Bộ môn An toàn Thông tin – Khoa MMT&TT – UIT

BÁO CÁO THỰC HÀNH HT2

Môn học: Tấn Công Mạng

Kỳ báo cáo: Buổi 03

Tên chủ đề:

GVHD: ThS Nguyễn Công Danh

Ngày báo cáo: 19/05/2025

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT205.P21.ANTT

Nhóm: Nhóm 11

STT	Họ và tên	MSSV	Email
1	Nguyễn Hoàng Duy Kha	22520597	22520597@gm.uit.edu.vn
2	Đào Duy Khang	22520607	22520607@gm.uit.edu.vn
3	Nguyễn Thành Thạo	22521371	22521371@gm.uit.edu.vn
4	Phan Nguyễn Nhật Trâm	22521501	22521501@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN

STT	Công việc	Kết quả tự đánh giá
1	Phân tích nhật ký sự kiện	100%
2	Đánh giá rủi ro bị khai thác lại sau khi bị tấn công. Đề xuất các biện pháp phòng ngừa tái khai thác	100%

MỤC LỤC

DANH MỤC HÌNH ẢNH

BÁO CÁO CHI TIẾT

I. Hạn chế trong quá trình thực hiện mô phỏng

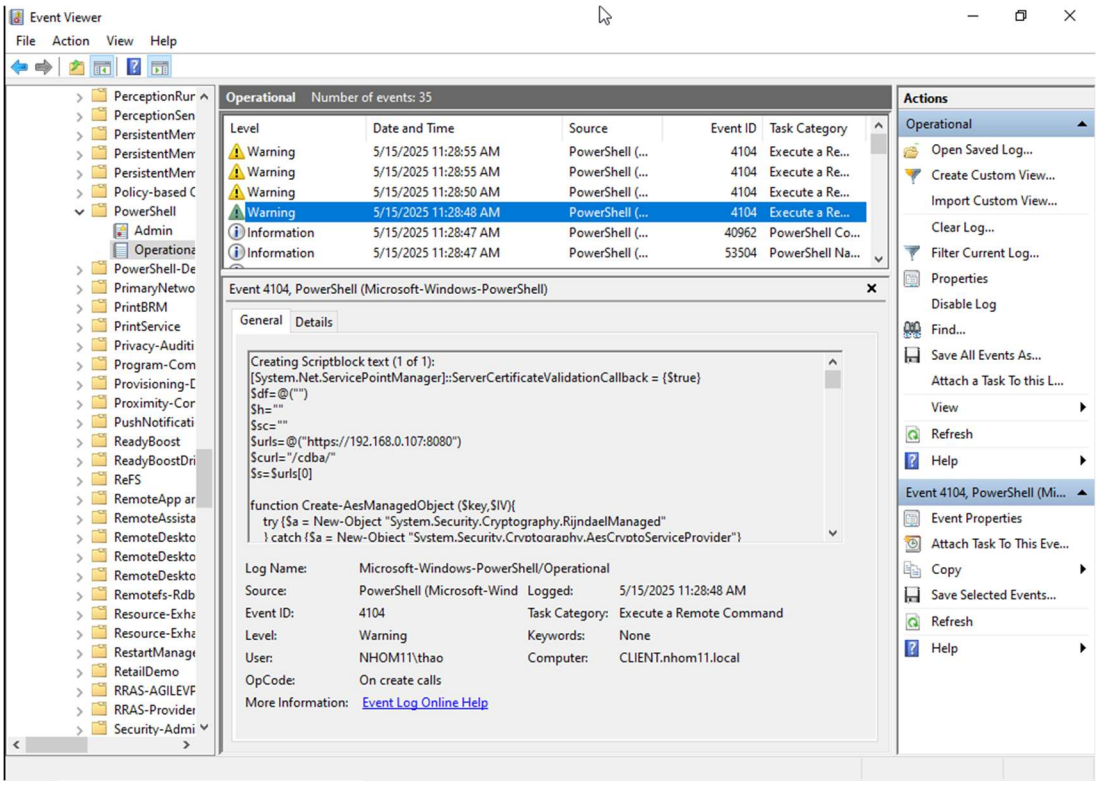
- Trong quá trình mô phỏng kịch bản tấn công post-exploitation bao gồm ba kỹ thuật: persistence, privilege escalation, và lateral movement, nhóm đã gặp một số khó khăn ảnh hưởng đến tính liên tục và độ chính xác của kết quả ghi nhận:
  - **Gián đoạn giữa các giai đoạn thực nghiệm**: Do thiếu ý tưởng và không khai thác được ở một số thời điểm, quá trình thực hiện bị ngắt quãng, dẫn đến khó đảm bảo sự liền mạch trong việc theo dõi hành vi của hệ thống.
  - **Không đồng bộ thời gian giữa các máy**: Các máy trong mô hình (máy client, và AD) không được cấu hình đồng bộ thời gian. Điều này dẫn đến sự chênh lệch đáng kể trong các timestamp của log hệ thống, gây khó khăn trong việc phân tích và đối chiếu sự kiện giữa các máy.

⇨ Thời gian log giữa các máy có sự sai lệch lớn

II. Phân tích nhật ký sự kiện

1. Kỹ thuật Persistence

- **Event ID 4104**
  - Nguồn: PowerShell
  - Thời gian: 15/5/2025 11:28:48 Sáng
  - User: NHOM11/thao
  - Máy tính: CLIENT.nhom11.local



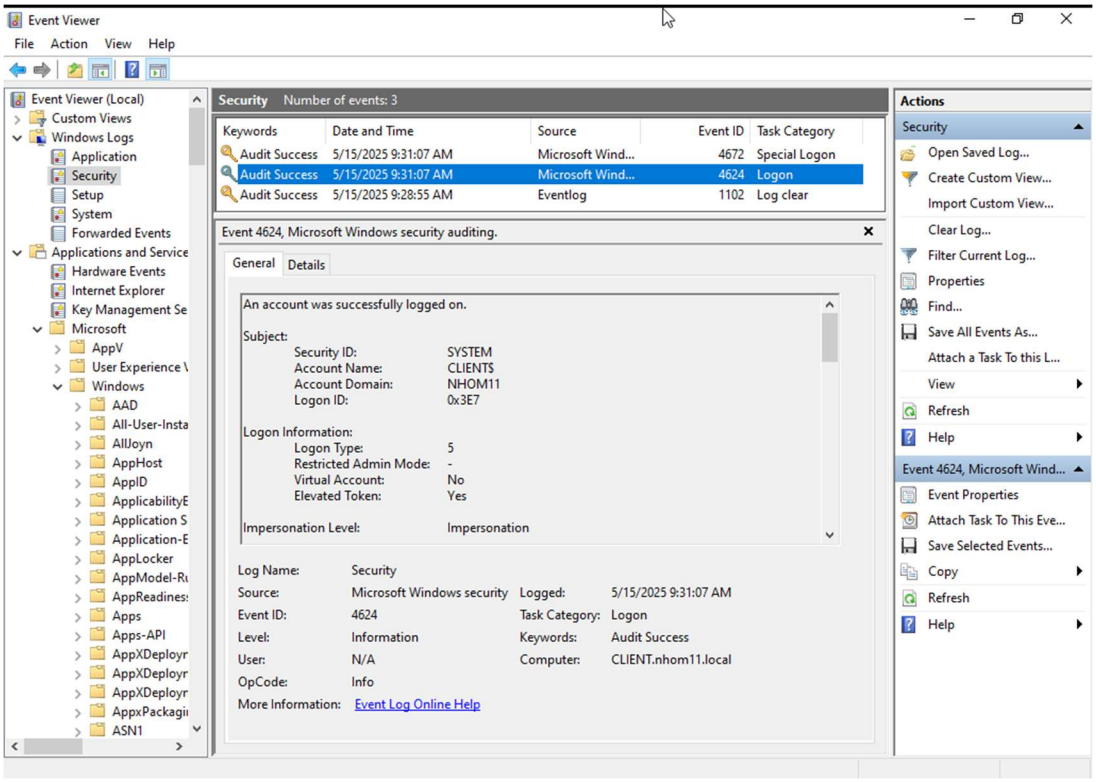
Hình 1. Persistence - Event ID 4104

- Dấu hiệu của tải mã độc từ xa thông qua đoạn script $urls=@("https://192.168.10.107:8080/") là địa chỉ IP nội bộ đang phục vụ mã độc hoặc payload từ cổng 8080. Đoạn mã đang chuẩn bị thiết lập kết nối TLS, bỏ qua kiểm tra chứng chỉ bằng cách [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true} -> Bỏ qua xác minh chứng chỉ SSL, dấu hiệu thường thấy trong kỹ thuật bypass bảo mật và truyền tải mã độc qua HTTPS.
- Hàm Create-AesManagedObject() tạo đối tượng AES từ .NET.Đây là hành vi mã hóa dữ liệu thường dùng để ẩn thông tin tải về hoặc mã hóa lưu trữ persistence payload.
- Event 4104 là kết quả của việc thực thi script qua PowerShell, hành vi tải payload từ xa và thiết lập cơ chế mã hóa là bước tiền đề của persistence.
- Mặc dù không có một Event ID nào thể hiện rõ ràng của việc thực hiện persistence, nhưng khi user đăng nhập và chưa thực hiện thêm bất kì thao tác nào khác, lại xuất hiện log ghi nhận việc mở powershell kết nối đến một địa chỉ IP lạ nên rất khả nghi

2. Kỹ thuật Privilege Escalation

- **Event ID 4624: Đăng nhập thành công**
    - Thời gian: 9:31:07 AM, 15/05/2025.
    - Tài khoản: SYSTEM (Security ID: SYSTEM, Logon ID: 0x3E7).
    - Loại đăng nhập: Logon Type 5 (Service Logon - đăng nhập dịch vụ).
    - Elevated Token: Yes - Token được cấp là token có đặc quyền cao.

