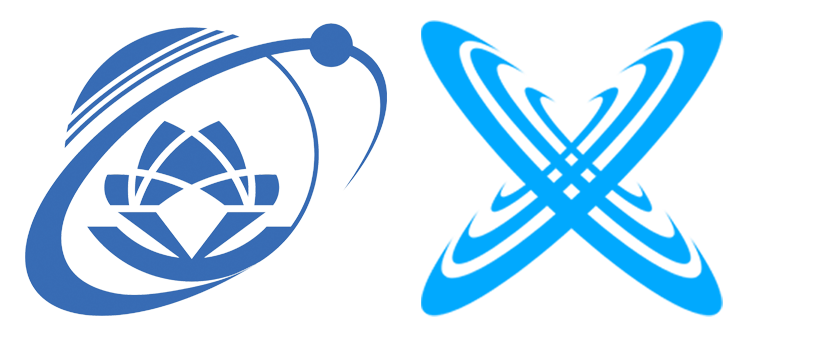
Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

|  |  |  |  |
| --- | --- | --- | --- |
| **Nhóm** | **Họ và tên** | **MSSV** | **Email** |
| 3Musketeers | Vương Minh Tiến | 19522346 | 19522263@gm.uit.edu.vn |
| Nguyễn Văn Tài | 19520250 | [19520250@gm.uit.edu.vn](mailto:19520250@gm.uit.edu.vn) |
| Phạm Thành Thái | 19520938 | [19520938@gm.uit.edu.vn](mailto:19520938@gm.uit.edu.vn) |
| Hoàng Văn Chúc | 19521288 | 19521288@gm.uit.edu.vn |



-- 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 local.txt và proof.txt 6](#_Toc57241323)

# 1.0 Tổng quan

3Musketeers 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, 3Musketeers 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, 3Musketeers 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 3Musketeers có thể truy cập vào được liệt kê dưới đây

* 192.168.19.115
* 192.168.19.116

## 1.1 Khuyến nghị bảo mật

3Musketeers 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

3Musketeers 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 3Musketeers 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, 3Musketeers 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:**

* 192.168.19.115
* 192.168.19.116

## 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, 3Musketeers đã có thể truy cập thành công vào 2 trong số 2 máy chủ.

### 2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.115

#### Thông tin dịch vụ

|  |  |
| --- | --- |
| **Địa chỉ IP** | **Các port đang mở** |
| 192.168.19.115 | **TCP: 22, 80, 49037, 50179, 53969** |
| **UDP:** [Liệt kê tất cả các port] |

#### Khởi tạo shell với quyền user thường

**Lỗ hổng đã khai thác: Lỗ hổng phpmyadmin, lỗ hổng WordPress**

**Giải thích lỗ hổng**:

* Lỗ hổng phpmyadmin: sử dụng lệnh GET, sau đó là POST để thực hiện các tác vụ của cơ sở dữ liệu. Ở đây, sử dụng lệnh POST để brute force tài khoản để xâm nhập vào trang web
* Lỗ hổng WordPress: lỗ hổng cho phép tin tặc xóa các tệp tin trên máy chủ và chiếm quyền điều khiển website

**Khuyến nghị vá lỗ hổng**:

* Lỗ hổng phpmyadmin: sử dụng các bản vá mới nhất,
* Lỗ hổng WordPress:
  + Rà soát lại danh sách người dùng và các quản trị viên
  + Thực hiện backup toàn bộ dữ liệu của website để tránh trường hợp bị tin tặc tấn công phá hoại

**Mức độ ảnh hưởng: Nghiêm trọng**

**Cách thức khai thác:**

|  |
| --- |
| [Lệnh tấn công/mã khai thác]  [màu đỏ nếu có thay đổi trong mã khai thác] |

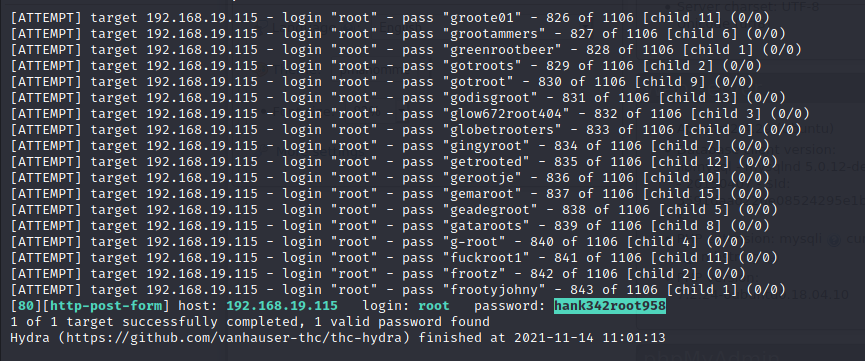
[Step-by-step cách thức để có quyền truy cập vào máy chủ]

