# Red Team: Summary of Operations

## Table of Contents

- Exposed Services

- Critical Vulnerabilities

- Exploitation

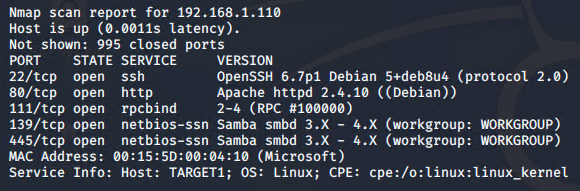
### Exposed Services

\_TODO: Fill out the information below.\_

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

$ nmap -sV 192.168.1.1-255





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

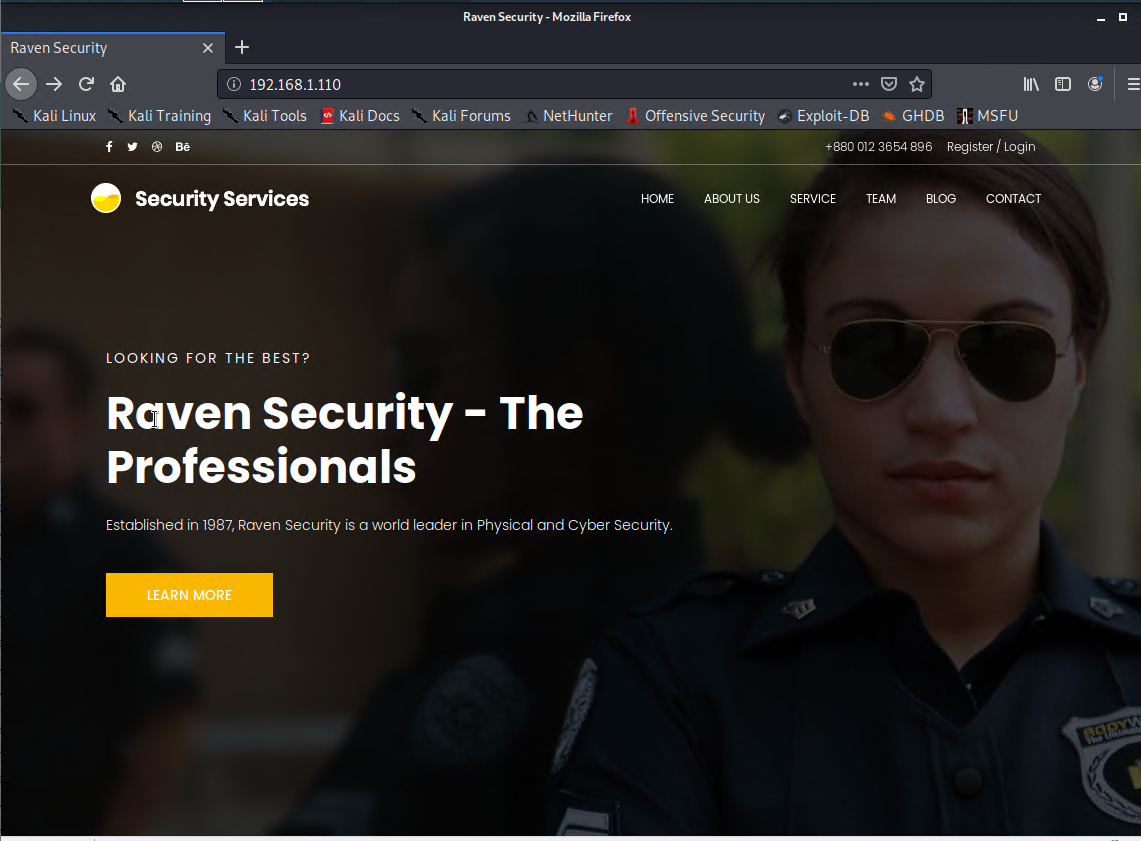
* Target 1 (192.168.1.110)
  + Service: SSH
    - Port: 22/TCP
    - Version: OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
    - CVE-2016-1908
    - Severity: High
    - Open to brute force login with weak credentials
  + Service: HTTP
    - Port: 80/tcp
    - Version: Apache httpd 2.4.10 ((Debian))
    - Open to script injection
  + Service: rpcbind
    - Port:111/tcp
    - Version: 2-4 (RPC #100000)
    - Open to malicious file uploads
  + Service: netbios-ssn
    - Port: 139/tcp
    - Version: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
    - Vulnerable to a reverse shell
  + Service: netbios-ssn
    - Port: 445/tcp
    - Version: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
    - Vulnerable to a reverse shell

Simplified usernames, weak passwords, root accessibility.

\_TODO: Fill out the list below. Include severity, and CVE numbers, if possible.\_

The following vulnerabilities were identified on each target:

- Target 1



- List of

- Critical

- Vulnerabilities

\_TODO: Include vulnerability scan results to prove the identified vulnerabilities.\_

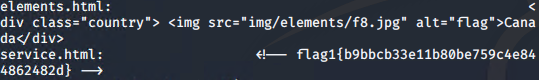
### Exploitation

\_TODO: Fill out the details below. Include screenshots where possible.\_

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

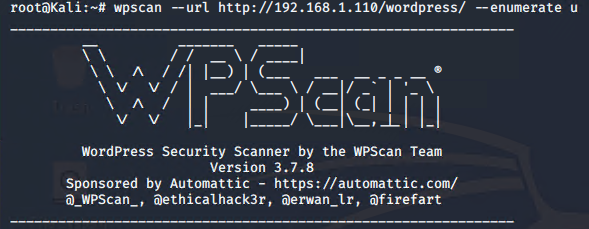
- Target 1

- `flag1.txt`:{b9bbcb33e11b80be759c4e844862482d}

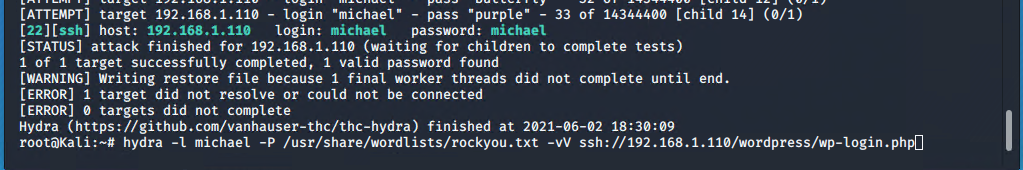


- \*\*Exploit Used\*\*

- \_TODO: Identify the exploit used\_

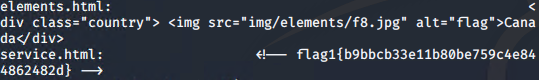






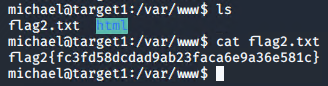
michael:michael





- \_TODO: Include the command run\_

- `flag2.txt`: \_TODO: Insert `flag2.txt` hash value\_



- \*\*Exploit Used\*\*

- \_TODO: Identify the exploit used\_

- \_TODO: Include the command run\_

