Assignment 2

New Attempt

- Due Sep 24, 2024 by 11:59pm
- Points 100
- Submitting a file upload
- File Types pdf

Due: Tuesday, September 24, 2024 (11:59 PM). Please submit your assignment on Canvas as a PDF.

Vulnerability Exploitation

After gathering information and identifying vulnerabilities, the next step is to exploit these vulnerabilities to attempt to gain access to the target system. The Metasploit Framework is an exploit development framework that facilitates penetration testing of computer systems by automating this process. The Metasploit framework has vulnerability scanning tools, malicious code generators, evasion applications (to escape IDS or antivirus for running exploits), password attack tools, and many more. In this assignment, you will get familiar with exploitation tools such as Metasploit and MSFvenom. The goal is to gain access to the target machine by setting up and delivering an exploit

We need to find the host IP address of the target to launch remote exploitation. This assignment is a continuation of Assignment 1, and it is assumed that you have the result of this assignment.

Setup

In order to fire up Metasploit type `msfconsole` in the terminal

Information about Metasploit

Below is the discretion of the Metasploit's modules:

- Exploits - Malicious software for exploiting a vulnerability in a remote machine to gain access and deliver a payload.
- Payloads: Applications or configurations that are used to establish a foothold on a system in the post-exploitation step.
- Encoders - Obfuscates exploits and payloads to bypass AV or IDS/IPS.
- Auxiliary - Any module which is not an exploit such asone-off actions such as port scanning, denial of service, and even fuzzing tool.
- Post - Automation modules for post-exploitation with the purpose of establishing access to a system or network.
- NOP - A node module generates no-operation instructions to pad out buffers.

After running the `msfconsole` command you can see the number of different modules in the Metasploit Framework.

Type `show exploits` and explore the result. Research about Name, Date, Rank, and Description fields in the output.

Another useful term is Common Vulnerabilities and Exposures (CVE). The Common Vulnerabilities and Exposures (CVE) provides a reference method for publicly known information-security vulnerabilities and exposures. An example CVE is CVE-2007-0994 (**https://nvd.nist.gov/vuln/detail/CVE-2007-0994 (https://nvd.nist.gov/vuln/detail/CVE-2007-0994)**).

Useful commands in Metasploit

- `search <name>` #searches exploits/attacks that match a particular string
- `use <exploit/attack>` #uses an exploit
- `show options` #shows the options of an exploit after using it
- `set <option> <value>` #set an option of an exploit
- `exploit` #run the exploit
- `info <exploit/attack>` #prints information about a particular exploit/attack

1 Auxiliary attacks

Select a suitable vulnerability you found in Nessus in the previous assignment and perform an auxiliary attack through Metasploit.

Task 1 (8%): Explain the steps and commands you used to perform it. What does this attack do? Analyze the results you got from performing this attack. Also, report the equivalent CVE of the attack you performed.

Meterpreter is an advanced, dynamically extensible payload that uses in-memory DLL injection stages and is extended over the network at runtime in order to execute code remotely. There are two main ways a Meterpreter works:

- Bind TCP: Starts a server on the target machine and a client running in the attacker machine sends remote commands to be executed
- Reverse TCP: Starts a server on the attacker machine and a client running in the target machine probes the server for commands to be executed

Because of the nature of Bind TCP, it is not a good idea to use this method because it would have to bypass any firewall that protects the target machine. The reverse TCP can easily bypass firewalls because it can start and listen on port 80 which is allowed by almost all firewalls.

2 Exploits

Use Metasploit to search for vulnerabilities MS11-030, MS12-020 and MS17-010, then select one to exploit and gain remote access to the target system.

Task 2 (8%): After setting all options perform the exploit. Report the steps & commands you used in order to gain remote access to the system.

Task 3 (8%): Do research and find out which vulnerability the exploit takes advantage of.

Task 4 (3%): What is the *CVE* of the exploit you used?

3 Meterpreter

After acquiring a session with Meterpreter you have several options. You can navigate out of the current Meterpreter session and explore more exploits. You can navigate back to the session and explore the commands that Meterpreter offers.

Task 5 (3%): Using the Meterpreter session you created, report how you can suppress the current Meterpreter session in the background and how you can navigate back to the current session

Task 6 (5%): What are the Meterpreter commands to capture the keys pressed by the target machine?

Task 7 (8%): What is the command to get the running processes in the target machine? Why is it useful according to your opinion?

Task 8 (8%): What is the command to get a real-time view of the target machine? Why is it useful according to your opinion?

Task 9 (10%): Without performing any extra exploit, explain, in your opinion, why you would need to background the current Meterpreter session in order to perform another task. What would this task be in relation to the current Meterpreter session?

MSFvenom is a payload generation tool within the Metasploit framework that allows users to generate custom payloads for exploitation, offering flexibility in crafting attacks for different operating systems and environments. This part is about creating a custom payload with the software MSFvenom and then serving it to the target. You will learn how to use the multi/handler from Metasploit in combination with a custom payload.

4 Custom Payloads and MsfVenom

Task 10 (10%): Using MSFvenom create an executable version of Meterpreter (payload) that connects to the port `4449` of the Windows system and any port of the Kali machine. The payload must be an executable Windows file (.exe) and must use a reverse shell. What command did you use?

Task 11 (5%): Next, start the Apache2 service (`service apache2 start`) and delete everything in the directory `/var/www/html`. Copy the payload you just created to that folder and create an HTML file with a link to the payload. Report the created HTML file.

Task 12 (10%): Open Metasploit (`msfconsole`) and using the multi/handler module create a server that listens to the port `4449` (same port as the Meterpreter you just configured). Report how you did it and the commands you used.

Task 13 (4%): Visit the attacker's IP from the target machine and download the malicious payload. Run it and confirm that a Meterpreter session is opened. Report a relevant screenshot of the session.

Task 14 (10%): Why would one use MSFvenom instead of Metasploit? Elaborate and explain one example scenario to do so.