



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](https://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).

The screenshot shows a workspace titled "My workspace" with a file named "Red Team Practical Report". The code editor on the left displays the following content:

```
1 # Red Team Practical Report
2
3 1. Network Scanning
4 Tool: Nmap
5 Target: Metasploitable2
6
7 **Command Used:**
8 nmap -sV -sC 192.168.29.132
9
10 | Port | State | Service | Version |
11 |-----|-----|-----|-----|
12 21/tcp | open | ftp | vsftpd 2.3.4
13 23/tcp | open | telnet | Linux telnetd
14 25/tcp | open | smtp | Postfix smtpd
15 53/tcp | open | domain | ISC BIND 9.4.2
16 80/tcp | open | http | Apache httpd 2.2.8 ((Ubuntu)
17 111/tcp | open | rpcbind | 2 (RPC #100000)
18 512/tcp | open | exec | netkit-rsh rexecd
19 513/tcp | open | login | OpenBSD or Solaris rlogind
20 514/tcp | open | tcpwrapped
21 1099/tcp | open | java-rmi | GNU Classpath grmiregistry
22 1524/tcp | open | bindshell | Metasploitable root shell
23 2049/tcp | open | nfs | 2-4 (RPC #100003)
24 2121/tcp | open | ftp | ProFTPD 1.3.1
25 3306/tcp | open | mysql | MySQL 5.0.51a-3ubuntu5
26 5432/tcp | open | postgresql | PostgreSQL DB 8.3.0 - 8.3.7
```

The preview view on the right shows the rendered report:

Red Team Practical Report

1. Network Scanning

Tool: Nmap

Target: Metasploitable2

Command Used:

```
nmap -sV -sC 192.168.29.132
```

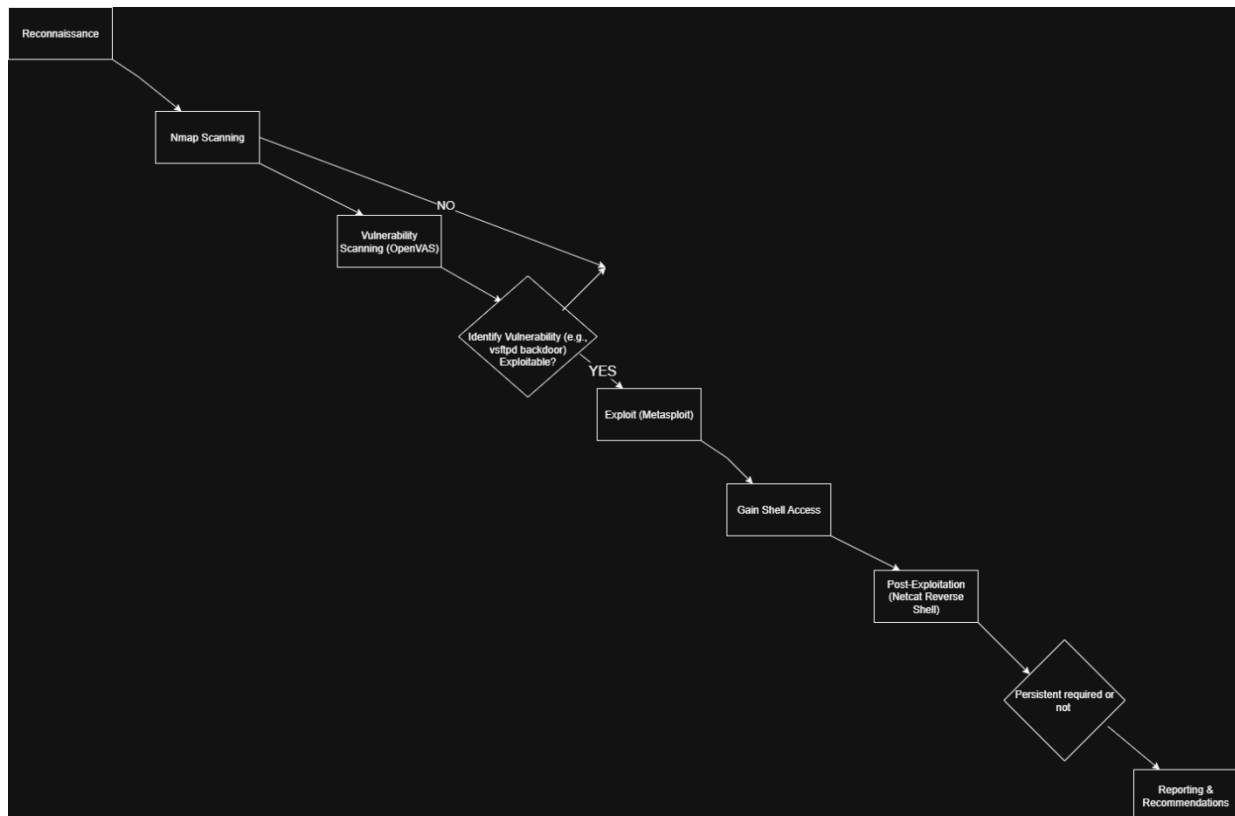
Port	State	Service	Version
21/tcp	open	ftp	vsftpd 2.3.4
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu)
111/tcp	open	rpcbind	2 (RPC #100000)
512/tcp	open	exec	netkit-rsh rexecd

HackMd URL

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



- **Attack Flowchart:** Use [Draw.io](https://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.