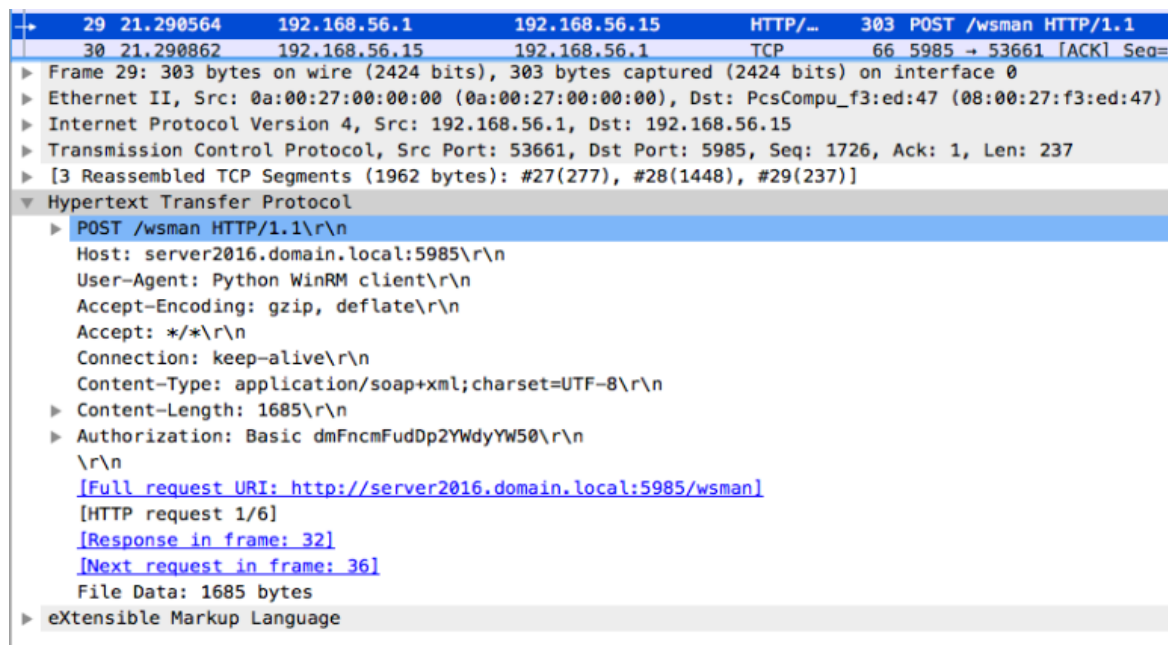


# Windows Remote Management

## Giới thiệu

- WinRM là tên của 1 **service** trên Windows và giao thức cho phép người dùng tương tác với remote system khác qua giao thức WS-Management. Sysadmin có thể sử dụng WinRM để kiểm tra hệ thống, quản lý hệ thống từ xa
- Kết nối WinRM qua HTTP được thực hiện qua port **5985**/TCP, qua HTTPS thì được thực hiện qua port **5986**/TCP
- WinRM hỗ trợ các kiểu xác thực sau
  - Basic: username và password sẽ được encode Base64, ví dụ ảnh chụp request sau:



The image shows a Wireshark packet capture of an HTTP POST request to the WinRM service. The packet is captured on interface 0, source IP 192.168.56.1, destination IP 192.168.56.15, port 5985. The request is a POST to /wsman HTTP/1.1. The request body is an XML document containing a Basic authentication header. The decoded Basic authentication string is 'username:password'.

```
29 21.290564 192.168.56.1 192.168.56.15 HTTP/1.1 303 POST /wsman HTTP/1.1
30 21.290862 192.168.56.15 192.168.56.1 TCP 66 5985 → 53661 [ACK] Seq=
▶ Frame 29: 303 bytes on wire (2424 bits), 303 bytes captured (2424 bits) on interface 0
▶ Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PcsCompu_f3:ed:47 (08:00:27:f3:ed:47)
▶ Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.15
▶ Transmission Control Protocol, Src Port: 53661, Dst Port: 5985, Seq: 1726, Ack: 1, Len: 237
▶ [3 Reassembled TCP Segments (1962 bytes): #27(277), #28(1448), #29(237)]
▼ Hypertext Transfer Protocol
▶ POST /wsman HTTP/1.1\r\n
Host: server2016.domain.local:5985\r\n
User-Agent: Python WinRM client\r\n
Accept-Encoding: gzip, deflate\r\n
Accept: */*\r\n
Connection: keep-alive\r\n
Content-Type: application/soap+xml;charset=UTF-8\r\n
▶ Content-Length: 1685\r\n
▶ Authorization: Basic dmFncmFudDp2YWdyYW50\r\n
\r\n
[Full request URI: http://server2016.domain.local:5985/wsman]
[HTTP request 1/6]
[Response in frame: 32]
[Next request in frame: 36]
File Data: 1685 bytes
▶ eXtensible Markup Language
```

