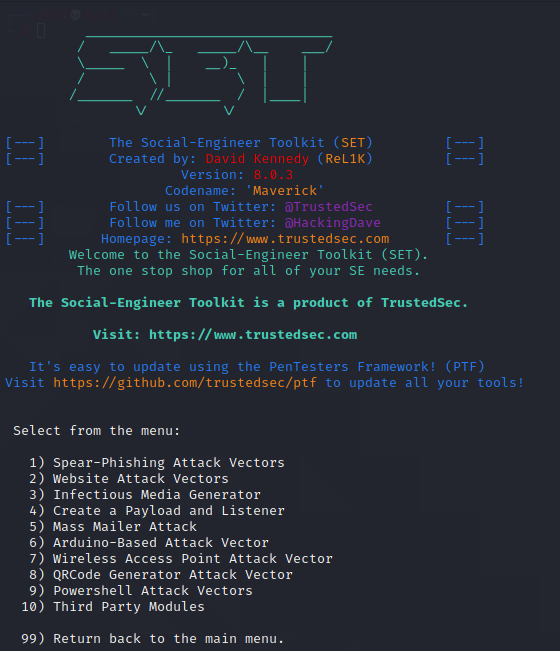
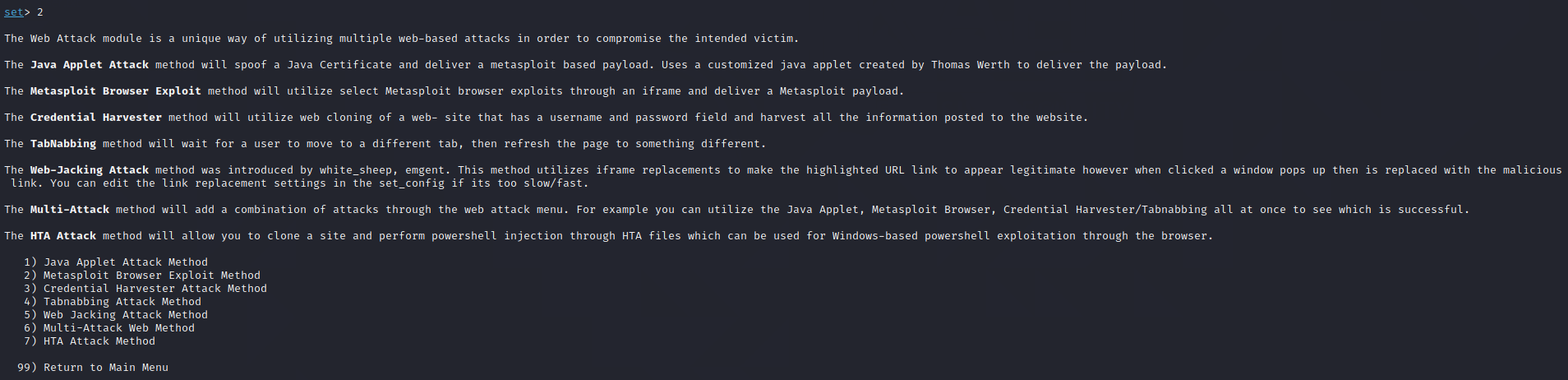
**ARYAMAN MISHRA**

**19BCE1027-EXPERIMENT 10-SEToolkit**

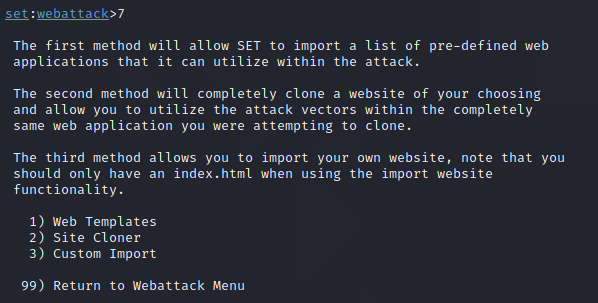
Start Social Engineering Toolkit on Kali Linux.