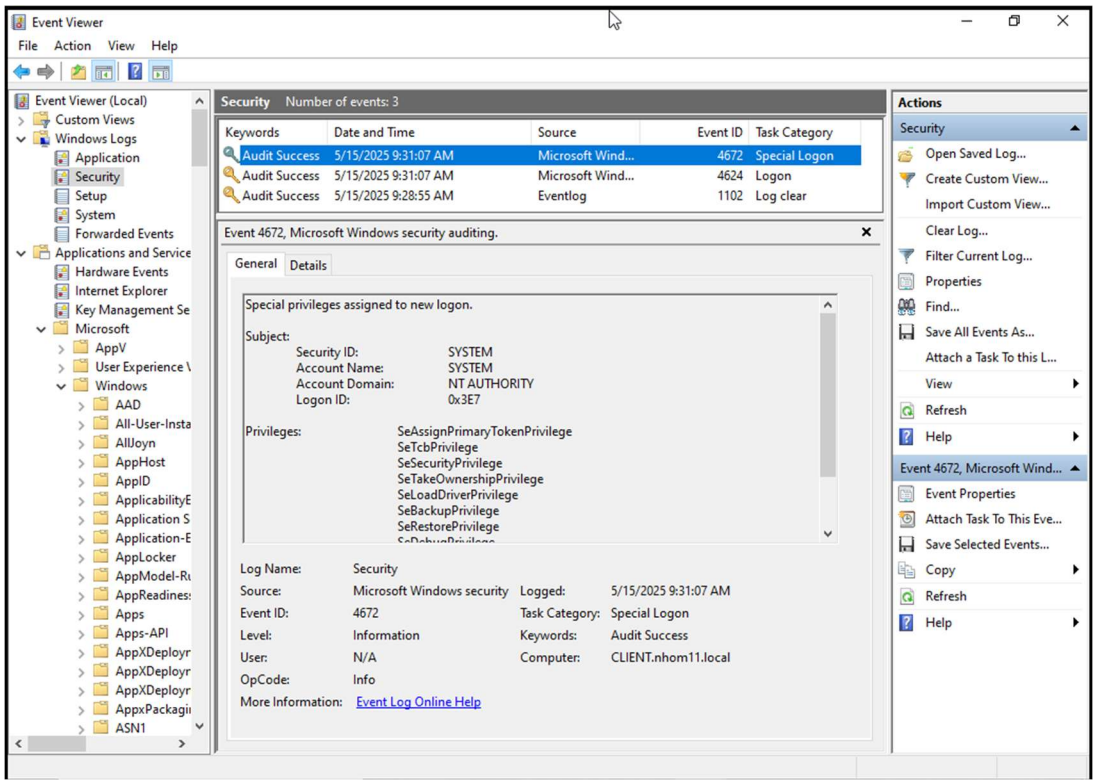
- Nhận xét:
    - Sự kiện này cho thấy một dịch vụ đã đăng nhập với tài khoản SYSTEM và token nâng cấp – tức là dịch vụ đã đạt được quyền tối đa (SYSTEM) trên hệ thống.
    - Thông thường, Service Logon được sử dụng bởi các tiến trình hệ thống hợp lệ. Tuy nhiên, trong một số trường hợp, đây có thể là dấu hiệu của hành vi Privilege Escalation, đặc biệt khi token được nâng quyền bất thường. Điều này có thể xảy ra nếu kẻ tấn công khai thác lỗ hổng của một dịch vụ đang chạy với quyền SYSTEM hoặc thực hiện kỹ thuật bypass UAC để đạt quyền quản trị.



Hình 2. Privilege Escalation - Event ID 4624

- **Event ID 4672: Gán đặc quyền đặc biệt (Special Privileges Assigned)**
    - Thời gian: 9:31:07 AM, 15/05/2025.
    - Tài khoản: SYSTEM (NT AUTHORITY, Logon ID: 0x3E7).
    - Đặc quyền được gán:
        - SeBackupPrivilege
        - SeAssignPrimaryTokenPrivilege
        - SeTcbPrivilege
        - SeSecurityPrivilege
        - SeTakeOwnershipPrivilege
        - SeLoadDriverPrivilege
        - SeRestorePrivilege
        - …

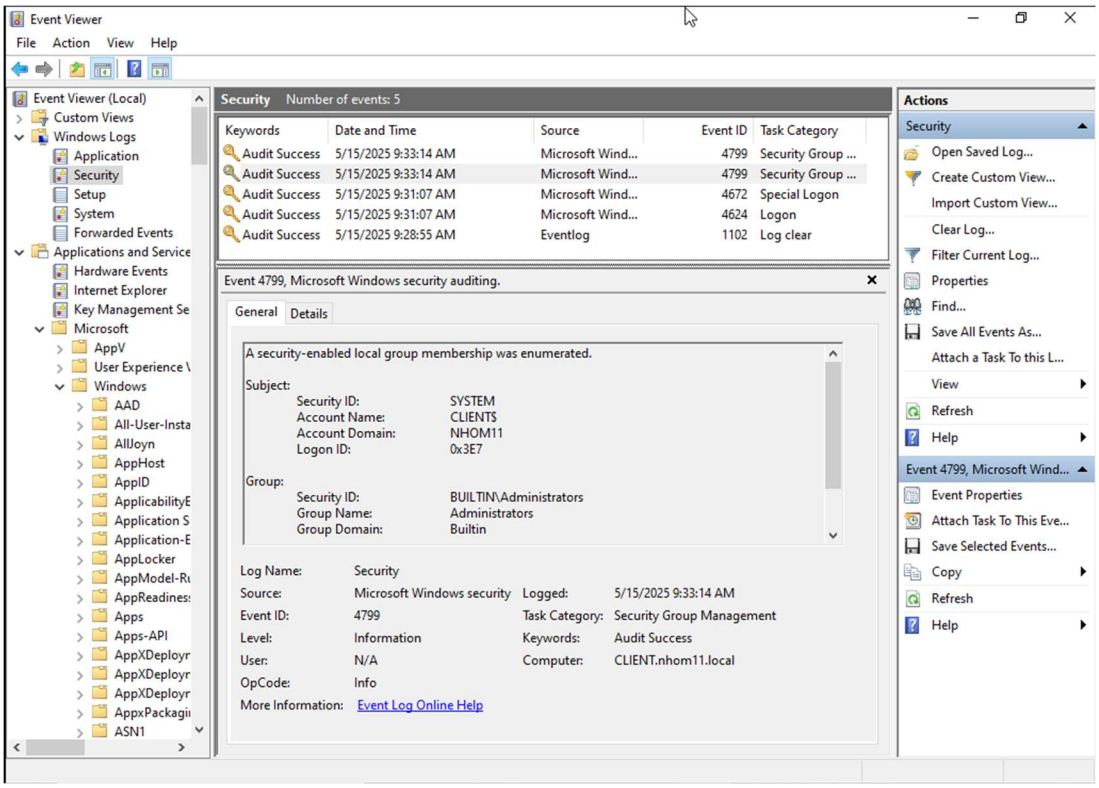
- Nhận xét:
    - Sự kiện này cho thấy tài khoản được gán nhiều đặc quyền hệ thống mạnh tại thời điểm đăng nhập. Đây là các đặc quyền nhạy cảm, có thể bị lạm dụng để leo thang đặc quyền, truy cập dữ liệu bảo mật, chiếm quyền sở hữu tệp hoặc tải driver độc hại…
    - Sự kiện này thường hợp lệ với tiến trình hệ thống, nhưng cũng có thể là chỉ báo cho việc khai thác dịch vụ hoặc chạy mã độc dưới quyền SYSTEM.



