plan

Well just paste thing here, later on ill make it into latex for final draft.
But paste it as if its fair. Without mistakes and with images and stuff.

general instructions

1. While pasting make sure links are not present
2. Whatever you take reference from, add it to references
3. Add images with your text
4. Make it atleast 2 3 pages for your content.

grp ppl and topic distribution

1. Khare :
2. karad :
3. Krish :

well start from next page.

KHARE'S CONTENT …..

Alternative softwares we can use -

1. SOCIALPHISH

Socialphish is an open-source phishing tool with a lot of features. Socialphish, which is used to conduct phishing attacks on targets, is growing increasingly popular. Socialphish is easier to use than Social Engineering Toolkit. Socialphish includes various templates created by another tool called Socialphish. Socialphish provides phishing templates for 33 famous websites, including Google, Facebook, Github, Yahoo, Snapchat, Spotify, Linkedin, Microsoft, Yahoo, Github, etc.

Socialphish also allows users to utilize a custom template. This tool makes phishing attacks simple to carry out. They can use a lot of creativity to make the email appear as real as possible.

FEATURES OF SOCIALPHISH -

1. Socialphish is an open source tool.
2. Socialphish is a very simple and easy tool. Socialphish is written in bash language.
3. It is a lightweight tool. It does not take extra space.

2. SHELLPHISH

ShellPhish is a tool that we can use to create phishing pages for the most prominent social networking sites, such as Facebook, Twitter, and Instagram. The application includes phishing templates for 18 well-known websites, the bulk of which are social media and email providers. This tool makes it simple to carry out a phishing attack. We can execute phishing in this tool (wide area network). We can use this tool to get ID and password credentials.

