Experiment No. 9

Batch:A3 **Roll No.: 16010421119 & 16010421091** **Experiment No.:9**

Aim: Demonstrating self-learning topic

Resources needed: kali linux

Pre Lab/ Prior Concepts:

Theory: The MITRE ATT&CK framework is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. It's structured around the concept of an adversary's tactics, techniques, and procedures (TTPs). MITRE, a not-for-profit organization, developed this framework to help cybersecurity professionals understand and counteract cyber threats more effectively.

The name "ATT&CK" stands for "Adversarial Tactics, Techniques, and Common Knowledge." It provides a comprehensive taxonomy of common tactics and techniques used by attackers during various stages of a cyberattack, from initial reconnaissance to exfiltration of data. The framework is widely used by security teams to assess their defenses, prioritize security investments, and improve incident response capabilities.

MITRE ATT&CK is continuously updated to reflect the evolving tactics and techniques used by cyber adversaries, ensuring that it remains a valuable resource for the cybersecurity community.

Attacks in these experiments:

Attack1 - Phishing

https://attack.mitre.org/techniques/T1566/

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages

Attack2 - Network sniffing

https://attack.mitre.org/techniques/T1040/

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network.

Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol.

Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent Lateral Movement and/or Defense Evasion activities.

Setting up Environment:
steps to set up Kali Linux on VirtualBox:

1. Download Software: Download and install Oracle VM VirtualBox and the Kali Linux ISO from their respective official websites.
2. Create Virtual Machine: Open VirtualBox, click "New", name your virtual machine, choose type as "Linux", version as "Debian", allocate memory (at least 2 GB), and create a virtual hard disk (at least 20 GB).
3. Configure Settings: Select the virtual machine, go to "Settings", under "Storage" select the Kali Linux ISO file, and under "Network" set to "NAT" or "Bridged Adapter".
4. Install Kali Linux: Start the virtual machine, follow the Kali Linux installer instructions for language, timezone, partitioning, and user account setup.
5. Post-Installation Setup: Log in to Kali Linux, update the system (apt update && apt upgrade), install necessary software, and optionally install VirtualBox Guest Additions for better integration.

Procedure:

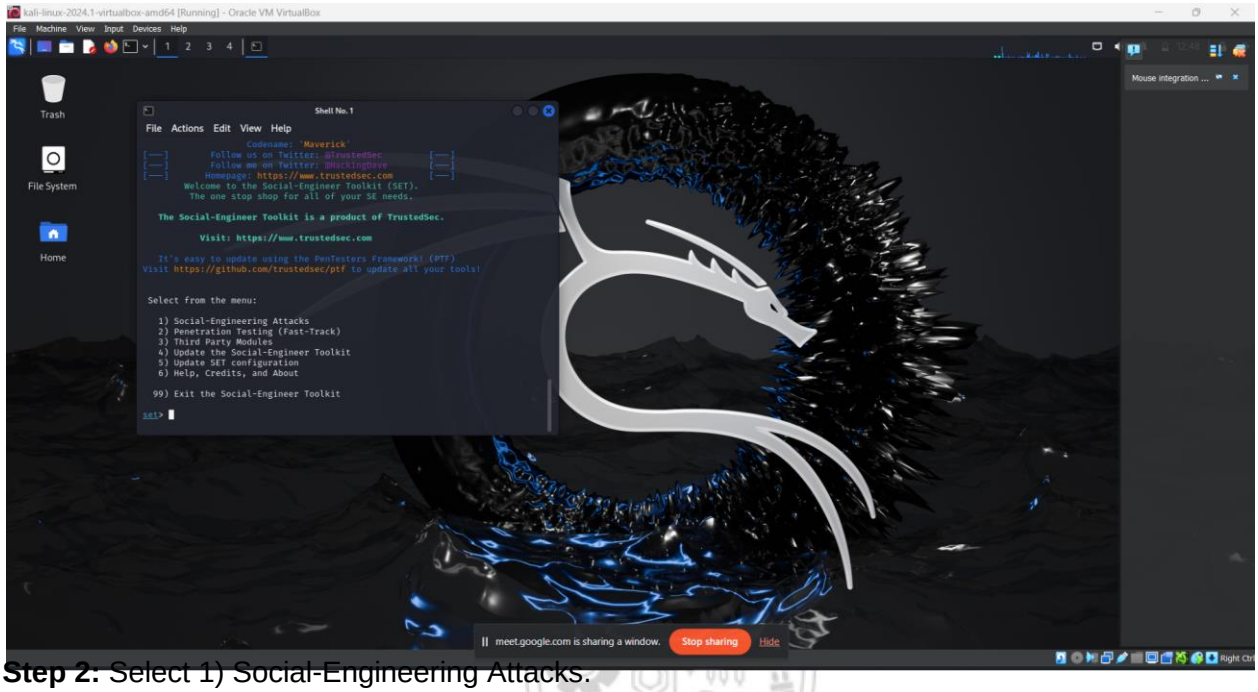
Phishing
Step 1: run `sudo setoolkit`
Step 2: Select 1) Social-Engineering Attacks.
Step 3: Select 2) Website Attack Vectors
Step 4: Select 3) Credential Harvesting Attack Method
Step 5: Select 1) Web Templates
Step 6: Setting up IP address to capture the credentials once the victim submits the form through post method.
Step 7: After setting up IP Address choose web template as Twitter.
Step 8: Cloning the Twitter Login page.
Step 9: Twitter Login page at Local Host.
Step 10: User enters the credentials for fake twitter login page thinking it as Genuine Website.
Step 11: Attacker captures the user's credentials and redirect the user to actual Login page of twitter.

