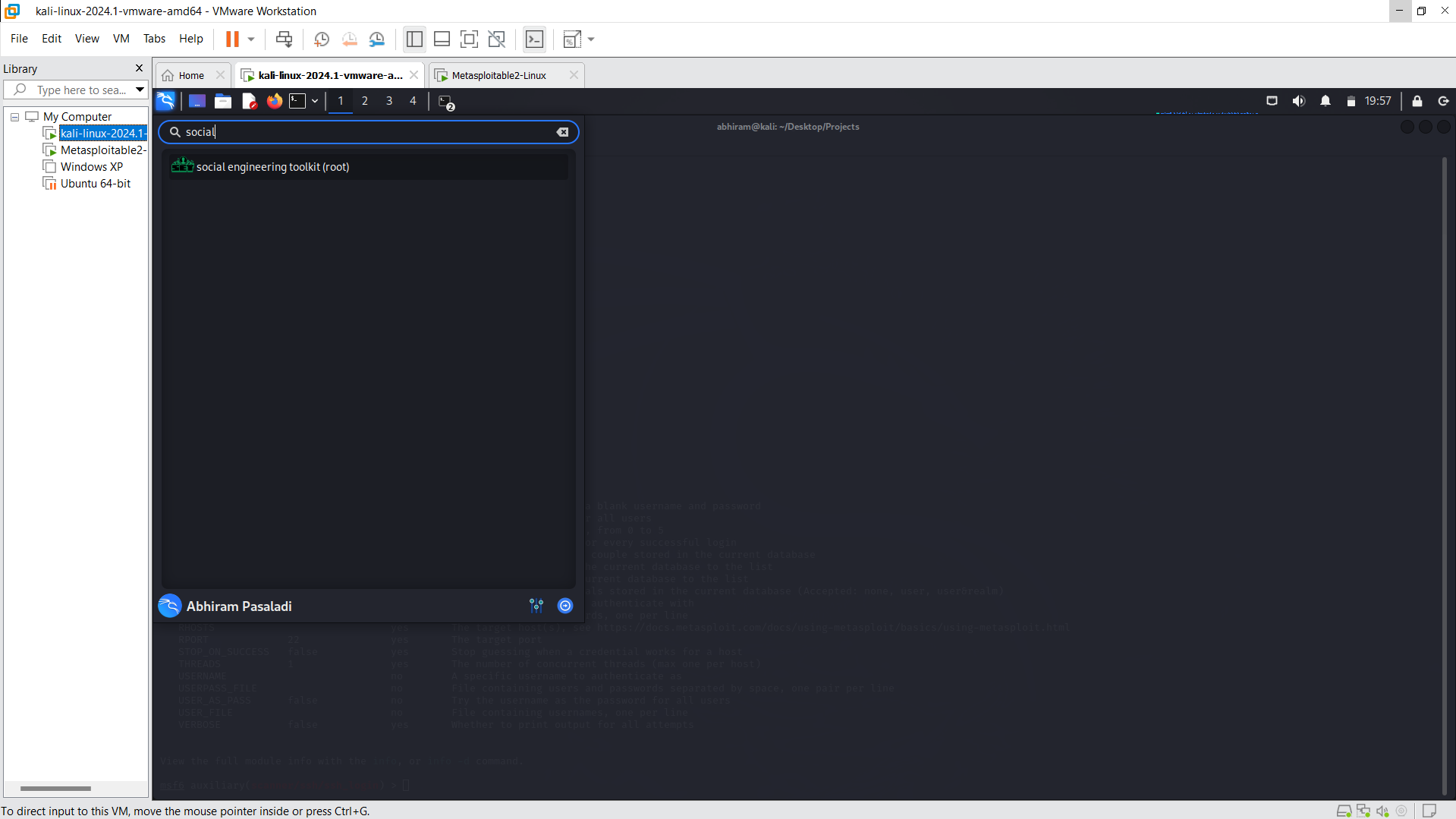
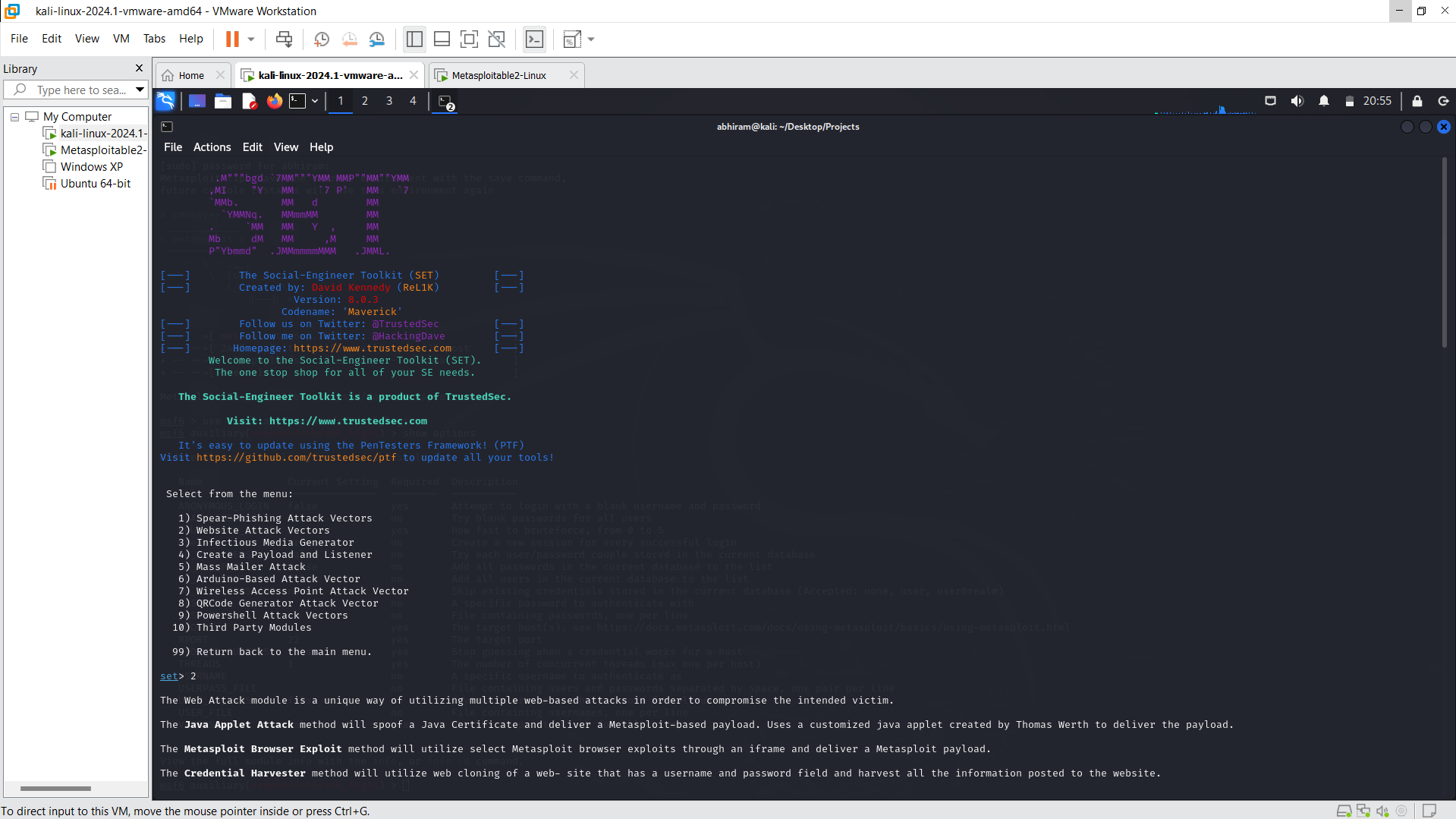
Credential Harvesting using Social Engineering Toolkit (SET)

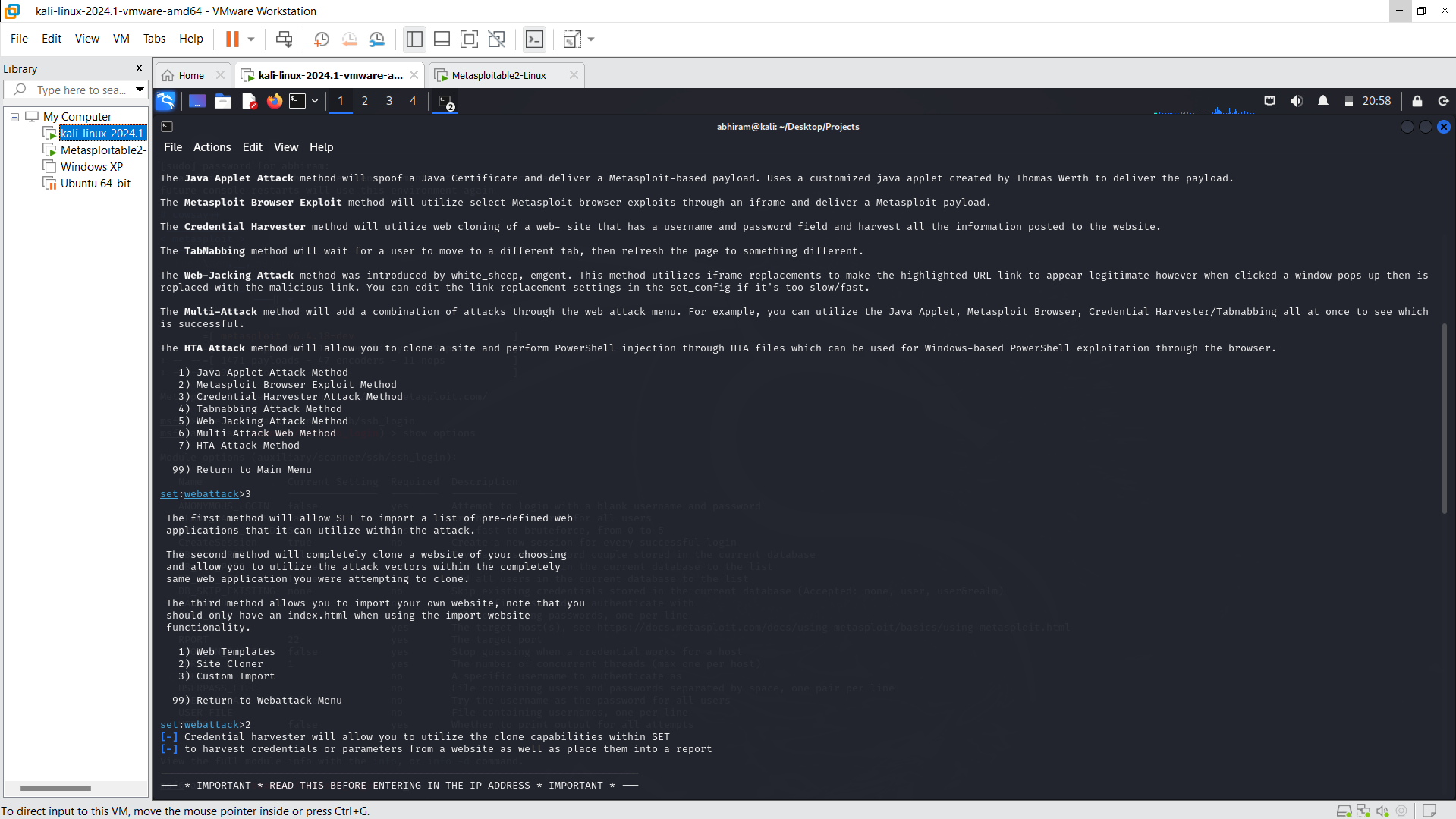
Introduction:  
 Credential harvesting using the Social Engineering Toolkit (SET) involves simulating phishing attacks to collect sensitive information like usernames and passwords. By creating convincing fake login pages or email phishing scenarios, SET can trick users into entering their credentials, which are then captured by the attacker. This method is widely used in penetration testing to evaluate an organization's security posture and identify vulnerabilities in user awareness and system defenses.

Steps:

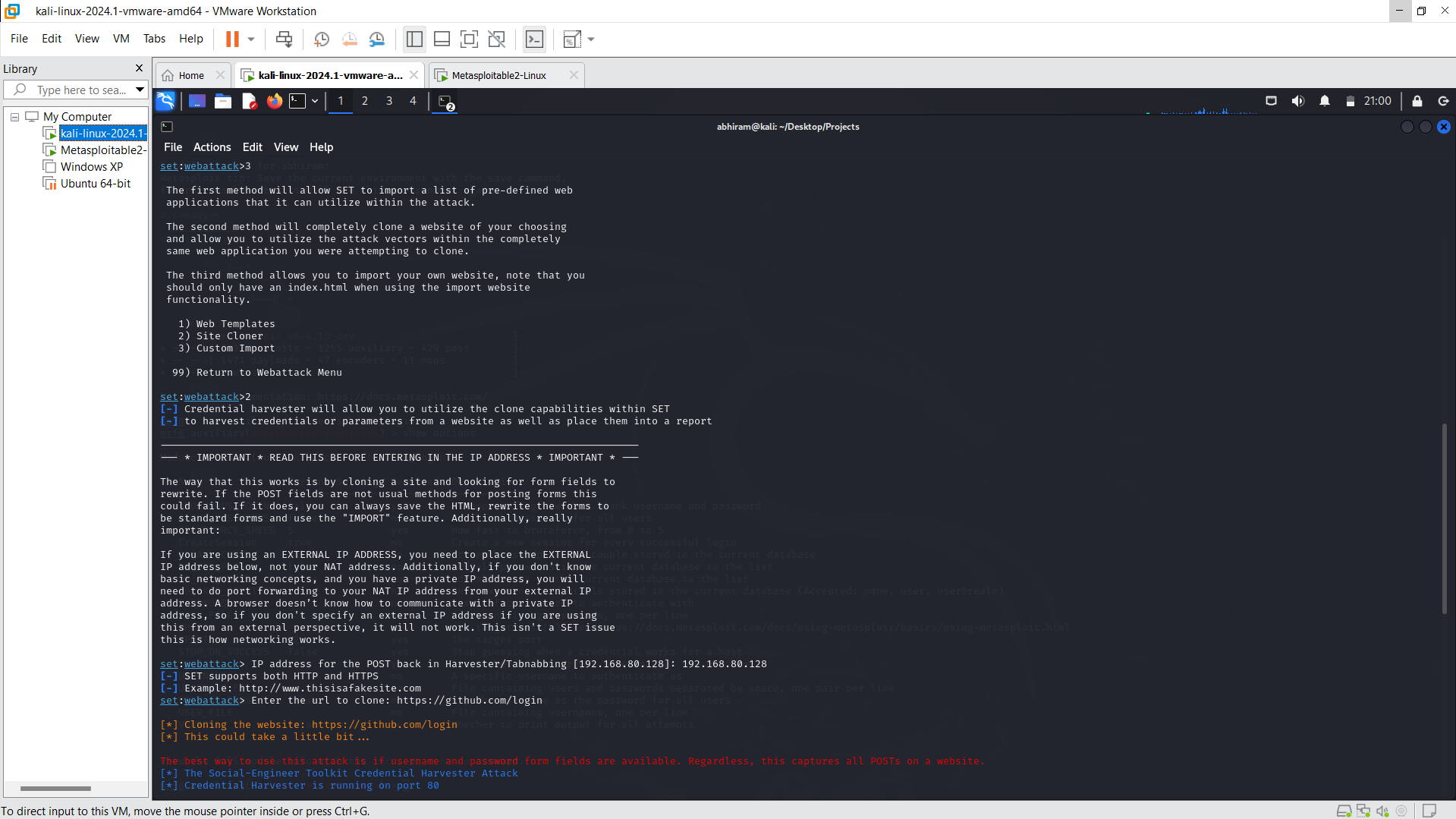
1. Open Social Engineering Tool Kit in Kali-Linux through search: 
2. Select 2->Website Attack Vectors.



1. Choose 3-> Credential Harvester Attack Method.

