eJPT Black Box Pentesting Lab

Enumeration

PORTSCAN

Using ipsweep to find all alive hosts, for some reason nmap -sn didn't work

```
┌──(kali㉿kali)-[~/ine]
└─$ ./ipsweep.sh 172.16.64
This tool allows users to scan IP Addresses in their network
172.16.64.11

Complete - the list can also be found in file iplist.txt

┌──(kali㉿kali)-[~/ine]
└─$ 172.16.64.101
172.16.64.140
172.16.64.182
172.16.64.199
```

Hosts alive:
172.16.64.11
172.16.64.101
172.16.64.140
172.16.64.182
172.16.64.199

172.16.64.11

Portscan

- Got some weird open ports

```
[+] 172.16.64.11:       - 172.16.64.11:35135 - TCP OPEN
[+] 172.16.64.11:       - 172.16.64.11:41757 - TCP OPEN
[+] 172.16.64.11:       - 172.16.64.11:43031 - TCP OPEN
[+] 172.16.64.11:       - 172.16.64.11:43603 - TCP OPEN
[+] 172.16.64.11:       - 172.16.64.11:44657 - TCP OPEN
[+] 172.16.64.11:       - 172.16.64.11:46501 - TCP OPEN
[*] 172.16.64.11:       - Scanned 1 of 1 hosts (100% complete)
```

172.16.64.101

Portscan

- one ssh port and a webserver on 8080 is open, the other port 9080 looks mysterious

```
[+] 172.16.64.101:      - 172.16.64.101:22 - TCP OPEN
[+] 172.16.64.101:      - 172.16.64.101:8080 - TCP OPEN
[+] 172.16.64.101:      - 172.16.64.101:9080 - TCP OPEN
[+] 172.16.64.101:      - 172.16.64.101:59919 - TCP OPEN
```

Detailed portscan

```
PORT    STATE SERVICE VERSION
22/tcp   open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)
|   256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)
|_  256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
9080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
59919/tcp open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: 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 25.29 seconds
```

DIRSCAN for both 8080 and 9080

```
/index.html         (Status: 200) [Size: 11321]
/manager            (Status: 302) [Size: 0] [--> /manager/]
```

172.16.64.140

Portscan

- Found a web server on port 80

```
[+] 172.16.64.140:      - 172.16.64.140:80 - TCP OPEN
```

- the /project endpoint is protected by a simple alert-popup type login, with credentials “**admin:admin**”
Finding directories using dirb with admin:admin creds

```
dirb http://172.16.64.140 -u admin:admin
```

- Found something in **/project/backup/test**

sdadas.txt
Driver={SQL Server};Server=foosql.foo.com;Database=;**Uid=fooadmin;Pwd=fooadmin;**
/var/www/html/project/354253425234234/flag.txt

test1.txt
https://stackoverflow.com/questions/1134319/difference-between-a-user-and-a-login-in-sql-server

- website uses “**colorlib**”
- https://www.cvedetails.com/cve/CVE-2015-1494/ - possible XSS exploit

172.16.64.182

Portscan

- Only one ssh port is open

```
[+] 172.16.64.182:      - 172.16.64.182:22 - TCP OPEN
```

172.16.64.199

Portscan

- A lot of ports are open here

```
[+] 172.16.64.199:      - 172.16.64.199:135 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:139 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:445 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:1433 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:49664 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:49668 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:49670 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:49666 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:49669 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:49667 - TCP OPEN
[+] 172.16.64.199:      - 172.16.64.199:49665 - TCP OPEN
[+] 172.16.64.199:     - 172.16.64.199:49943 - TCP OPEN
```

- I don't have access to the smb server

DETAILED PORTSCAN

```
PORT    STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1433/tcp open  ms-sql-s     Microsoft SQL Server 2014 12.00.2000.00; RTM
|_ssl-date: 2022-03-18T11:37:41+00:00; -11s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2022-03-18T07:12:36
|_Not valid after:  2052-03-18T07:12:36
| ms-sql-ntlm-info:
|   Target_Name: WIN10
|   NetBIOS_Domain_Name: WIN10
|   NetBIOS_Computer_Name: WIN10
|   DNS_Domain_Name: WIN10
|   DNS_Computer_Name: WIN10
|_  Product_Version: 10.0.10586
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -11s, deviation: 0s, median: -11s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WIN10, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:9f:0d (VMware)
| smb2-time:
|   date: 2022-03-18T11:37:35
|_  start_date: 2022-03-18T07:12:33
| ms-sql-info:
|   172.16.64.199:1433:
|     Version:
|       name: Microsoft SQL Server 2014 RTM
|       number: 12.00.2000.00
|       Product: Microsoft SQL Server 2014
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.21 seconds
```

used metasploit mssql_payload module to get a shell on the sql server as NT AUTHORITY\SYSTEM

Found the flag in C:\Users\AdminELS\Desktop\flag.txt
also found **id_rsa.pub** with creds to **developer** account in .182 machine

Exploitation

172.16.64.101:8080

- Used default credentials **tomcat:s3cret** to get into the /manager dashboard
- Uploaded a reverse shell payload and got a shell

netstat -ano

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 0.0.0.0:9080            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp6       0      0 127.0.0.1:8005          :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 :::59919                :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 :::8080                 :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 :::22                   :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 ::1:631                 :::*                    LISTEN      off (0.00/0/0)
tcp6       0    334 172.16.64.101:49226     172.16.64.10:4444       ESTABLISHED on (0.47/0/0)
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           off (0.00/0/0)
udp        0      0 0.0.0.0:44382           0.0.0.0:*                           off (0.00/0/0)
udp        0      0 0.0.0.0:631             0.0.0.0:*                           off (0.00/0/0)
udp6       0      0 :::5353                 :::*                                off (0.00/0/0)
udp6       0      0 :::56642                :::*                                off (0.00/0/0)
```

Files worth checking out

```
  Group tomcat8:
/etc/tomcat8/Catalina
/etc/tomcat8/Catalina/localhost
/var/lib/tomcat8/webapps

╔══════════╣ Modified interesting files in the last 5mins (limit 100)
/tmp/hsperfdata_tomcat8/1095
/var/log/auth.log
/var/log/syslog
/var/log/kern.log

╔══════════╣ Files inside /usr/share/tomcat8 (limit 20)
total 40
drwxr-xr-x   4 root root  4096 Mar 27  2020 .
drwxr-xr-x 254 root root 12288 Mar 27  2020 ..
drwxr-xr-x   2 root root  4096 Mar 27  2020 bin
-rw-r--r--   1 root root    39 Dec 12  2018 defaults.md5sum
-rw-r--r--   1 root root  1929 Dec 12  2018 defaults.template
drwxr-xr-x   2 root root  4096 Mar 27  2020 lib
-rw-r--r--   1 root root    53 Dec 12  2018 logrotate.md5sum
```

```
-rw-r--r--  1 root root  118 Dec 12  2018 logrotate.template
```

```
-rwsr-sr-x 1 root root 97K Jan 29  2019 /usr/lib/snapd/snap-confine  --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privile
ge_Escalation(CVE-2019-7304)
```

```
-rwsr-xr-x 1 root root 23K Jan 15  2019 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-2019-13272)/
rhel_6(CVE-2011-14
85)
```

The Pwnkit exploit worked - pkexec had SUID bit set
EZ Root

NOTE:
I couldn't login to this system using ssh or via id_rsa file, the hostname of this one is ‘xubuntu’
It's possible that this is a container or maybe this is a different system entirely