Network sniffing
Step 1: Using command 'ifconfig' to check for IPv4 address and also testing for network connectivity for that address.
Step 2: Run 'sudo responder -I eth0' for responder tool to capture credentials over windows network.
Step 3: Enter the file system by entering the IP of kali into file explorer of windows and enter the user ID password
Step 4: Without entering any credentials we were able to capture hashed password of the user computer

Output(Code with result Snapshot)

Phishing

Step 1: run `sudo setoolkit`

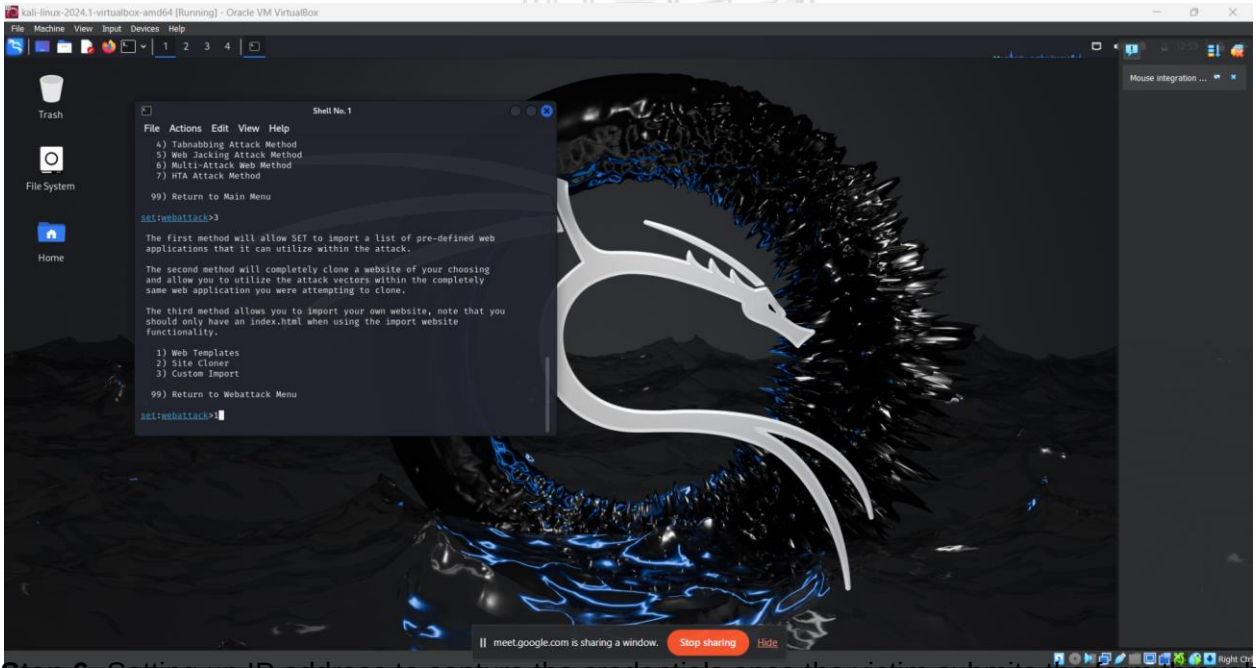


Step 2: Select 1) Social-Engineering Attacks.

Step 3: Select 2) Website Attack Vectors

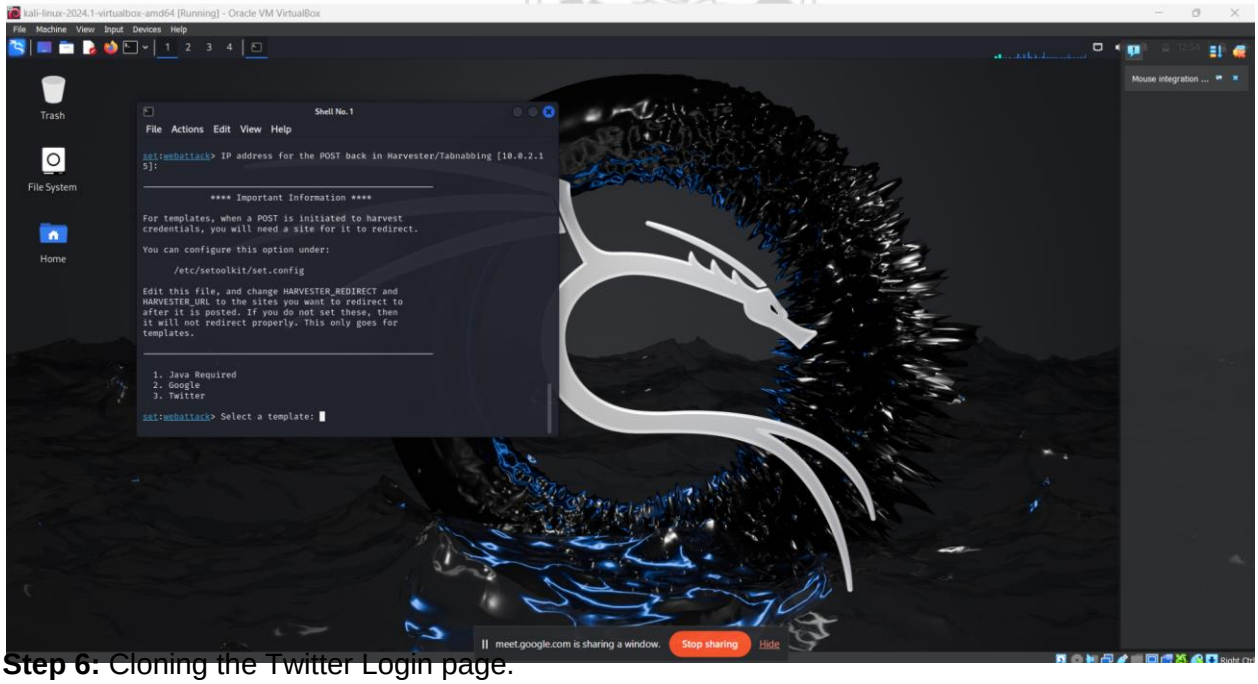
Step 4: Select 3) Credential Harvesting Attack Method

