



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

ACCA7033 LON ASSESSMENT

Ethical Hacking

Habibur Rahman | 2428138

To

Dr Mohamed Ghanem

Submission Date: 17/12/2025

Table of Contents

List of Tables	3
Table of Figures, Diagrams	3
1 Abstract	5
2 Introduction	5
3 Literature Review	5
4 Task 1	5
4.1 Case Selection	5
4.2 Executive Summary of Case	5
4.3 Case Incident Timeline	6
4.4 MITRE ATT&CK Enterprise Mapping of Adversary TTPs	6
4.5 Root-Cause Analysis (Technical, Architectural, Human factors)	7
4.5.1 Human factors	7
4.5.2 Architectural/technical debt	7
4.5.3 Backup/BCP issues	7
4.5.4 Threat tactics	8
4.5.5 Monitoring gaps	8
4.5.6 Public health implications	8
4.6 Strategic Recommendations	8
4.6.1 Prevention	8
4.6.2 Architecture	8
4.6.3 Detection	8
4.6.4 Rate the Threats	9
4.6.5 Governance & Policy	10
5 Discussion	10
6 Task 2	10
6.1 Operation IP Shield – Red Team Engagement	10
6.1.1 Campaign Design	10
6.1.2 Environment & Execution	12
6.1.3 Reporting & Analysis	53
7 Conclusion	54
8 References	54

List of Tables

Table 1:TTPs Mappings	7
Table 2: DREAD Threat Modeling.....	9

Table of Figures, Diagrams

Figure 1: Attack Lifestyle process	6
Figure 2: Campaign Design with Environmental Process	11
Figure 3: Emulation Narrative	12
Figure 5: Installation process of Kali - 1	13
Figure 6: Installation process of Kali - 2	14
Figure 7: Installation process of Kali - 3	14
Figure 8: Installation process of Kali - 4	15
Figure 9: Installation process of AWS VPC - 1	16
Figure 10: Installation process of AWS VPC - 2	16
Figure 11: Installation process of AWS VPC - 3	17
Figure 12: Installation process of AWS VPC - 4	17
Figure 13: Installation process of CI-CD - 1	18
Figure 14: Installation process of CI-CD - 2	18
Figure 15: Installation Process of CI-CD - 3	19
Figure 16: Installation Process of CI-CD - 4	19
Figure 17: Installation process of R&D - 1	20
Figure 18: Installation process of R&D - 2	20
Figure 19: Installation process of R&D - 3	21
Figure 20: Installation process of R&D - 4	21
Figure 21: The whole environment	22
Figure 22: Ping test from Kali to AWS VPC process	23
Figure 23: Nmap from Kali to AWS VPC	23
Figure 24: Db_nmap from Kali to AWS VPC	24
Figure 25: Db_nmap -sV Command from Kali to AWS VPC	25
Figure 26: Db_nmap -A Command from Kali to AWS VPC 1	25
Figure 27: Db_nmap -A Command from Kali to AWS VPC 2	26
Figure 28: Db_nmap -A command from Kali to AWS VPC 3	26
Figure 29: Search ftpd from Kali to AWS VPC	27
Figure 30: Exploiting a vulnerable Proftpd service from Kali to AWS VPC	27
Figure 31: Evasion techniques from Kali to AWS VPC	28
Figure 32: HTTP Header Test and Evasion from Kali to AWS VPC	28
Figure 33: Payload Configuration and Exploitation from Kali to AWS VPC	29
Figure 35: Netcat connection and system verification from Kali to AWS VPC	29
Figure 36: Ping test from Kali to R&D AD	30
Figure 37: Operating system detection scan from Kali to Active Directory	31
Figure 38: Metasploit console access from Kali to R&D AD	31
Figure 39: Host discovery scan from Kali to R&D AD	32

Figure 40: Database service scan using db_nmap from Kali to R&D AD	32
Figure 41: DNS service enumeration using db_nmap from Kali to R&D AD	33
Figure 42: Aggressive database and service scan using db_nmap from Kali to R&D AD 1	33
Figure 43: Aggressive database and service scan using db_nmap from Kali to R&D AD 2	34
Figure 44: Ping test from Kali to CI-CD	35
Figure 45: Operating system detection scan from Kali to CI-CD	35
Figure 46: Web traffic inspection using Burp Suite - 1	36
Figure 47: Web traffic inspection using Burp Suite - 2	36
Figure 48: Web traffic inspection using Burp Suite - 3	37
Figure 49: Web traffic inspection using Burp Suite - 4	37
Figure 50: Web traffic inspection using Burp Suite - 5	38
Figure 51: Web traffic inspection using Burp Suite - 6	38
Figure 52: Web traffic inspection using Burp Suite - 7	39
Figure 53: Web traffic inspection using Burp Suite - 8	39
Figure 54: SQL injection vulnerability in database query	40
Figure 55: SQL injection vulnerability in database query - 2	40
Figure 56: SQL injection enabling authentication bypass	41
Figure 57: SQL injection enabling authentication bypass - 2	41
Figure 58: Cross-site scripting vulnerability	42
Figure 59: Cross-site scripting vulnerability - 2	42
Figure 60: Cross-site scripting vulnerability - 3	43
Figure 61: Cross-site scripting vulnerability - 4	43
Figure 62: All scan overview in Nessus	44
Figure 63: Nessus scan results for AWS VPC resources - 1	44
Figure 64: Nessus scan results for AWS VPC resources - 2	45
Figure 65: Nessus scan results for AWS VPC resources - 3	45
Figure 66: Nessus scan results for AWS VPC resources - 4	46
Figure 67: Nessus scan results for AWS VPC resources - 5	46
Figure 68: Nessus scan results for AWS VPC resources - 6	47
Figure 69: Nessus scan results for CI-CD resources - 1	47
Figure 70: Nessus scan results for CI-CD resources - 2	48
Figure 71: Nessus scan results for CI-CD resources - 3	48
Figure 72: Nessus scan results for CI-CD resources - 4	49
Figure 73: Nessus scan results for CI-CD resources - 5	49
Figure 74: Nessus scan results for CI-CD resources - 6	50
Figure 75: Nessus scan results for R&D AD resources - 1	51
Figure 76: Nessus scan results for R&D AD resources - 2	51
Figure 77: Nessus scan results for R&D AD resources - 3	52
Figure 78: Nessus scan results for R&D AD resources - 4	52

1 Abstract

This report examines the evolution of offensive security from traditional penetration testing to advanced practices such as Adversary Emulation and Red Team operations. By analyzing a recent major cyber incident, the study identifies attacker tactics and applies these insights to design a realistic red team engagement on a simulated corporate network. The objective is to move beyond vulnerability identification and demonstrate how advanced threats operate, while providing actionable strategies to strengthen organizational security and reduce business risks.

2 Introduction

Robust cybersecurity measures are essential in today's digital world, with sophisticated attacks [1] . Right now, Penetration testing and vulnerability assessment are vital for identifying and addressing security threats in business networks, systems, and online applications [1] [2]. Vulnerability assessment selects and finds security flaws using both automatic and human-based techniques to disclose vulnerabilities before attackers do [1] [2]. Penetration testing, on the other hand, aims to take advantage of these vulnerabilities to examine how successfully security measures prevent unwanted access [1] [2]. Vulnerability assessment and penetration testing both aim to identify and address security vulnerabilities, but they do so in different ways. Vulnerability assessment focuses on finding potential weaknesses; on the other hand, penetration testing tries to target such faults in a controlled setting [2] . These techniques are very important for maintaining the security of an organization's computer systems, networks, and applications. They are regularly employed as part of a full security testing and assessment program [2].

3 Literature Review

This paper focuses on two tasks. Firstly, it examines a recent major cyberattack to understand how and why it happened. Then, secondly, based on incident requirements, it simulates a realistic red team exercise, which is to act like a highly skilled hacker and try to break into CPC's systems, just like a real advanced persistent threat (APT) would, to see how strong their security really is.

4 Task 1

Here will be discussed a detailed examination of a single, sophisticated, and recent cybersecurity attack.

4.1 Case Selection

The National Health Laboratory Service (NHLS) in South Africa was the target of a ransomware attack in June 2024, which is an important cyber incident in the African healthcare sector [3]. Many patients in the nation, between 80 to 85 percent, are supported by the NHLS, which is basically the foundation of public diagnostic services. As a result, its impact affected hospitals and clinics across the country [3].

4.2 Executive Summary of Case

A ransomware attack on 22nd June 2024 caused NHLS to lose access to key laboratory IT systems, interfere with laboratory information system (LIS) communications, and delete portions of production and backup infrastructure [3][4]. As a result, urgent results need to be communicated over the phone and contribute to large test backlogs across public facilities [3] [4]. Official statements highlighted "no patient data lost" while accepting severe operational losses and the need to repair systems [3] [4] . After testimony and media reports linked initial access to phishing and accused the

BlackSuit extortion outfit as the culprit [3] [4]. The BlackSuit (Royal) ransomware group later claimed responsibility and asserted exfiltration of approximately 1.2 TB of data [3][4].

4.3 Case Incident Timeline

- **22–26 Jun 2024:** If NHLS detects a ransomware compromise, systems are shut down to limit further harm. Databases and LIS cannot communicate. A preliminary examination found that no patient data was lost [3].
- **25 Jun 2024:** Recorded Future News reports “Deletion of backup servers and manual/telephonic result dissemination amid a national mpox response” [5].
- **3–8 Jul 2024:** Recovery continues; WebView portal remains offline. A critical test list is issued to triage workloads; mid-July restoration is projected [6].
- **5–12 Jul 2024:** BlackSuit claims responsibility and around 1.2 TB of exfiltration. NHLS repeats its no-negotiation stance [7].
- **15 Jul 2024:** NHLS publishes an interim eLABS approach for TB/HIV historical results and phased service restoration [6].
- **22 Aug 2024:** SA Department of Health announces full restoration of NHLS operations and future cybersecurity fortification [8].
- **Dec 2024:** A peer-reviewed article in the South African Medical Journal comments on the ramifications, immediate actions, and continuity planning advice taken from departmental experience with the attack [9].

4.4 MITRE ATT&CK Enterprise Mapping of Adversary TTPs

The following diagram is the process of the attack lifestyle:

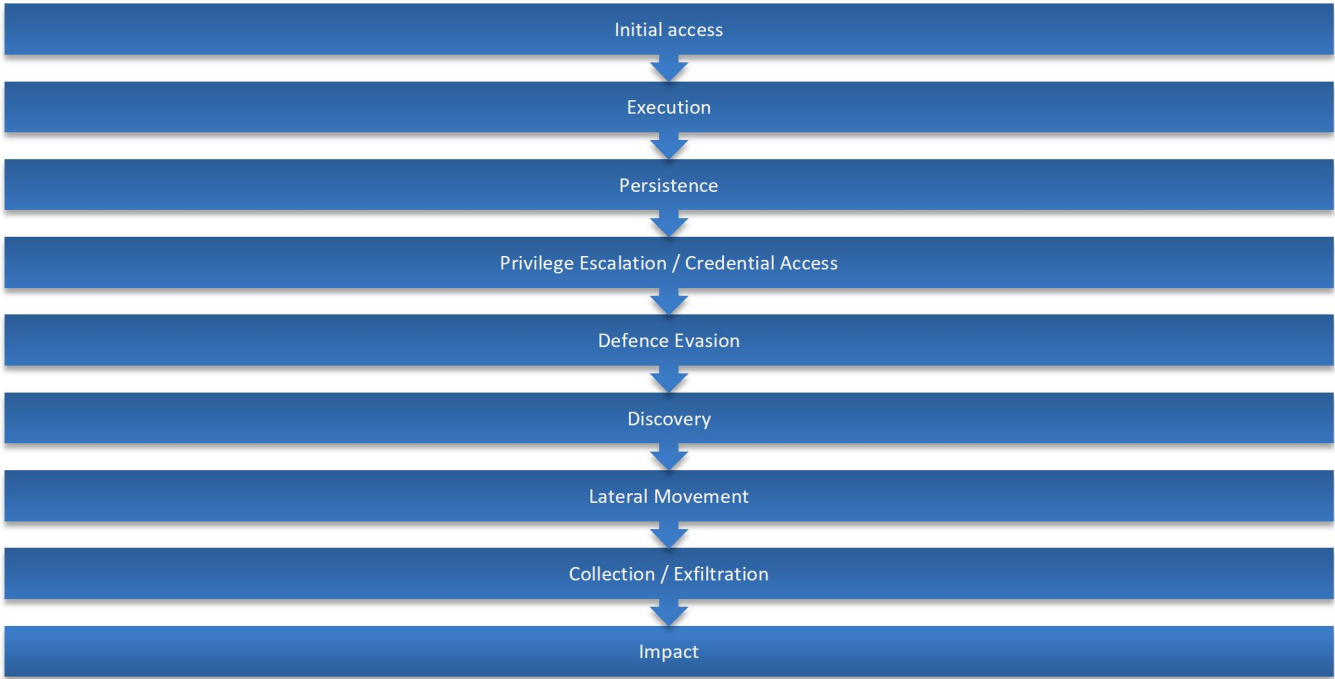


Figure 1: Attack Lifestyle process

In the following Table 1 some techniques apply the MITRE ATT&CK matrix to report BlackSuit campaigns and observed activities in NHLS. There is supporting documentation for technique IDs.

Tactic	Technique (ID)	Explanation
Initial Access	Spear phishing (T1566.001/002)	Employee clicked phishing link (parliament testimony) [10] [11].
Execution	PowerShell (T1059.001)	Scripted staging & execution observed in BlackSuit intrusions [10] [11] [12]
Persistence	Run Keys/Startup (T1547.001)	Common persistence path in ransomware campaigns. [3][11] [12]
Privilege Escalation / Credential Access	Kerberoasting (T1558.003); OS Credential Dumping (T1003)	ReliaQuest observed Kerberoasting and credential access.[10][13][11]
Defense Evasion	Inhibit System Recovery (T1490)	Shadow copies/backup deletions; NHLS reported backup server deletions. [11]
Discovery	System/Network Discovery (T1082, T1046)	Discovery tools (ADFind/SharpHound/Cobalt Strike). [3][5][11] [12]
Lateral Movement	RDP (T1021.001), SMB/Admin shares/PsExec (T1021.002)	Lateral tool transfer and PsExec execution. [13][11]
Command & Control	Web protocols/SystemBC (T1071.001)	Cloud- fronted beacons/proxy C2. [11] [12]
Exfiltration	Exfiltration over Alt Protocol (FTP) (T1048)	Data theft before encryption (double extortion). [13][11]
Impact	Data Encrypted for Impact (T1486)	Final ransomware encryption phase.[3][7][11]

Table 1:TTPs Mappings

4.5 Root-Cause Analysis (Technical, Architectural, Human factors)

4.5.1 Human factors

According to information presented to Parliament, a phishing click opened the door through which BlackSuit gained access (yet another indicator of breaches that came down to security awareness, and failings in email controls [10].

4.5.2 Architectural/technical debt

NHLS management admitted on record to outdated facilities that couldn't be patched/updated, implying technical debt, which increased exploitability and delayed bounce-back [10].

4.5.3 Backup/BCP issues

Deleting backups and portal outages show weaknesses in the backup immutability/segmentation and single points of failure between LIS, data warehouse, and serving services, blasting radius is increased [3][8].

4.5.4 Threat tactics

BlackSuit/Royal TTPs often involve credential theft, lateral movement over SMB/RDP, and the destruction of recovery artifacts, which is consistent with the NHL symptoms, and a double-extortion model as reported by media and industry [13].

4.5.5 Monitoring gaps

NHLS reported ongoing attacks following the intrusion, necessitating additional security layers and shutdowns; this shows inadequacies in continuous monitoring, threat intelligence, and incident containment orchestration [3].

4.5.6 Public health implications

A peer-reviewed SAMJ article highlights healthcare cyberattack variants operational fragility and “unavoidable” call for business continuity plans in laboratory services; larger studies connect ransomware to delayed care, worse patient outcomes, strengthening that resilience shortfalls directly hazard patient safety [9].

4.6 Strategic Recommendations

4.6.1 Prevention

- Phishing-resistant MFA for email/VPN; DMARC/DKIM/SPF, attachment sandboxing, link isolation; continuous user training targeted to healthcare phish variants [14].
- EDR/XDR with behavioral ransomware blocking (e.g., vssadmin/shadow copy tamper alerts), and server application allow-listing; adopt ATT&CK-informed detection engineering [15].

4.6.2 Architecture

- Immutable, offline, and segmented backups (3-2-1-1-0), credential separation, and routine restore testing under NIST SP 800-184 recovery playbooks [15].
- Network/identity segmentation (tiered domains, admin plane isolation), least privilege, and strong service account governance to blunt Kerberoasting and SMB/RDP lateral movement [13].
- Separate critical lab systems (LIS, data warehouse, portals) with brokered interfaces to reduce cascade failures seen during the outage [3].

4.6.3 Detection

- Detections for PowerShell abuse (T1059.001), shadow copy deletion (T1490), AD reconnaissance (ADFind/SharpHound), PsExec/ SMB movement, and FTP exfiltration (T1048); hunt for Cobalt Strike/ SystemBC beacons (T1071.001) [13].
- Using CISA ‘Best Practices for ATT&CK Mapping’ to continuously identify and close gaps; monitor IOCs/TTPs from [14][15].
- Incident runbooks and tabletop exercises with NIST SP 800-184 metrics; simulate dissemination failover (e.g., eLABS) [15].

4.6.4 Rate the Threats

According to [16], Risk prioritization is a fundamental element in the threat modeling approach. Security teams may prioritize their limited time and resources by methodically assessing risks based on their likelihood and possible effect. This pragmatic approach ensures that the most serious risks are mitigated as soon as possible, while also realizing that it may not be viable or cost-effective to handle every single potential hazard, particularly those with a very low likelihood of occurring.

4.6.4.1 Calculation of Risk

As described by [16], Risk is measured as the probability of a damage potential ($\text{Risk} = \text{Probability} * \text{Damage Potential}$). Both probability and damage potential have a range from 1 to 10, with higher numbers indicating a greater impact. This model shows how even a low-probability, high-impact threat may be as much of a source of danger as the more apparent high-probability/low-consequence situation. The resulting risk score is between 1 and 100, which corresponds to Low, Medium, and High levels of risk.

4.6.4.2 Calculation of Ratings

As reported by [16], using a simple High, Medium, or Low scale to prioritize threats. High threats are those that could cause the maximum level of impact to the application and must be dealt with straight away, as they may result in high security, operational, or reputational damage. There is also an address is medium threats, but these can be addressed in less urgent ways that might involve planned controls or future defects. Low threats present little risk and might be tolerated or ignored, especially if the mitigation introduces more than it eliminates.

4.6.4.3 DREAD Threat Model

The risk is calculated using the DREAD (Damage potential, Reproducibility, Exploitability, Affected Users, and Discoverability) threat model [16]. With the help of the DREAD model [16], used to rate and rank the threats for the selected attack vectors found in the NHLS ransomware incident. Scores and risk ratings are listed in Table 2

Threat	D	R	E	A	D	Total	Avg	Rating
Phishing initial access	8	9	8	8	8	41	8.2	High
Privilege Escalation + lateral movement (Kerberoast/RDP)	9	7	7	9	7	39	7.8	High
Backup sabotage (shadow copy/backup deletion)	10	8	7	8	6	39	7.8	High
Data exfiltration (FTP/cloud/leak)	8	7	6	7	7	35	7.0	High
Unencrypted login requests	5	8	6	6	8	33	6.6	Medium

Table 2: DREAD Threat Modeling

High-risk threats like phishing-based initial entry, privilege escalation, and backup sabotage need to be addressed instantly. Recommended mitigations include phishing-resistant MFA, privileged access locking down, and immutable backups. Average issues with unencrypted login requests, for example, should also be knocked off to lower risk.

4.6.5 Governance & Policy

- Utilize peer-reviewed evidence and sector statistics to prioritize identification, backups, segmentation, and SOC capabilities [17].
- Use financial crime/ransom patterns to support no-pay rules, law enforcement involvement, and data loss mitigation measures [18].

5 Discussion

Attack on NHLS provides a clear demonstration, how one successful phishing attack can turn into a sector-wide disruption when backups, segmentation, and privileged identity are all weak. It also shows the “double-extortion” pressure tactic, and the need for open, non-negotiable attitude in preserving clinical continuity through alternative transitory channels (telephone contact, papers printed result, eLABS). Finally, it amplifies the real-world ransomware in healthcare paradigm that has been documented by both industry and peer-reviewed research; attacks not only occur often and are expensive, but they’re patient-safety relevant, requiring threat-informed defense and tested recovery [3][7][9][10].

6 Task 2

Here, the focus is on simulating the actions of an Advanced Persistent Threat (APT) actor to realistically assess Cureton Pharmaceutical Company’s security defences and identify potential risks to its intellectual property.

6.1 Operation IP Shield – Red Team Engagement

6.1.1 Campaign Design

6.1.1.1 Rules of Engagement (RoE)

A clearly defined RoE ensures red team activities are ethical, legal, and aligned with organizational objectives. The RoE limits testing to synthetic data within the on-premises Active Directory, the AWS-hosted clinical trial portal, and the CI/CD pipeline. Destructive actions, denial-of-service attacks, and interaction with real customer data are explicitly excluded.

To identify potential risks, a small virtual lab is set up using “Oracle VirtualBox”. This lab represents key parts of the target environment. For that there will be Four virtual machines are going to be used:

1. Kali Linux as the attacker system, named “Kali2019”
2. Metasploitable to simulate a vulnerable cloud service, named “AWS VPC”
3. OWASP Broken Web Applications to represent insecure CI/CD applications, named “CI-CD”
4. Windows Server to model the R&D Active Directory network, named “R&D AD”

Together, these systems create a realistic and safe environment for simulating attacks and evaluating security controls.

To illustrate, Figure 2 Shows the full environmental process of the host machine that uses a virtual machine to emulate vulnerability assessment

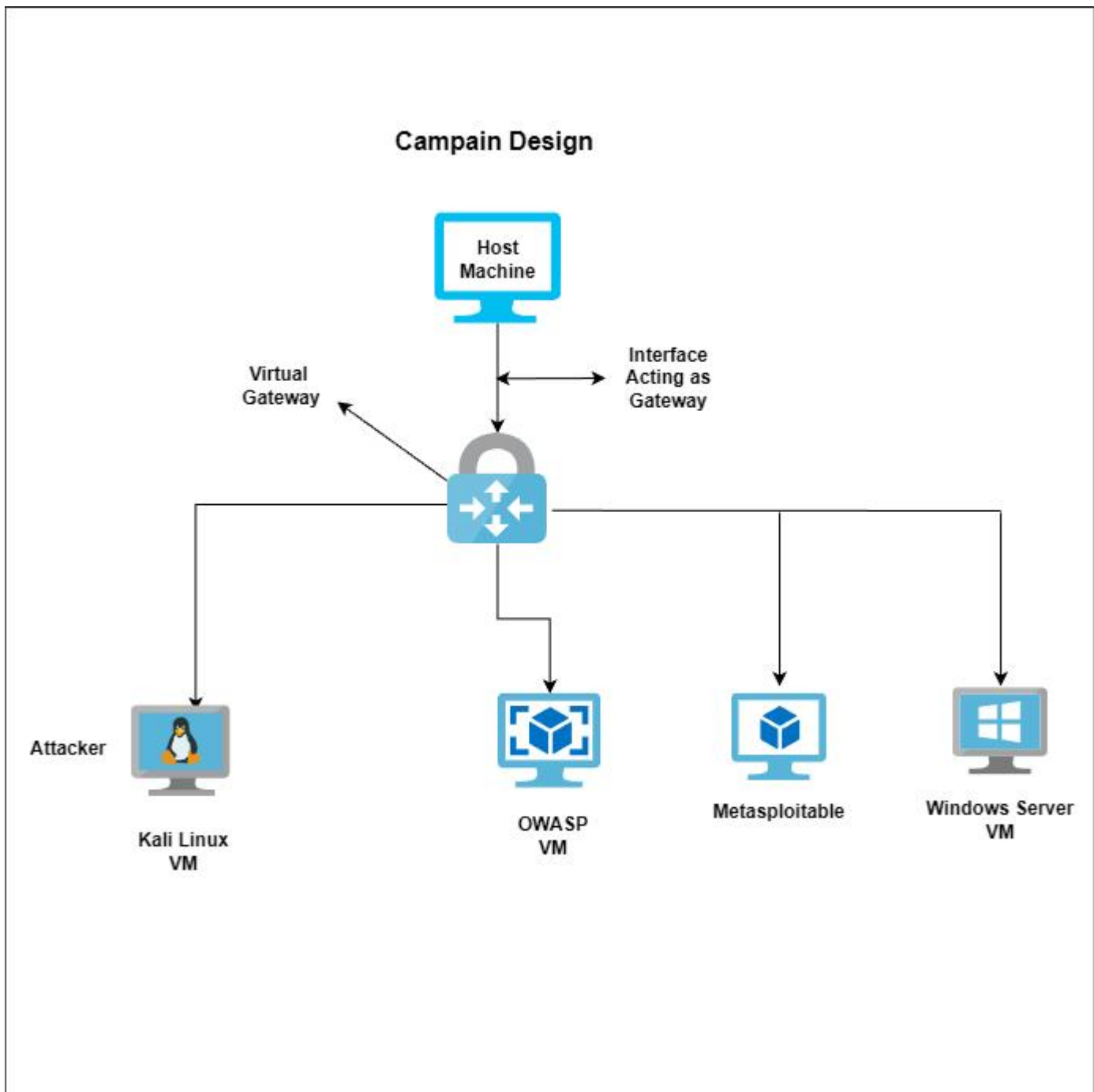


Figure 2: Campaign Design with Environmental Process

To emulate a vulnerability assessment, the following tools are used, each serving a specific purpose in the assessment process:

- **Kali Linux:** Kali Linux is the primary operating system for vulnerability testing. Including a large amount of built-in security and penetration testing tools, it's suitable for scanning, testing, and analysis. [19]
- **Metasploitable:** Metasploitable is a vulnerable virtual machine used as a testing target. Allows vulnerability assessment tools to be safely tested without impacting real systems.
- **Nmap:** Nmap is for network scanning and discovery. It helps identify active hosts, open ports, running services, and operating systems, which is for understanding the network attack surface.

- **DB_nmap:** DB_nmap detects database services. It helps to expose database ports and insecure database configurations that may be exploited.
- **Burp Suite:** Burp Suite is a testing tool for web applications. It detects web traffic and common vulnerabilities such as SQL injection, cross-site scripting (XSS), and weak points.
- **Nessus:** Nessus is for automated vulnerability scanning. It detects hosts, vulnerabilities, recommended remediation actions, and notes [20].

6.1.1.2 Threat Emulation Plan

The attacker is trying to obtain access using CI/CD flaws rather than noisy technical vulnerabilities. After gaining access, only built-in system and cloud tools are utilized to navigate the network and avoid detection. The attacker gains access to a dummy research dataset and exfiltrates it via traffic that seems to be standard cloud connectivity.

6.1.2 Environment & Execution

6.1.2.1 Attack Narrative

The attack narrative describes a threat simulation strategy that acts like a genuine attacker. It starts with Nmap and DB_nmap scanning for open ports and services. Burp Suite searches online apps for common security flaws, whereas Nessus looks for known vulnerabilities and misconfigurations. Metasploitable is then used to show how to exploit a susceptible victim. This method aids in identifying flaws and improving defenses prior to an actual attack. In Figure 3 to demonstrate how the attack will happen.

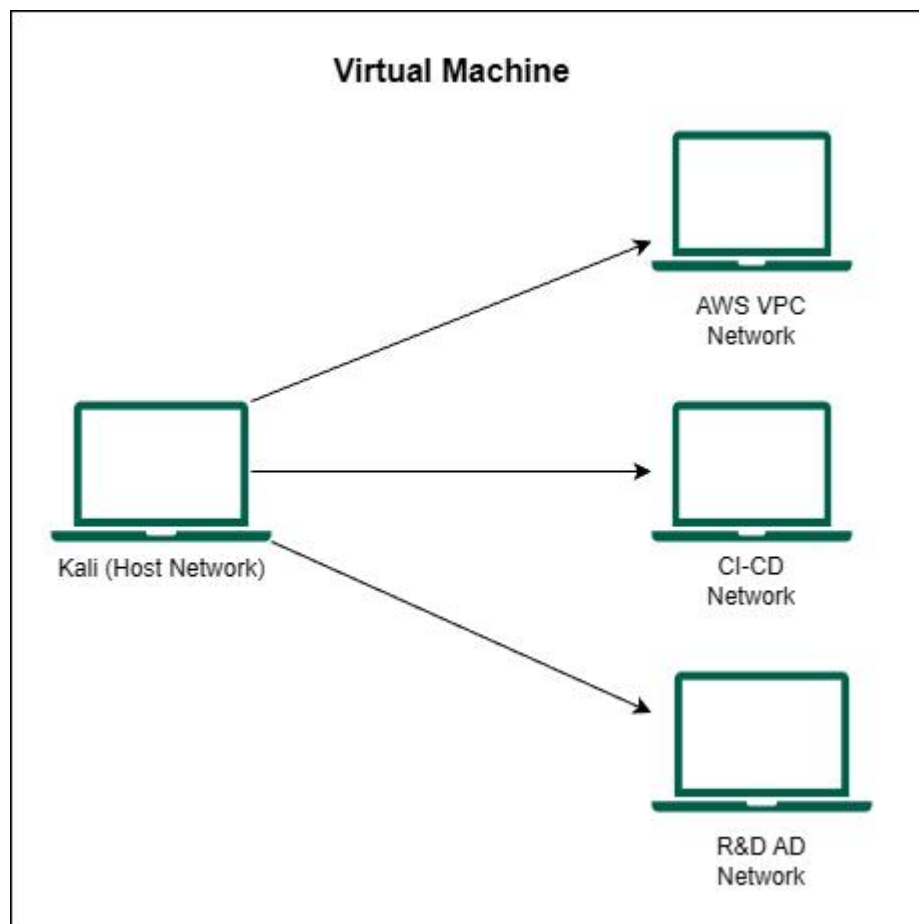


Figure 3: Emulation Narrative

6.1.2.2 Environment Design

The lab environment is designed to resemble and feel like CPC's actual system. It covers office systems like Active Directory, user workstations, R&D file servers, and AWS VPC-hosted cloud services.

In the VirtualBox -

- **Kali installation:** From Figure 5 to Figure 8 show the steps of installation of Kali Linux. For that, the VM name will be “Kali2019”, the OS, OS Distribution, and OS version will be according to “Linux”, “Other Linux”, and “Other Linux (64-bit)”. Because the main emulator will be from Kali Linux, for that “Base Memory”, “Number of CPUs” should be high. After importing the VM from the local disc, and network should be attached to “Bridge Adapter”.

