**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 192.168.1.110

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

* Target 1
  + Port 22 - Open ssh
  + Port 80 - Open http
  + Port 111 - Open rpcbind
  + Port 139 - Open netbios-ssn Samba
  + Port 445 - Open netbios-ssn Samba

The following vulnerabilities were identified on each target:

* Target 1
  + Open ssh allowing remote access for users.
  + rpcbind 2.4 does not consider the maximum RPC data size, which allows remote attackers to effectively Dos your network. CVE-2017-8779
  + Samba is vulnerable to remote code execution vulnerability, allowing a user to upload a script for the server to execute. CVE-2017-7494

A screenshot of a computer

Description automatically generated with medium confidence

**Exploitation**

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

* Target 1
  + Flag1
    - **Exploit Used**
      * To find this flag I just navigated around the Security Services home page and inspected their source code for their page and found flag1 within the html code.

Graphical user interface, text

Description automatically generated

* + Flag2
    - **Exploit Used**
      * ssh with weak passwords.
      * ssh michael@192.168.1.110(guess the password is michael)
      * Text

        Description automatically generatedcat /var/www/flag2.txt
  + Flag3 and Flag4
    - **Exploit Used**
      * Text

        Description automatically generatedTo find these flags we would need to find another users credentials. I found in the word press config file another user and their password. nano /var/www/html/wordpress/wp-config.php

From here we logged into their word press database

mysql -u root -p

show databases;

use wordpress;

show tables;

A screenshot of a computer

Description automatically generated with low confidenceselect \* from wp\_posts;

I can see from here that the flags have been posted by one of their users. I need to gain access to another user to look further.

Text

Description automatically generatedselect \* from wp\_users;

Now I have the hashes, I copy them into a file and run it through John the ripper to get their password

Text

Description automatically generatedjohn --wordlist=/usr/share/wordlists/rockyou.txt /root/Desktop/Hashes.txt

Text

Description automatically generatedUse our new credentials and ssh into their network with steven and check for privileges. Noticed we have sudo privileges for python

As we have sudo privileges for python we can exploit this sudo python privilege to escalate our privileges to root to look for the final flag.

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

Text

Description automatically generatedFrom here we can navigate around to find the flag. Flag 4 was found ‘/root/flag4.txt’