- Khi decode chuỗi **dXNlcm5hbWU6cGFzc3dvcmQ=** thì được kết quả là **username:password**
- Digest: truyền hash của username và password trên mạng
- Kerberos

- WinRS là thành phần client, tức là nó chạy trên máy từ xa và được sử dụng nó để quản lý WinRM server.
- Tương tự như PSEXec, WinRS cũng cho phép khởi chạy một tiến trình từ xa, tuy nhiên WinRS khác ở chỗ:
  1. Nó là công cụ có sẵn trên Windows (từ Win 7) còn PsExec phải được tải từ bộ SysInternals
    - Tuy nhiên thiết bị đích phải được setup bằng `winrm quickconfig` mới chấp nhận kết nối
  2. WinRS có khả năng vượt qua tường lửa dễ hơn bởi nó sử dụng HTTP và HTTPS để truyền tải dữ liệu so với PsExec sử dụng SMB, do một số cổng SMB có thể bị chặn
- Chính vì những điểm trên mà attacker có thể lợi dụng WinRM để thực hiện lateral movement sau khi đã compromise 1 máy (giai đoạn Action on Objectives trong Cyber Kill Chain)

## Các cách attacker sử dụng WinRM

1. Qua `winrm.vbs` (file script có sẵn ở C:\Windows\System32 cho phép sysadmin cấu hình WinRM và quản lý tài nguyên)

- Ví dụ:

Process `c:\windows\system32\cscript.exe`

Command Line

```
cscript //nologo "C:\Windows\System32\winrm.vbs" invoke create wmicimv2/win32_process @{CommandLine="notepad.exe"} -r:https://10.10.10.10:443 -a:Certificate -c:10.10.10.10
```

1 netconns 0 childprocs 0 filemods 1 regmods 85 modloads 3 crossprocs

Spawned by `c:\windows\system32\cmd.exe`

Binary `C:\Windows\System32\winrm.vbs` Related AV VT

Seen on 3 of recent endpoints

Info `002c2dc41d60de55a9dc3dd4482e4d21`

Signed as `Microsoft Corporation`

at 2016-07-16 09:52:00 +00:00 (4 days before first seen)

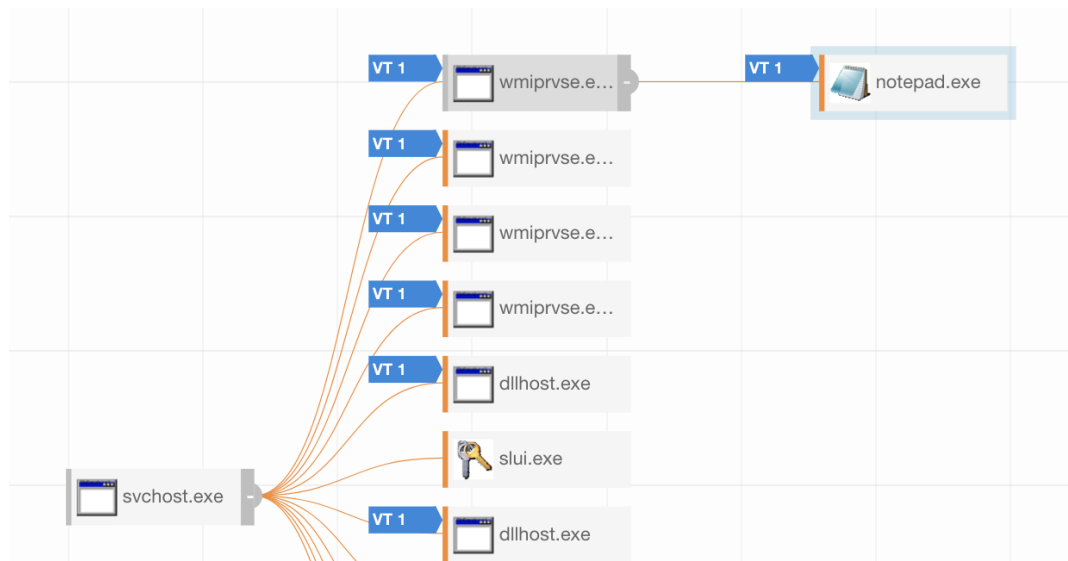
Reputation: `None`

- (1) WinRM -r flag: lệnh WinRM Invoke được thực thi ở host nằm ở địa chỉ HTTPS
- (2) -a và (3) -c: chỉ ra attacker xác thực vào remote host dùng cert được nhập trong câu lệnh

