BÁO CÁO THỰC HÀNH HT2

Môn học: Tấn Công Mạng

Kỳ báo cáo: Buổi 03

Tên chủ đề:

GVHD: ThS Nguyễn Công Danh

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT205.P21.ANTT

STT	Họ và tên	MSSV	Email
1	Nguyễn Hải Phong	22521088	22521088@gm.uit.edu.vn
2	Hồ Trung Kiên	22520704	22520704@gm.uit.edu.vn
3	Nguyễn Đức Thụy Hưng	21520893	21520893@gm.uit.edu.vn
4	Lê Công Danh	22520199	22520199@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN

STT	Công việc	Thực hiện	Kết quả tự đánh giá
1	Câu 1	Nguyễn Đức Thụy Hưng	9
2	Câu 2	Lê Công Danh	
3	Câu 3	Hồ Trung Kiên	

BÁO CÁO CHI TIẾT

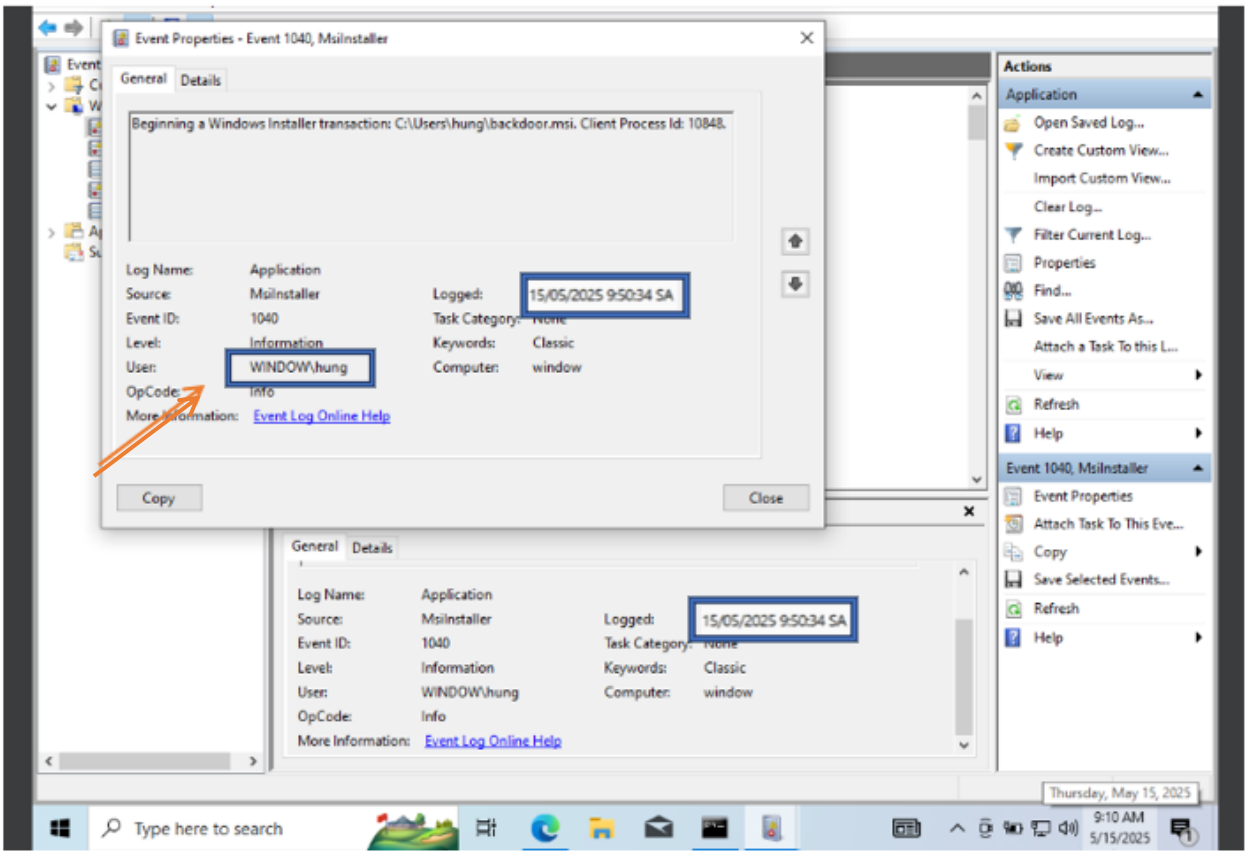
1. Kỹ thuật Privilege Escalation

1.1.Kịch bản ví dụ: Privilege Escalation qua cấu hình sai AlwaysInstallElevated:

Kịch bản tấn công: Máy client trong mạng nội bộ đã bị Attacker xâm chiếm và Attacker đã thực hiện Privilege Escalation thông qua việc lạm dụng "AlwaysInstallElevated" registry key để lấy được quyền admin

Quá trình truy vết trên Window Client thông qua Window Event View.