Step 5: Select 1) Web Templates



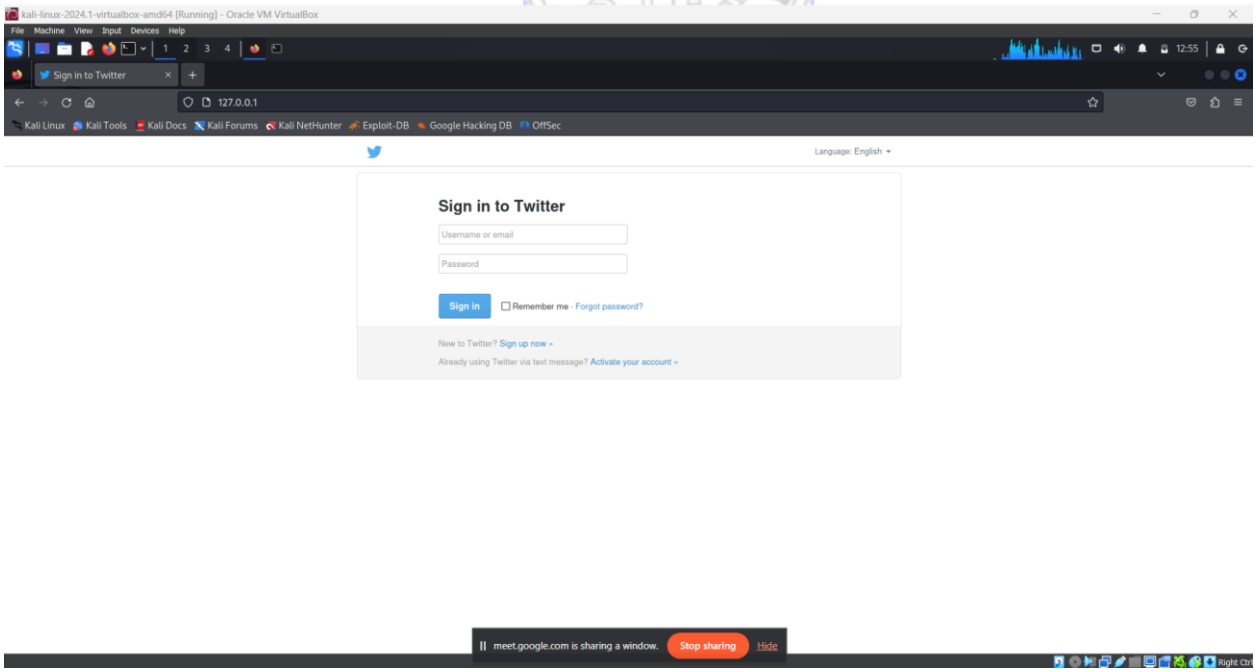
Step 6: Setting up IP address to capture the credentials once the victim submits the form through post method.

Step 7: After setting up IP Address choose web template as Twitter.

