# **Red Team: Summary of Operations**

## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

nmap 192.168.0.90/24

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

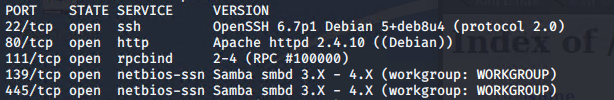
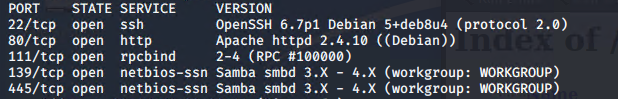
$ nmap -sV 192.168.1.110

# TODO: Insert scan output

$ nmap -sV 192.168.1.115

# TODO: Insert scan output

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

* Target 1
  + 
* Target 2
  + 

### **Critical Vulnerabilities**

*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
* Target 2
  + 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 both Target 1 and Target 2, and retrieve the following confidential data:

* Target 1
  + flag1.txt: *flag1[b9bbcb33e11b80be759c4e844862482d}*
    - **Exploit Used**
      * *Word Press was used to exploit*
      * *Wpscan --url* [*http://192.168.1.110/wordpress/*](http://192.168.1.110/wordpress/) *-enumerate u*

1. *Was able to find users Steven and Michael*

Used ssh to get into michael’s account

1. Ssh michael@192.168.1.110

Password: michael

1. Used grep -RE ‘flag1’ to find flag1 in /var/www/html/service.html

* + flag2.txt: *TODO: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}*
    - **Exploit Used**
      * *Ssh into michael’s account*
      * *Due to the clue I knew to look into /var/www for flag 2*
  + Flag3.txt: flag3{afc01ab56b50591e7dccf93122770cd2}
    - **Exploit Used**
      * *Used the information from the wp-config.php file inorder to gain access to mysql*
        + *Mysql -u root -p (password is R@v3nSecurity)*
      * *I used the Database wordpress using: show databases; > use wordpress;*
        + *Used “show table;” to see whats in the tables.*
      * *Was able to find flag3 in the table wp\_posts*
  + Flag4.txt: flag4{715dea6c055b9fe3337544932f2941ce}
    - **Exploit Used**
      * While in the same table as the last flag I was able to find the 4th flag in the same place