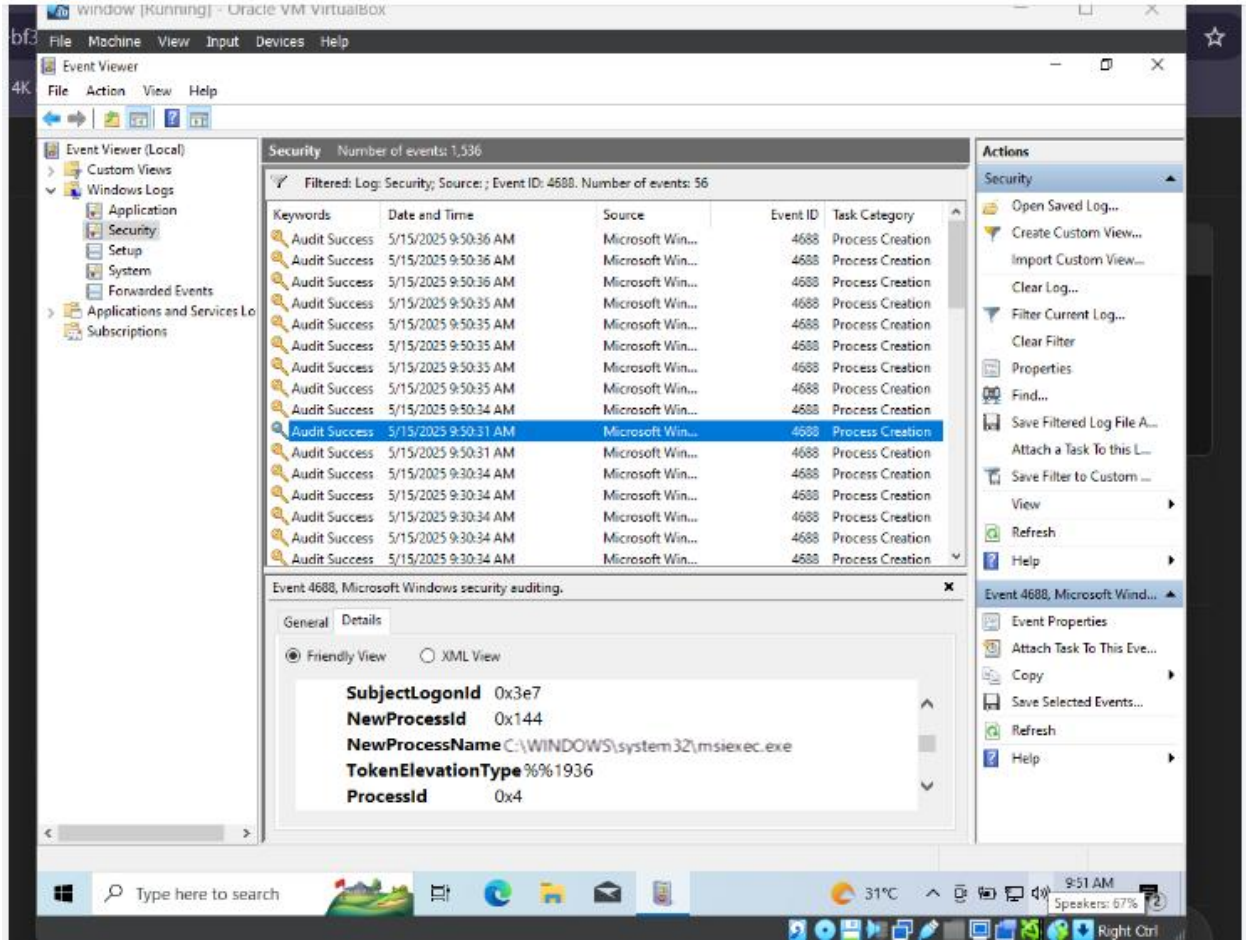
Truy cập vào Window Client, theo dõi Event View, ta thấy có một sự kiện cài đặt file .msi bất thường do user hung cài đặt (user này không có quyền Admin nên việc user này cài đặt được file .msi là một điều đáng ngờ). Đây là một dấu hiệu cho việc client đã bị Privilege Escalation.



