NAME- KHUSHEE VIPIN RANE

INTERN ID - 2049

Exploring Port Vulnerabilities in Metasploitable-2 Using Kali Linux

Port Scanning

Description:

Port scanning is the process of probing a target system to identify open network ports and the services listening on them. By analyzing the responses from these probes, one can determine whether a port is open, closed, or filtered. This activity helps in identifying exposed services, operating systems, and possible security weaknesses.

Impact:

- Service Exposure: Reveals running services and their versions.
- System Mapping: Helps attackers understand the internal structure of the target.
- Attack Preparation: Provides a foundation for selecting suitable exploits.
- Firewall Weakness Identification: Detects improperly configured network defenses.

Severity:

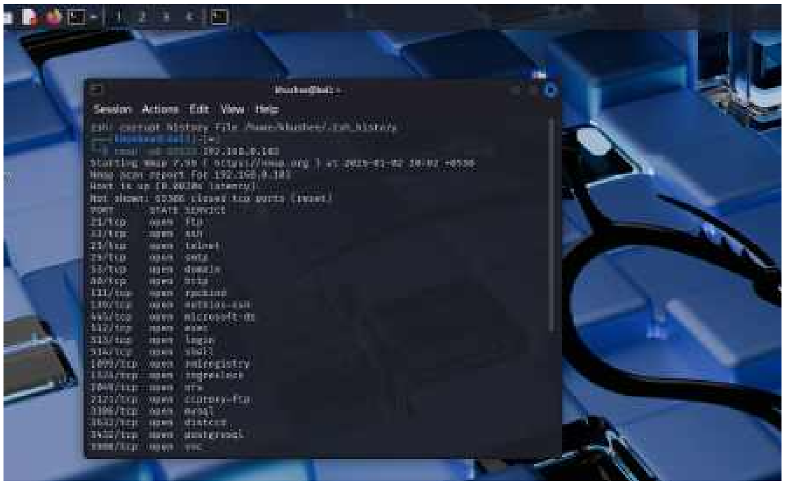
Critical

Remedial:

- Apply restrictive firewall policies
- Monitor traffic using IDS/IPS
- Disable unnecessary services
- Conduct periodic internal scans

To Scan All Ports
Command:

nmap -p0-65535 192.168.0.103



```
zsh: corrupt history file /home/khushee/.zsh_history
┌──(khushee㉿kali)-[~]
└─$ nmap -p0-65535 192.168.0.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-02 20:02 +0530
Nmap scan report for 192.168.0.103
Host is up (0.0020s latency).
Not shown: 65506 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
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
```

1)FTP – Port 21

Description:

Port 21 is used by the File Transfer Protocol to manage file transfer commands. FTP does not encrypt authentication details or transmitted data. In Metasploitable-2, the FTP service runs a vulnerable version of vsFTPd that contains a built-in backdoor.

Impact:

- **Unencrypted Credentials:** Usernames and passwords can be intercepted.
- **Remote Shell Access:** Exploitation leads to direct system access.
- **Automated Attacks:** Frequently targeted by brute-force tools.

Severity:

Critical

Remedial Actions:

- Replace FTP with SFTP
- Disable anonymous access
- Use strong authentication mechanisms
- Keep FTP services updated

Method 1: FTP Client Access

```
ftp 192.168.0.103
```

Connects to the FTP service to upload/download files.
Often used to check anonymous or weak authentication.

Method 2: Anonymous Login Check

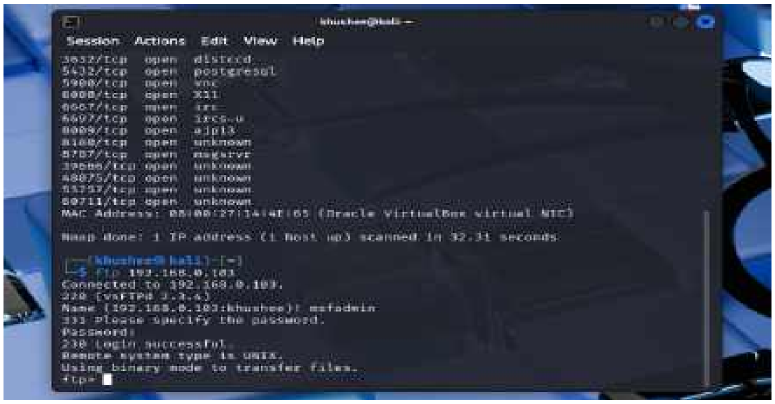
```
ftp
open 192.168.0.103 user: anonymous
password: anonymous
```

Check if the FTP server allows anonymous access without credentials.