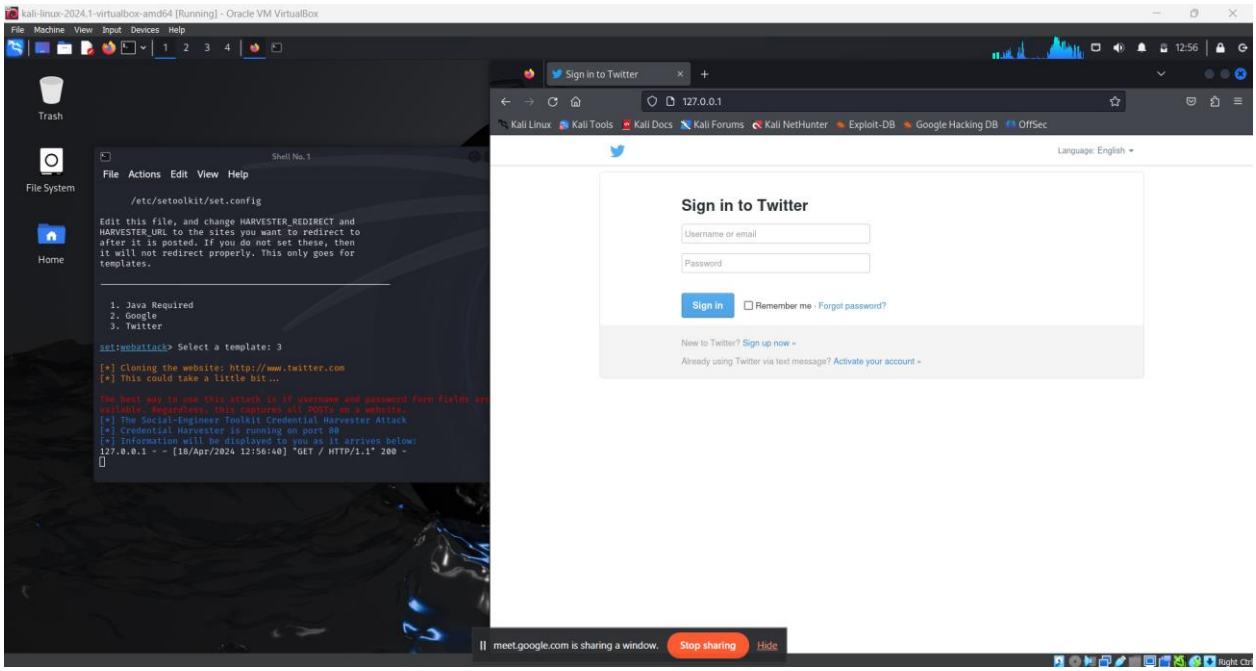


Step 6: Cloning the Twitter Login page.

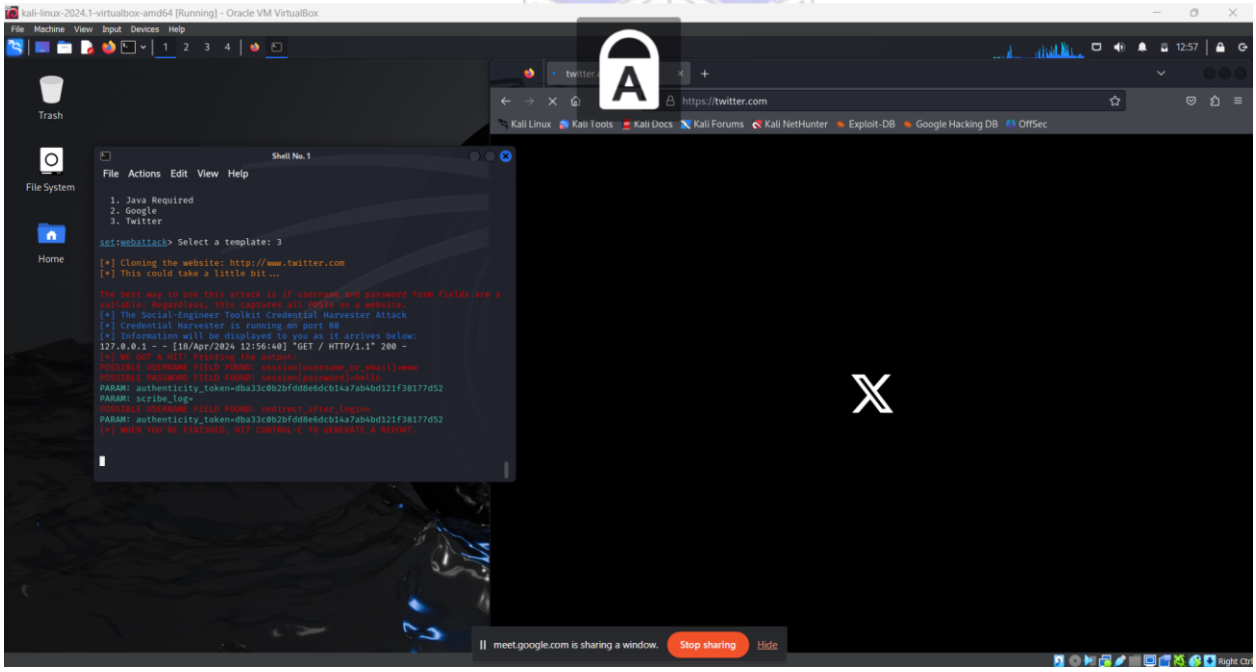
Step 7: Twitter Login page at Local Host.



Step 8: User enters the credentials for fake twitter login page thinking it as Genuine Website.



Step 9: Attacker captures the user's credentials and redirect the user to actual Login page of twitter.