Hình 1 File backdoor.msi được user hung tiến hành cài đặt

Để đảm bảo đây đúng là một cuộc tấn công Privilege Escalation. Để xác nhận, ta chuyển sang **Security log** trong Event Viewer và thấy tiến trình

C:\Windows\System32\msiexec.exe. được tạo ra với quyền hệ thống.



Hình 2. Tiến trình C:\Windows\System32\msiexec.exe được tạo

Sự kiện này khẳng định attacker đã khai thác AlwaysInstallElevated, ép Windows cài đặt package độc hại dưới ngữ cảnh SYSTEM, và do đó chiếm được quyền

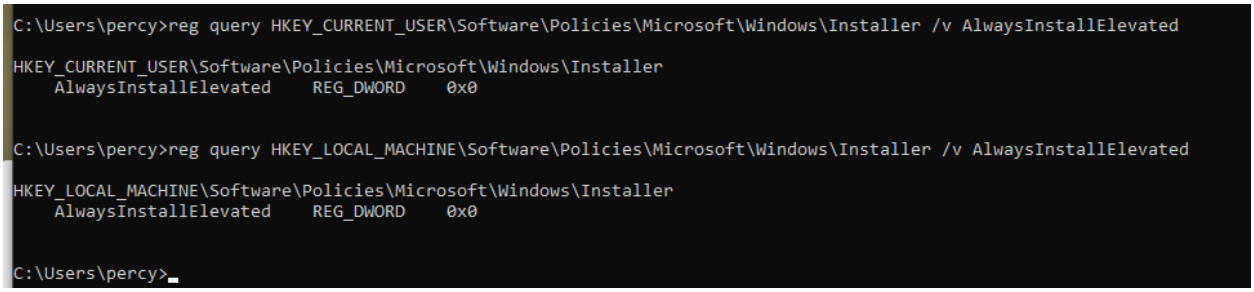
1.2.Phòng chống

1.2.1. Vô hiệu hóa AlwaysInstallElevated (biện pháp quan trọng nhất)

Khi cả hai khóa registry liên quan đến AlwaysInstallElevated được thiết lập giá trị 1, mọi người dùng – kể cả người dùng không có quyền quản trị – đều có thể cài đặt file .msi với đặc quyền SYSTEM, gây nguy cơ nghiêm trọng về bảo mật. Để ngăn chặn điều này, cần vô hiệu hóa tùy chọn này bằng cách đặt cả hai khóa về giá trị 0, sử dụng hai lệnh sau:*reg add HKLM\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated /t REG_DWORD /d 0 /f*

reg add HKCU\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated /t REG_DWORD /d 0 /f

Sau khi thực hiện trên Client với quyền SYSTEM, ta kiểm tra 2 khóa registry này xác nhận rằng cả hai khóa đã được vô hiệu hóa..



Hình 3. Hai khóa này đã bị vô hiệu hóa

1.2.2. Chặn thực thi msiexec.exe nếu không cần thiết.

Nếu không sử dụng định dạng .msi để triển khai phần mềm, nên chủ động chặn hoặc giới hạn quyền sử dụng công cụ msiexec.exe nhằm giảm thiểu nguy cơ bị khai thác.

Có thể áp dụng một trong các biện pháp sau:

- Sử dụng AppLocker hoặc Windows Defender Application Control (WDAC) để:
  - Chặn msiexec.exe đối với người dùng không phải quản trị viên.
  - Chỉ cho phép thực thi các gói cài đặt đã được ký số và xác minh từ nhà cung cấp đáng tin cậy.

Biện pháp này giúp ngăn chặn client tải hoặc cài đặt các phần mềm độc hại ngụy trang dưới định dạng .msi, đặc biệt là trong các tình huống leo thang đặc quyền hoặc thực thi mã từ xa.

Ngoài ra, có thể chuyển sang sử dụng định dạng **MSIX** – một định dạng cài đặt được Microsoft khuyến nghị. MSIX hỗ trợ sandbox hóa, kiểm soát truy cập tốt hơn, và bảo mật nâng cao, giúp giảm thiểu rủi ro khi triển khai ứng dụng.