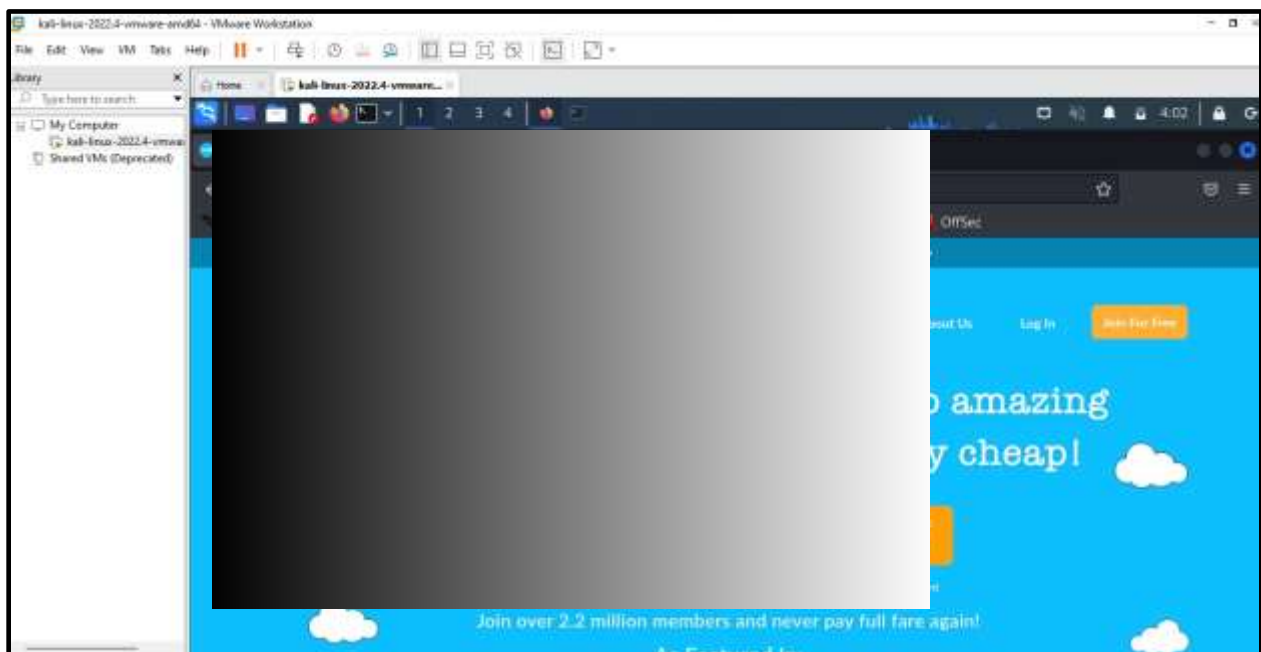


VAPT REPORT [REDACTED] OF [https://\[REDACTED\].com](https://[REDACTED].com)

Summary of the Web site-

- **Founded by** - [REDACTED] Wintermantle
- **Purpose** - It is a travel agency website and mobile app focusing on helping users find the best and cheapest flights, using flight deal alerts and price tracking.
- **Status** - There are over 2.2 million members in the United Kingdom and the United States.

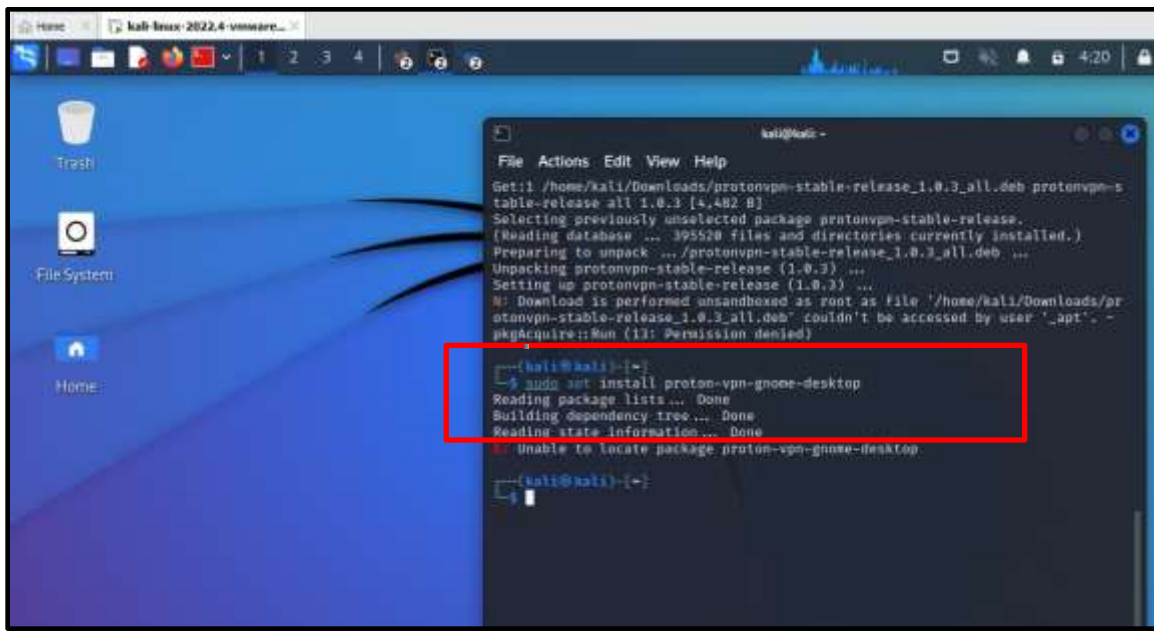
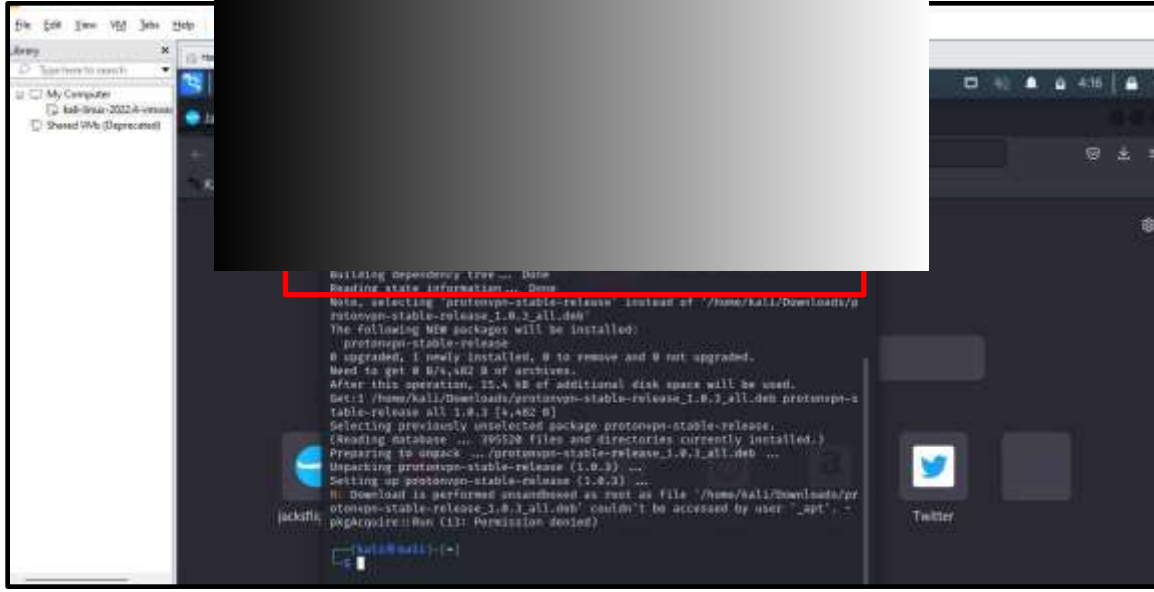