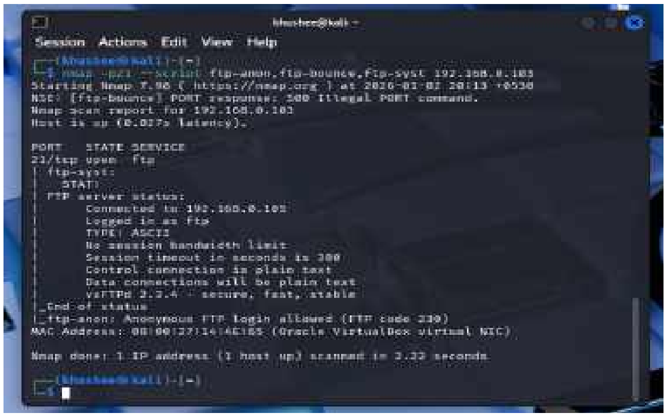
Method 3: Nmap Enumeration

```
nmap -p21 --script ftp-anon,ftp-bounce,ftp-syst
192.168.0.103
```

Enumerates FTP configuration, system info, and anonymous access.



```
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
39606/tcp open  unknown
48875/tcp open  unknown
55757/tcp open  unknown
60711/tcp open  unknown
MAC Address: 08:00:27:14:4E:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 32.31 seconds

┌──(khushee㉿kali)-[~]
└─$ ftp 192.168.0.103
Connected to 192.168.0.103.
220 (vsFTPd 2.3.4)
Name (192.168.0.103:khushee): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```



```
┌──(khushee㉿kali)-[~]
└─$ nmap -p21 --script ftp-anon,ftp-bounce,ftp-syst 192.168.0.103
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-02 20:13 +0530
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Nmap scan report for 192.168.0.103
Host is up (0.027s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.103
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 08:00:27:14:4E:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds

┌──(khushee㉿kali)-[~]
└─$
```

2) SSH – Port 22

Description:

SSH provides encrypted remote login. In Metasploitable-2, SSH is misconfigured with weak credentials, making it vulnerable to brute-force attacks.

Impact:

- **Unauthorized Access:** Attackers can gain shell access.
- **Privilege Escalation:** Can lead to root compromise.

Severity:

High

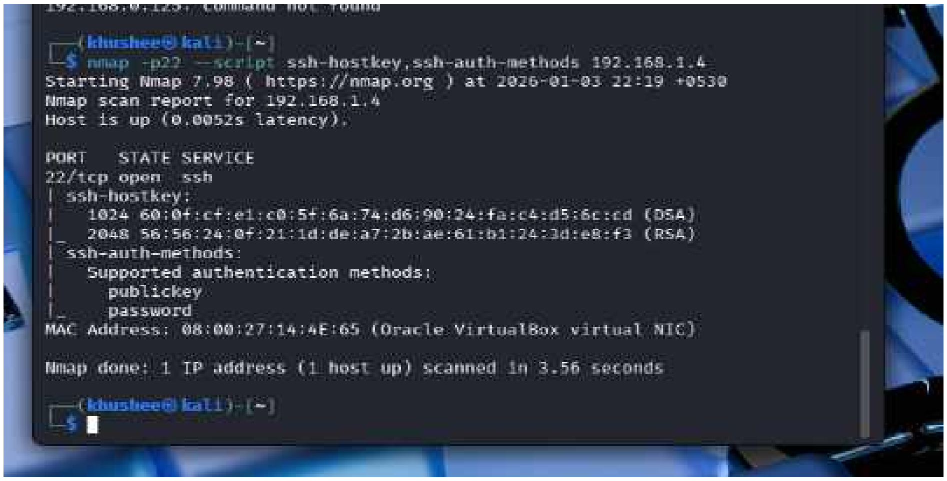
Remedial Actions:

- Disable password authentication
- Use key-based login
- Limit login attempts
- Change default credentials

Method 1: Nmap Enumeration

nmap -p22 --script ssh-hostkey,ssh-auth-methods 192.168.0.125

➡ Extracts SSH version and encryption keys.



```
192.168.0.125: command not found

┌──(khushee㉿kali)-[~]
└─$ nmap -p22 --script ssh-hostkey,ssh-auth-methods 192.168.1.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-03 22:19 +0530
Nmap scan report for 192.168.1.4
Host is up (0.0052s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
MAC Address: 08:00:27:14:4E:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.56 seconds

