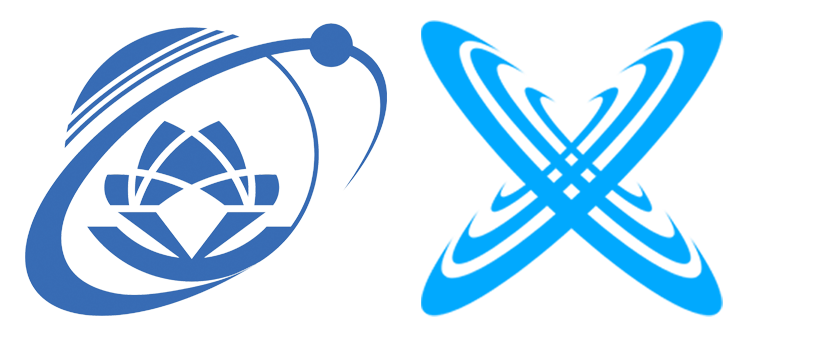
Báo cáo kết quả Thi giữa kỳ An toàn mạng

[NT140.O11.ANTN.1.7]



|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | Email | Đóng góp (%) |
| 1 | Phạm Ngọc Thơ | 21522641@gm.uit.edu.vn | 40% |
| 2 | Hà Thị Thu Hiền | 21522056@gm.uit.edu.vn | 60% |

-- Lưu hành nội bộ --

Mục lục

[1.0 Tổng quan 3](#_Toc57241311)

[1.1 Khuyến nghị bảo mật 3](#_Toc57241312)

[2.0 Phương pháp kiểm thử 3](#_Toc57241313)

[2.1 Thu thập thông tin 3](#_Toc57241314)

[2.2 Kiểm thử xâm nhập 4](#_Toc57241315)

[2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: X.X.X.X 4](#_Toc57241316)

[Thông tin dịch vụ 4](#_Toc57241317)

[Khởi tạo shell với quyền user thường 4](#_Toc57241318)

[Leo thang đặc quyền 5](#_Toc57241319)

[2.3 Duy trì quyền truy cập 5](#_Toc57241320)

[2.4 Xóa dấu vết 6](#_Toc57241321)

[3.0 Phụ lục 6](#_Toc57241322)

[3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt 6](#_Toc57241323)

# 1.0 Tổng quan

[NT140.O11.ANTN1.7] 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.ANTN1.7] 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.ANTN1.7] 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.ANTN1.7] có thể truy cập vào được liệt kê dưới đây

* Địa chỉ IP máy nạn nhân: 192.168.19.140

## 1.1 Khuyến nghị bảo mật

[NT140.O11.ANTN1.7] 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.ANTN1.7] 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.ANTN1.7] 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.ANTN1.7] được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

**Địa chỉ IP máy kẻ tấn công:**

* [Địa chỉ IP]

**Địa chỉ IP của máy nạn nhân:**

* 192.168.19.140

## 2.2 Kiểm thử xâm nhập

Giai đoạn kiểm thử xâm nhập tập trung vào việc chiếm quyền kiểm soát vào nhiều loại máy chủ. Trong đợt kiểm thử xâm nhập này, [NT140.O11.ANTN1.7] đã có thể truy cập thành công vào 1 trong số 1 máy chủ.

### 2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.140

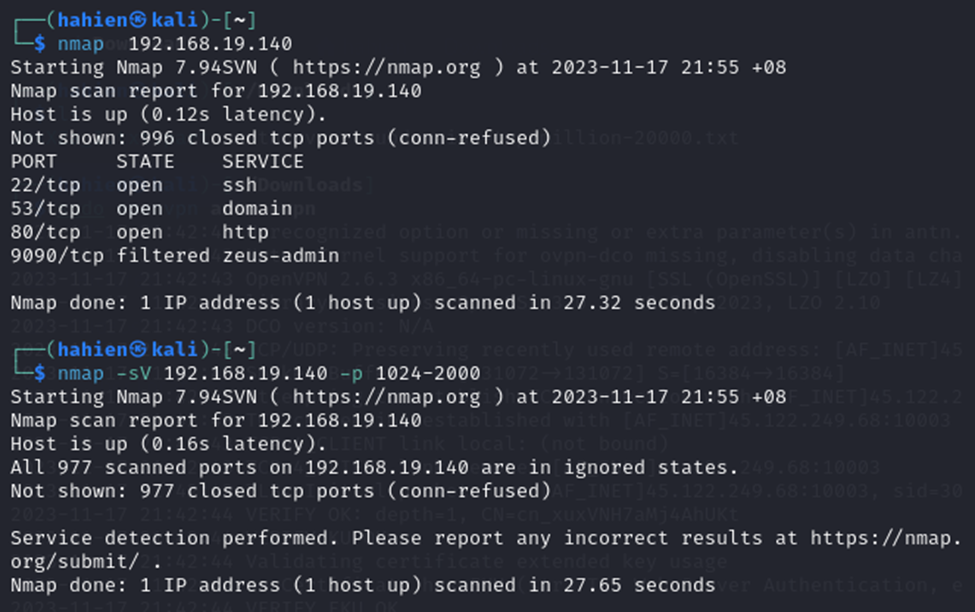
#### Thông tin dịch vụ

|  |  |
| --- | --- |
| **Địa chỉ IP** | **Các port đang mở** |
| X.X.X.X | **TCP:** [Liệt kê tất cả các port] |
| **UDP:** [Liệt kê tất cả các port] |