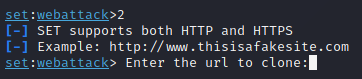


SELECT OPTION 2-WEBSITE ATTACK VECTORS

SELECT OPTION 7-HTA ATTACK METHOD

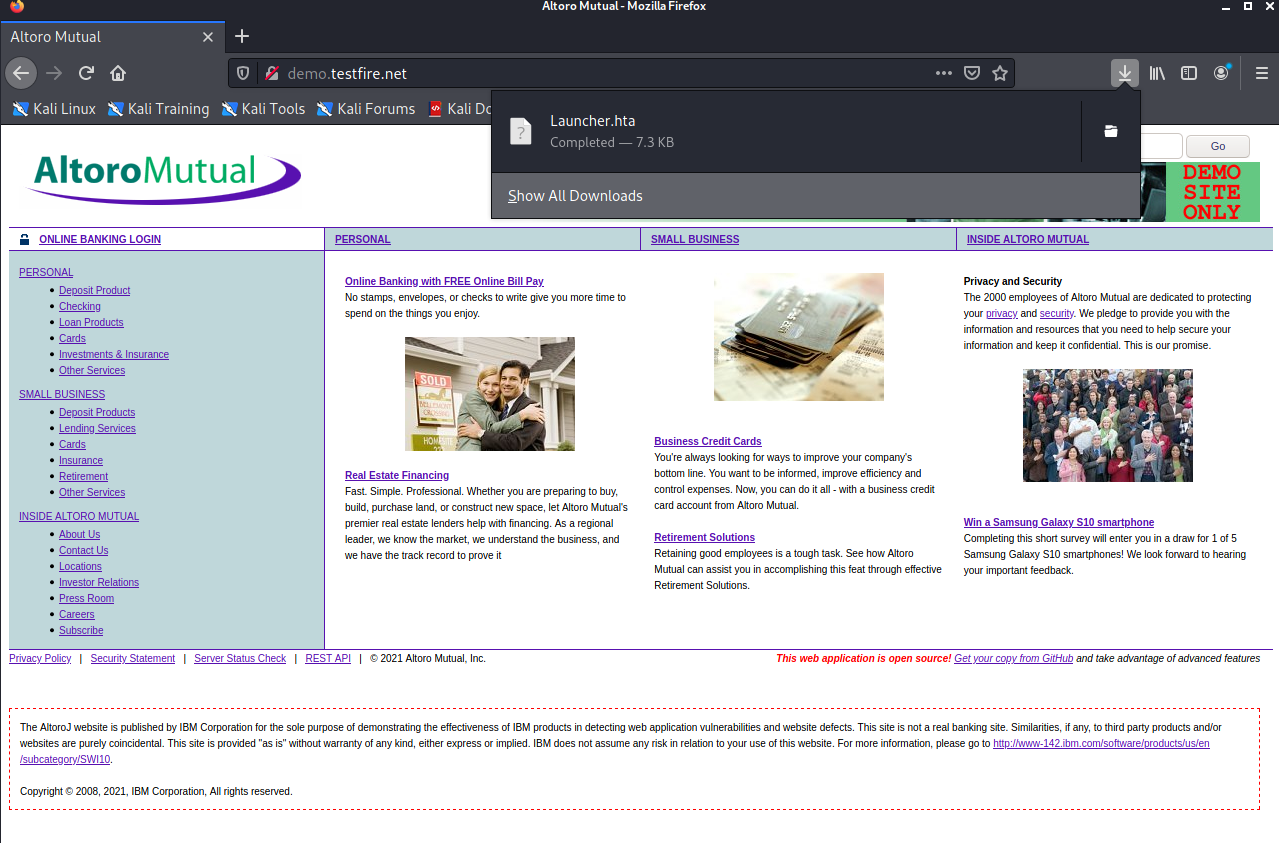


SELECT OPTION 2

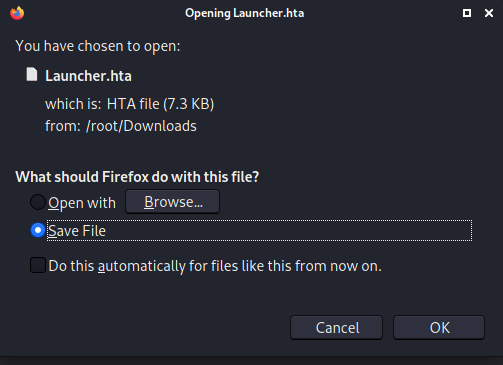


ENTER URL: <http://demo.testfire.net/>

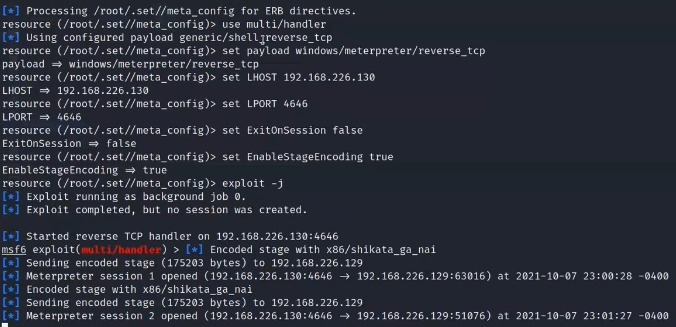
ENTER PORT: 443/4646/4747

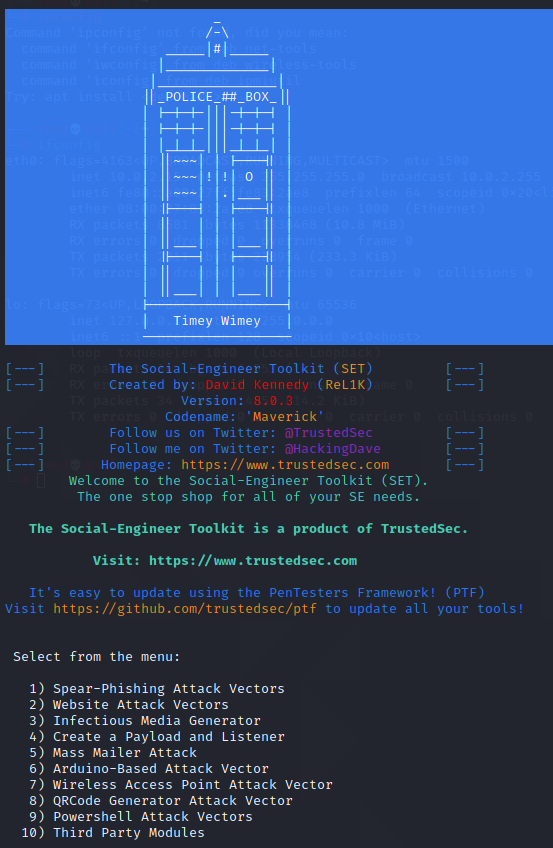
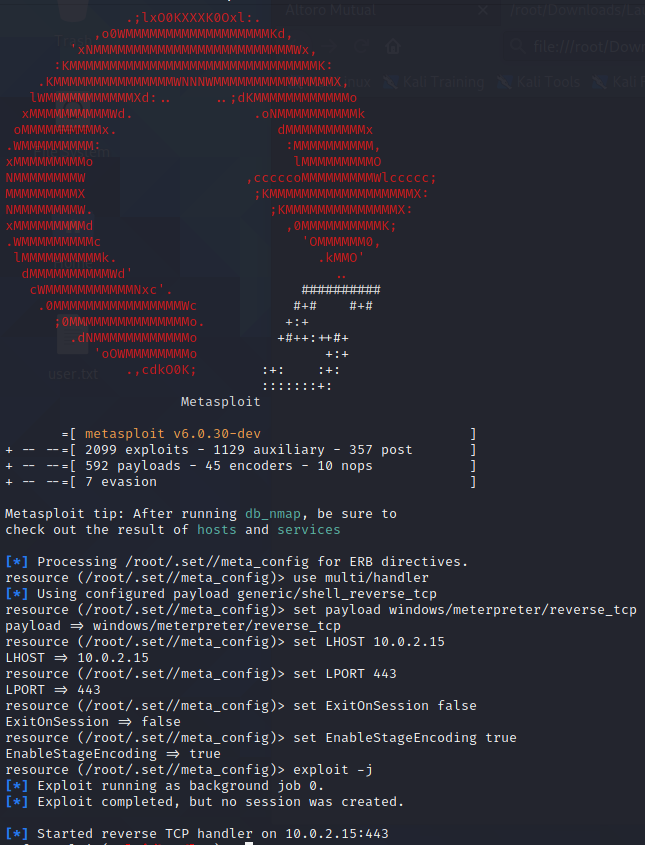


USE IP AS 10.0.2.15 TO ACCESS WEBSITE ON FIREFOX AND DOWNLOAD A .HTA FILE