┌──(khushee㉿kali)-[~]
└─$ 
```

3) Telnet – Port 23

Description:

Telnet allows remote login but transmits data in plaintext. Metasploitable-2 allows login using default credentials, making it extremely insecure.

Impact:

- **Credential Sniffing**

- **Unauthorized Access**

- **Session Hijacking**

Severity:

Critical

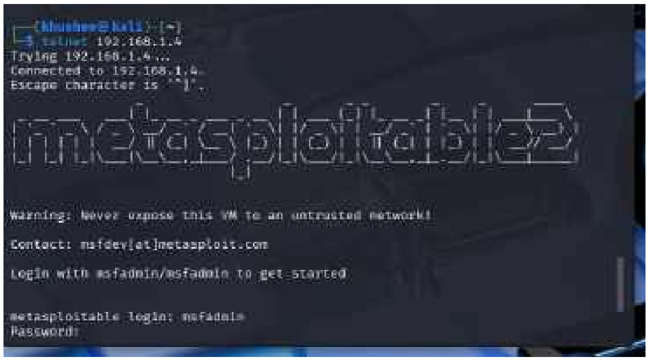
Remedial Actions:

- Disable Telnet

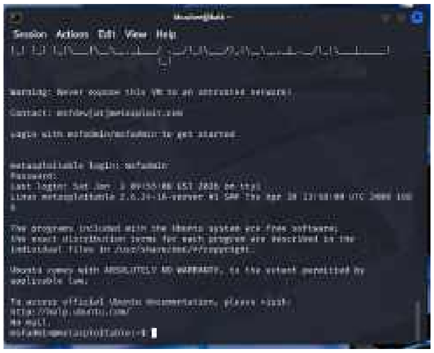
- Replace with SSH

- Enforce encrypted communication

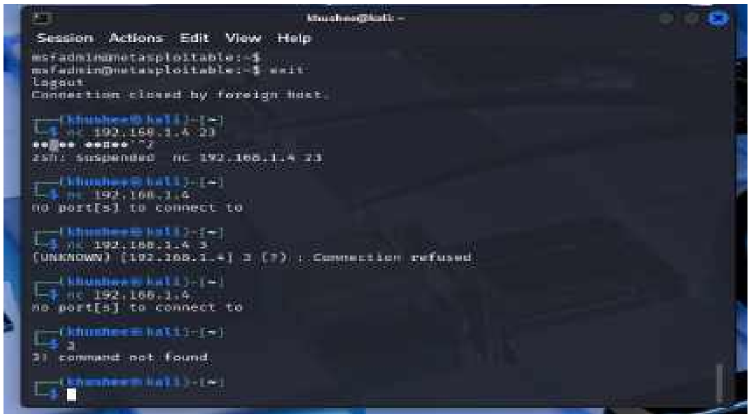
Method 1: Telnet Access
telnet 192.168.0.125
➡ Attempts plaintext remote login to the system.
Method 2: Netcat
nc 192.168.0.125 23
➡ Check if the Telnet service responds and accepts input.



```
┌──(khushee㉿kali)-[~]
└─$ telnet 192.168.1.4
Trying 192.168.1.4...
Connected to 192.168.1.4.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
```



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: [illegible] on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```



```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ exit
logout
Connection closed by foreign host.

┌──(khushee㉿kali)-[~]
└─$ nc 192.168.1.4 23
●●●●● ●●●●●'^Z
zsh: suspended  nc 192.168.1.4 23

┌──(khushee㉿kali)-[~]
└─$ nc 192.168.1.4
no port[s] to connect to

┌──(khushee㉿kali)-[~]
└─$ nc 192.168.1.4 3
(UNKNOWN) [192.168.1.4] 3 (?) : Connection refused

┌──(khushee㉿kali)-[~]
└─$ nc 192.168.1.4
no port[s] to connect to

┌──(khushee㉿kali)-[~]
└─$ 3
3: command not found

┌──(khushee㉿kali)-[~]
└─$ 
```

4) SMTP – Port 25

Description:

SMTP (Simple Mail Transfer Protocol) is responsible for sending emails between servers. In Metasploitable-2, the SMTP service is misconfigured and vulnerable to user enumeration and information disclosure. These weaknesses allow attackers to identify valid system accounts, which can later be used for brute-force or privilege-escalation attacks.

Impact:

- **User Enumeration:** Valid usernames can be discovered.
- **Information Disclosure:** Reveals internal user accounts.
- **Attack Chaining:** Enumerated users can be used in SSH/FTP brute-force attacks.
- **Email Abuse:** Server can be misused for spam or phishing.

Severity:

High

Remedial Actions:

- Disable SMTP VRFY and EXPN commands
- Restrict SMTP access using firewall rules
- Enable authentication for mail services
- Regularly update and harden mail server configuration

Method 1: SMTP User Enumeration Using Nmap

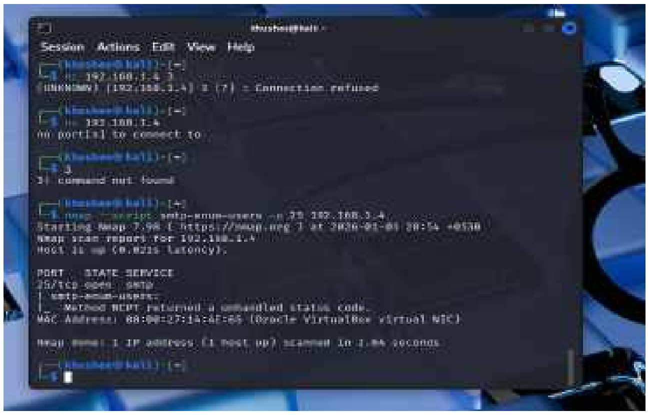
Command:

```
nmap --script smtp-enum-users -p 25 192.168.1.4
```

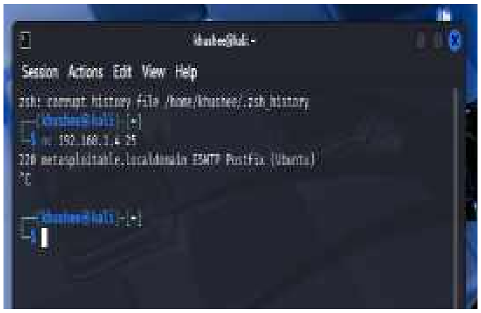
Method 2: Banner Grabbing (Information Disclosure)

Command:

```
nc 192.168.1.4 25
```



```
┌──(khushee㉿kali)-[~]
└─$ nc 192.168.1.4 3
(UNKNOWN) [192.168.1.4] 3 (?) : Connection refused

┌──(khushee㉿kali)-[~]
└─$ nc 192.168.1.4
no port[s] to connect to

┌──(khushee㉿kali)-[~]
└─$ 3
3: command not found

┌──(khushee㉿kali)-[~]
└─$ nmap --script smtp-enum-users -p 25 192.168.1.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-01 20:54 +0530
Nmap scan report for 192.168.1.4
Host is up (0.0021s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
MAC Address: 08:00:27:14:6E:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds

┌──(khushee㉿kali)-[~]
└─$ 
```



```
zsh: corrupt history file /home/khushee/.zsh_history
┌──(khushee㉿kali)-[~]
└─$ nc 192.168.1.4 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
^C

┌──(khushee㉿kali)-[~]
└─$ 
```

5) DNS – Port 53

Description:

Domain Name System (DNS) operates on port 53 and is responsible for translating domain names into IP addresses. A DNS server may also store records related to hosts, mail servers, and name servers. In Metasploitable-2, DNS is intentionally misconfigured, allowing attackers to gather sensitive domain information through enumeration techniques.

Impact:

- Network Mapping: Reveals internal hostnames and IP addresses.
- Information Disclosure: Exposes DNS records such as A, MX, and NS.
- Attack Planning: Helps attackers identify potential targets within the network.
- Facilitates Further Attacks: Discovered hosts can be used for service exploitation.

Severity:

High

Remedial Actions:

- Disable DNS zone transfers for unauthorized hosts
- Restrict DNS queries using access control lists
- Monitor DNS logs for suspicious requests
- Keep DNS software updated and hardened

Method 1: DNS Enumeration

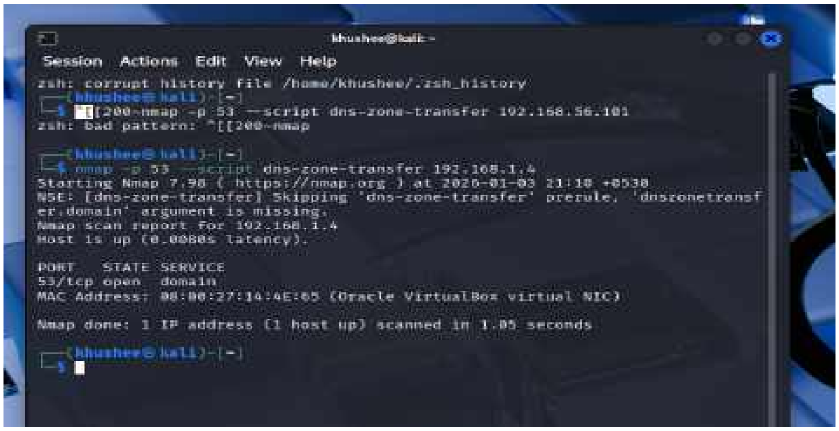
```
nmap -p53 --script dns-recursion 192.168.1.4
```

➡ Checks if recursive queries are allowed.

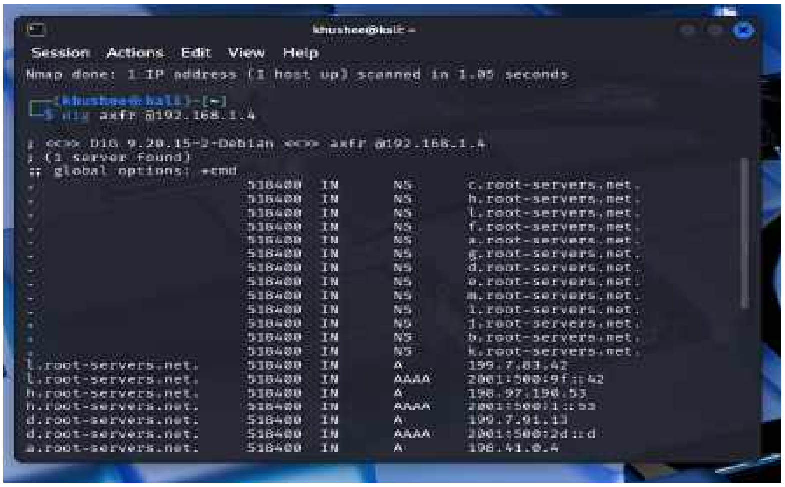
Method 2: Zone Transfer Attempt

dig axfr @192.168.1.4

➡ Attempts to dump DNS records.