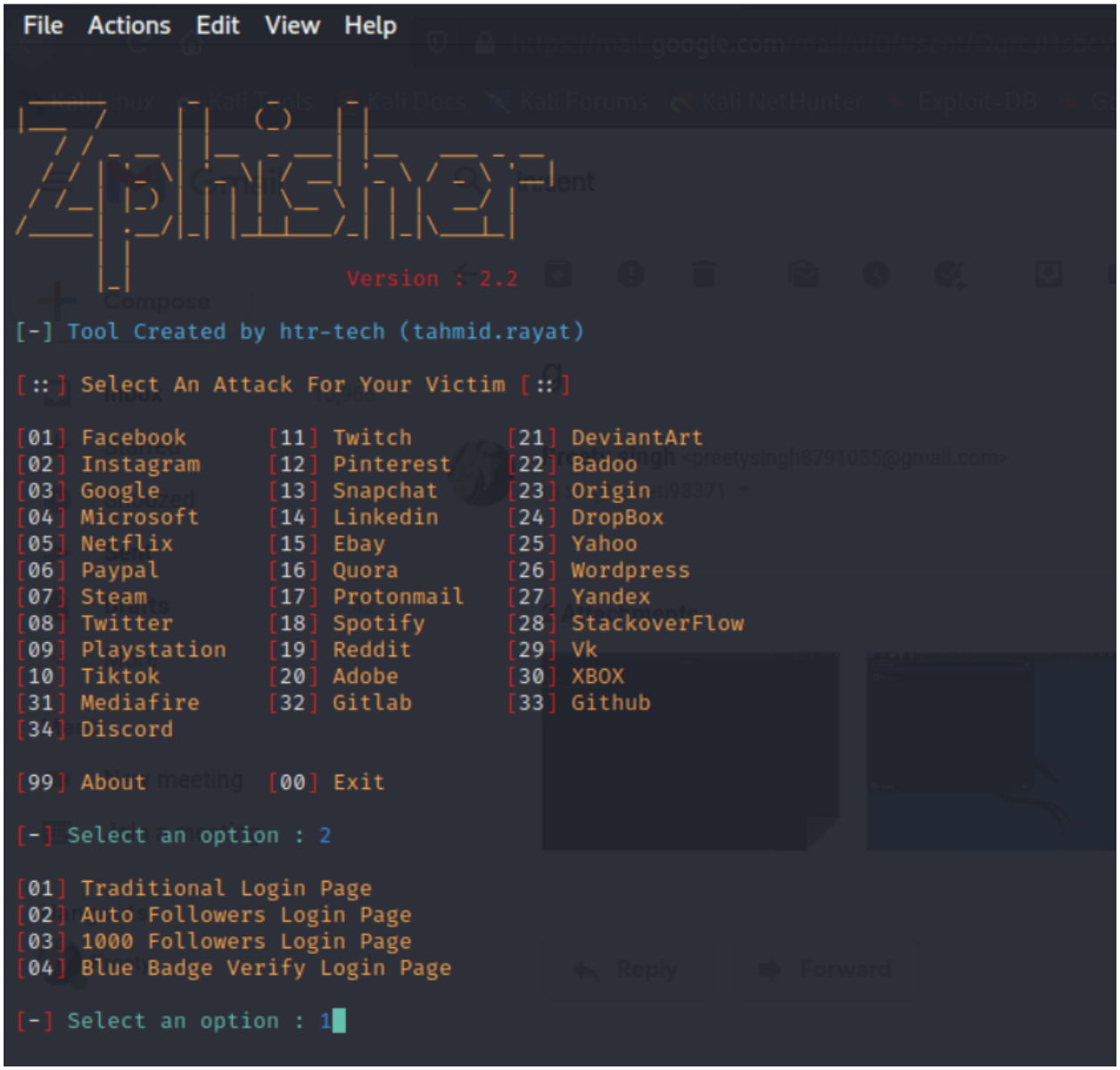
3.ZPHISHER

Zphisher is an open-source phishing tool with a lot of features. It has become increasingly popular in recent years for phishing attacks on Target. Zphisher is less difficult to use than the Social Engineering Toolkit. It includes various templates generated by a tool called Zphisher.

FEATURES OF ZPHISHER-

1.Zphisher is an open-source tool.
2. We can use Zphisher in phishing attacks.

3.The Zphisher tool is a simple and easy tool.
4. Zphisher is written in bash language.



