

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.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-09 17:41 PST
Nmap scan report for 192.168.1.110
Host is up (0.0016s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.17 seconds
```

The following vulnerabilities were identified on each target:

- Target 1
 - User Enumeration (wordpress)
 - Simple/weak user password
 - Unsalted password hash from wordpress database
 - Misconfiguration of user privileges/escalation

Exploitation

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

- Target 1
 - flag1.txt: **flag1{b9bbcb33e11b80be759c4e844862482d}**
 - Exploit Used
 - WPScan to enumerate users from the Target 1 WordPress site
 - \$ wpscan -url <http://192.168.1.110/wordpress> -enumerate u
 - This gave us the username michael and just by guessing we were able to find out the password for this user which was the same as the username, michael. After connecting to the target machine via SSH we were able to find the first flag in service.html file in the /var/www/html/ directory.
 - flag2.txt: **flag2{fc3fd58dcdad9ab23faca6e9a36e581c}**
 - Exploit Used
 - After connecting to the victim machine via SSH, we were able to search the system for the second flag. It was located in the var/www directory.
 - Commands: cd /var/www; ls -al, cat flag2.txt
 - flag 3 and flag 4: **flag3{afc01ab56b50591e7dccf93122770cd2}**
flag4{715dea6c055b9fe3337544932f2941ce}

- Exploit Used

- Accessing MySQL database. After we find wp-config.php we will find gaining database credentials for Michael. Flags 3 and 4 were found in wp_posts table in the wordpress database.
- Commands: `mysql -u root -p'R@v3nSecurity' | show databases | use wordpress; | show tables; | select * from wp_posts;`