Hình 3. Privilege Escalation - Event ID 4672

- **Event ID 4799: Kiểm tra thành viên nhóm bảo mật (Security Group Management)**
    - Thời gian: 9:33:14 AM, 15/05/2025.
    - Tài khoản: CLIENT$ (máy tính, NHOM11 domain, Logon ID: 0x3E7).
    - Nhóm được kiểm tra: BUILTIN\Administrators.

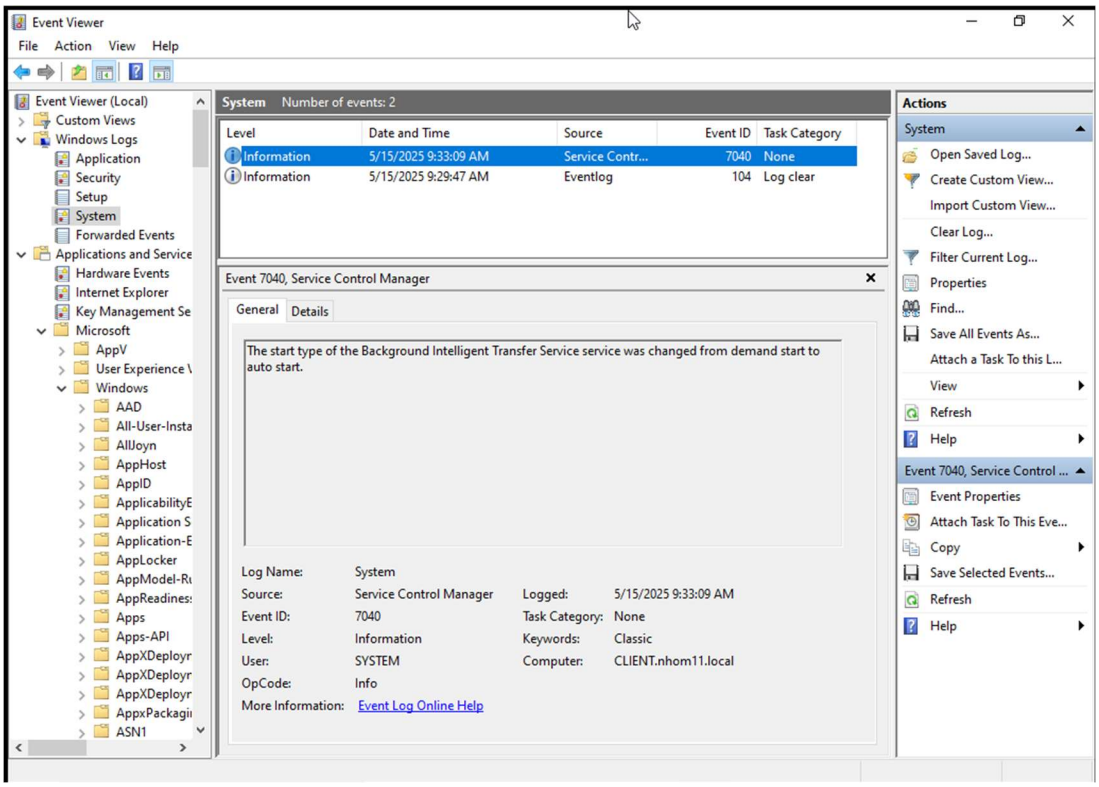
- Nhận xét:
    - Sự kiện này thể hiện việc kiểm tra thành viên của nhóm quản trị viên cục bộ, có thể là bước chuẩn bị để thêm tài khoản vào nhóm nhằm duy trì quyền truy cập lâu dài.



Hình 4. Privilege Escalation - Event ID 4799

- **Event ID 7040: Service Control Manager**
    - Thời gian: 9:33:09 AM, 15/05/2025.
    - Dịch vụ Background Intelligent Transfer Service (BITS) được thay đổi từ demand start sang auto start.
    - Tài khoản: SYSTEM.
    - Máy tính: CLIENT.nhom11.local.

- Nhận xét:
    - BITS là một dịch vụ hợp pháp của Windows, thường được sử dụng để tải xuống các bản cập nhật hoặc tệp từ internet. Tuy nhiên, việc thay đổi trạng thái khởi động của BITS sang auto start là bất thường và có thể là dấu hiệu của hành vi tấn công.
    - Kẻ tấn công có thể đã sửa đổi cấu hình BITS để đảm bảo dịch vụ chạy liên tục.

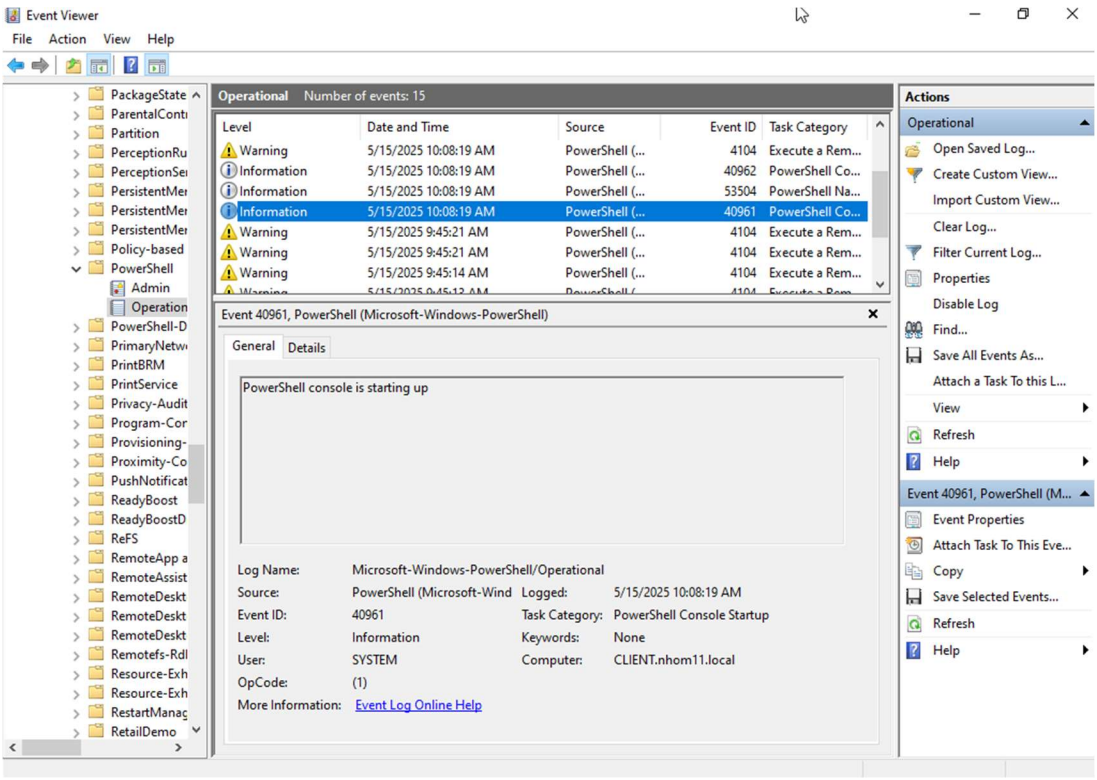


Hình 5. Privilege Escalation - Event ID 7040

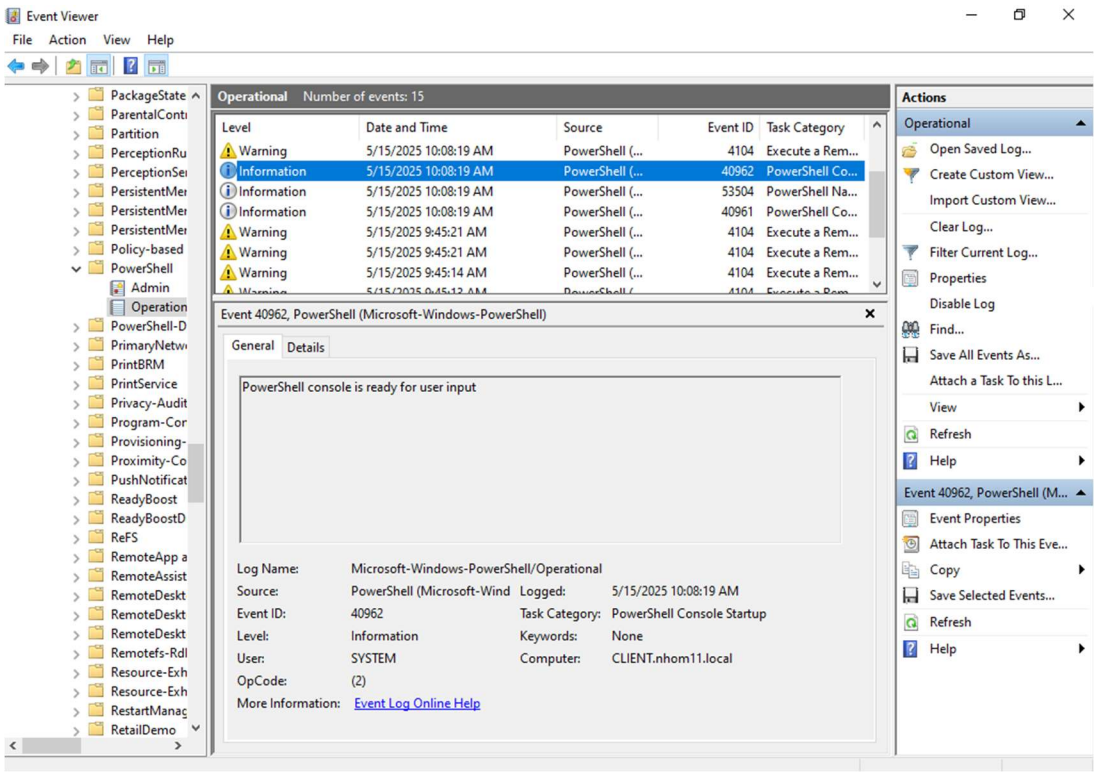
- **Event ID 40961 & 40962 & 53504: PowerShell Console Startup và Named Pipe IPC**
    - Thời gian: 10:08:19 AM, 15/05/2025.
    - Event 40961: PowerShell console khởi động.
    - Event 40962: PowerShell console sẵn sàng nhận đầu vào người dùng.
    - Event 53504: PowerShell khởi tạo một luồng IPC (Inter-Process Communication) trên tiến trình với PID 2844 trong DefaultAppDomain.
    - Tài khoản: SYSTEM.
    - Máy tính: CLIENT.nhom11.local.