```
zsh: corrupt history file /home/khushee/.zsh_history
┌──(khushee㉿kali)-[~]
└─$ ^[[200~nmap -p 53 --script dns-zone-transfer 192.168.56.101
zsh: bad pattern: ^[[200~nmap

┌──(khushee㉿kali)-[~]
└─$ nmap -p 53 --script dns-zone-transfer 192.168.1.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-03 21:10 +0530
NSE: [dns-zone-transfer] Skipping 'dns-zone-transfer' prerule, 'dnszonetransf
er.domain' argument is missing.
Nmap scan report for 192.168.1.4
Host is up (0.0080s latency).

PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 08:00:27:14:4E:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds

┌──(khushee㉿kali)-[~]
└─$ 
```



```
Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds

┌──(khushee㉿kali)-[~]
└─$ dig axfr @192.168.1.4

; <<>> DiG 9.20.15-2-Debian <<>> axfr @192.168.1.4
; (1 server found)
;; global options: +cmd
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
l.root-servers.net.     518400  IN      A       199.7.83.42
l.root-servers.net.     518400  IN      AAAA    2001:500:9f::42
h.root-servers.net.     518400  IN      A       198.97.190.53
h.root-servers.net.     518400  IN      AAAA    2001:500:1::53
d.root-servers.net.     518400  IN      A       199.7.91.13
d.root-servers.net.     518400  IN      AAAA    2001:500:2d::d
a.root-servers.net.     518400  IN      A       198.41.0.4
```

6) HTTP – Port 80

Description:

Port 80 hosts web applications such as DVWA and Mutillidae, which are intentionally vulnerable. These applications allow exploitation through common web attacks like SQL injection and command execution.

Impact:

- **Database Exposure:** Sensitive information can be extracted.
- **Web Shell Deployment:** Attackers can upload malicious scripts.
- **Remote Command Execution:** Full control of the server.

Severity:

Critical

Remedial Actions:

- Validate and sanitize user input
- Apply security patches
- Use web application firewalls
- Remove vulnerable test applications

Method 1: Web Browser

```
dirb http://192.168.56.101
```

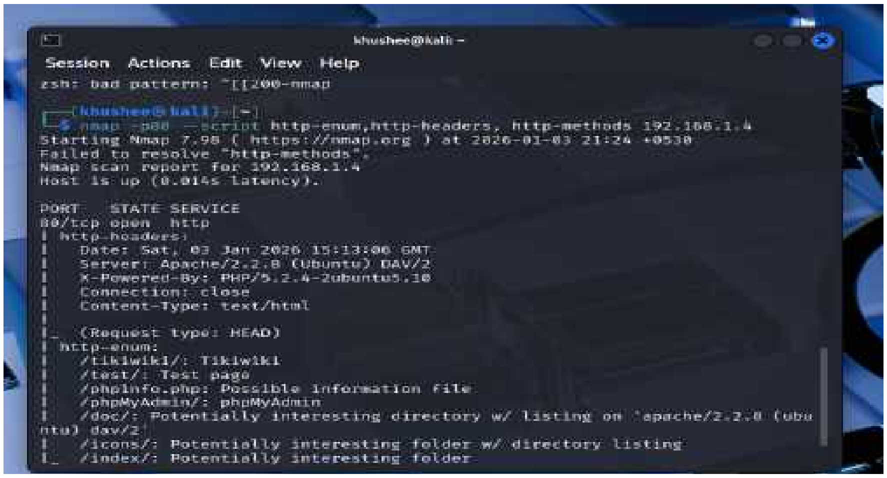
```
sqlmap -u "http://192.168.56.101/..." --dbs
```

➡ Directly accesses the web application hosted on the server.

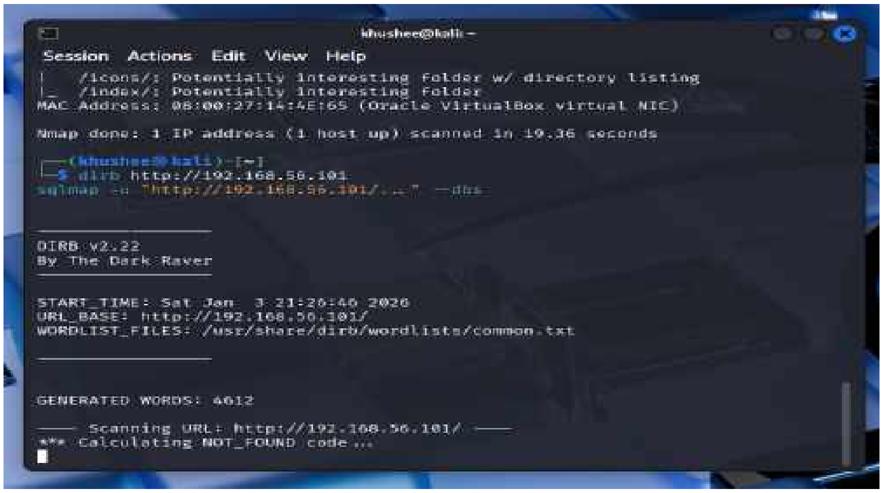
Method 2: Nmap Web Scripts

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

192.168.1.4
```

