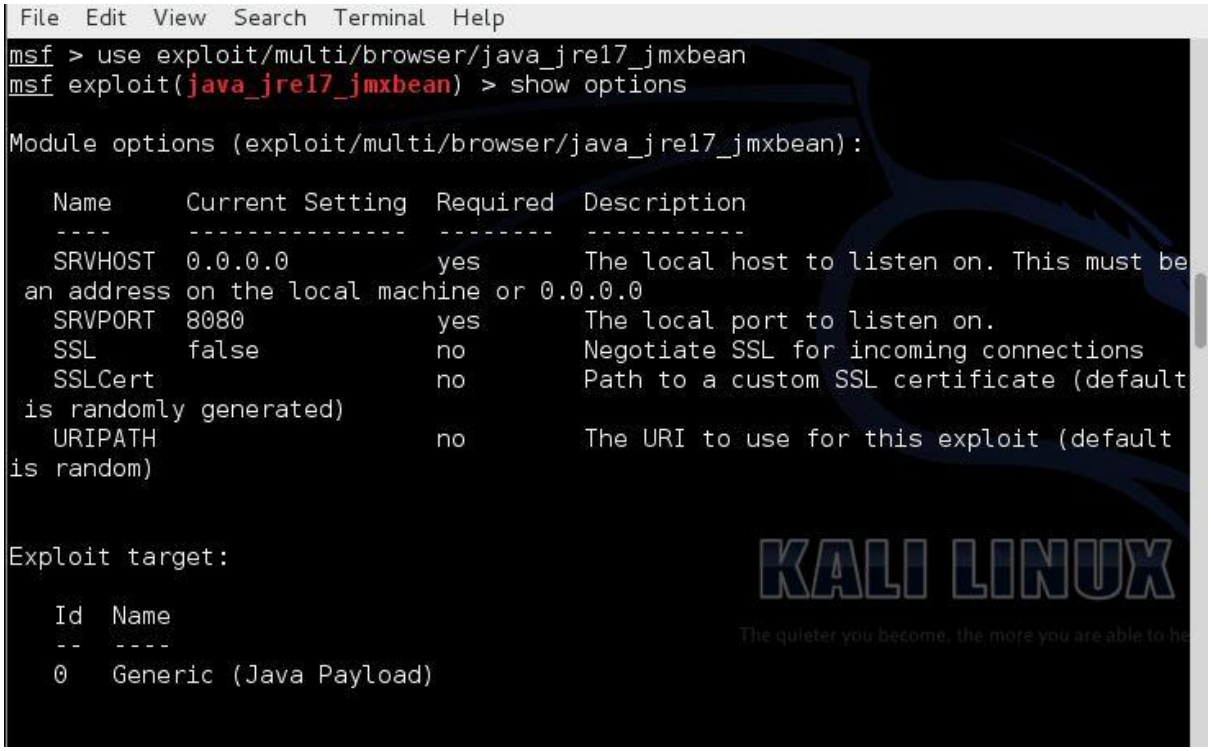
Client-side Attacks

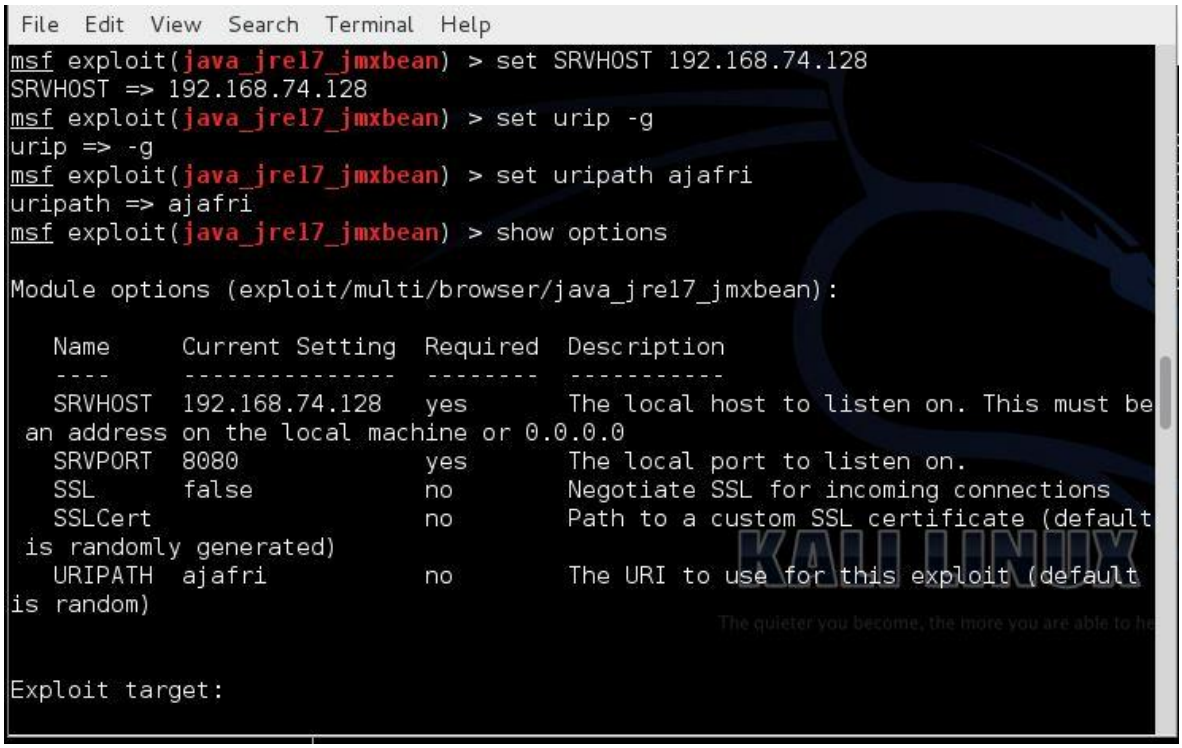
Name: Alizeh Jafri

Task 1:

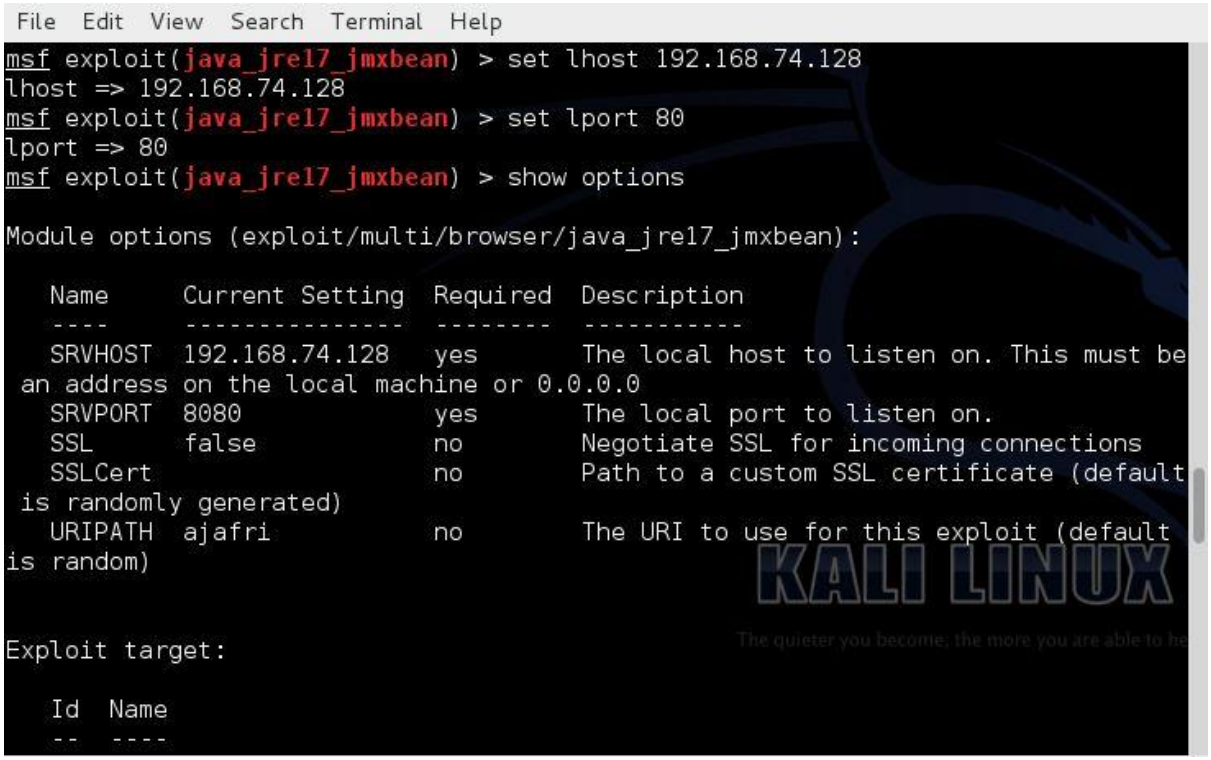
Firstly, in Kali linux I started apache2 using the command ‘service apache2 start’. Then, I accessed msfconsole. Next, I typed the command as shown below and entered ‘show options:



I set SRVHOST, urip and uripath as shown below:

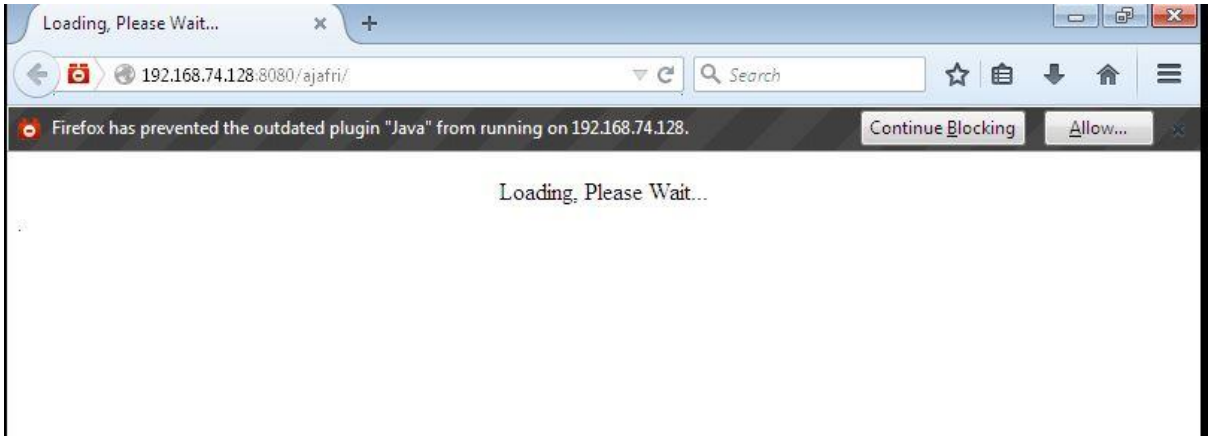


Then I set the Lhost to that of the target machine and lport to 80 as shown below:

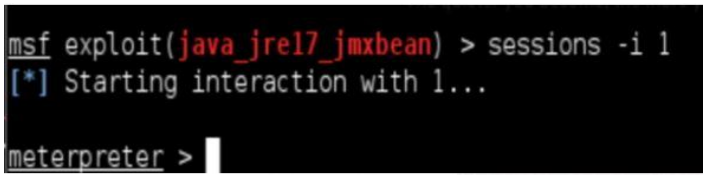


Now, I exploited and got the URL :