- Đây có thể là một hành vi đáng ngờ bởi có nhiều cách đơn giản hơn để chạy Notepad như click đúp hoặc qua Command Shell hoặc PowerShell
- Phân tích:
  - Kiểm tra `cscript` xem sinh ra các tiến trình con nào thì thấy tiến trình này không sinh ra các tiến trình con nào



- Tìm tiến trình cha của tiến trình được tạo ra `notepad.exe` thì thấy nó được sinh ra bởi `winprvse.exe`, là file thực thi cho phép thao tác với WMI interface trên Windows



- Câu lệnh WinRM trên thực chất là sử dụng class `Win32_Process` của WMI, submit câu lệnh cần chạy tới WMI. WMI sẽ thực thi câu lệnh đã nhập qua interface của nó.

- Lí do thấy `svchost.exe` là cha của `wmiprvse.exe` là bởi WinRM là một service, và nếu có kết nối tới bên ngoài, `svchost` chứ không phải `wmiprvse` là tiến trình thay mặt thực hiện kết nối

## 2. `winrs.exe`

## 3. PowerShell PSRemoting

## 4. Công cụ bên thứ 3: VD như Evil-WinRM, Metasploit, CrackMapExec

Cụ thể cách 2, 3 và 4 sẽ được trình bày ở phần thực hành lab

# Lab

- Kịch bản
  - Đã compromised được một máy trong domain `phuongbm6.lab` với IP `192.168.186.200`
  - Để đơn giản, giả sử đã có username và password của máy DC (thực tế thì có thể dump NTLM hash để thực hiện pass the hash), mục đích là thực hiện remote sang máy DC có IP `192.168.186.130`

## winrs.exe

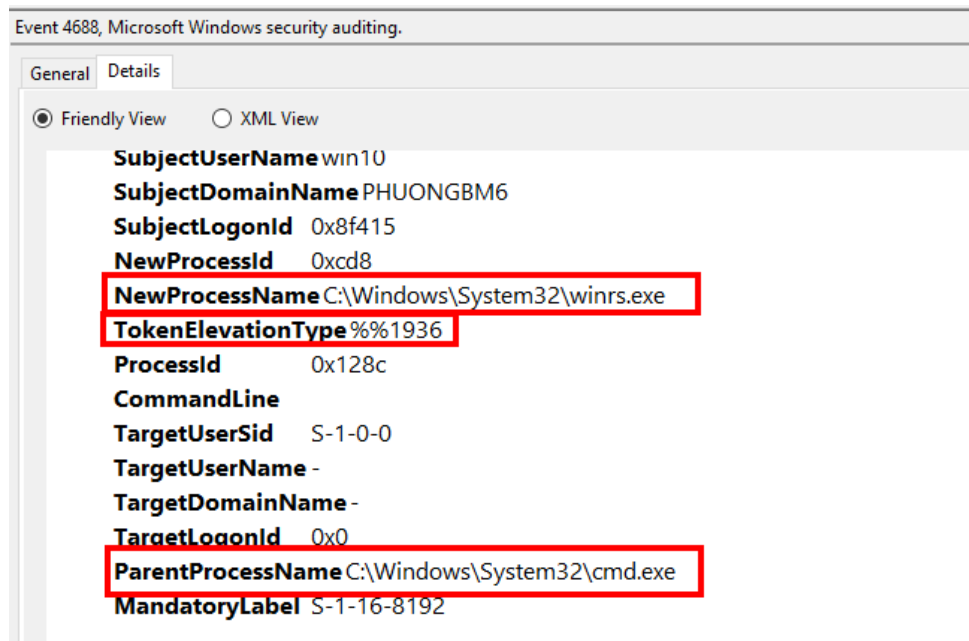
- Source machine: chạy lệnh `winrs -r:192.168.186.130 -u:Administrator CMD`

```
C:\Users\win10>winrs -r:192.168.186.130 -u:Administrator CMD
Enter the password for 'Administrator' to connect to '192.168.186.130':
Microsoft Windows [Version 10.0.20348.2762]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>
```