Theo hint, ta có thể đoán được rằng trong password có chứa “root”, do đó ta lọc những password có chứa “root” trong rockyou.txt và lưu vào file passroot.txt

**$ cat /usr/share/wordlists/rockyou.txt | grep “root” > passroot.txt**

Với user là “root”, ta tiến hành brute force bằng hydra để tìm mật khẩu:

**$hydra -l root -P passroot.txt** [**192.168.19.115**](http://192.168.19.115/?fbclid=IwAR1Kn-5-QDqUGPt5cUQDHIhPd17Hf2gRVj_2f30pGecHmhNpR1zxq-VLyog) **-V http-post-form "/phpmyadmin/index.php:pma\_username=^USER^&pma\_password=^PASS^&server=1:denied"**



Sử dụng cặp user password vừa lấy được là **root:hank342root958** để đăng nhập vào **192.168.19.115/phpmyadmin/** và tiến hành tạoaccount để đăng nhập vào trang **192.168.19.115/wp-login.php**

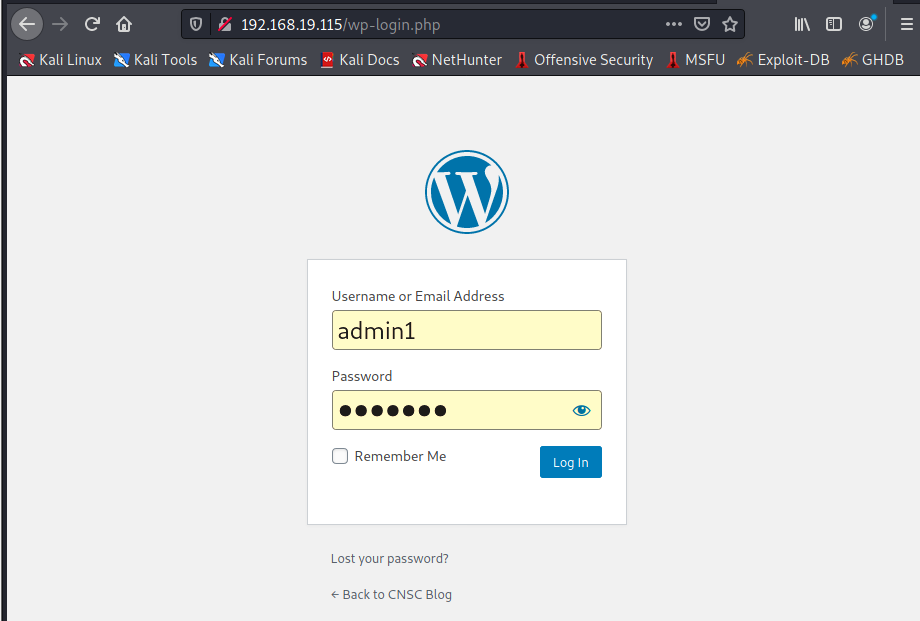
Graphical user interface, text, application, chat or text message

