- Sử dụng lệnh sc để tạo một dịch vụ từ một trình nghe Netcat backdoor

- Để điều khiển một dịch vụ lắng nghe backdoor bằng cách sử dụng lệnh sc

- Thiết lập khả năng theo dõi cổng bằng cách sử dụng lệnh netstat của Windows

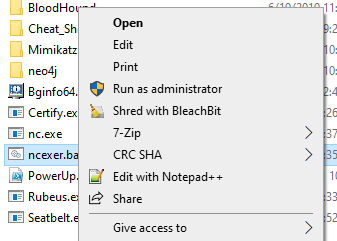
- Sử dụng wmic để tạo một trình nghe Netcat backdoor

- Phân tích cách wmic có thể theo dõi các tiến trình bằng cú pháp /every:1 của nó

# Mục tiêu:

thực hiện một lệnh kích hoạt Netcat listener, cho phép truy cập từ xa và tương tác với một command shell trên máy mục tiêu.

# 1.Setup



Nó sẽ hiện ra hai màn hình là màu xám và vàng, trong đó màu xám là nạn nhân (victim) còn màu vàng là của attacker.

e

lệnh sử dụng Netcat (nc) để tạo một kết nối nghe (listening) trên cổng 2222 và khi có kết nối đến, nó sẽ mở một phiên dòng lệnh cmd.exe trên máy tính đang chạy Netcat.

-nc.exe: Đây là chương trình Netcat được gọi để tạo và quản lý kết nối mạng.

-nvlp 2222: Các tùy chọn được sử dụng như sau:

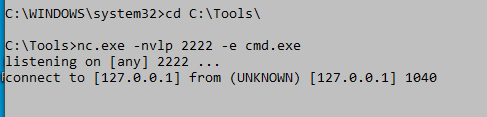
-n: Vô hiệu hóa việc sử dụng DNS (Domain Name System) để giải quyết tên miền.

-v: Hiển thị thông báo chi tiết.

-l: Chế độ lắng nghe (listening) cho phép Netcat chờ đợi kết nối đến.

-p 2222: Xác định cổng 2222 là cổng mà Netcat sẽ lắng nghe trên.

-e cmd.exe: Tùy chọn này chỉ định cho Netcat thực thi một lệnh cụ thể sau khi kết nối thành công. Trong trường hợp này, khi có kết nối đến cổng 2222, Netcat sẽ mở một phiên dòng lệnh cmd.exe trên máy tính đó.



Lệnh bạn đã cung cấp sử dụng Netcat (nc) để kết nối đến một máy chủ địa phương (localhost) trên cổng 2222.

nc.exe: Đây là chương trình Netcat được gọi để tạo và quản lý kết nối mạng.

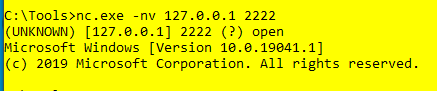
-nv: Các tùy chọn được sử dụng như sau:

-n: Vô hiệu hóa việc sử dụng DNS (Domain Name System) để giải quyết tên miền.

-v: Hiển thị thông báo chi tiết.

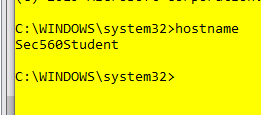
127.0.0.1: Đây là địa chỉ IP của máy chủ đích, trong trường hợp này là localhost (máy chủ địa phương). Địa chỉ IP 127.0.0.1 luôn đề cập đến máy tính hiện đang chạy lệnh, nghĩa là máy chủ địa phương.

2222: Đây là số cổng mà Netcat sẽ cố gắng kết nối đến trên máy chủ đích.