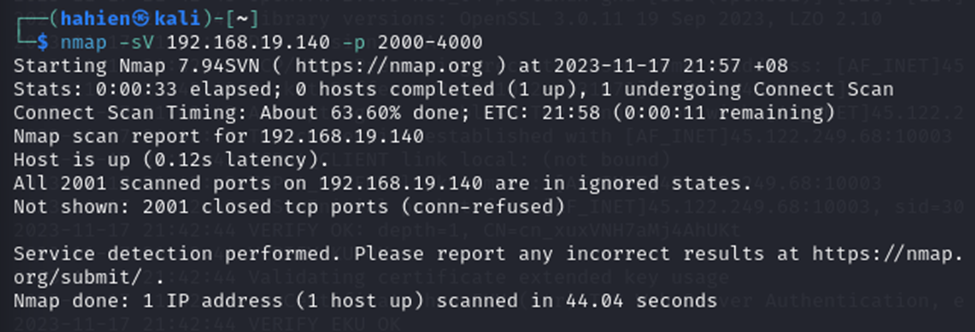
#### *\*Các Flag Bonus vui lòng trình bày tích hợp trong phần khởi tại shell với quyền user người dùng và leo thang đặc quyền.*

1. **Challenge 1:**

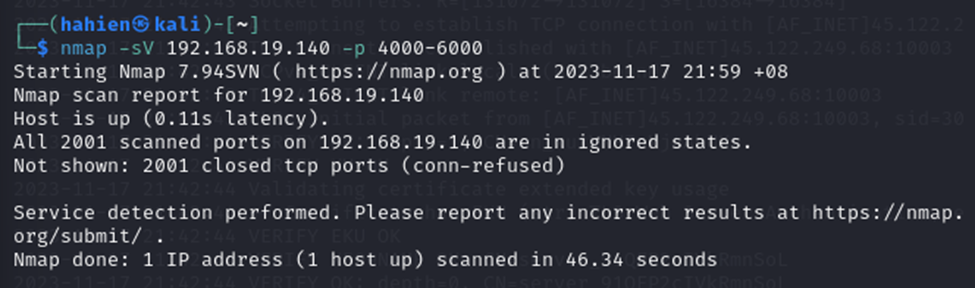
* Port scanning là phương pháp tìm các port đang mở trên máy chủ. Một port có thể được xem như một địa chỉ cho một dịch vụ cụ thể. Mọi máy tính đều có số port từ 0-65535. Một số dịch vụ có port mặc định như HTTP/80 hoặc SSH/22. Một port mở có nghĩa là máy chủ (host) cung cấp dịch vụ mạng trên port này.
* Nmap là một máy quét mạng (network scanner). Nó có thể thực hiển khám phá máy chủ (host discovery), version detection (service detection), và nhiều hơn thế nữa. Áp dụng kiến thức làm từ bandit17, option -p cho phép chọn port nào để quét và theo mặc định thì Nmap quét top 1000 ports (không phải là 1000 ports đầu tiên). Sử dụng -p- để quét tất cả 65535 ports, -sV quét phát hiện phiên bản/ dịch vụ (version detection/ service detection). Nmap có thể thực hiện tất cả các lần quét có thể bằng cờ -A nhưng sẽ mất thời gian. Quét toàn bộ: **nmap -p- -A <host>** (<host>: IP address/ name)
* Bây giờ, ta sẽ tiến hành xem tất cả các port trên địa chỉ IP 192.168.19.140 có dịch vụ nào đang mở khả nghi hay không. Để máy chạy nhanh hơn thì ta sẽ thực hiện dò một số lượng port nhất định kể từ port 1024.
* Đầu tiên, chúng ta cần tìm các cổng mở trong khoảng từ 1024 đến 2000 trên 192.168.19.140 và kiểm tra xem dịch vụ nào đang chạy trên chúng.



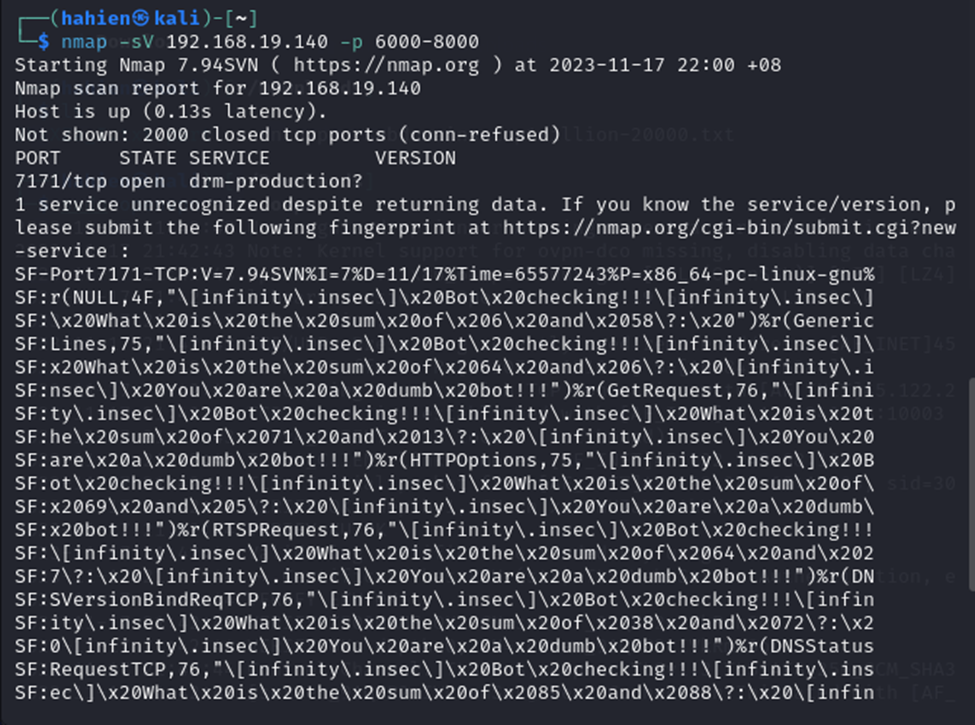
* Tiếp theo, chúng ta cần tìm các cổng mở trong khoảng từ 2000 đến 4000 trên 192.168.19.140 và kiểm tra xem dịch vụ nào đang chạy trên chúng.



