Bushra Akter

Class:12

192.168.68.86

Penetration test → find vulnerability

- VA (Vulnerability assessment)
- PT (Penetration Test)

Gaining Access

- Password Attacks → sniffing, Trojan,key logger, spyware
- Password Creaking → brute force,dictionary attack

Vulnerability Exploitation

- Identify the vulnerability
- Determine the risk associated with the vulnerability
- Determine the capability of the vulnerability
- Exploit development(Adv. Level) / Exploit Modification(Mid level)/Exploit selection
- Payload selection
- Gain the access

Exploit → snack, Payload→ poison

There are two types of shell:

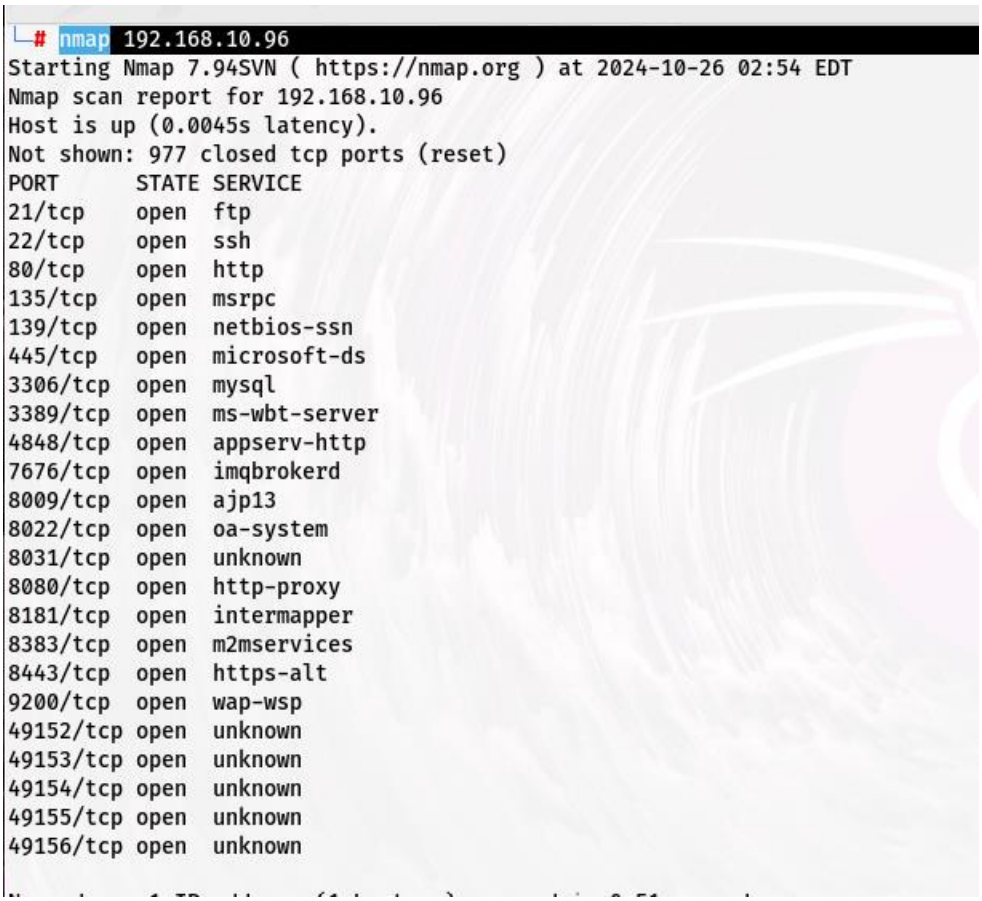
- Bind shell → attacker to target
- Reverse Shell → target to attacker

Exdploitation Freamework

- msfconsole
- Auxiliary
- Exploits
- Payload
- Post

- Encoder
- Nops
- Evasion

nmap 192.168.10.96



```
└─# nmap 192.168.10.96
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 02:54 EDT
Nmap scan report for 192.168.10.96
Host is up (0.0045s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
```

