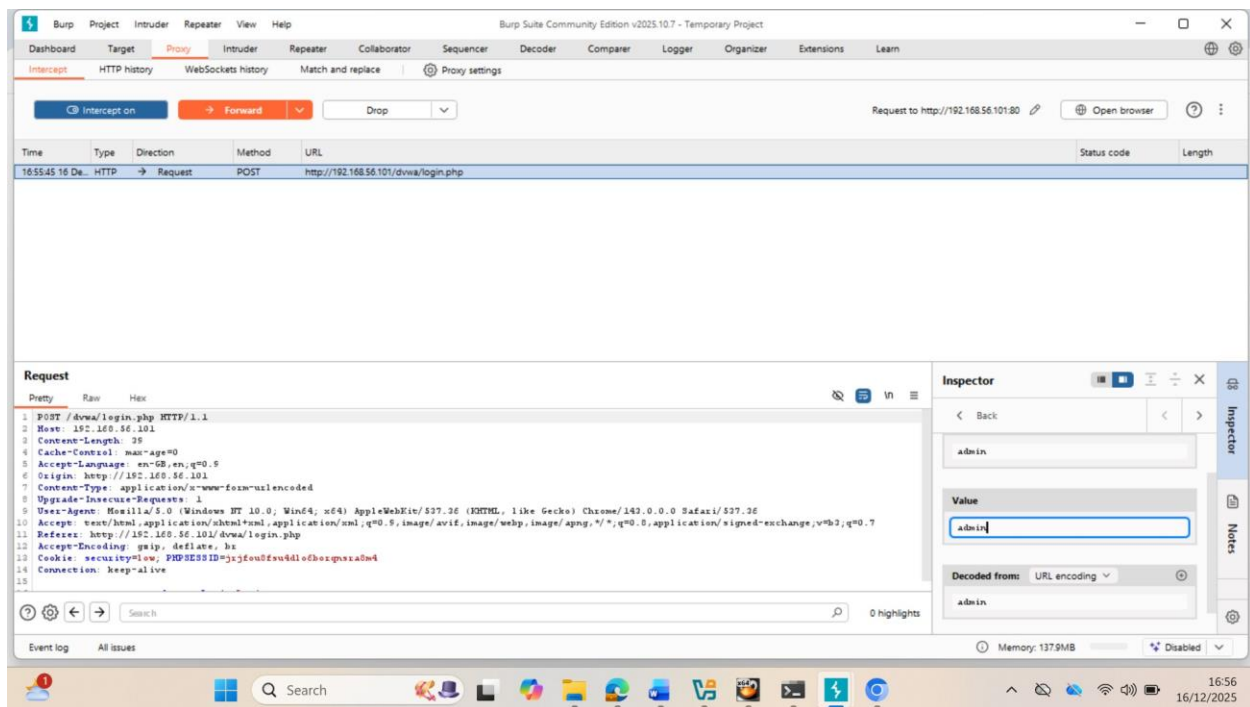
Browse the target page, here target page is DVWA of CI/CD webserver.