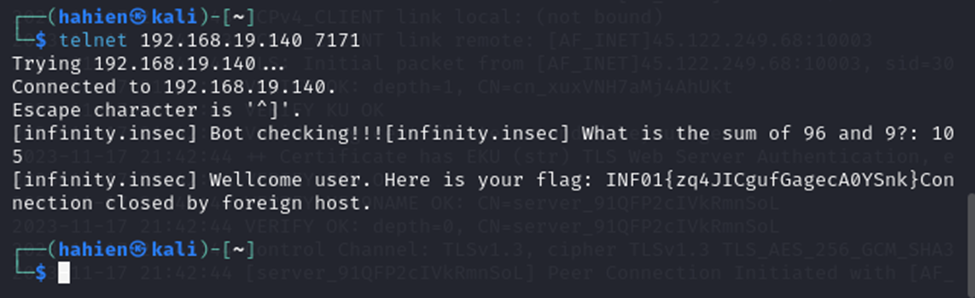
* Tiếp theo, chúng ta cần tìm các cổng mở trong khoảng từ 4000 đến 6000 trên 192.168.19.140 và kiểm tra xem dịch vụ nào đang chạy trên chúng.



* Tiếp theo, chúng ta cần tìm các cổng mở trong khoảng từ 6000 đến 8000 trên 192.168.19.140 và kiểm tra xem dịch vụ nào đang chạy trên chúng.



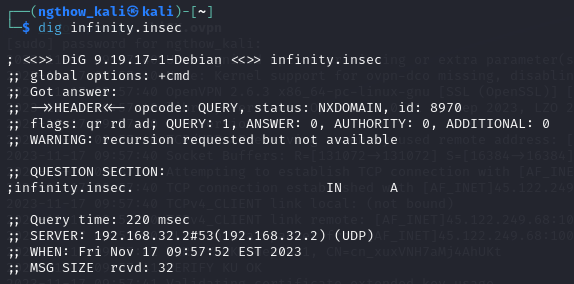
* Nmap cho chúng ta biết rằng có cổng 7171 đang mở và chạy dịch vụ **drm-production**? Đáng khả nghi. Nên ta sử dụng telnet truy cập đến địa chỉ IP 192.168.19.140 trên port 7171 để kiểm tra.



* Kết quả ta thu được FLAG: **NF01{zq4JICgufGagecA0YSnk}**

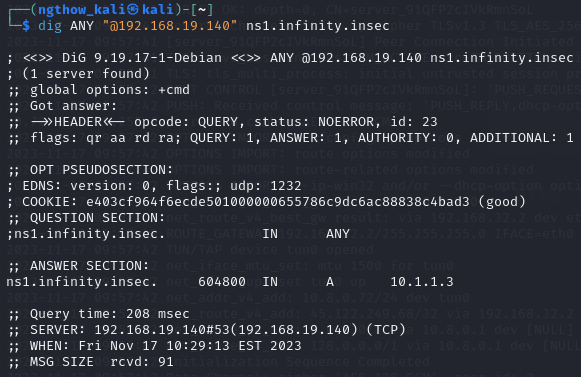
1. **Challenge 2:**

* Từ kết quả thu được ở challenge 1, ta đã thu được thêm một thông tin về tên miền của máy mục tiêu, đó là **infinity.insec**, em sẽ dựa vào thông tin này để khai thác lỗ hổng tiếp theo:
* Ở challenge này, em sẽ sử dụng **dig** - là một câu lệnh dùng để tra cứu thông tin DNS. Cú pháp cơ bản nhất là: **dig <domainnames>**



Sau khi thực thi câu lệnh, thông tin về DNS sẽ được trình bày dưới dạng các dòng thông tin để người dùng có thể truy vấn. Những thông tin đáng chú ý của kết quả là:

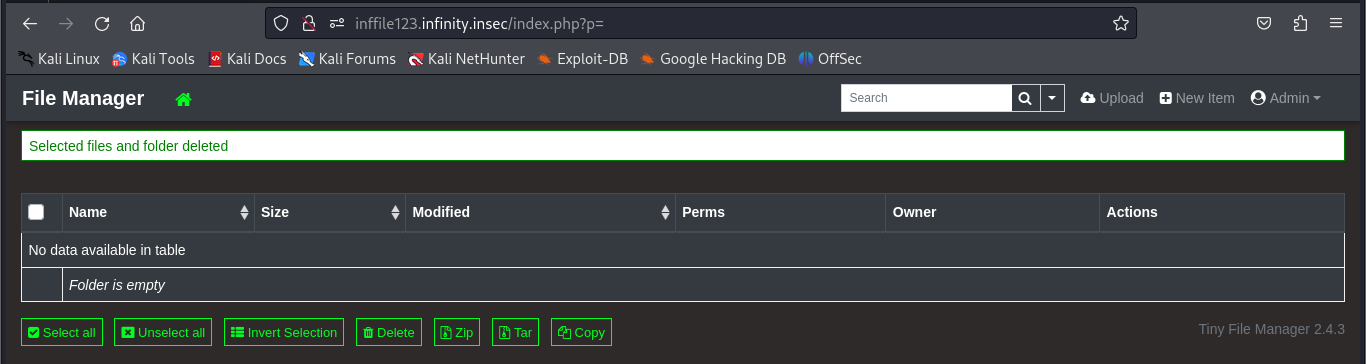
* QUESTION SECTION: hiển thị nội dung truy vấn của chúng ta.
* ANSWER SECTION: chứa câu trả lời cho câu truy vấn.
* STATUS: bao gồm thời gian thực hiện truy vấn, thời gian phản hồi và kích thước của gói tin phản hồi.
* Một loại truy vấn phổ biến của lệnh **dig** là **axfr**, dùng để truy vấn một zone DNS đầy đủ. Em sử dụng lệnh này để thu thập nhiều thông tin hơn. Sau khi thực thi, nhận thấy số lượng bản ghi đã tăng lên, gồm SOA, NS, A và xuất hiện thêm những **ns1.infinity.insec. ns2.infinity.insec. l**à những domain con của **infinity.insec:**
* Chọn tùy ý một subdomain để kiểm tra, sử dụng tùy chọn ANY để truy vấn tất cả bản ghi. Tuy nhiên phản hồi lại không chứa gợi ý nào liên quan đến flag:



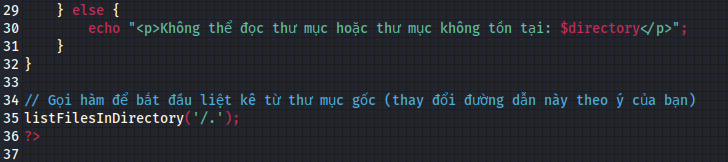
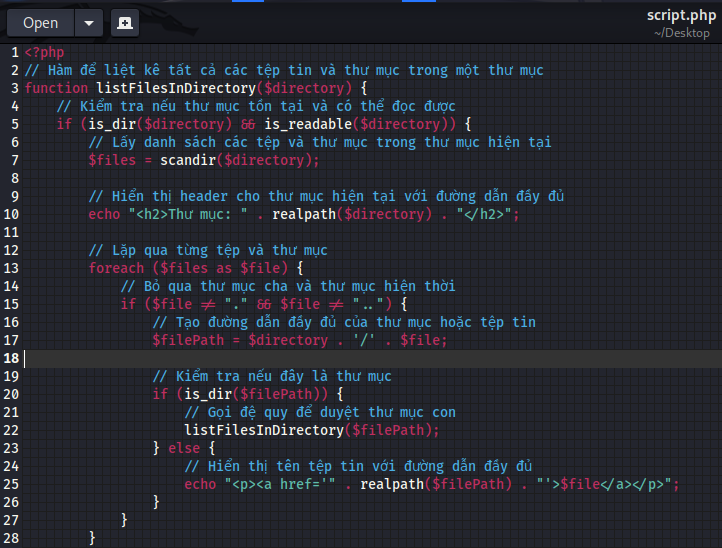
* Tiếp tục sẽ duyệt hết các subdomain còn lại, để nhận phản hồi truy vấn DNS liệu có chứa thông tin flag hay không? Đến **unk.infinity.insec**, tại ANSWER SECTION, đã thu được flag cần tìm:
* Kết quả flag: **INF02{74t1Frq4ZlHvGsSKGMxr}**

1. **Challenge 3:**

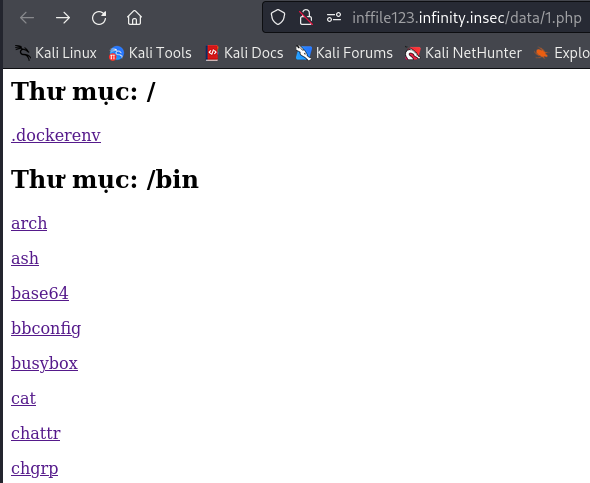
* Đầu tiền chúng ta thực hiện câu lệnh **dig @192.168.19.140 axfr infinity.insec** được sử dụng để thực hiện một hoạt động gọi là "zone transfer" trên tên miền "infinity.insec" từ một máy chủ DNS có địa chỉ IP là 192.168.19.140.
* Zone transfer cho phép máy chủ DNS yêu cầu tất cả hoặc một phần của dữ liệu zone (bao gồm các thông tin về tên miền như các bản ghi A, bản ghi MX, bản ghi NS, v.v.) từ một máy chủ DNS khác. Câu lệnh dig với tham số axfr là một trong những cách thức để thực hiện zone transfer.
* Thêm thông tin địa chỉ IP và tên miền vào tệp /etc/hosts trên hệ thống máy tính, việc này giúp máy tính ánh xạ tên miền (như example.com) thành địa chỉ IP cụ thể.
* Bây giờ, ta sẽ truy cập vào domain đã định nghĩa, thì kết quả hiển thị như sau:
* Vào trang github được giới thiệu ở dưới chúng ta sẽ thấy username/password mặc định và chúng ta có thể sử dụng chúng để đăng nhập.



* Bây giờ chúng ta sẽ tiến hành upload script lên để nó scan tất cả các file và thư mục.



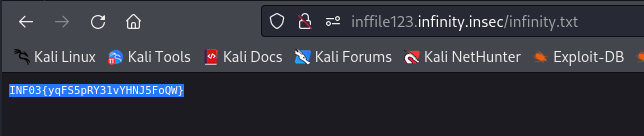
* Chúng ta có thể thấy danh sách ở đây:



* Click vào “dnsdomainname” ta sẽ thấy được script.
* Sau khi script được hiển thị bấm open để xem và thấy được subdomain infinity.txt khả nghi.



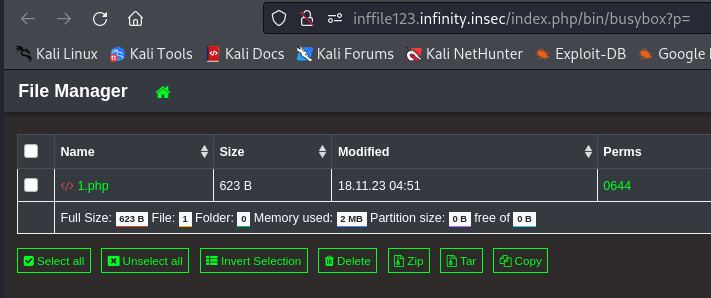
* Bỏ vào sau domain ban đầu, ta tìm thấy được FLAG.