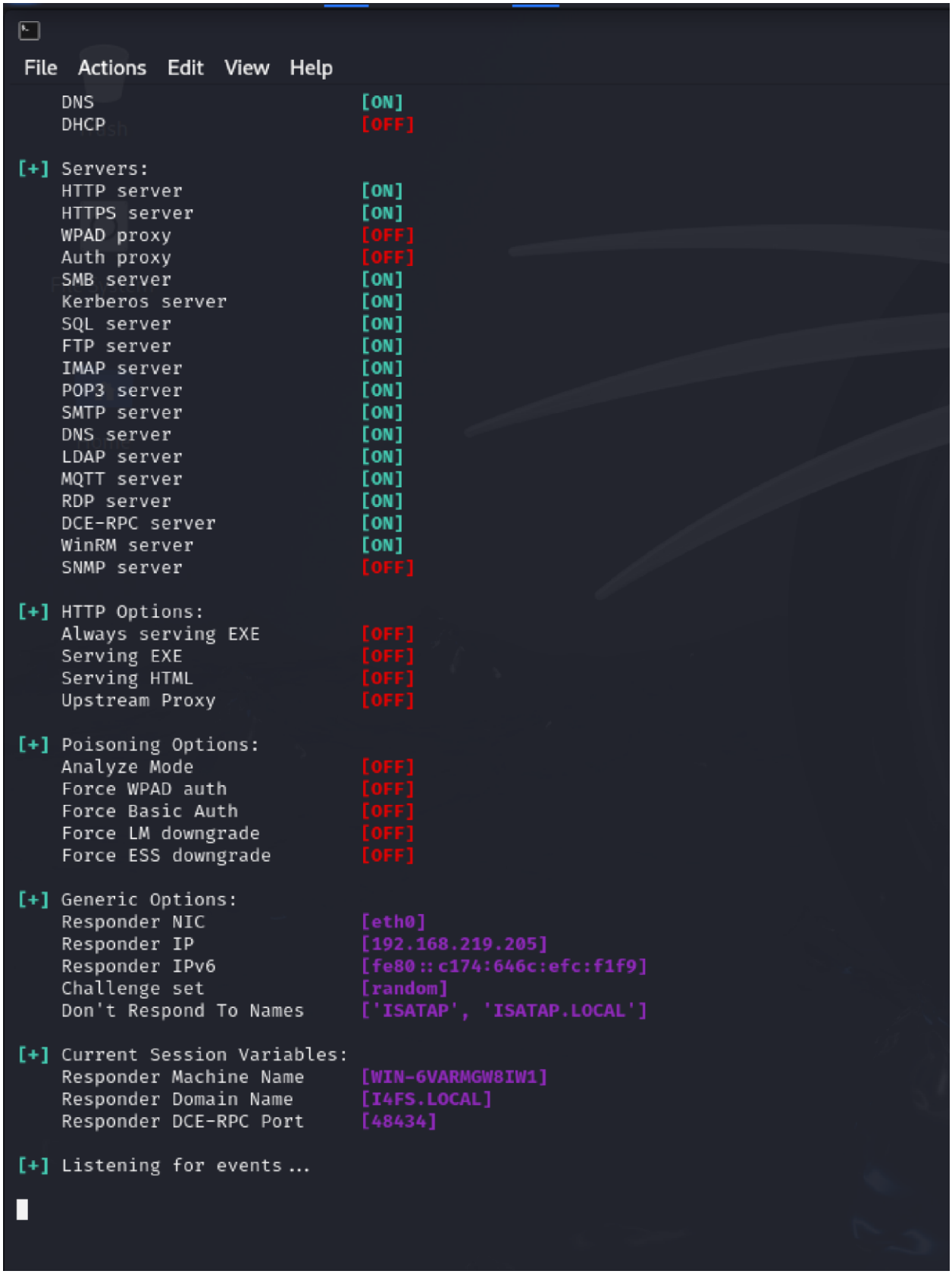


Network sniffing

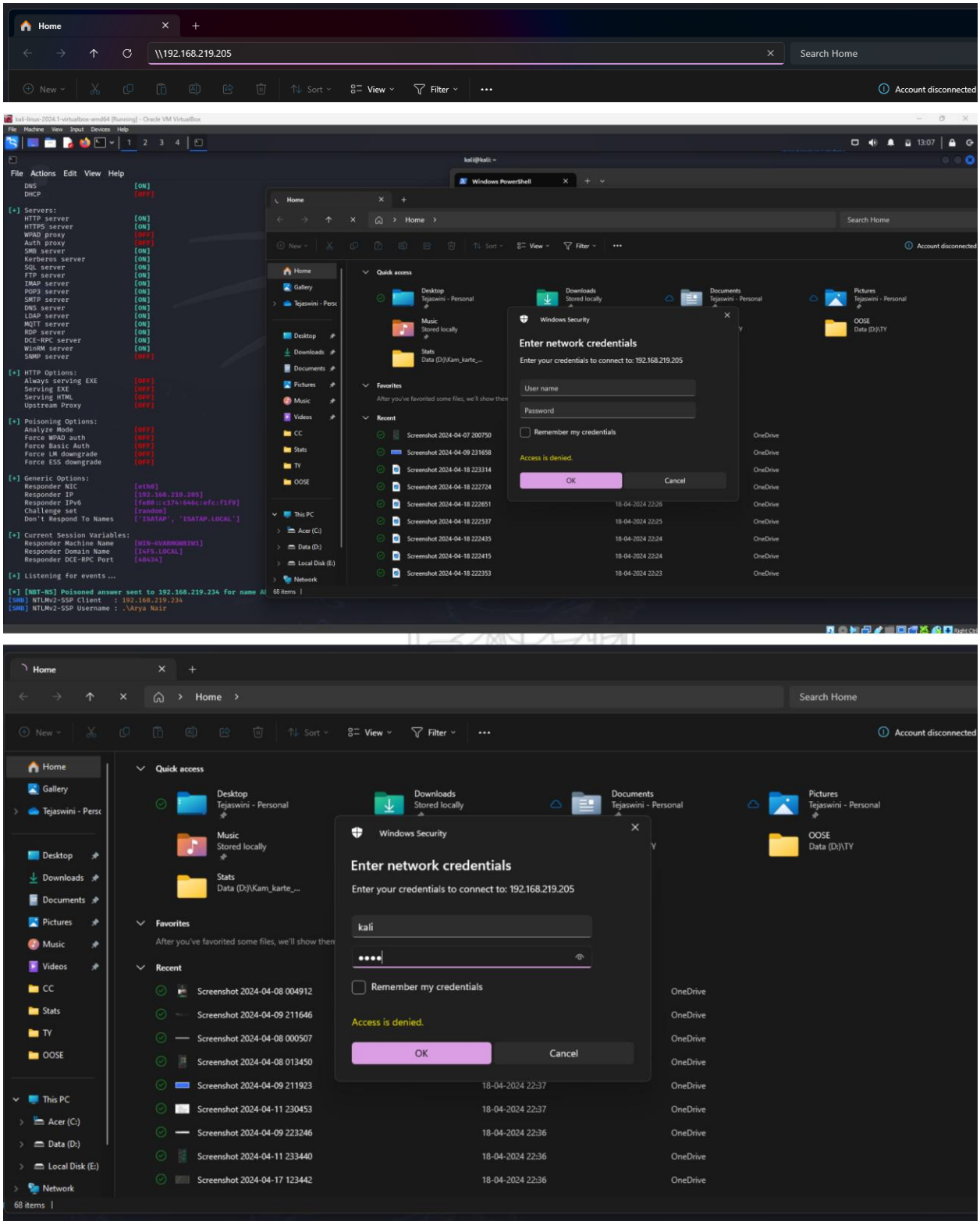
Step 1: Using command 'ifconfig' to check for IPv4 address and also testing for network connectivity for that address.

Step 2: Run ‘sudo responder -I eth0’ for responder tool to capture credentials over windows network.


File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth0
[sudo] password for kali:
NBT-NS, LLMNR & MDNS Responder 3.1.4.0
To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [OFF]
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
SNMP server [OFF]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]



Step 3: Enter the file system by entering the IP of kali into file explorer of windows and enter the user ID password



Step 4: Without entering any credentials we were able to capture hashed password of the user computer

Outcomes:CO3 Understand attack methodology

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Explore MITRE Attack framework and implement the same

Signature of faculty in charge with date