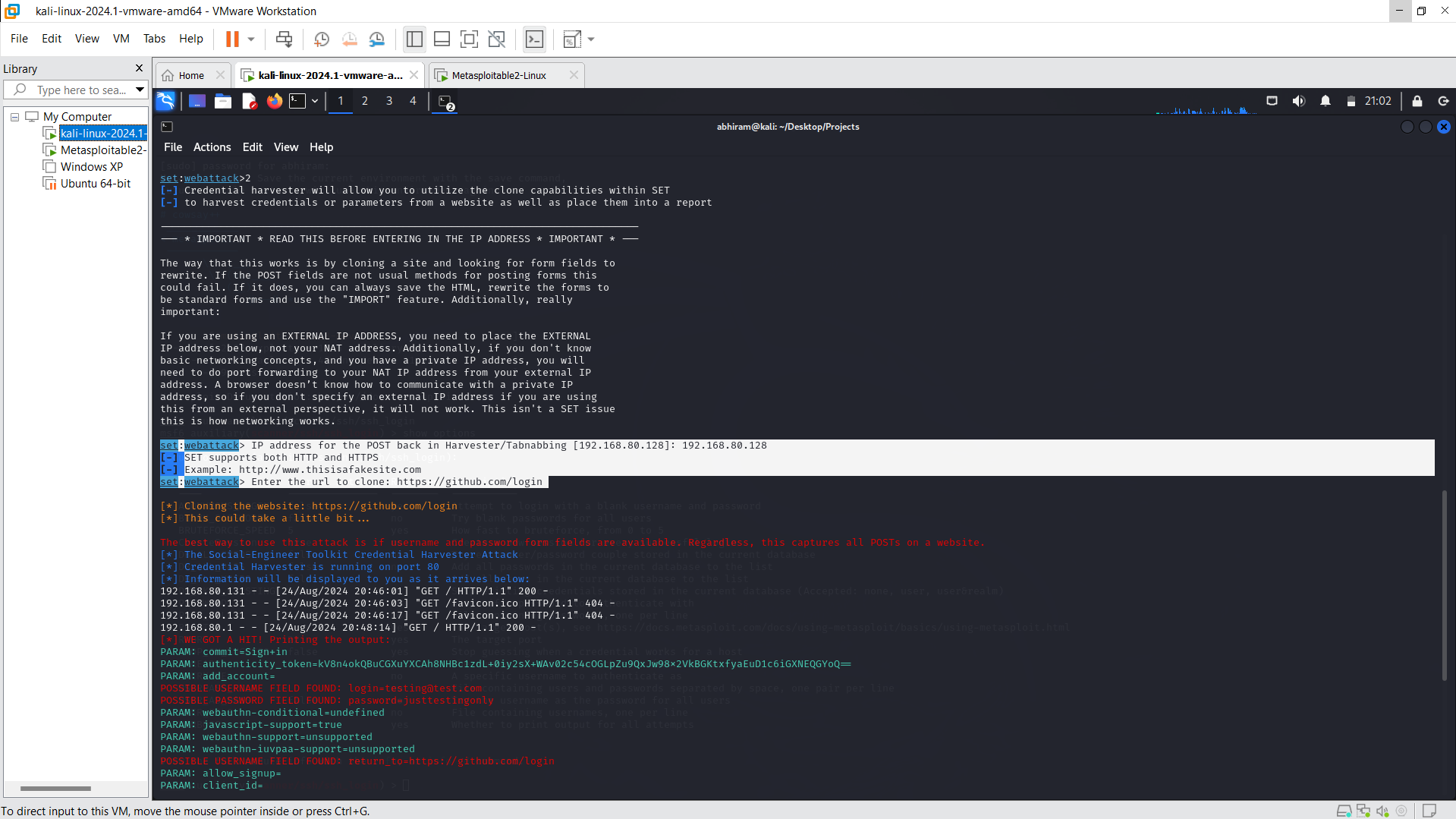


1. Choose 2->Site Cloner

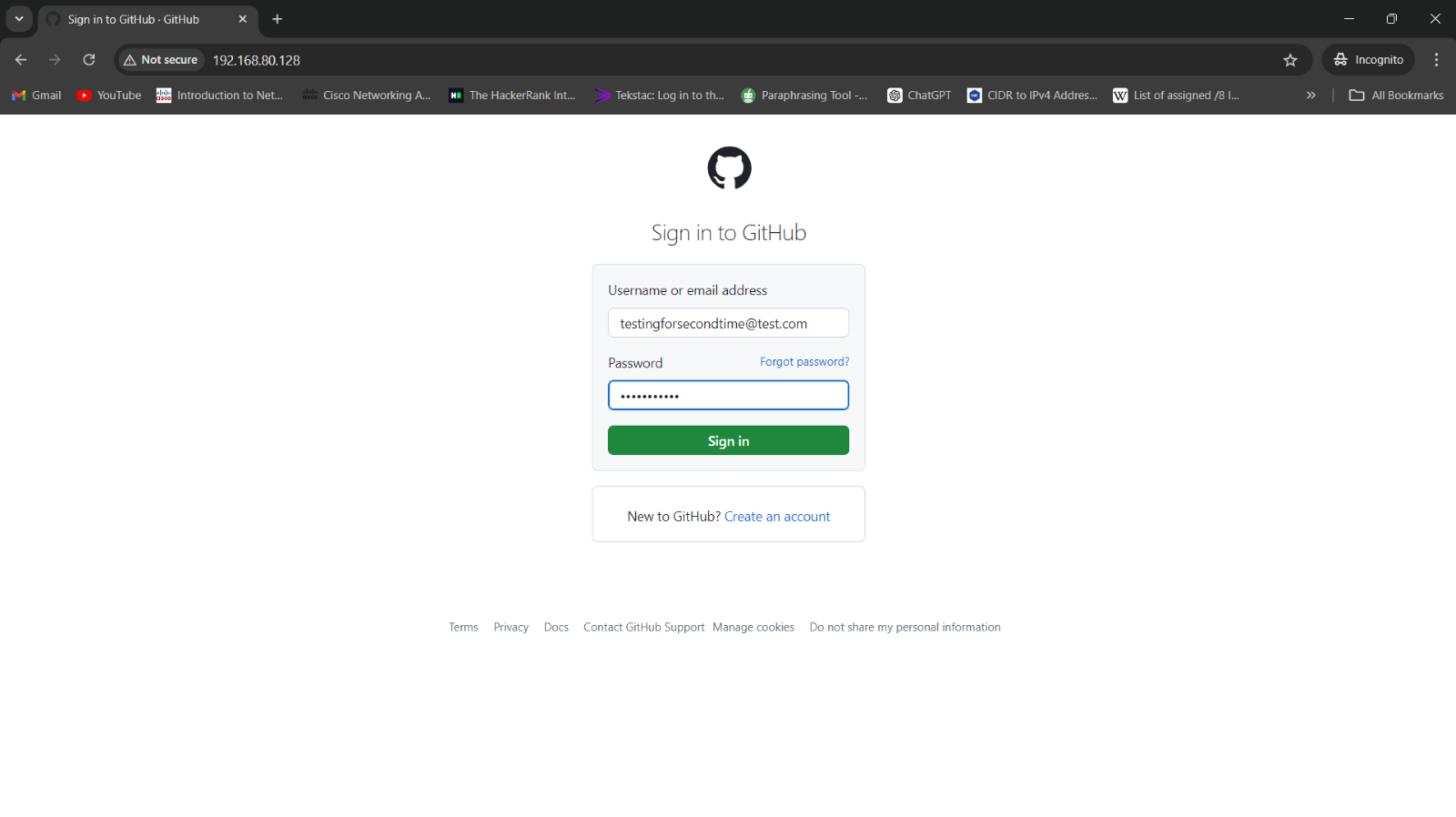
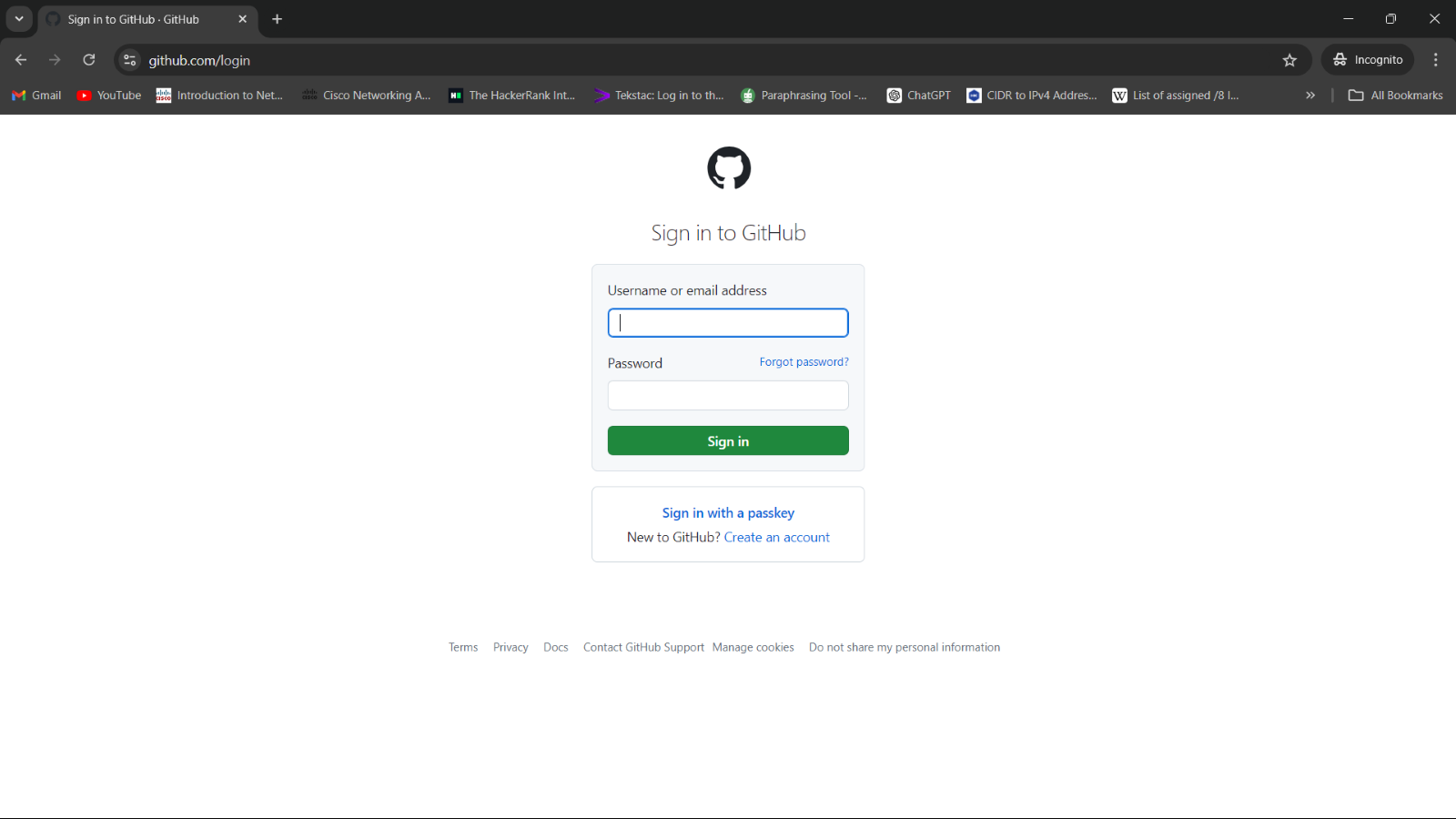


1. Provide IP (Kali-Linux IP) of where the credentials are