METASPLOIT FOR PENTEST & IDS DEVELOPMENT

Metasploit is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It offers many exploits and payloads, making it an asset for offensive and defensive cybersecurity teams.

Key Features of Metasploit are…

- Penetration Testing
- Exploits and Payloads
- Exploit Development
- Post-Exploitation Modules
- Automation

The Metasploit Framework is written in the Ruby language. Its architecture is built around a client-server model.

In this lab we are using the Metasploitable 2 VM. Just remember your IPs will be different than the ones we are using.

HttpUsername and HttpPassword: These are the credentials used for HTTP authentication.

RHOSTS: Remote Hosts specifies the IP address or addresses of the target system(s) you are trying to exploit.

RPORT: Remote Port specifies which port on the target system to attack.

TARGETURI: This is the directory path on the target system the exploit will target.

LHOST: Local Host is the IP address of your machine which will receive connection from the exploited target.

LPORT: Local Port is the port on your machine that will listen for incoming connections from the target.

Starting the Console

You can start Metasploit in Kali in two different ways:
- Go to Applications -> 08 Exploitation Tools -> metasploit framework and click on it.
- Alternatively, open a terminal and start it by running the command msfconsole.

Searching for Modules

1. search eternalblue to exploit a vulnerability in Microsoft's Server Message Block (SMB) Protocol.
2. search cve:2024 type:exploit platform:windows to locate Windows exploits related to CVEs reported in 2024
3. search type:post platform:windows rank:normal to see Windows post modules with a normal ranking.
4. search name:backdoor platform:windows rank:excellent to identify the top Windows backdoor modules.
5. search type:auxiliary name:scanner ftp to find scanner auxiliary modules with a keyword of ftp.
6. search tomcat manager upload to list all the modules with the keyword "tomcat manager upload."

Launching an Exploit

To run the exploit, you can type run. But if you want to channel your inner hacker, type exploit. You now have a *Meterpreter* shell for the target machine that allows you to download and upload files easily, run other modules, and perform tasks such as capturing screenshots, logging keystrokes, escalating privileges, gathering system information, and even moving laterally across a network to compromise additional systems.

Upload a File

- To upload a file from your machine to the target machine type help upload
- If you want to upload the popular Linux privilege escalation script LinPeas the command is: meterpreter > upload linpeas.sh /tmp