Description automatically generated

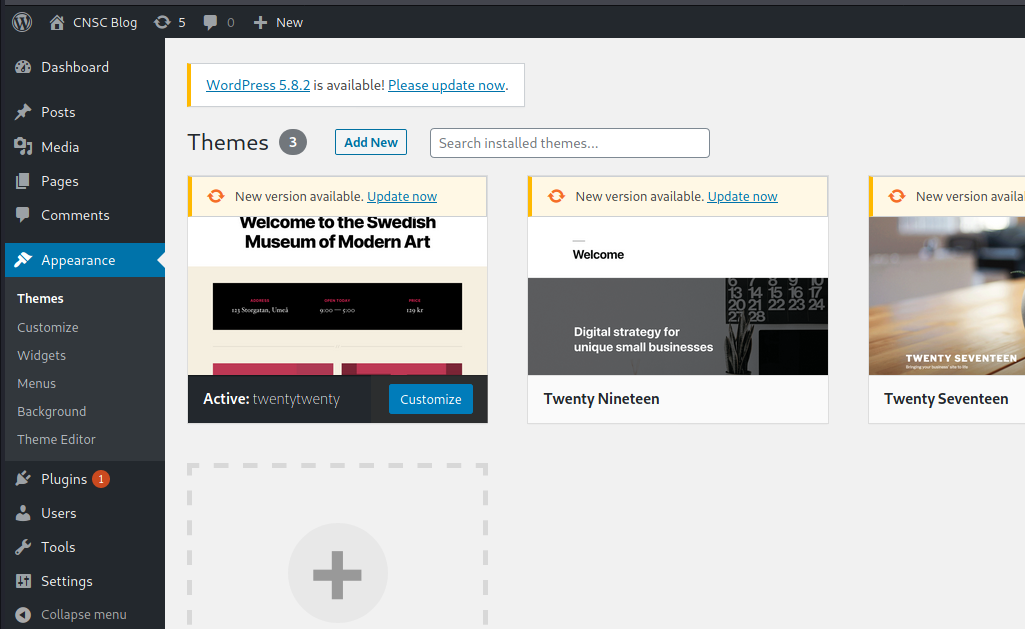
Graphical user interface, text, application

Description automatically generated

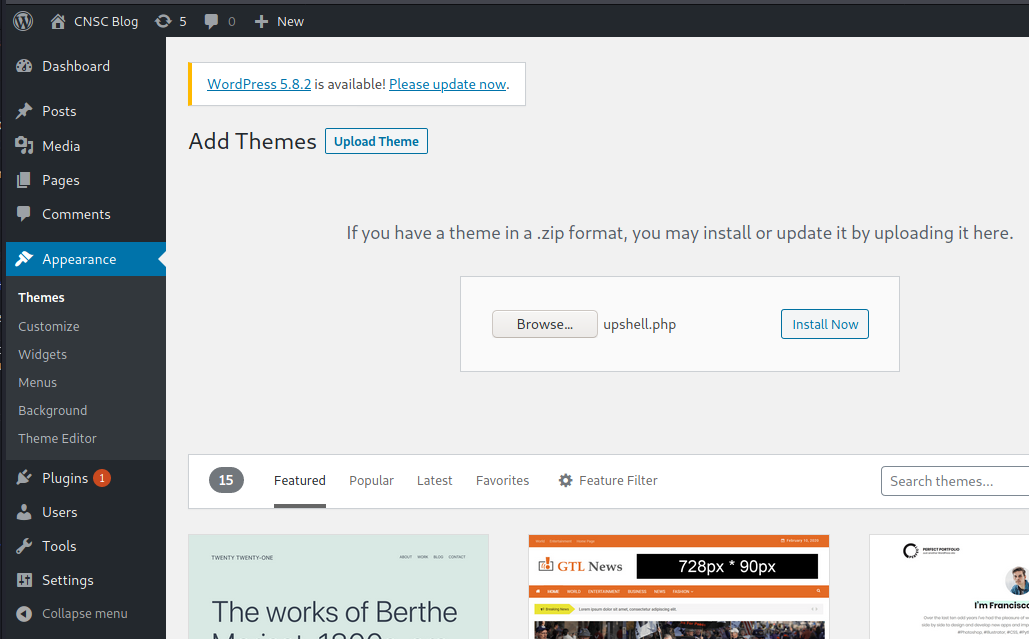
Với user và password vừa tạo truy cập vào trang web



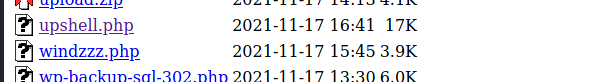
Ở đây ta tiến hành upshell bằng php. Tiến hành tìm kiếm cách upshell trên mạng thì ta tìm được cách upshell thông qua các theme php trên wordpress. Và có luôn cả code cho file php.