VAPT [REDACTED] process details-

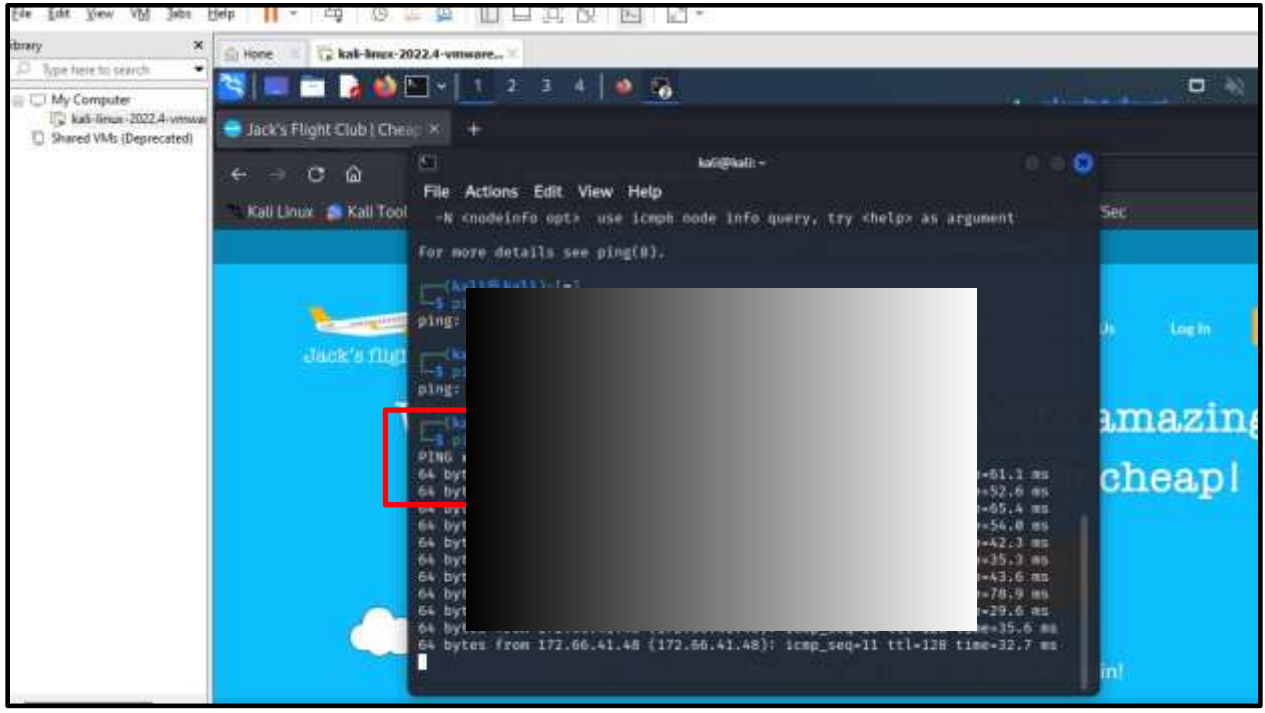
- Web scan, Network scan, Application scan and open source tools mainly utilized
- The detail information shown with screenshots to identify the vulnerabilities
- The Remedial Action Plan for the threats to overcome the security breaches.