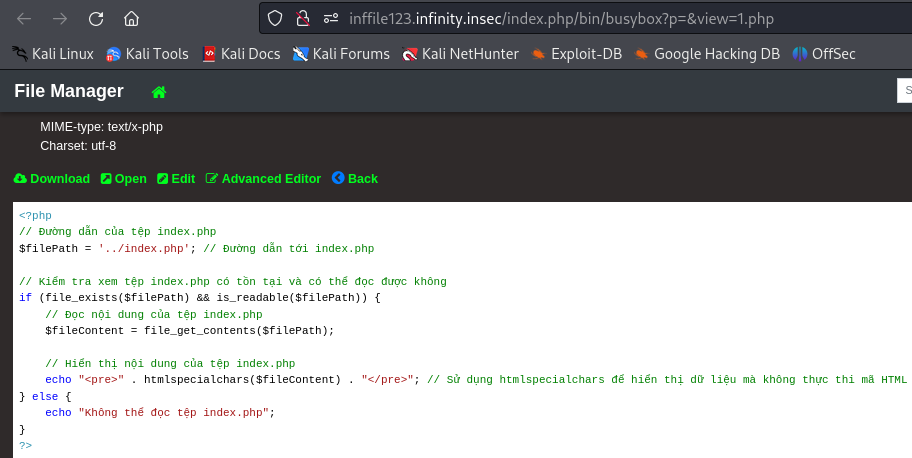


* **Kết quả flag: INF03{yqFS5pRY31vYHNJ5FoQW}**

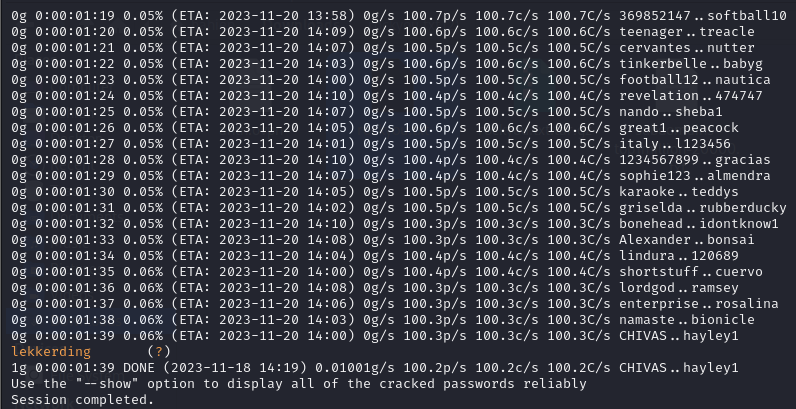
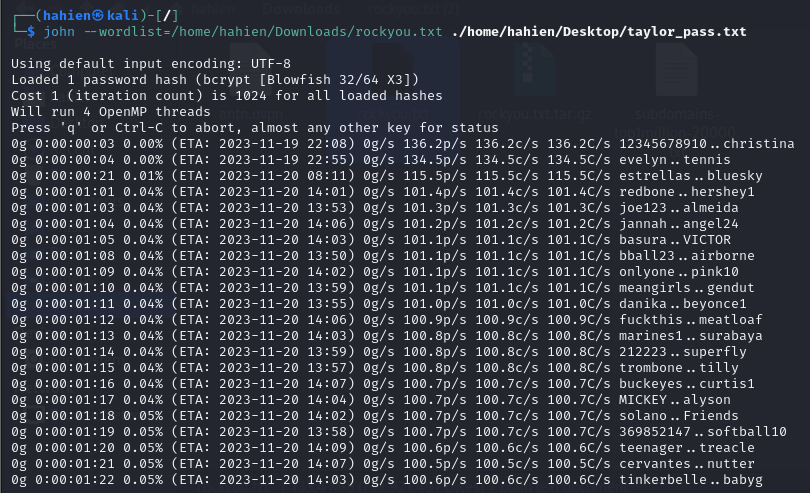
1. **Challenge 4:**

* Chúng ta tiếp tục kiểm tra các file và đường dẫn để xem các lỗ hổng tiếp theo.

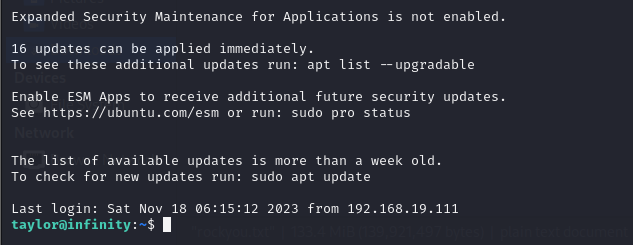
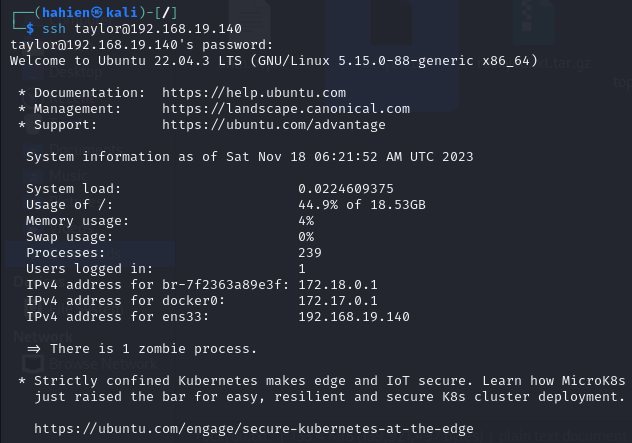




