Offensive Analysis

# 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:

```bash

$ nmap -sV 192.168.1.110

(See screenshot of nmap scan)

```

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

- Target 1

- Port 22: ssh

- Port 80: http

- Port 111: rpcbind

- Port 139: netbios-ssn

- Port 445: netbios-ssn

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

The following vulnerabilities were identified on each target:

- Target 1

- CVE-2019-6579- Port 80: This Port being open would allow attackers to gain access to administrative privileges.

- CVE-2008-0852-Port 22: Denial of service attacks due to this port being open.

- CVE-2017-8779-Port 111: vulnerability allowing portmapper and metasploit module that can exploit it.

\_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`::$P$$8jRvZQ.VQcGZ1DeiKToCQd.cPw5XCe0

- ID Brute Force was used for this attack.

- Used WPscan

- Gained User Shell

- SSH Into Shell

-:/var/www$ grep -RE flag html

- `flag2.txt`::$P$8kJVD9jsxx/loJoqNsURgHiaB23j7W/

- Brute Force

- \_WPscan

- Gained User Shell

- SSH Into Shell

-:/var/www$ cat flag2.txt