Initialization (Reconnaissance through the identity)-

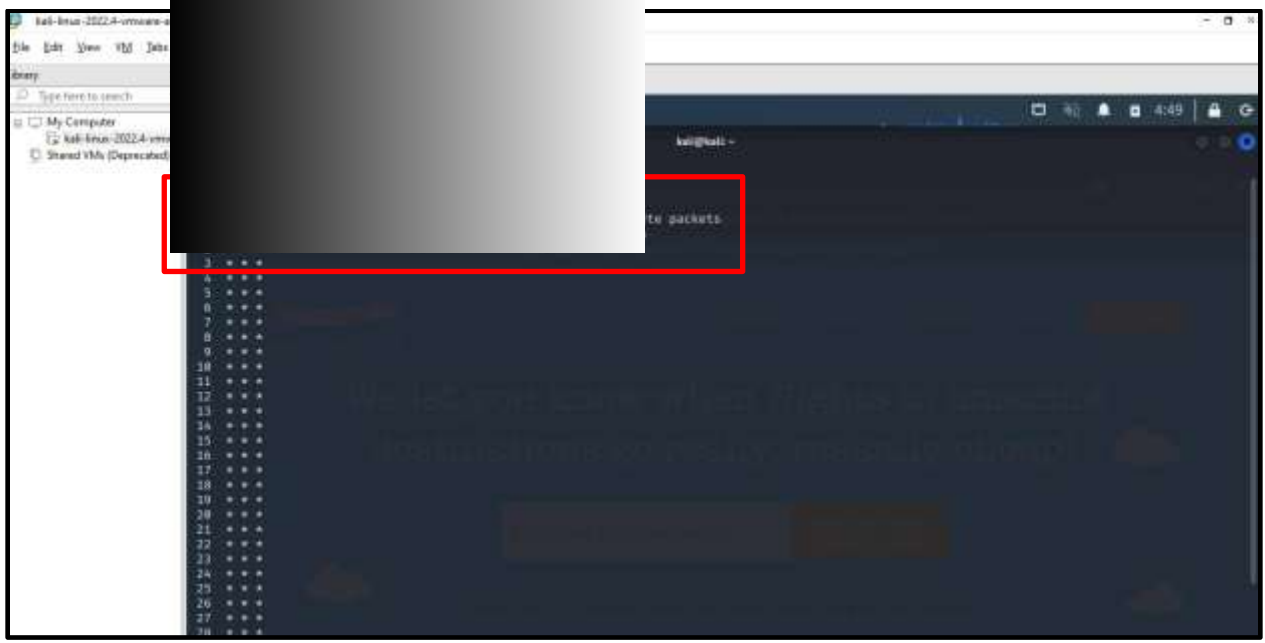
- Install



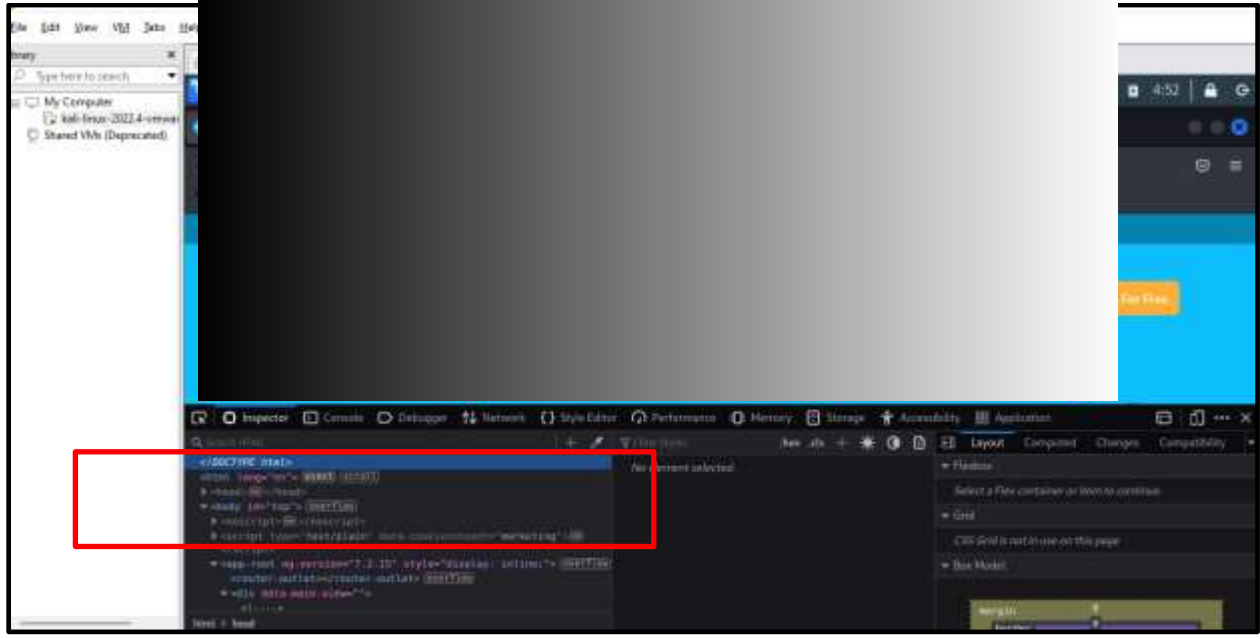
Identification of the IP through Kali Linux-



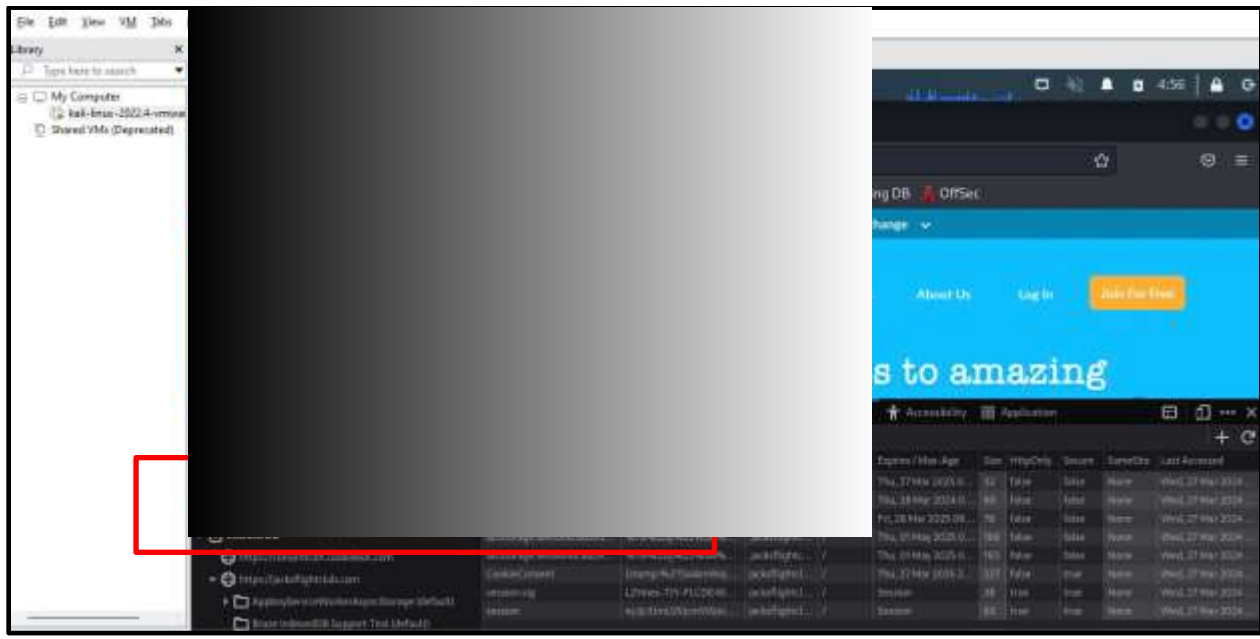
The Network Path Detection-



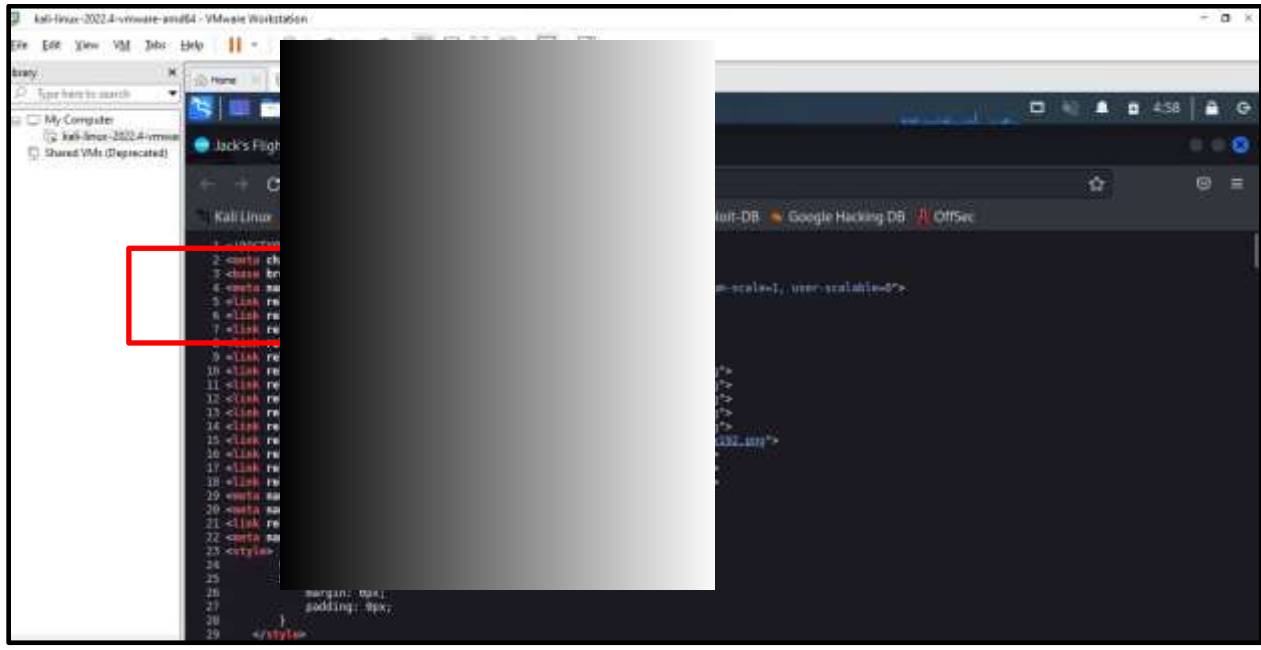
The Insp Language



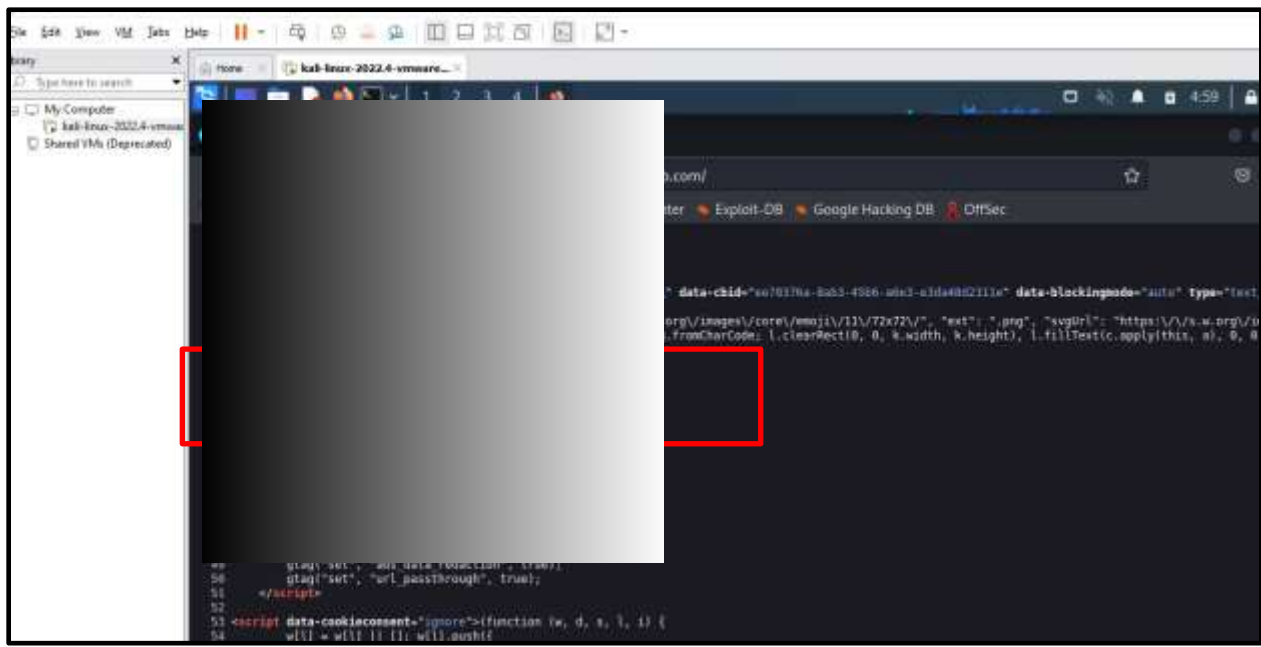
Identification of the Web designed company-