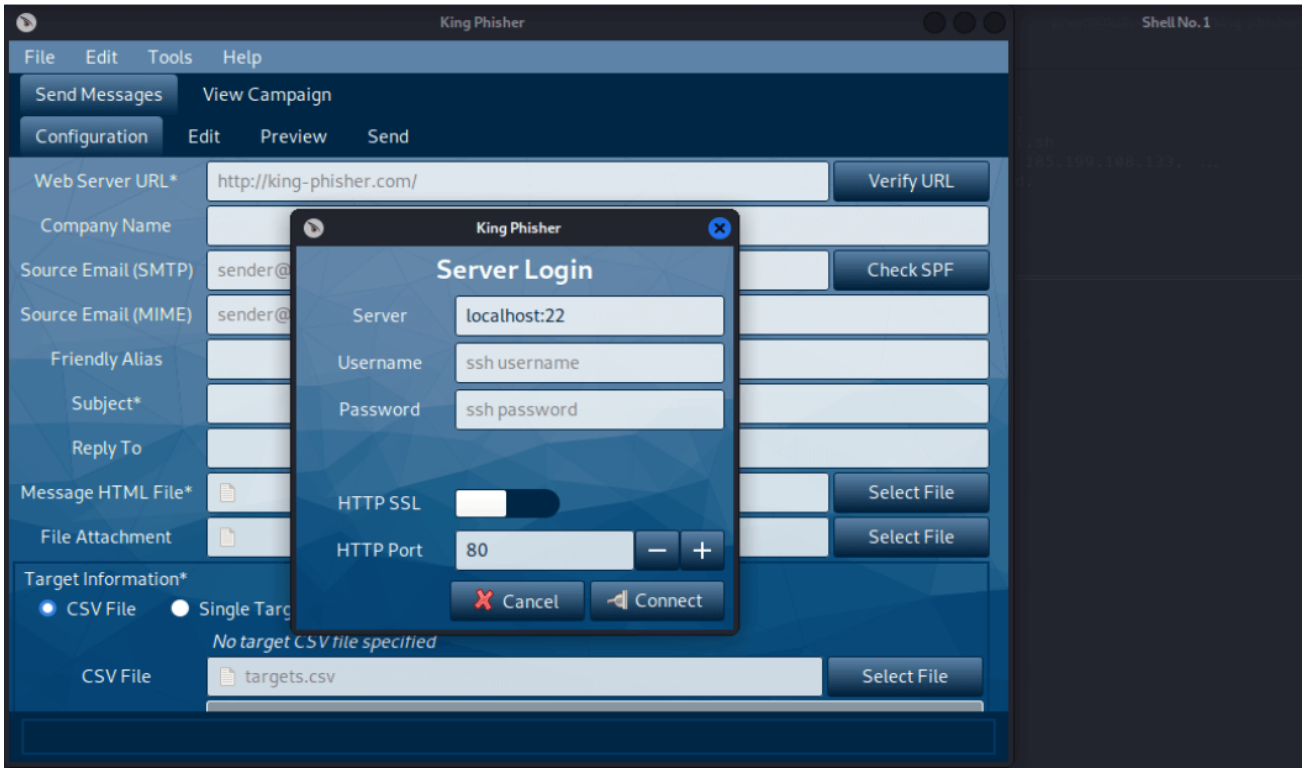
4.KING-PHISHER

King Phisher is a tool that simulates real-world phishing attacks in order to test and promote. It is an open-source tool that can simulate real-world phishing attacks. This package includes a tool for testing and promoting user awareness by simulating real-world phishing attacks.It is a user-friendly yet extremely flexible architecture that gives us complete control over email and server content. King Phisher can be used to

perform campaigns ranging from basic awareness training to more complex scenarios where user-aware content is served for credential harvesting.

FEATURES OF KING-PHISHER -

1.Run multiple phishing campaigns.
2.Optional Two-factor authentication.
3.SMS *alerts* regarding campaign status.
4.Web page cloning capabilities.



5.BLACKPHISH

Blackphish is an open-source phishing tool with a lot of features. Blackphish, which is used to conduct phishing attacks on Target, is growing increasingly popular. The Social Engineering Toolkit is more difficult than Blackphish.

REQUIREMENTS-

1. Compatible system.
2. Python 3
3. PHP

4. Apache2
5. npm

Wireshark:

Methodology:

Wireshark is a network protocol analyzer that allows you to capture and inspect the data traveling back and forth on a network in real-time. Its methodology involves the following steps:

Capture Packets:
- Wireshark captures packets from the network in promiscuous mode, meaning it captures all packets regardless of the destination.

Filtering:
- You can apply various filters to focus on specific types of traffic, such as HTTP, TCP, UDP, etc., making it easier to analyze specific aspects of the network communication.