➡ Discovers directories, server headers, and web technologies.



```
zsh: bad pattern: ^[[200~nmap

┌──(khushee㉿kali)-[~]
└─$ nmap -p80 --script http-enum,http-headers, http-methods 192.168.1.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-03 21:24 +0530
Failed to resolve "http-methods".
Nmap scan report for 192.168.1.4
Host is up (0.014s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-headers:
|   Date: Sat, 03 Jan 2026 15:13:06 GMT
|   Server: Apache/2.2.8 (Ubuntu) DAV/2
|   X-Powered-By: PHP/5.2.4-2ubuntu5.10
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubu
ntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
```



```
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
MAC Address: 08:00:27:14:4E:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.36 seconds

┌──(khushee㉿kali)-[~]
└─$ dirb http://192.168.56.101
sqlmap -u "http://192.168.56.101/..." --dbs


-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jan  3 21:26:46 2026
URL_BASE: http://192.168.56.101/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.101/ ----
*** Calculating NOT_FOUND code...
█
```

7) Port 111 – RPCBind

Description:

RPCBind (Remote Procedure Call Binder) operates on port 111 and acts as a directory service for RPC-based applications. It maps RPC program numbers to their corresponding network port numbers, allowing clients to locate services such as NFS, mountd, and statd. In Metasploitable-2, RPCBind is openly accessible and exposes detailed information about running RPC services.

Impact:

- **Service Enumeration:** Reveals active RPC services and their ports.
- **Information Leakage:** Discloses internal service architecture.
- **Attack Chaining:** Enables attackers to identify exploitable services like NFS.
- **Network Reconnaissance:** Assists in mapping backend services.

Severity:

High

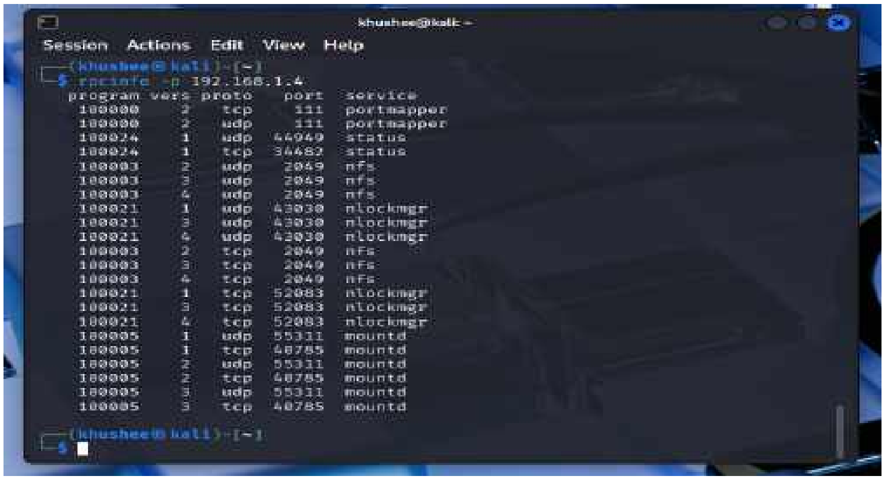
Remedial Actions:

- Restrict RPCBind access using firewall rules
- Disable unnecessary RPC services
- Allow RPC traffic only from trusted hosts
- Monitor RPC-related activity in system logs