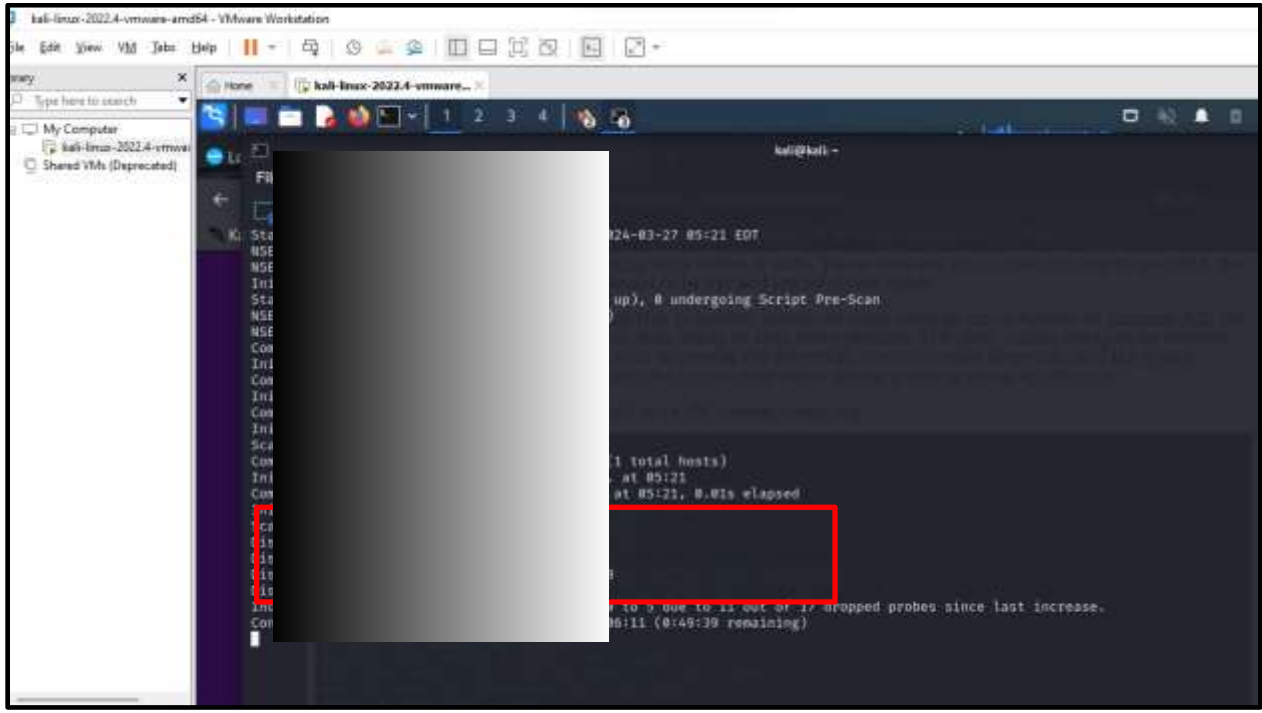
Identification of the Page Source 1-



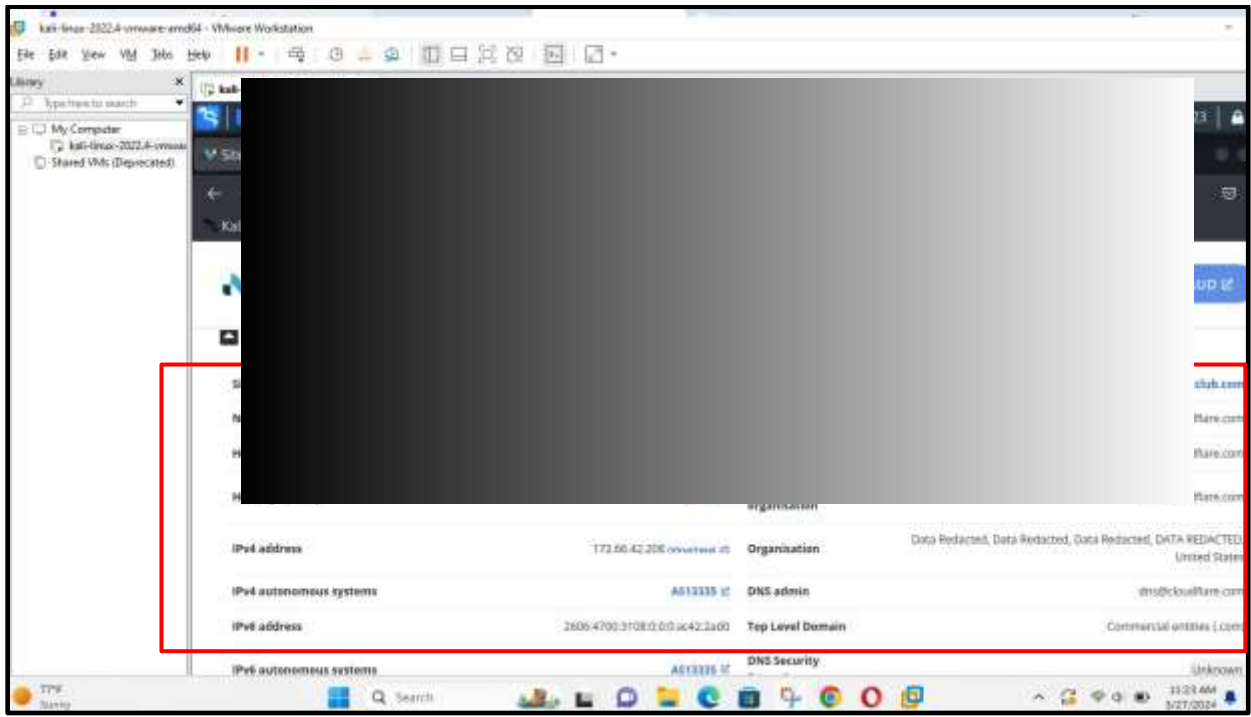
Identification of the Page Source 2-



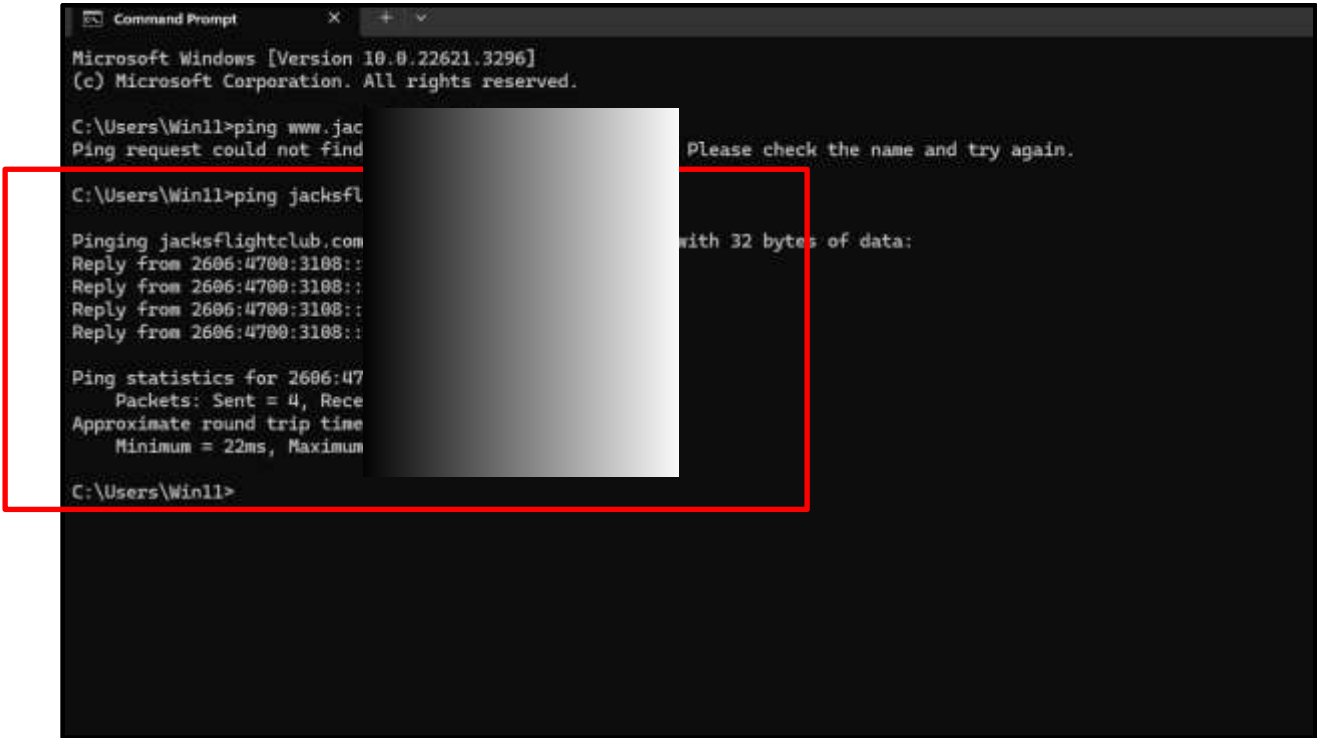
Open Ports Detection through NMAP-



Netcraft to obtain IPV4 and Server Information-



IPV6 Information-



```
Microsoft Windows [Version 10.0.22621.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Win11>ping www.jack
Ping request could not find

Please check the name and try again.

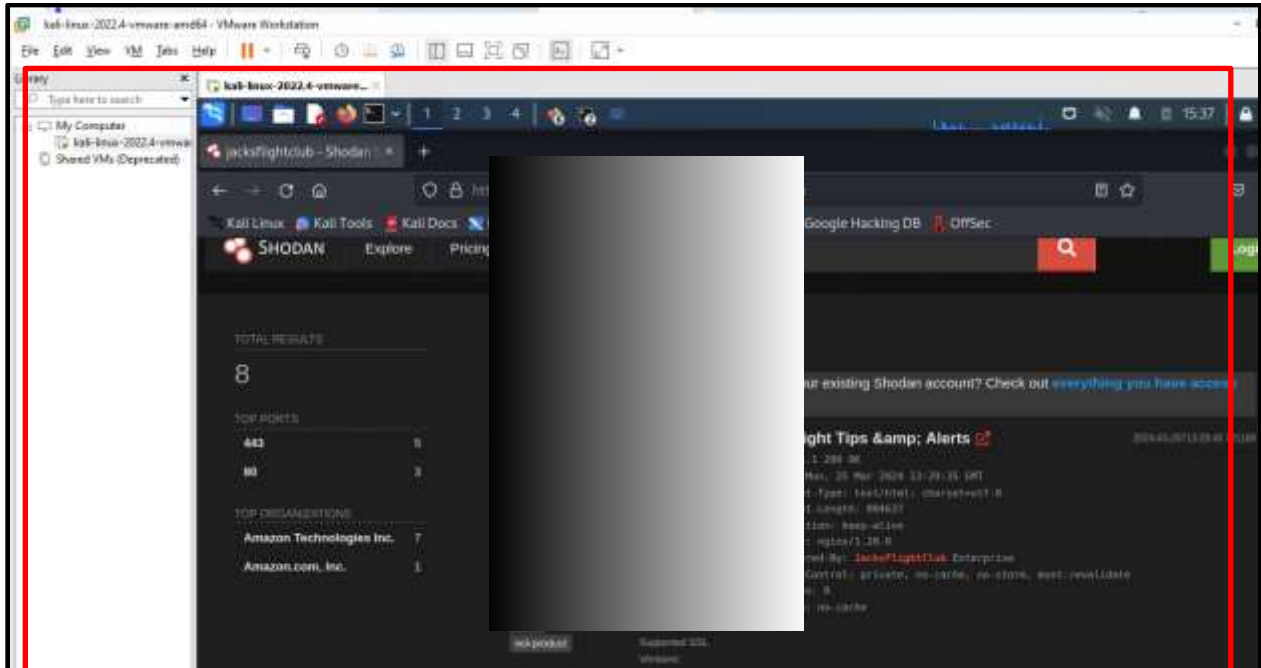
C:\Users\Win11>ping jacksfl

Pinging jacksflightclub.com
Reply from 2606:4700:3108::
Reply from 2606:4700:3108::
Reply from 2606:4700:3108::
Reply from 2606:4700:3108::

Ping statistics for 2606:47
Packets: Sent = 4, Rece
Approximate round trip time
Minimum = 22ms, Maximum

C:\Users\Win11>
```

