**Red Team: Summary of Operations – TARGET1**

**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploition

**Exposed Services**

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

$ nmap -sV 192.168.1.110

Text

Description automatically generated

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

* Target 1
  + Port 22 SSH
  + Port 80 HTTP

The following vulnerabilities were identified on each target:

* Weak passwords
* User enumeration
* Unsalted hashed passwords
* Sql database password in plain text
* Privilege escalation via python script

**Exploitation**

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

**User Enumeration**

wpscan –url http://192.168.1.110/wordpress --enumerate u. Users Michael and Steven were discovered.

Text

Description automatically generated

**Weak Passwords**

Michael’s password was guessed and was able to gain access via ssh.

Text

Description automatically generated

Once logged in as Michael, we navigated to /var/www/html and were able to find flag1

Flag 1

Text

Description automatically generated

Flag 2 was located one directory above flag 1

Text

Description automatically generated

**SQL Database Password in plain text**

The password for the database was found in plain text within the wp-config.php file.

**Text

Description automatically generated**

Using the following commands was able to access the database

-Mysql -u root -p’R@v3nSecurity’

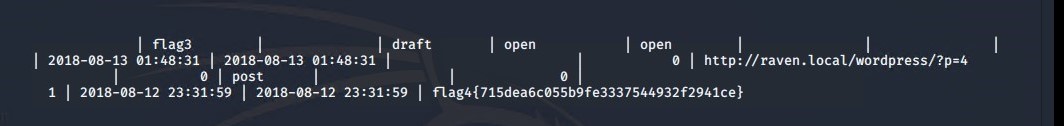
-show databases;

-use wordpress;

-show tables

-show wp-users

Flag 3



**Unsalted Hashed Passwords**

Using the following commands was able to access the database

-Mysql -u root -p’R@v3nSecurity’

-show databases;

-use wordpress;

-show tables

-select wp-users

Graphical user interface

Description automatically generated

Flag 4

-created a new file called hashes.txt and added the hashed passwords for both Michael and steven. Then ran the file through “john”

Discovered Stevens password was “Pink84”

SSH as stevenText

Description automatically generated

**Privilege Escalation via Python Script**

In order to escalate to root, used a python script to gain root access.

Text

Description automatically generated