to be sent back to machine using POST method through harvester.

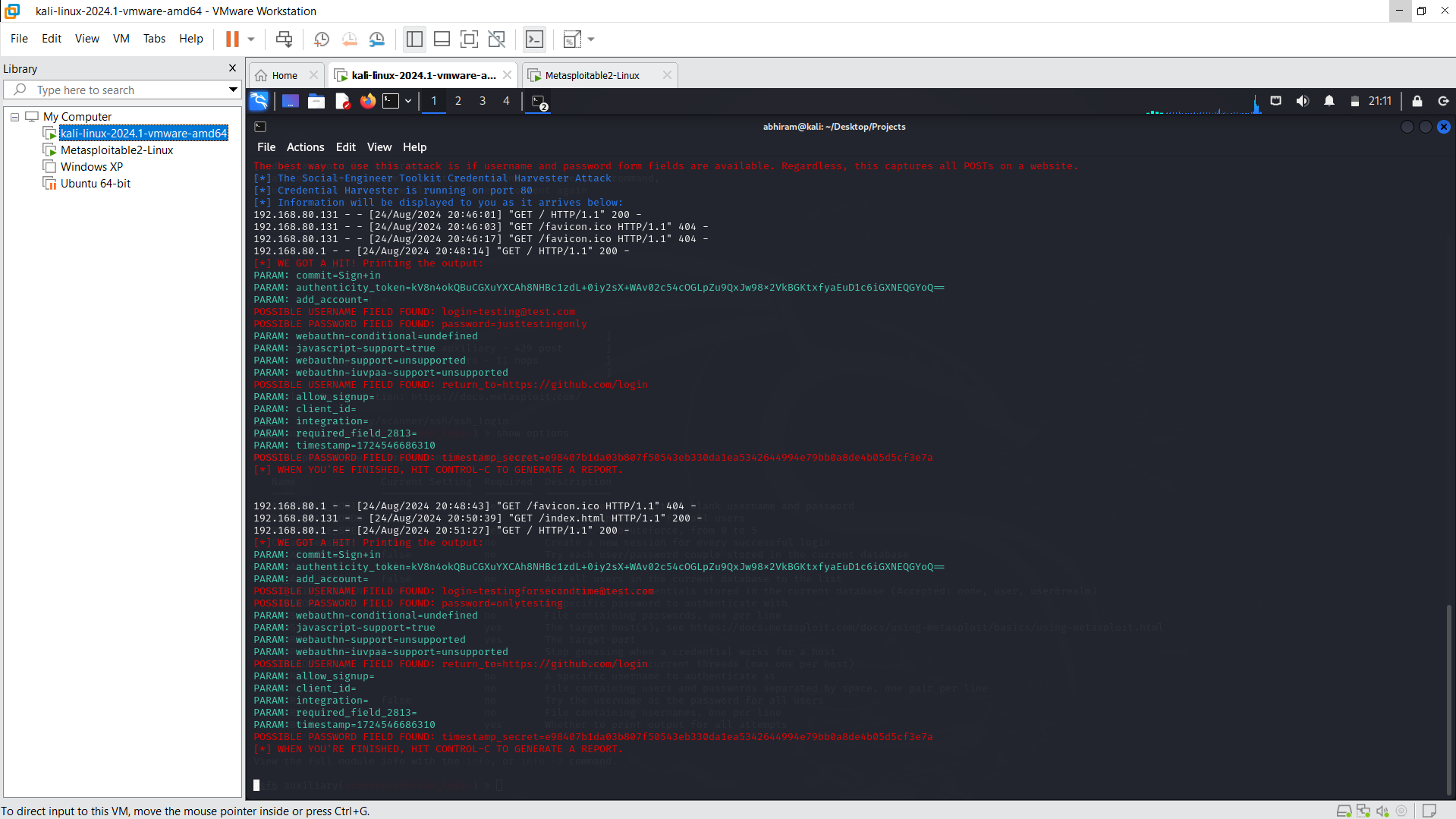
Also, the “github” login site is cloned and used to get the victim’s credentials.

