# 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:

* Nmap 192.168.1.0/24

IP Address 192.168.1.110 has the following ports open:

* 22 ssh
* 80 http
* 111 rpcbind
* 139 netbios-ssn
* 445 microsoft-ds

Nmap -sV 192.168.1.110

* Ssh version is 7.7p1 Debian 5+deb84u (protocol 2.0)
* Apache httpd 2.4.10 (Debian)
* Netbios Samba smbd 2.x-4.x (Ports 139 and 445)

Ip Address 192.168.1.115 has the following ports open:

* 22 ssh
* 80 http
* 111 rpcbind
* 139 netbios-ssn
* 445 microsoft-ds

For this project, the machine on 192.168.1.115 will not be attacked.

**Target Machine**

1. ssh
2. http
3. Netbios-ssn
4. Rpcbind (DoS attack)

### **Critical Vulnerabilities**

The following vulnerabilities were identified on each target:

**Target Machine**

1. Old Wordpress Blog Version (Medium Severity)
2. Weak Passwords/No password policies (Critical Severity)
3. Unencrypted Passwords on target machine (Critical Severity)
4. Apache Vulnerabilities
   1. [CVE-2017-7679](https://www.cvedetails.com/cve/CVE-2017-7679/)
   2. [CVE-2013-2249](https://www.cvedetails.com/cve/CVE-2013-2249/)
5. WordPress Version 4.8.14
   1. [CVE-2018-20148](https://www.cvedetails.com/cve/CVE-2018-20148/)
   2. [CVE-2019-8942](https://www.cvedetails.com/cve/CVE-2019-8942/)
   3. [CVE-2019-9787](https://www.cvedetails.com/cve/CVE-2019-9787/)

A wordpress scan was used after discovering that the HTTP server had a wordpress blog published on it.

**Wpscan --url** [**http://192.168.1.110/wordpress/**](http://192.168.1.110/wordpress/) **--enumerate u**

WordPress version 4.8.14

Two users found: Michael and Steven (michael, steven)

**Exploitation**

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

After exploiting the ssh port on the target machine using michael’s username and easily guessable password:

**Target Machine**

* Flag1 found inside of service.html file in /var/www/html directory
  + Grep “\*flag\*” /var/www/html
    - flag1{b9bbcb33e11b80be759c4e844862482d}
* Flag2.txt found in /var/www directory
* Exploit Used
  + Inside of /var
    - Find -iname “\*flag\*”
    - Cat /var/www/flag2.txt
    - Flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

The next few pages show the screenshots captured for documentation purposes.