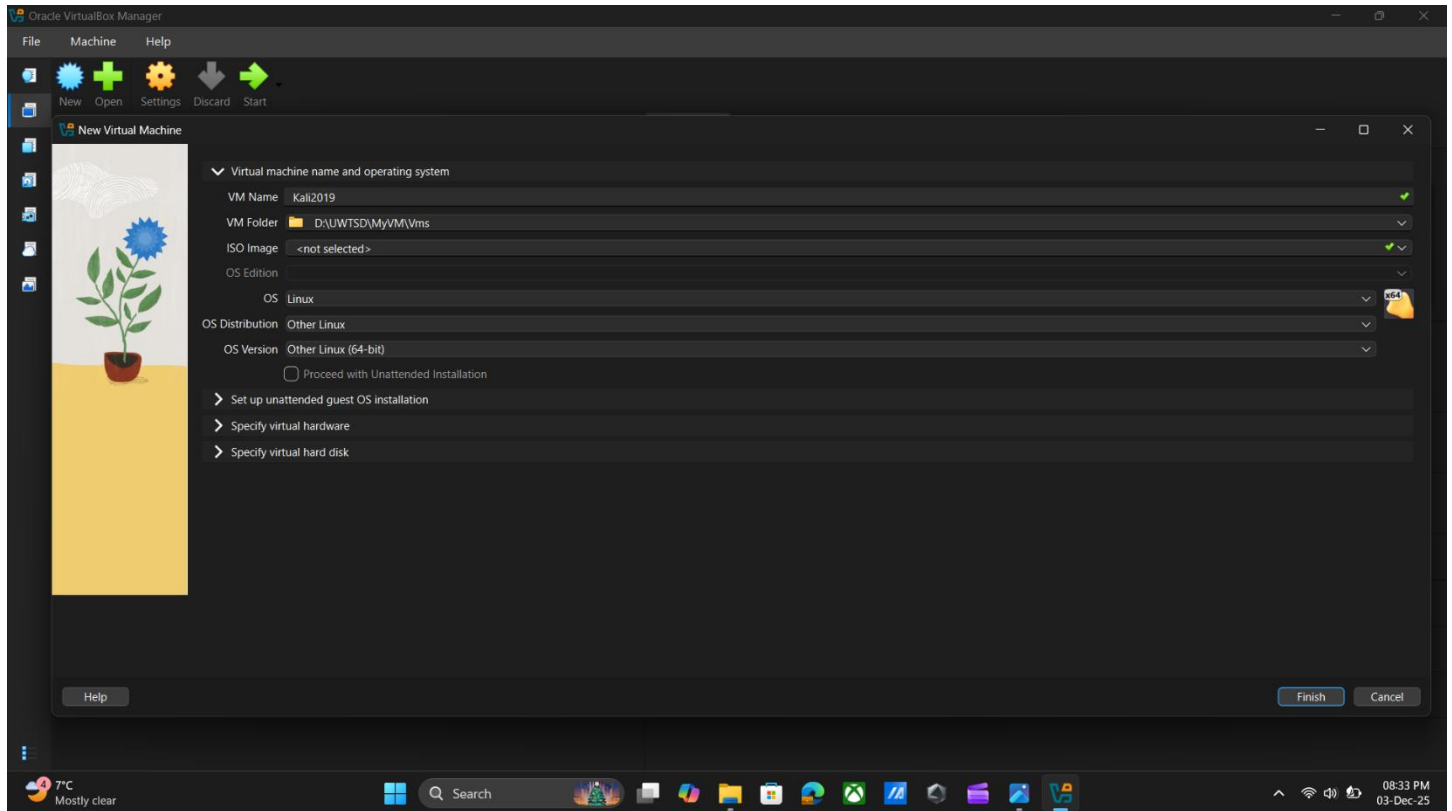


Figure 5: Installation process of Kali - 1

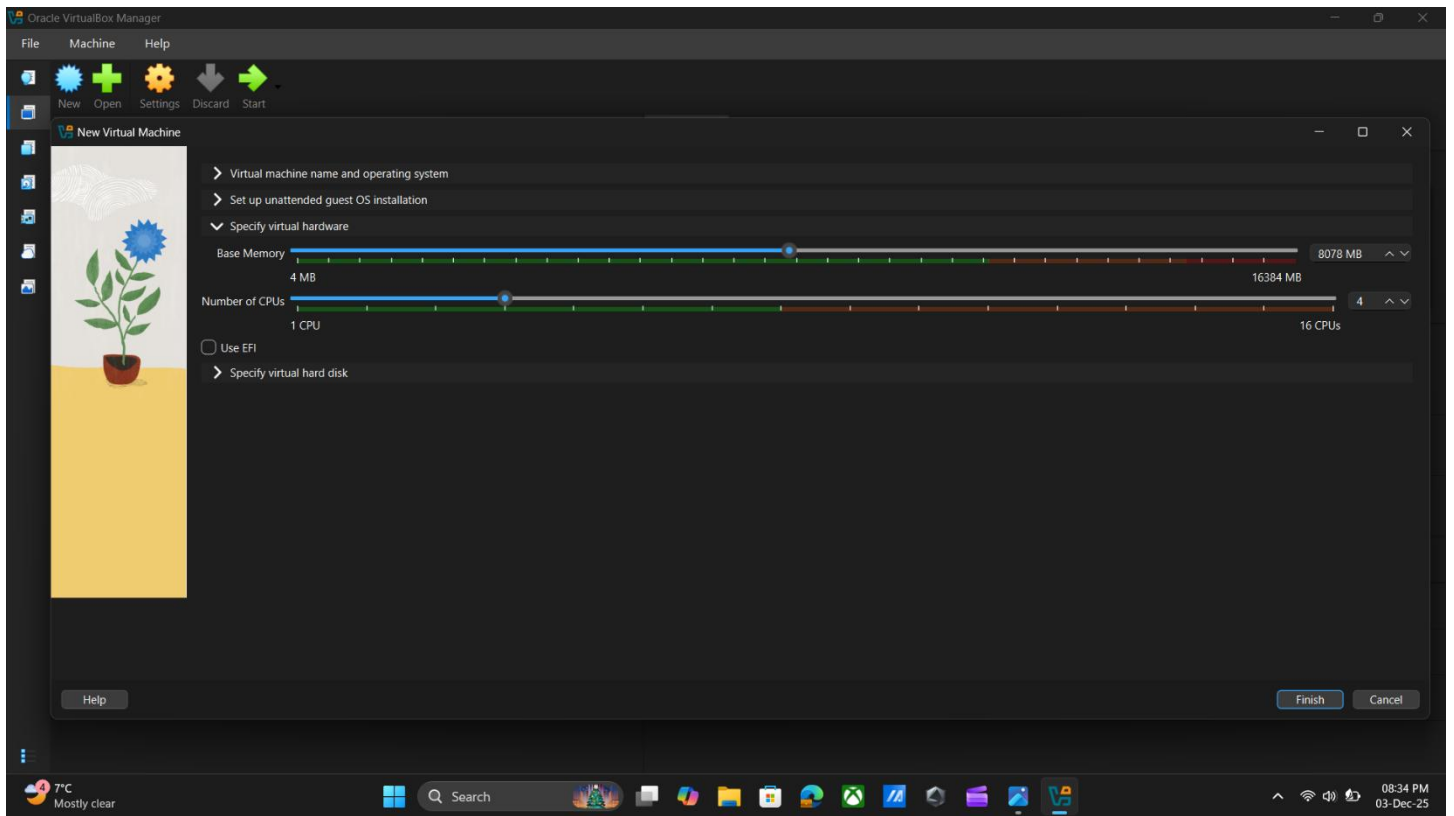


Figure 6: Installation process of Kali - 2

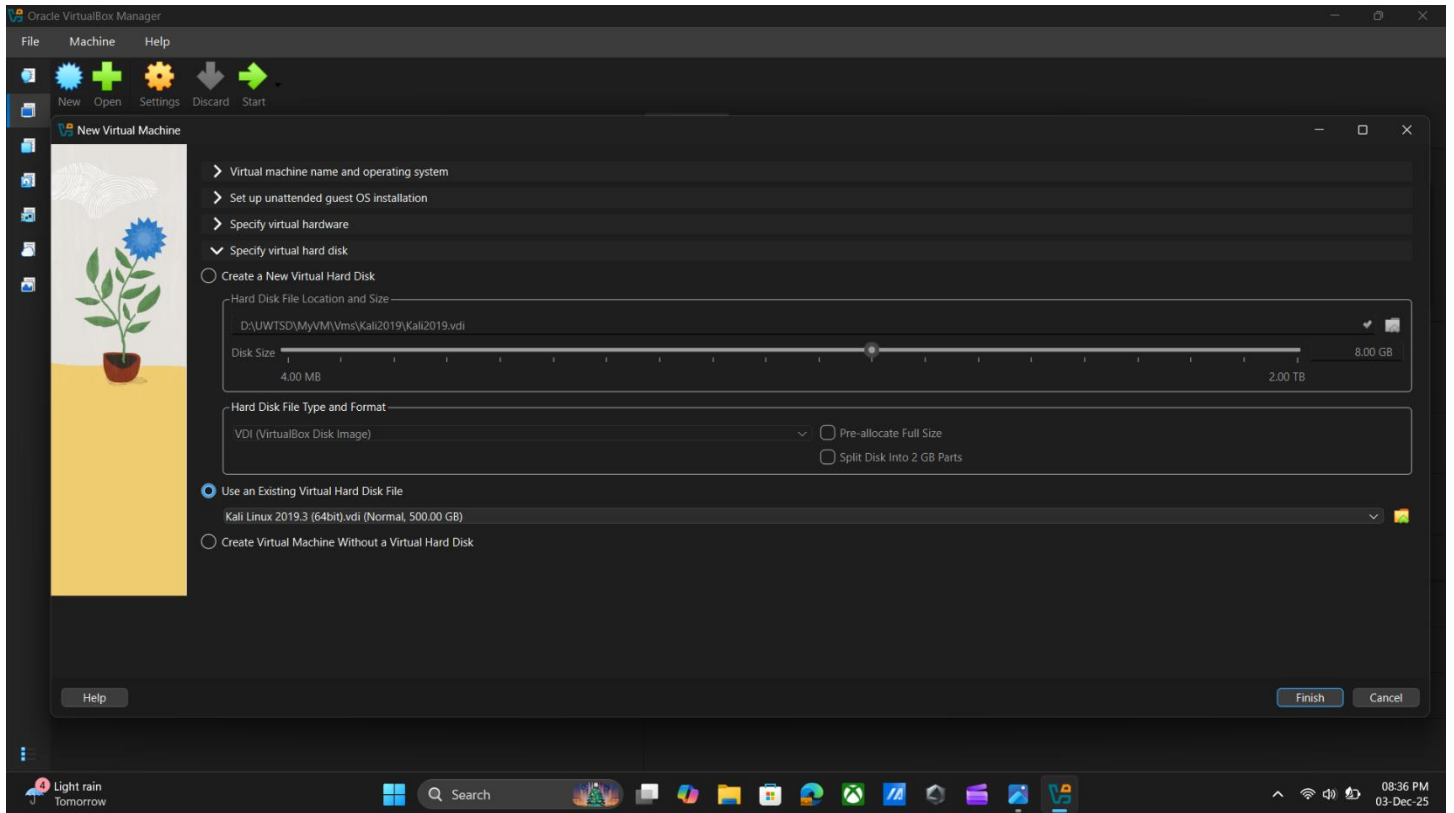


Figure 7: Installation process of Kali - 3

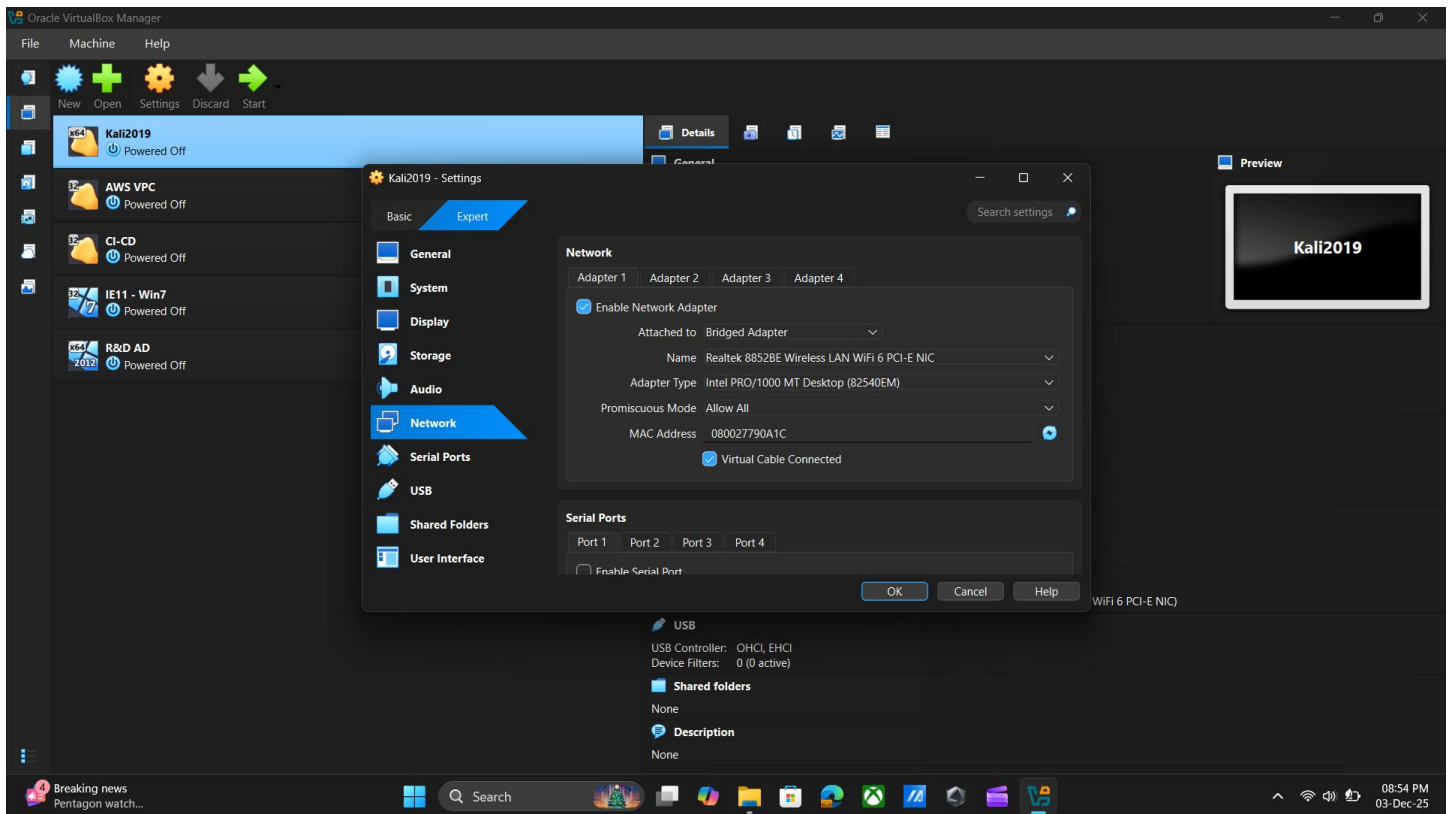


Figure 8: Installation process of Kali - 4

- AWS VPC Installation:** Figure 9 to Figure 12 illustrate the process of installing Metasploitable. For that, the VM name will be “AWS VPC”, the OS, OS Distribution, and OS version will correspond to “Linux”, “Other Linux”, and “Other Linux (32-bit)”. “Base Memory”, “Number of CPUs” should be minimum. After importing the VM from the local disc, the network should be attached to “Bridge Adapter” with “Allow all”.

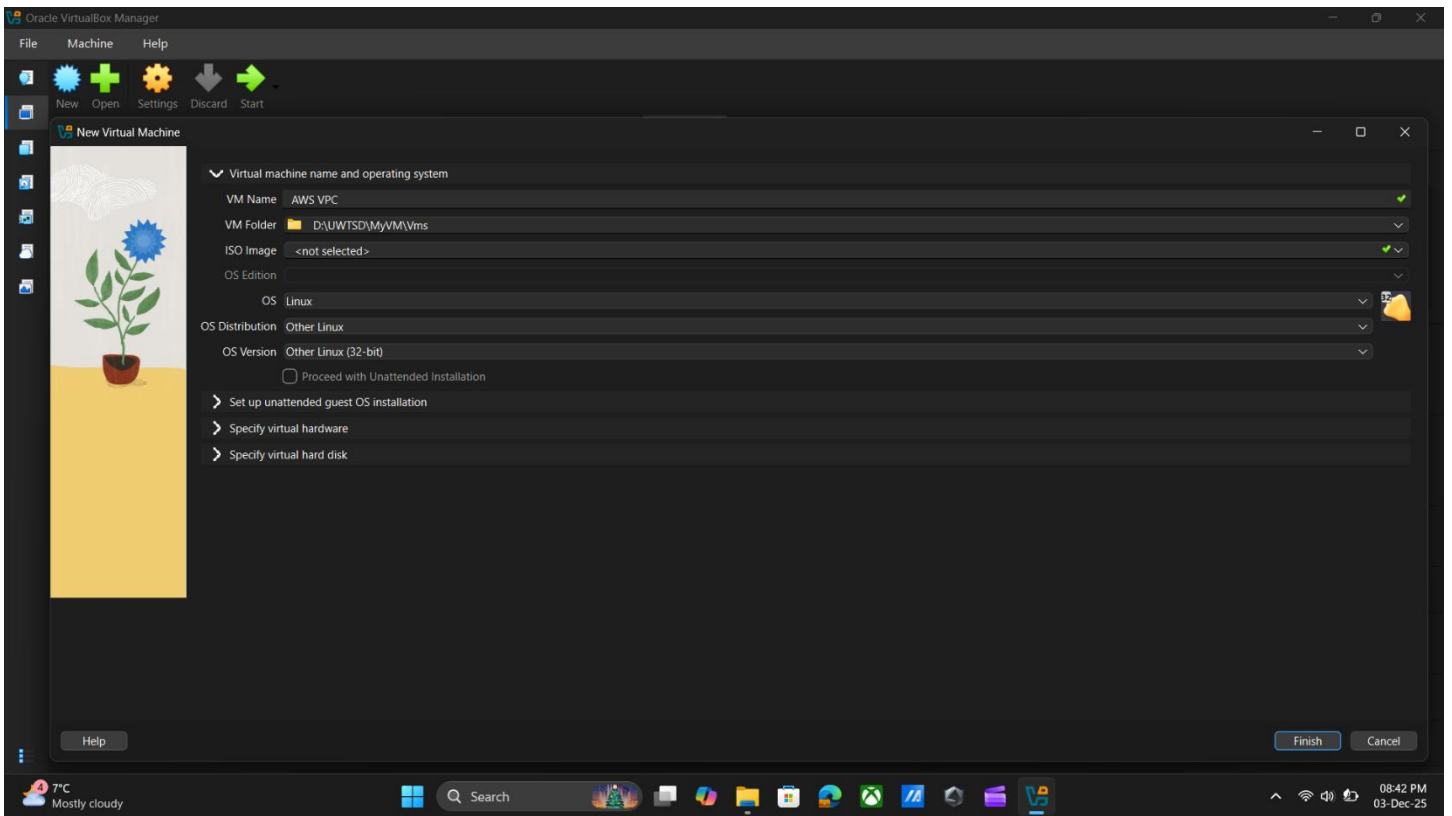


Figure 9: Installation process of AWS VPC - 1

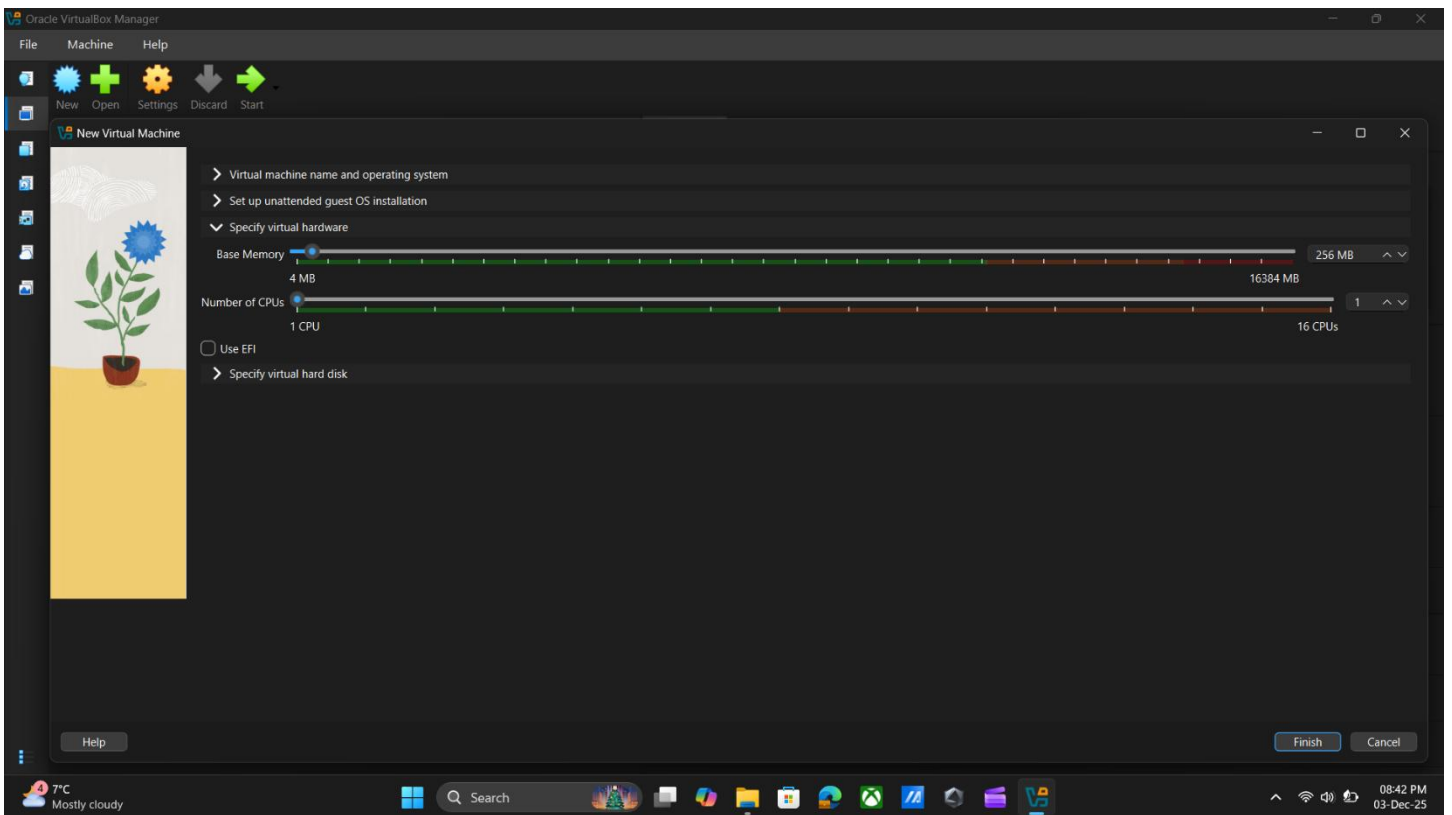


Figure 10: Installation process of AWS VPC - 2

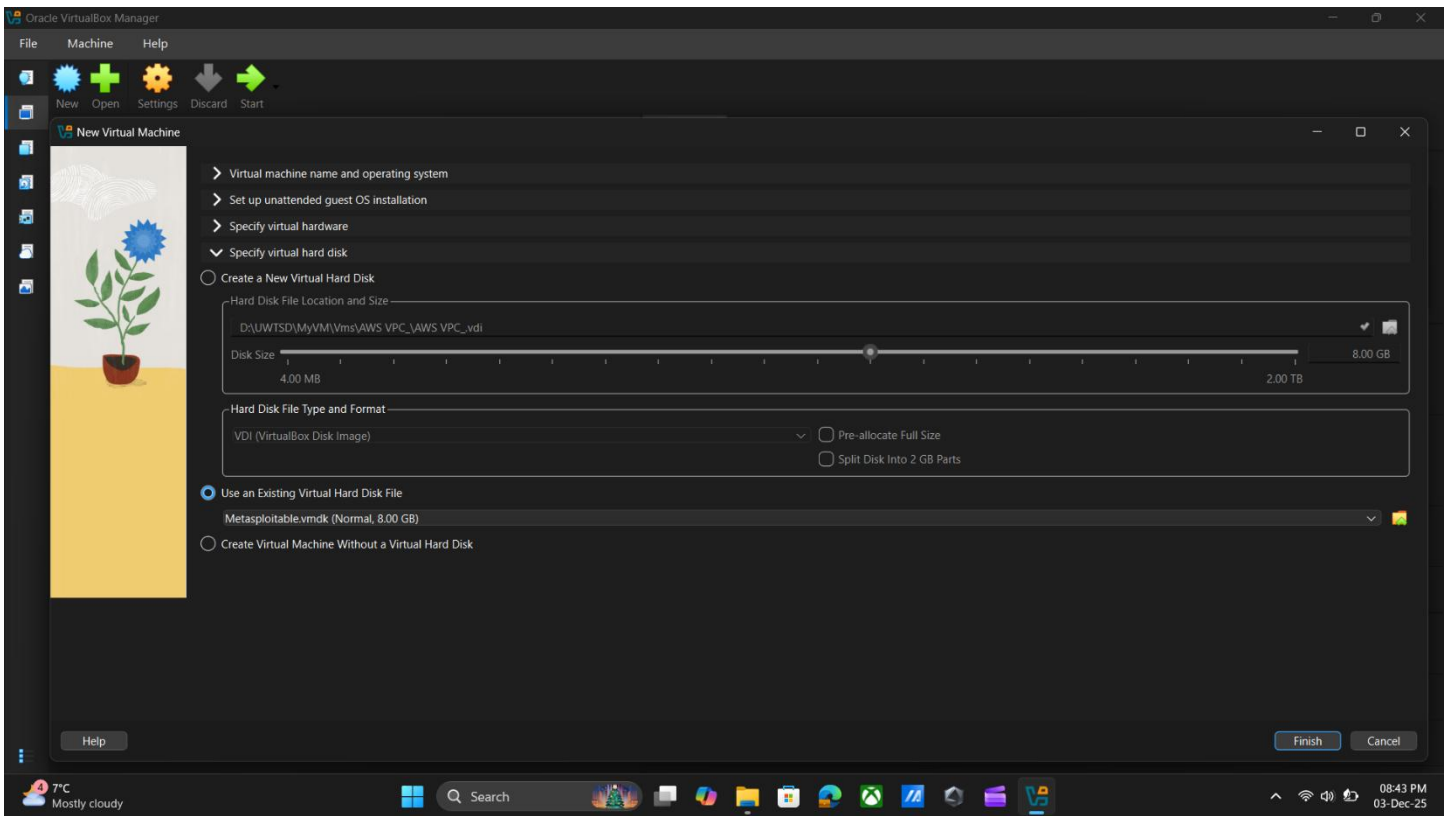


Figure 11: Installation process of AWS VPC - 3

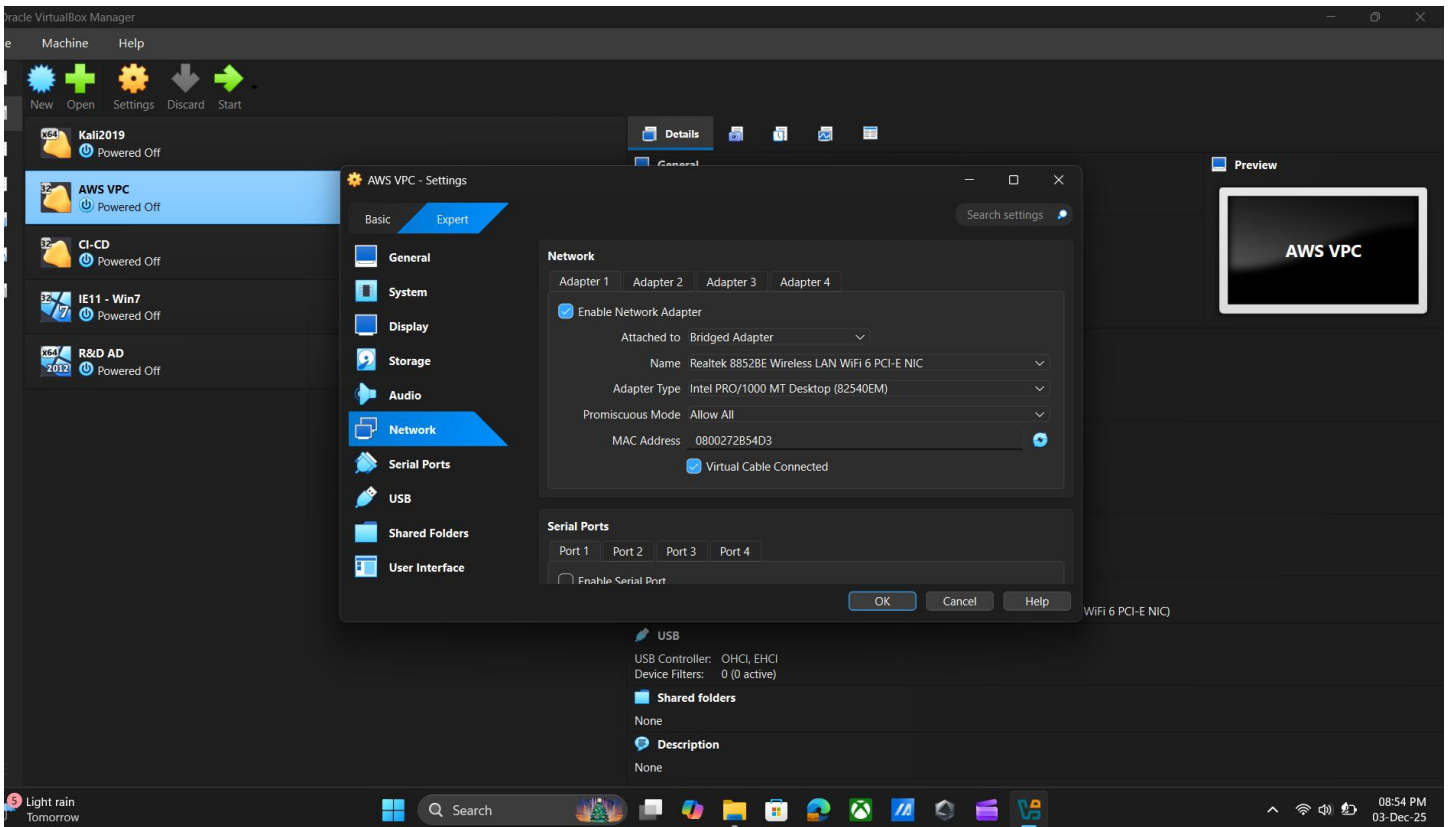


Figure 12: Installation process of AWS VPC - 4

- **CI/CD Installation:** Figure 13 to Figure 16 highlight the methods of installing OWASP. For that, the VM name will be “CI-CD”, the OS, OS Distribution, and OS version will follow “Linux”, “Other Linux”, and “Other Linux (32-bit)”.

“Base Memory”, “Number of CPUs” should be minimum. After importing the VM from the local disc, the network should be attached to “Bridge Adapter” with “Allow all”.

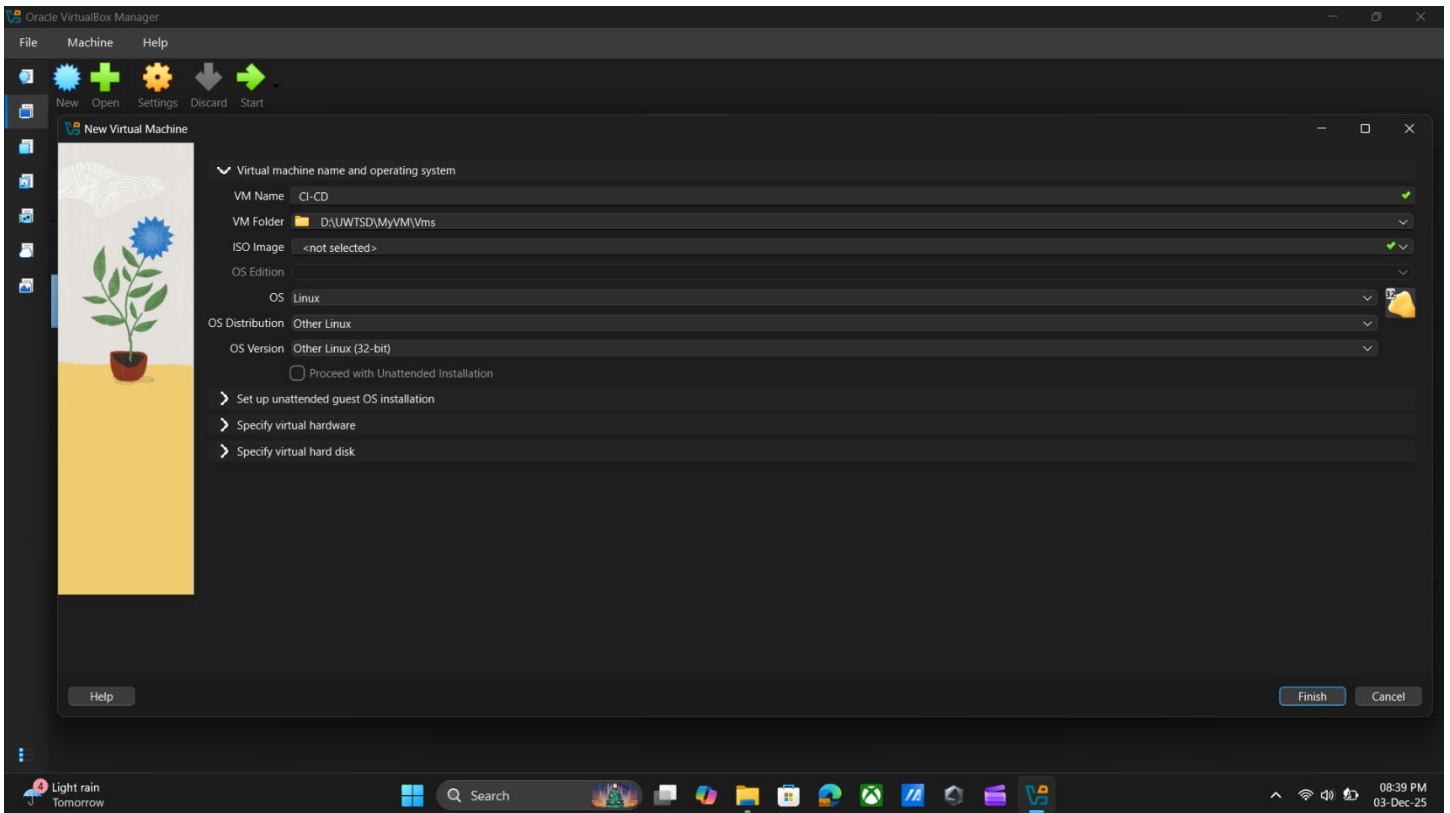


Figure 13: Installation process of CI-CD - 1

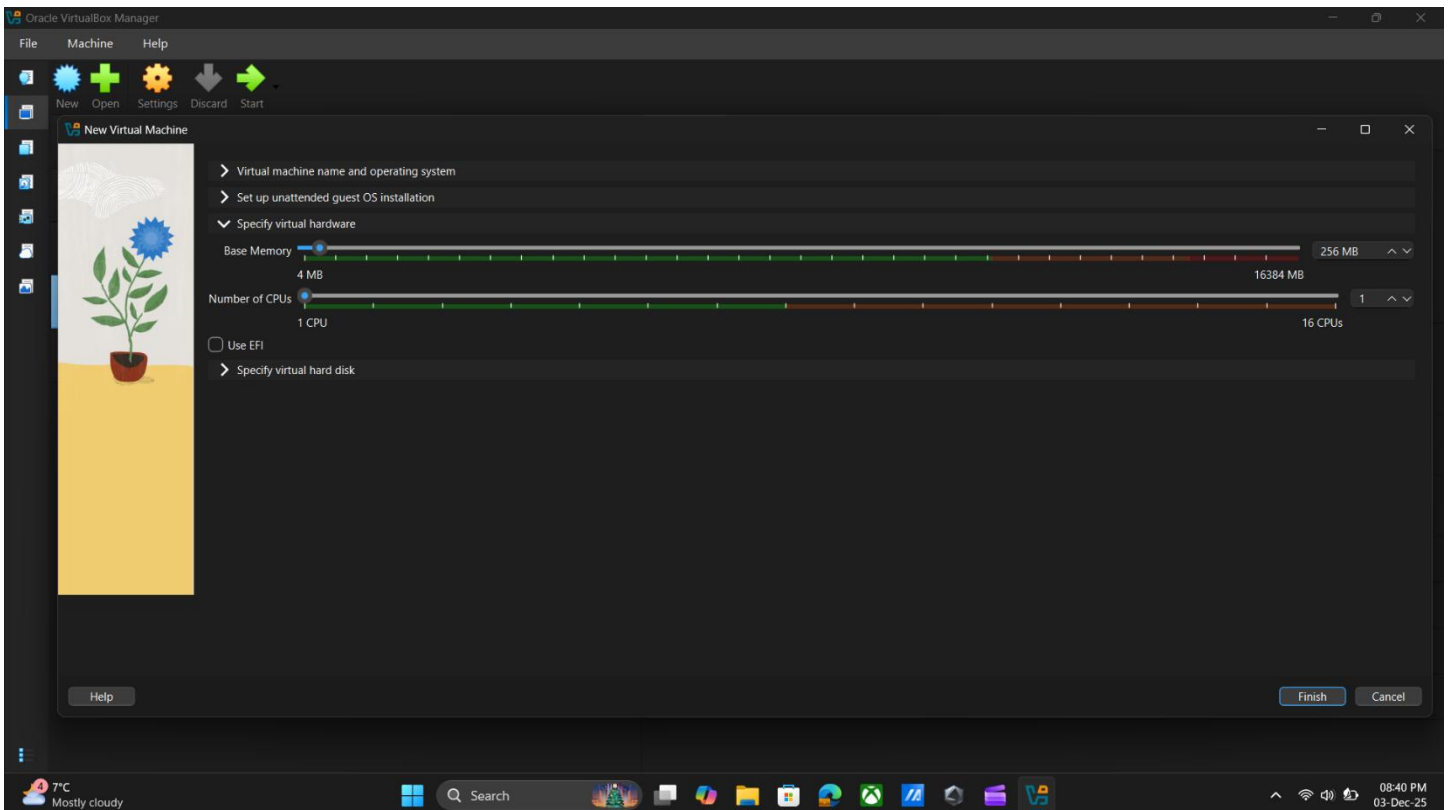


Figure 14: Installation process of CI-CD - 2

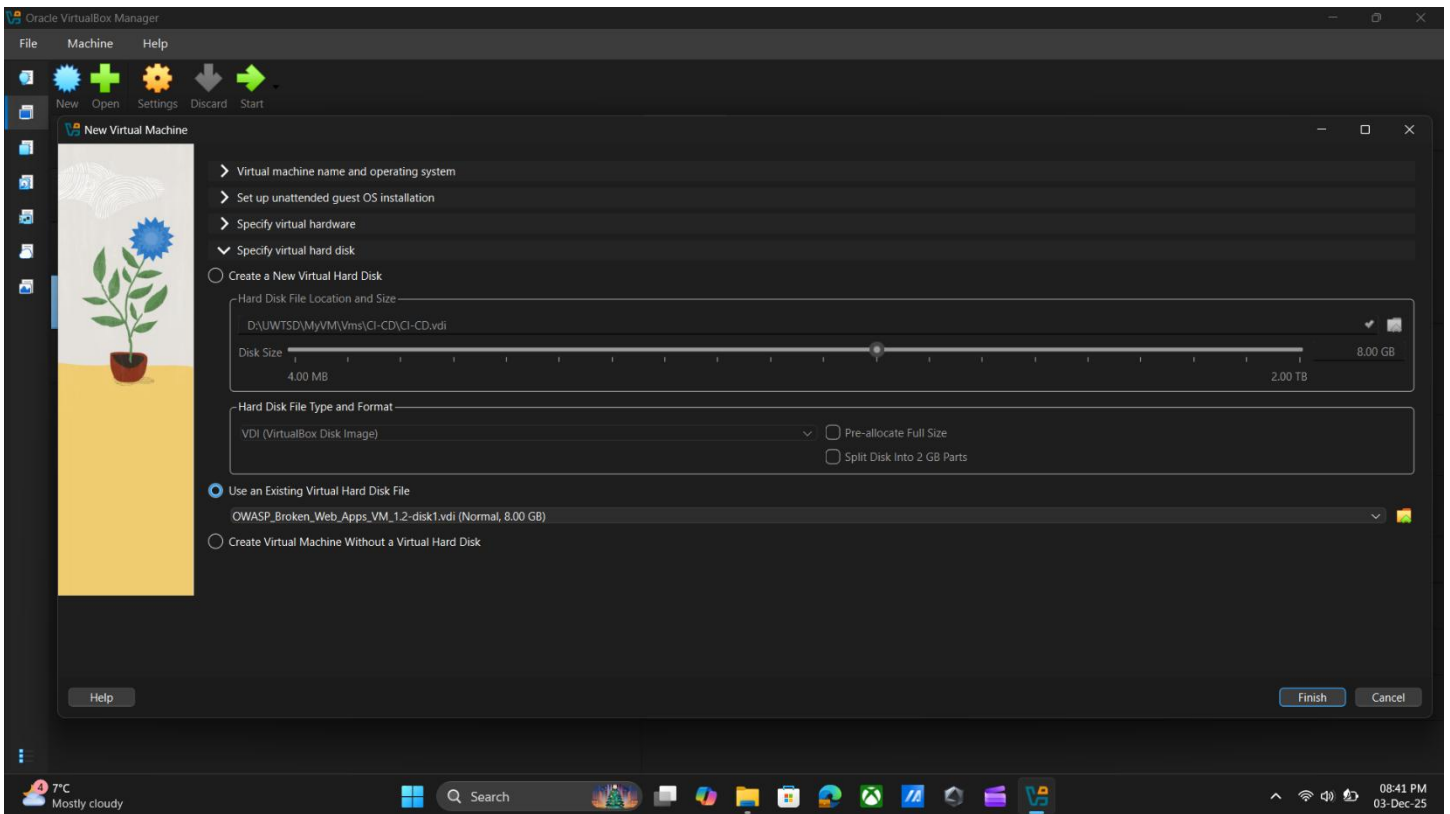


Figure 15: Installation Process of CI-CD - 3

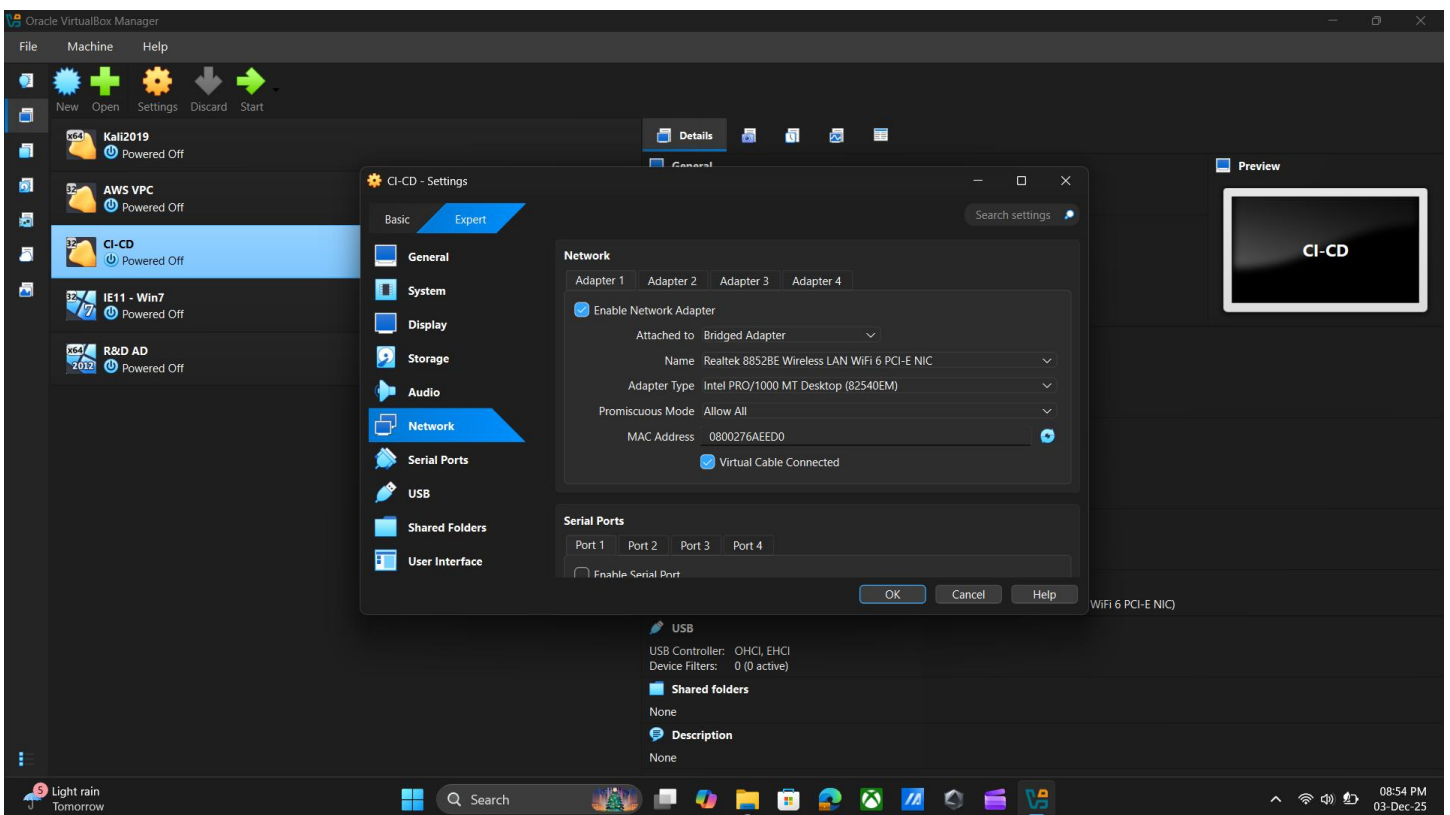


Figure 16: Installation Process of CI-CD - 4

- **R&D AD Installation:** looking into Figure 17 to Figure 20 explains the techniques of installing Windows Server. For that, the VM name will be “R&D AD”. Before that, from the Local disc, it should be imported. It will take all the necessary steps itself, and finally, the network should be attached to the “Bridge Adapter” with “Allow all”.