* Ta đã thấy thông tin về user và password đã được mã hoá tương ứng, ở đây thì 2 user đầu tiên là 2 user mặc định ban đầu đã có, vậy bây giờ chúng ta cần khai thác user tiếp theo là “taylor”.
* Thông tin này cung cấp danh sách người dùng và mật khẩu đã được mã hóa bằng bcrypt để xác thực đăng nhập vào ứng dụng Tiny File Manager. Ta có thể sử dụng các cặp tên người dùng và mật khẩu đã được mã hóa để đăng nhập vào ứng dụng.
* Ví dụ:
  + Người dùng: admin, Mật khẩu đã mã hóa: $2y$10$/K.hjNr84lLNDt8fTXjoI.DBp6PpeyoJ.mGwrrLuCZfAwfSAGqhOW
  + Người dùng: user, Mật khẩu đã mã hóa: $2y$10$Fg6Dz8oH9fPoZ2jJan5tZuv6Z4Kp7avtQ9bDfrdRntXtPeiMAZyGO
  + Người dùng: taylor, Mật khẩu đã mã hóa: $2y$10$Z51V0BOLzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW
* Khi đăng nhập vào ứng dụng Tiny File Manager, ta cần sử dụng một trong các cặp tên người dùng và mật khẩu đã được mã hóa để xác thực và truy cập vào các tính năng quản lý tệp của ứng dụng.
* Bây giờ, để chúng ta có thể tìm được password của user “Taylor” ta sử dụng john và wordlist rockyou.txt cùng với password đã được mã hoá. Ta thực hiện chạy lệnh sau:



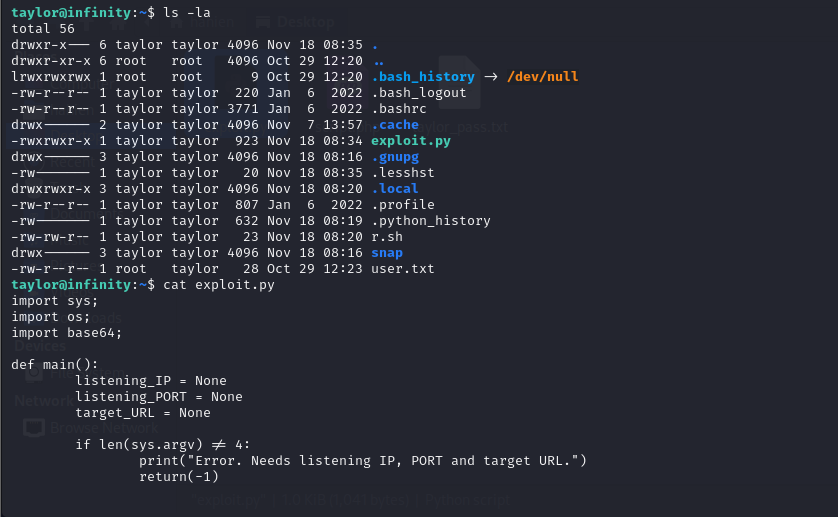
* Sau khi chạy xong, ta truy cập vào đường dẫn ~/.john để mở john.pot và ta thấy được mật khẩu của user “Taylor” là “lekkerding”.
* Tiếp theo, chúng ta kết nối ssh đến user Taylor cùng với địa chỉ IP và sau đó nhập password đã tìm ra ở trên. Ta sẽ vào được taylor@infinity.



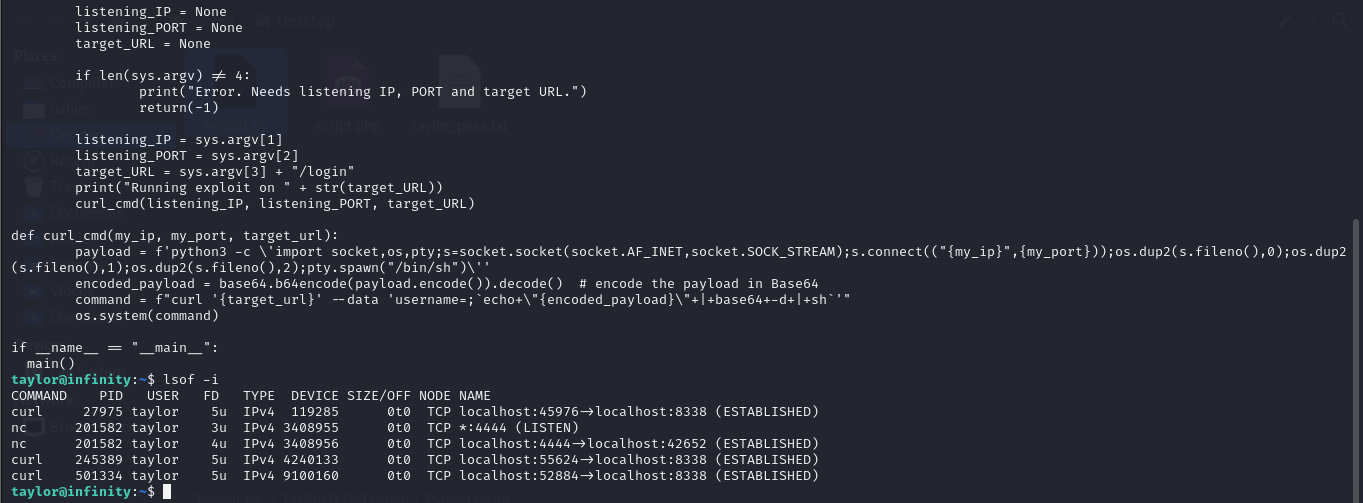
* Bây giờ ta thực hiện lệnh cat user.txt thì ta thấy FLAG đã xuất hiện.
* **Kết quả flag: INF04{38vxzg3tQAa7HRNaJbY6}**

1. **Challenge 5:**

* Tiếp tục với nhiệm vụ tiếp theo, trước tiên, thực hiện lệnh ls –la để xem rõ đang có những gì ở đây. Sau khi hiển thị thì ta thấy file exploit.py rất khả nghi và ta cat exploit.py ra để xem.