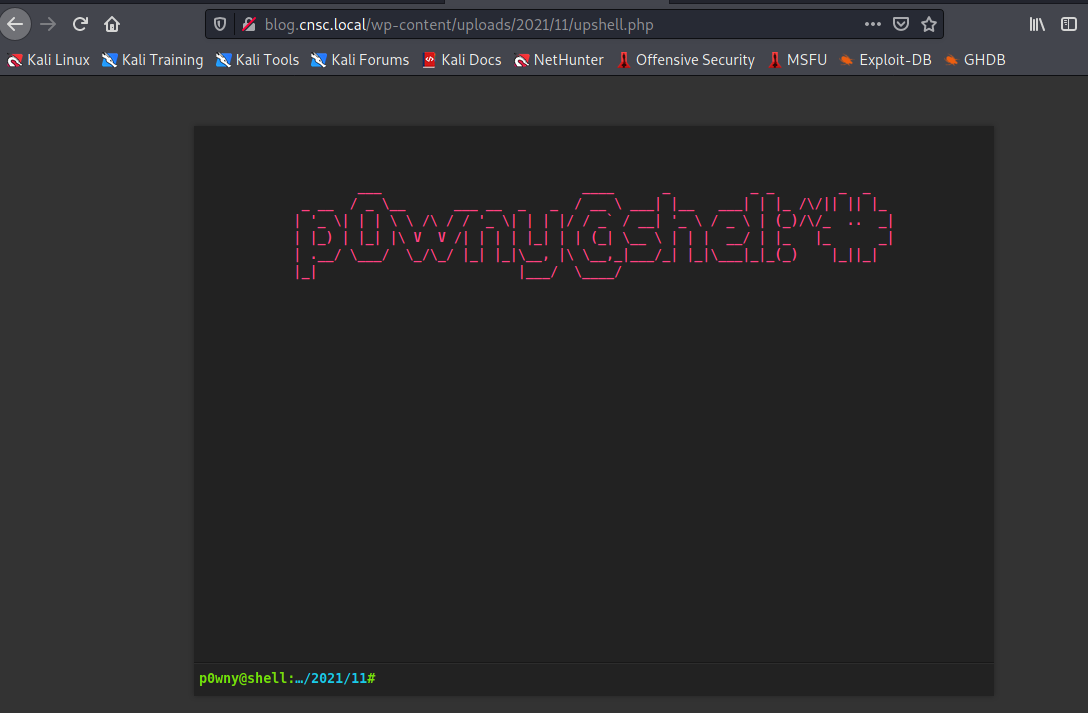


Ta chọn add new --> chọn upload theme sau đó upload file code upshell.php chứa shell vừa tạo ở máy chúng ta. Sau đó install để upshell lên thành công.

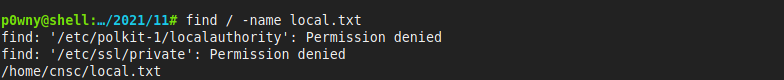


Tiếp theo kiểm tra ở thư mục /wp-content/uploads/2021/11 xem file chúng ta up đã có chưa nếu có thì t mở nó lên bằng cách click vào nó nếu thành công thì shell sẽ hiện lên và đã thành công upshell

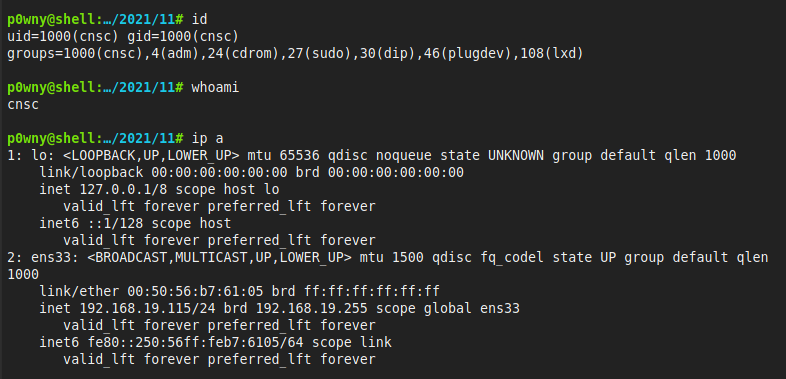




Tiếp tục tìm file local.txt và mở lên ta sẽ có được flag của Ghost Baby



**Hình ảnh minh chứng:**



**Nội dung tập tin Local.txt:**



#### Leo thang đặc quyền

**Lỗ hổng đã khai thác: Không cài đặt tài khoản vào root**

**Giải thích lỗ hổng: Khi kiểm tra đặc quyền của người dùng, có thể xuất hiện một cách truy cập vào root mà không cần mật khẩu, do đó có thể sử dụng đặc quyền của root để tấn công.**