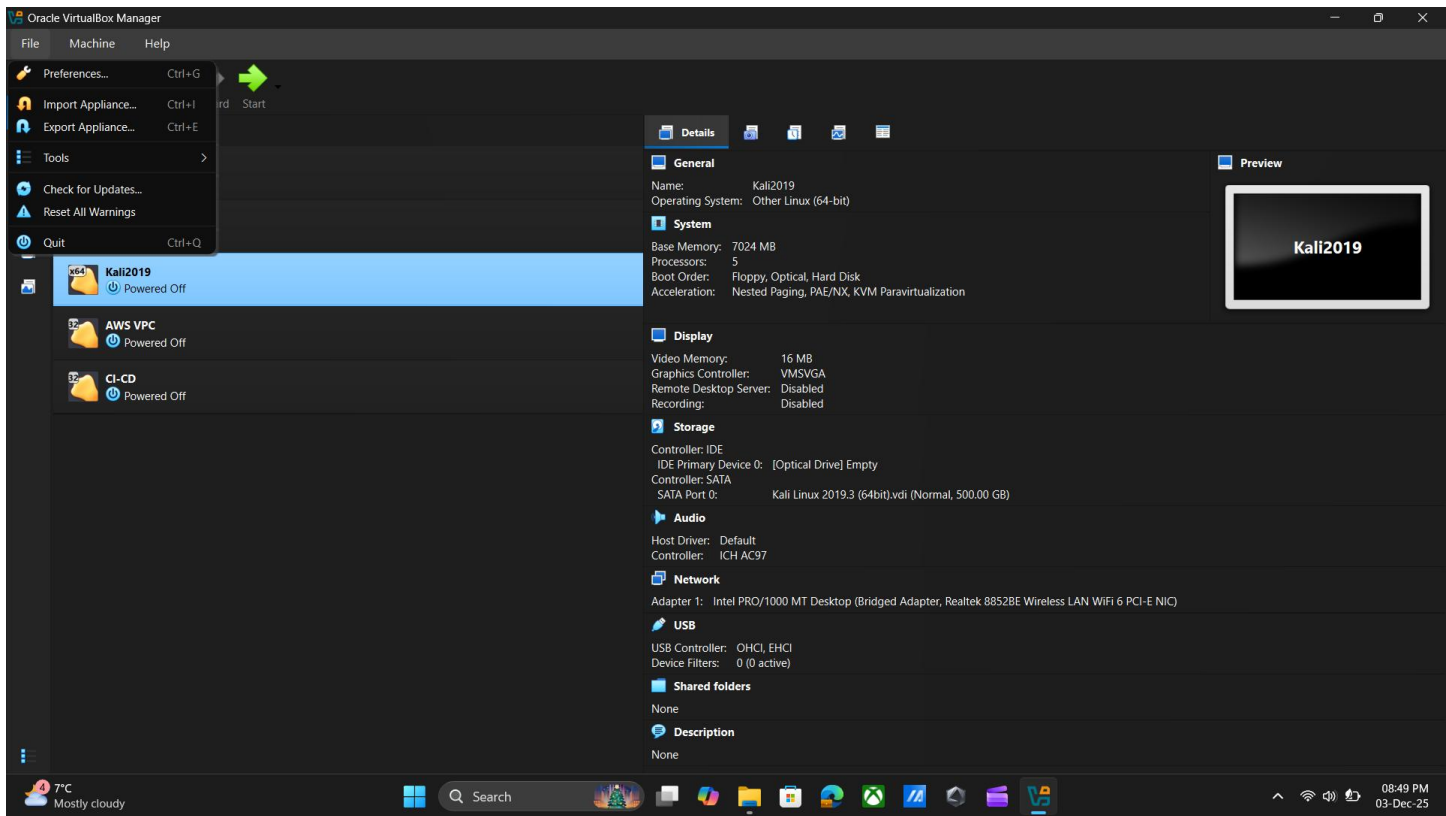


Figure 17: Installation process of R&D - 1

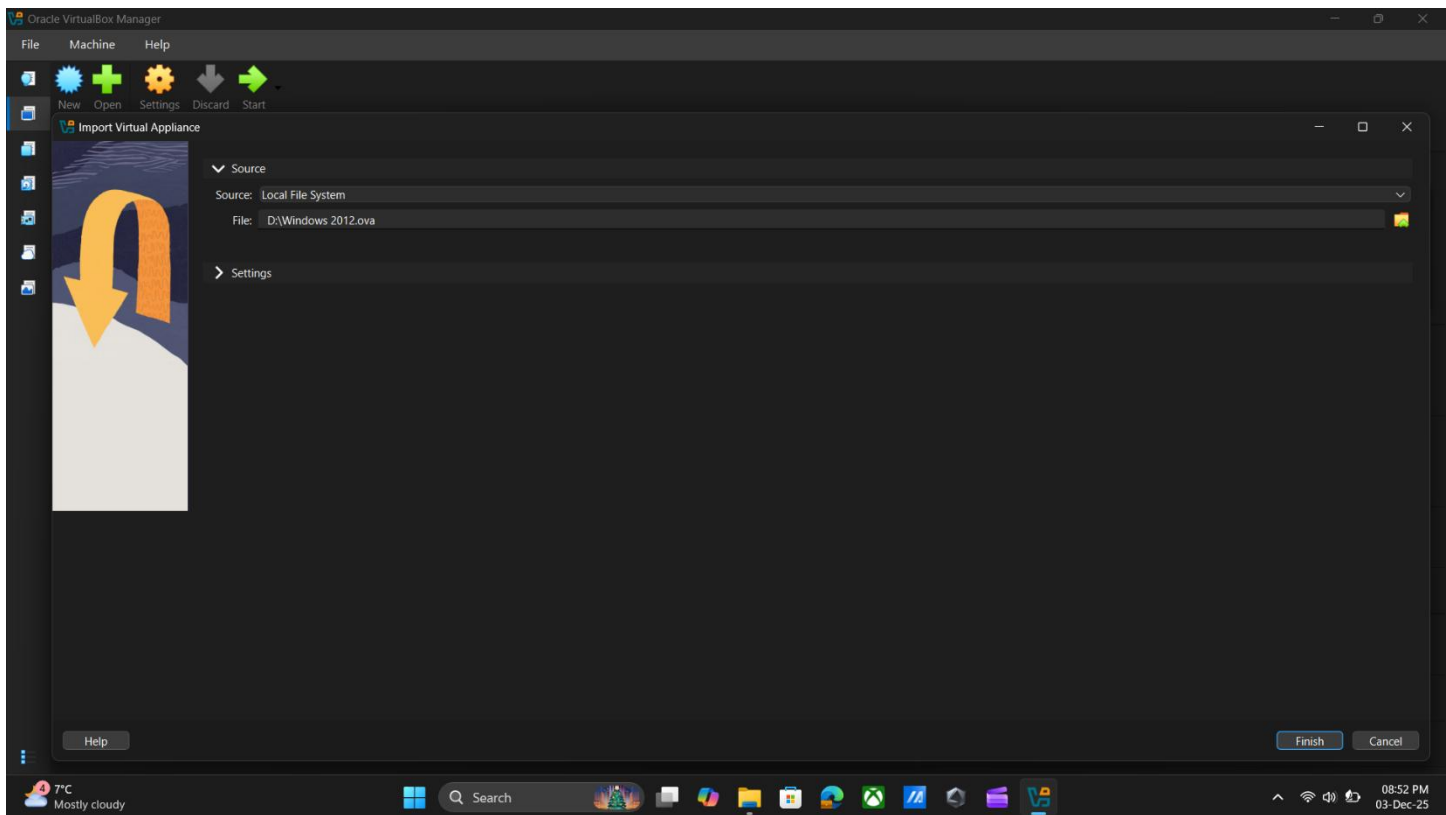


Figure 18: Installation process of R&D - 2

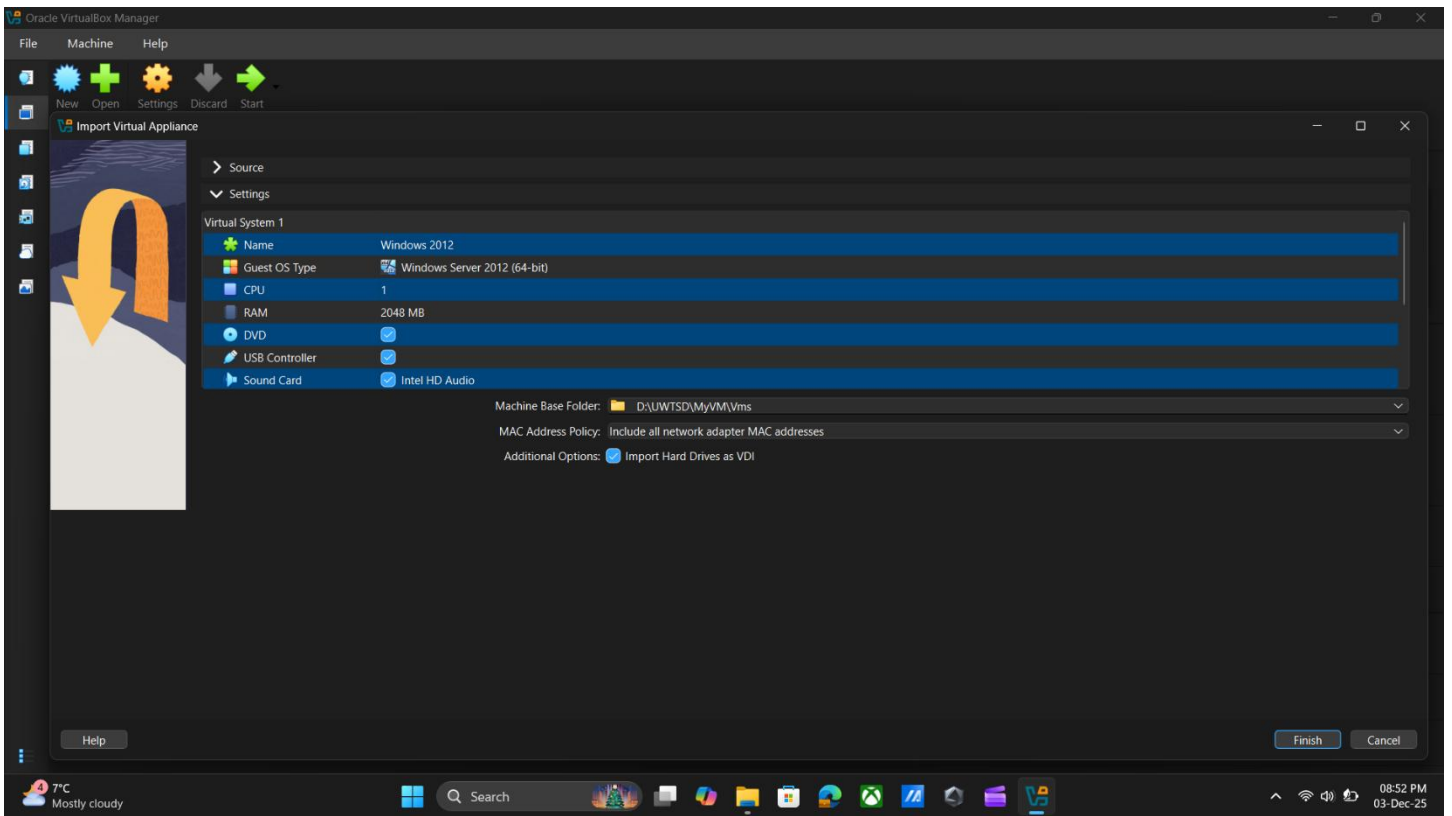


Figure 19: Installation process of R&D - 3

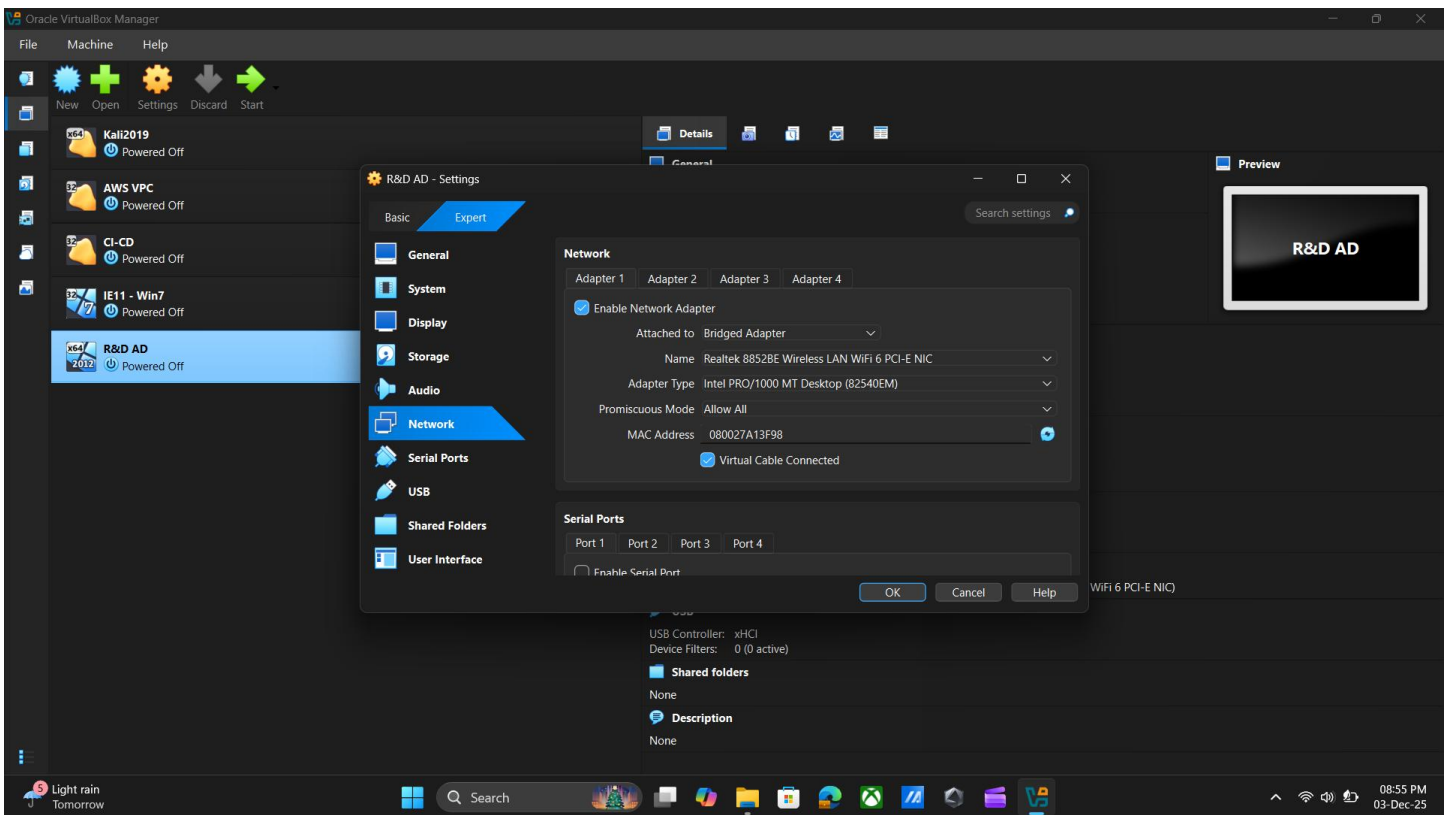


Figure 20: Installation process of R&D - 4

The Figure 21 below shows that, after all the installation, the VirtualBox should be like this.

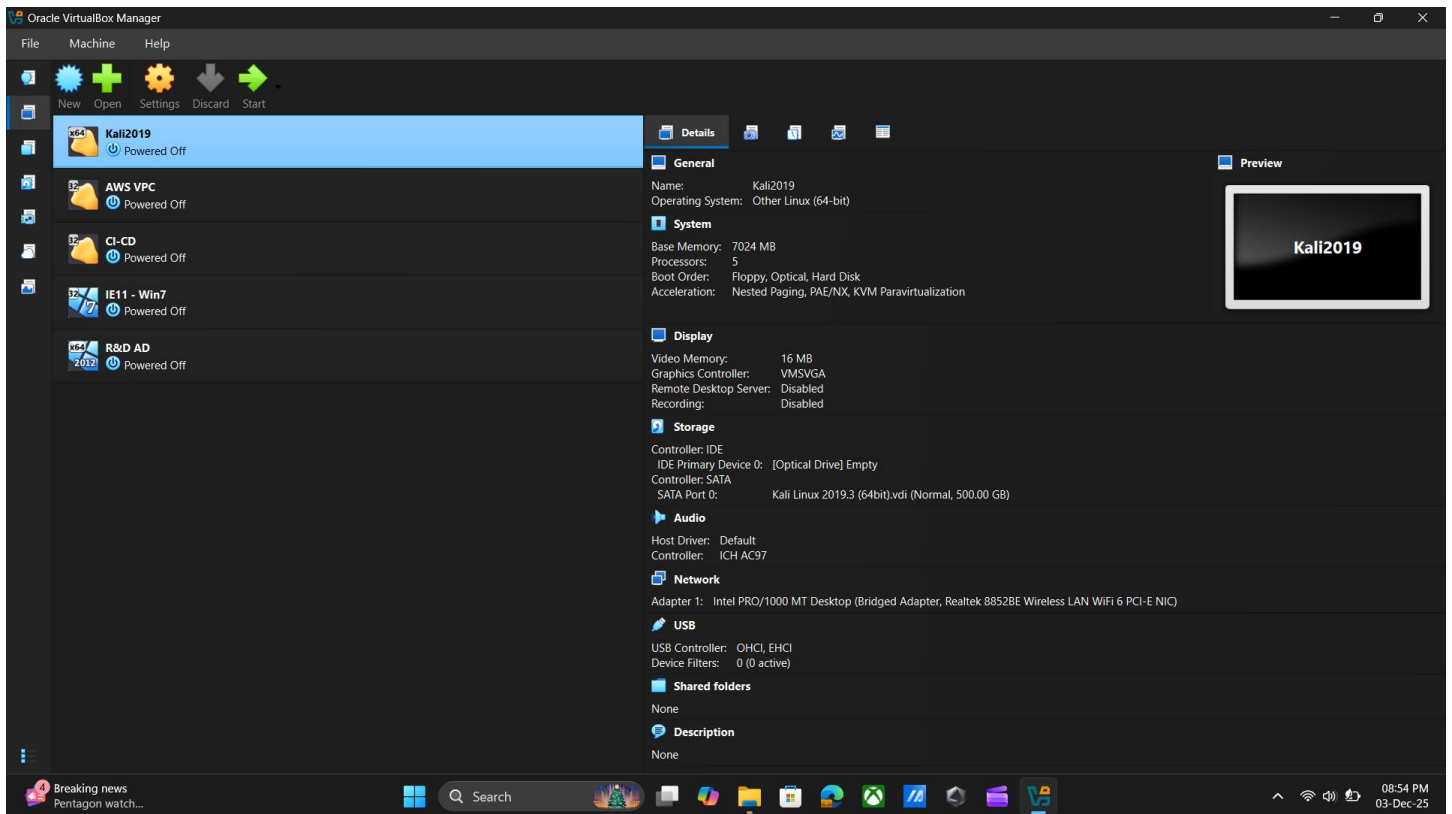


Figure 21: The whole environment

6.1.2.3 Execution Approach

The attack simulation is conducted with caution to prevent any harm. The method uses system tools and moderate, low-profile operations to remain quiet and less noticeable. There are no actual exploits or malicious behaviors. Instead, the experiment demonstrates how data may be accessed and shared safely in an academic atmosphere.

- Kali to AWS VPC -

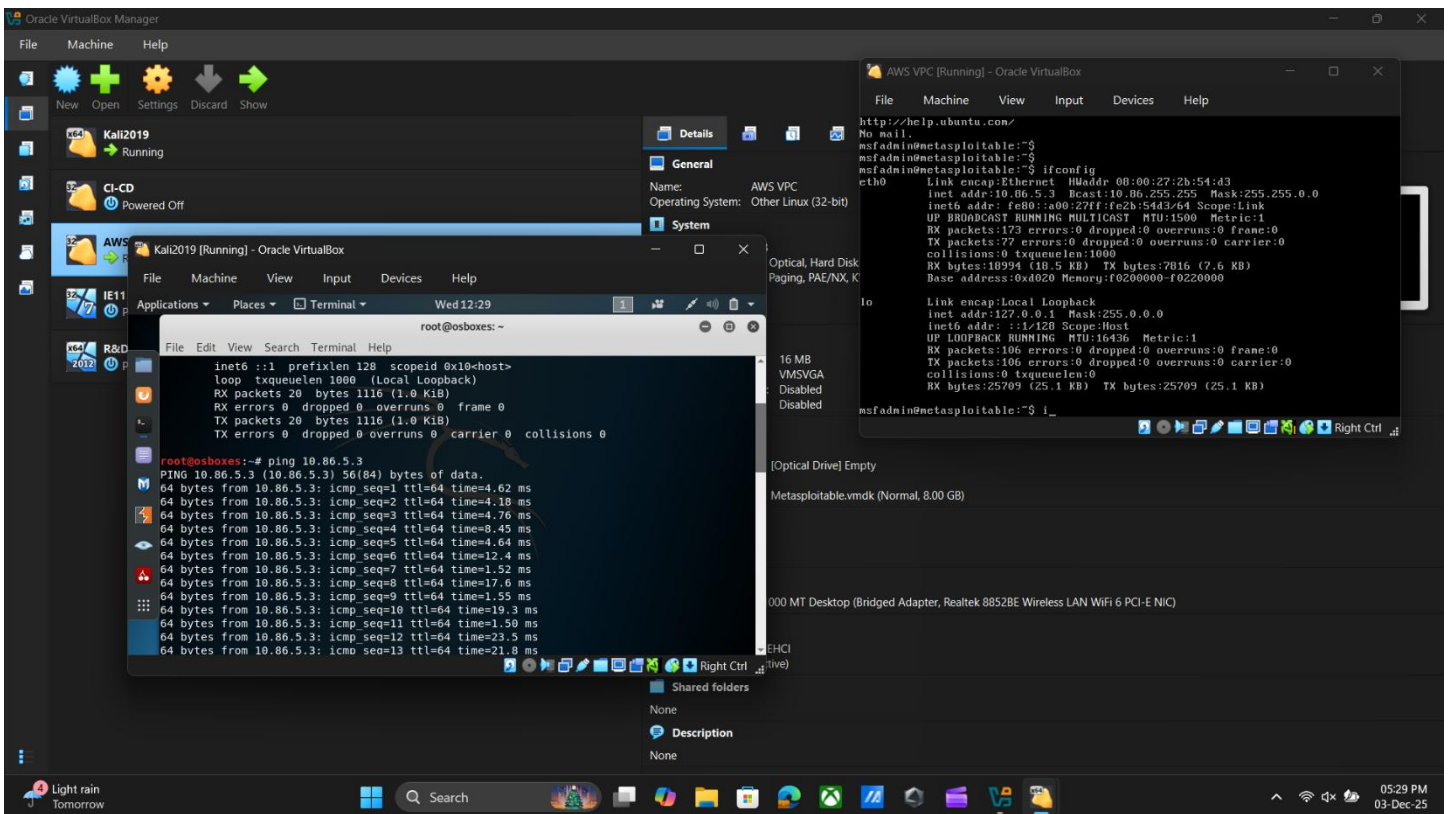


Figure 22: Ping test from Kali to AWS VPC process

Figure 22 shows a successful ping test from the Kali machine to the AWS VPC, confirming that network connectivity between the two environments is working.

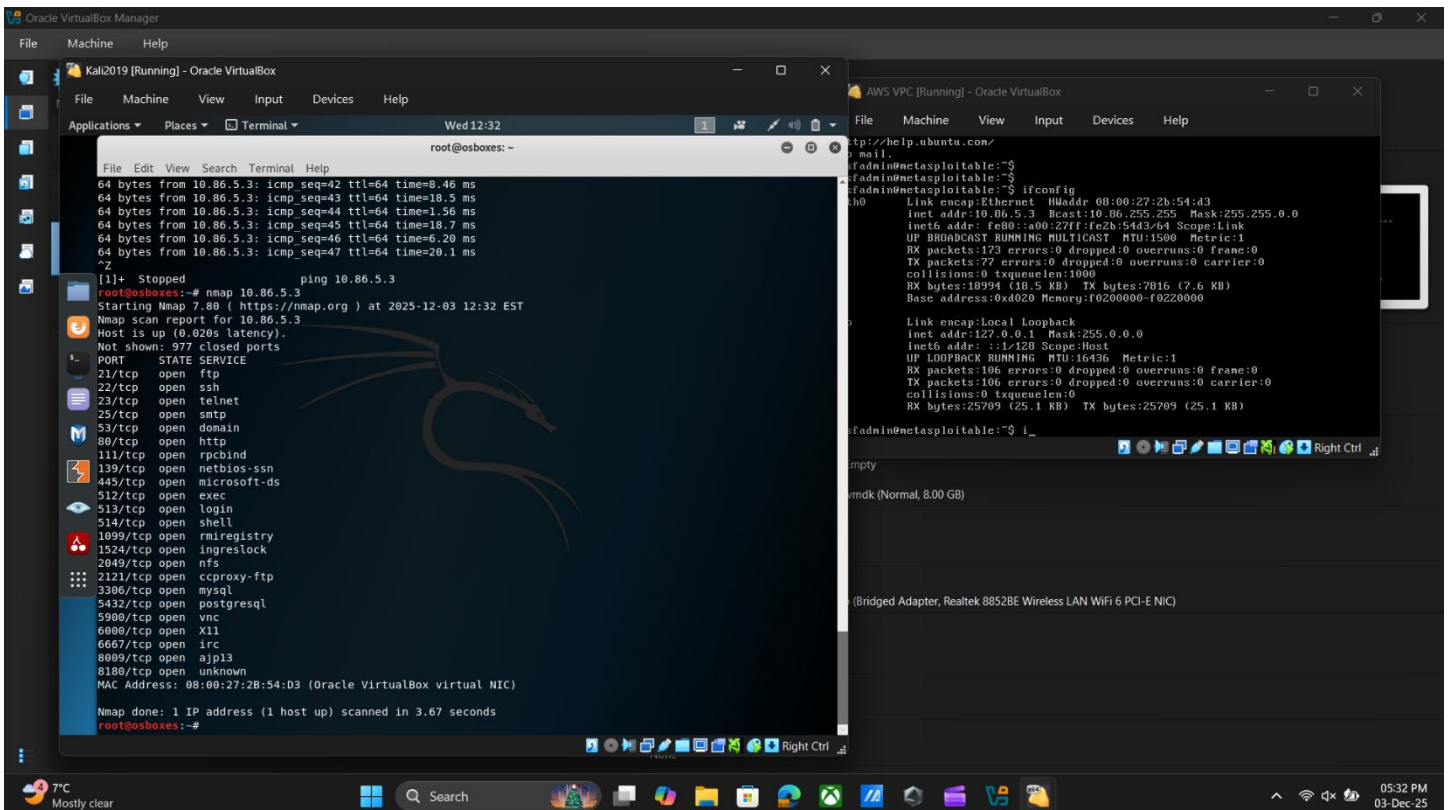


Figure 23: Nmap from Kali to AWS VPC

Figure 23 explain the use of Nmap from Kali to check connectivity and discover open services on the AWS environment.

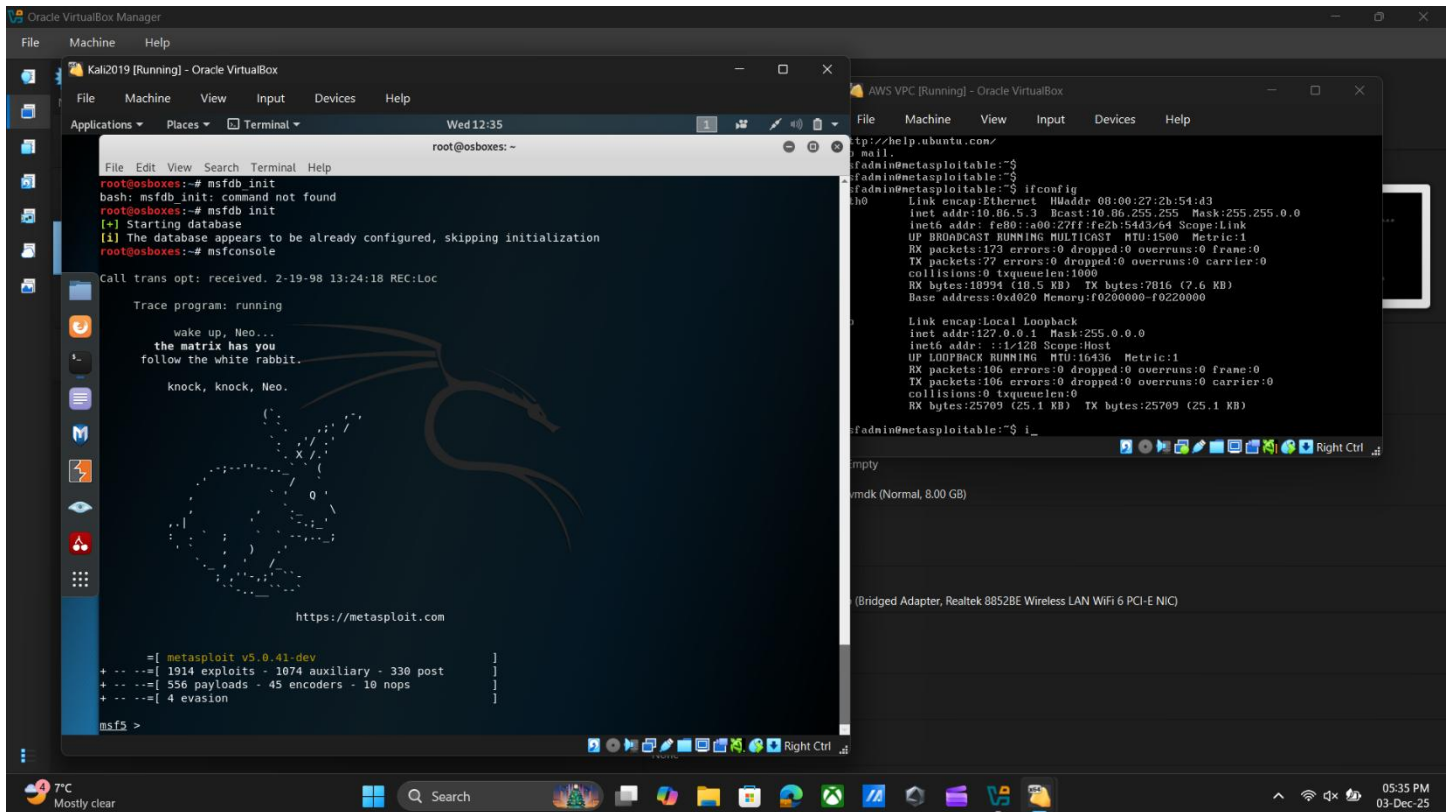


Figure 24: Db_nmap from Kali to AWS VPC

Figure 24 illustrates DB_nmap being used from the Kali system to identify accessible database services within the AWS VPC.

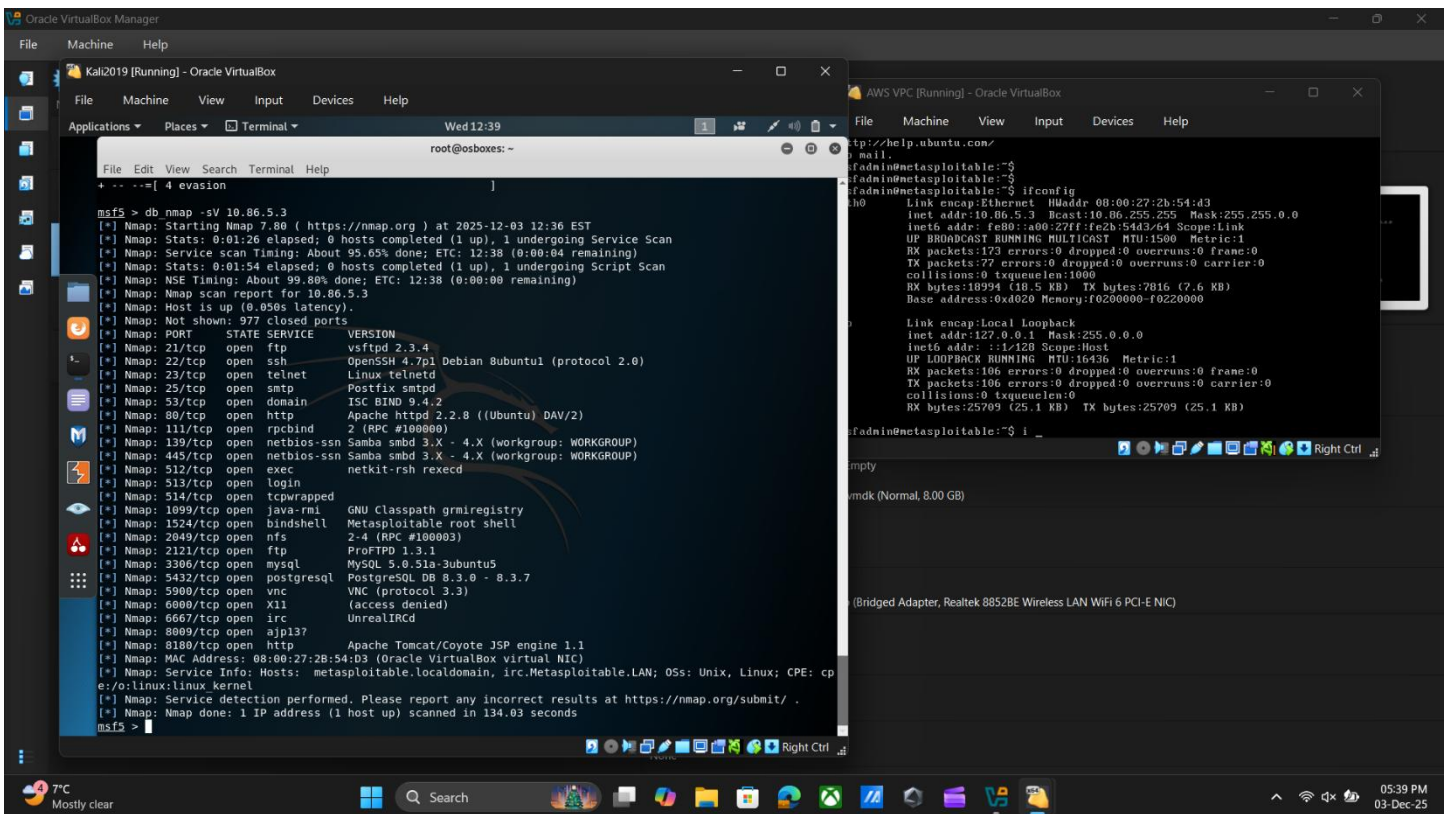


Figure 25: Db_nmap -sV Command from Kali to AWS VPC

Figure 25 db_nmap -sV demonstrates the command being run from Kali to identify database services and their versions within the AWS VPC.

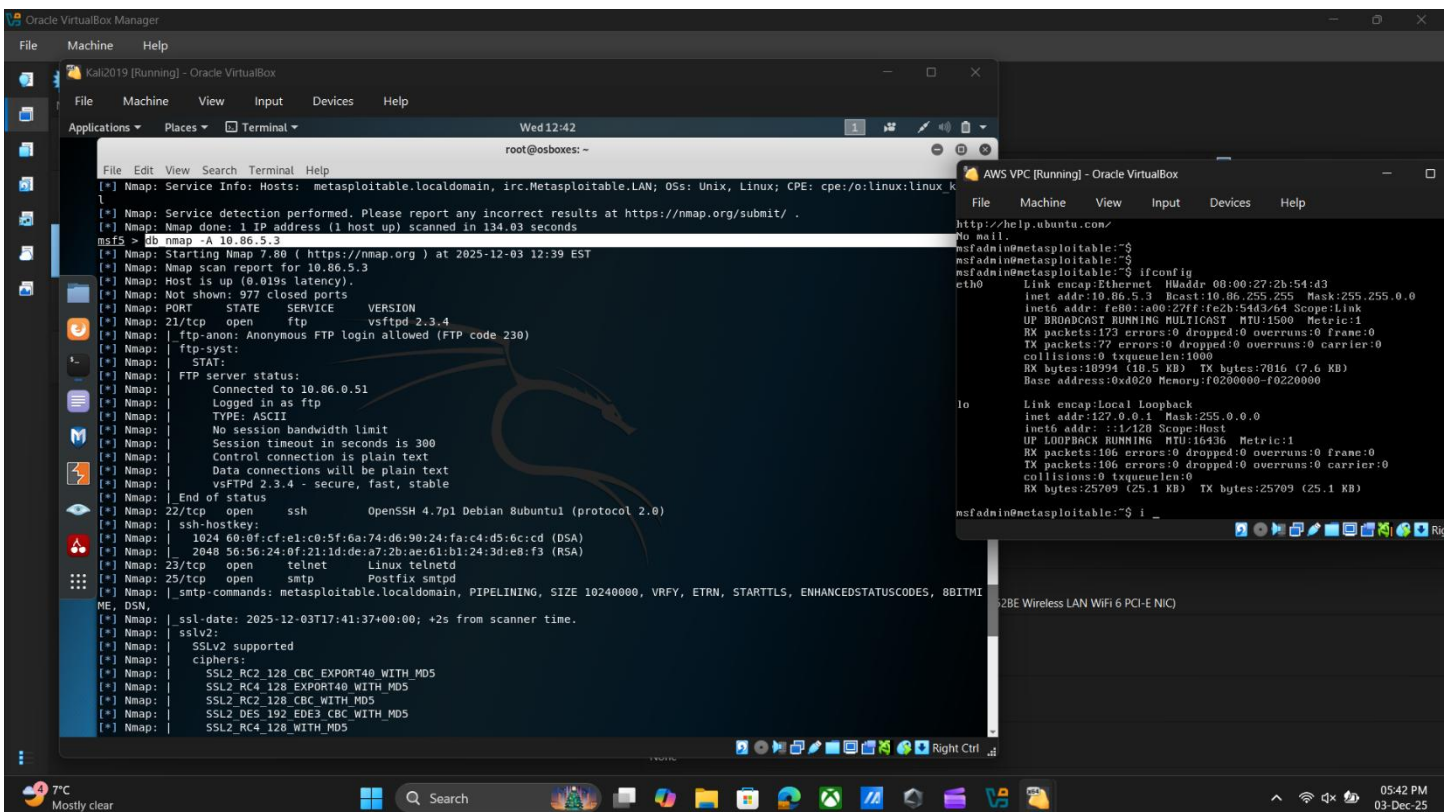


Figure 26: Db_nmap -A Command from Kali to AWS VPC 1

From Figure 26 to Figure 28 the db_nmap -A command being used from Kali to perform an advanced scan, detecting database services, versions, and additional information within the AWS VPC.

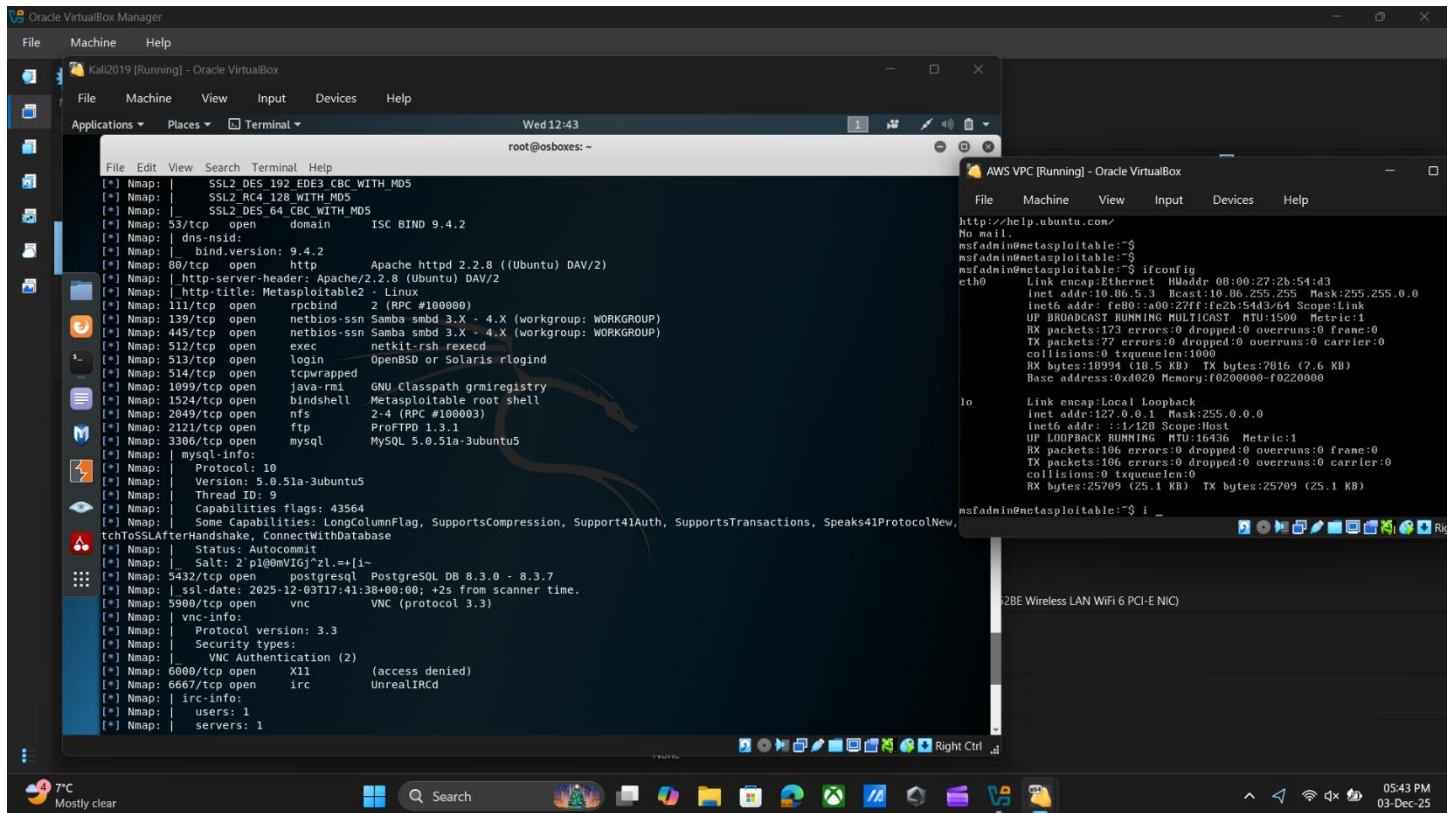


Figure 27: Db_nmap -A Command from Kali to AWS VPC 2

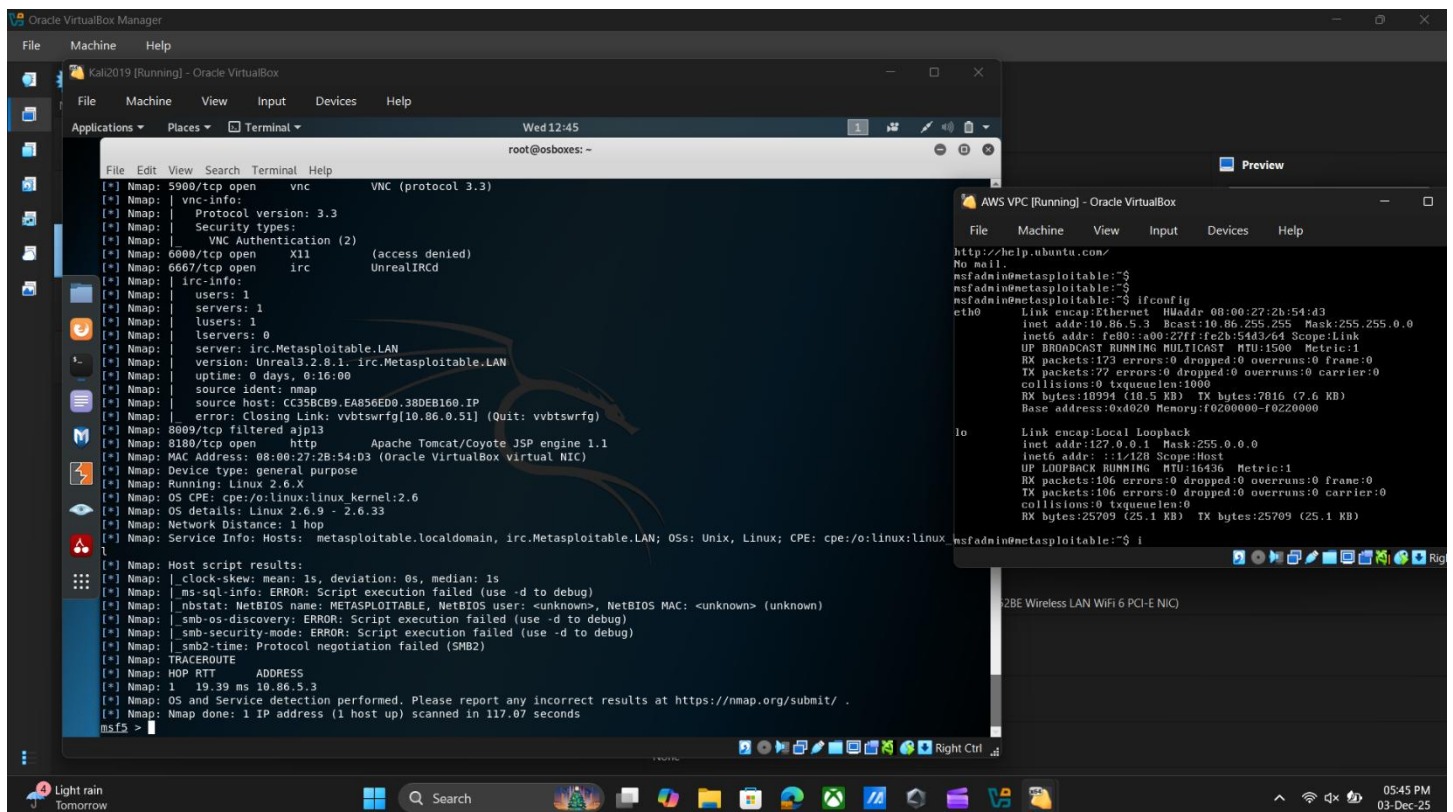


Figure 28: Db_nmap -A command from Kali to AWS VPC 3

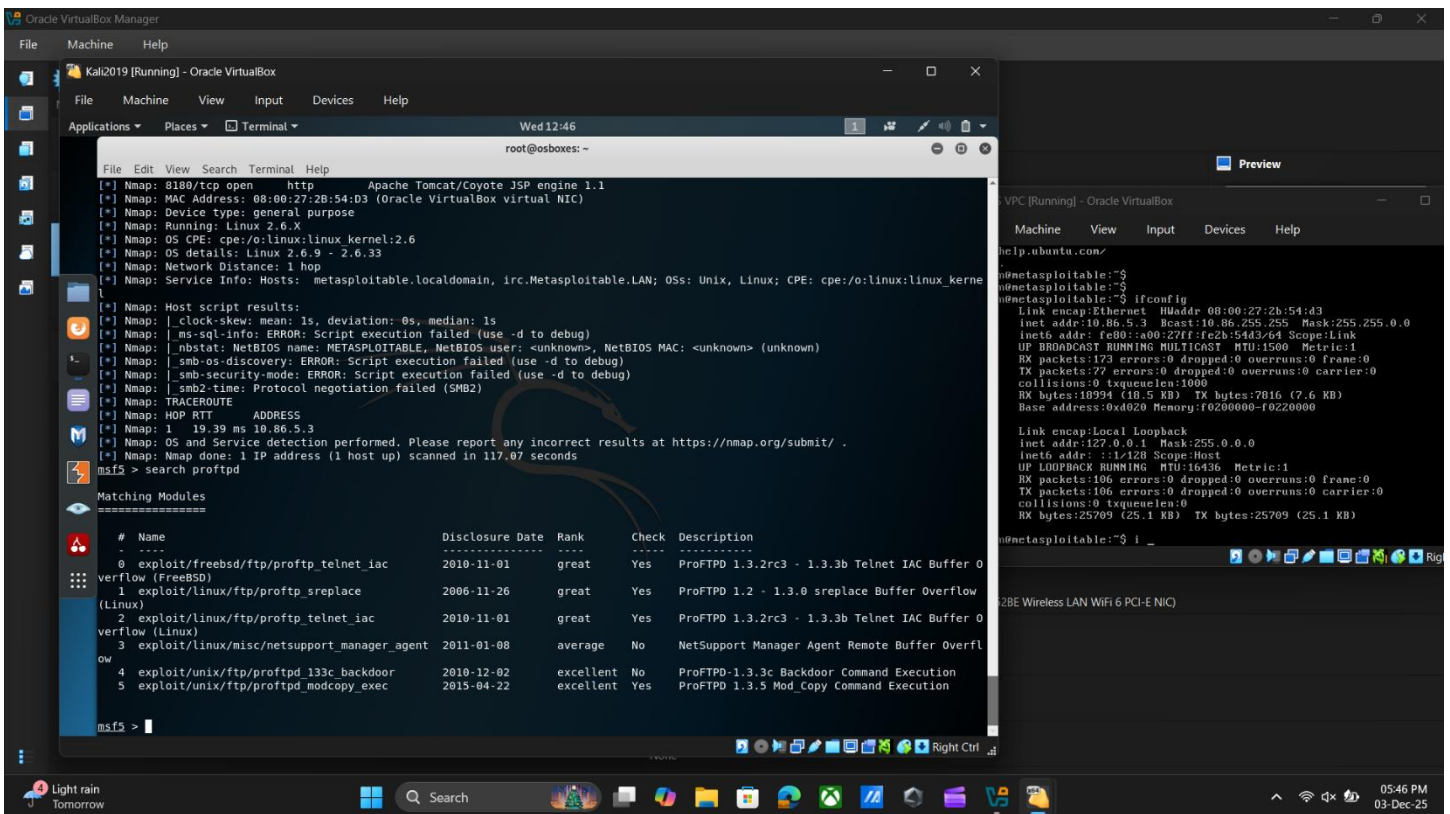


Figure 29: Search ftpd from Kali to AWS VPC

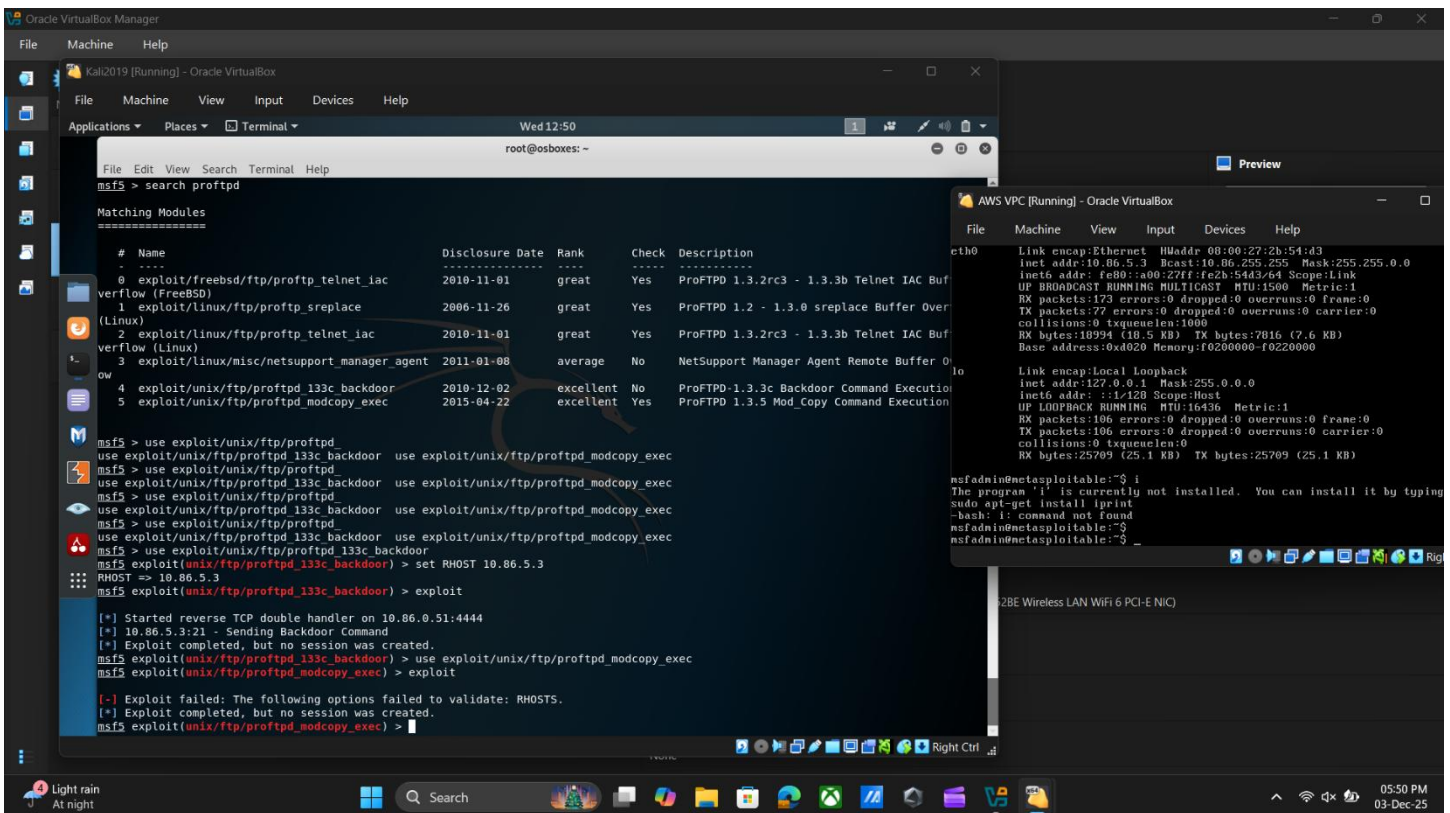


Figure 30: Exploiting a vulnerable Proftpd service from Kali to AWS VPC

Figure 30 shows how an attacker could use a known weakness in the Proftpd service to gain access.

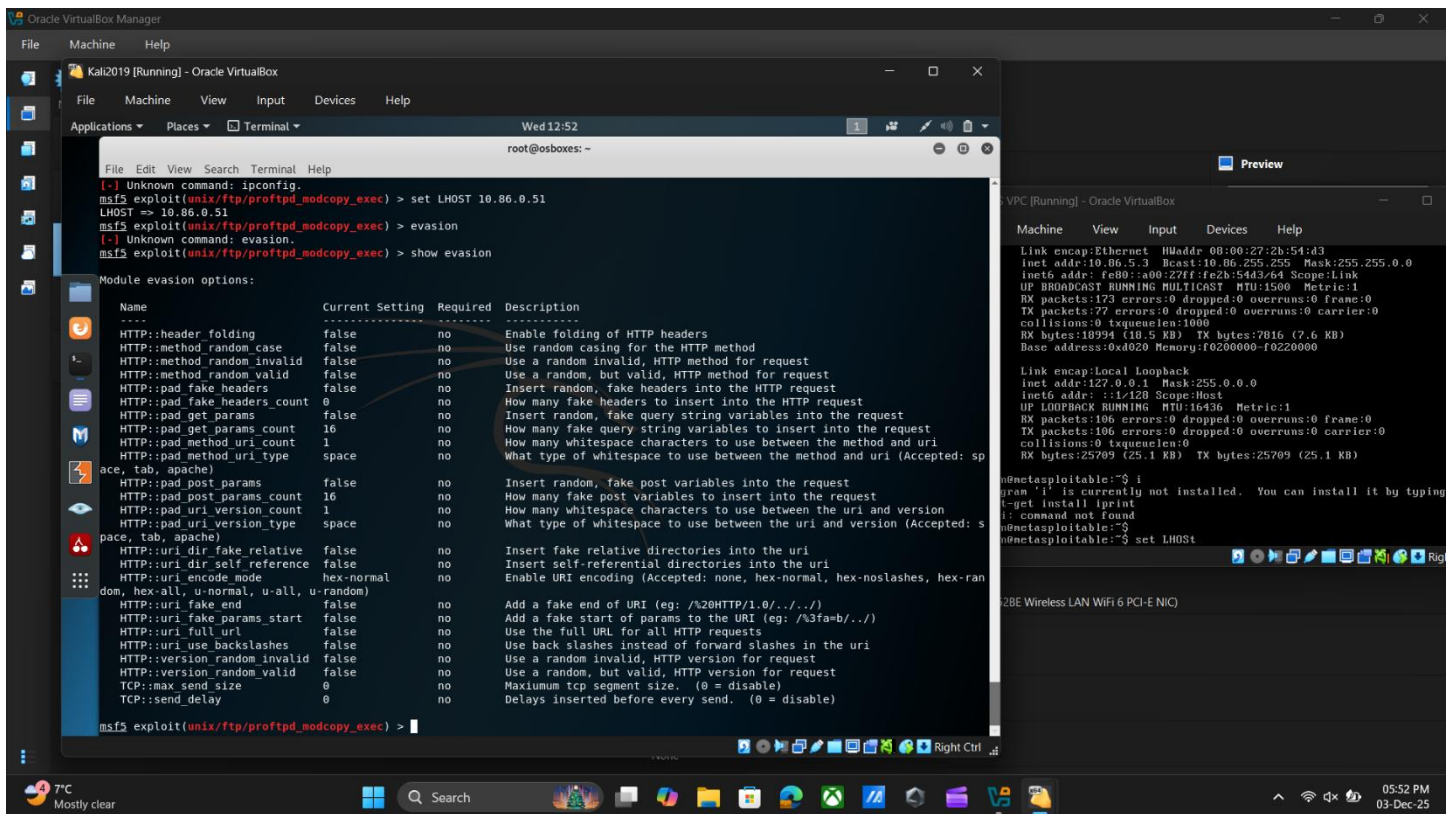


Figure 31 demonstrates how basic evasion techniques are used from Kali to communicate with AWS while avoiding obvious detection.

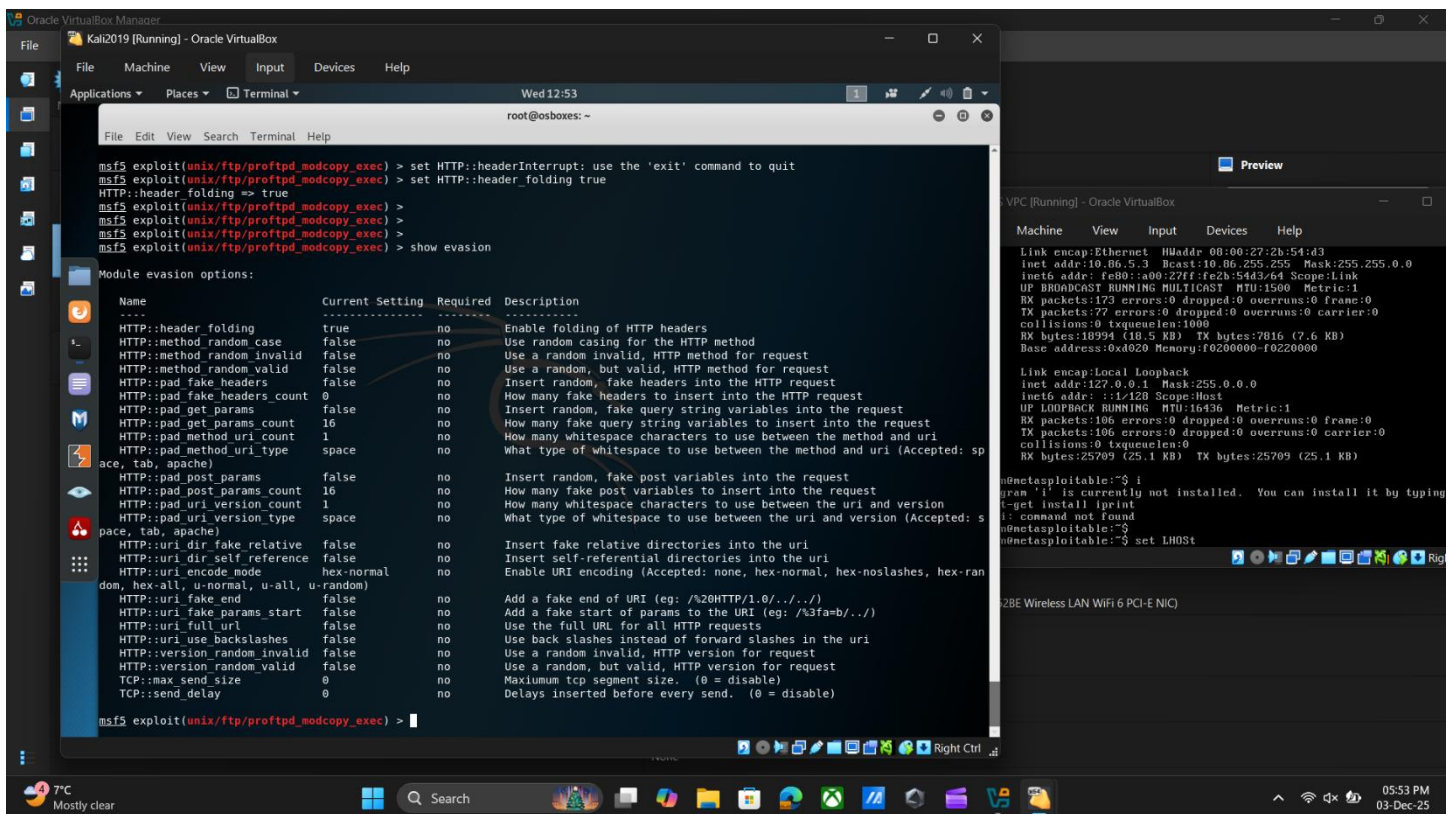


Figure 32 portraits, sending HTTP headers from Kali to AWS, and using simple evasion techniques to simulate.

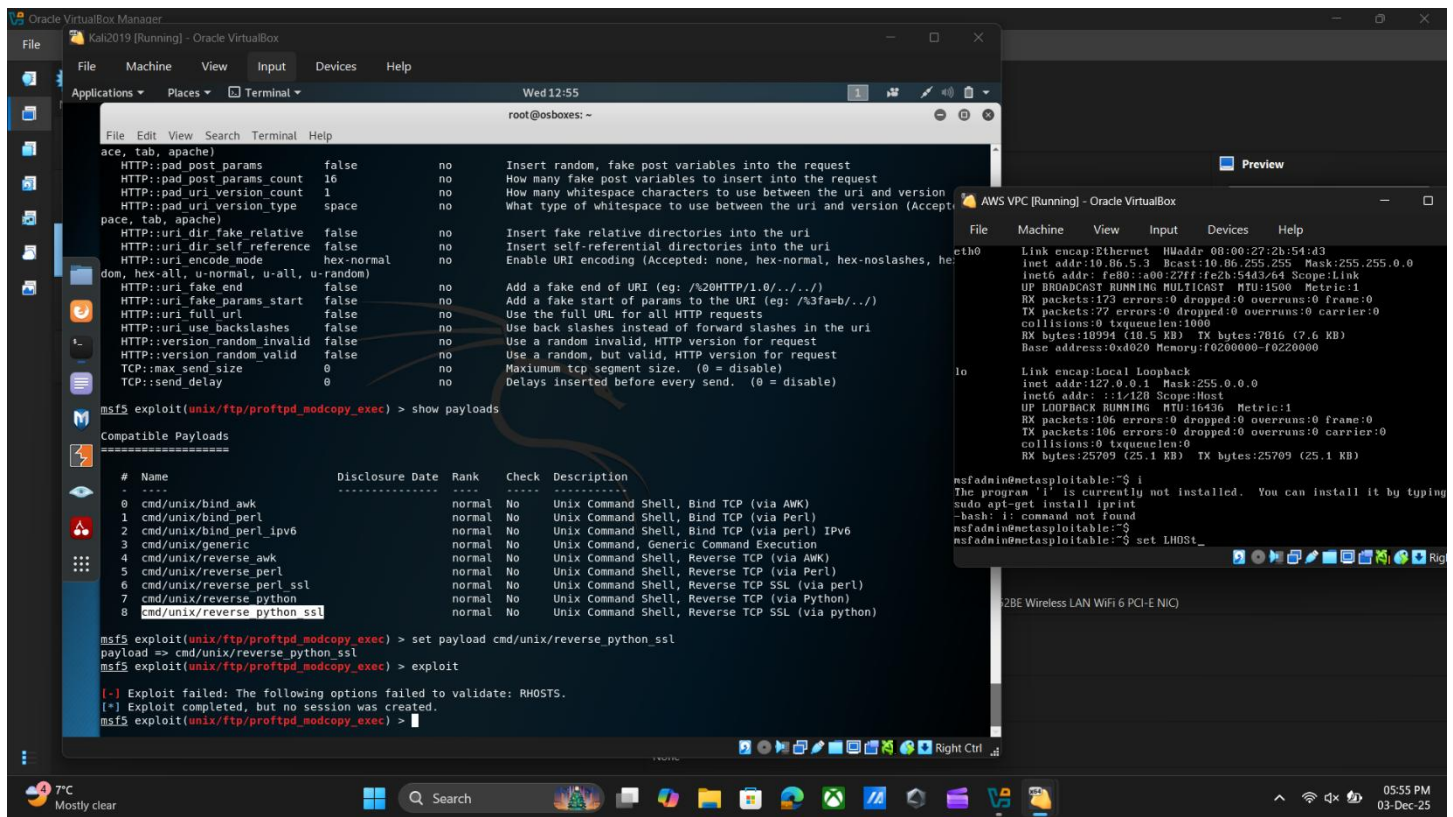


Figure 33: Payload Configuration and Exploitation from Kali to AWS VPC

Figure 33 shows a test payload is selected and used to see how an attacker could gain access to a target system.

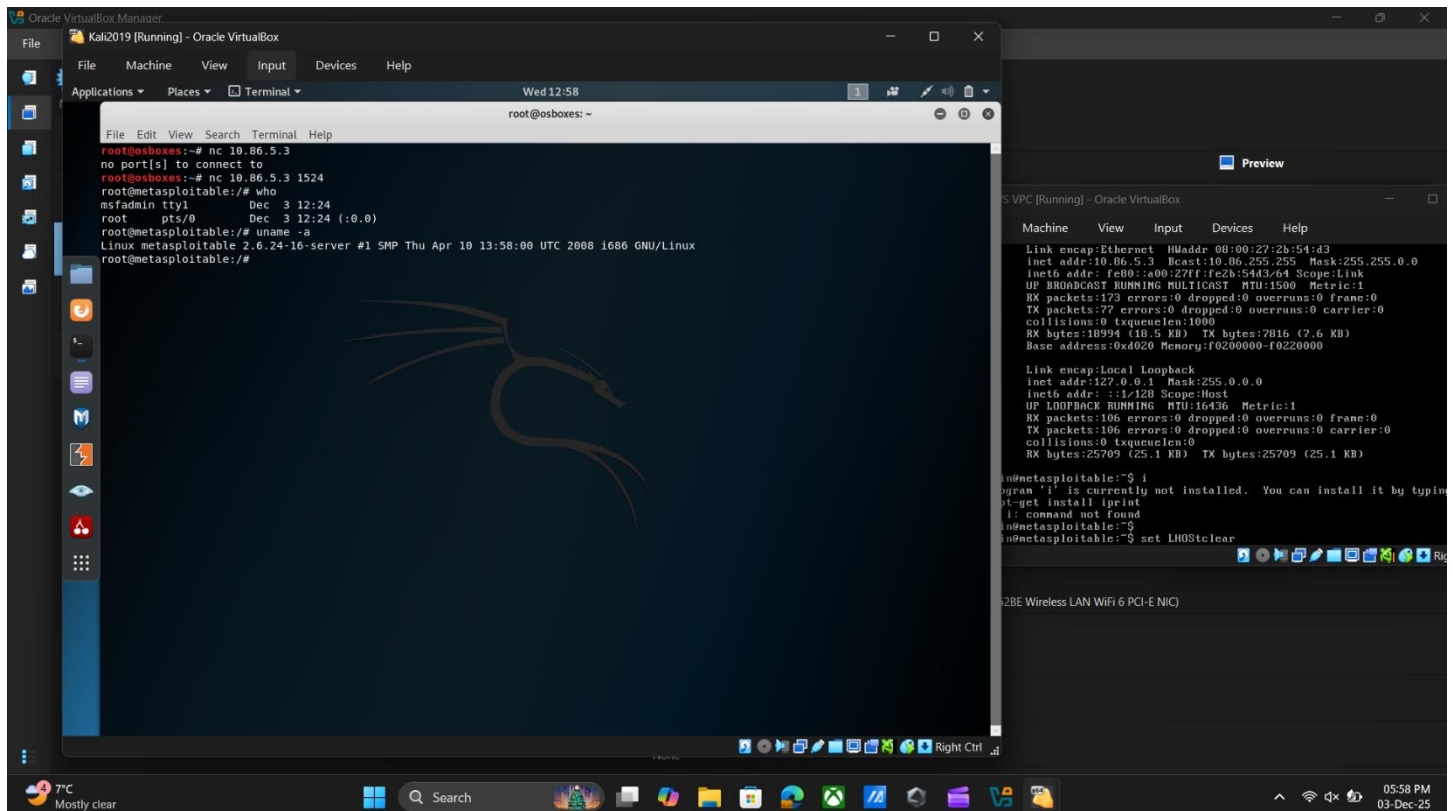


Figure 35: Netcat connection and system verification from Kali to AWS VPC

Figure 35 shows connecting to the target using Netcat and running basic commands to confirm access and system details in the lab.

- From Kali to R&D AD -

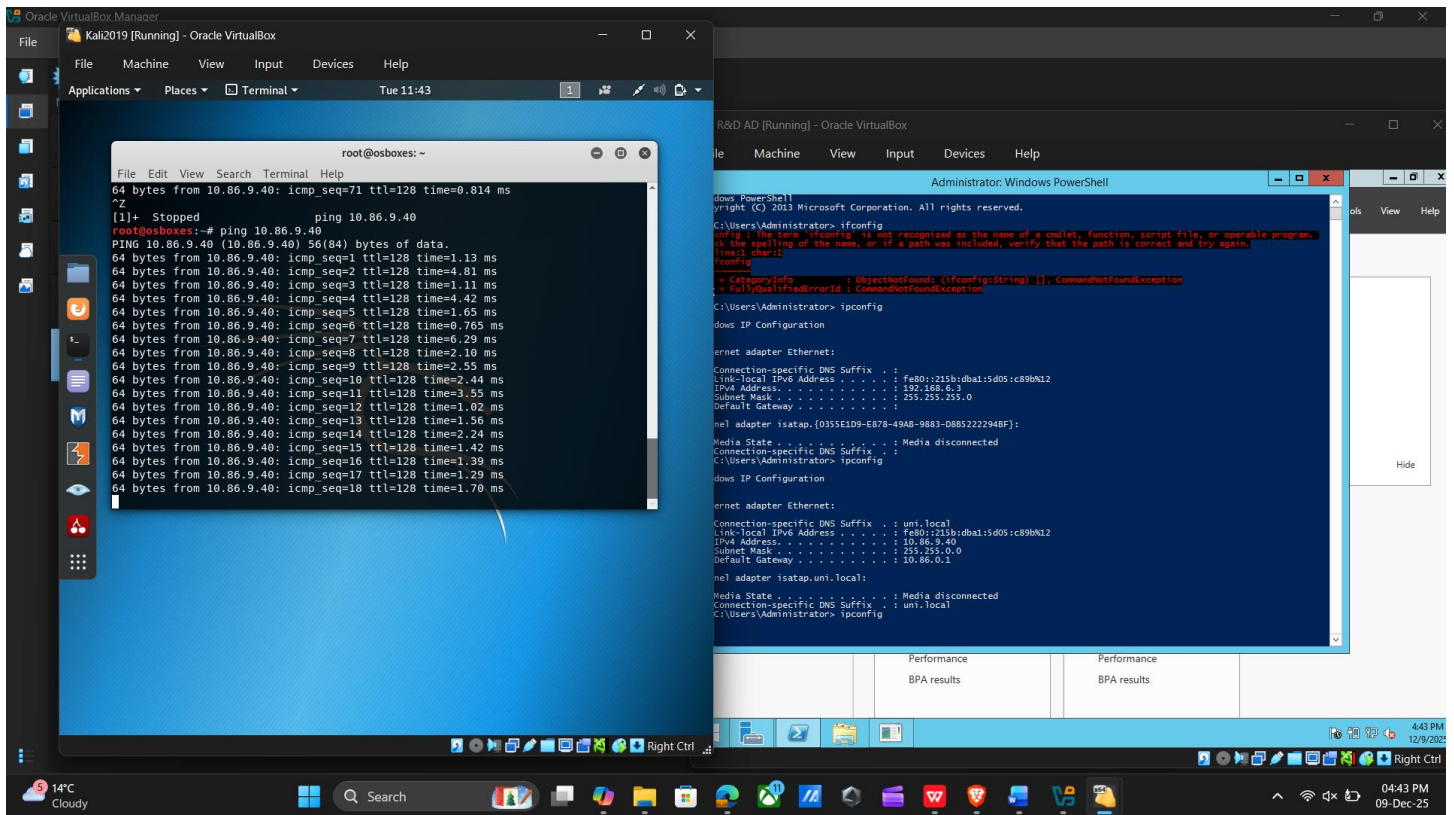


Figure 36: Ping test from Kali to R&D AD

According to Figure 36 a successful ping from the Kali machine to the R&D AD.

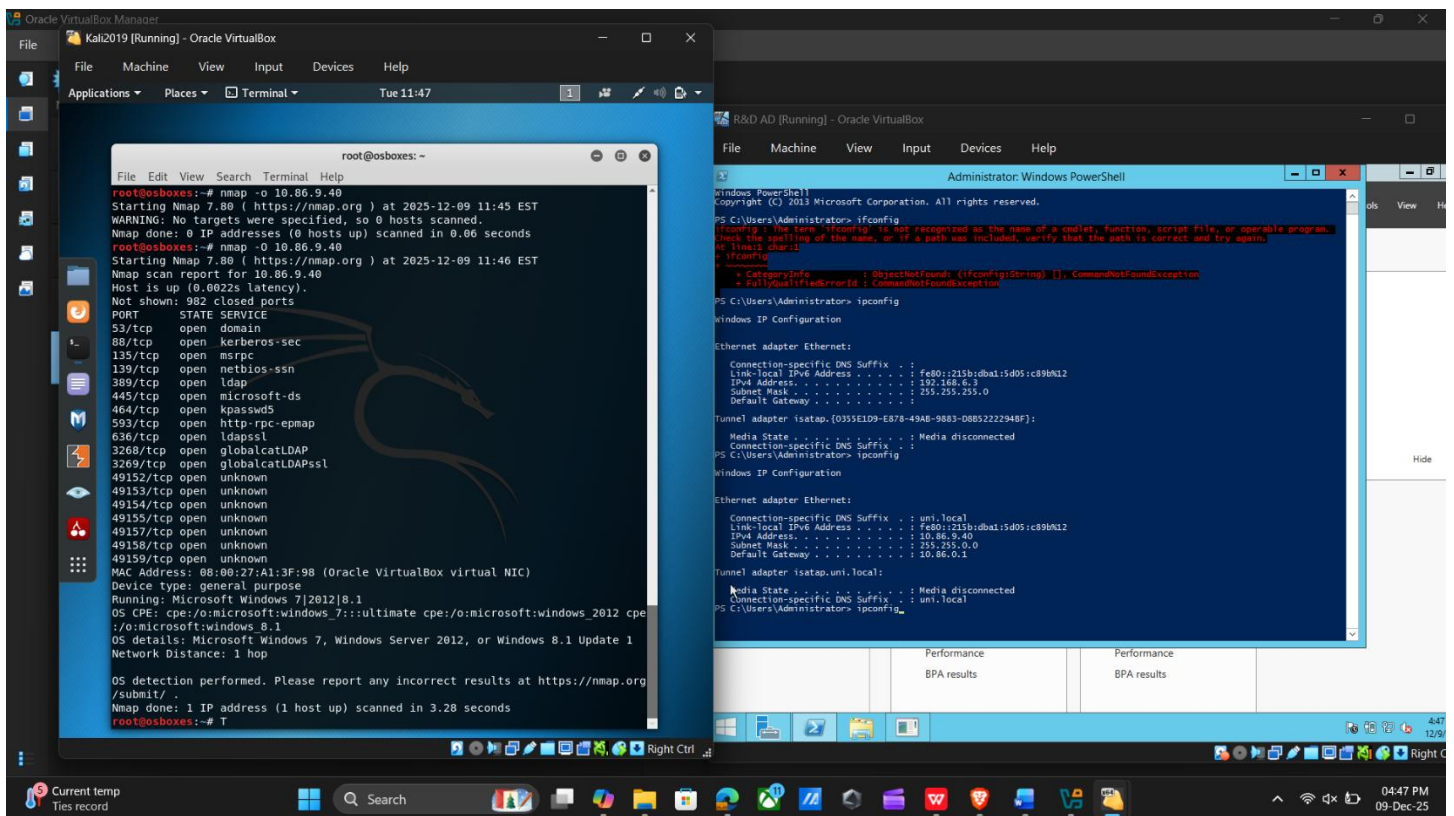


Figure 37: Operating system detection scan from Kali to Active Directory

Figure 37 shows the use of Nmap OS detection to identify the operating system of the R&D AD server.

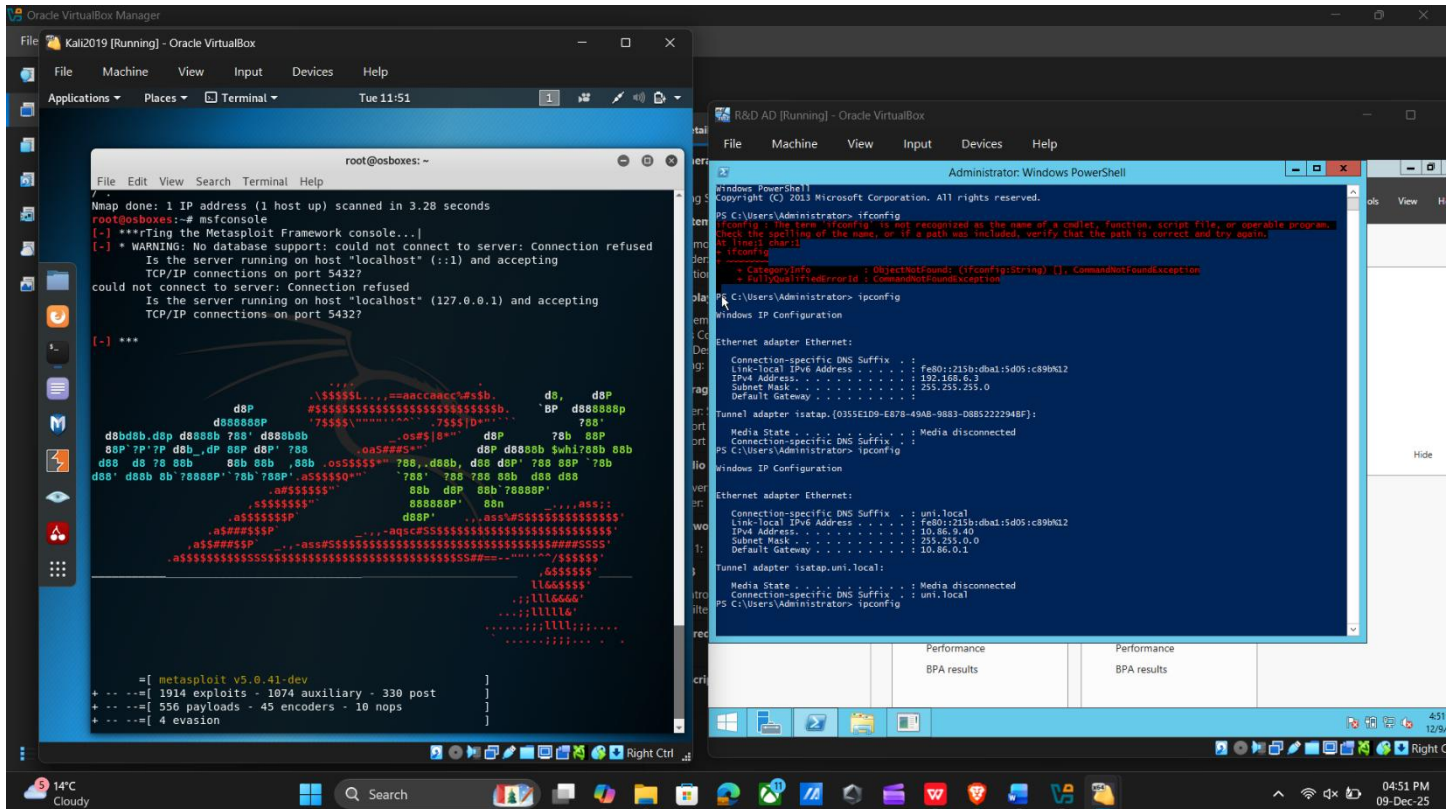


Figure 38: Metasploit console access from Kali to R&D AD

Figure 38 Demonstrate Metasploit being used from Kali to interact with the R&D AD system.

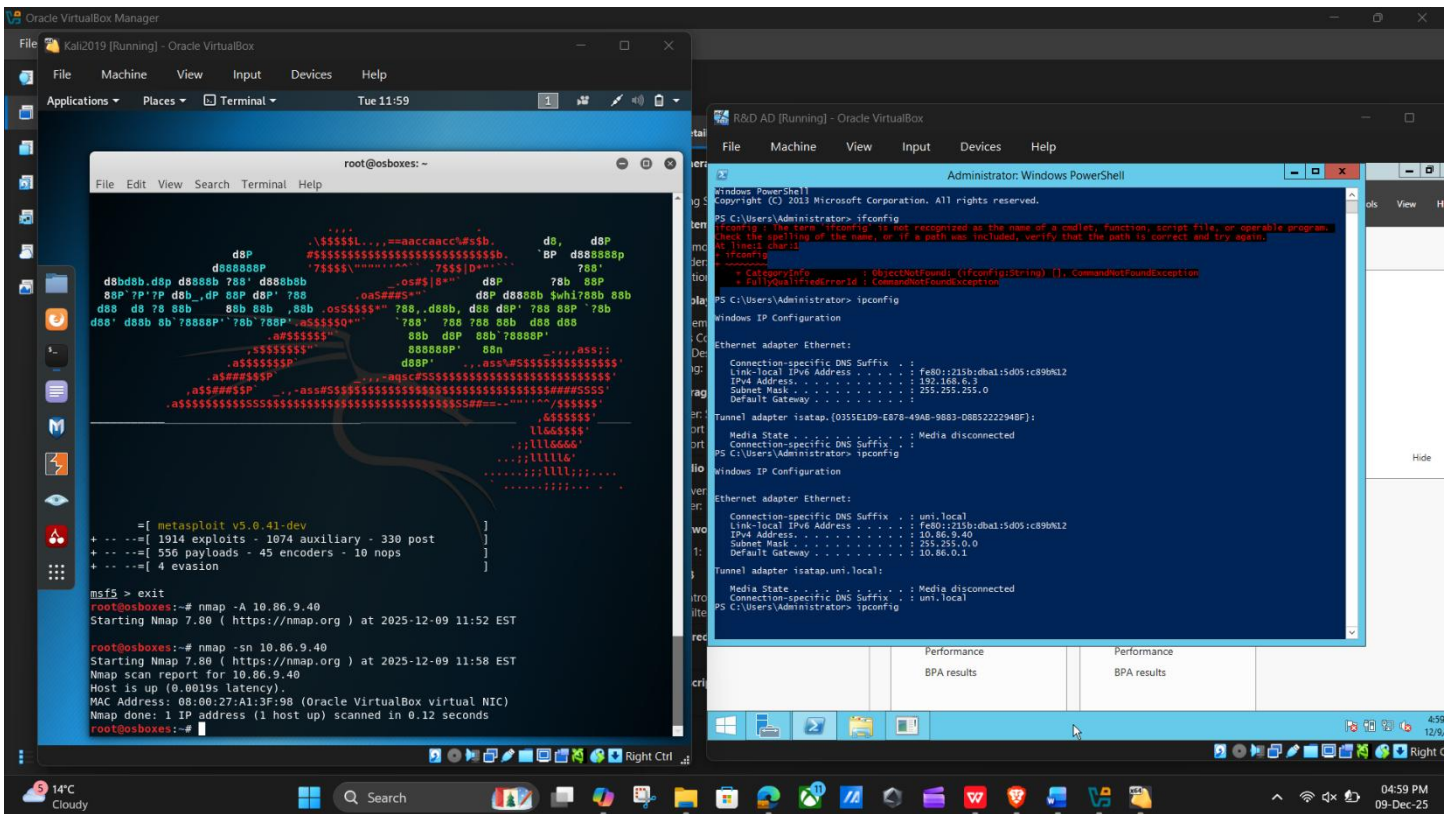


Figure 39: Host discovery scan from Kali to R&D AD

The Figure 39 shows an Nmap ping scan used to confirm that the Active Directory server is online and reachable.

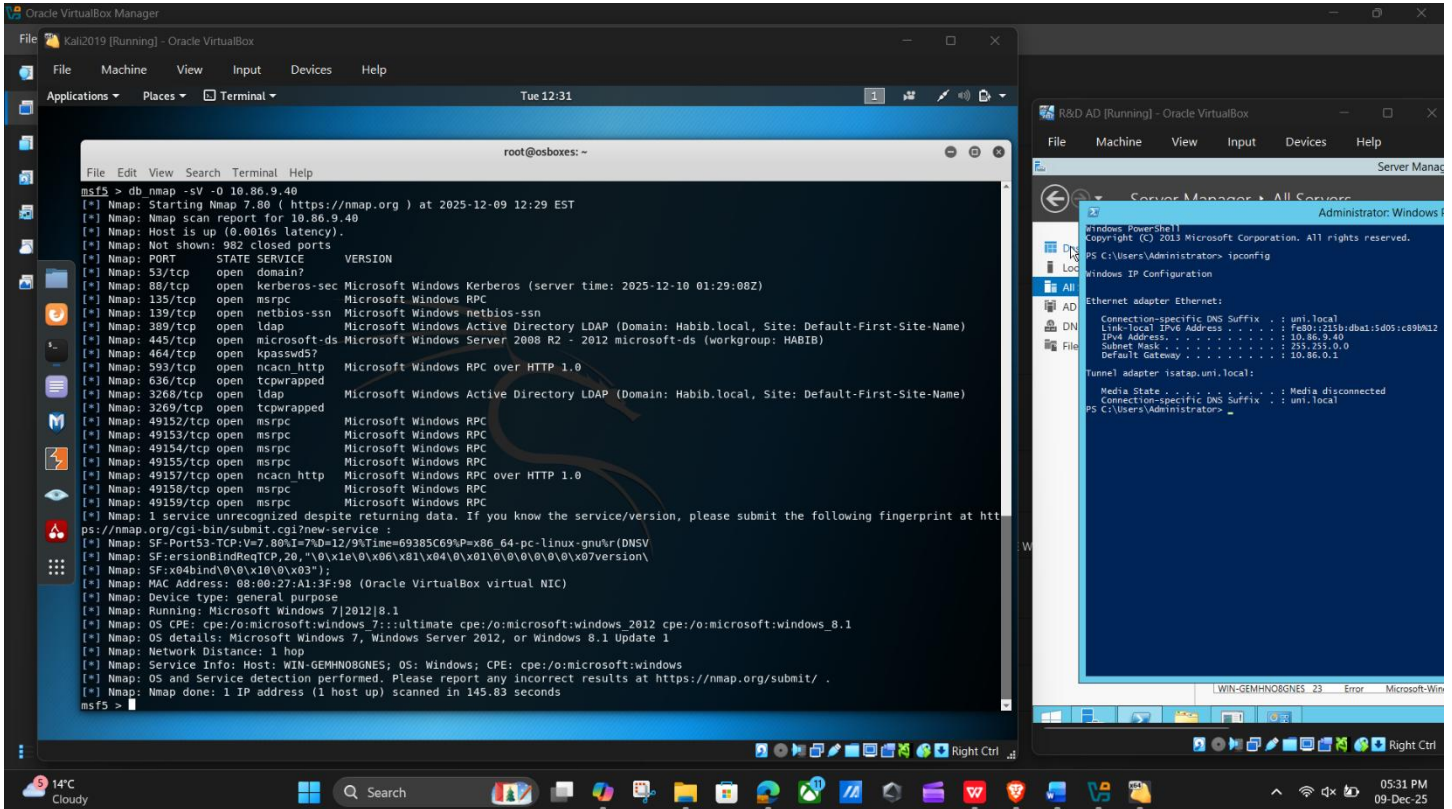


Figure 40: Database service scan using db_nmap from Kali to R&D AD

Highlight in Figure 40, db_nmap is used to identify database services and their versions on the target system.

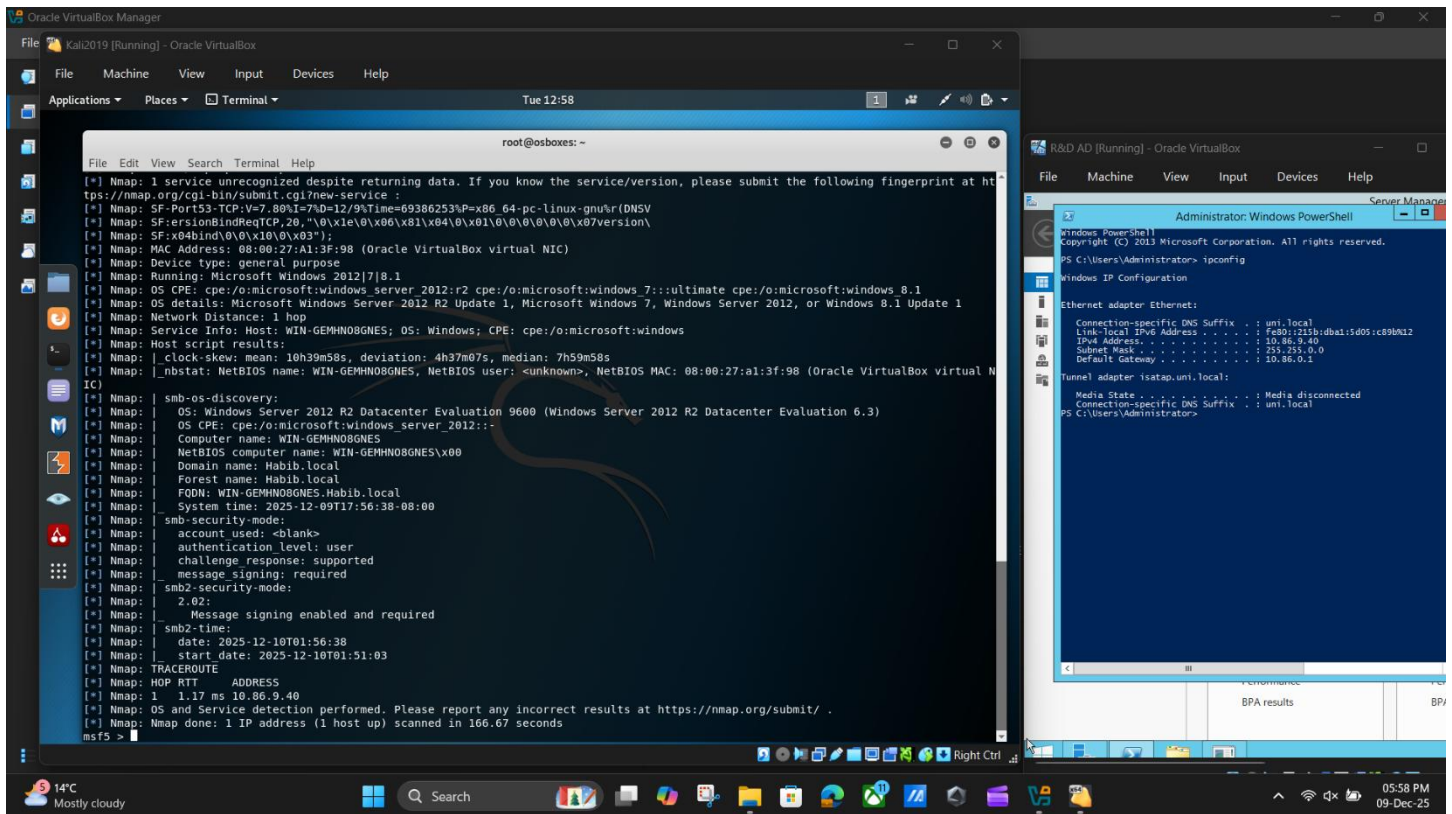


Figure 43: Aggressive database and service scan using db_nmap from Kali to R&D AD 2

The Figure 42 and Figure 43 demonstrates db_nmap performing a detailed, aggressive scan to gather service, version, and system information during testing.

- From Kali to CI-CD -

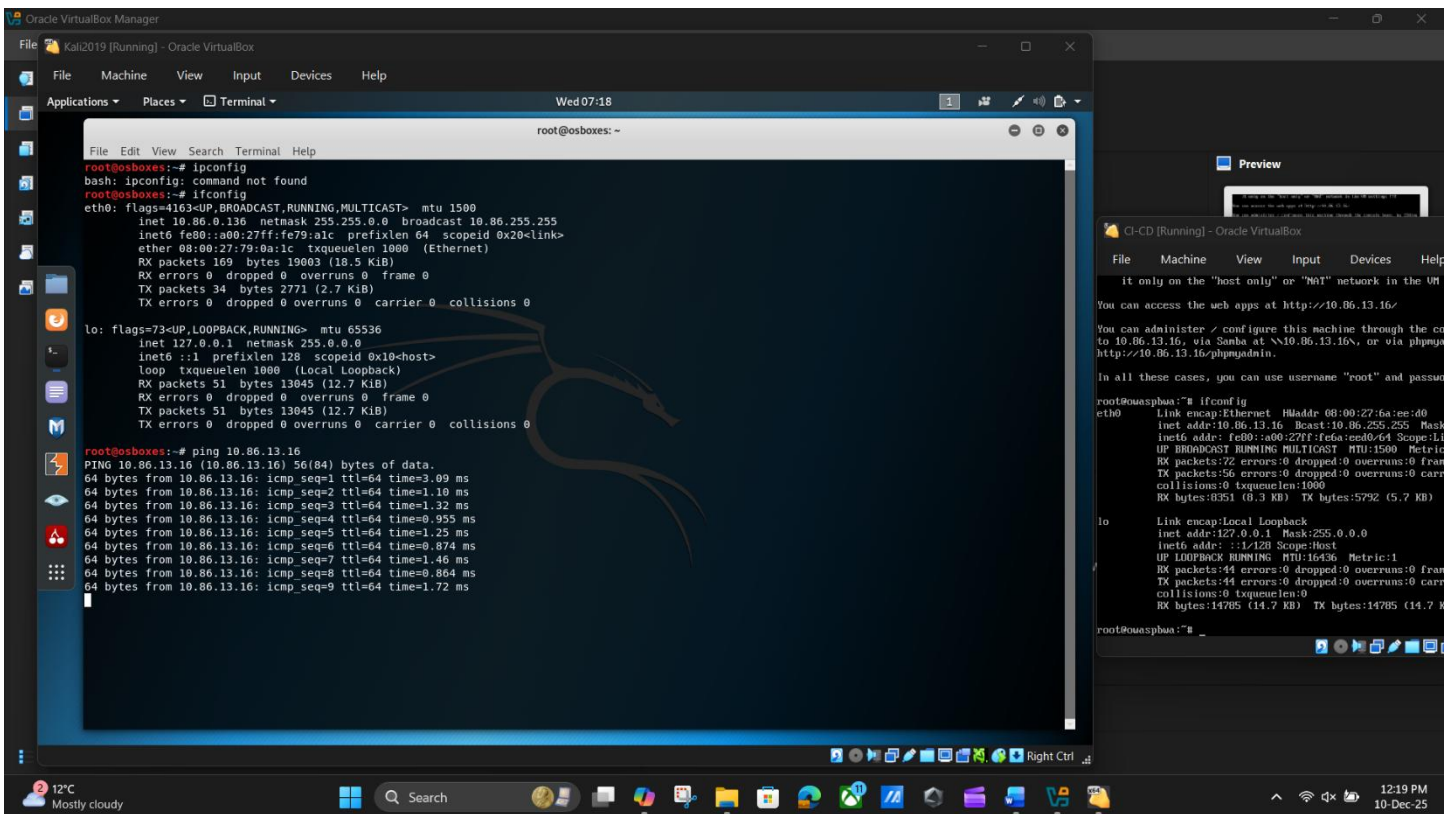


Figure 44: Ping test from Kali to CI-CD

Figure 44 shows a successful ping from the Kali to CI-CD, confirming network connectivity.

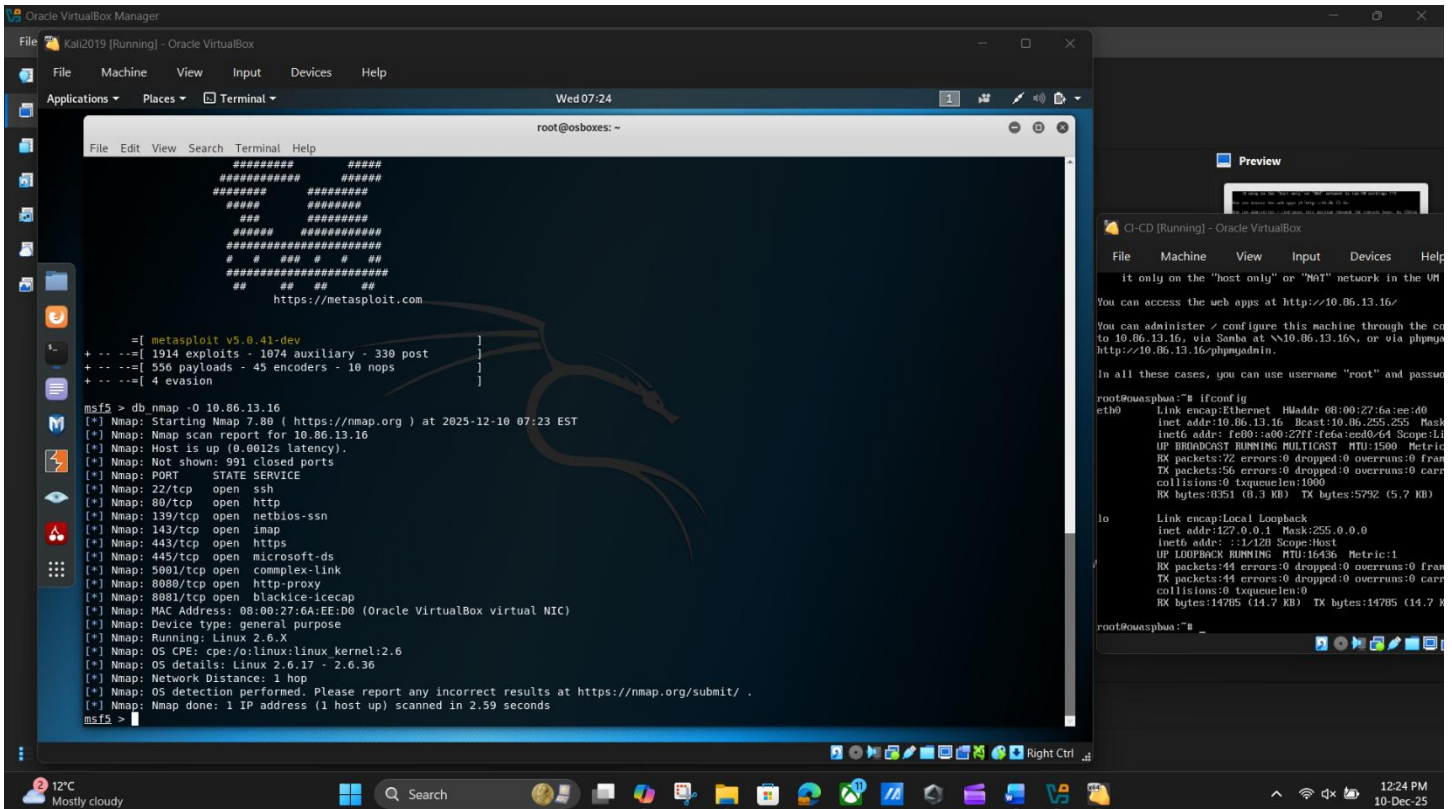


Figure 45: Operating system detection scan from Kali to CI-CD

Figure 45 reveals that db_nmap is being used to identify the operating system of the CI-CD.