Method 1: RPC Enumeration

```
rpcinfo -p 192.168.1.4
```

➡ Lists all RPC services.



```
┌──(khushee㉿kali)-[~]
└─$ rpcinfo -p 192.168.1.4
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  44949  status
    100024    1   tcp  34482  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  43030  nlockmgr
    100021    3   udp  43030  nlockmgr
    100021    4   udp  43030  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  52083  nlockmgr
    100021    3   tcp  52083  nlockmgr
    100021    4   tcp  52083  nlockmgr
    100005    1   udp  55311  mountd
    100005    1   tcp  40785  mountd
    100005    2   udp  55311  mountd
    100005    2   tcp  40785  mountd
    100005    3   udp  55311  mountd
    100005    3   tcp  40785  mountd

┌──(khushee㉿kali)-[~]
└─$ 
```

8)rexec-Port 512

Description:

Port 512 is used by the **rexec (Remote Execution)** service, which allows users to execute commands on a remote system after authentication. The rexec protocol is considered insecure because it transmits usernames and passwords in plaintext. In Metasploitable-2, the rexec service is enabled and configured with weak credentials, making it vulnerable to unauthorized access.

Impact:

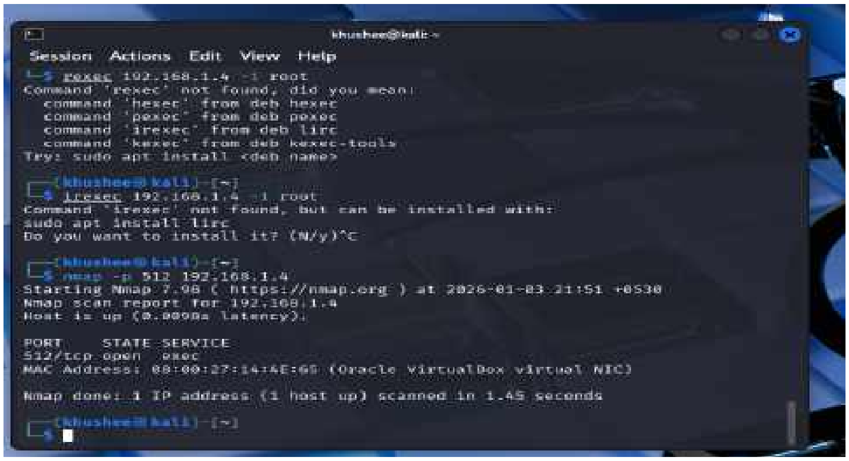
- **Plaintext Credential Exposure:** Login details can be intercepted.
- **Remote Command Execution:** Attackers can run system commands remotely.
- **Unauthorized Access:** Weak credentials allow easy compromise.
- **Privilege Escalation:** May lead to higher-level access on the system.

Severity:

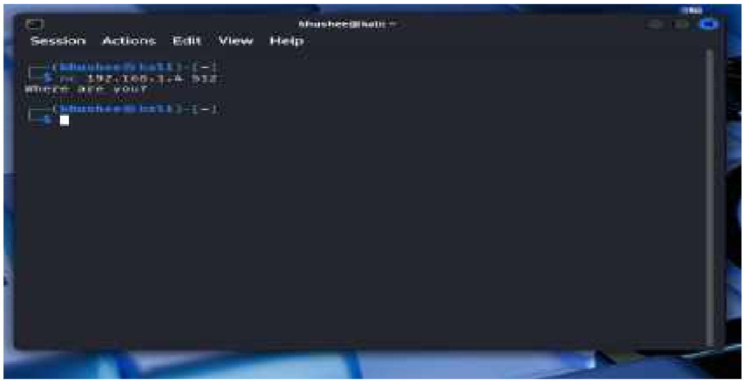
High

Remedial Actions:

- Disable rexec service if not required
- Replace rexec with secure alternatives like SSH
- Enforce strong authentication mechanisms
- Block port 512 at the firewall



```
└─$ rexec 192.168.1.4 -l root
Command 'rexec' not found, did you mean:
  command 'hexec' from deb hexec
  command 'pexec' from deb pexec
  command 'irexec' from deb lirc
  command 'kexec' from deb kexec-tools
Try: sudo apt install <deb name>

┌──(khushee㉿kali)-[~]
└─$ irexec 192.168.1.4 -l root
Command 'irexec' not found, but can be installed with:
sudo apt install lirc
Do you want to install it? (N/y)^C

┌──(khushee㉿kali)-[~]
└─$ nmap -p 512 192.168.1.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-03 21:51 +0530
Nmap scan report for 192.168.1.4
Host is up (0.0098s latency).

PORT    STATE SERVICE
512/tcp open  exec
MAC Address: 08:00:27:14:4E:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds

┌──(khushee㉿kali)-[~]
└─$ 
```



```
┌──(khushee㉿kali)-[~]
└─$ nc 192.168.1.4 512
Where are you?

┌──(khushee㉿kali)-[~]
└─$ 
```

9) rlogin-Port 513

Description:

Port 513 is used by the **rlogin (Remote Login)** service, which allows users to log into a remote system over a network. The rlogin protocol relies on host-based authentication and transmits data, including credentials, in plaintext. In Metasploitable-2, rlogin is enabled with weak trust relationships, making it vulnerable to unauthorized access.