**Khuyến nghị vá lỗ hổng: cung cấp mật khẩu để bảo vệ root toàn vẹn**

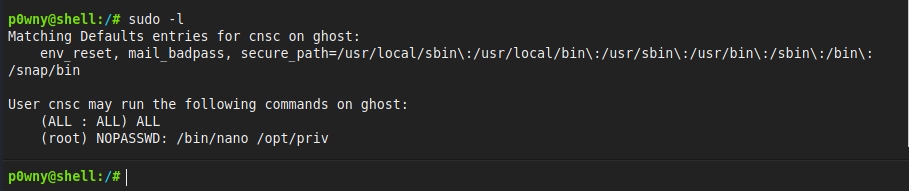
**Mức độ ảnh hưởng: Nghiêm trọng**

**Cách thức khai thác:**

|  |
| --- |
| [Lệnh tấn công/mã khai thác]  [màu đỏ nếu có thay đổi trong mã khai thác] |

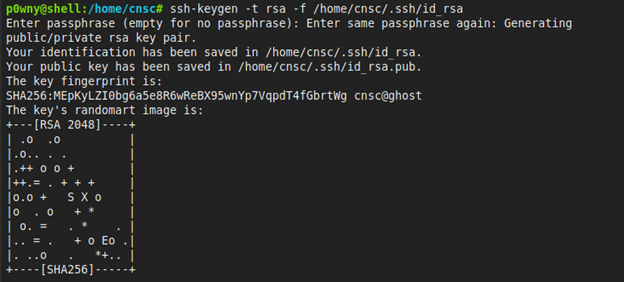
[Step-by-step cách thức để có quyền truy cập vào máy chủ]

Sử dụng sudo –l để kiểm tra đặc quyền của user **cnsc**

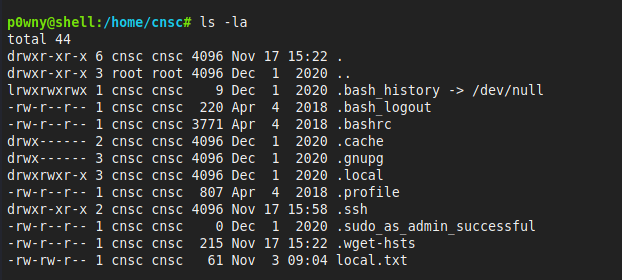


Ta nhận thấy khi sử dụng sudo /bin/nano /opt/priv thì không cần mật khẩu vẫn có thể vào được quyền root.

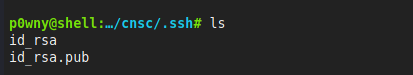
Tuy nhiên ở trên shell không thể truy cập vào root, do đó ta tạo một cặp khóa để kết nối thông qua ssh Tiến hành tạo cặp key rsa cho quá trình xác thực bằng lệnh: **ssh-keygen -t rsa -f /home/cnsc/.ssh/id\_rsa**



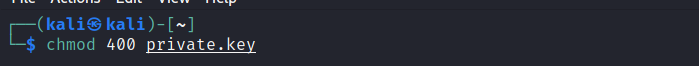
Kiểm tra thấy key nằm tại thư mục /home/cnsc/.ssh



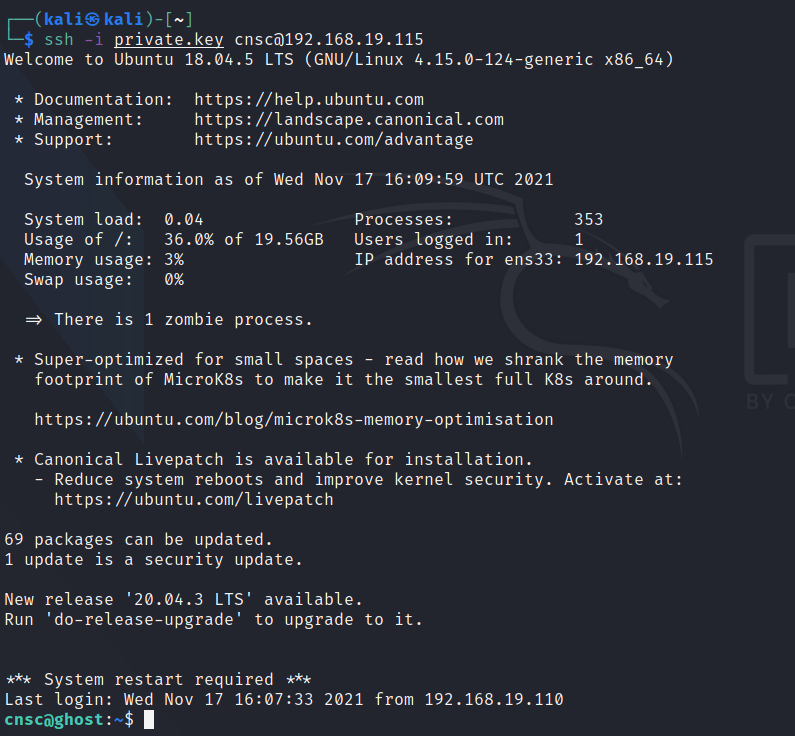
Lúc này trong thư mục .ssh chứa hai khóa là id\_rsa (khóa private) và id\_rsa.pub (khóa công khai)