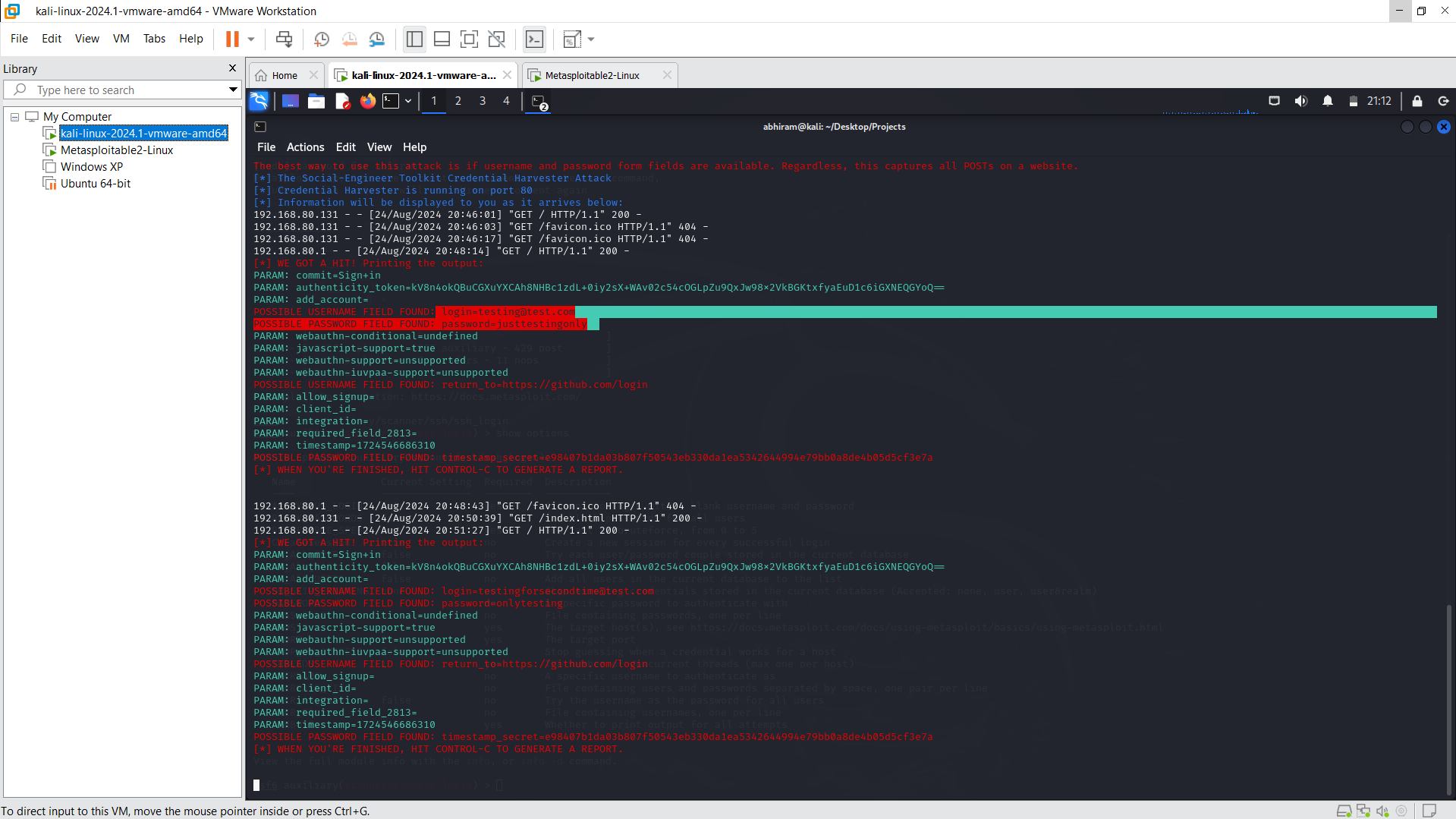


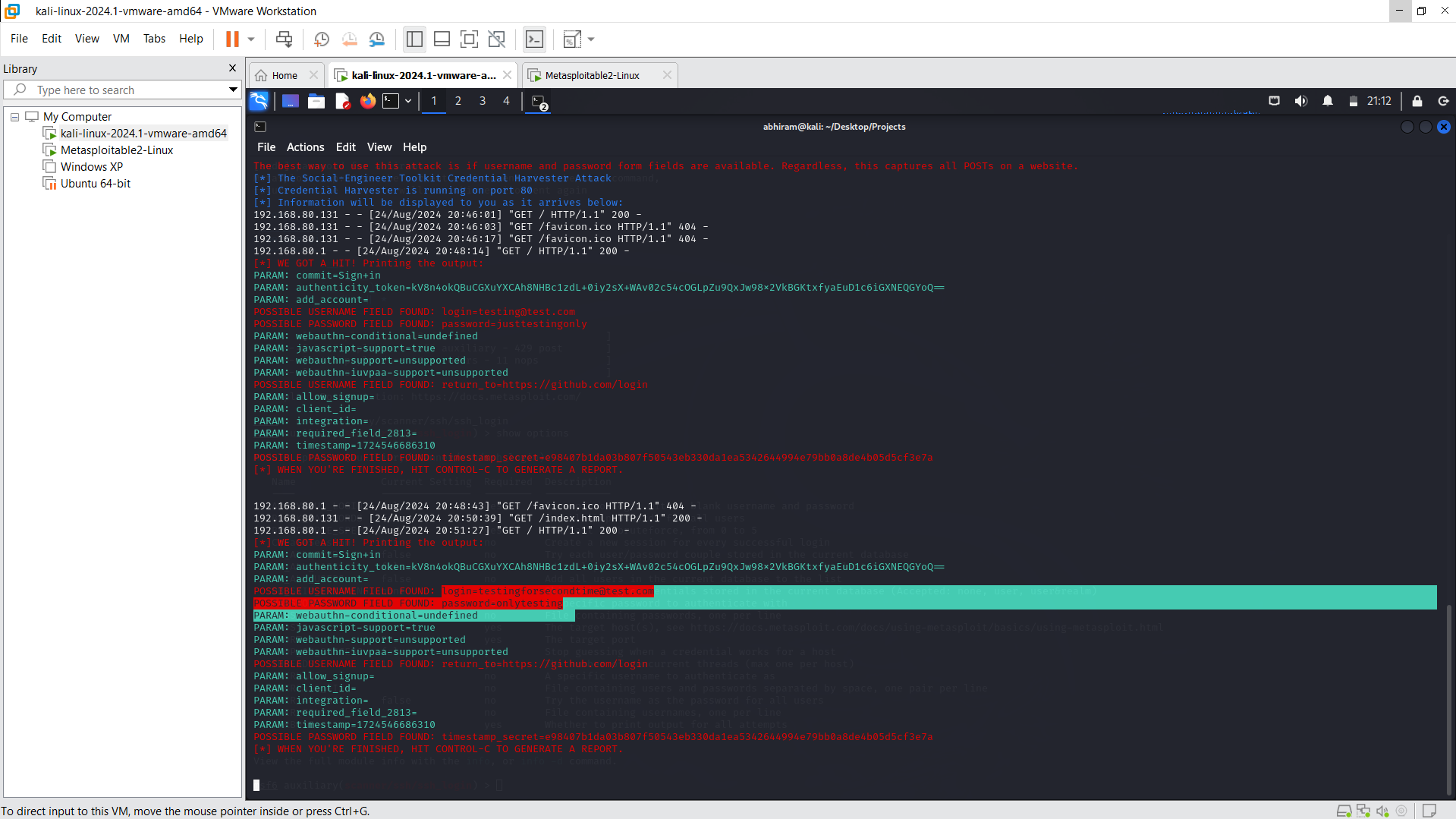
1. The IP of Kali-Linux, when hit on the browser of the same network VM (my local machine), i get the github login page, which resembles the actual github page. When the login credentials are entered in this page, then the page refreshes for the first time and opens an actual login page of github.

1. These entered credentials are saved in the Kali-Linux Social engineering tool kit page, which shows IPs trying to access fake github page and credentials.







1. So, the login credentials are obtained and can be used by attackers to misuse.