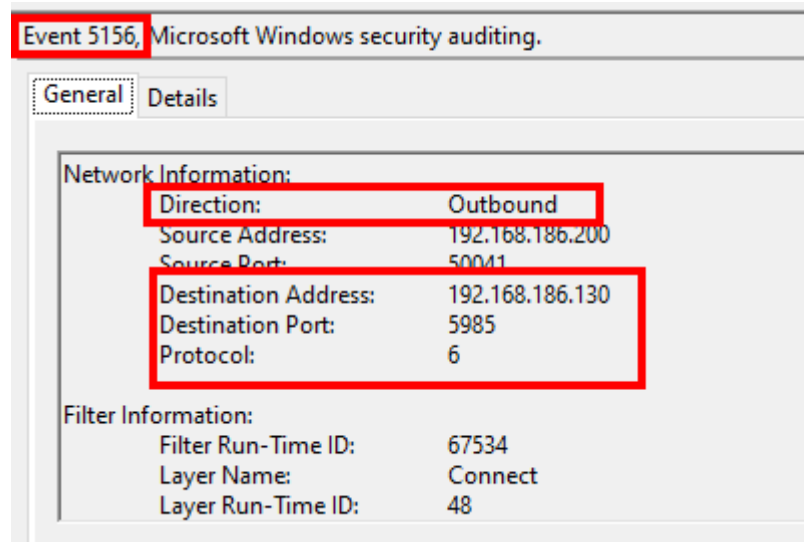
- Detect

- Trên máy source
  - Log 4688 - có tiến trình mới được tạo: Chú ý các trường
    - NewProcessName là winrs.exe
    - Tên người dùng thực hiện SubjectUserName

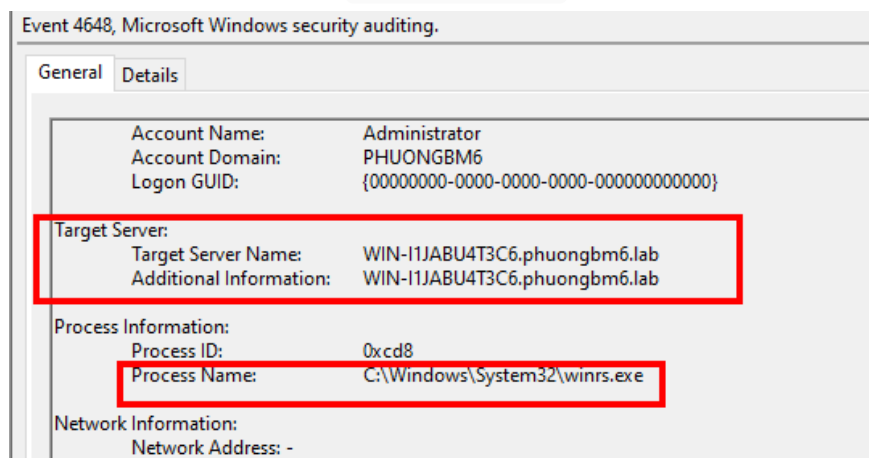


- Log 5156 - Windows Filtering Platform cho phép kết nối: Chú ý trường
  - Direction là Outbound (từ máy source kết nối sang máy đích)
  - Destination Address: IP được kết nối tới
  - Destination Port: 5985 (HTTP) hoặc 5986 (HTTPS)

- Protocol: 6 (TCP)