Ta tiến hành lấy file id\_rsa lưu vào phía máy của mình và cấp phát quyền cho file private.key (id\_rsa)



Sau đó tiến hành kết nối ssh vào [cnsc@192.168.19.115](mailto:cnsc@192.168.19.115)



Truy cập vào root với lệnh s**udo /bin/nano /opt/priv** thì truy cập thành công

Nhấn tố hợp Ctrl R sau đó Ctrl X để thực thì lệnh trên nano

Và ta nhập lệnh bên dưới thì sẽ vào được root và từ đó tìm proof.txt và flag

Graphical user interface

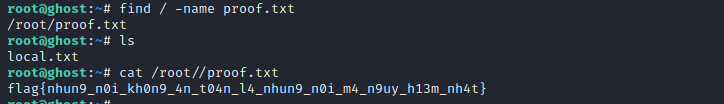
Description automatically generated

**Hình ảnh minh chứng:**

Graphical user interface

Description automatically generated

**Nội dung tập tin Proof.txt:**



### 2.2.2 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.116

#### hông tin dịch vụ

|  |  |
| --- | --- |
| **Địa chỉ IP** | **Các port đang mở** |
| 192.168.19.116 | **TCP: 42, 53, 80, 135, 445, 3389, 5985, 49666, 49669, 49670** |
| **UDP:** [Liệt kê tất cả các port] |

#### Khởi tạo shell với quyền user thường

**Lỗ hổng đã khai thác:** Lỗ hổng trên giao thức SMB

Text

Description automatically generated

**Giải thích lỗ hổng**: SMB (Server Message Block) là một giao thức chia sẻ tệp mạng cho phép người dùng hoặc ứng dụng yêu cầu tệp và dịch vụ qua mạng. Khi sử dụng giao thức SMB, một ứng dụng (hoặc người dùng ứng dụng) có thể truy cập file trong máy chủ từ xa cũng như các nguồn tài nguyên khác, bao gồm máy in, mailslots và named pipe. Khi attacker khai thác lỗ hổng này có thể chiếm được các đặc quyền giống như tài khoản đang chạy máy chủ SMB và các quy trình khách. Kẻ tấn công sau đó có thể cài đặt các chương trình; xem, thay đổi hoặc xóa dữ liệu; hoặc tạo tài khoản mới với đầy đủ quyền của người dùng.

**Khuyến nghị vá lỗ hổng**:

* Update window: cập nhật các bản vá mới nhất của window để tránh gặp phải các lỗ hổng
* Chặn các port 135, 445 nếu không cần thiết sử dụng
* Chạy tất cả các phần mềm như một người dùng không có đặc quyền (một phần mềm không có đặc quyền quản trị) để giảm tác động của một cuộc tấn công thành công.
* Nhắc nhở người dùng không truy cập trang web hoặc theo dõi các liên kết được cung cấp bởi các nguồn không xác định hoặc không đáng tin cậy.
* Thông báo và giáo dục người dùng về các mối đe dọa do các liên kết siêu văn bản có trong email hoặc tệp đính kèm đặc biệt là từ các nguồn không đáng tin cậy.
* Áp dụng nguyên tắc ít đặc quyền nhất cho tất cả các hệ thống và dịch vụ.