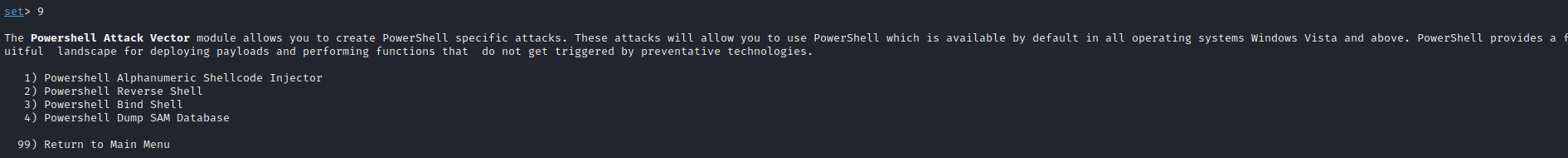


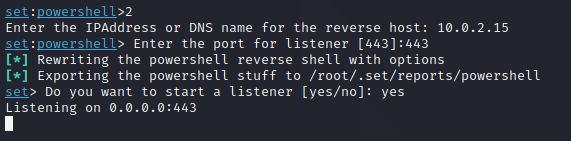
When you launch the file in Windows VM,your Kali Linux Terminal will show this and launch Metasploit automatically.





Conduct a Powershell Bind Shell Test:



Navigate thorugh the options and listen on the victim machine:

Perform operations in the powershell and the Kali terminal will reflect those changes via Social Enginnering Toolkit.