- Nhận xét:
    - Các sự kiện này cho thấy một phiên PowerShell được khởi động dưới tài khoản SYSTEM, điều này là bất thường vì PowerShell thường được sử dụng bởi người dùng hoặc quản trị viên, không phải tài khoản SYSTEM.
    - Việc PowerShell chạy dưới SYSTEM có thể là kết quả của:
        - Khai thác dịch vụ: Một dịch vụ bị xâm nhập (như BITS) đã kích hoạt PowerShell.

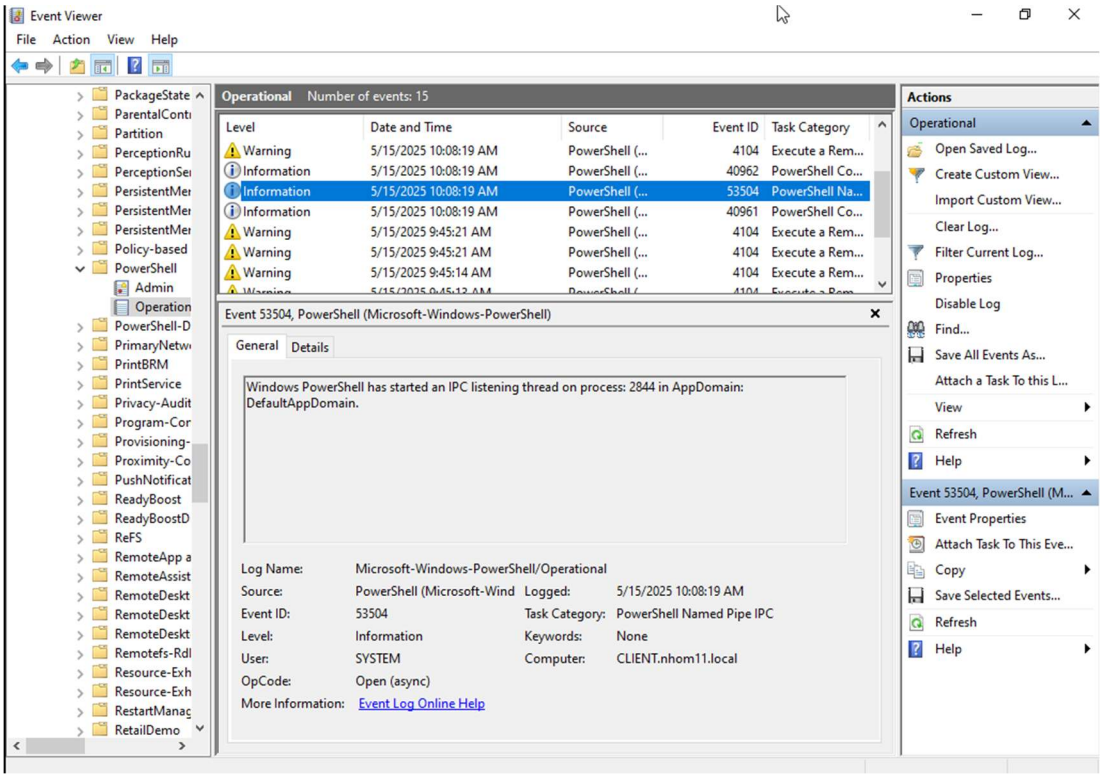
- Privilege Escalation: Kẻ tấn công đã đạt được đặc quyền SYSTEM và sử dụng PowerShell để thực thi mã độc.
  - PID 2844 cần được điều tra để xác định tiến trình cụ thể khởi tạo PowerShell



Hình 6. Privilege Escalation - Event ID 40961



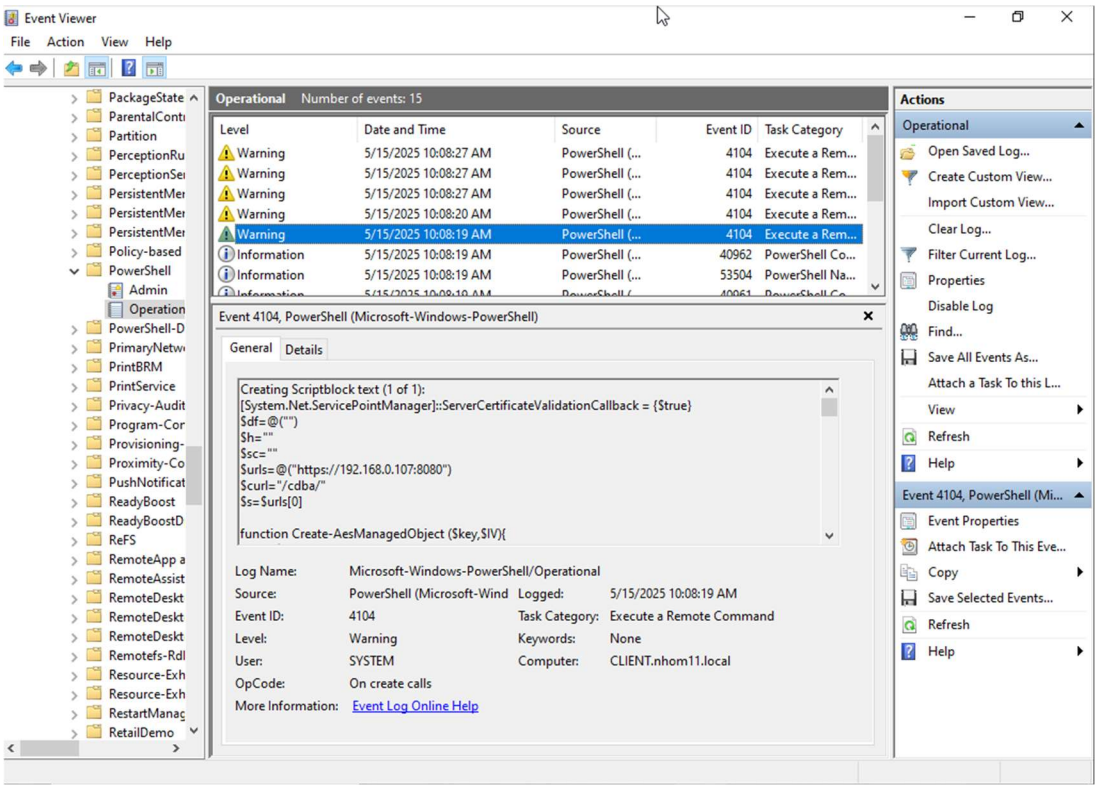
Hình 7. Privilege Escalation - Event ID 40962



Hình 8. Privilege Escalation - Event ID 53504

- **Event ID 4104: Execute a Remote Command**
    - Thời gian: 10:08:19 AM - 10:08:27 AM, 15/05/2025.
    - Scriptblock được thực thi chứa mã liên quan đến:
    - Vô hiệu hóa kiểm tra chứng chỉ SSL: [System.Net.ServicePointManager]::ServerCertificateValidationCallback = ($true).
    - Kết nối đến một URL: https://192.168.0.107:8080/cdba/.
    - Hàm Create-AesManagedObject, có thể liên quan đến mã hóa/giải mã dữ liệu.
    - Tài khoản: SYSTEM.
    - Máy tính: CLIENT.nhom11.local.