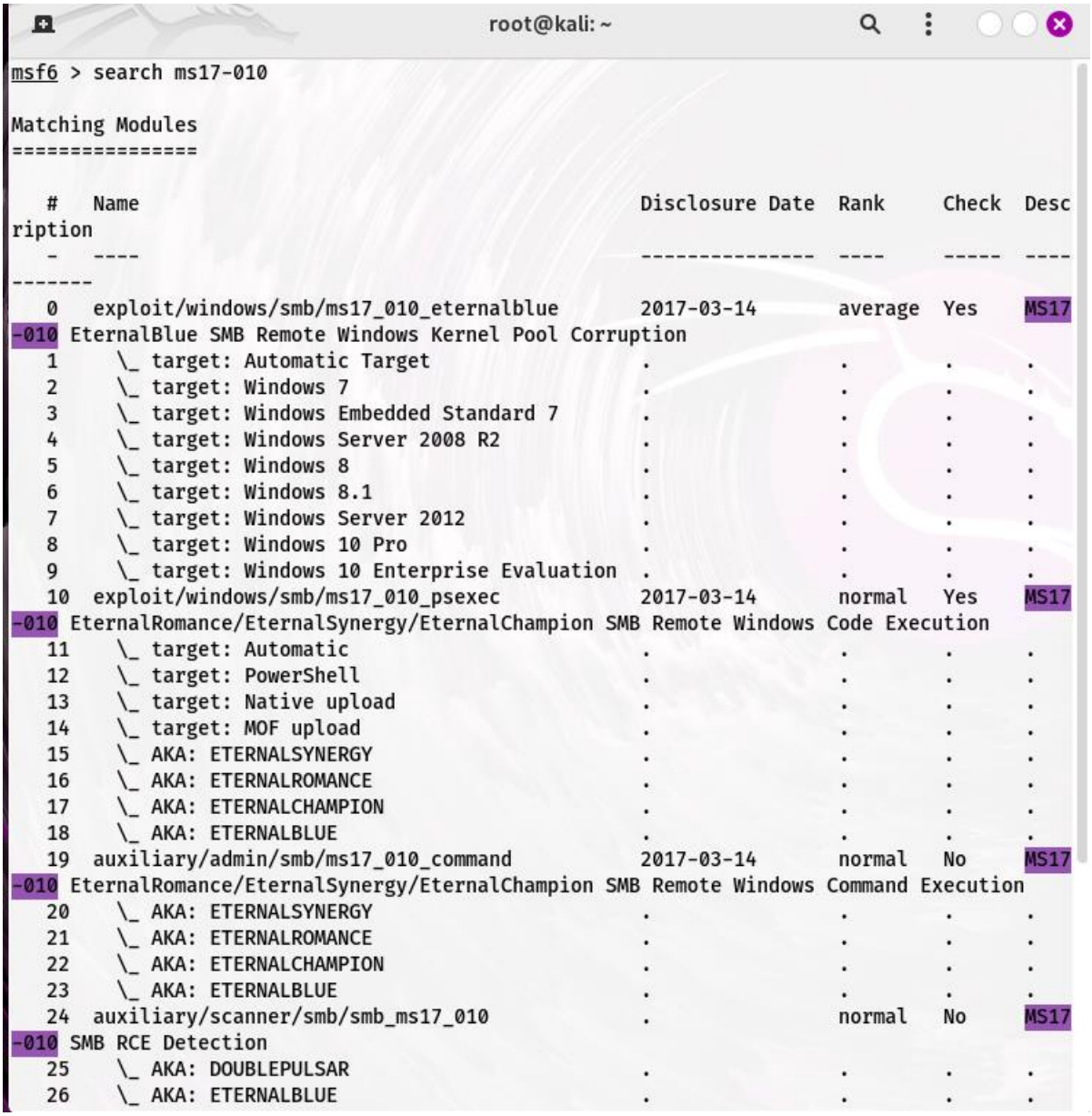
─# locate .nse (.nse mean nmap script)

nmap -p 445 --scripts=smb-vuln-* 192.168.10.96

msfconsole

msf6 >help

msf6 > search ms17-010


root@kali: ~
msf6 > search ms17-010
Matching Modules
Name Disclosure Date Rank Check Description
- ---- --- --- --- ---
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 _ target: Automatic Target . . . .
2 _ target: Windows 7 . . . .
3 _ target: Windows Embedded Standard 7 . . . .
4 _ target: Windows Server 2008 R2 . . . .
5 _ target: Windows 8 . . . .
6 _ target: Windows 8.1 . . . .
7 _ target: Windows Server 2012 . . . .
8 _ target: Windows 10 Pro . . . .
9 _ target: Windows 10 Enterprise Evaluation . . . .
10 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 _ target: Automatic . . . .
12 _ target: PowerShell . . . .
13 _ target: Native upload . . . .
14 _ target: MOF upload . . . .
15 _ AKA: ETERNALSYNERGY . . . .
16 _ AKA: ETERNALROMANCE . . . .
17 _ AKA: ETERNALCHAMPION . . . .
18 _ AKA: ETERNALBLUE . . . .
19 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 _ AKA: ETERNALSYNERGY . . . .
21 _ AKA: ETERNALROMANCE . . . .
22 _ AKA: ETERNALCHAMPION . . . .
23 _ AKA: ETERNALBLUE . . . .
24 auxiliary/scanner/smb/smb_ms17_010 . normal No MS17-010 SMB RCE Detection
25 _ AKA: DOUBLEPULSAR . . . .
26 _ AKA: ETERNALBLUE . . . .