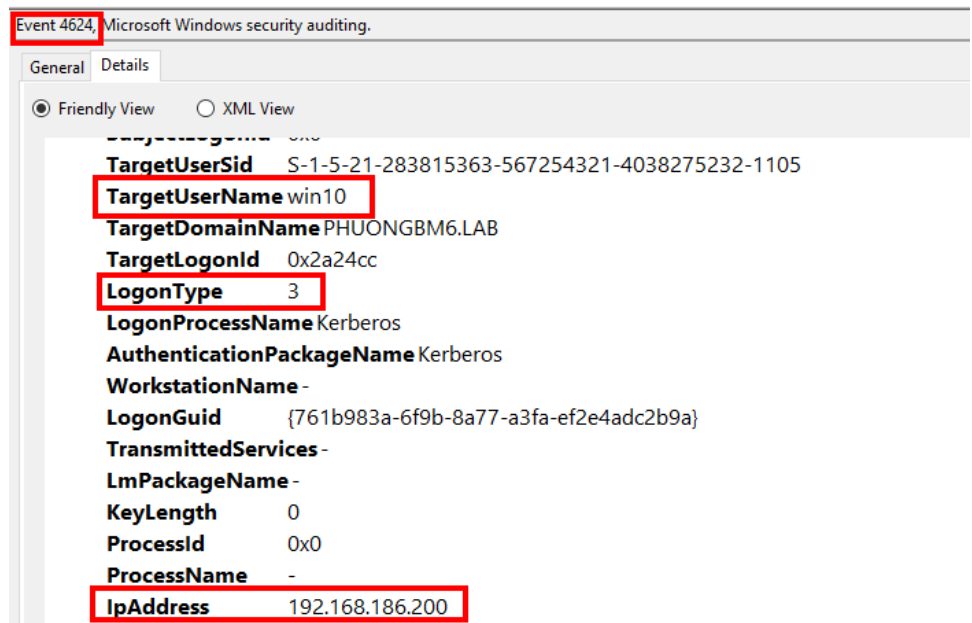


- Log 4648 - A logon was attempted using explicit credentials: Chú ý các trường
  - Target Server: tên máy mà có tiến trình thực hiện đăng nhập
  - Process Name là `winrs.exe`

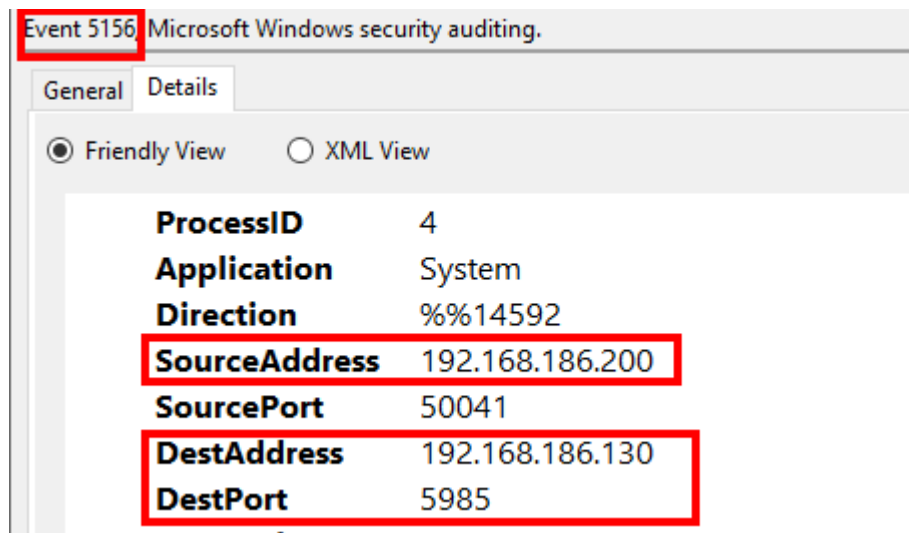


- Trên máy destination
  - Log 4624: Chú ý trường
    - TargetUserName
    - LogonType là 3