- Nhận xét:
    - Mã PowerShell này cho thấy một hành vi độc hại rõ ràng:
        - Vô hiệu hóa kiểm tra chứng chỉ SSL: Cho phép kết nối đến một máy chủ không tin cậy, thường được sử dụng để tải xuống mã độc hoặc giao tiếp với C2.
        - Kết nối đến URL lạ: Địa chỉ 192.168.0.107:8080 không phải là địa chỉ hợp pháp của Microsoft hoặc dịch vụ đáng tin cậy, có thể là máy chủ C2 của kẻ tấn công.
        - Mã hóa AES: Hàm Create-AesManagedObject có thể được sử dụng để mã hóa dữ liệu liên lạc với C2, che giấu nội dung truyền tải.
        - Các sự kiện này xảy ra khoảng 35 phút sau các sự kiện trước (9:33 AM), cho thấy đây là giai đoạn tiếp theo của cuộc tấn công, có thể là lateral movement hoặc payload execution sau khi đã leo thang đặc quyền.



Hình 9. Privilege Escalation - Event ID 4104

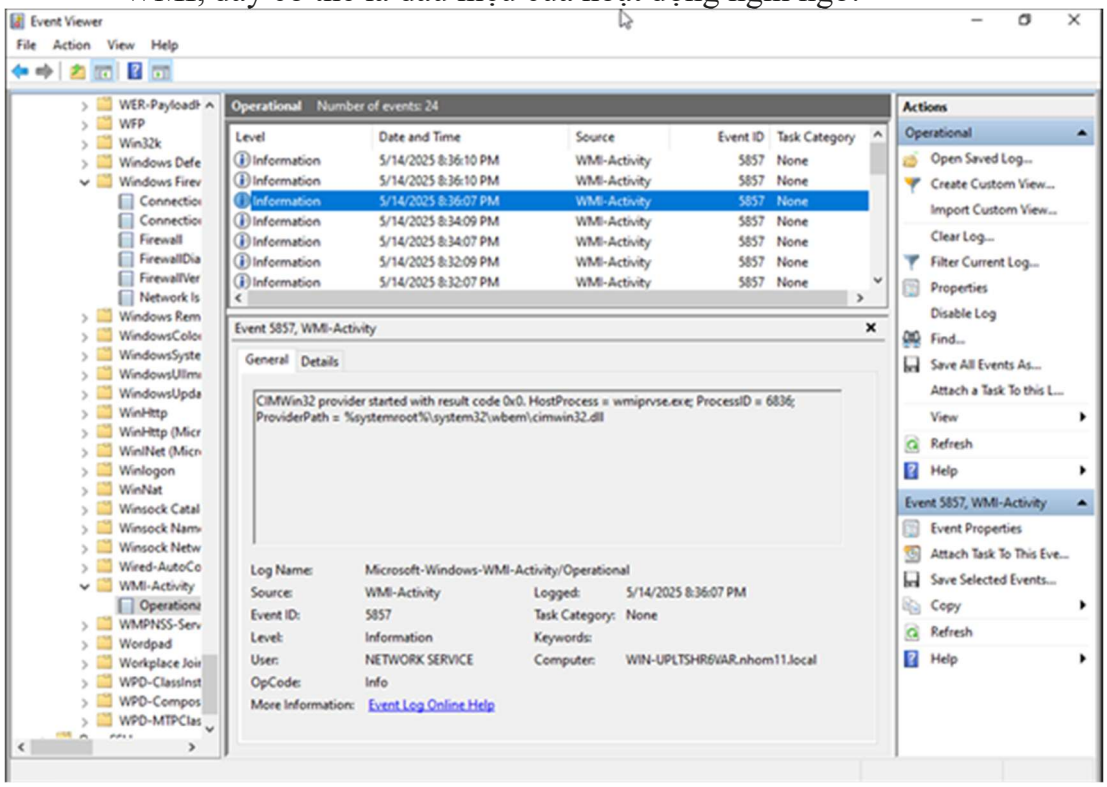
- Tài liệu tham khảo:
  - 4624(S) An account was successfully logged on. - Windows 10 | Microsoft Learn
  - 4672(S) Special privileges assigned to new logon. - Windows 10 | Microsoft Learn
  - 4799(S) A security-enabled local group membership was enumerated. - Windows 10 | Microsoft Learn
  - https://kb.eventtracker.com/evtpass/evtpages/EventId_7040_ServiceControlManager_50628.asp
  - EventTracker KB --Event Id: 40961 Source: LSASRV
  - https://kb.eventtracker.com/evtpass/evtpages/EventId_40961_LSASRV_45904.asp

3. Kỹ thuật Lateral Movement

- **Event ID 5857**
  - Nguồn: WMI-Activity
  - Tên Log: Microsoft-Windows-WMI-Activity/Operational
  - Event ID: 5857
  - Thời gian: 14/5/2025 lúc 8:36:07 Tối
  - Mô tả: "CIMWin32 provider started with result code: 0x0."

- Process ID: 6836 (liên quan đến tiến trình wmiprvse.exe).

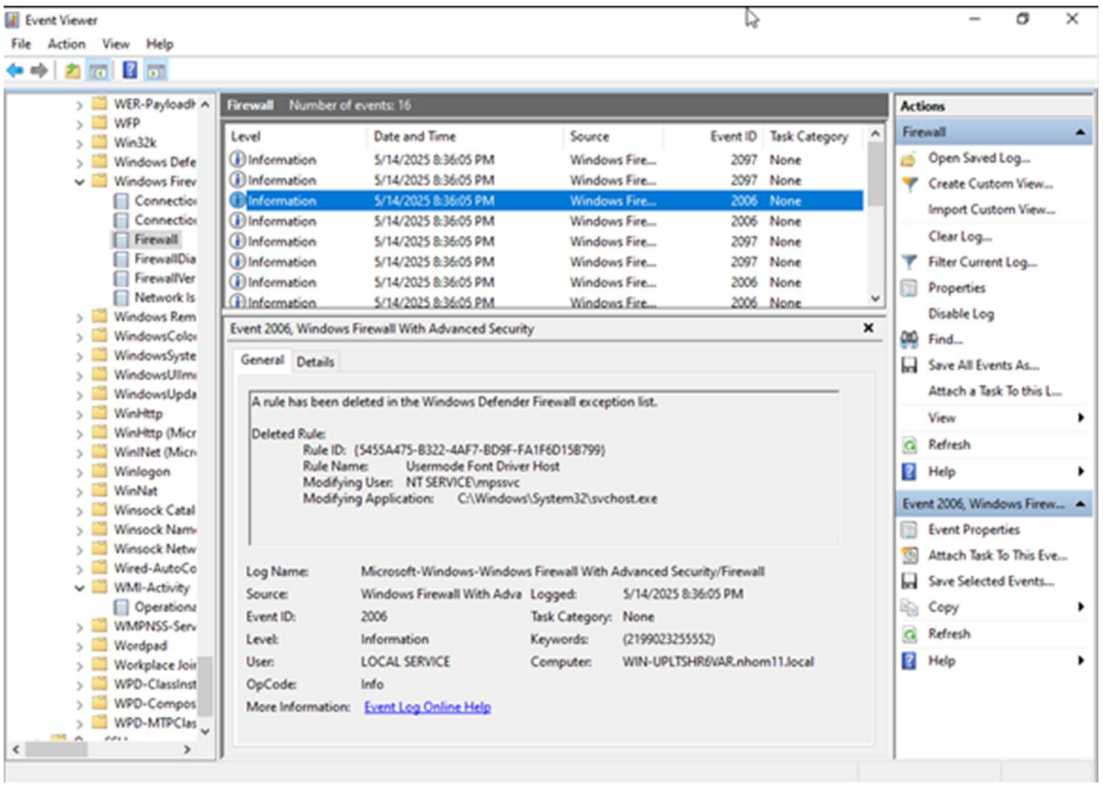
- Nhận xét:
  - Sự kiện này cho thấy nhà cung cấp WMI được khởi chạy thành công. Liên quan đến việc giám sát hệ thống hoặc thực thi lệnh từ xa qua WMI.
  - Nếu không có người dùng hoặc ứng dụng nào được biết trước đó sử dụng WMI, đây có thể là dấu hiệu của hoạt động nghi ngờ.



Hình 10. Lateral Movement - Event ID 5857

- **Event ID 2006**
  - Nguồn: Windows Firewall With Advanced Security
  - Tên Log: Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
  - Event ID: 2006
  - Thời gian: 14/5/2025 lúc 8:36:05 Tối
  - Mô tả: "A rule has been deleted in the Windows Defender Firewall exception list."
  - Tên Rule: "RemoteEndPoint Driver Host."
  - Người điều chỉnh: NT SERVICE\mpssvc
  - Ứng dụng điều chỉnh: C:\Windows\System32\svchost.exe.

- Nhận xét:
  - Một luật tường lửa bị xóa. Việc thay đổi rule của tường lửa là một hành vi rất đáng ngờ có thể là bước chuẩn bị cho cuộc tấn công, bao gồm việc mở cổng hoặc vô hiệu hóa bảo vệ.