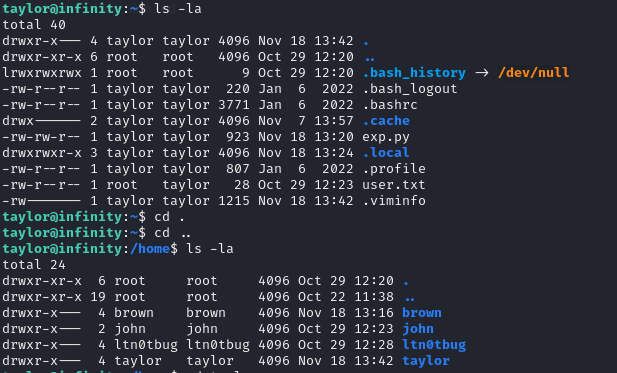
* Tiếp đến ta sử dụng lsof -I để quét tất cả các port đang mở.



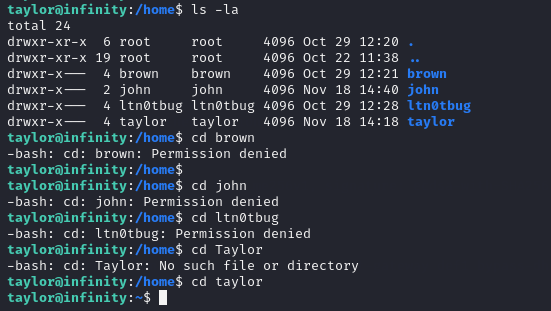
* Cuối cùng chúng ta mở port đang lắng nghe là 4444, và chạy file python3 exploit.py 127.0.0.1 4444 <http://localhost:8338> và ta đã truy cập được vào shell, tiếp tục tiến hành cat flag.txt khả nghi và ta thấy FLAG đã xuất hiện.
* **Kết quả flag: INF05{laFkXsmCsIwcskSMgMbG}**

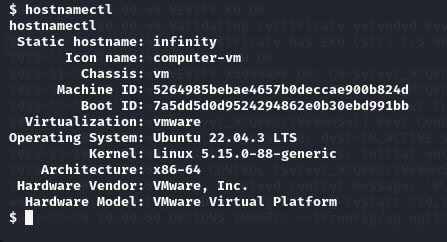
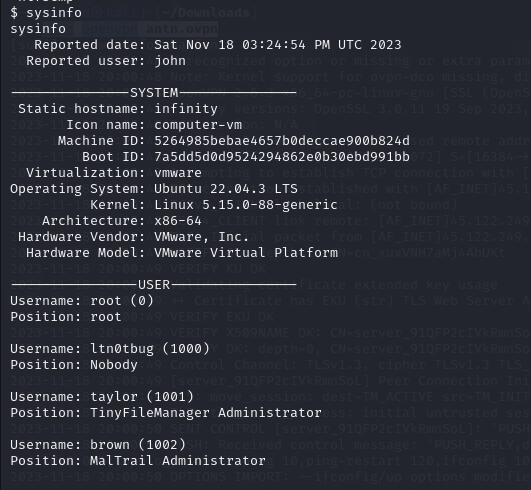
1. Challenge 6:

* Ta tiếp tục khai thác ở đây, thì ta thấy những thư mục như brown, john, ltn9tbug đều rất khả nghi.

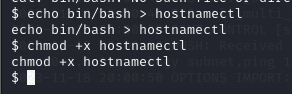


* Thử truy cập vào các thư mục này, ta thấy chưa đủ quyền để vào nên có khả năng cao chúng ta phải leo quyền (privilege-escalation) để vào được các thư mục kiểm tra xem flag có ở trong đó không.

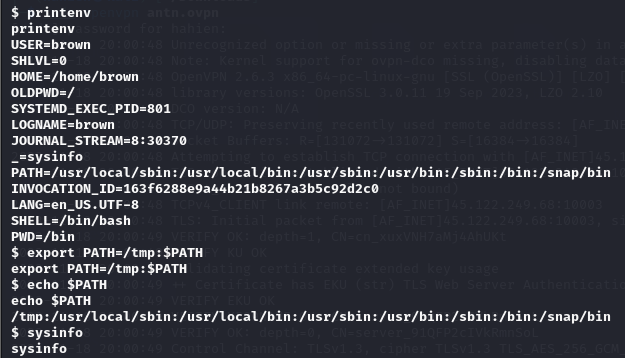


* Ở bài trước thì ta đã vào được shell của brown, bây giờ chúng ta tiến hành khai thác /bin/sysinfo,/bin/hostnamectl.
* Ta thấy 2 file này có phần giống với nhau, từ đây ta thấy có thể nó có thể bị ghi đè, tận dụng điều này để leo quyền.
* Vào /tmp tạo hostnamectl và cấp quyền thực thi cho nó.

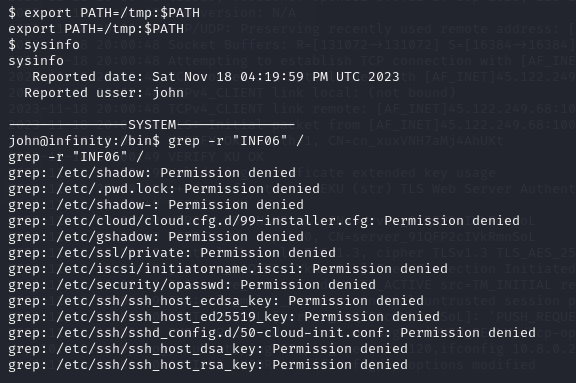


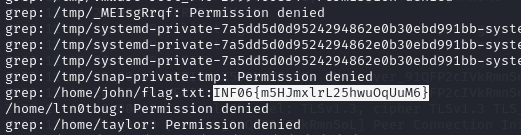


* Sau đó export PATH=/tmp:$PATH để set chạy trong môi trường /tmp



* Kết quả chúng ta đã leo quyền lên john thành công.