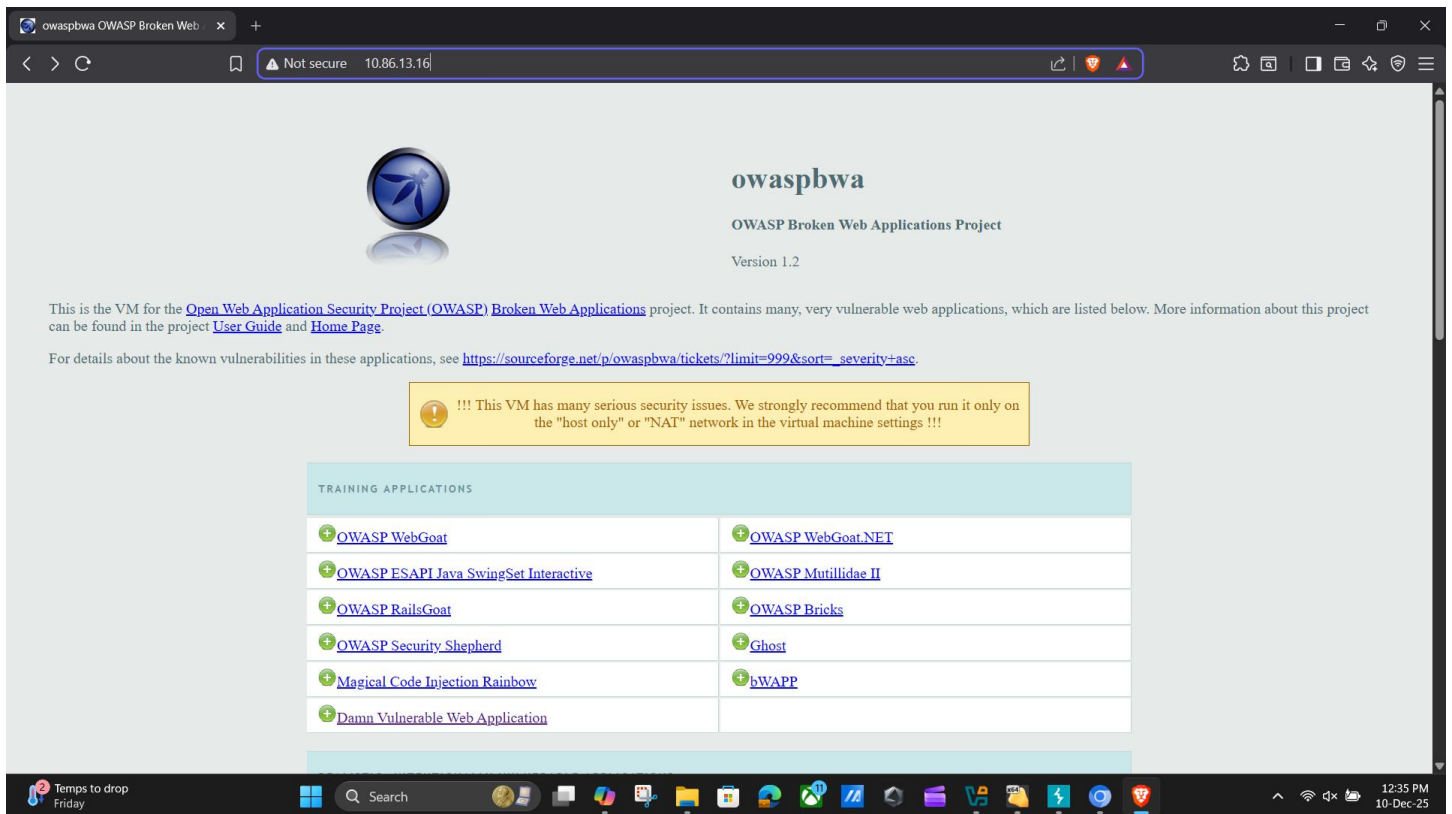


Figure 46: Web traffic inspection using Burp Suite - 1

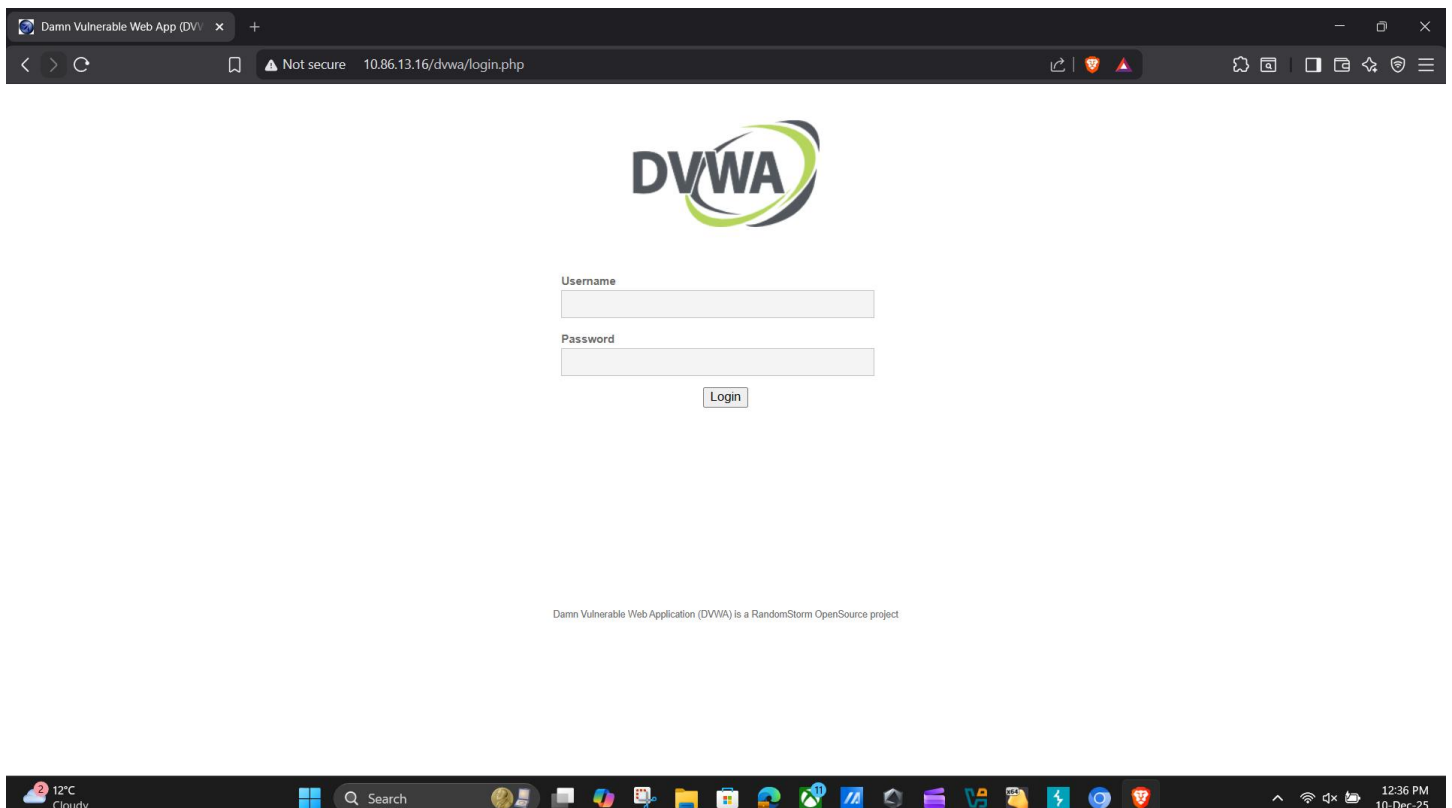


Figure 47: Web traffic inspection using Burp Suite - 2

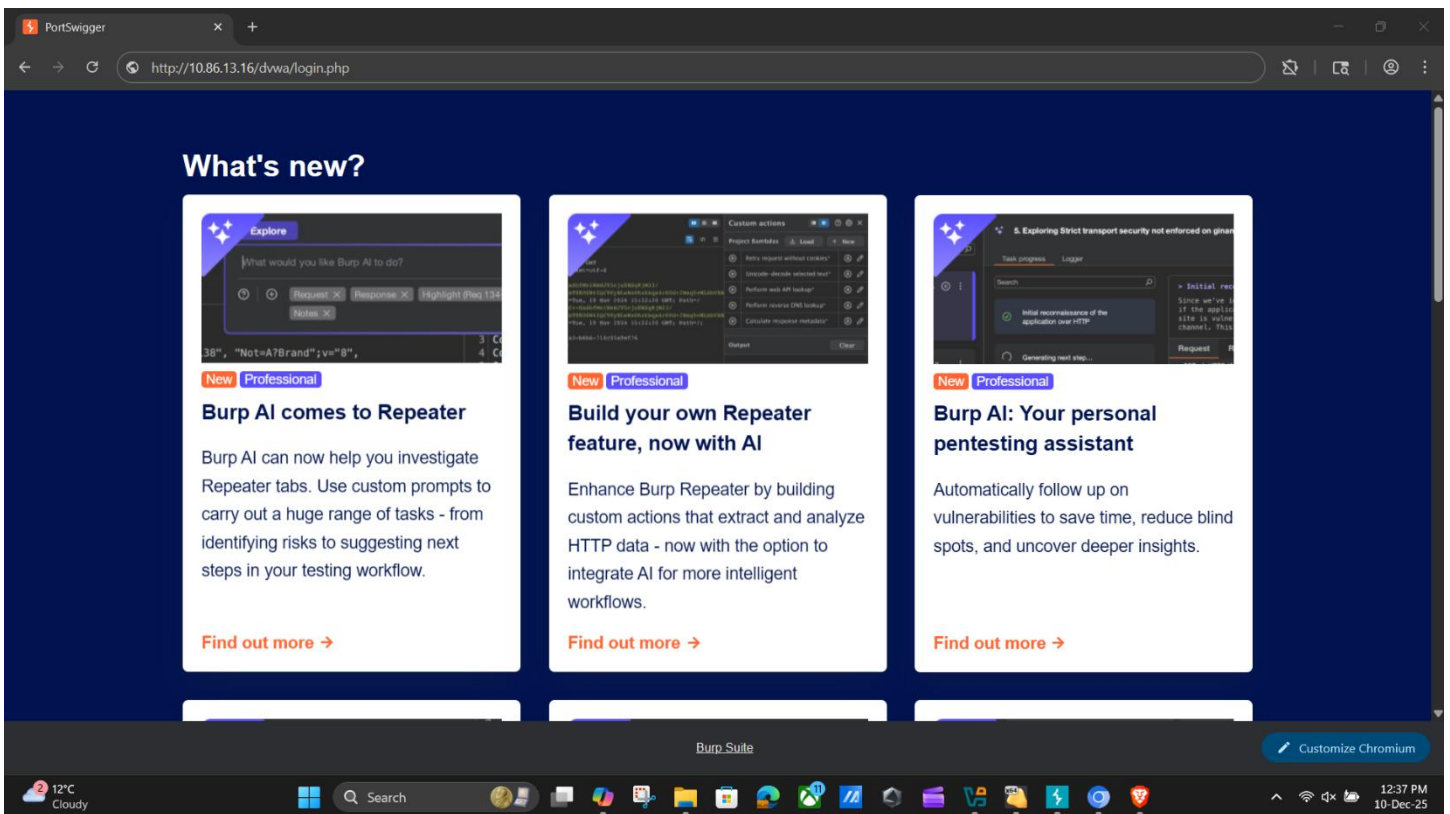


Figure 48: Web traffic inspection using Burp Suite - 3

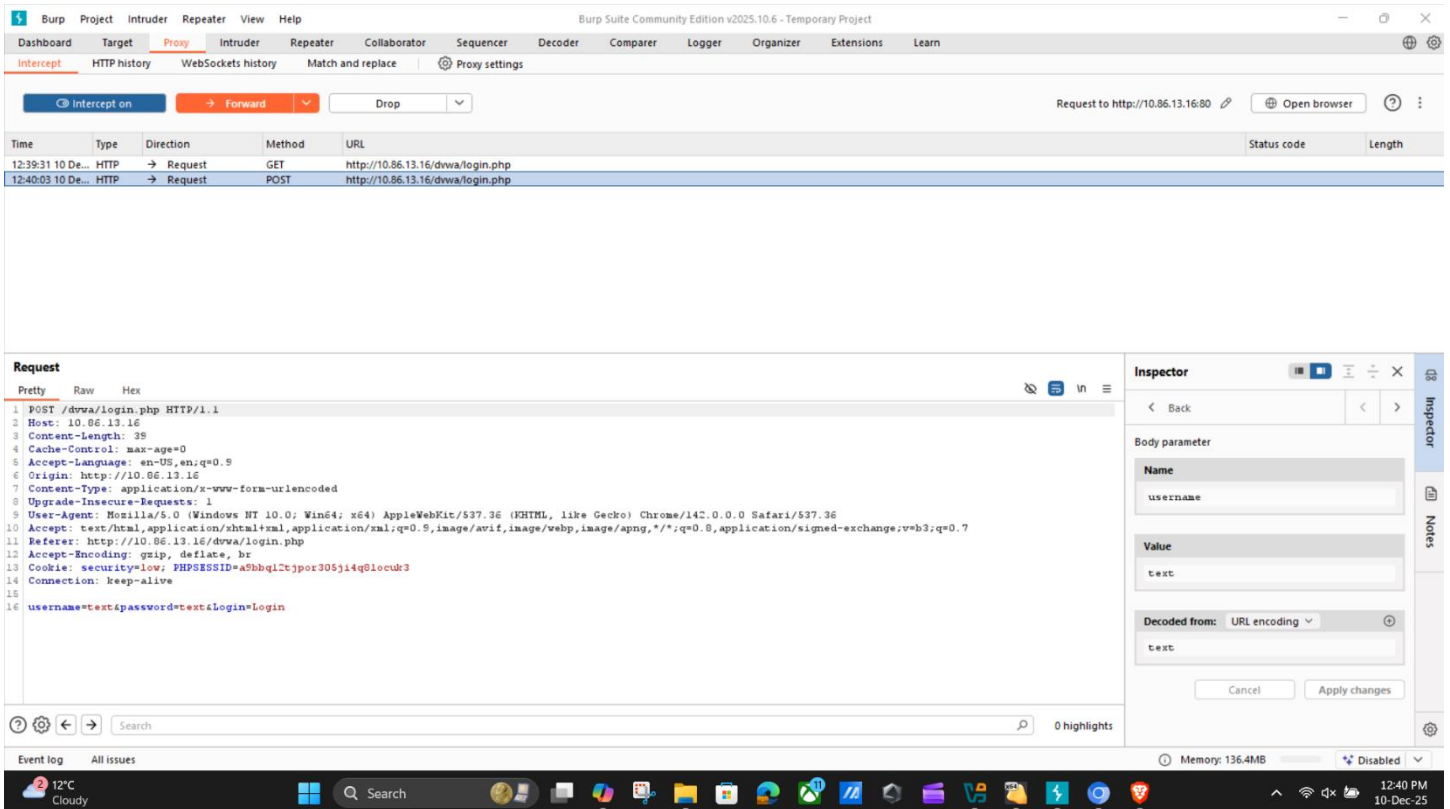


Figure 49: Web traffic inspection using Burp Suite - 4

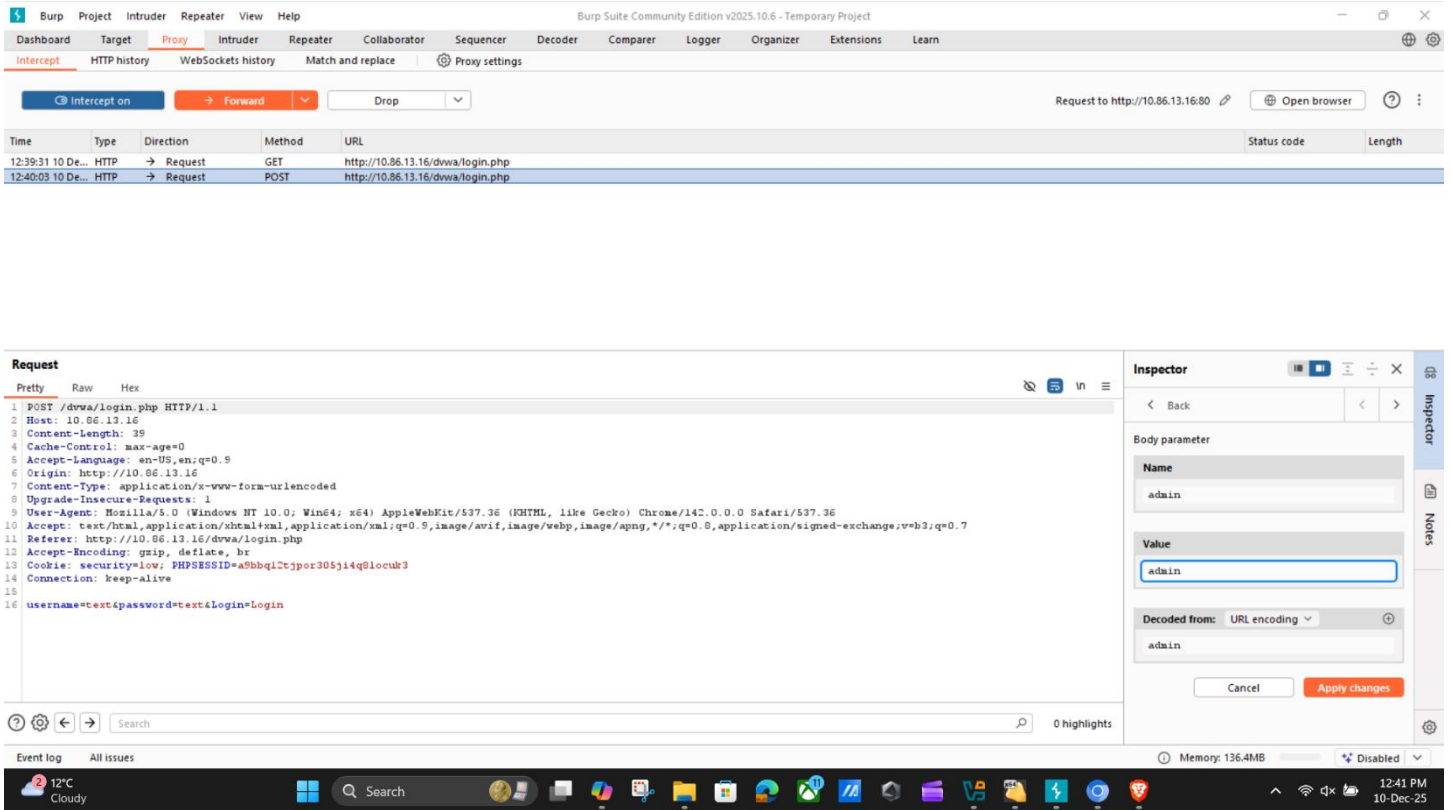


Figure 50: Web traffic inspection using Burp Suite - 5

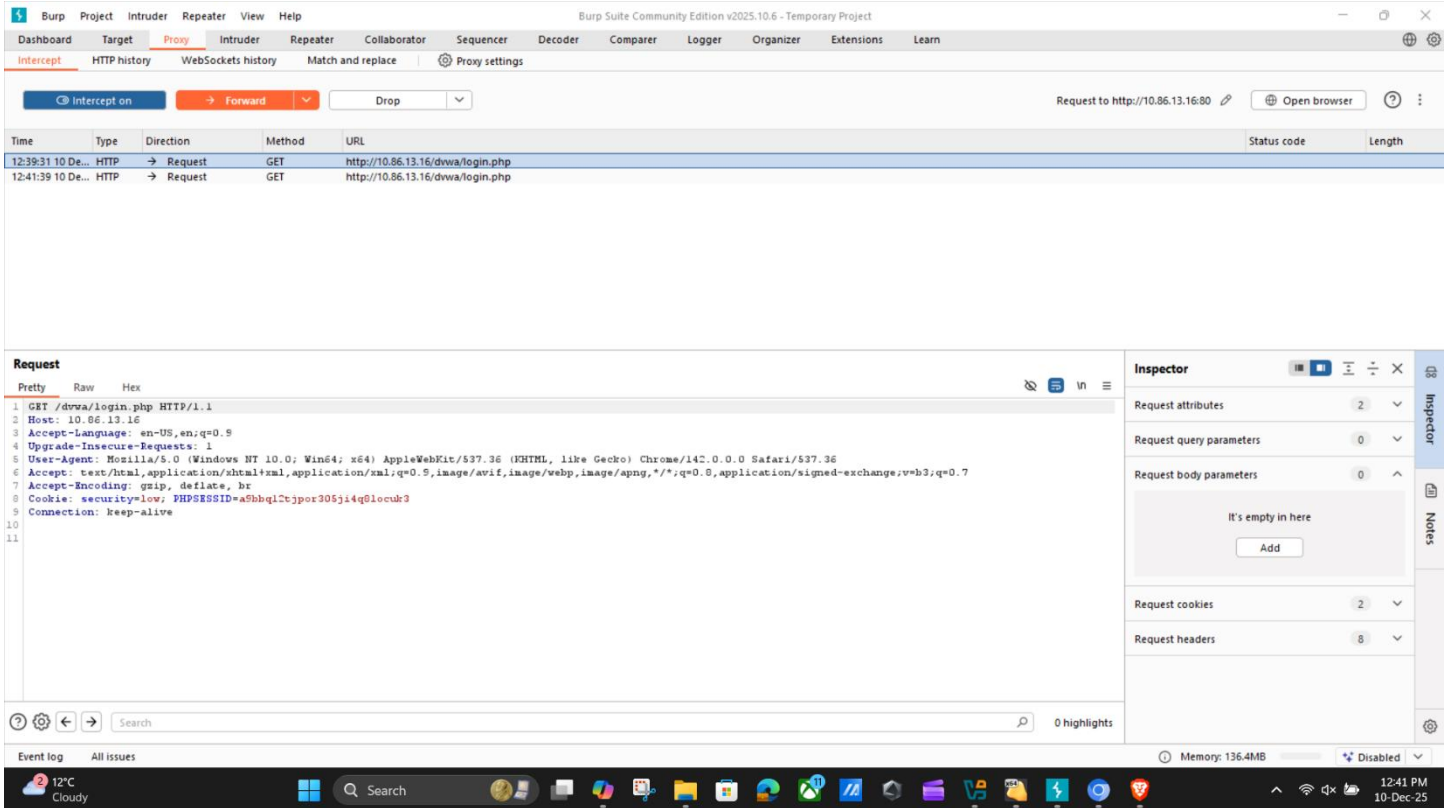


Figure 51: Web traffic inspection using Burp Suite - 6

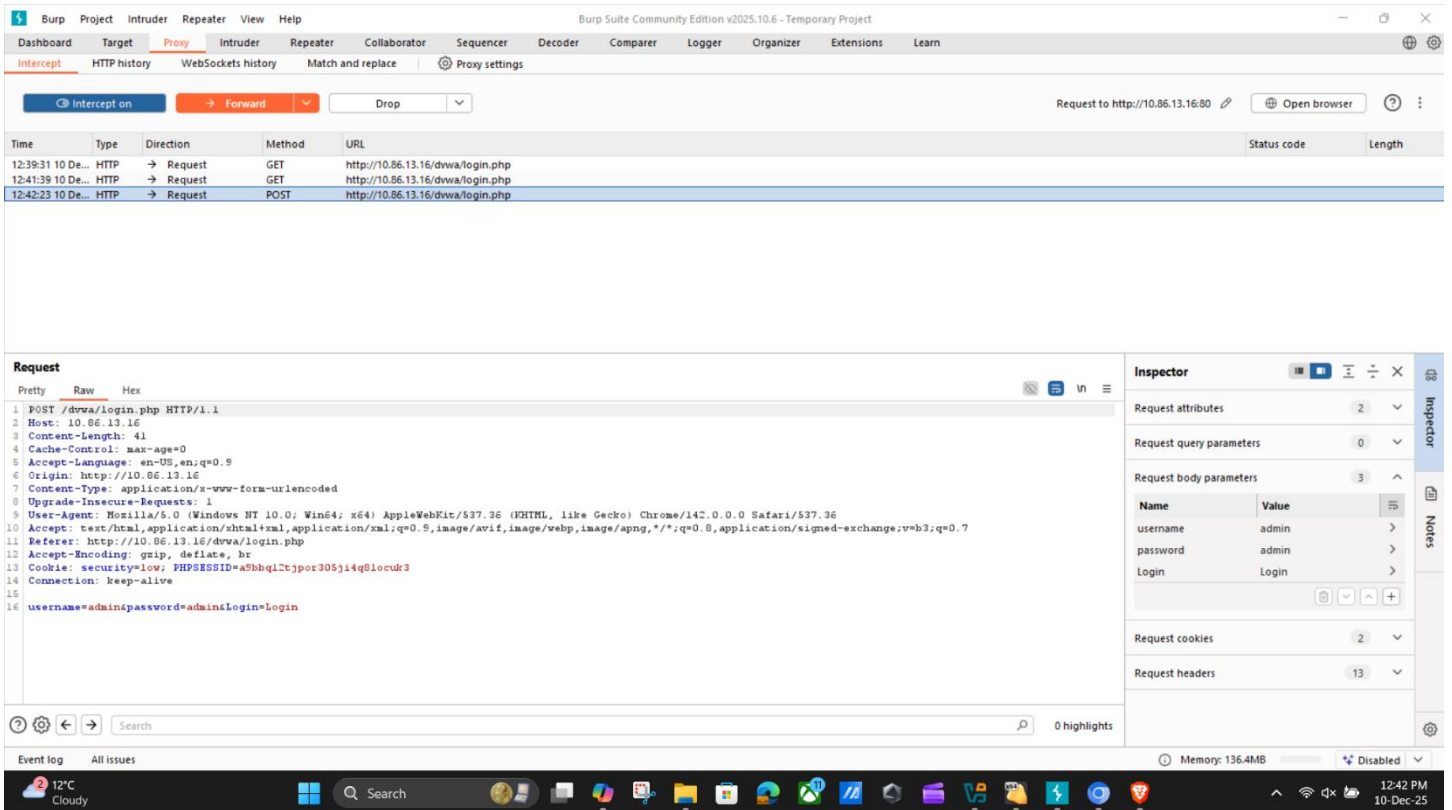


Figure 52: Web traffic inspection using Burp Suite - 7

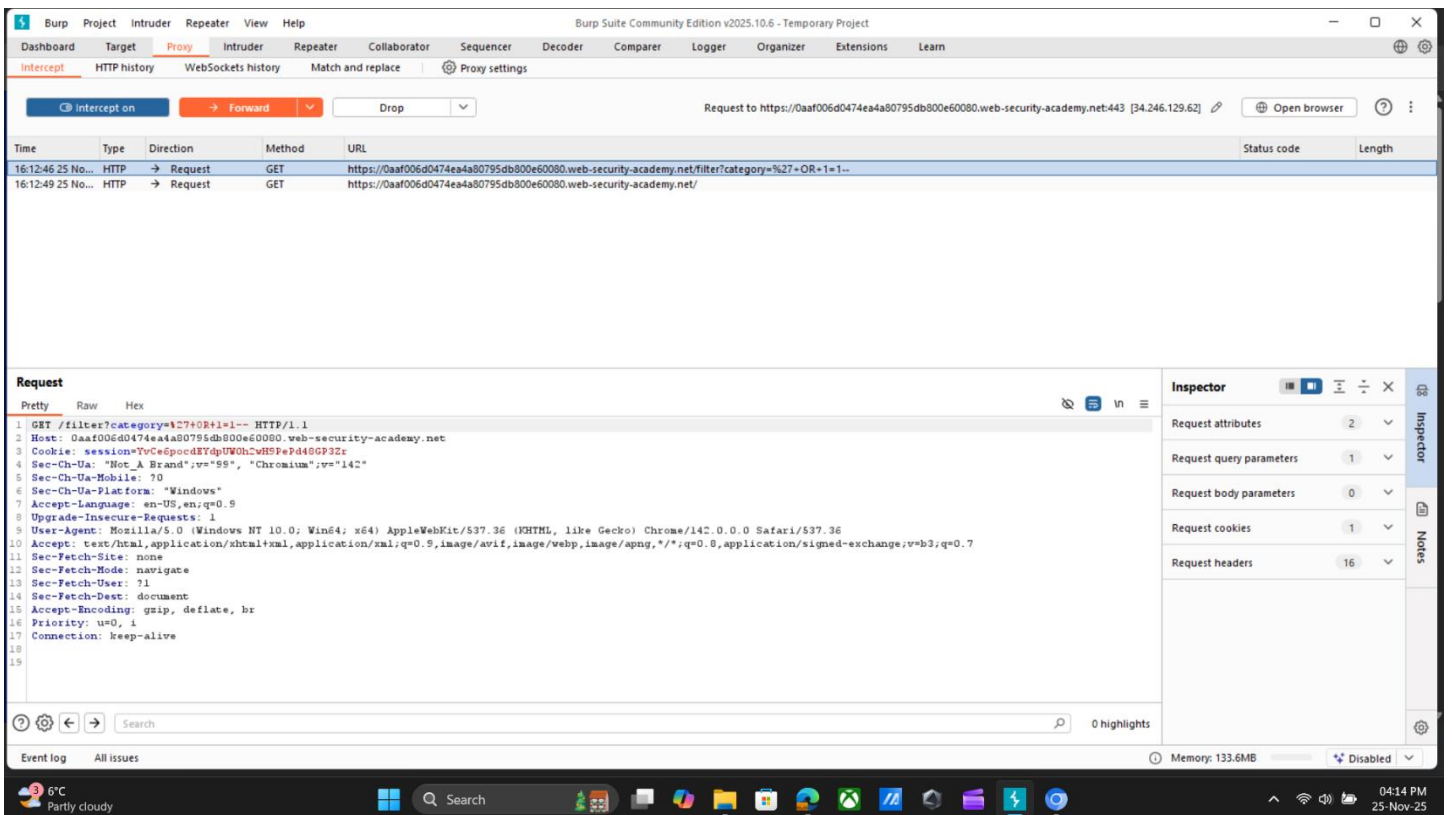


Figure 53: Web traffic inspection using Burp Suite – 8

From Figure 46 to Figure 53 shows Burp Suite being used to intercept and analyze web application requests during security testing.

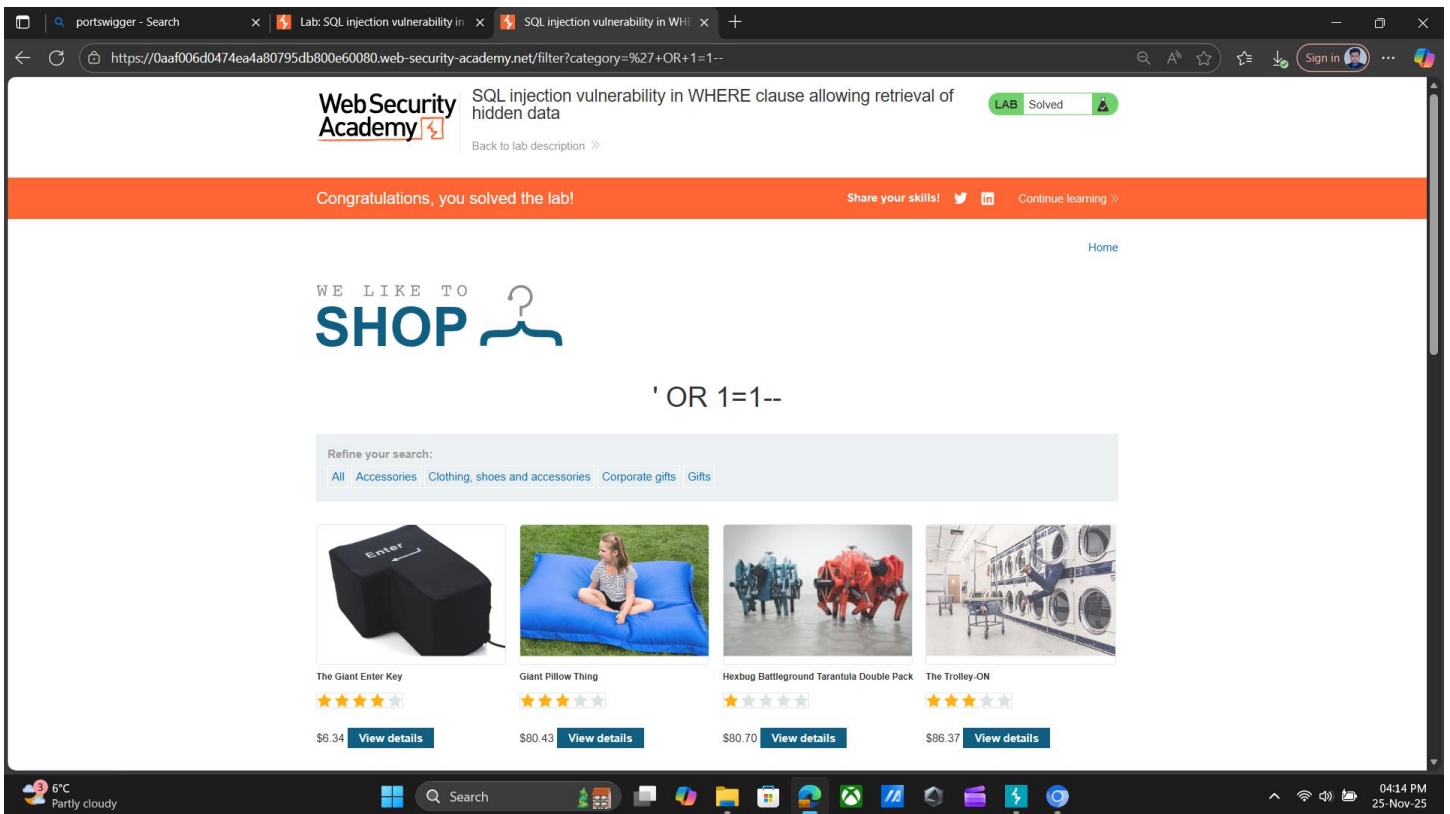


Figure 54: SQL injection vulnerability in database query

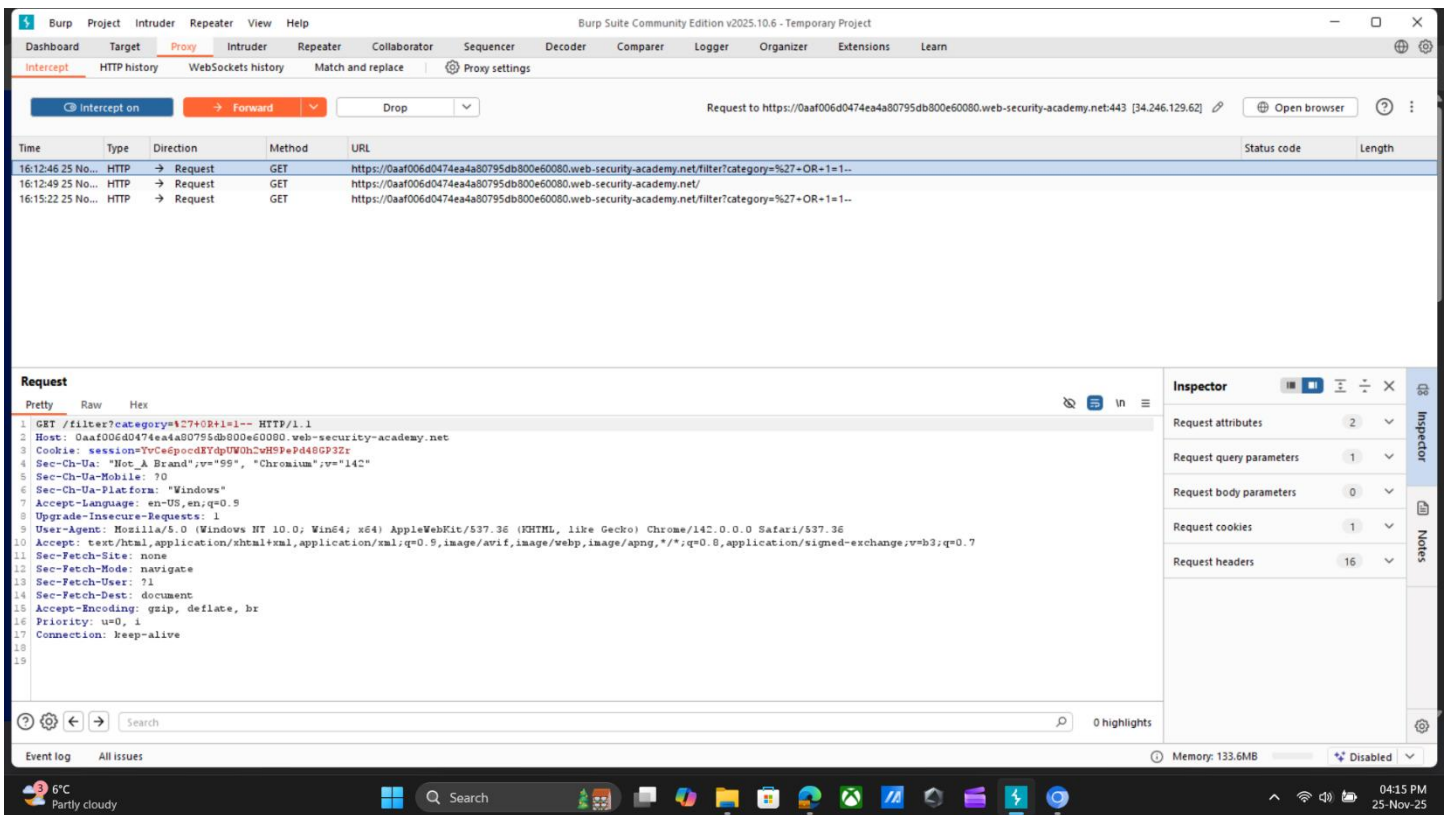


Figure 55: SQL injection vulnerability in database query – 2

In highlighting Figure 54 and Figure 55 that, how improper input handling allows hidden database data to be accessed using SQL injection.

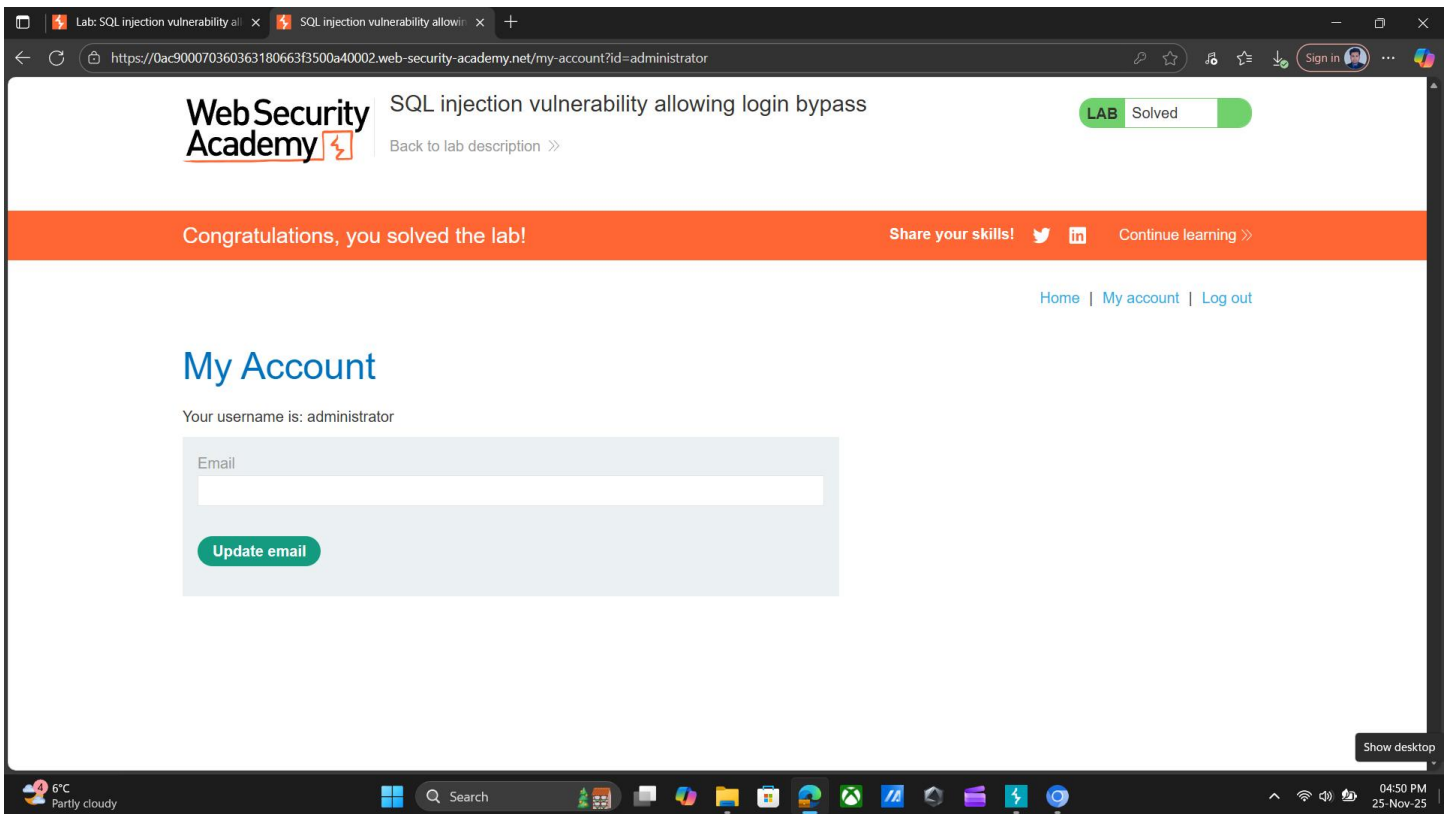


Figure 56: SQL injection enabling authentication bypass

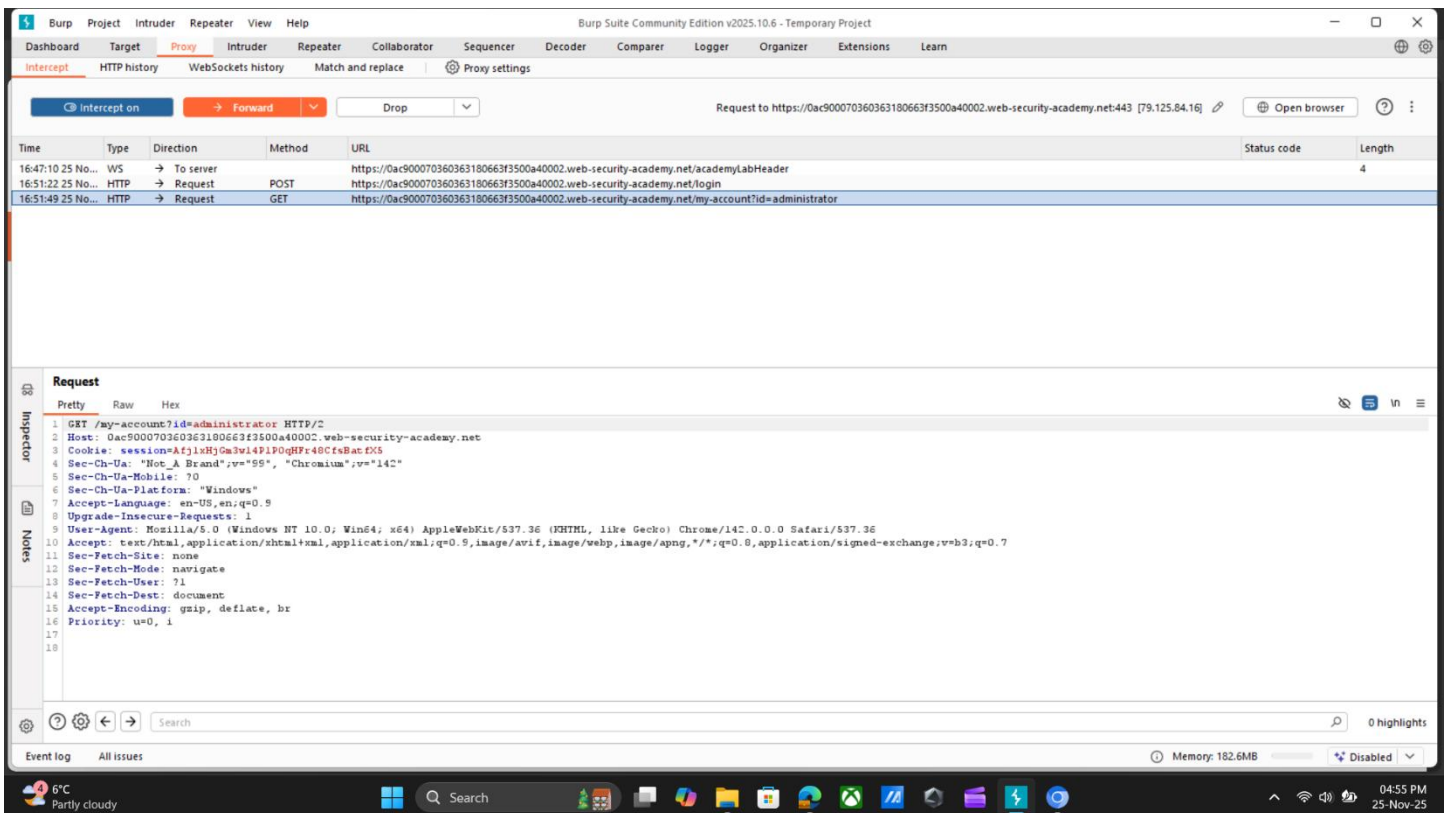


Figure 57: SQL injection enabling authentication bypass – 2

It demonstrates Figure 56 and Figure 57 how a SQL injection flaw can be used to bypass the login process and gain unauthorized access.

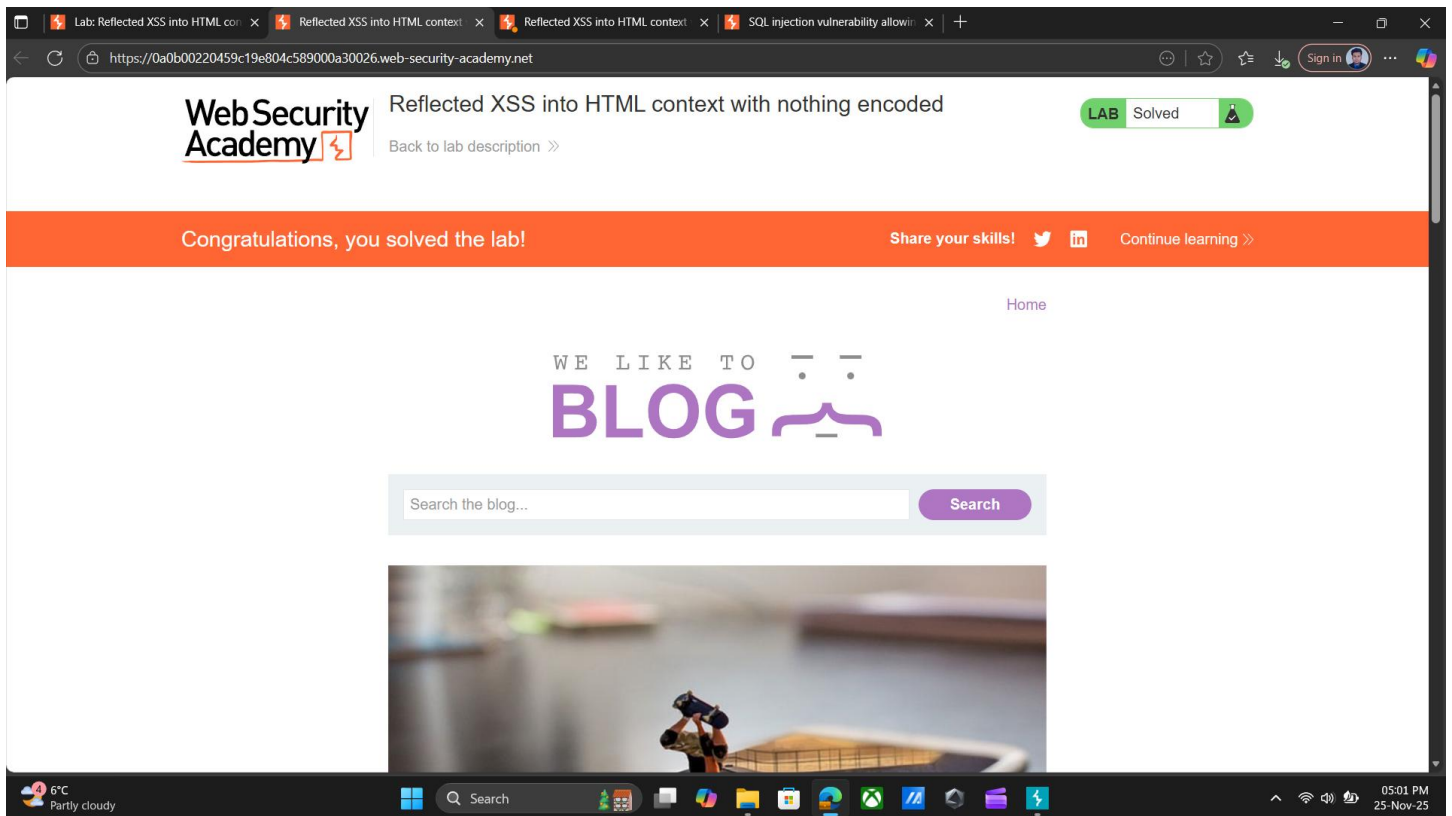


Figure 58: Cross-site scripting vulnerability

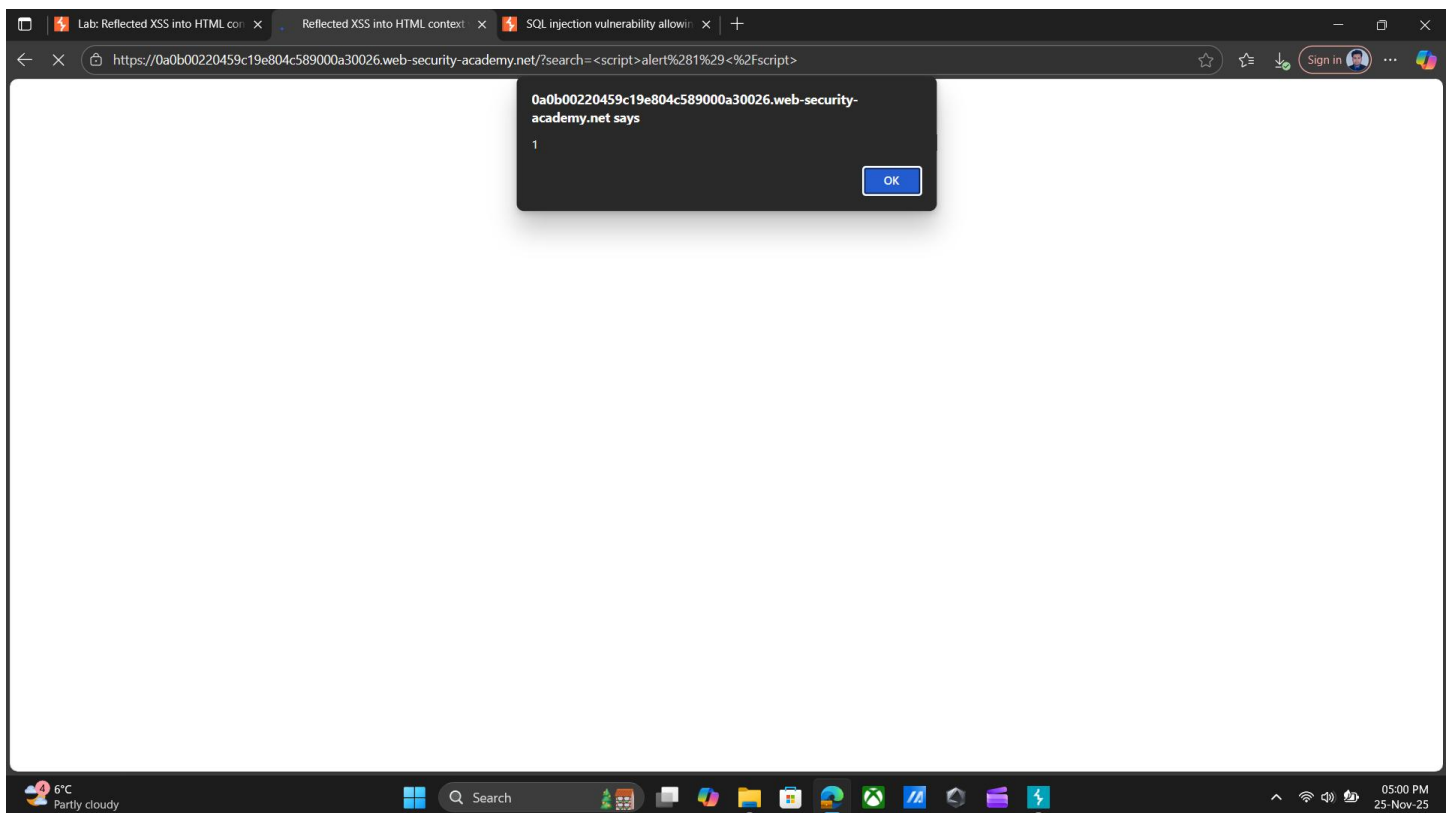


Figure 59: Cross-site scripting vulnerability - 2

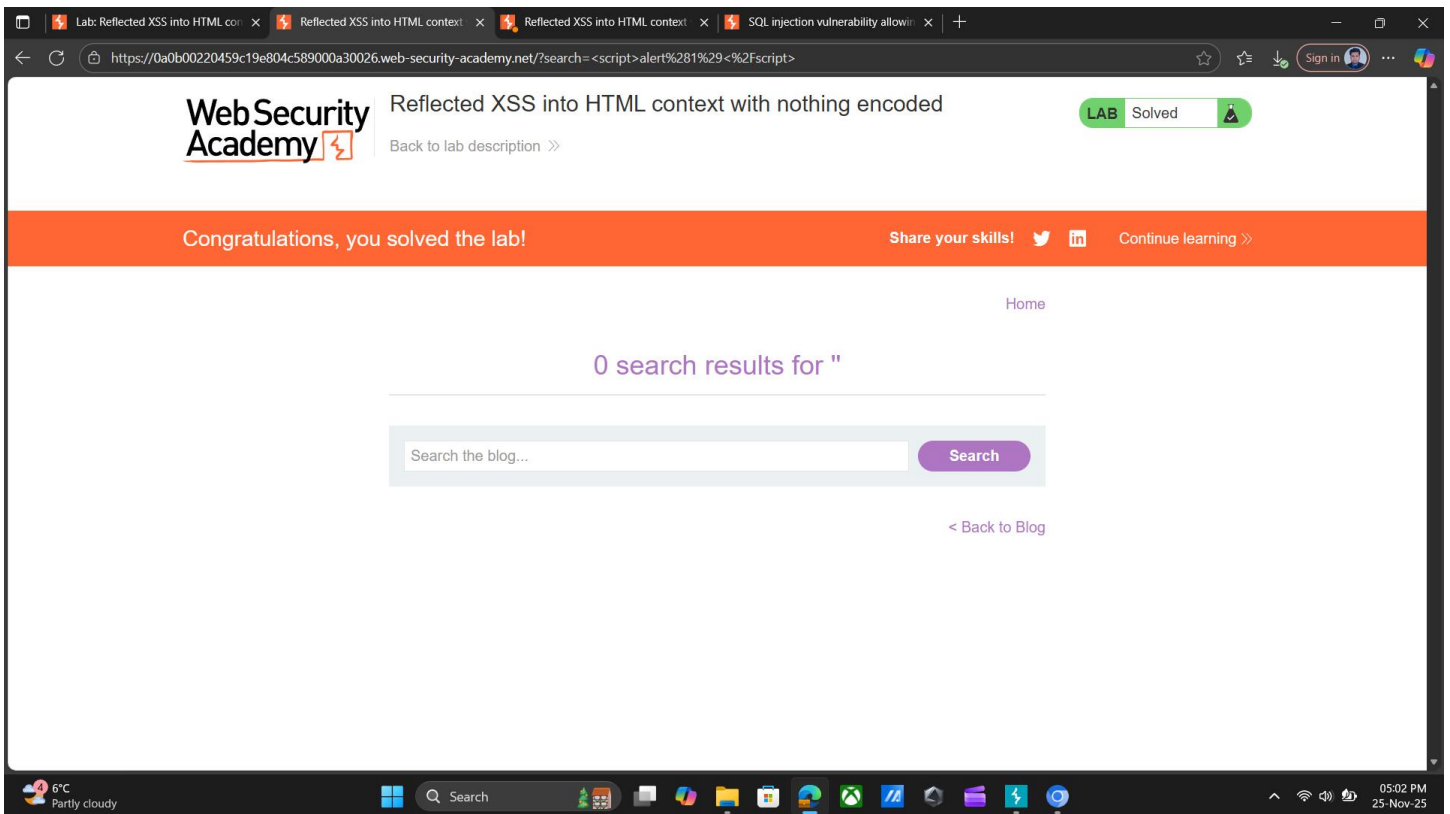


Figure 60: Cross-site scripting vulnerability - 3

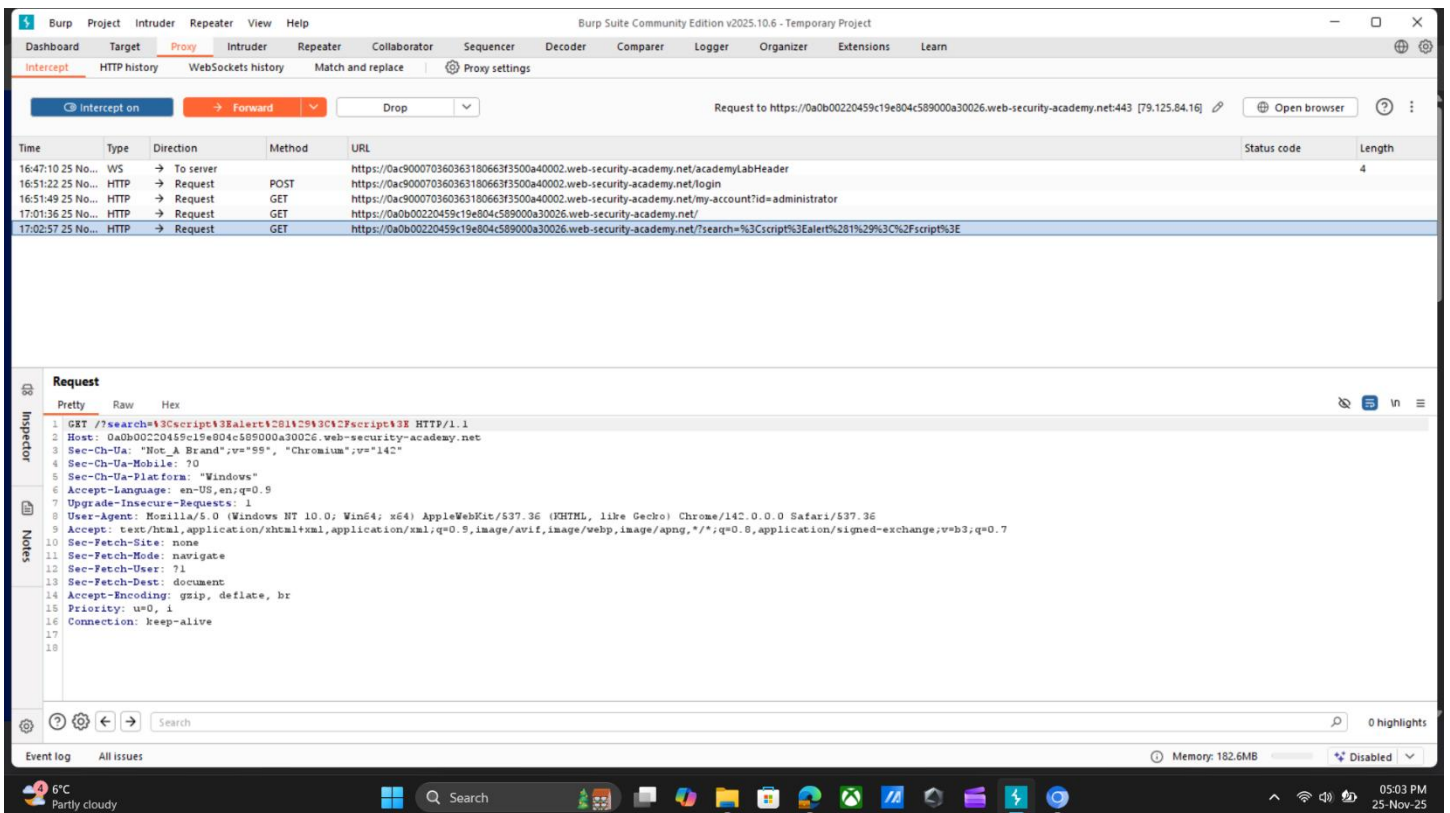


Figure 61: Cross-site scripting vulnerability – 4

From Figure 58 to Figure 61 shows, XSS vulnerability where user input is not properly sanitized, allowing script execution in the browser.