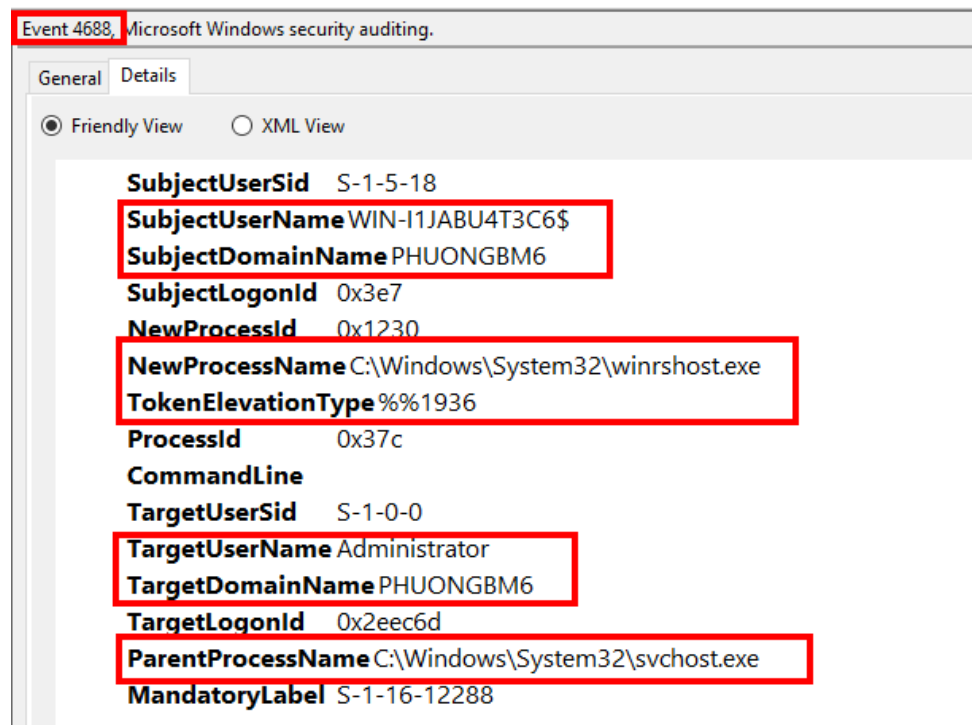
- IP máy được đăng nhập



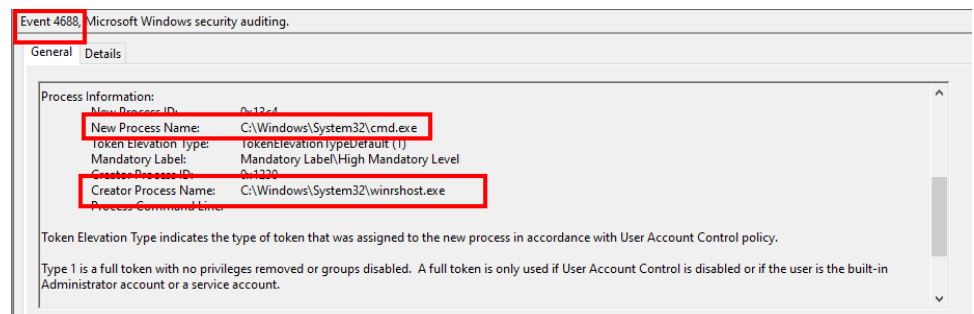
- Log 5156: tương tự trên nhưng Direction là Inbound



- Log 4688: đặc biệt chú ý tới tên tiến trình được tạo là `winrshost` và tiến trình cha của nó là `svchost`, cũng như tiến trình con của `winrshost` là gì



Nếu thấy trường hợp này cần nghi ngờ bởi `cmd.exe` được sinh ra bởi một tiến trình quản lý từ xa



## PowerShell PSRemoting

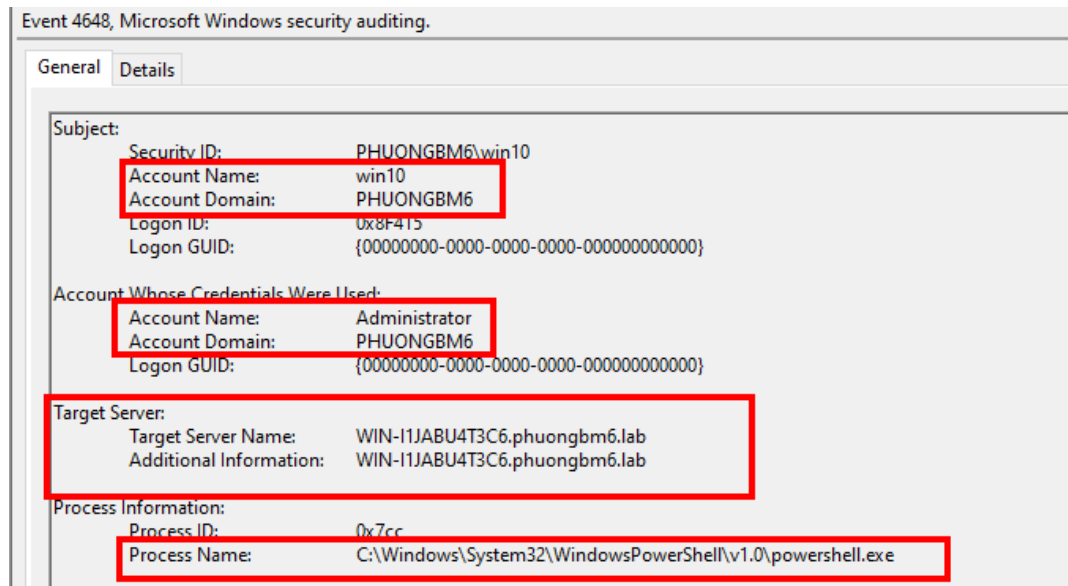
- Một cách khác là dùng PSSRemoting, vốn được bật mặc định từ Win Server 2012

```
PS C:\Users\win10> Enter-PSSession -ComputerName 192.168.186.130 -Credential Administrator
[192.168.186.130]: PS C:\Users\Administrator\Documents> whoami
phuongbm6\administrator
```