SHODAN Information to obtain Top ports and Top Organizations-

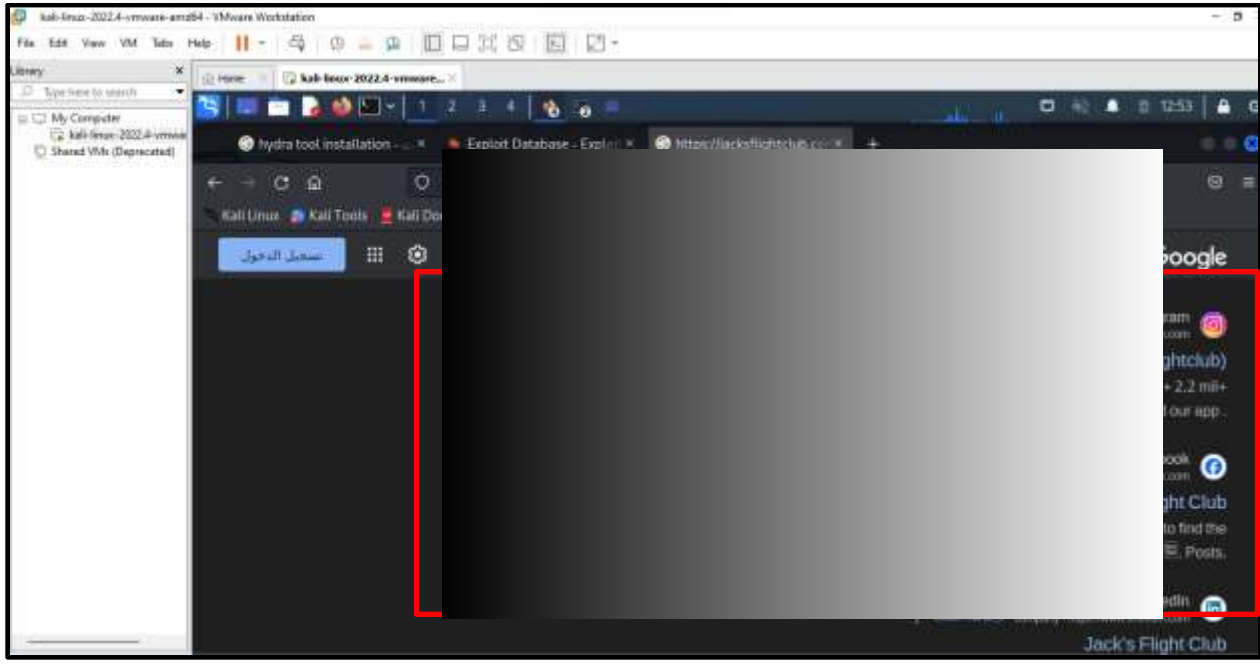


The screenshot shows the SHODAN search results for the query 'jacksflightclub-shodan'. The interface includes a search bar, navigation tabs for 'SHODAN', 'Explore', and 'Pricing', and a summary of search results.

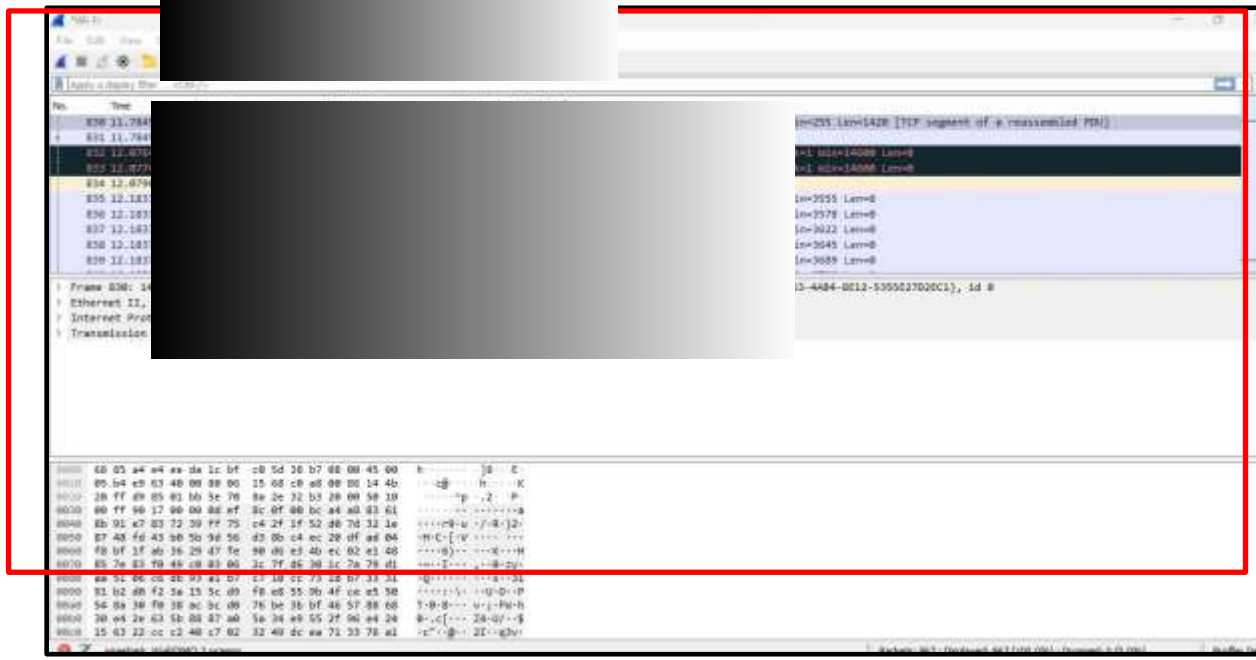
Category	Value
TOTAL RESULTS	8
TOP PORTS	443 (8)
TOP ORGANIZATIONS	Amazon Technologies Inc. (7)
	Amazon.com, Inc. (1)

The results list includes details for a specific host, such as IP address (2606:4700:3108::), status (http-alive), and organization (jacksflightclub Enterprise).