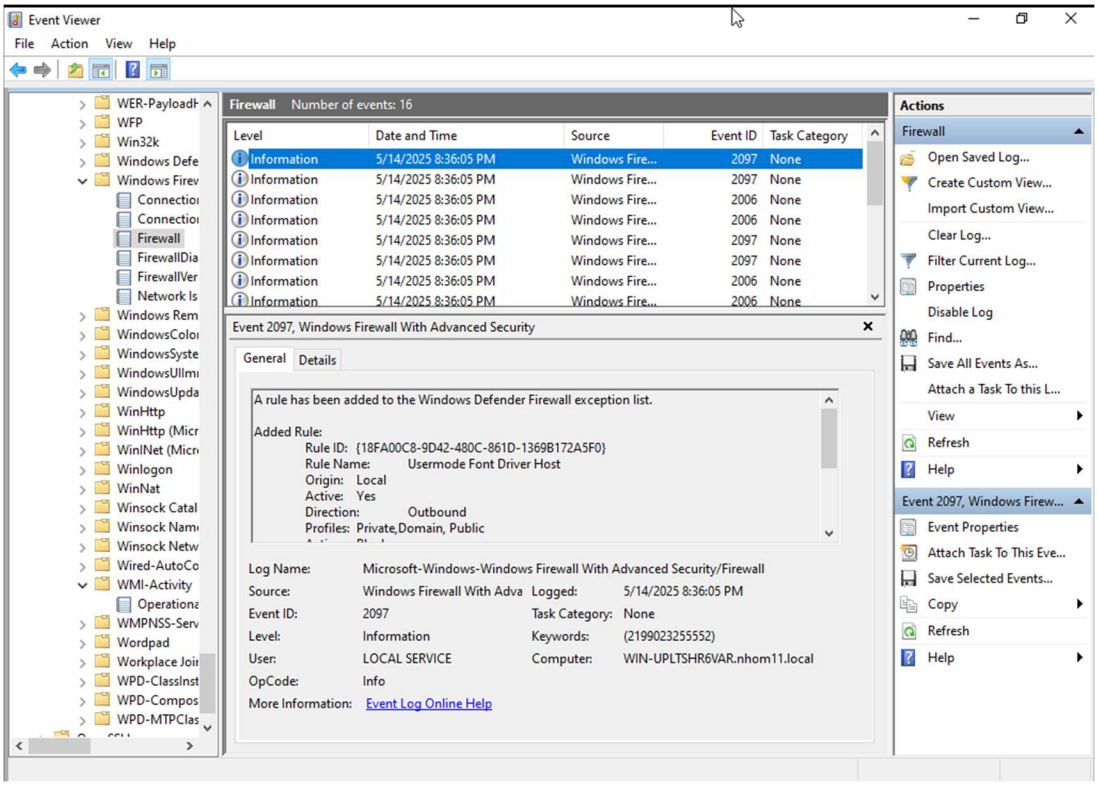


Hình 11. Lateral Movement - Event ID 2006

- **Event ID 2097**
  - Nguồn: Windows Firewall With Advanced Security
  - Tên Log: Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
  - Event ID: 2007
  - Thời gian: 14/5/2025 lúc 8:36:05 Tối
  - Mô tả: "A rule has been added in the Windows Defender Firewall exception list."
  - Tên Rule: "Usermode Font Driver Host."
  - Direction: Outbound
  - Profiles: Private, Public, Domain.
  - Đối tượng điều chỉnh: NT SERVICE\mpssvc.

- Nhận xét:
  - Một Rule mới được thêm vào tường lửa, cho phép lưu lượng đi ra ngoài mở ra cổng giao tiếp cho kẻ tấn công.

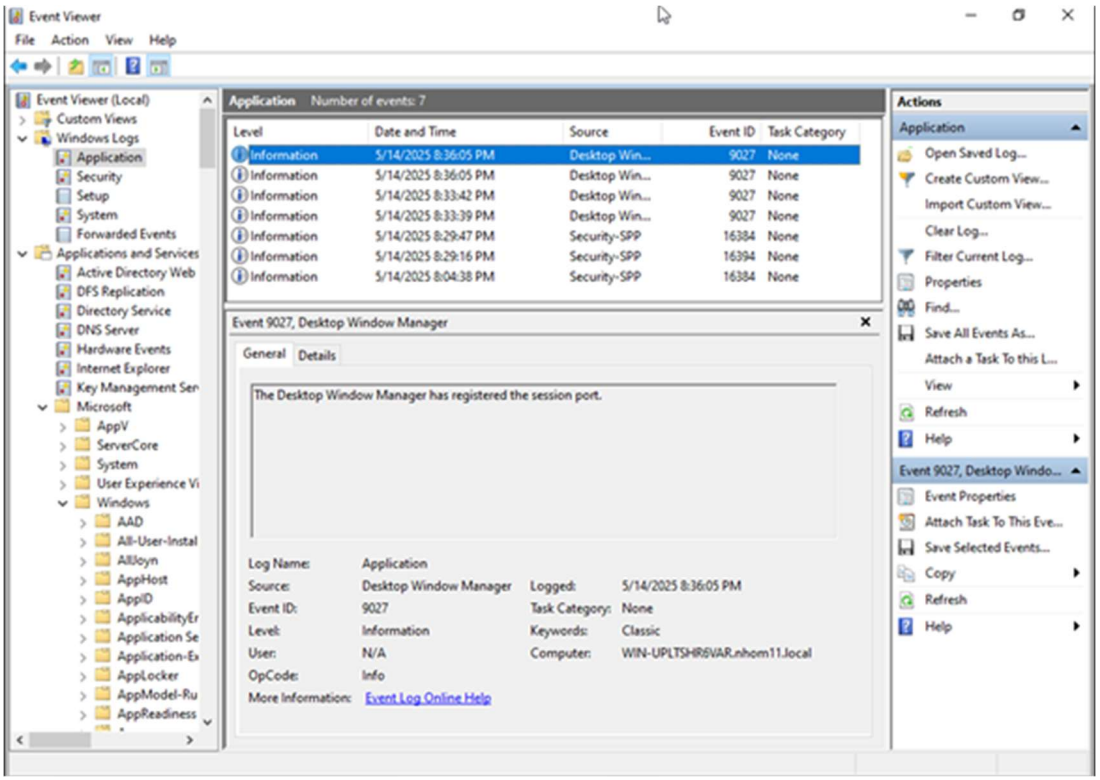
- Kết hợp với Event ID 2006, đây là một chuỗi hành vi thay đổi tường lửa để tạo điều kiện cho lưu lượng truy cập từ bên ngoài phục vụ cho 1 cuộc tấn công.



Hình 12. Lateral Movement - Event ID 2097

- **Event ID 9027**
  - Nguồn: Desktop Window Manager
  - Tên Log: Application
  - Event ID: 9027
  - Thời gian: 14/5/2025 lúc 8:36:05 Tối
  - Mô tả: "The Desktop Window Manager has registered the session port."

- Nhận xét
  - Sự kiện liên quan đến việc quản lý giao diện người dùng trên hệ thống. Có thể attacker vừa tạo session GUI từ xa hoặc thông qua Remote Desktop.

