# Red Team: Summary of Operations

## Table of Contents

- Exposed Services

- Critical Vulnerabilities

- Exploitation

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

**Screenshot**

* Scanning network range
* Nmap -sP 192.168.1.1-255

Graphical user interface, text

Description automatically generated

**Screen shot**

* NMAP service Version Scan
* nmap -sV 192.168.1.110

Text

Description automatically generated

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

- Target 1

- HTTP

- SSH

- Samba

The following vulnerabilities were identified on each target:

- Target 1

- User Michael when scanning word press had a very weak password

- MYSQL credentials left unsecured in WP-Config file

- Unsalted hashes left in the database

- python command with sudo permissions to spawn a root shell

**Screenshot**

**Wp-config.php**Text

Description automatically generated

**Screenshot Logging in as Michael**

Text

Description automatically generated

**Screenshot of cracking the hashes in John the Ripper**

**Text

Description automatically generated**

**Screenshot getting user’s hash**

Graphical user interface, text

Description automatically generated with medium confidence

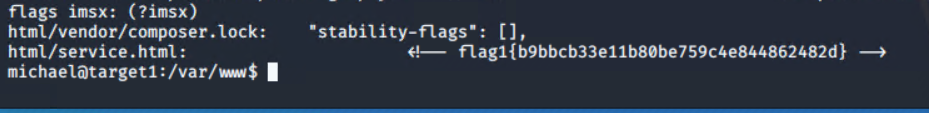
**Screenshot running sudo python command**

Text

Description automatically generated

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

- Target 1



- `flag1.txt`:

- \*\*Exploit Used\*\*

-: Identify the exploit used\_

- After obtaining credentials from Michael’s weak password and successfully logging in via ssh. I was able to browse the system files and changed directory to /var/www where I was able to run a grep command to find flag 1 in HTML file

-: Include the command run\_

- grep -RE flag html 

- `flag2.txt`:

Text

Description automatically generated

- \*\*Exploit Used\*\*

-: Identify the exploit used

- After finding flag 1 I noticed flag2.txt located in the “www” directory. So, I just had to back up a couple of directories and “Cat” out the file to display the results of flag2.

-: Include the command run

- cat /var/www/flag2.txt

- `flag3.txt`:

- \*\*Exploit Used\*\*

-: Identify the exploit used\_

- After logging into MYSQL with the credentials I found via the wp-config.php file I Went to wp\_posts and ran a command that did a select everything from wp\_posts and found the flag on the last line.

-: Include the command run\_

- select \* from wp\_posts

A picture containing text

Description automatically generated

Screenshot

* Bottom of wp-config.php file

Text

Description automatically generated

`flag4.txt`:

- \*\*Exploit Used\*\*

-: Identify the exploit used

- Ran sudo -l on user Steven found out that he could use sudo with python

-: Include the command run\_

- sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’

Text

Description automatically generated