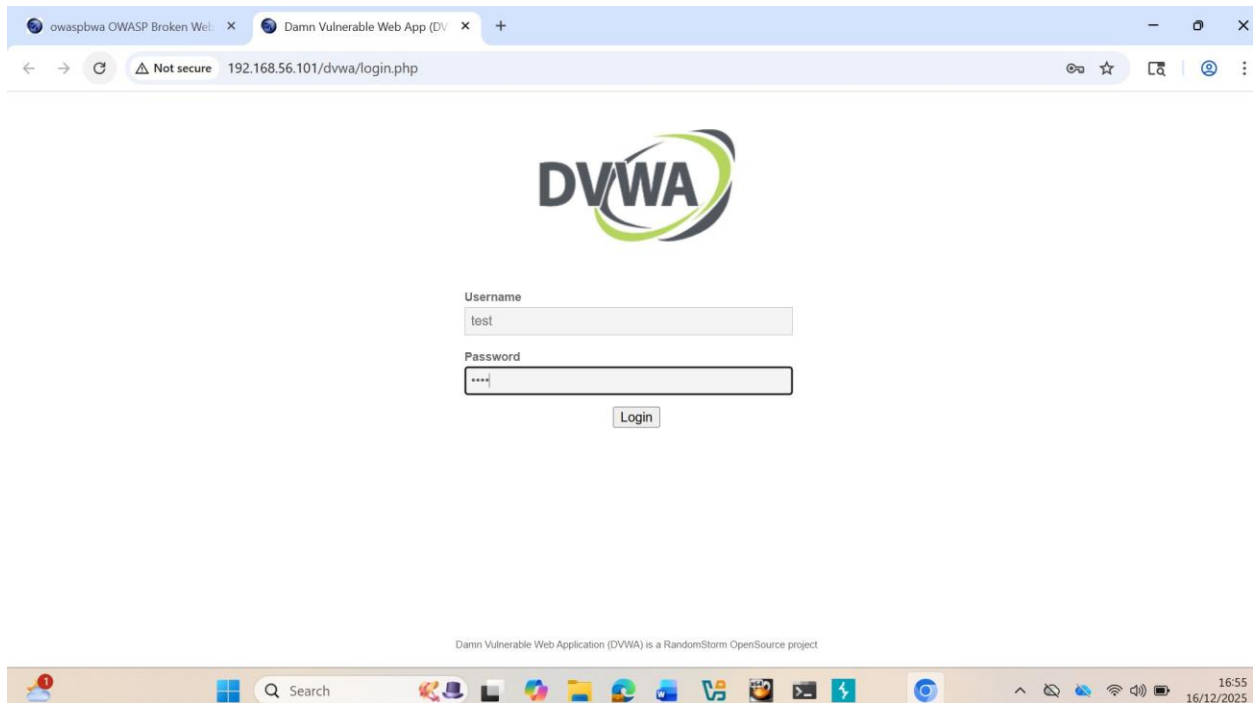


Burp suit capture the session and here is it observed that user put username test password test.

Change the username and password to admin admin



Browser and trying to login through provided credentials.



6. Technical Report for the Blue Team

Defensive perspective on Operation IP Shield is presented in this section. It talks about what happened from the perspective of the defender, rather than diving in depth into attacker techniques and highlights where current controls did not work. The goal is to help CPC's blue team carry out more effective detection and incident response and long-term resilience efforts.

6.1 Executive Summary for Blue Team

Through the engagement, the red team was able to successfully infiltrate CPC's hybrid environment and bypass existing security controls without detection alerts. The Organizations were initially compromised via a phishing campaign, followed by the threat actors obtaining persistent access to the victim environment, elevating privileges and moving laterally in the internal network.

Following this, the R&D file server and cloud-based assets hosted in AWS were accessed. We stole sensitive research data and configuration files and managed to exfiltrate this secret hoardacks despite systems from wellrespected companies. In no step of the kill chain endpoint detection, SIEM monitoring, or AWS CloudTrail raised any actionable alerts.

6.2 Key Weaknesses Identified

Several recurring issues contributed to the success of the attack:

1. **Phishing defences were insufficient.**
Email filtering was outdated and multi-factor authentication was not enforced, allowing stolen credentials to be used directly.
2. **Excessive privilege exposure on endpoints.**
Cached local administrator tokens in memory enabled attackers to escalate privileges without exploiting the kernel.
3. **Endpoint Detection and Response gaps.**
Some workstations were running outdated EDR agents, limiting visibility into process injection and abnormal PowerShell usage.
4. **Lack of internal network segmentation.**
The corporate LAN and R&D VLAN were not adequately separated, allowing lateral movement once administrative access was obtained.
5. **Poor cloud credential hygiene.**
AWS credentials were stored in plain text on a developer workstation, providing unnecessary access to cloud resources.
6. **CI/CD security misconfigurations.**
The GitHub Actions runner exposed sensitive configuration details and lacked proper secret protection.
7. **Insufficient command-and-control monitoring.**
Network traffic resembling C2 communication was not flagged or investigated.
8. **DNS traffic not inspected.**
This allowed data exfiltration over DNS without detection, despite its known use in advanced attacks.