**Mức độ ảnh hưởng: Cao**

**Cách thức khai thác:**

|  |
| --- |
| [Lệnh tấn công/mã khai thác]  [màu đỏ nếu có thay đổi trong mã khai thác] |

Tìm kiếm thông tin bằng **SMB Enumeration** bằng user **invaliduser**

A screenshot of a computer

Description automatically generated with medium confidence

Thực hiện download folder Backup bằng lệnh mount

***mount -t cifs -o username=guest //192.168.19.116/Backups /mnt/bastion/***

Nếu báo lỗi chưa tồn tại folder thì nên tạo sẵn file

**Text

Description automatically generated**

Có thấy trong folder “Backup … 102804” có tồn tại 2 file vhdx

guestmount --add "/mnt/bastion/WindowsImageBackup/Sammy-PC/Backup 2020-11-30 102804/88e506b5-0000-0000-0000-602200000000.vhdx" --inspector --ro /mnt/vhd

Thực hiện guestmount file vhdx để lấy data

**A screenshot of a computer

Description automatically generated with medium confidence**

Có thể thấy đây là ổ C của máy Windows được backup lại với các thư mục như Users, Program Files, ….

**Text

Description automatically generated**

Tại Windows/System32/config có chứa 2 file SAM và SYSTEM, dump 2 file này chúng ta có thể thấy được thông tin xác thực của user.

Có 1 số tool dump sẵn trong máy nhưng nó khá cùi bắp, nên sử dụng Impacket để dump (github)

python3 secretsdump.py -sam SAM -system SYSTEM LOCAL

Nên copy 2 file SAM và SYSTEM từ folder config sau khi mount vào folder impacket/example để dễ thực hiện và lưu trữ.

Text

Description automatically generated

Sau đó ta thấy có xuất hiện user sammy, với info

sammy:1001:aad3b435b51404eeaad3b435b51404ee:acb6c481b437b1239fe4746a87b76c07:::

Thực hiện crask NTLM ta được pass là iluvstarbucks94



Tuy nhiên server không bật ssh, thế nên phải sử dụng tool khác để remote tới máy này.

evil-winrm -i 192.168.19.116 -u sammy -H acb6c481b437b1239fe4746a87b76c07

Text

Description automatically generated

**Hình ảnh minh chứng:**

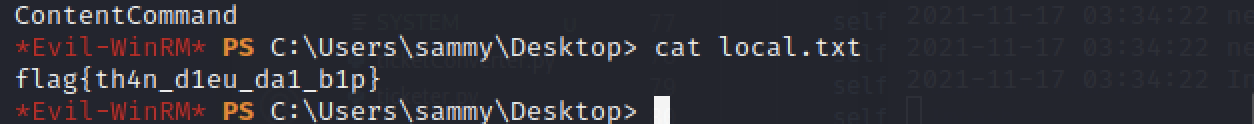
[Hình ảnh chứa nội dung: tên user đã bị kiểm soát (whoami), địa chỉ IP (ipconfig)]

A picture containing text

Description automatically generated

**Nội dung tập tin Local.txt:**

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

****

flag{th4n\_d1eu\_da1\_b1p}

#### Leo thang đặc quyền

**Lỗ hổng đã khai thác: SMB**

**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]

Graphical user interface

Description automatically generated with medium confidence

Quay lại ổ đĩa C để tiến hành khai thác từ các folder đã lấy được, tuy nhiên nó ít hơn so với các folder đã mount được ở /mnt/vhdA screenshot of a computer

Description automatically generated with medium confidence

Thực hiện với cú pháp ls -hidden để kiểm tra, thì thấy có xuất hiện thêm folder Transcripts, đây là thư mục khả nghi.

Text

Description automatically generated

Bên trong thư folder Transcript lại chứa folder hidden khác =))

Text

Description automatically generated

Trong folder bị hidden chứa fake flag và 1 file bị hidden =))))

Cat file này ra ta đọc được khá nhiều thông tin, nhưng cụ thể thì đây chính là file lịch sử của powershell bên máy win.

A screenshot of a computer

Description automatically generated with medium confidence

Có thông tin cuối cùng thì john là tài khoản admin, kéo lên trên để điều tra tiếp và phát hiện một đoạn code với các biến $foo và $fO0 khả nghi.