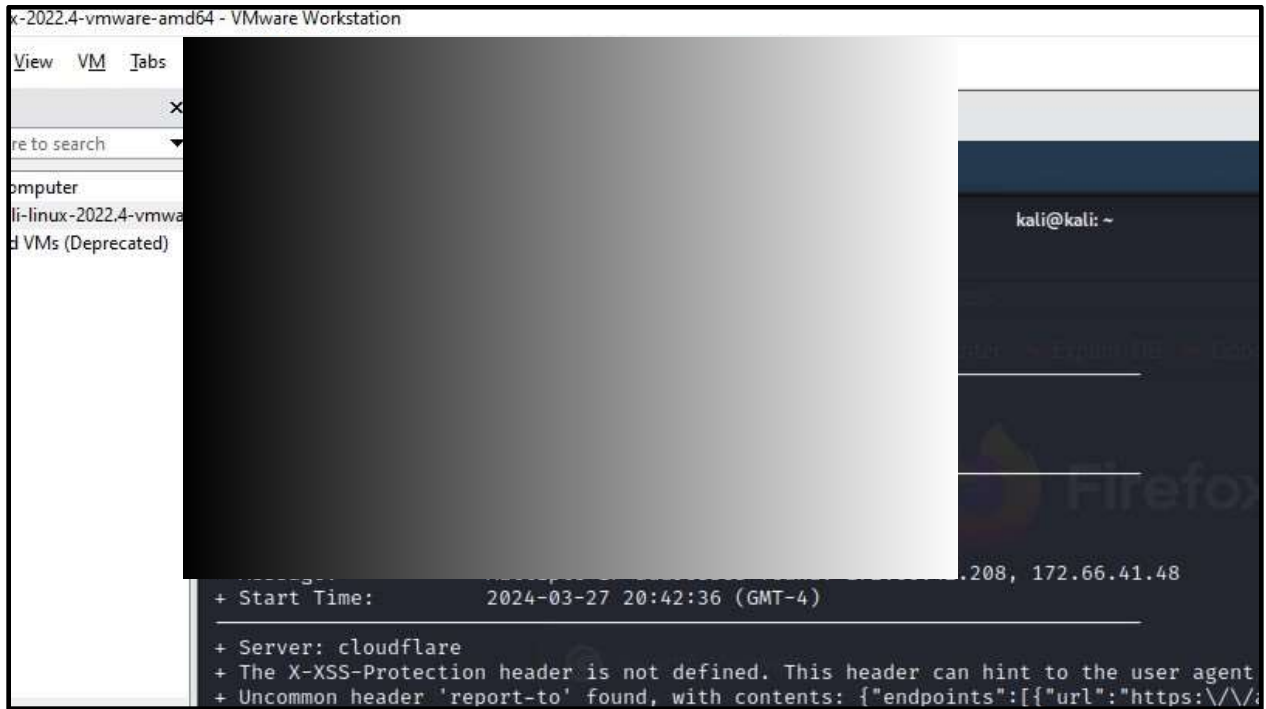
Google Exploit to know the Social Media Presence Information -



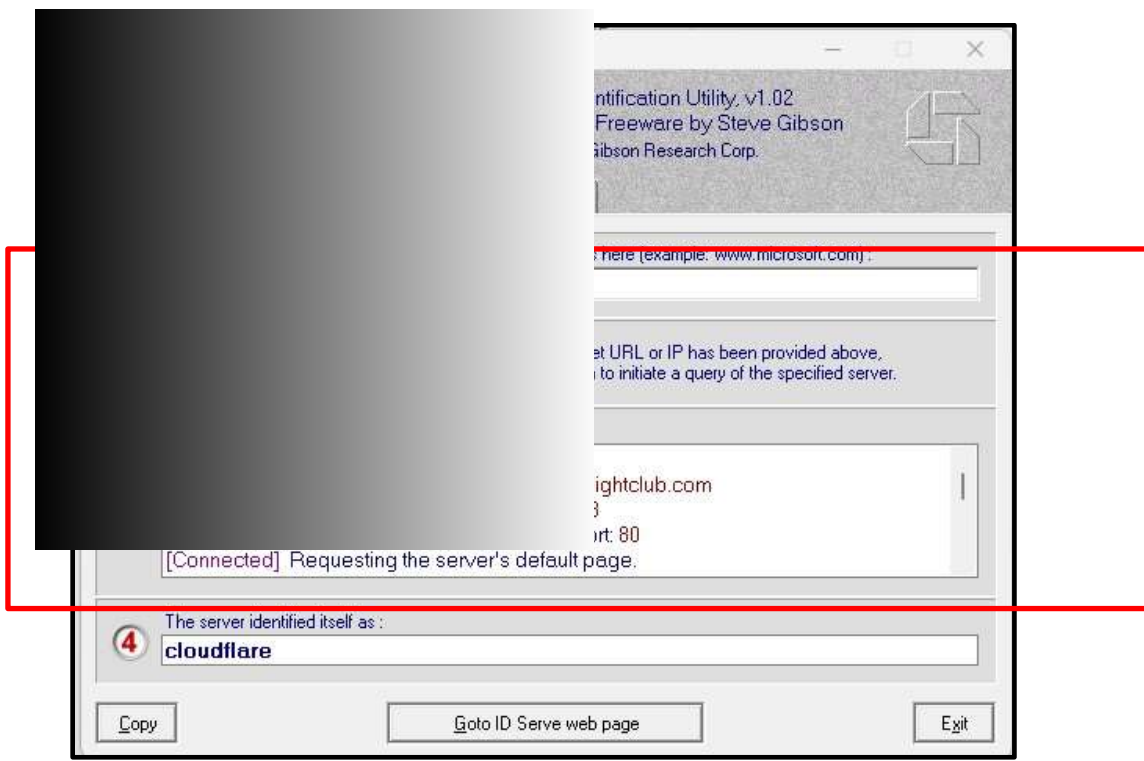
The TCP ARP ACK Source and Destination info of the https://blackofflightclub.com by using Wireshark-



