CYART

inquiry@cyart.io

www.cyart.io

AUGUST 14, 2025

RED TEAMING TASK 01

Kshitij Patil

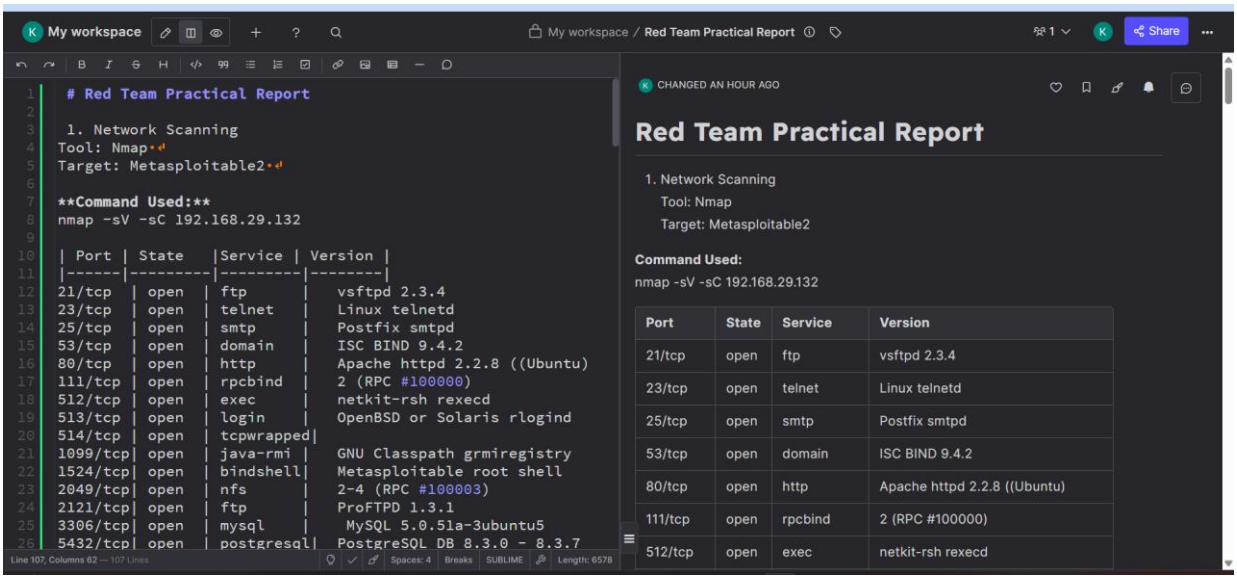
3. Red Team Operations and Documentation

Activities:

- **Tools:** HackMD, Draw.io, Trello
- **Tasks:** Document attack techniques, create flowcharts, and build checklists.

Enhanced Tasks:

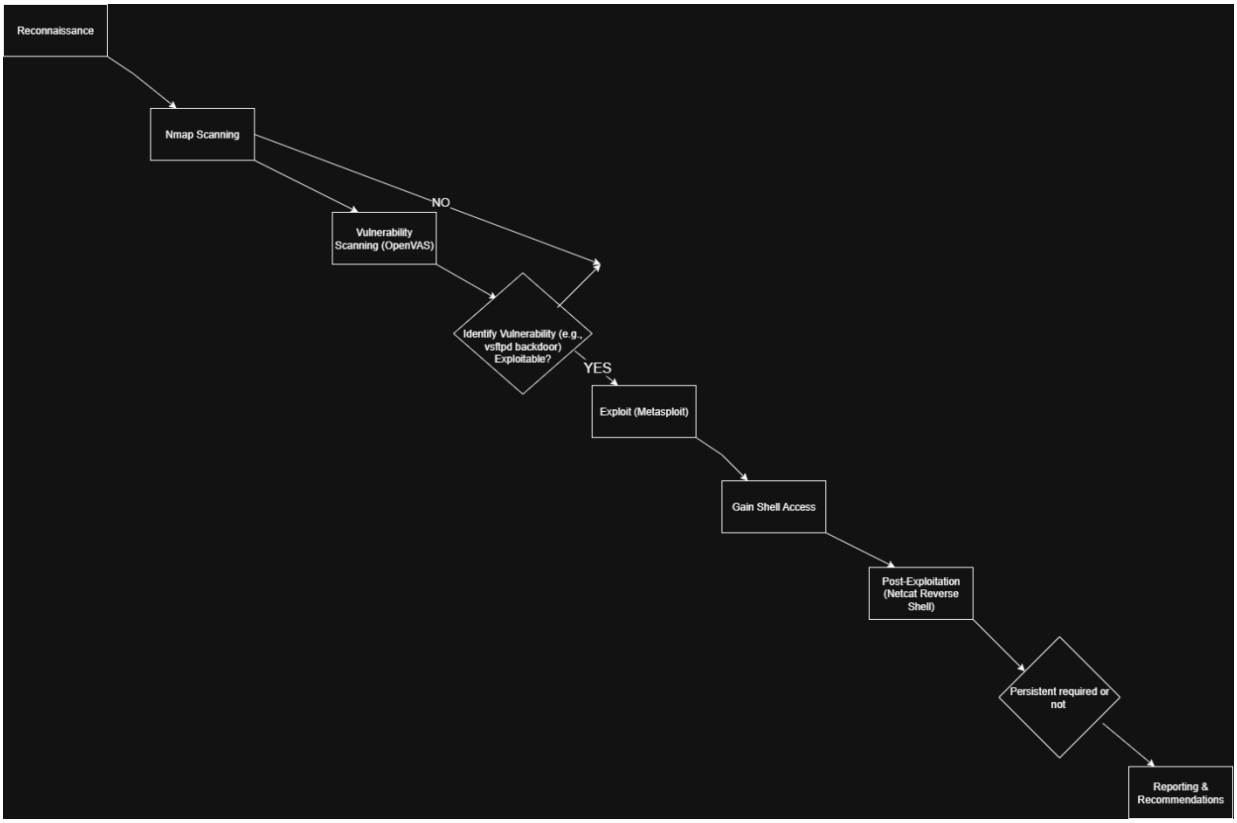
- **Technique Summary:** Document a Metasploit exploit in HackMD, using 5 Red Team terms (e.g., payload, exploit, persistence).



HackMd URL

https://hackmd.io/@h5LGbDMtRDyCXoYI2Du0iQ/ryMWka8txg

- **Attack Flowchart:** Use Draw.io to diagram an attack path (e.g., Recon → Exploit → Post-Exploitation).



Miscellaneous Tasks:

- **MITRE ATT&CK Mapping:** Map a Metasploit exploit to a MITRE ATT&CK technique (e.g., T1059 - Command and Scripting Interpreter). Summarize in 50 words.

In Metasploit, an attacker might use an exploit like exploit/windows/smb/ms17_010_eternalblue which, upon successful exploitation, could lead to the execution of a payload like windows/meterpreter/reverse_tcp. This payload, once executed, establishes a reverse shell on the victim's machine, allowing the attacker to execute arbitrary commands.
This post-exploitation activity of executing commands using the established shell directly relates to the MITRE ATT&CK Technique T1059: Command and Scripting Interpreter. This technique details how adversaries can leverage system's built-in command-line interpreters (like cmd.exe or PowerShell on Windows) or scripting environments to execute malicious code and interact with compromised systems.