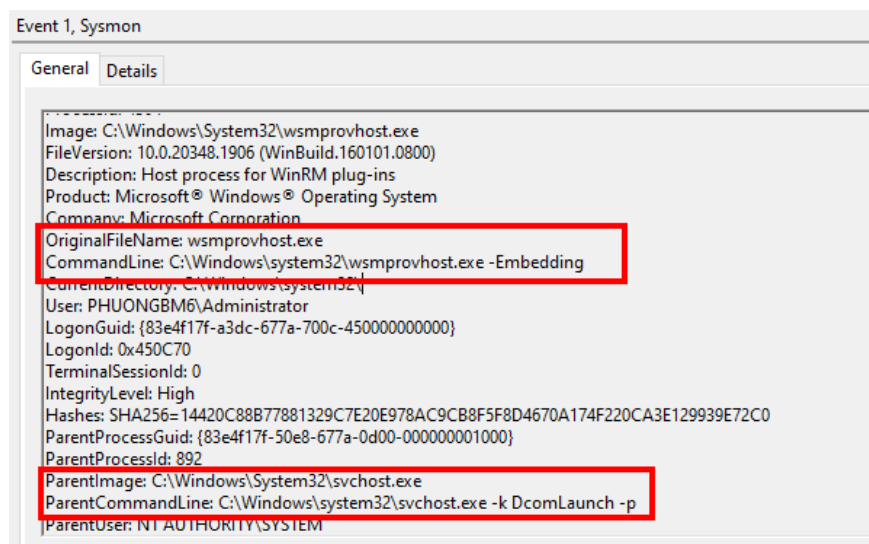
- Detect:
  - Source
  - Log 5156 tương tự trên



- Log 4648: thực hiện đăng nhập dùng username và password tương minh nên cần chú ý tới tiến trình thực hiện đăng nhập, ở đây là `powershell.exe`



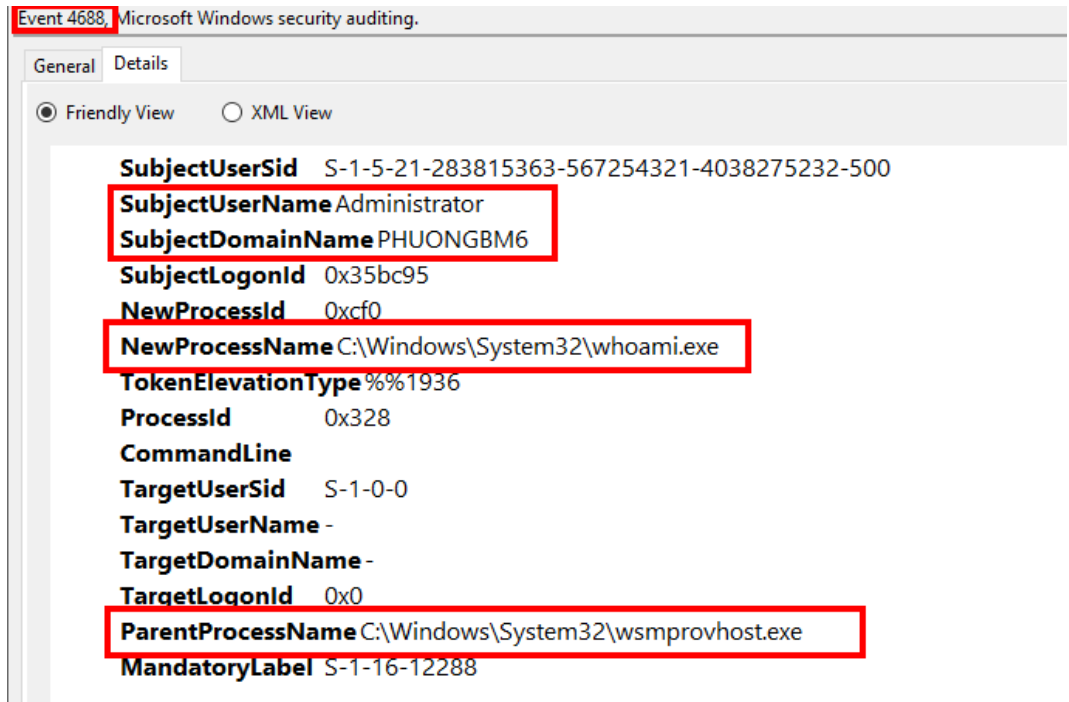
- Sysmon ID 1: chú ý tới CommandLine là `wsmprovhost.exe` và cha của nó `svchost.exe`
  - Chi tiết hơn về `wsmprovhost.exe` thì đây là tiến trình remote session của PowerShell khi chạy WinRM