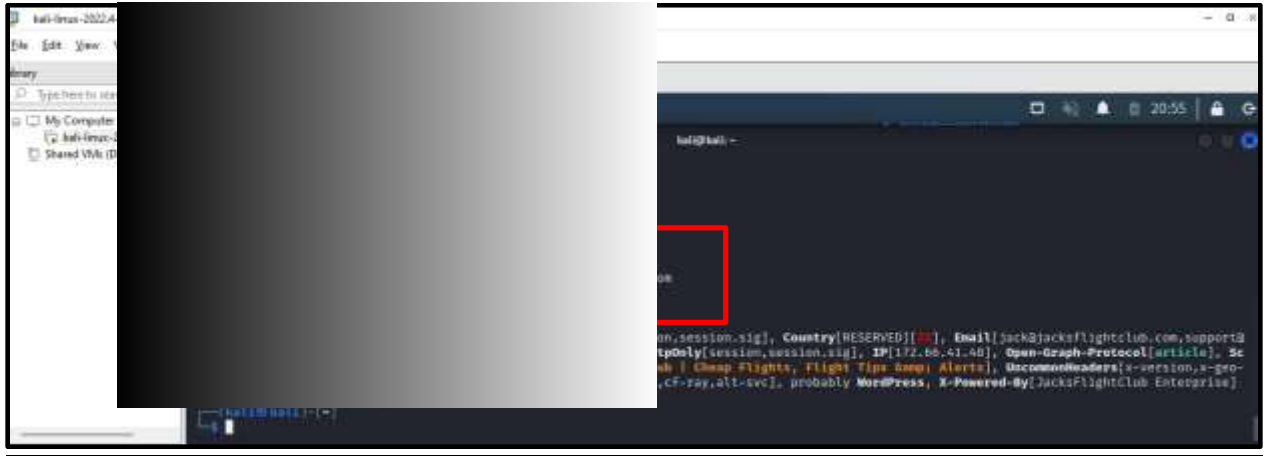
Nikto to Detect IP, Hostname, Port and etc., -



ID Serve to obtain Web Site Information -



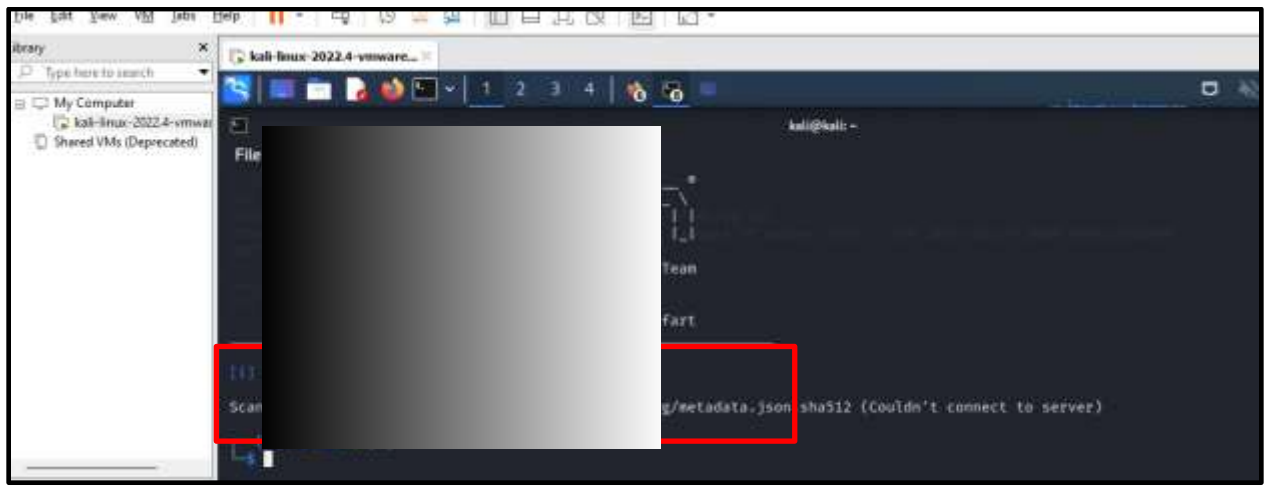
Whatweb to obtain Web Site Information -



Webdata Extractor to obtain Web Site Information –



WpScan Extractor to obtain Web Site Information (Processing)-



SQLmap Extractor to obtain Web Site Information (Processing)-



Ghost in Web Site Information

```
msf5> use multi/http/ghost
msf5 multi/http/ghost >

# Job
# Bul
# Web
# list
# Fac
# Fac
# Fac
# You
# www

# Cre
# www

#####

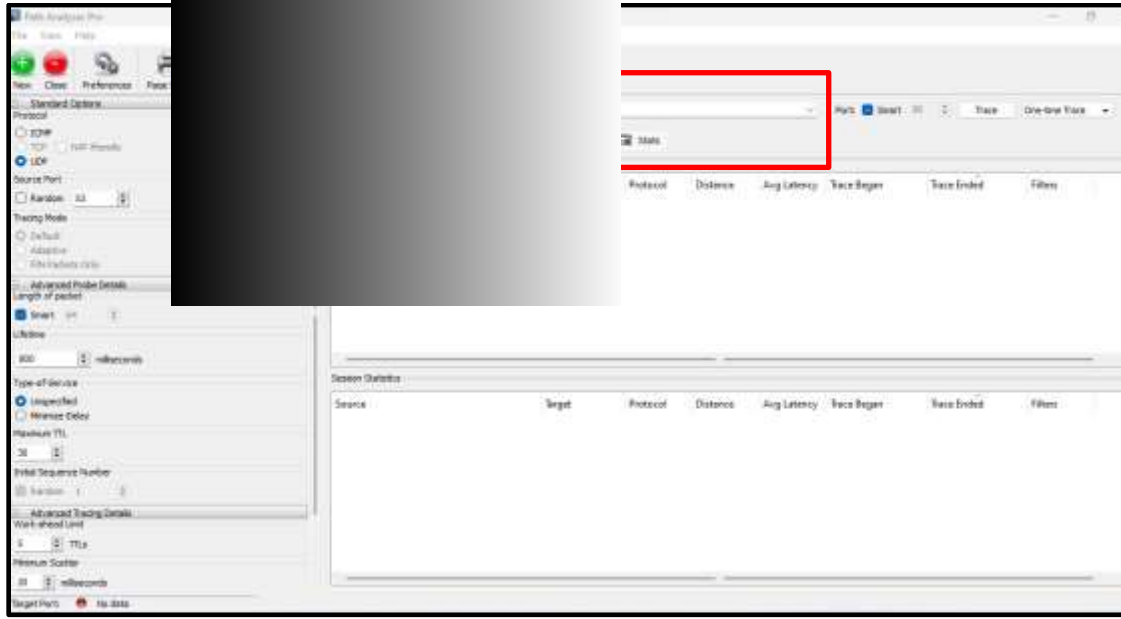
# A notice to all nerds and n00bs...
# If you will copy the developer's work it will not make you a hacker..!
# Respect all developers, we doing this because it's fun...

#####

from bs4 import BeautifulSoup
from collections import deque
import json
import mmap
import os
import re
import requests
import requests.exceptions
import time
from time import gmtime, strftime
from urllib.error import URLError
from urllib.parse import urlsplit
import urllib3
import urllib3.request
```

Path Analysis (Process)

Web Site Information



Summery (Identified Information)-

- IP addresses
- Open ports
- Host websites information
- Web Programming information (Language, Databases)
- Email addresses
- Web site complete information
- Login information

- **Web logs and Web initiative information**
- **Web vulnerabilities**
- **Payloads accessibilities**
- **Clear the tracks (VPN use)**
- **All the stakeholders and insights**