A picture containing text, bottle, screenshot, plaque

Description automatically generated

Xuất ra màn hình giá trị của biến $fO0 và phát hiện ra password:



Sau khi có được pass, ta tiến hành remote tới bằng lệnh “**rdesktop -u john 192.168.19.116**”

A picture containing graphical user interface

Description automatically generated

Tiếp tục đăng nhập

Graphical user interface, website

Description automatically generated

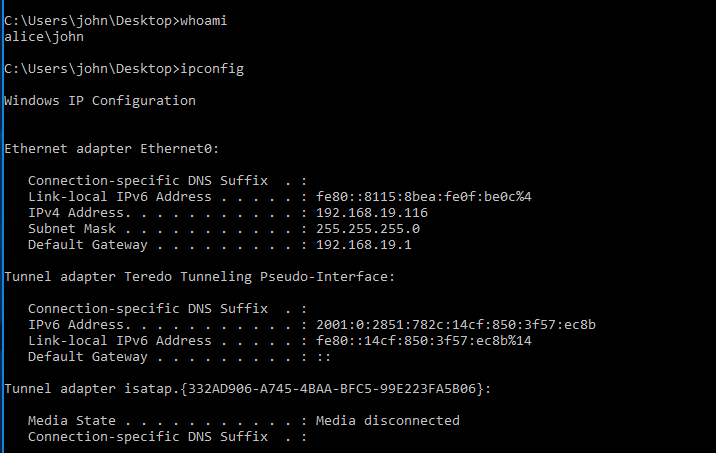
Đăng nhập thành công

A screenshot of a computer

Description automatically generated with medium confidence

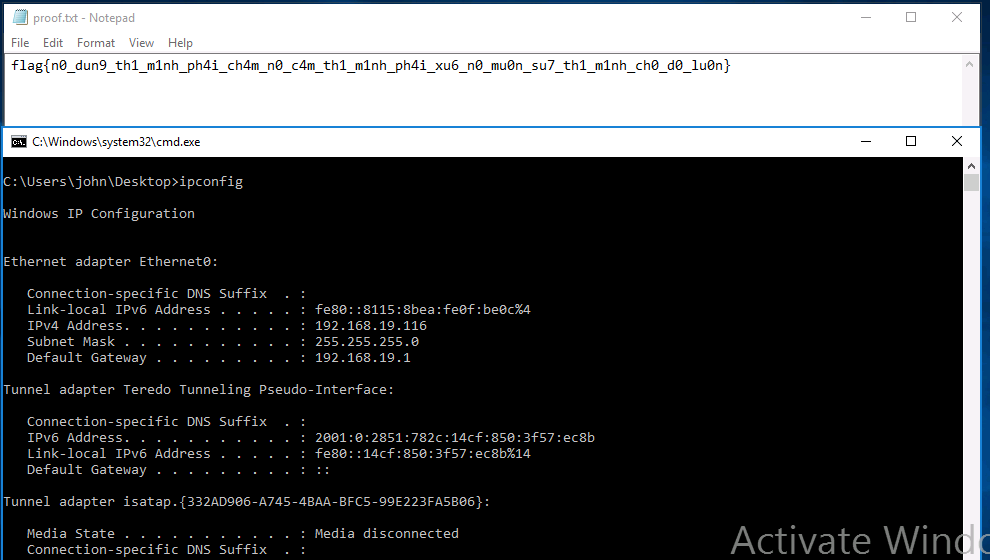
**Hình ảnh minh chứng:**

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



**Nội dung tập tin Proof.txt:**

[Hình ảnh chứa nội dung: địa chỉ IP (ipconfig), nội dung tập tin proof.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. 3Musketeers 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, 3Musketeers 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 local.txt và proof.txt

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Địa chỉ IP (Hostname)** | | **Nội dung local.txt** | | **Nội dung proof.txt** |
| 192.168.19.115 | flag{ph4i\_b13t\_ch4n\_l1\_0\_d4u\_dun9\_d3\_b1\_du4\_v40\_ch4n\_tu0ng9} | | flag{nhun9\_n0i\_kh0n9\_4n\_t04n\_l4\_nhun9\_n0i\_m4\_n9uy\_h13m\_nh4t} | |
| 192.168.19.116 | flag{th4n\_d1eu\_da1\_b1p} | | flag{n0\_dun9\_th1\_m1nh\_ph4i\_ch4m\_n0\_c4m\_th1\_m1nh\_ph4i\_xu6\_n0\_mu0n\_su7\_th1\_m1nh\_ch0\_d0\_lu0n} | |
|  |  | |  | |
|  |  | |  | |

**- HẾT-**