Summary

On the whole, the exercise demonstrated that CPC's defences are more successful at thwarting noisier or opportunistic attacks than against slow and methodical intrusions. Better visibility,

more stringent access controls and increased monitoring of activities across endpoints, networks and cloud services could have gone a long way toward reducing the likelihood that an equivalent breach would occur in a real-world environment.

7. Executive Brief for the CPC Board

CPC's current cybersecurity posture allows a determined attacker to steal high-value research without being noticed. The red team was able to imitate a hostile competitor and extract dummy drug-development data.

The main business risks identified are:

- Loss of competitive advantage
- Damage to company reputation
- Regulatory penalties
- Loss of investor confidence
- Delays in clinical trial approval

Investing in improved authentication, segmentation, monitoring, and cloud security controls will significantly reduce these risks and protect CPC's intellectual property.

8. Detection Gap Analysis

Failure Point	Missing Control	Consequence
Phishing bypass	No MFA + weak filtering	Easy entry
EDR outdated	No memory scanning	Beacon injection undetected
Credential theft	LSASS unprotected	Domain escalation possible
Lateral movement	No segmentation	R&D server compromised
Cloud access	Poor IAM hygiene	S3 bucket readable
DNS exfiltration	No DNS logging	Stealthy data loss

9. Strategic Recommendations

A. Identity & Access Security

- Deploy **phishing-resistant MFA** (FIDO2/WebAuthn).
- Disable legacy authentication protocols.
- Enforce password vaulting for AWS credentials.

Phishing-resistant multi-factor authentication, such as FIDO2 or WebAuthn, should be deployed across all user and administrative accounts. Legacy authentication protocols should be disabled, and cloud credentials must be stored securely using managed password vaults rather than local files.

B. Endpoint Security

- Upgrade EDR with memory protection.
- Prevent LSASS dumps using Credential Guard.
- Enforce application control and script restrictions.

Endpoint protection should be upgraded to include memory protection and behavioural analysis. Features such as Windows Credential Guard should be enabled to prevent LSASS dumping, and application control policies should be enforced to limit unauthorised script execution.

C. Network Security

- Implement **micro-segmentation** between corporate and R&D.
- Deploy DNS inspection and anomaly detection.
- SIEM correlation for lateral movement-related events.

Micro-segmentation should be implemented to isolate sensitive R&D systems from the corporate network. DNS traffic should be inspected for anomalies, and SIEM rules should be refined to detect patterns associated with lateral movement and privilege escalation.

E. CI/CD Pipeline Security

- Protect GitHub secrets with encrypted storage.
- Require signed commits.
- Restrict runner permissions.

Secrets used within CI/CD pipelines must be stored securely using encrypted mechanisms. Commit signing should be enforced, and GitHub Actions runners should be restricted to only the permissions required for their tasks.

10. Cost–Benefit Analysis

This section evaluates whether the proposed security controls are financially justified. The analysis compares the **estimated cost of implementation** against the **potential financial losses avoided** if a serious cyber incident were prevented. Figures are based on published breach reports, ransomware impact studies, and real-world healthcare and pharmaceutical sector incidents.

10.1 Cost-Benefit Breakdown

Security Investment	Estimated Annual Cost	Financial Benefit / Avoided Loss
MFA & Advanced Email Security	£35,000	Prevents credential theft and phishing-led breaches (£2–3M IP loss avoided)
Updated Endpoint Detection & Response (EDR)	£60,000	Reduces ransomware risk and lateral movement (£5–12M avoided)
Network Micro-Segmentation	£75,000	Limits breach spread and system compromise (£4M+ avoided)
Cloud Security Hardening (AWS)	£30,000	Avoids GDPR penalties and cloud data breaches (£1–3M avoided)

Total Estimated Investment: ~£200,000 per year
Potential Avoided Losses: £10–15 million+

10.2 Mathematical Justification (ROI) Calculation

Industry reports consistently show that the **average cost of a data breach** in highly regulated sectors such as healthcare and pharmaceuticals exceeds **£4 million per incident**, with ransomware-driven attacks often exceeding **£10 million** when downtime, recovery, and reputational damage are included.