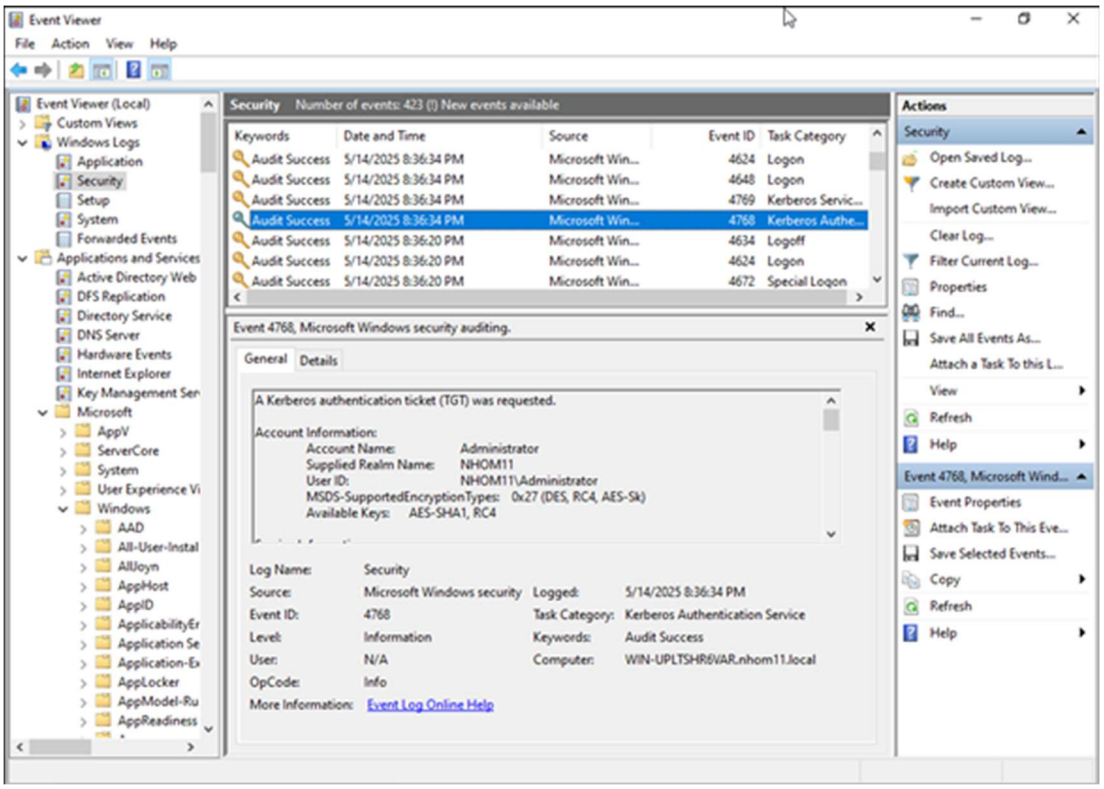


Hình 13. Lateral Movement - Event ID 9027

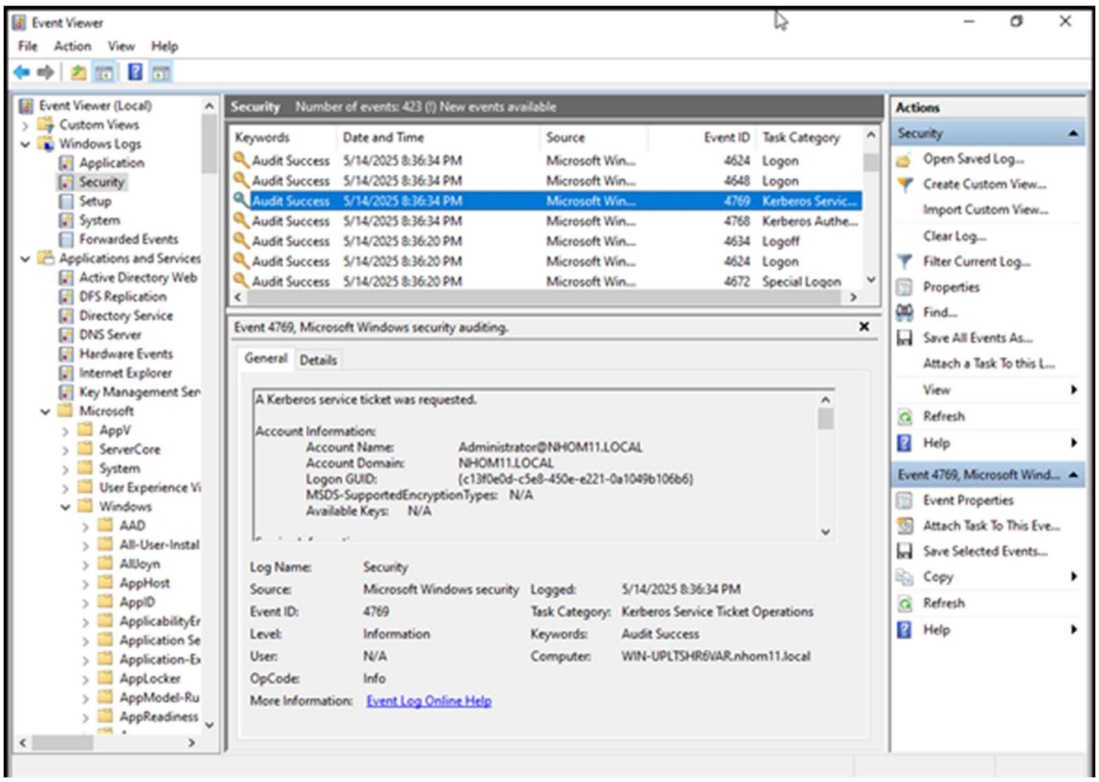
- **Event ID 4768 & 4769**

- Event 4768
  - Nguồn: Microsoft Windows Security
  - Tên Log: Security
  - Event ID: 4768
  - Thời gian: 14/5/2025 lúc 8:36:34 Tối
  - Mô tả: "A Kerberos authentication ticket (TGT) was requested."
  - Tên tài khoản: Administrator
- Event 4769
  - Nguồn: Microsoft Windows Security
  - Tên Log: Security
  - Event ID: 4769
  - Thời gian: 14/5/2025 lúc 8:36:34 Tối
  - Mô tả: "A Kerberos service ticket was requested."
  - Tên tài khoản: Administrator@NHOM11.LOCAL
- Nhận xét

- Cả hai sự kiện này đều là quá trình xác thực Kerberos. Đây là dấu hiệu của một cuộc tấn công Pass the Hash nhằm sử dụng kỹ thuật Lateral Movement để tấn công ngang hàng qua các máy khác trong mạng nội bộ.
- Kẻ tấn công đang cố gắng xác thực với tài khoản Administrator để xâm nhập hệ thống.



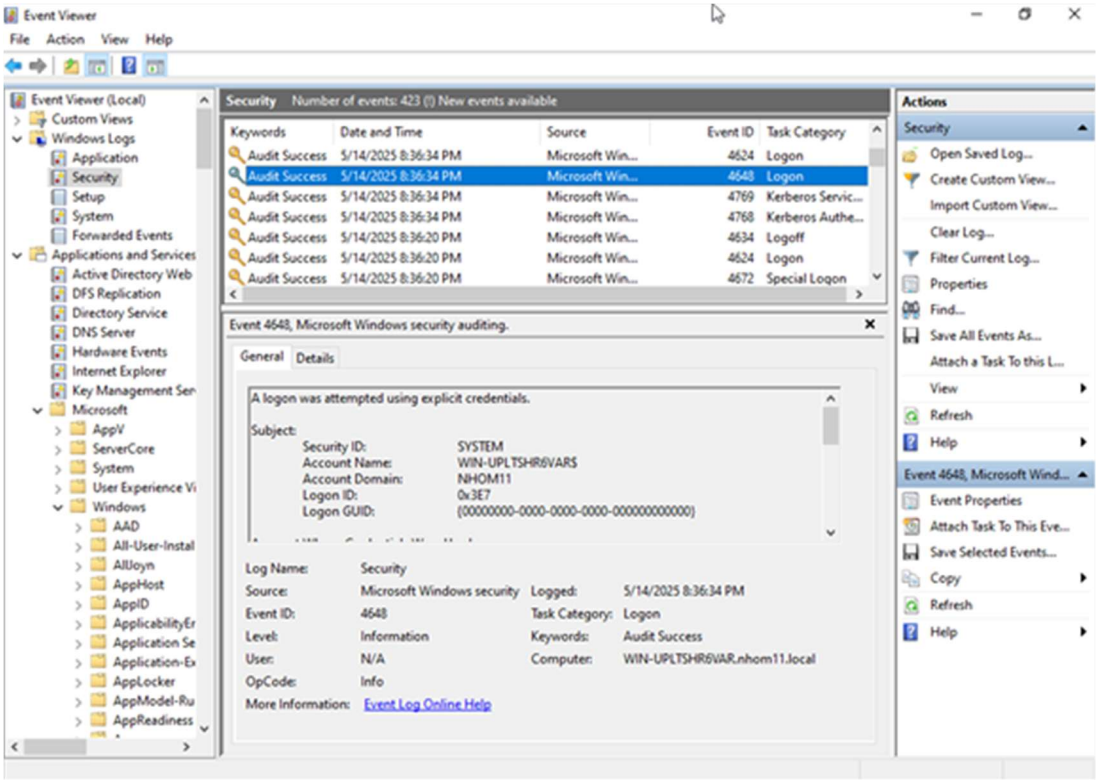
Hình 14. Lateral Movement - Event ID 4768



Hình 15. Lateral Movement - Event ID 4769

- **Event ID 4648**
  - Nguồn: Microsoft Windows Security
  - Tên Log: Security
  - Event ID: 4768
  - Thời gian: 14/5/2025 lúc 8:36:34 Tối
  - Mô tả: "A logon was attempted using explicit credentials."
  - Tên tài khoản: WIN-UPLTSHR0VAR$.
  - Tên Domain: NHOM11.LOCAL

