# Red Team: Summary of Operations

## Table of Contents

- Exposed Services

- Critical Vulnerabilities

- Exploitation

### Exposed Services

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

**Name of VM: Target1**

**Operating System: Linux**

**Purpose: Defensive Blue Team**

**IP Address: 192.168.1.110**

**Name of VM: Target2**

**Operating System: Linux**

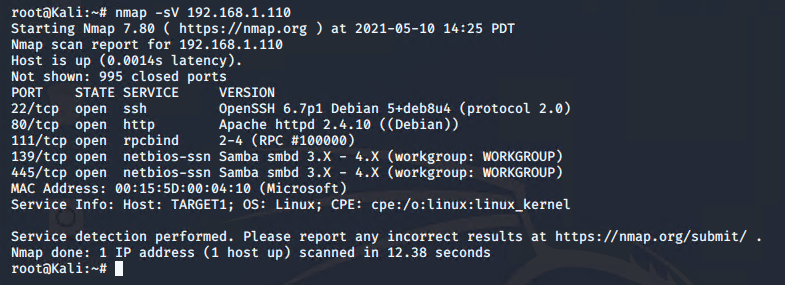
**Purpose: Offensive Red Team**

**IP Address: 192.168.1.115**

* Bash
* $ Command to Scan Target 1
* Nmap -sV 192.168.1.110/24

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

- Target 1



The following vulnerabilities were identified on each target:

- Target 1

- CVE-2017-15710 Apache https 2.4.10

- CVE[-2017-7494](https://www.cvedetails.com/cve/CVE-2017-7494/) Samba Netbios

- CVE-2021-28041 open SSH

### Exploitation

* Wpscan displays the brute force of users “michael and steven”

Text

Description automatically generated

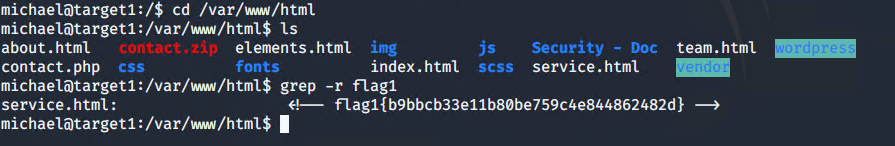
Text

Description automatically generated

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

- Target 1

- `flag1.txt`:



- `flag2.txt`: 