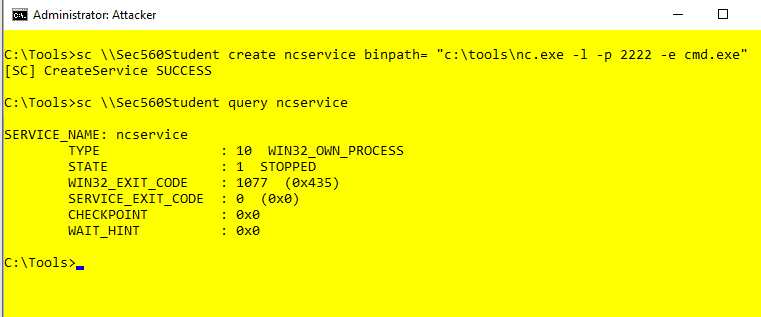


# 2. Tạo service

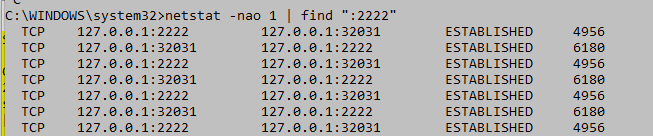
Check lại hostname của cmd atk:



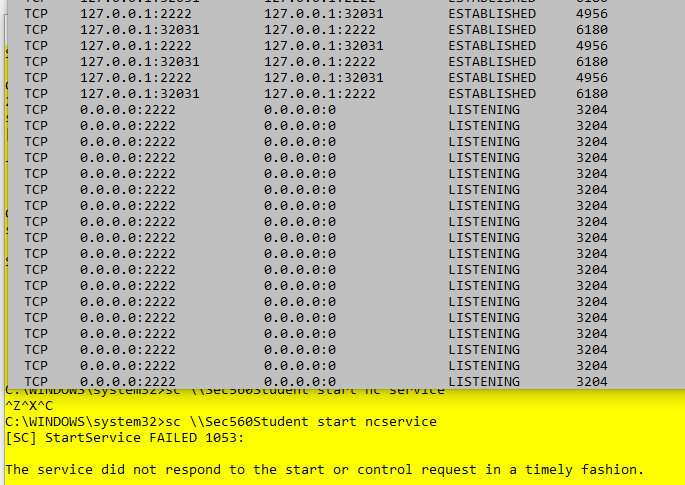
Dùng lệnh sc để tạo serivce Netcat là ncservice



Thiết lập giám sát dịch vụ trên máy nạn nhân, thực hiện bằng việc giám sát cổng TCP 2222 để xác định khi nó bắt đầu nghe (listening). Chạy lệnh netstat như sau:



Sau đó trên máy tấn công bắt đầu khởi chạy dịch vụ ncservice:



Trên máy mục tiêu sẽ hiện ra kết quả cổng 2222 TCP đang lắng nghe.

Bạn có thể thấy có vẻ như cổng của bạn vẫn mở và lắng nghe ngay cả sau khi Windows tắt dịch vụ. Đó là một trình nghe cổng ảo. ID tiến trình được chỉ ra bởi đầu ra của netstat có thể không còn chạy trên Windows, vì vậy không ai có thể kết nối với cổng đó, mặc dù đầu ra của netstat vẫn hiển thị LISTENING . Sau vài giây, Windows nhận ra điều này và giải phóng cổng.

Xóa ncservice sử dụng lệnh dưới đây:

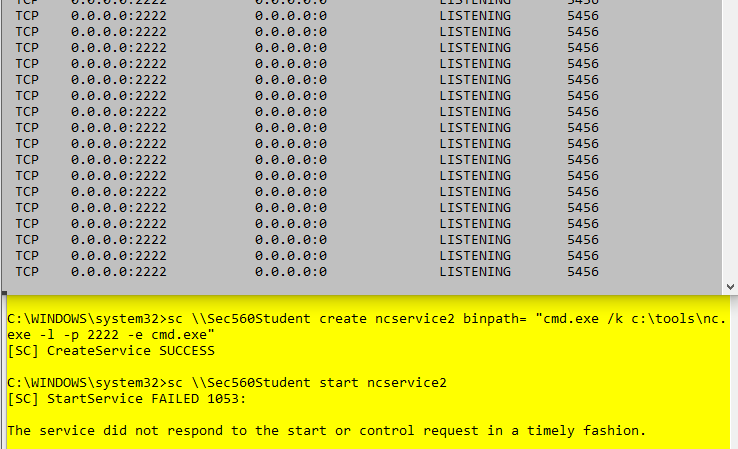


# 3. Tạo service tốt hơn

Tiếp tục chạy netstat để giám sát việc lắng nghe kết nối trên máy mục tiêu

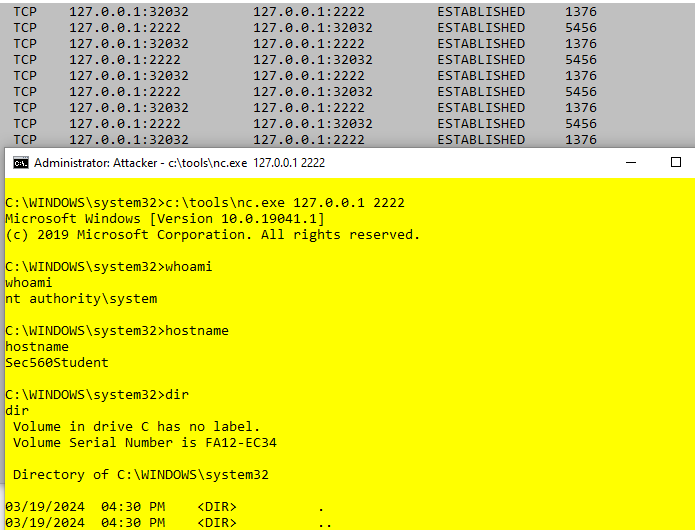
Trên máy tấn công, thực hiện tạo dịch vụ netcat với tên ncservice2 tương tự như trên nhưng thêm vào option /k trong binpath, option này sẽ giữ cửa sổ cmd sau khi thực hiện xong lệnh được chỉ định.

Sau đó khởi chạy dịch vụ với sc.



Trên máy tấn công, thực hiện kết nối tới cổng đang lắng nghe bằng Netcat client, dịch vụ ncservice2 đã được khởi chạy, nó sẽ tạo ra một quá trình Netcat chạy trong nền với quyền hạn local SYSTEM. Khi có kết nối tới cổng TCP 2222 (cổng mà Netcat đang lắng nghe) từ máy attacker, Netcat sẽ kích hoạt một command shell trên máy tính mục tiêu, cho phép attacker có quyền truy cập và tương tác với máy tính đó thông qua command shell này.

Sau khi nhận được cmd, thực hiện 1 số lệnh như whoami, hostname, dir để tương tác với máy mục tiêu.



**NOTE:** Khi ấn CTRL-C trong Netcat client (trên máy vàng), nó sẽ ngắt kết nối đồng thời Netcat listener cũng dừng theo, vì option -l: tùy chọn tạo 1 trình nghe 1 kết nối, dừng chạy khi kết nối đó biến mất. Nếu là option -L: tạo ra trình nghe liên tục giữa các kết nối.

-l(listen mode):

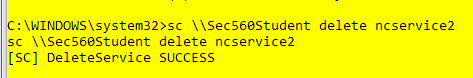
Khi sử dụng nc -l, Netcat sẽ hoạt động ở chế độ "listen", tức là nó sẽ lắng nghe và chấp nhận các kết nối đến từ các máy tính khác trên mạng.

Thường được sử dụng để tạo ra một lỗ hổng nghe trên một cổng cụ thể để kết nối từ xa đến và tạo một kênh truyền thông hai chiều giữa hai máy tính.

-L (Listen harder):

Tùy chọn này tạo ra một server lắng nghe có khả năng ghi nhận và chấp nhận nhiều kết nối liên tiếp. Nó tương tự như tùy chọn -l, nhưng nó sẽ tiếp tục lắng nghe sau khi kết nối hiện tại kết thúc, cho phép kết nối tiếp theo.

