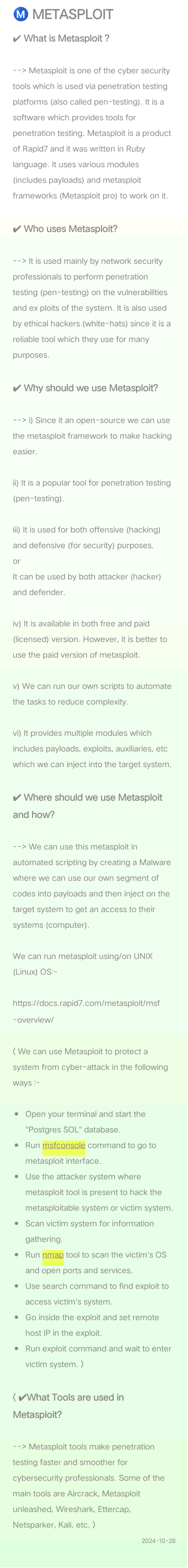

Ⓜ METASPLOIT

✔ What is Metasploit ?

--> Metasploit is one of the cyber security tools which is used via penetration testing platforms (also called pen-testing). It is a software which provides tools for penetration testing. Metasploit is a product of Rapid7 and it was written in Ruby language. It uses various modules (includes payloads) and metasploit frameworks (Metasploit pro) to work on it.

✔ Who uses Metasploit?

--> It is used mainly by network security professionals to perform penetration testing (pen-testing) on the vulnerabilities and ex ploits of the system. It is also used by ethical hackers (white-hats) since it is a reliable tool which they use for many purposes.

✔ Why should we use Metasploit?

--> i) Since it an open-source we can use the metasploit framework to make hacking easier.

ii) It is a popular tool for penetration testing (pen-testing).

iii) It is used for both offensive (hacking) and defensive (for security) purposes.
or
It can be used by both attacker (hacker) and defender.

iv) It is available in both free and paid (licensed) version. However, it is better to use the paid version of metasploit.

v) We can run our own scripts to automate the tasks to reduce complexity.

vi) It provides multiple modules which includes payloads, exploits, auxiliaries, etc which we can inject into the target system.

✔ Where should we use Metasploit and how?

--> We can use this metasploit in automated scripting by creating a Malware where we can use our own segment of codes into payloads and then inject on the target system to get an access to their systems (computer).

We can run metasploit using/on UNIX (Linux) OS:-

https://docs.rapid7.com/metasploit/msf-overview/

⟨ We can use Metasploit to protect a system from cyber-attack in the following ways :-

- Open your terminal and start the "Postgres SOL" database.
- Run msfconsole command to go to metasploit interface.
- Use the attacker system where metasploit tool is present to hack the metasploitable system or victim system.
- Scan victim system for information gathering.
- Run nmap tool to scan the victim's OS and open ports and services.
- Use search command to find exploit to access victim's system.
- Go inside the exploit and set remote host IP in the exploit.
- Run exploit command and wait to enter victim system. ⟩

⟨ ✔What Tools are used in Metasploit?

--> Metasploit tools make penetration testing faster and smoother for cybersecurity professionals. Some of the main tools are Aircrack, Metasploit unleashed, Wireshark, Ettercap, Netsparker, Kali, etc. ⟩

2024-10-28