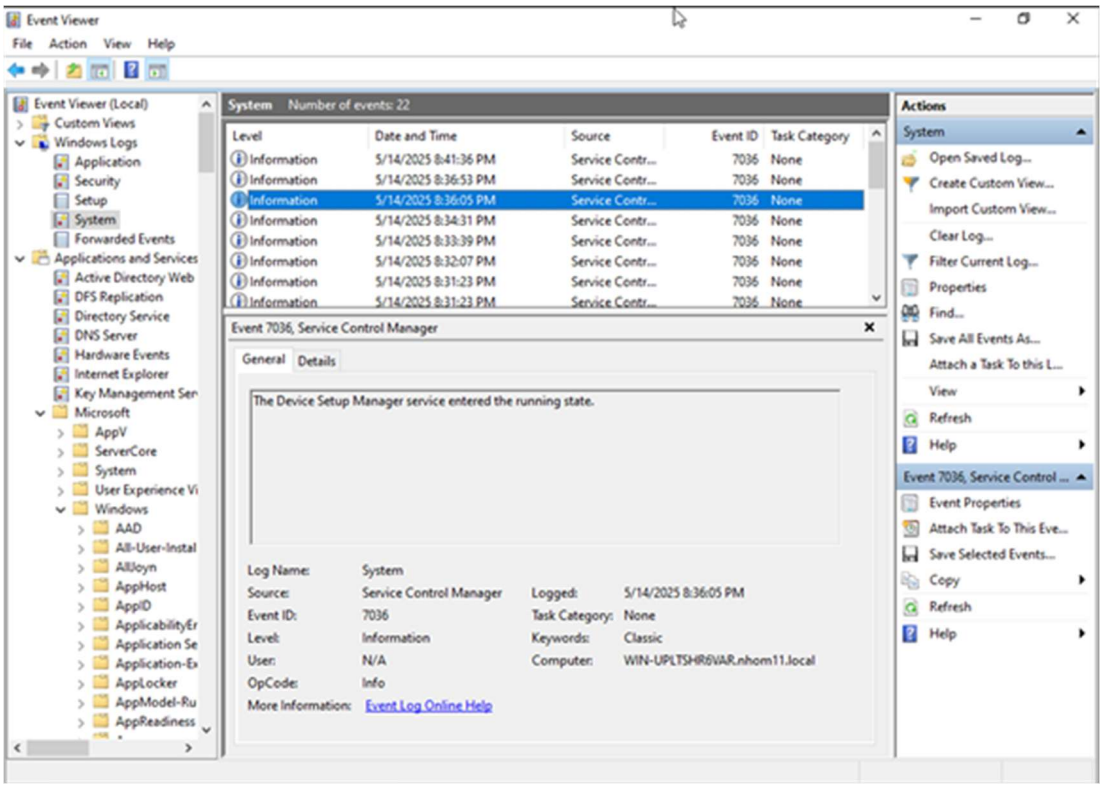
- Nhận xét
  - Ghi lại việc sử dụng thông tin xác thực rõ ràng để đăng nhập, Attacker đã thu được tài khoản hoặc hash đăng nhập từ máy trước đó đang đăng nhập sang máy khác bằng cách sử dụng WMI. Tài khoản SYSTEM trên một máy đã dùng explicit credentials để cố gắng kết nối vào hệ thống đích WIN-UPLT5HRV8ARS.rhcom11.local.



Hình 16. Lateral Movement - Event ID 4648

- **Event ID 7036**
  - Nguồn: Service Control Manager
  - Tên Log: System
  - Event ID: 7036
  - Thời gian: 14/5/2025 lúc 8:36:34 Tối
  - Mô tả: "The Device Setup Manager service entered the running state."

- Nhận xét
  - Dịch vụ Device Setup Manager vừa được khởi động thành công và chuyển sang trạng thái running, có thể để kết nối điều khiển thiết bị từ xa phục vụ cho quá trình Lateral Movement.



Hình 17. Lateral Movement - Event ID 7036

- Tài liệu tham khảo:
  - EventTracker KB --Event Id: 5615 Source: Microsoft-Windows-WMI
  - Understanding and auditing WMI | NXLog Blog
  - 4768(S, F) A Kerberos authentication ticket (TGT) was requested. - Windows 10 | Microsoft Learn

III. Đánh giá rủi ro bị khai thác lại sau khi bị tấn công. Đề xuất các biện pháp phòng ngừa tái khai thác

1. Kỹ thuật Privilege Escalation

- **Đánh giá rủi ro**

- Mô tả rủi ro:
  - Sự kiện đăng nhập với tài khoản SYSTEM và token có đặc quyền cao (Event ID 4624, 4672) cho thấy kẻ tấn công đã hoặc có thể đã khai thác thành công lỗ hổng leo thang đặc quyền. Các đặc quyền hệ thống như SeBackupPrivilege, SeLoadDriverPrivilege… được gán cho tài khoản là những đặc quyền nguy hiểm, có thể bị lạm dụng để truy cập dữ liệu, thay đổi cấu hình hoặc cài đặt mã độc có quyền hệ thống cao nhất.

  - Thêm vào đó, việc thay đổi dịch vụ BITS từ trạng thái khởi động theo yêu cầu sang tự động khởi động (Event ID 7040) là dấu hiệu rõ ràng về persistence (cơ chế tồn tại lâu dài của mã độc).
  - Phiên PowerShell chạy dưới quyền SYSTEM (Event ID 40961, 40962, 53504) thực thi đoạn mã vô hiệu hóa kiểm tra chứng chỉ SSL và tải payload từ máy chủ nội bộ cũng cho thấy mã độc hoạt động với quyền cao và nguy cơ tái tấn công hoặc tái khởi chạy mã độc rất cao.
- Rủi ro tái khai thác:
  - Nếu không phát hiện và loại bỏ triệt để persistence mechanism và tiến trình độc hại, kẻ tấn công có thể tái sử dụng các đặc quyền đã leo thang để kiểm soát hệ thống trở lại hoặc duy trì quyền truy cập lâu dài.

- **Đề xuất biện pháp phòng ngừa tái khai thác**

- Loại bỏ persistence:
  - Quét, phát hiện và xóa các dịch vụ, scheduled tasks, registry keys được kẻ tấn công thiết lập như dịch vụ BITS bị chỉnh sửa.
  - Giám sát liên tục các event đăng nhập với token nâng quyền, cảnh báo kịp thời các bất thường.
- Vá lỗ hổng và kiểm soát quyền:
  - Cập nhật hệ điều hành và phần mềm đầy đủ bản vá bảo mật.
  - Giới hạn quyền truy cập của dịch vụ, thực thi nguyên tắc ít quyền nhất (Least Privilege).
- Giám sát và phát hiện:
  - Áp dụng công cụ Endpoint Detection and Response (EDR) để phát hiện hành vi độc hại khi leo thang quyền.
  - Thiết lập cảnh báo cho các hành vi bất thường như chạy PowerShell dưới tài khoản SYSTEM.

2. **Kỹ thuật Lateral Movement**

- **Đánh giá rủi ro**

- Mô tả rủi ro:
  - Các sự kiện xóa và thêm rule tường lửa (Event ID 2006, 2097) nhằm mở cổng giao tiếp outbound cho kẻ tấn công giao tiếp với máy chủ điều khiển hoặc di chuyển ngang mạng nội bộ.
  - Sử dụng WMI để thực thi lệnh từ xa (Event ID 5857) cho thấy kẻ tấn công tận dụng công cụ hợp pháp để mở rộng kiểm soát mà không bị phát hiện.
  - Các sự kiện xác thực Kerberos (Event ID 4768, 4769) và đăng nhập sử dụng explicit credentials (Event ID 4648) chứng minh việc sử dụng kỹ thuật Pass-the-Hash/Pass-the-Ticket để tấn công ngang hàng.
  - Dịch vụ Device Setup Manager khởi động (Event ID 7036) hỗ trợ kết nối điều khiển thiết bị từ xa, mở rộng quyền kiểm soát trong mạng.
- Rủi ro tái khai thác:

- Nếu các rule tường lửa chưa được khôi phục, các tài khoản chưa được kiểm soát và xác thực chưa đủ mạnh, kẻ tấn công có thể tiếp tục di chuyển ngang, duy trì và mở rộng quyền kiểm soát mạng.

- **Đề xuất biện pháp phòng ngừa**
  - Phục hồi và kiểm soát chặt chẽ cấu hình tường lửa, loại bỏ các rule do kẻ tấn công tạo hoặc chỉnh sửa.
  - Hạn chế và kiểm soát quyền sử dụng WMI, chỉ cho phép các tài khoản tin cậy thực thi.
  - Áp dụng xác thực đa yếu tố (MFA) cho tất cả tài khoản quản trị và các tài khoản nhạy cảm.
  - Đổi mật khẩu định kỳ, khóa hoặc xóa các tài khoản nghi ngờ bị lộ thông tin.
  - Giám sát liên tục các sự kiện đăng nhập, xác thực và hoạt động điều khiển thiết bị từ xa.
  - Nâng cao nhận thức bảo mật cho người dùng và quản trị viên, hạn chế truy cập và thao tác trên các thiết bị không an toàn.

HẾT