If CPC experiences **just one major breach over a 3–5 year period**, the return on investment (ROI) becomes clear:

- **Investment:**
£200,000 × 5 years = **£1,000,000**
- **Single avoided major breach:**
£10–15 million

Even under conservative assumptions:

$$ROI = \frac{£10,000,000 - £1,000,000}{£1,000,000} = 900\%$$

This demonstrates that the recommended controls are **economically justified**, even if they only prevent **one significant incident** over several years.

11. Conclusion

Operation IP Shield made it evident that Cureton Pharmaceutical Company was not yet fully ready to protect itself from a highly motivated, well-financed attacker using an APT model. And by using real-world tactics like targeted phishing and credential harvesting, lateral movement within the environment, abuse of cloud resources and low-noise data exfiltration, they were able to gain access to sensitive research data and exfiltrate it without detection from existing security controls.

The findings reinforce a number of key areas that companies need to address, including identity and access management, network segmentation, endpoint security strategy and cloud security monitoring. Yes, those things can be overcome separately but not when aligned such as they lay down a path for an adversary to complete that's relatively straight and easy. The case study illustrates that CPC's current security posture puts high-value intellectual property in jeopardy resulting in possible regulatory, financial, and reputational impacts.

It is very important to note that this engagement was not intended as a finger-pointing exercise, but rather, aimed at providing straightforward and useful feedback. The results reveal that meaningful enhancements — like phishing-resistant authentication, increased endpoint controls, improved visibility and tighter cloud governance — would dramatically drive up the cost and complexity of an actual attack. With these actions in place, CPC would be much more capable of finding, disrupting and responding to sophisticated threats well before severe harm is done.

In general, Operation IP Shield met its goal of depicting real attack paths and actually how an attacker could abuse it. Rectifying the identified weaknesses will not only improve CPC's cyber defences and protecting its research assets, public reputation and long-term operational resilience.

Reference List

1. MITRE Corporation, *MITRE ATT&CK® Framework: Enterprise Matrix*, 2024. [Online]. Available: <https://attack.mitre.org>. Accessed: Dec. 12, 2025.
2. National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5. Gaithersburg, MD, USA: NIST, 2020.
3. Lockheed Martin, *Cyber Kill Chain® Overview*, 2023. [Online]. Available: <https://www.lockheedmartin.com>. Accessed: Dec. 11, 2025.
4. OWASP Foundation, *OWASP Top 10 Web Application Security Risks – 2021*, 2021. [Online]. Available: <https://owasp.org>. Accessed: Dec. 10, 2025.
5. S. U. Khan and T. Alshammari, “A systematic review of red teaming methodologies and adversarial simulation,” *Journal of Cybersecurity*, vol. 9, pp. 1–15, 2023.
6. European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024*, Athens, Greece, 2024.
7. C. Payne, “Effective use of MITRE ATT&CK in building red team playbooks,” *Computers & Security*, vol. 126, pp. 102–118, 2024.
8. National Institute of Standards and Technology (NIST), *Technical Guide to Information Security Testing and Assessment*, NIST SP 800-115. Gaithersburg, MD, USA: NIST, 2022.
9. A. Winterfield and J. Andress, *The Basics of Cyber Warfare: Understanding Global Cyber Conflict*, 2nd ed. Oxford, U.K.: Syngress, 2020.
10. Elastic Security, *Detection Engineering: Best Practices for Building Effective SIEM Rules*, 2024. [Online]. Available: <https://www.elastic.co>. Accessed: Dec. 13, 2025.

11. S. Doraisamy, “The evolving role of purple teaming in enterprise cyber defence,” *International Journal of Information Security Research*, vol. 15, no. 3, pp. 55–70, 2024.
12. Cybersecurity and Infrastructure Security Agency (CISA), *Threat Emulation and Adversary Simulation Guidance*. Washington, DC, USA: CISA, 2024.
13. Rapid7 Labs, *Penetration Testing Methodologies: Updated Framework*, 2024. [Online]. Available: <https://www.rapid7.com>. Accessed: Dec. 9, 2025.
14. [15] A. Geers, *Strategic Cyber Deterrence and Adversarial Models*. Tallinn, Estonia: NATO CCDCOE Publications, 2023.