**## 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 ... # TODO: nmap -sV -A 192.168.1.110

# TODO: Debian 5+deb8u4, port 22 open, http raven security on port 80, rcpbind port 111, Samba 3.X - 4.X, Samba 4.2.14-Debian port 445, Linux 3.2 - 4.9

$ nmap ... # TODO: nmap -sV -A 192.168.1.115

# TODO: Same as Target 1

```

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

- Target 1

- SSH Port 22

- Samba Share

- Target 2

- SSH Port 22

- Samba Share

**### Critical Vulnerabilities**

The following vulnerabilities were identified on each target:

- Target 1

- OpenSSH

- Weak Passwords

- Password hashes stored on weak MSQL database

**### Exploitation**

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

- Target 1

- `flag1.txt`: fc3fd58dcdad9ab23faca6e9a36e581c

- **\*\*Exploit Used\*\***

-SSH using Michael's credentials

-ssh micahel@192.168.1.110

- `flag2.txt`: fc3fd58dcdad9ab23faca6e9a36e581c

- **\*\*Exploit Used\*\***

- Root escallation

-sudo su

- Target 2

- `flag1.txt`: a2c1f66d2b8051bd3a5874b5b6e43e21

- **\*\*Exploit Used\*\***

- Laying around in the vendor directory

- /var/www/html/vendor

- `flag2.txt`: 6a8ed560ff0b5358ecf844108048eb337

- **\*\*Exploit Used\*\***

- netcat reverse shell

- nc -lvp 9001 (found in /var/www)