Impact:

- **Plaintext Authentication:** User credentials can be intercepted.
- **Trust Exploitation:** Misconfigured `.rhosts` files allow passwordless access.
- **Unauthorized Login:** Attackers can gain shell access remotely.
- **System Compromise:** Can lead to further privilege escalation.

Severity:

High

Remedial Actions:

- Disable rlogin service entirely
- Remove trust-based authentication files
- Replace rlogin with SSH
- Block port 513 at the firewall

Method 1: rlogin Access

rlogin 192.168.1.4 -l root

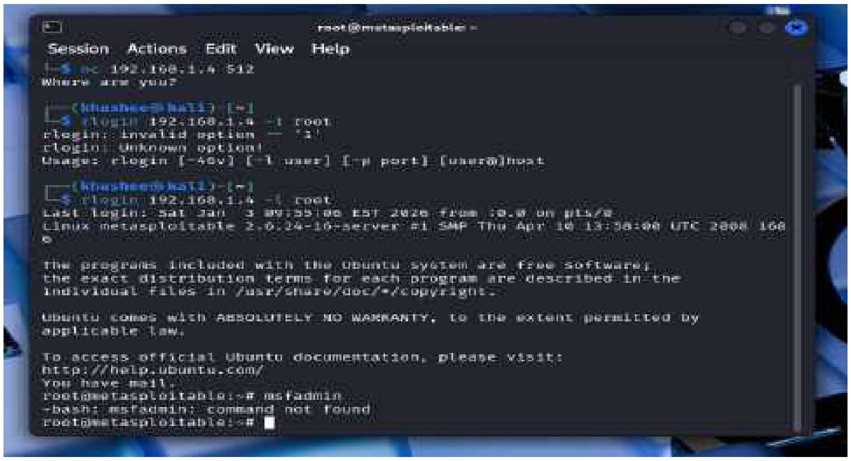
➡ Attempts remote login.

Method 2: Banner Verification Using Netcat

Command:

```
nc 192.168.1.4 513
```

➡Netcat is used to confirm that the rlogin service is accessible on the specified port.



```
└─$ nc 192.168.1.4 512
Where are you?

┌──(khushee㉿kali)-[~]
└─$ rlogin 192.168.1.4 -1 root
rlogin: invalid option -- '1'
rlogin: Unknown option!
Usage: rlogin [-46v] [-l user] [-p port] [user@]host

┌──(khushee㉿kali)-[~]
└─$ rlogin 192.168.1.4 -l root
Last login: Sat Jan  3 09:55:06 EST 2026 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# msfadmin
-bash: msfadmin: command not found
root@metasploitable:~# █
```

10) rsh-Port 514

Description:

Port 514 is used by the **rsh (Remote Shell)** service, which enables users to execute commands on a remote system without establishing a full login session. The rsh protocol relies on host-based trust relationships and transmits data without encryption. In Metasploitable-2, rsh is enabled with insecure configurations, allowing attackers to execute commands remotely.

Impact:

- **Unauthenticated Command Execution:** Commands may run without proper authentication.

- **Plaintext Communication:** Data and commands can be intercepted.

- **Trust Abuse:** Misconfigured trust files allow attackers to bypass passwords.

- **System Takeover:** Remote execution can lead to full compromise.

Severity:

High

Remedial Actions:

- Disable rsh service completely

- Remove `.rhosts` and host-based trust configurations

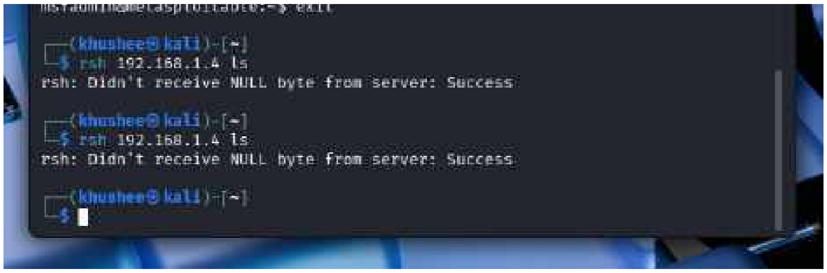
- Use SSH instead of rsh

- Block port 514 using firewall rules

Method 1: rsh Command Execution

rsh 192.168.0.125 ls

➡ Executes commands remotely



```
msfadmin@metasploitable:~$ exit

┌──(khushee㉿kali)-[~]
└─$ rsh 192.168.1.4 ls
rsh: Didn't receive NULL byte from server: Success

┌──(khushee㉿kali)-[~]
└─$ rsh 192.168.1.4 ls
rsh: Didn't receive NULL byte from server: Success

┌──(khushee㉿kali)-[~]
└─$ 
```