- Nessus -

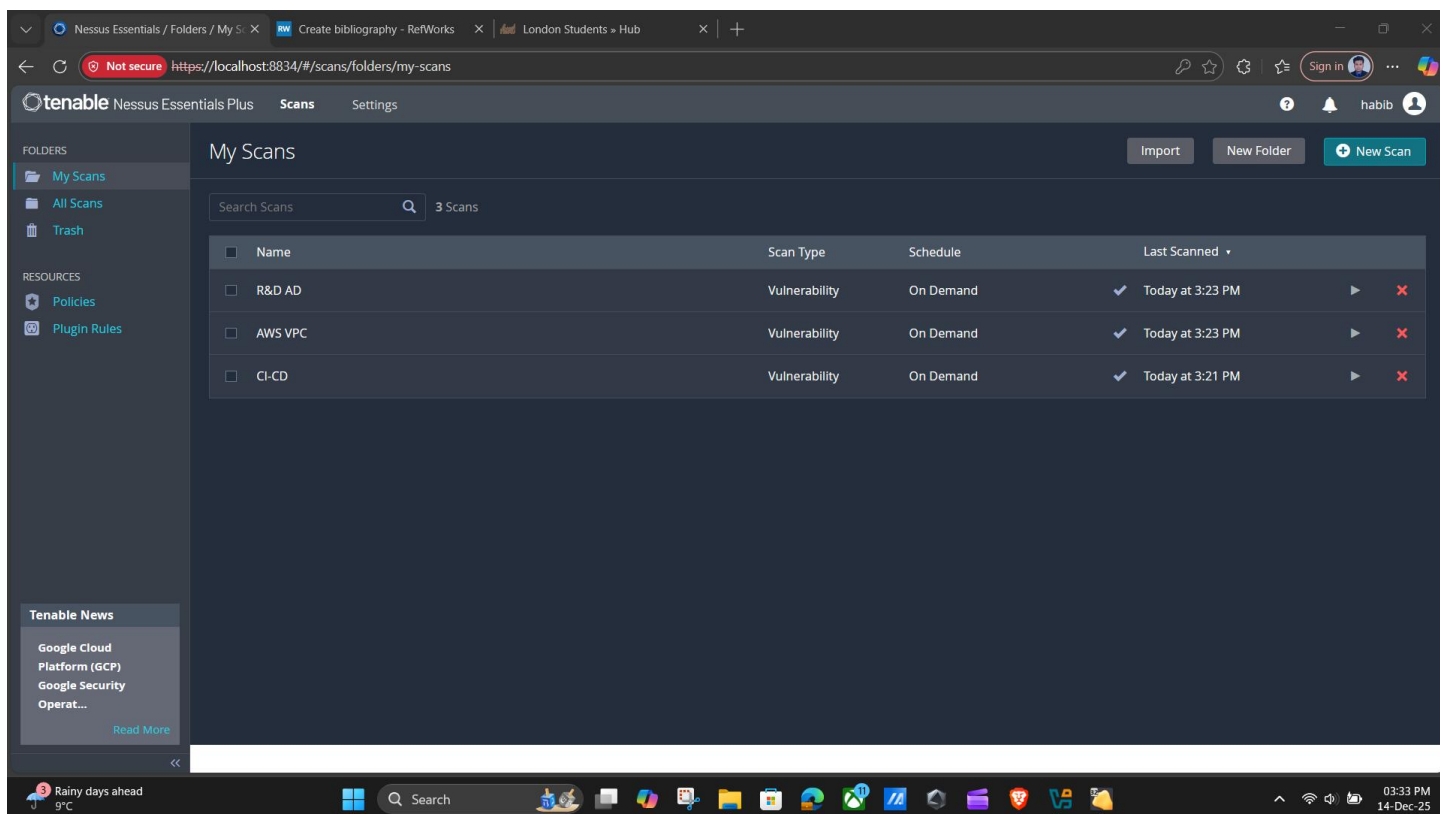


Figure 62: All scan overview in Nessus

Figure 62 illustrates an overview of all the scans, which are R&D AD, AWS VPC, and CI-CD.

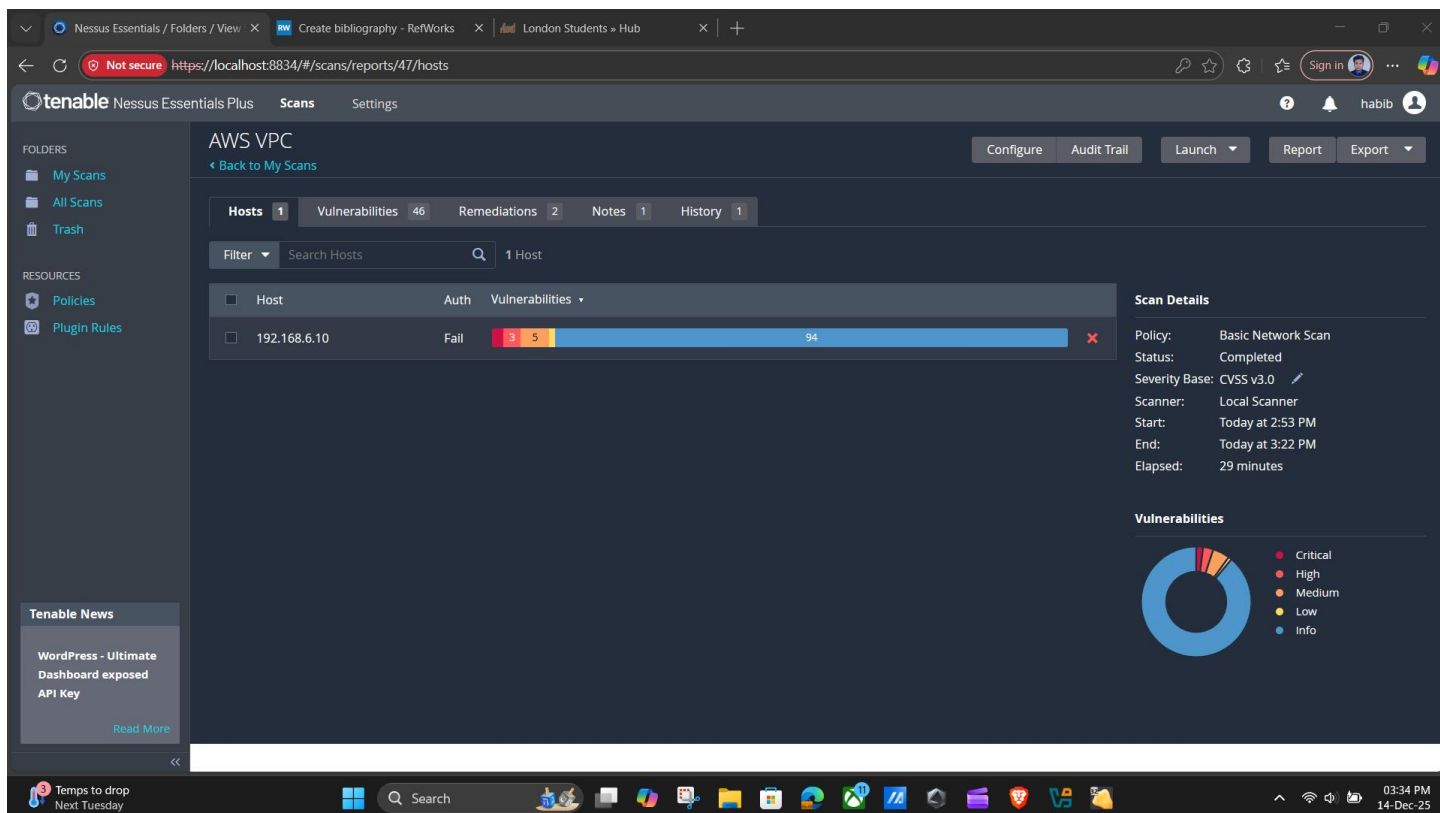


Figure 63: Nessus scan results for AWS VPC resources - 1

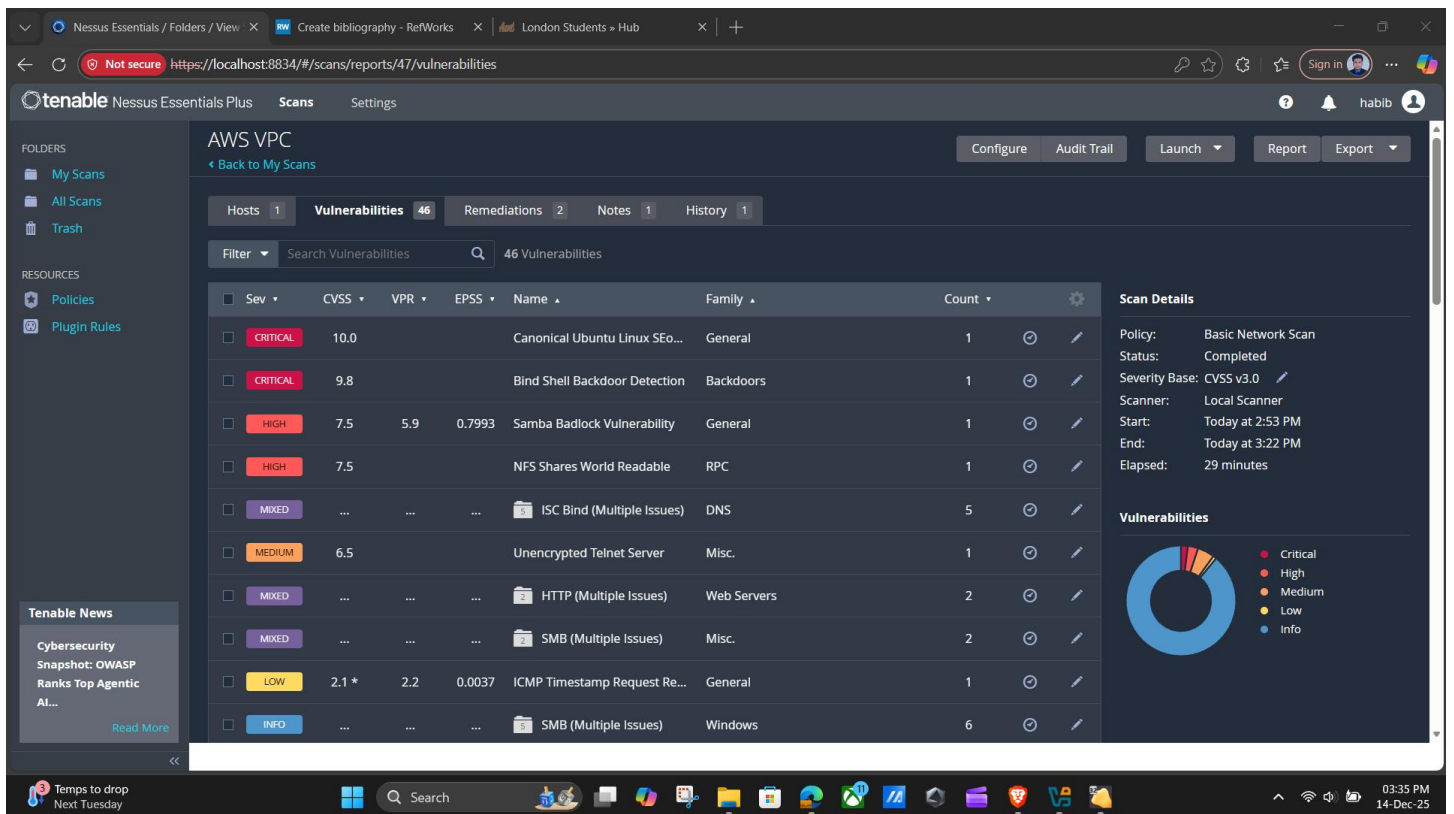


Figure 64: Nessus scan results for AWS VPC resources - 2

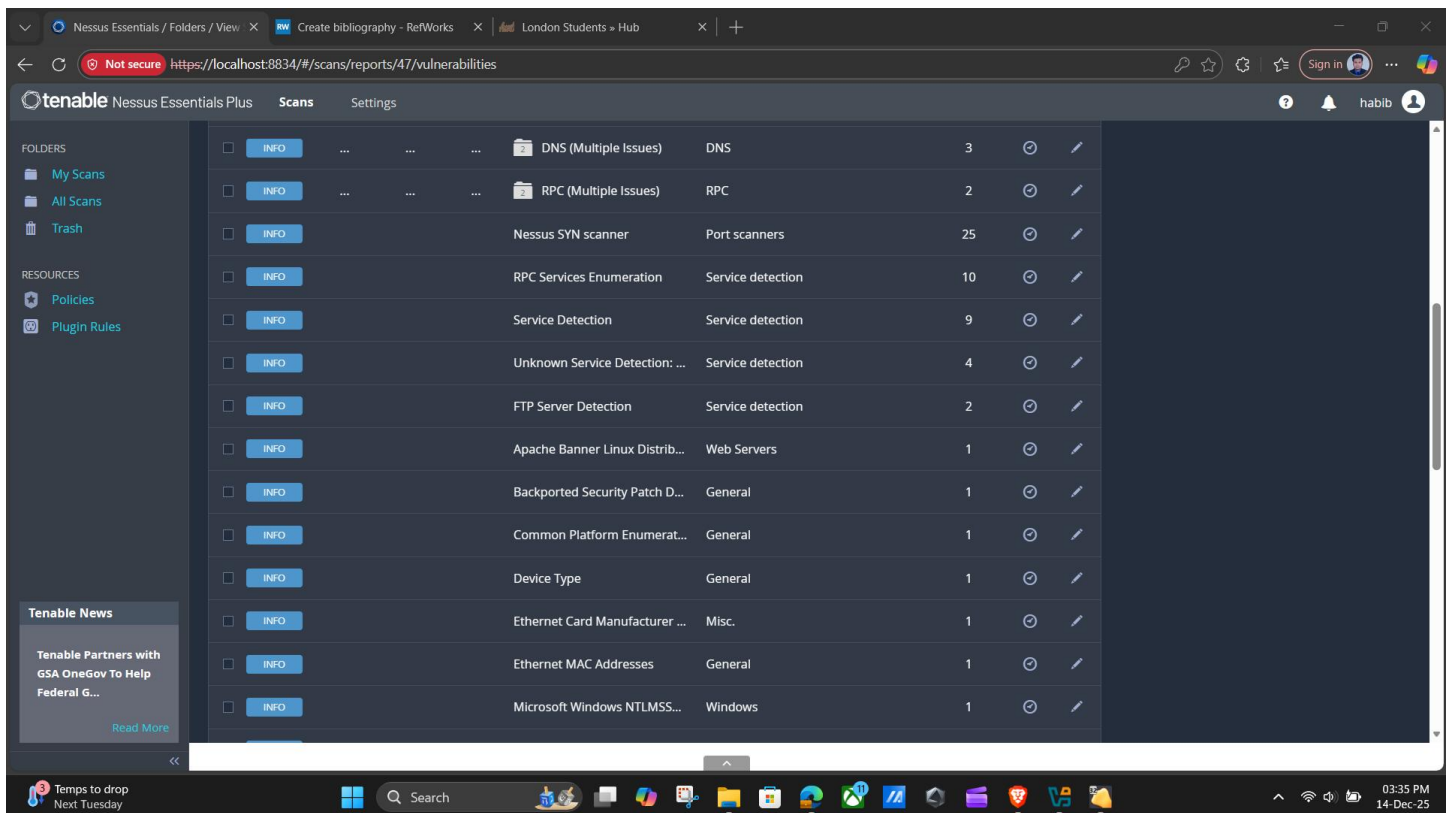


Figure 65: Nessus scan results for AWS VPC resources - 3

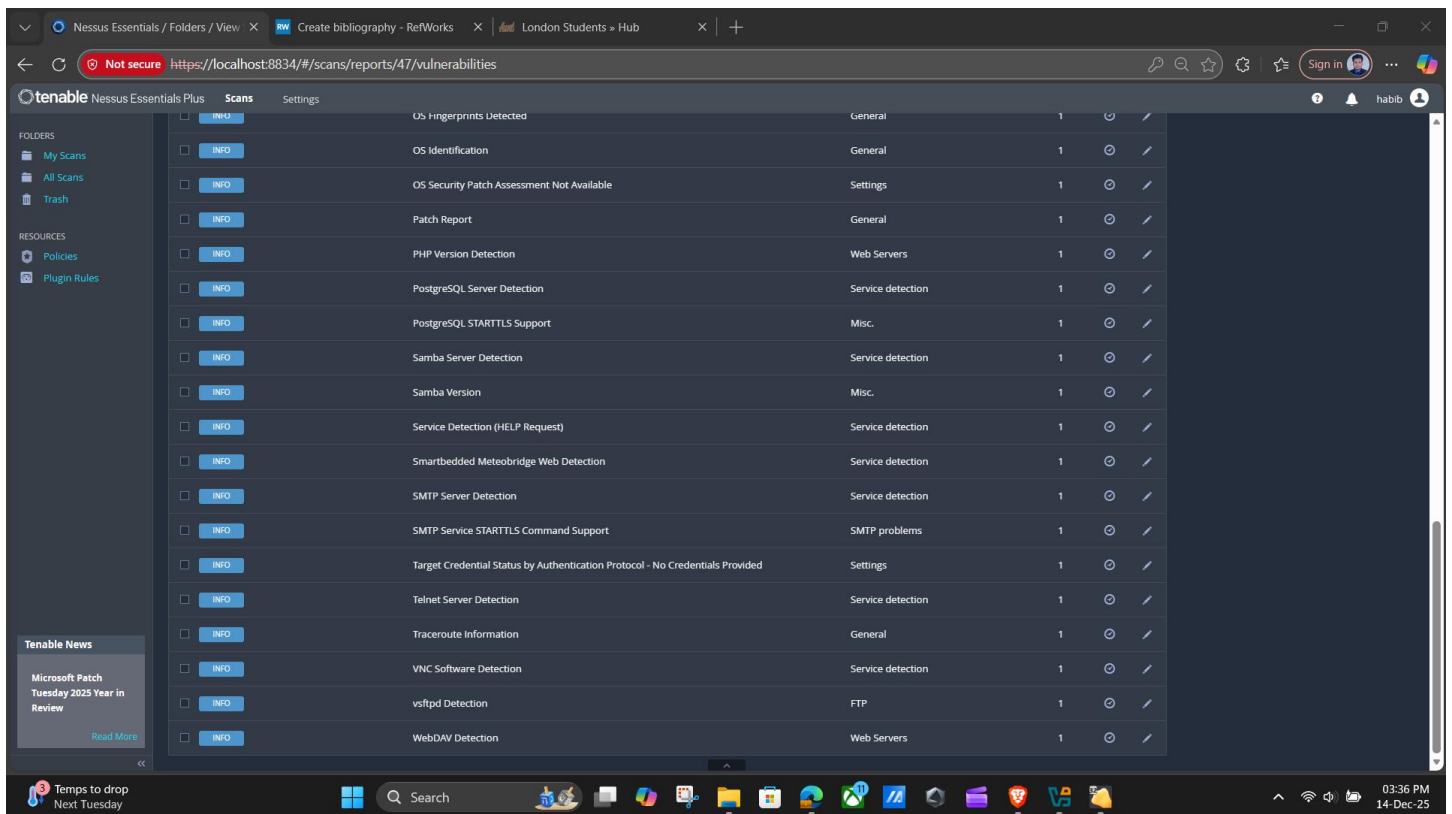


Figure 66: Nessus scan results for AWS VPC resources - 4

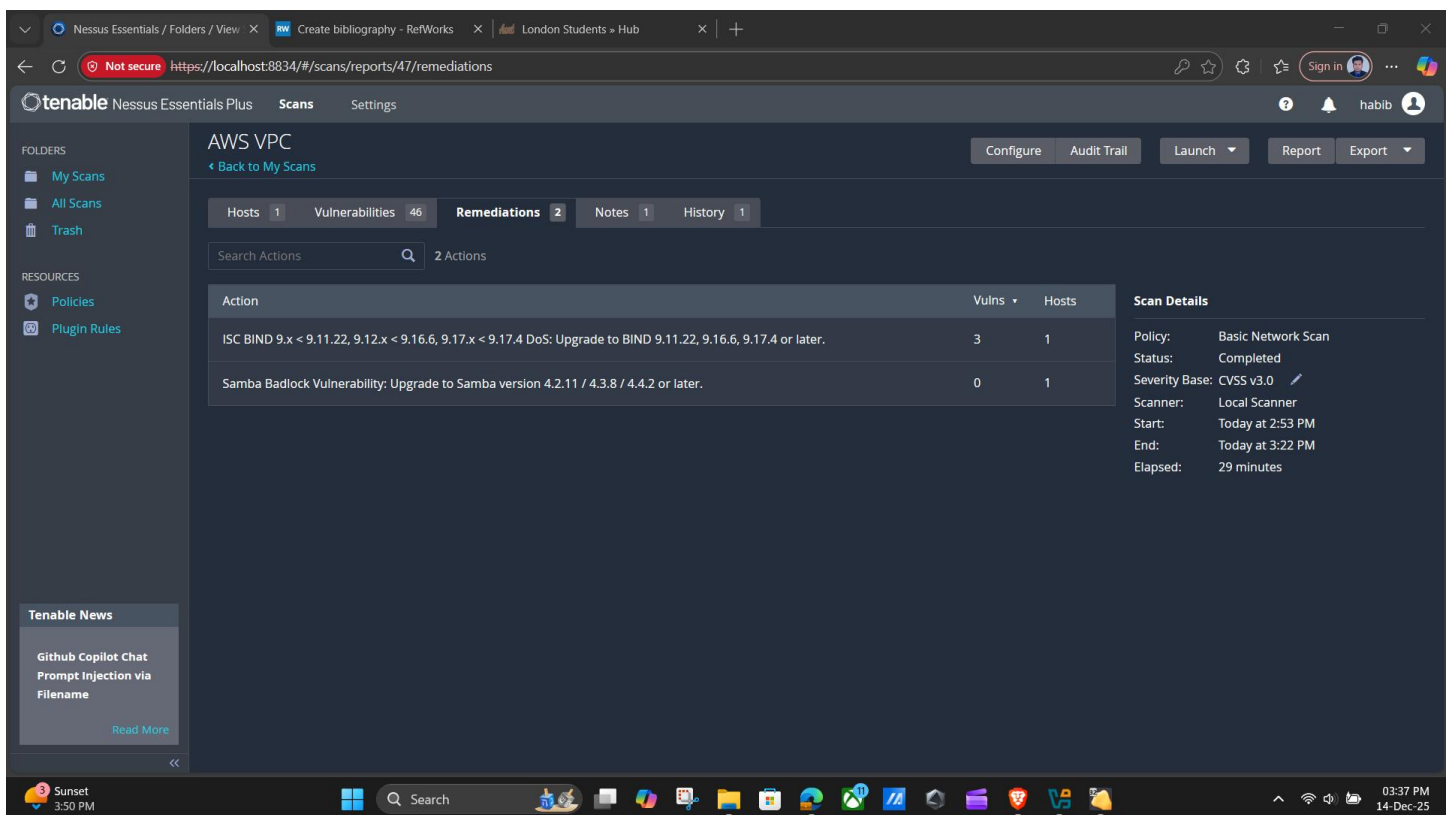


Figure 67: Nessus scan results for AWS VPC resources - 5

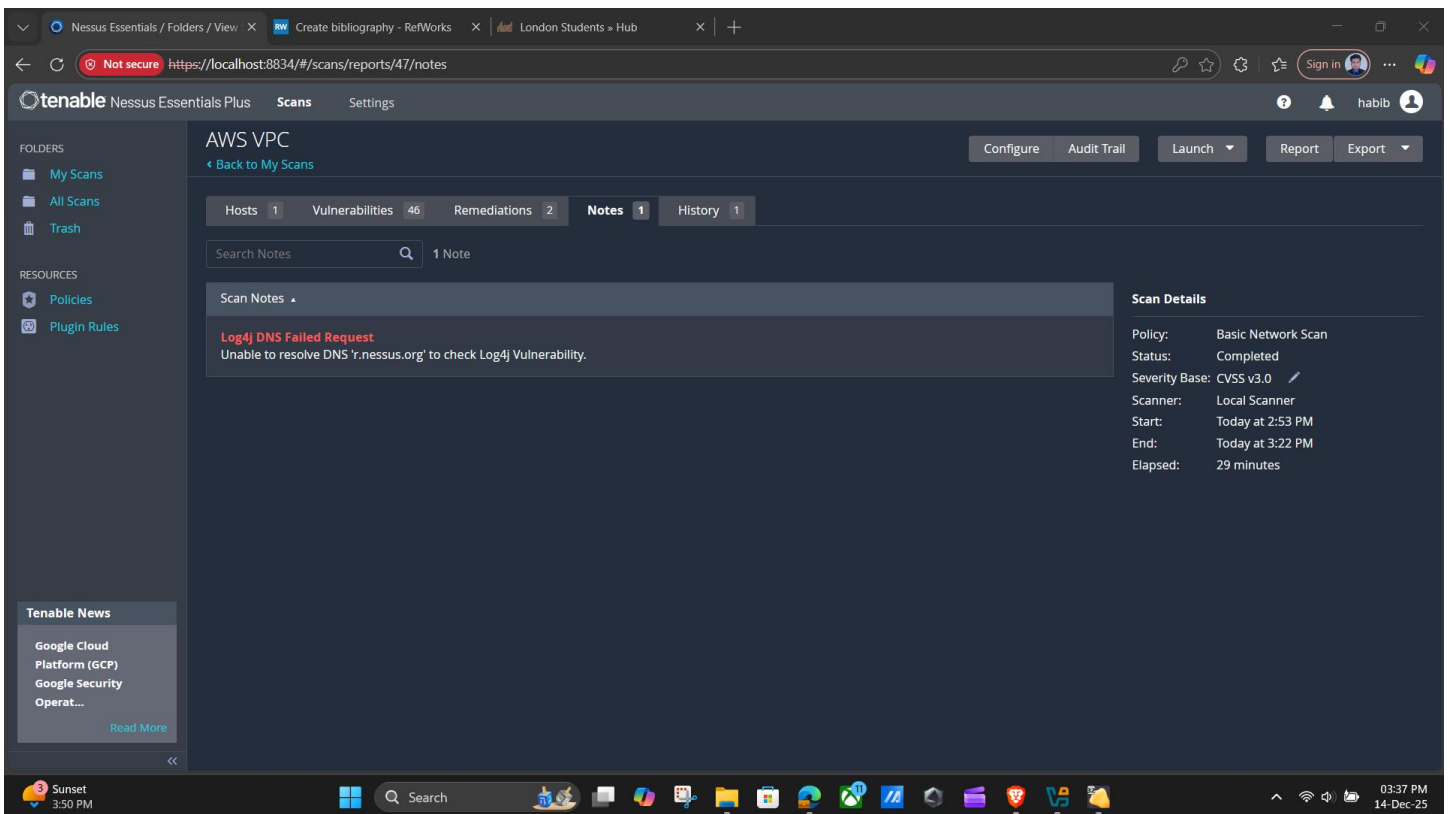


Figure 68: Nessus scan results for AWS VPC resources - 6

From Figure 63 to Figure 68 highlights the scan lists of hosts, vulnerabilities, and suggested remediation steps, with notes to explain risk and priority for fixing the issues.