- Dest
  - Log 5156, 4624 như trên

- Log 4688: chú ý các tiến trình được sinh ra từ

`wsmprovhost.exe`



- Nếu chạy native cmdlet trong `wsmprovhost.exe` thì nó sẽ không có tiến trình con của `powershell.exe` và khi cmdlet chạy xong thì tiến trình này tự kết thúc
  - Nếu lệnh PowerShell chạy 1 file nhị phân khác thì tiến trình có image path là file này sẽ là tiến trình con của `wsmprovhost.exe` và `wsmprovhost.exe` sẽ tự kết thúc khi tiến trình con exit

## Evil-WinRM

```

(kali㉿kali)-[~]
$ evil-winrm -i 192.168.186.130 -u Administrator
Enter Password:

Evil-WinRM shell v3.5

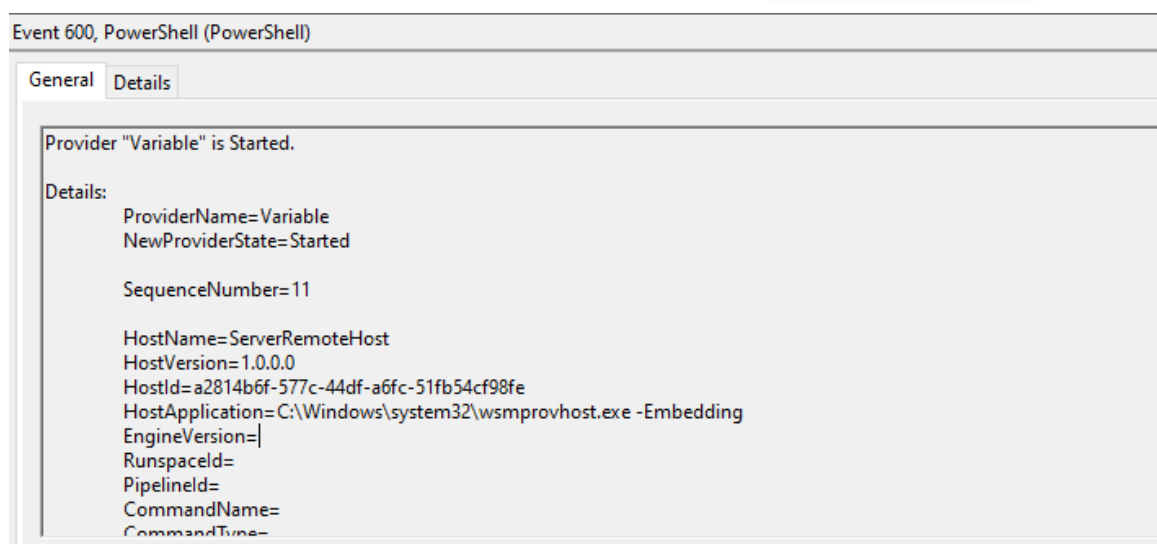
Warning: Remote path completions is disabled due to ruby limitation: quoting_
detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackp
layers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
phuongbm6\administrator

```

- Ngoài nêu rõ thông tin đăng nhập như trên thì có thể dùng option -H với NTLM hash đã dump
- Detect:
  - Log 600 PowerShell - A process was assigned a primary token: Chú ý trường HostApplication là `wsmprovhost`



- Log 4100 hoặc 4103 (log liên quan tới sự kiện PowerShell): Chú ý trường HostApplication là `wsmprovhost`, với 4103 thì

## chú ý thêm CommandName

Event 4100, PowerShell (Microsoft-Windows-PowerShell)

General

Details

Error Message = System error.

Context:

Severity = Warning  
Host Name = ServerRemoteHost  
Host Version = 1.0.0.0  
Host ID = a2018ede-189d-46c8-8a7c-627580d3aedd  
Host Application = C:\Windows\system32\wsmprovhost.exe -Embedding  
Engine Version = 5.1.20348.2760  
Runspace ID = 7eb1dd5f-084d-4fb0-8382-c5df7218f6a9  
Pipeline ID = 4  
Command Name =  
Command Type =  
Script Name =  
Command Path =  
Sequence Number = 15  
User = PHUONGBM6\Administrator  
Connected User = PHUONGBM6\Administrator  
Shell ID = Microsoft.PowerShell