Impacket là bộ công cụ Python giúp thực hiện tấn công vào hệ thống Windows bằng cách khai thác các giao thức mạng như SMB,WMI,DCOM,Kerberos,….

1. Wmiexec.py: Thực hiện lệnh từ xa qua WMI

Nó yêu cầu quyền Admin trên máy mục tiêu. Nhược điểm lớn nhất là nó sử dụng DCOM( là công nghệ cho phép các ứng dụng trên máy tính khác nhau tương tác được với nhau) và ta cần phải truy cập vào các cổng DCOM trên máy mục tiêu, nhưng đôi khi chúng lại bị chặn lại bới tường lửa, và bạn sẽ phải sử dụng những công cụ khác như smbclient.py

Xem thông tin hostname:

A computer screen with numbers and letters

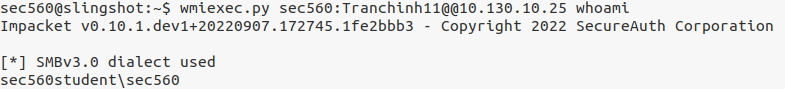
AI-generated content may be incorrect.

Xem thông tin người dung của máy mục tiêu

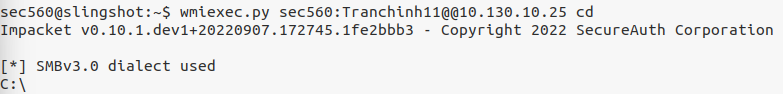
A computer screen shot of numbers

AI-generated content may be incorrect.

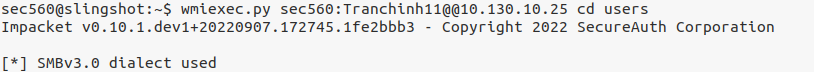
Thêm mật khẩu ngay sau user để dễ thực hiện lệnh



Hiển thị thư mục hiện tại



Thử dịch chuyển đến thư mục users



Ta sẽ thấy ko có output. Ghi nhớ rằng lệnh này sẽ dịch chuyển ta đến thư mục users. Tuy nhiên wmi không giữ nguyên trạng thái của shell sau mỗi lệnh. Tức là ta vừa dịch chuyển đến users trong phiên đó thì nó sẽ bị đóng phiên ngay

Chạy lại tool mà ko có lệnh

A screen shot of a computer code

AI-generated content may be incorrect.

Ta sẽ nhận lại 1 shell tương tác. Thử 1 vài lệnh

A computer screen shot of a computer code

AI-generated content may be incorrect.

1. Smbexec.py

Công cụ này tương tự với wmiexec. Tuy nhiên nó có 2 chế độ, phụ thuộc vào cách công cụ này khởi chạy.

* Share mode: sử dụng share để thực hiện chia sẻ hoặc tương tác
* Server mode: vì 1 số lý do nào mà share ko khả dụng, mà sẽ tạo ra 1 SMB server local, và output của những lệnh thực thi sẽ được gửi lại bời máy mục tiêu bên trong các thư mục cục bộ chia sẻ. Và nhớ rằng bạn cần quyền root để mở cổng 445 trên máy cục bộ

Trong sharemode, công cụ sẽ viết trực tiệp lên đĩa của máy mục tiêu. Ta thường không muốn điều này vì nó sẽ để lại dấu vết. Trong server mode, máy nạn nhân sẽ kết nối với máy tấn qcoong thông qua server SMB đã tạo. Server sẽ chạy trên port 445 và yêu cầu quyền root để có thể lắng nghe trên port này. Chúng ta sẽ chạy công cụ trên server mode với quyền root

Chạy smbexec.py

A screenshot of a computer

AI-generated content may be incorrect.

Giống với công cụ wmiexec. Chạy lệnh whoami



Ta đang chạy với quyền system. Thử di chuyển đến thư mục users



Không thành công vì shell này ko duy trì phiên. Thử liệt kê các thư muc jtrong users

A screenshot of a computer

AI-generated content may be incorrect.

Xem thông tin file sec560

A screenshot of a computer

AI-generated content may be incorrect.

Thông tin Desktop

A screenshot of a computer program

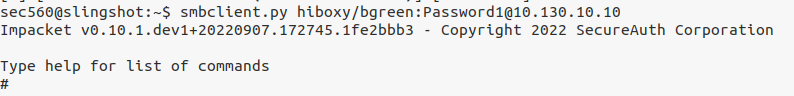
AI-generated content may be incorrect.

Việc lựa chọn smbexec hay wmiexec phụ thuộc vào hệ thống và sở thích cá nhân

1. Smbclient.py

Có sự khác biệt với smbexec. Được sử dụng để tương tác với các shares trên máy tính sử dụng giao thức smb. Kết nối với các shares với các máy từ xa để tải file lên và xuống, liệt kê các file và thư mục, và thực hiện nhiều thao tác thông qua SMB

Khởi động smbclient.py để kết nối với file server bằng tài khoản bgreen



H chúng ta có thể tương tác với client.

Help

A screenshot of a computer screen

AI-generated content may be incorrect.

Shares: liệt kê các các shares

Use {sharename}: kết nối đến share chỉ định

Cd {path}: điều hướng đến thư mục

Lcd{path}:

Put{filename}: uploads filename ở đường dẫn hiện tại

Get{filename}: downloads filename đến đường dẫn hiện tại

Shares

A screen shot of a computer

AI-generated content may be incorrect.

Những shares kết thúc bằng $ là những shares ẩn. ADMIN$, C$, IPC$ là những shares mặc định. Nó chỉ được truy cập bằng admin.

Sử dụng CertEnroll và xem các file trong thư mục hiện tại

A screen shot of a number

AI-generated content may be incorrect.

Tải 1 file và xem quyền của nó

A computer screen shot of a computer code

AI-generated content may be incorrect.

1. Lookupsid.py

Được sử dụng để tra cứu sid của tất các users trong domain. Ta cần phải chỉ định domain user. Trong trường hợp này là domain controller

A screenshot of a computer

AI-generated content may be incorrect.

Smbexec: Sử dụng giao thức smb(chia sẻ file, thực thi lệnh), ko duy trì phiên(chỉ tạo 1 dịch vụ từ xa tạm thời để thực thi lệnh và được ghi ra 1 file tạm trên hệ thống rồi đọc lại)

Wmiexec: Sử dụng giao thức wmi(quản lý hệ thống, thực thi lệnh), có duy trì phiên(output được chuyển tiếp dòng lệnh trực tiếp như interactive shell)