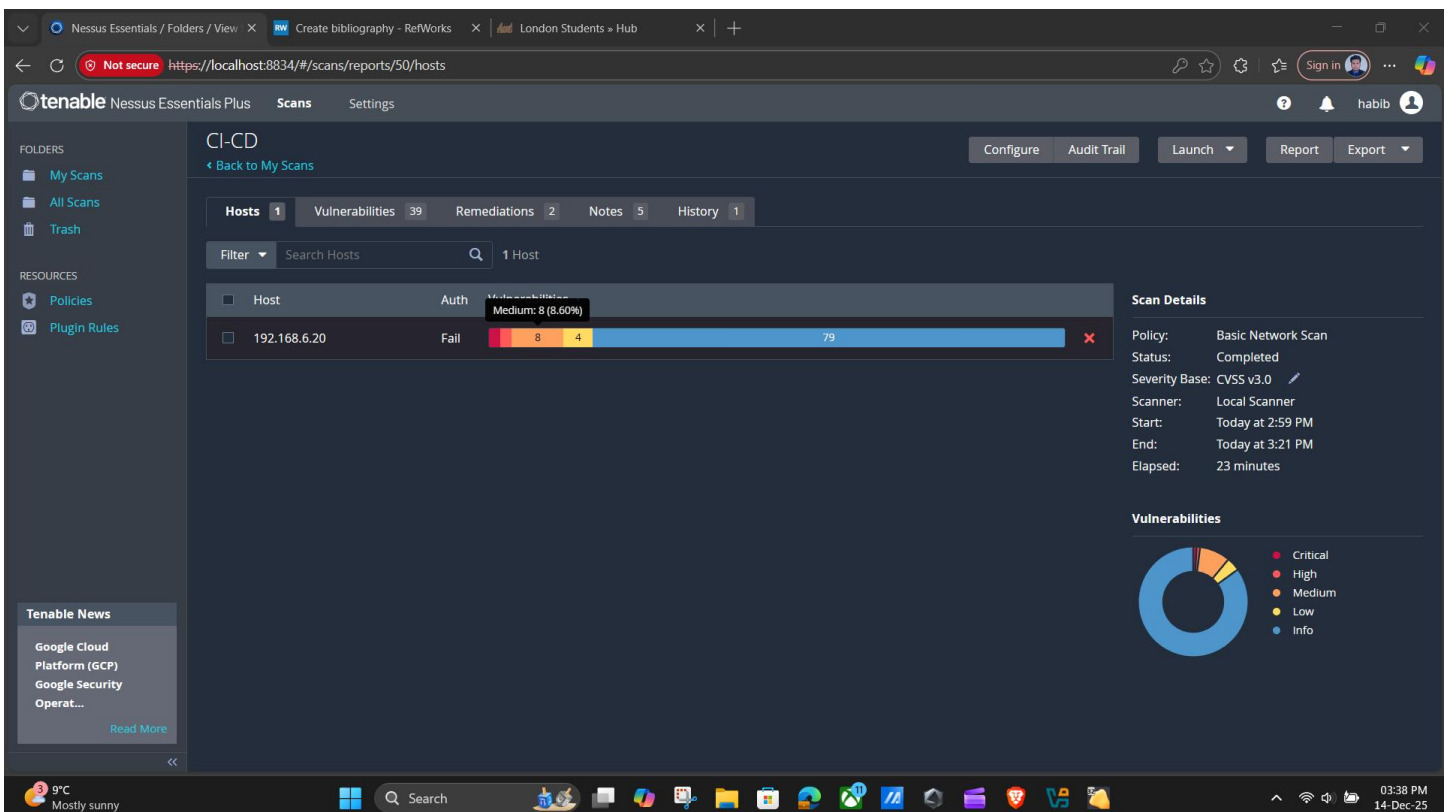


Figure 69: Nessus scan results for CI-CD resources - 1

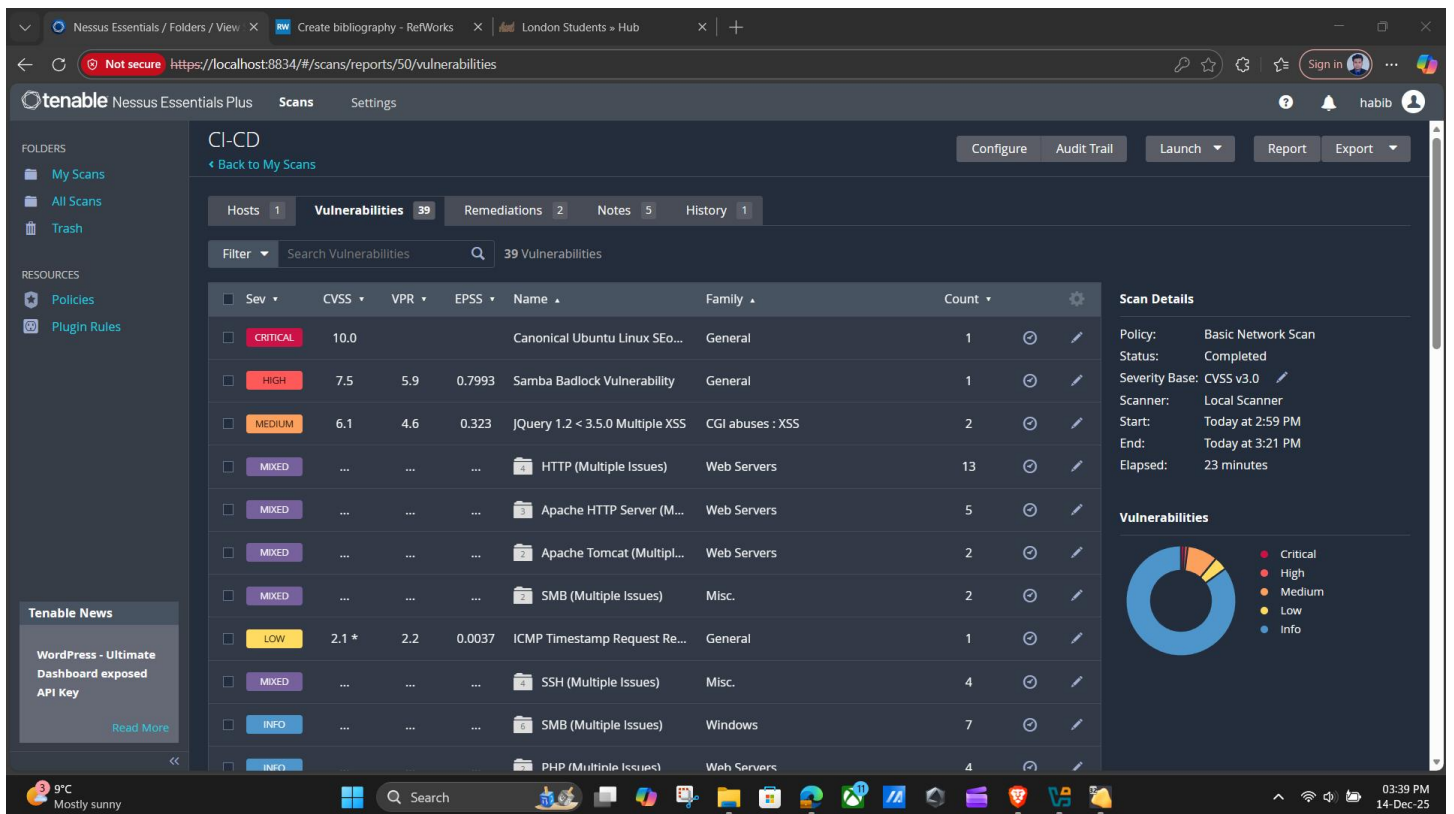


Figure 70: Nessus scan results for CI-CD resources - 2

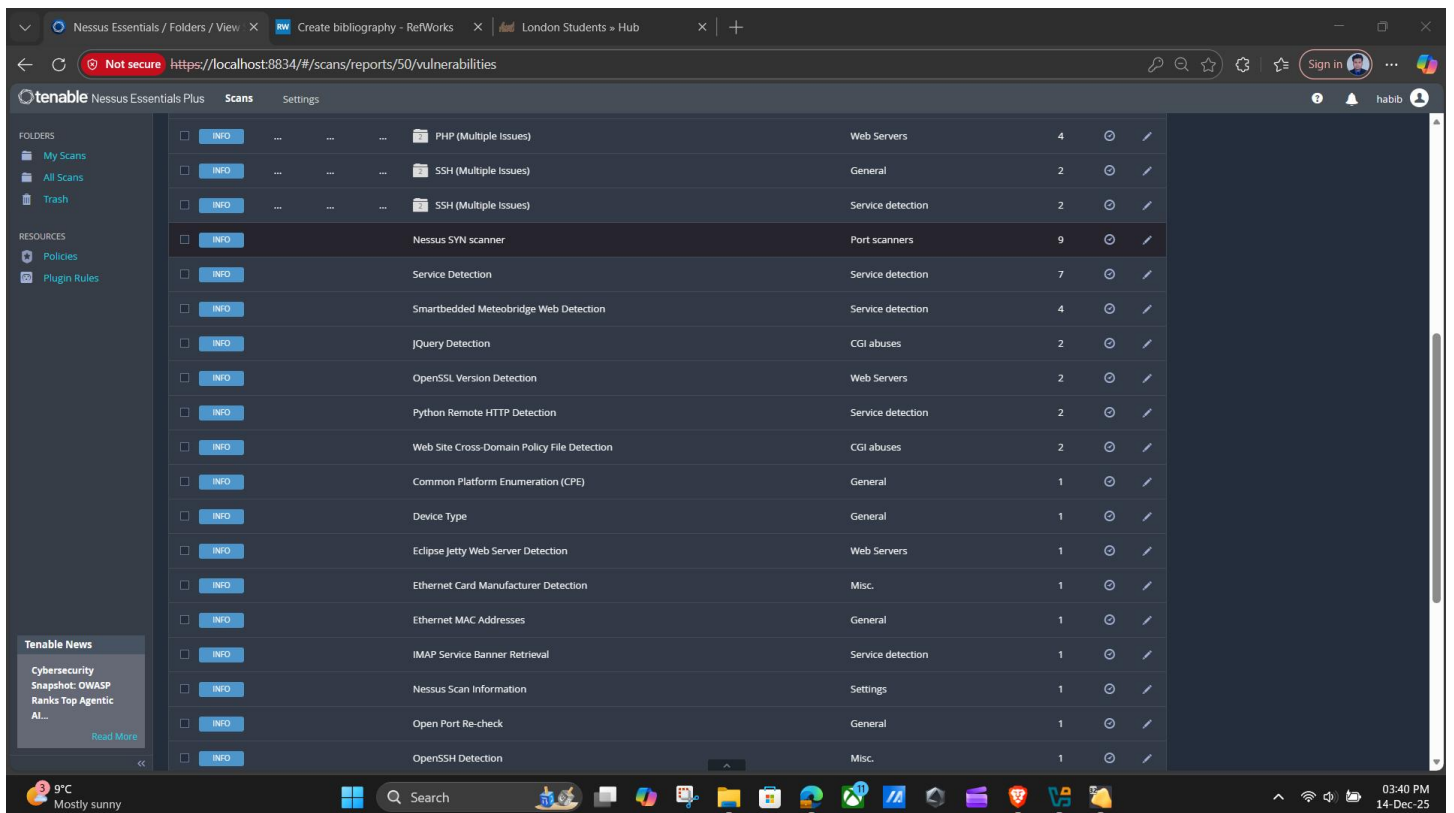


Figure 71: Nessus scan results for CI-CD resources - 3

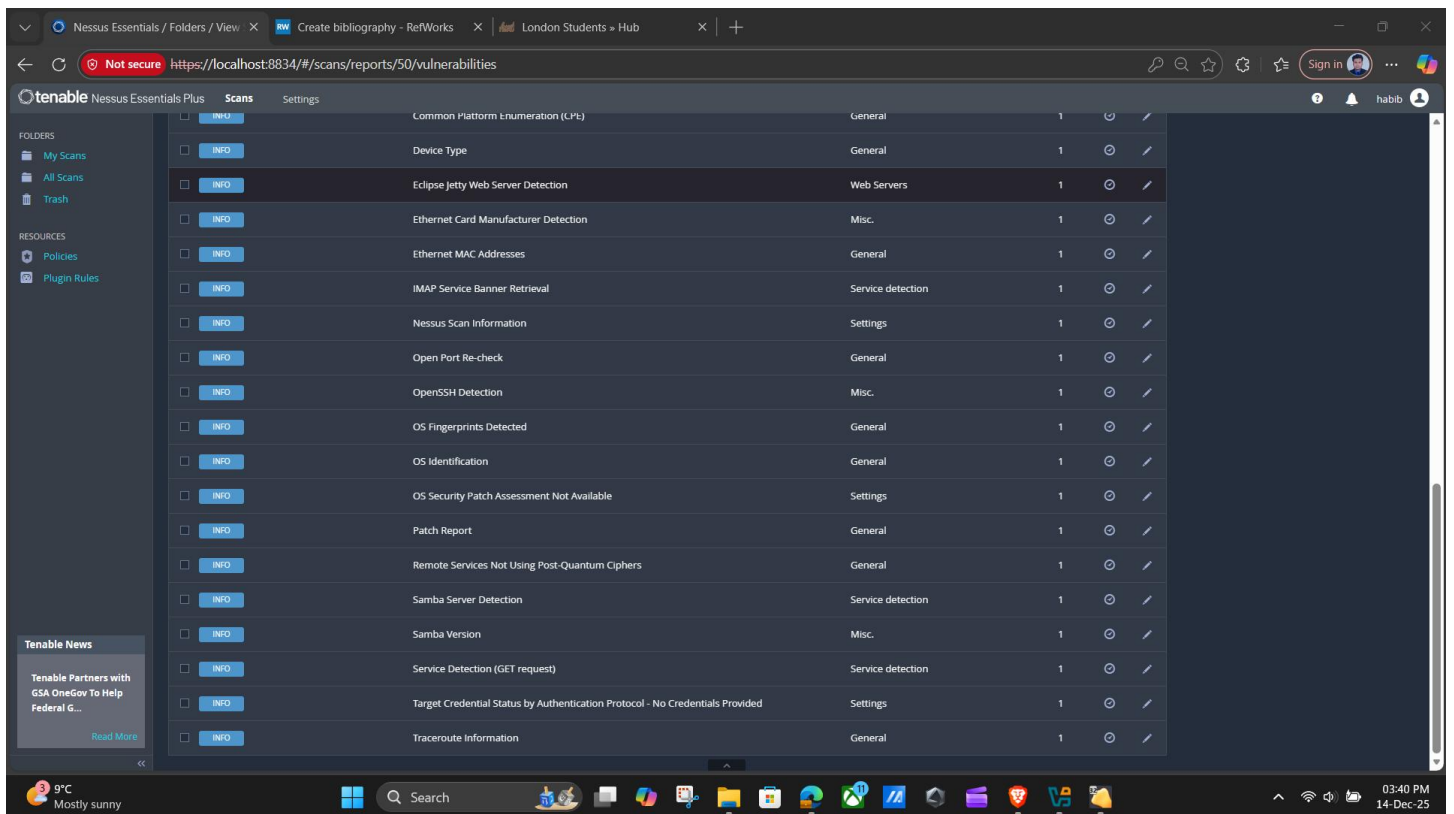


Figure 72: Nessus scan results for CI-CD resources - 4

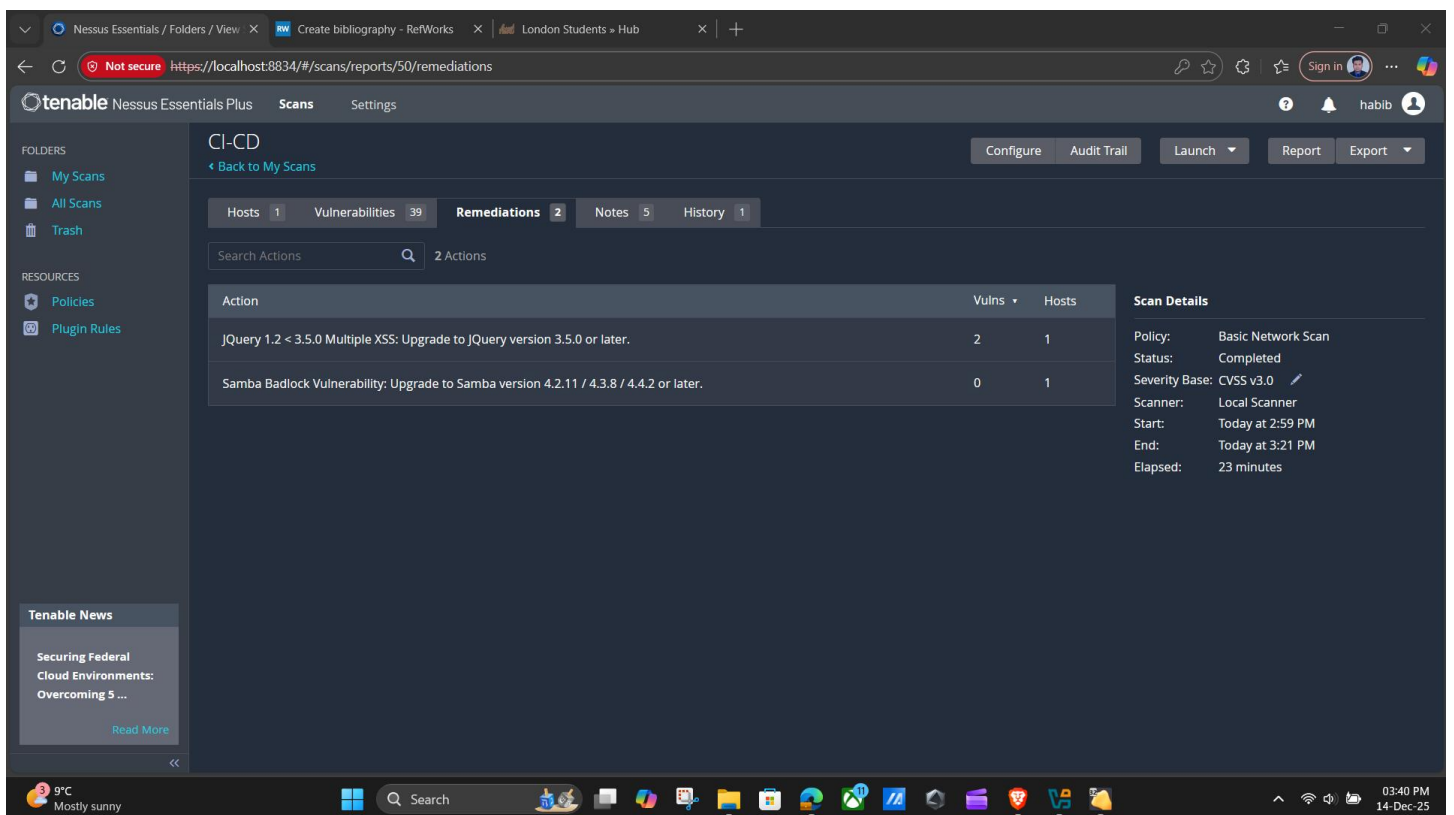


Figure 73: Nessus scan results for CI-CD resources - 5

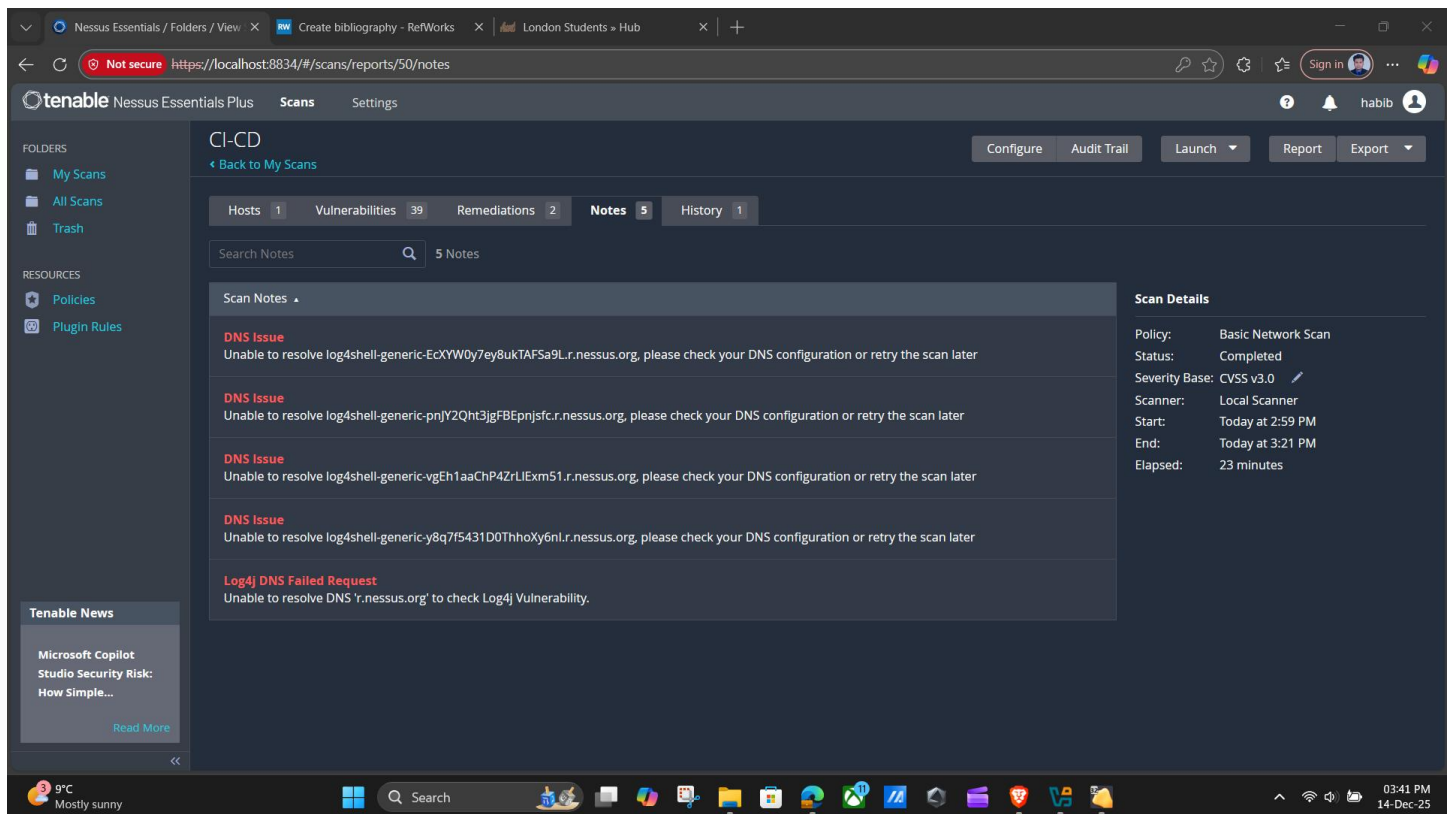


Figure 74: Nessus scan results for CI-CD resources – 6

From Figure 69 to Figure 74 Demonstrate that the Nessus results scanned hosts, vulnerabilities, the recommended remediation actions, and notes that explain the risk level.

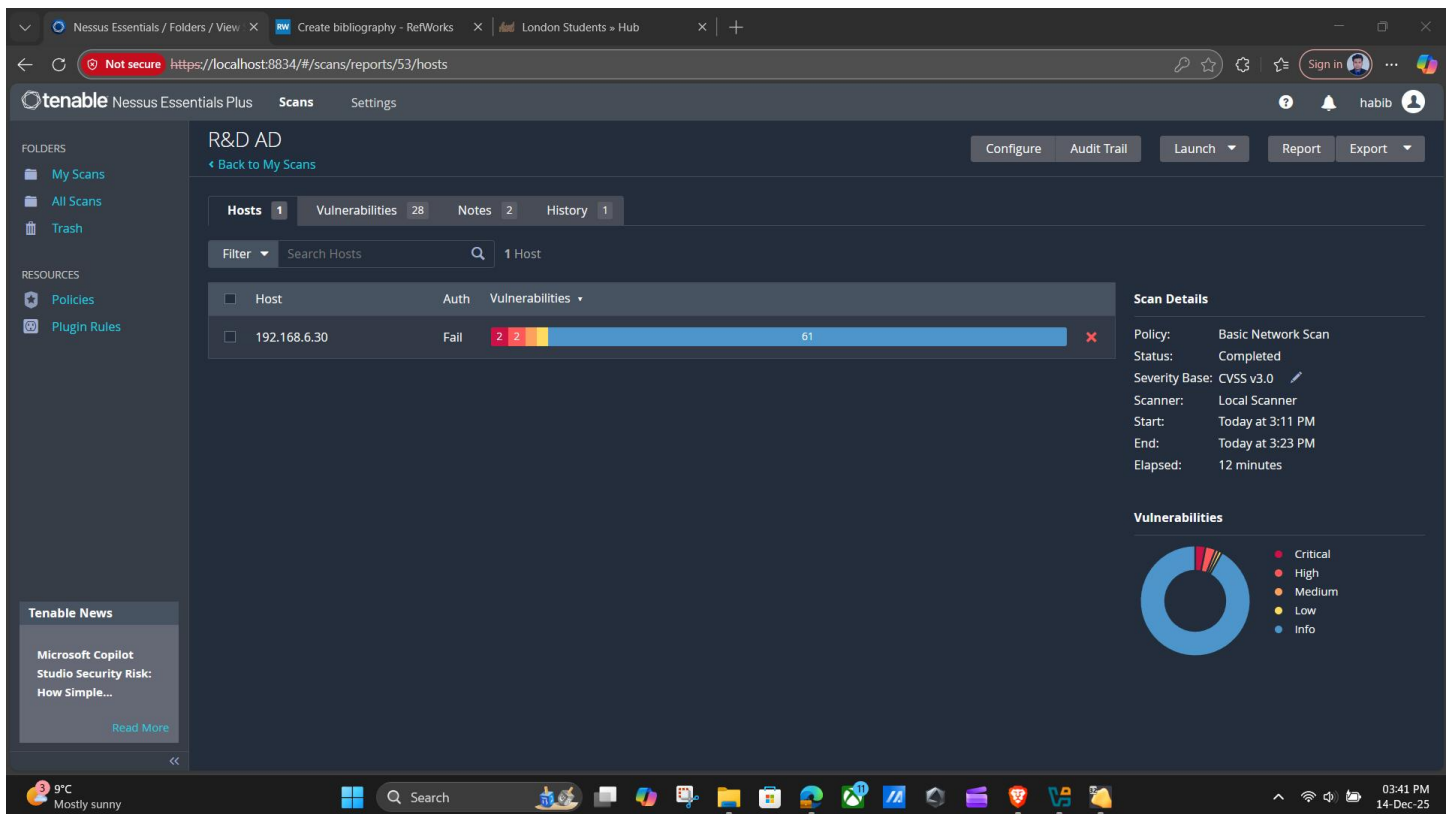


Figure 75: Nessus scan results for R&D AD resources – 1

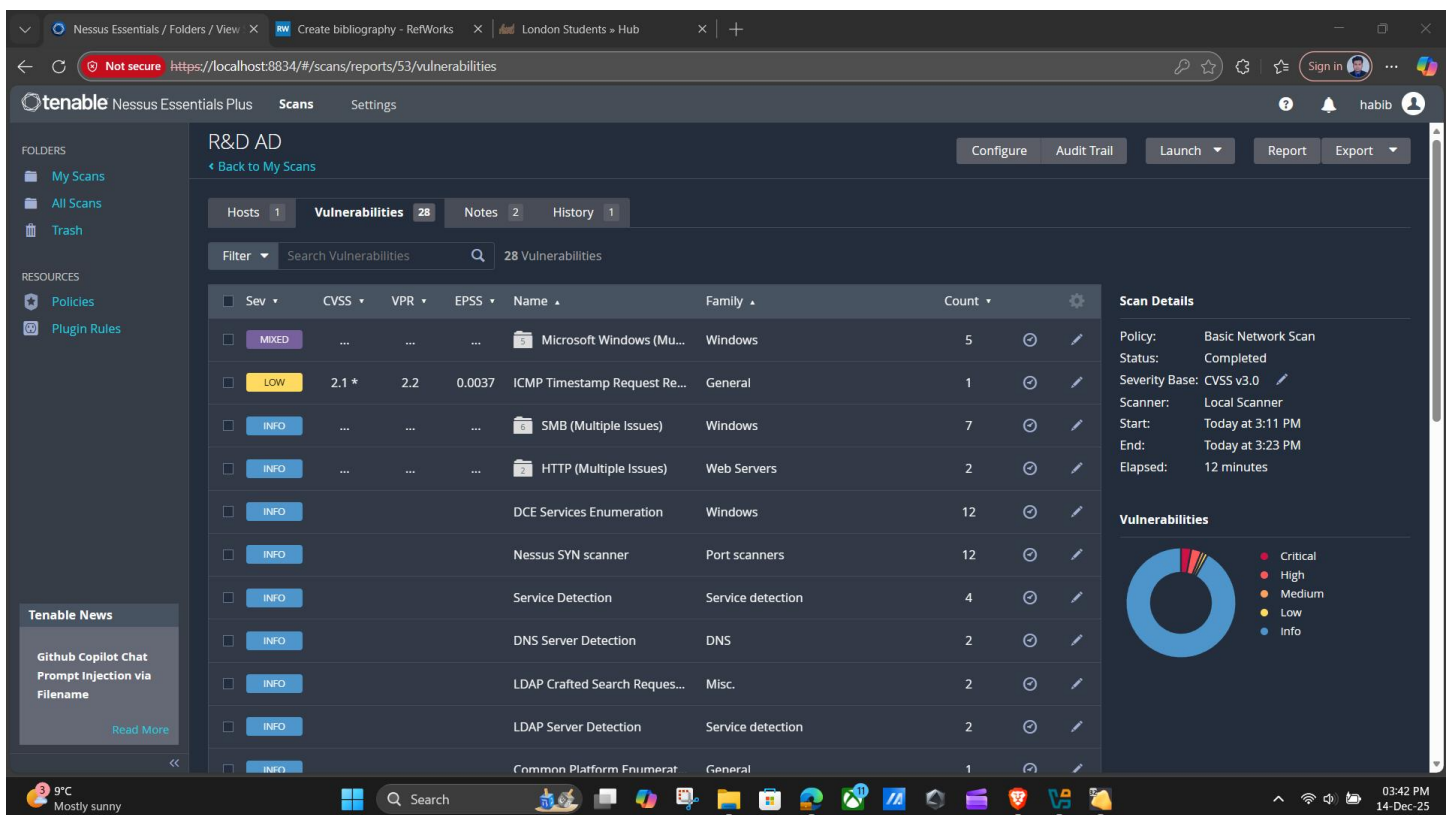


Figure 76: Nessus scan results for R&D AD resources – 2

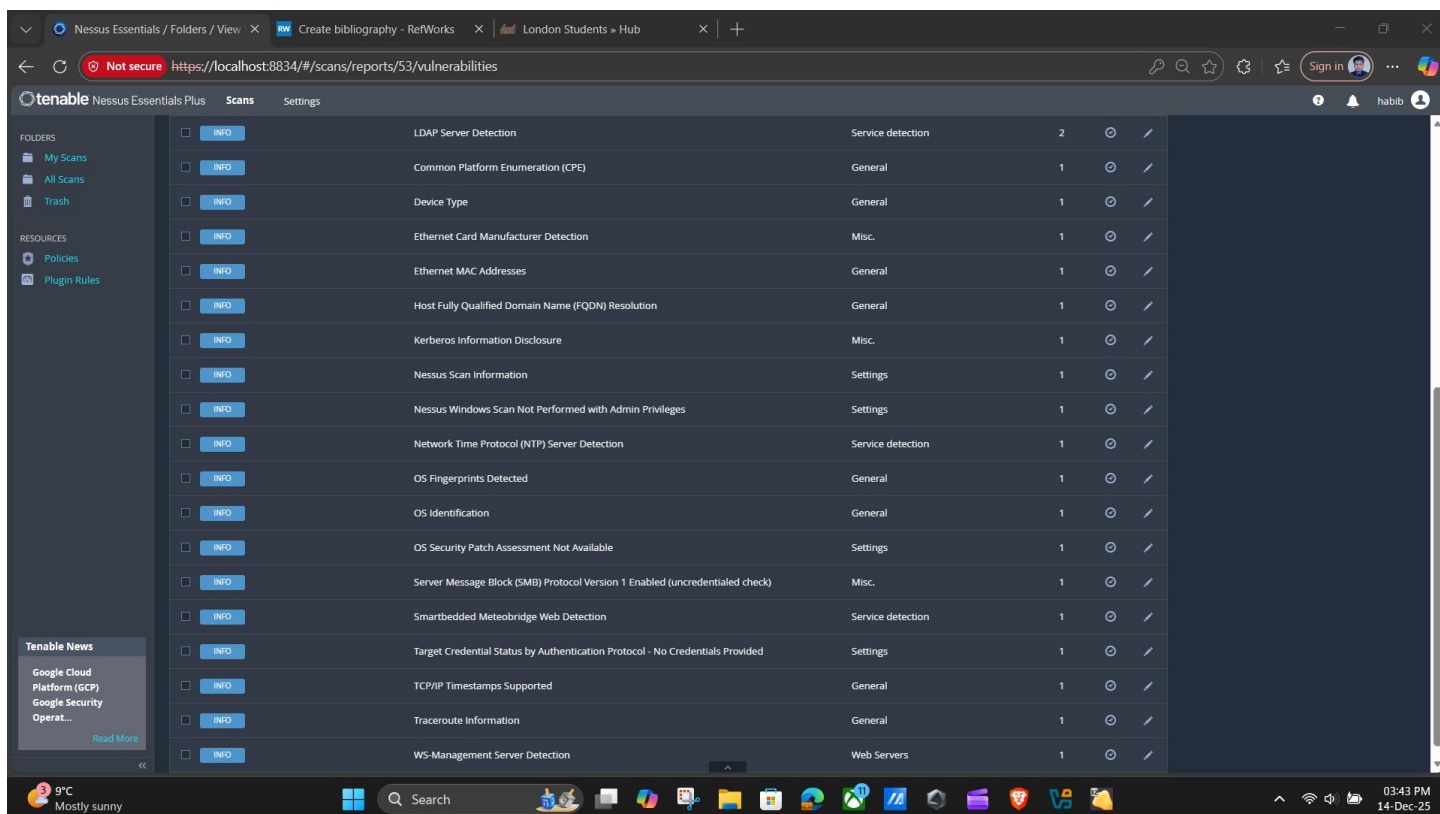


Figure 77: Nessus scan results for R&D AD resources – 3

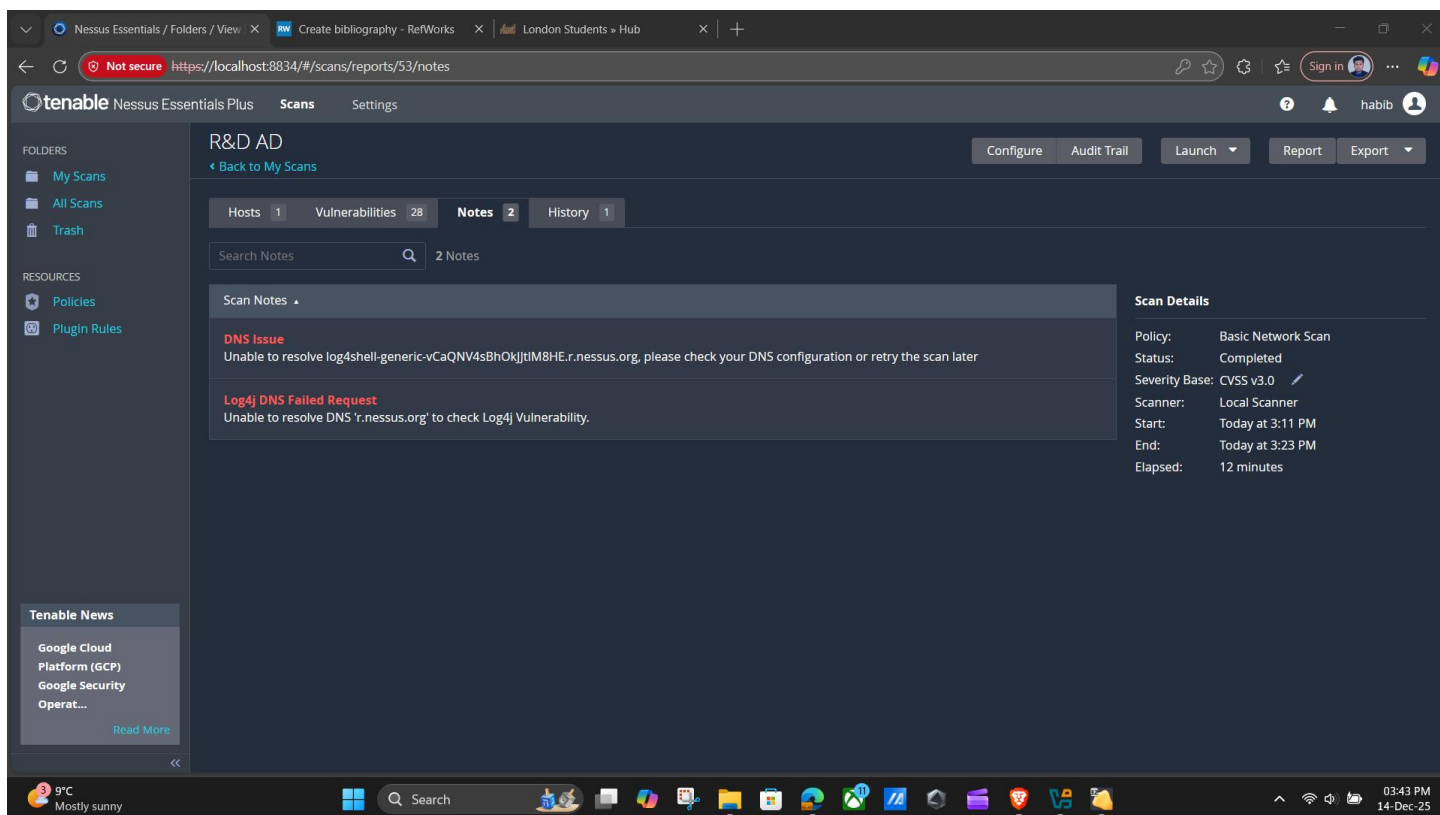


Figure 78: Nessus scan results for R&D AD resources – 4

According to Figure 75 to Figure 78 shows the scanned hosts, vulnerabilities, the recommended remediation actions, and notes that explain the risk level.

6.1.3 Reporting & Analysis

6.1.3.1 Detection Gap Analysis

Big gaps in how threats were detected came to light during the red team test. The problem was that the people interested in bad behavior with valid credentials looked almost exactly like regular users. For the most part, such monitoring was for networks and established threats, which couldn't sniff out more advanced attacks that make use of regularly available system tools.

Another was the CI/CD pipeline. There were not enough logging or alerts, so the physical or virtual operators could easily hide unauthorized actions among normal routine automated operations. It's typical because these systems typically have access to high-level information but are left unwatched.

Finally, logs from on-premises systems and the cloud were not aggregated in a single location. This complicated attempt to link user activity, lateral movement, and data exfiltration. Thanks to these shortcomings, the emulated attacker was able to conduct reconnaissance, lateral movement, and data exfiltration stages without causing meaningful alarms. The attack worked not because it was sophisticated, but rather because the detection was weak.

6.1.3.2 Strategic Recommendations

First, privileged accounts will be protected by phishing-resistant multi-factor authentication (MFA) for both administrative and remote user accounts to minimize the risk from stolen credentials, a factor that paved the way for APT actors [21].

Second, enhancing endpoint detection and response (EDR) to detect unusual usage of built-in tools and utilities such as PowerShell, command-line executables remote administration software. The advertisement shows how connecting detection to MITRE ATT&CK techniques promotes more effective behavioral detection, as well as minimizing the need for simple signature-based alerts [11].

Third, it's critical to centralize logs and integrate them into a SIEM from both on-premises and cloud-based CI/CD environments. Mapping user activities, integrity of pipeline execution, and network communications can be useful in identifying stealthy attacks. This must be combined with automated alerts and periodic threat-hunting drills [22].

And finally, network segmentation, enforcing least-privileged access, and improving management for CI/CD secrets can restrict lateral movement and narrow the impact following a compromise. These measures combined form a layered security strategy to protect both organizational and technical vulnerabilities identified in the assessment.

6.1.3.3 Cost–Benefit Analysis

To justify the recommended security improvements identified during Operation IP Shield, a basic cost–benefit calculation is used. The analysis compares the annual cost of implementing security controls against the expected financial loss from a potential breach involving intellectual property theft.

6.1.3.3.1 Assumptions (Reasonable & Defensible)

- Estimated cost of security improvements per year (MFA, EDR tuning, SIEM integration, CI/CD hardening):
£150,000

- Estimated financial impact of an IP breach
(R&D loss, delayed product release, legal and reputational damage):
£5,000,000
- Estimated annual likelihood of a successful APT-style breach without improvements:
20% (0.2)
(ENISA and NIST indicate high-value sectors face persistent APT targeting)

6.1.3.3.2 Expected Loss Equation

$$\begin{aligned}\text{Expected Annual Loss (EAL)} &= \text{Breach Impact} \times \text{Probability} \\ \text{Expected Annual Loss (EAL)} &= £5,000,000 \times 0.2 = £1,000,000\end{aligned}$$

6.1.3.3.3 Cost–Benefit Comparison

$$\begin{aligned}\text{Net Benefit} &= \text{Expected Annual Loss (EAL)} - \text{Cost of Controls} \\ \text{Net Benefit} &= £1,000,000 - £150,000 = £850,000\end{aligned}$$

6.1.3.3.4 Result

The cost–benefit analysis shows that investing £150,000 per year in improved security controls avoids an expected loss of £1,000,000, resulting in a net annual benefit of approximately £850,000. Therefore, the recommended security improvements are financially justified and economically favorable.

7 Conclusion

In conclusion, security is a crucial element for an organization’s success. This report has highlighted the importance of moving beyond basic vulnerability assessments to adopt advanced offensive security strategies such as adversary emulation and red team operations. By understanding real-world attacker behaviors and applying them ethically, organizations can improve detection, response, and overall resilience against sophisticated threats. These practices not only uncover technical weaknesses but also translate findings into practical, business-focused risk mitigation strategies.

8 References

- [1] S. Kandaswamy, C. Campbell and M. Murira, "Analysing Scope Risk in Vulnerability Assessment and Penetration Testing Methodology," 2024-12-18. doi: 10.1109/contesa64738.2024.10891284.
- [2] A. Fatima, et al., "Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat," 2023-03-07. doi: 10.1109/icbats57792.2023.10111168.
- [3] "National Health Laboratory Service hit by cyber attack." SAnews. <https://www.sanews.gov.za/south-africa/national-health-laboratory-service-hit-cyber-attack> (accessed 4 December).
- [4] D. Sunny. "Cyber attack on South Africa’s laboratory service puts healthcare at risk." Techpoint Africa. <https://techpoint.africa/news/cyber-security-attack-south-africas-healthcare/> (accessed 5 December).
- [5] J. Greig. "South Africa’s national health lab hit with ransomware attack amid mpox outbreak." The Record. <https://therecord.media/south-africa-lab-ransomware-mpox-outbreak> (accessed 7 December).

- [6] J. Greig. "South Africa national lab says ransomware recovery to last until mid-July." The Record. <https://therecord.media/south-africa-national-health-laboratory-service-ransomware-recovery> (accessed 7 December).
- [7] P. Bischoff. "Ransomware gang BlackSuit claims ransomware attack on South Africa's National Health Laboratory Service." Comparitech. <https://www.comparitech.com/news/ransomware-gang-blacksuit-claims-ransomware-attack-on-south-africas-national-health-laboratory-service/> (accessed 7 December).
- [8] "National health lab now fully operational after cyber attack." SAnews. <https://www.sanews.gov.za/south-africa/national-health-lab-now-fully-operational-after-cyber-attack> (accessed 7 December).
- [9] S. Cassim and Z. C. Chapanduka, "Cyberattack on the National Health Laboratory Service of South Africa – implications, response and recommendations," *S Afr Med J*, -11-29 2024. doi: 10.7196/samj.2024.v114i12.2549.
- [10] E. Ellis. "Cyber hack attack: How one click on an email link paralysed SA's National Health Laboratory Service." Daily Maverick. <https://www.dailymaverick.co.za/article/2025-03-22-cyber-hack-attack-how-one-click-on-an-email-link-paralysed-sas-national-health-laboratory-service/> (accessed 7 December).
- [11] "MITRE ATT&CK." MITRE ATT&CK®. <https://attack.mitre.org/> (accessed 5 December).
- [12] "BlackSuit Ransomware." The DFIR Report. <https://thedfirreport.com/2024/08/26/blacksuit-ransomware/> (accessed 7 December).
- [13] "ReliaQuest Threat Research Team, "BlackSuit Attack Analysis"." ReliaQuest. <https://reliaquest.com/blog/blacksuit-attack-analysis/> (accessed 7 December).
- [14] "#StopRansomware: BlackSuit (Royal) Ransomware." CISA. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a> (accessed 12 December).
- [15] "Best Practices for MITRE ATT&CK® Mapping." CISA. <https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping> (accessed 12 December).
- [16] M. Curphey, J. Scambray and E. Olson, "Improving web application security: Threats and countermeasures," Redmond, WA, USA. 2003. Accessed: 15 December 2025. [Online]. <https://www.microsoft.com/en-in/download/details.aspx?id=1330>
- [17] S. Cassim and Z. C. Chapanduka, "Cyberattack on the National Health Laboratory Service of South Africa – implications, response and recommendations," *S Afr Med J*, -11-29 2024. doi: 10.7196/samj.2024.v114i12.2549.
- [18] Financial Crimes Enforcement Network, "Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024," 2025. Accessed: 15 December 2025. [Online]. <https://www.fincen.gov/system/files/2025-12/FTA-Ransomware.pdf>
- [19] "What is Kali Linux?" Kali Linux Documentation. <https://www.kali.org/docs/introduction/what-is-kali-linux/> (accessed 16 December).
- [20] I. Tenable. "Nessus." tenable.com. <https://www.tenable.com/products/nessus> (accessed 16 December).
- [21] Cybersecurity and Infrastructure Security Agency (CISA) & National Security Agency (NSA). "Identity and Access Management: Recommended Best Practices for Administrators." CISA. https://www.cisa.gov/sites/default/files/2023-12/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.pdf (accessed 16 December).

- [22] S. W. Rose, O. Borchert, S. Mitchell and S. Connelly, "Zero Trust Architecture (NIST Special Publication 800- 207)." NIST. <https://csrc.nist.gov/pubs/sp/800/207/final> (accessed 16 December).