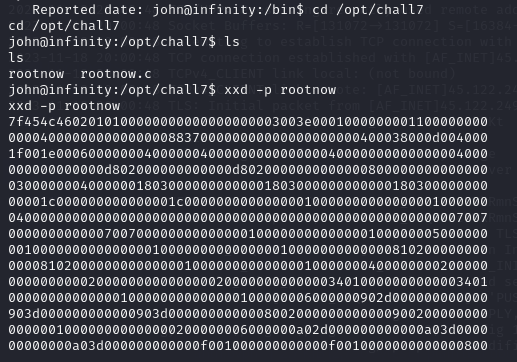




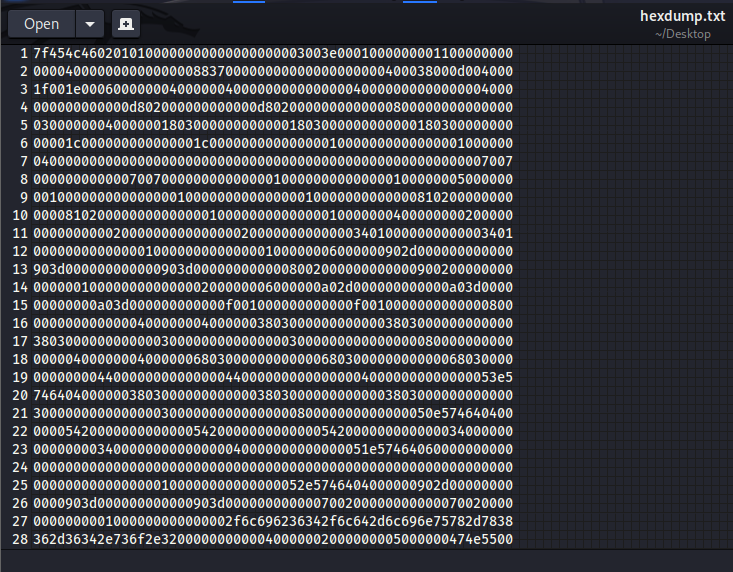
* **Kết quả flag: INF06{m5HJmxlrL25hwuOqUuM6}**

1. Challenge 7:

* Tiếp tục tận dụng quyền của John để truy cập vào /opt/chall7, sau đó sử dụng lệnh ls để xem trong thư mục có gì.
* Kết quả cho thấy có 2 file rootnow và rootnow.c
* Tiến hành thực hiện lệnh xxd –p rootnow để thực hiện việc chuyển đổi nội dung của file có tên là rootnow thành mã hex (hexadecimal).



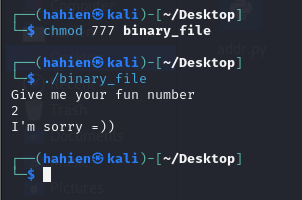
* Sau đó copy bản mã hex vào 1 file có tên là hexdump.txt.



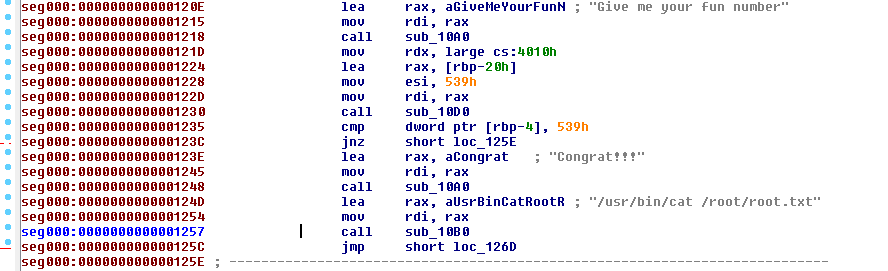
* Tiếp đến, thực hiện lệnh xxd -r -p hexdump.txt > binary\_file để chuyển đổi từ mã hex trong file hexdump.txt thành dạng dữ liệu nhị phân và lưu kết quả vào binary\_file.



* Sau đó cấp quyền thực thi và thử chạy ./binary\_file



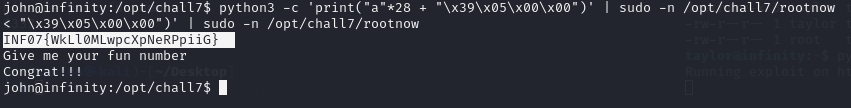
* Bây giờ ta copy file binary\_file ra ngoài để bỏ vào IDA Pro để phân tích.
* Ta có thể thấy một chuỗi hàm gọi và so sánh giá trị được lưu tại [rbp-4] với giá trị 539h. Nếu chúng không khớp (jnz), chương trình sẽ nhảy đến loc\_125E để in ra chuỗi "I'm sorry =))". Ngược lại, nếu giá trị tại [rbp-4] là 539h, chương trình sẽ tiếp tục chạy và in ra chuỗi "Congrat!!!" và thực hiện lệnh /usr/bin/cat /root/root.txt. Vì vậy chuổi cần được ghi đè là \x39\x05\x00\x00 trong định dạng little-endian.



* Ta cũng sẽ có stack như sau:

|  |  |
| --- | --- |
| Parameter |  |
| Return address | Ebp + 0x4 |
| Saved ebp | ebp |
| Local variables | Ebp - 0x20 |

* Việc thực thi câu lệnh **python3 -c 'print("a"\*28 + "\x39\x05\x00\x00")' | sudo -n /opt/chall7/rootnow** thực hiện việc tạo ra một chuỗi ký tự có độ dài 28 (được tạo từ 28 ký tự "a") kết hợp với \x39\x05\x00\x00 trong định dạng little-endian (địa chỉ memory trong bộ nhớ). Sau đó, lệnh sử dụng sudo để chạy một chương trình có đặc quyền (/opt/chall7/rootnow) và truyền chuỗi này vào chương trình đó thông qua đầu vào chuẩn (stdin).
* Khi các bước trên được thực hiện, lỗ hổng buffer overflow trong chương trình /opt/chall7/rootnow sẽ bị khai thác và in ra FLAG.



* **Kết quả flag: 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.O11.ANTN1.7] 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.ANTN1.7] 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** |
| 192.168.19.140 | Ssh [taylor@192.168.19.140](mailto:taylor@192.168.19.140)  Password: lekkerding | INF04{38vxzg3tQAa7HRNaJbY6} | INF07{WkLl0MLwpcXpNeRPpiiG} |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**- HẾT-**