Thực hiện xóa ncservice2:

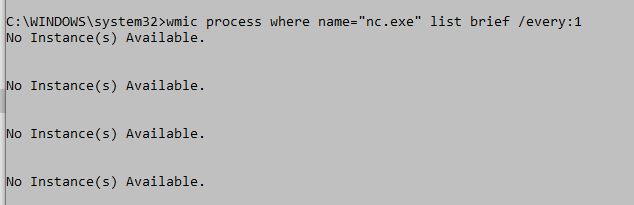


# 4. WMIC

WMIC khác với sc ở chỗ không cần khởi tạo dịch vụ rồi xóa sau đó, điều này giúp wmic để lại ít dấu vết hơn.

Quá trình ta tiến hành sẽ không có quyền local System, thay vào đó, ta sẽ chạy với quyền administrator.

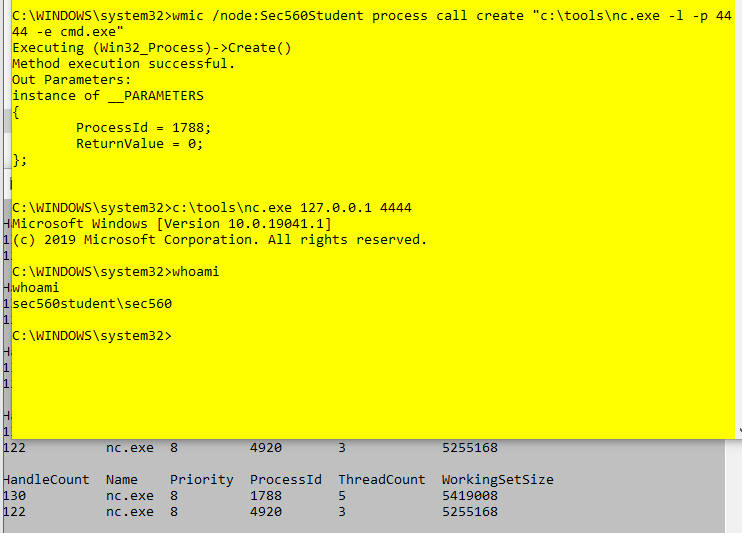
Bắt đầu bằng việc khởi tạo trình giám sát với tiến trình bắt đầu bằng nc.exe như sau:



/every:1 chỉ định tần suất thực thi lệnh, trong trường hợp này là mỗi giây (1 đại diện cho mỗi giây). Điều này có nghĩa là lệnh được chỉ định sẽ được thực thi một lần sau mỗi giây, liên tục và lặp lại cho đến khi quy trình được dừng lại hoặc kết thúc.

Tiếp theo, sử dụng wmic để gọi trình nghe Netcat trên máy đích, sau đó thực hiện kết nối tới trình nghe Netcat.

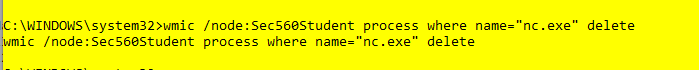
"c:\tools\nc.exe -l -p 4444 -e cmd.exe": Đây là đường dẫn của chương trình mà chúng ta muốn thực thi. Trong trường hợp này, sử dụng Netcat (nc.exe) để tạo một lỗ hổng nghe trên cổng TCP 4444 và kích hoạt một command shell khi có kết nối được thiết lập tới lỗ hổng này.



Khi thực hiện lệnh khởi tạo trình nghe trên máy đích từ máy tấn công, một cửa sổ trống sẽ hiện lên, cửa sổ này cung cấp một giao diện để xem và tương tác trực tiếp với Netcat.

Sử dụng option -d nếu không muốn hiển thị console này, -d nghĩa là chạy dưới nền.

Thực hiện hủy toàn bộ tiến trình Nc còn lại với câu lệnh:



Tổng kết: sử dụng sc để tạo và chạy một dịch vụ (từ đó mô phỏng psexec nhưng chỉ sử dụng các công cụ tích hợp sẵn) và chạy wmic để khiến mục tiêu bắt đầu một quy trình, đặc biệt hữu ích cho những người kiểm tra thâm nhập vì ứng dụng của họ được tích hợp sẵn trong các tính năng của Windows.