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

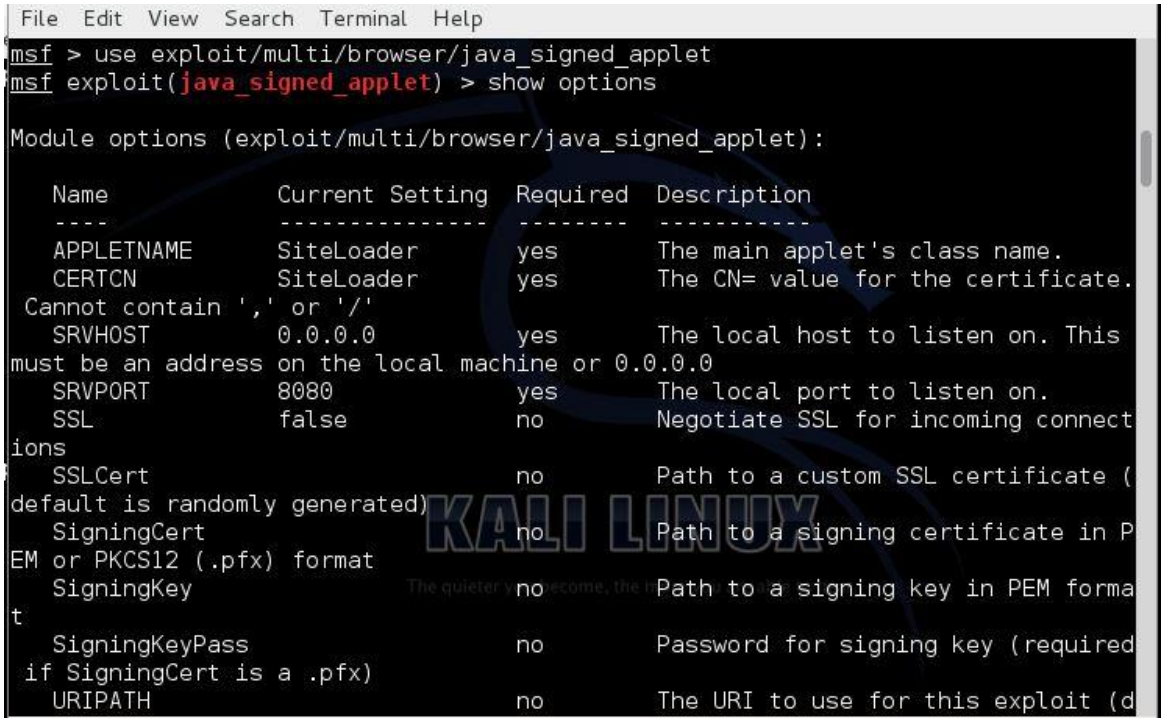


Then I entered sessions -I -1:

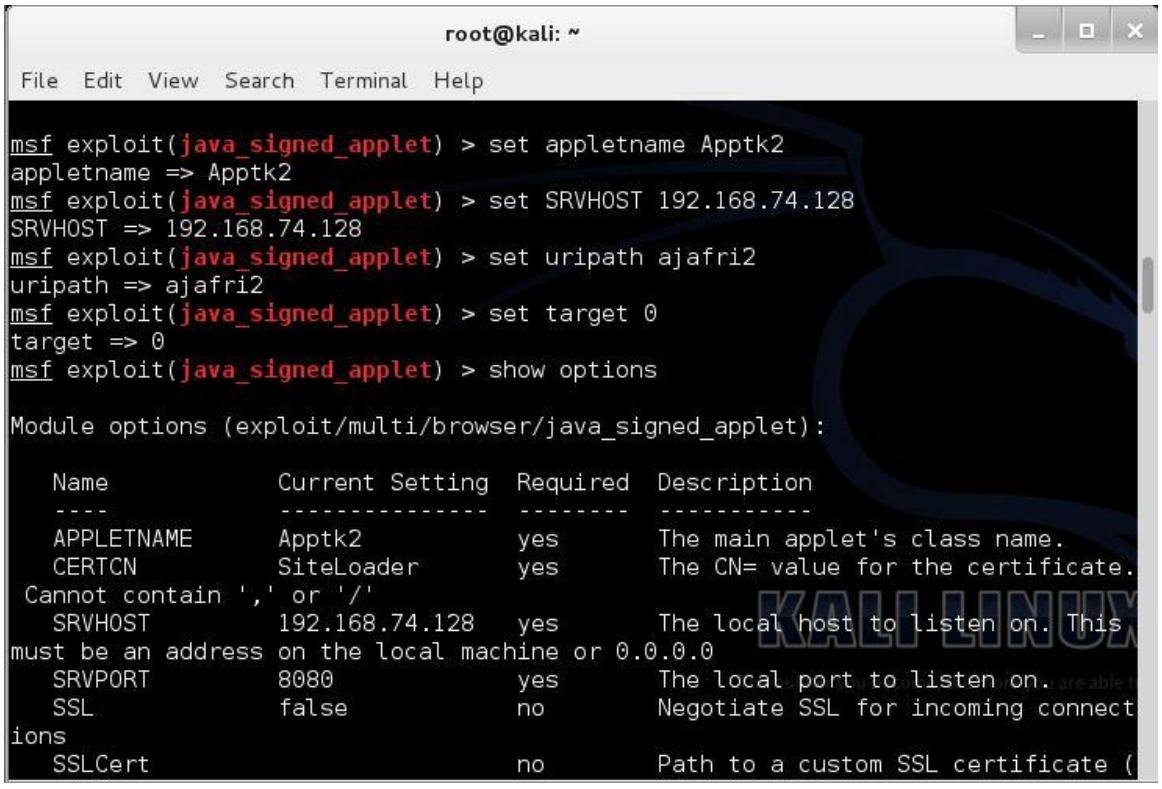


Task 2:

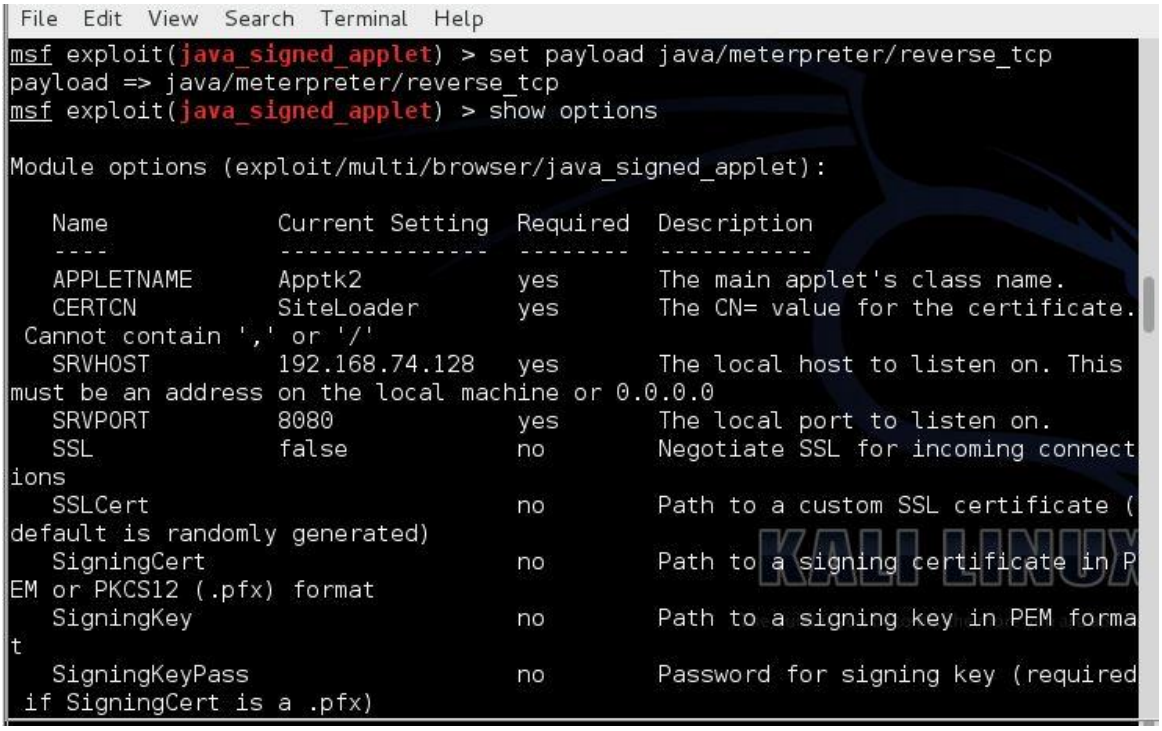
In this I used Metasploit to exploit this kind of Java Signed Applet vulnerabilities in my Windows 7 virtual machine. Firstly, I started apache using the command 'service apavhe2 start' then I opened msfconsole. In msf I typed the command shown below:



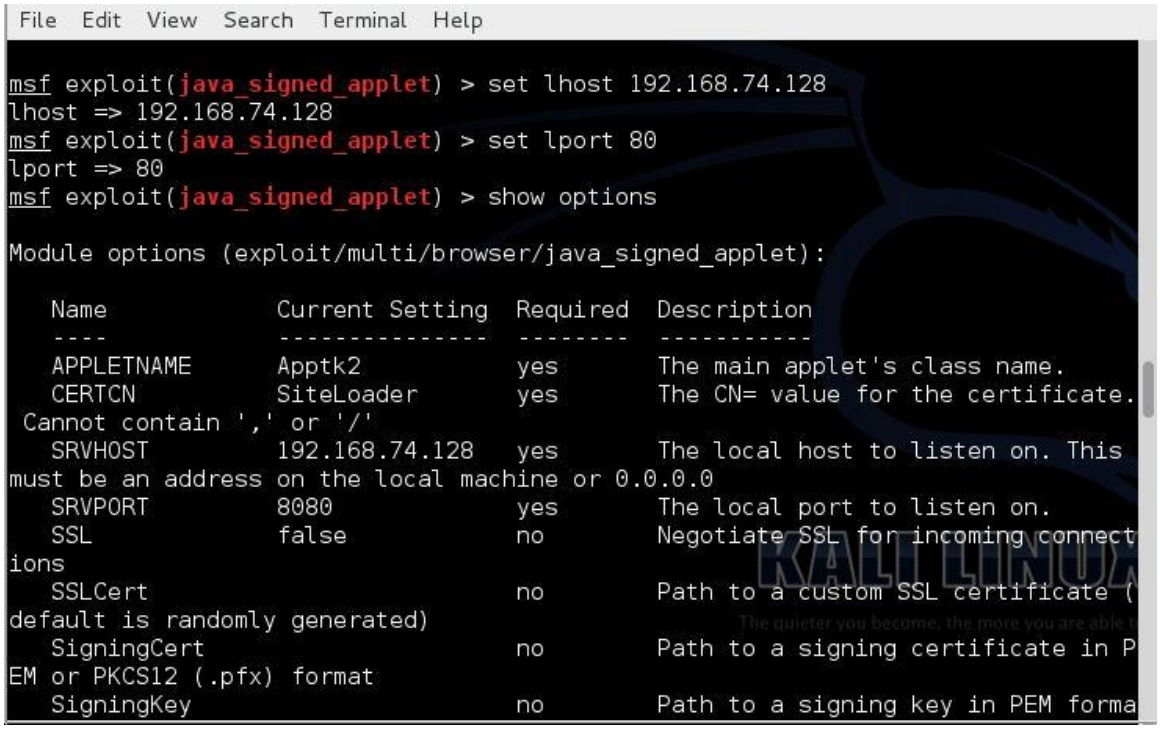
Next, I set appletname Apptk2, set SRVHOST to that of the IP of Kali. Then I set uripath as 'ajafri', target 0 and typed show options:



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



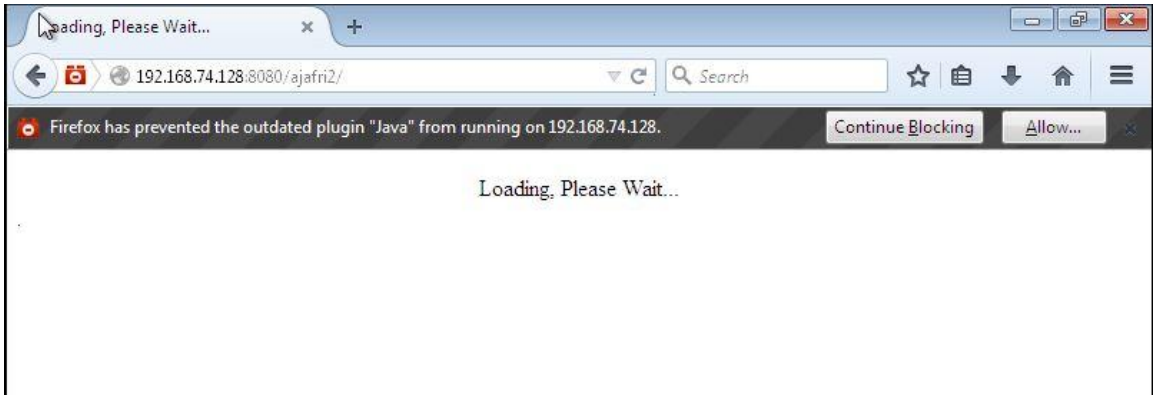
Next, I set the Lhost to the IP of Kali, port as 80 and typed show options:



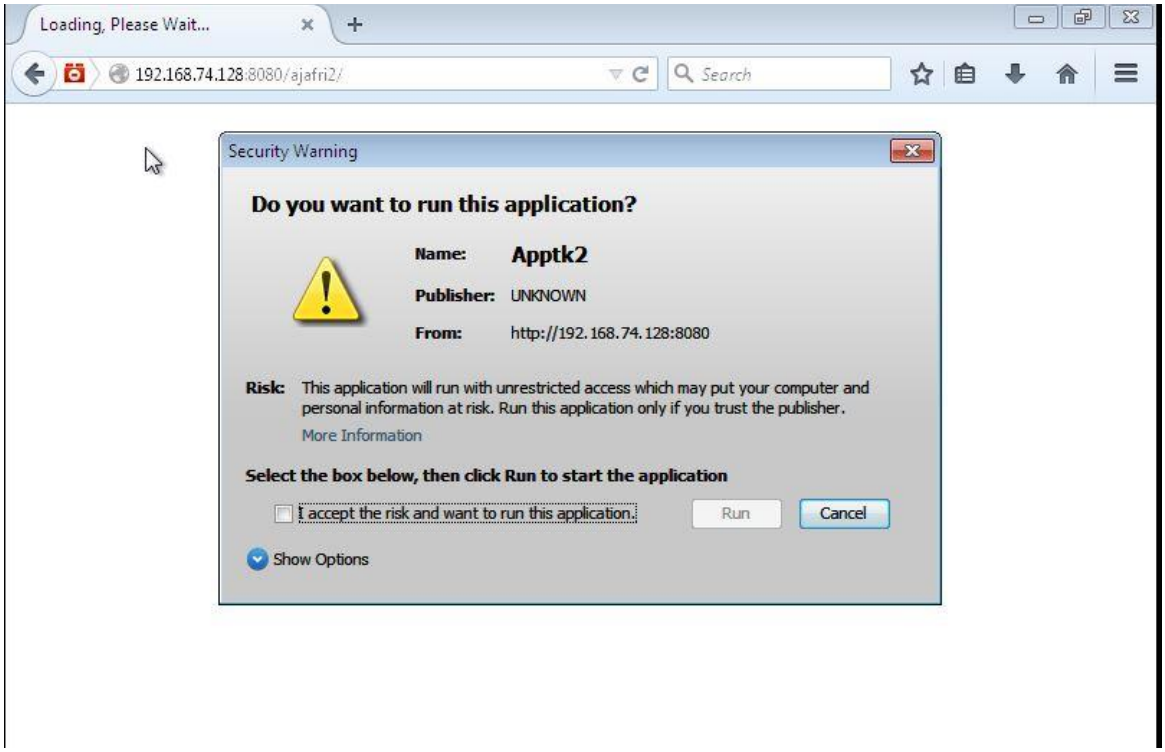
Here, I exploited and got the URL:

```
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 -I 1’ and entered ls to see what is in the meterpreter: