Name : Ritesh Lakhani
Enrollment No : 22010101099

Metasploit Room

Task 1 Introduction to Metasploit

Metasploit is the most widely used exploitation framework. Metasploit is a powerful tool that can support all phases of a penetration testing engagement, from information gathering to post-exploitation.

Metasploit has two main versions:

- **Metasploit Pro**: The commercial version that facilitates the automation and management of tasks. This version has a graphical user interface (GUI).
- **Metasploit Framework**: The open-source version that works from the command line. This room will focus on this version, installed on the AttackBox and most commonly used penetration testing Linux distributions.

The Metasploit Framework is a set of tools that allow 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 exploit development.

The main components of the Metasploit Framework can be summarized as follows;

- **msfconsole**: The main command-line interface.
- **Modules**: supporting modules such as exploits, scanners, payloads, etc.
- **Tools**: Stand-alone tools that will help vulnerability research, vulnerability assessment, or penetration testing. Some of these tools are msfvenom, pattern_create and pattern_offset. We will cover msfvenom within this module, but pattern_create and pattern_offset are tools useful in exploit development which is beyond the scope of this module.

This room will cover the main components of Metasploit while providing you with a solid foundation on how to find relevant exploits, set parameters, and exploit vulnerable services on the target system. Once you have completed this room, you will be able to navigate and use the Metasploit command line comfortably.

Press the **Start Machine** button below.

Start the AttackBox by pressing the **Start AttackBox** button at the top of this page to complete tasks and answer the questions. The AttackBox machine will start in Split-Screen view. If it is not visible, use the blue **Show Split View** button at the top of the page.

Answer the questions below

No answer needed

No answer needed ✓ Correct Answer

Task 2 Main Components of Metasploit

If you wish to familiarize yourself further with these modules, you can find them under the modules folder of your Metasploit installation. For the AttackBox these are under /opt/metasploit-framework/embedded/framework/modules

Answer the questions below

What is the name of the code taking advantage of a flaw on the target system?

Exploit — ✓ Correct Answer

What is the name of the code that runs on the target system to achieve the attacker's goal?

Payload — ✓ Correct Answer

What are self-contained payloads called?

Singles — ✓ Correct Answer

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

Singles — ✓ Correct Answer

Task 3 MfsConsole

```
   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   auxiliary/admin/http/dlink_dir_300_600_exec_noauth  2013-02-04       normal  No     D-Link DIR-600 / DIR-300 Unauthenticated Remote
   1   auxiliary/admin/http/netgear_r6700_pass_reset       2020-06-15       normal  Yes    Netgear R6700v3 Unauthenticated LAN Admin Passw
   2   auxiliary/dos/cisco/ios_telnet_rocem                2017-03-17       normal  No     Cisco IOS Telnet Denial of Service
   3   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof        2010-12-21       normal  No     Microsoft IIS FTP Server Encoded Response Overf
   4   auxiliary/scanner/ssh/juniper_backdoor              2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   5   auxiliary/scanner/telnet/brocade_enable_login                        normal  No     Brocade Enable Login Check Scanner
   6   auxiliary/scanner/telnet/lantronix_telnet_password                   normal  No     Lantronix Telnet Password Recovery
   7   auxiliary/scanner/telnet/lantronix_telnet_version                    normal  No     Lantronix Telnet Service Banner Detection
   8   auxiliary/scanner/telnet/satel_cmd_exec             2017-04-07       normal  No     Satel Iberia SenNet Data Logger and Electricity
   9   auxiliary/scanner/telnet/telnet_encrypt_overflow                     normal  No     Telnet Service Encryption Key ID Overflow Detec
   10  auxiliary/scanner/telnet/telnet_login                                normal  No     Telnet Login Check Scanner
   11  auxiliary/scanner/telnet/telnet_ruggedcom                            normal  No     RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/telnet_version                              normal  No     Telnet Service Banner Detection
   13  auxiliary/server/capture/telnet                                      normal  No     Authentication Capture: Telnet


Interact with a module by name or index, for example use 13 or use auxiliary/server/capture/telnet

msf6 >
```

Please remember that exploits take advantage of a vulnerability on the target system and may always show unexpected behavior. A low-ranking exploit may work perfectly, and an excellent ranked exploit may not, or worse, crash the target system.

Answer the questions below

How would you search for a module related to Apache?

search apache — ✓ Correct Answer

Who provided the auxiliary/scanner/ssh/ssh_login module?

todb — ✓ Correct Answer — Hint

Task 4 Working With Modules

Interacting with sessions

```
msf6 > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12.229)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12.229)

msf6 > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Answer the questions below

How would you set the LPORT value to 6666?

set LPORT 6666 — ✓ Correct Answer

How would you set the global value for RHOSTS to 10.10.19.23 ?

setg RHOSTS 10.10.19.23 — ✓ Correct Answer

What command would you use to clear a set payload?

unset PAYLOAD — ✓ Correct Answer

What command do you use to proceed with the exploitation phase?

exploit — ✓ Correct Answer

Task 5 Summary

Task 5 Summary

As we have seen so far, Metasploit is a powerful tool that facilitates the exploitation process. The exploitation process comprises three main steps; finding the exploit, customizing the exploit, and exploiting the vulnerable service.

Metasploit provides many modules that you can use for each step of the exploitation process. Through this room, we have seen the basic components of Metasploit and their respective use.

It would be best if you also had used the ms17_010_eternalblue exploit to gain access to the target VM.

In the following rooms, we will cover Metasploit and its components in more detail. Once completed, this module should give you a good understanding of the capabilities of Metasploit.

Answer the questions below

No answer needed.

No answer needed — ✓ Correct Answer