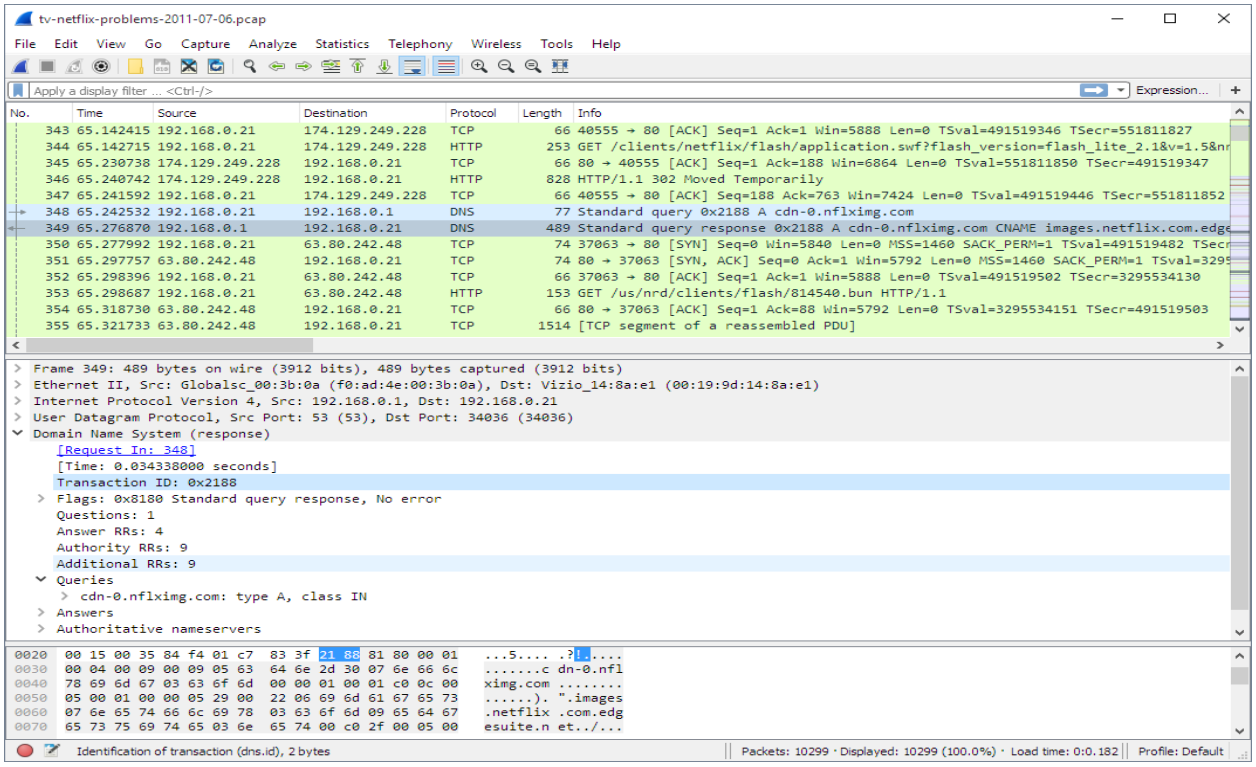
Analysis:
- After capturing packets, Wireshark provides a detailed analysis of the captured data. It decodes the protocols used in the communication and displays the information in a readable format.

Follow Streams:
- Wireshark allows you to follow a particular stream of communication, making it easier to understand the flow of data between devices.

Statistics:
- Wireshark provides statistical information about the captured packets, such as the number of packets, data rate, and protocol distribution.

Protocol Hierarchy:
- It shows the protocols used in the captured data in a hierarchical manner, helping to identify the different layers of the network stack involved.

Export and Save:
- You can export and save the captured data for further analysis or share it with others.



Understanding:

Wireshark helps network administrators, security professionals, and developers in understanding network behavior. It provides insights into how devices communicate, identifies potential issues, and aids in troubleshooting network problems. Understanding Wireshark involves grasping the basics of networking protocols, packet structure, and being able to interpret the captured data.

Explanation:

Wireshark is a versatile tool used for network analysis. It captures packets from a network, allowing users to inspect the details of each packet. The tool supports various filters and display options to focus on specific aspects of network traffic. By analyzing the captured data, users can identify issues like bottlenecks, errors, or suspicious activities.

Wireshark's graphical interface displays a list of captured packets, and clicking on a packet reveals detailed information about its contents. It decodes protocols, such as TCP, UDP, HTTP, DNS, etc., making it easier to understand the communication between devices.

Wifiphisher:

Methodology:
Wifiphisher is a wireless security tool designed for social engineering attacks on Wi-Fi networks. Its methodology involves:

Probe Requests:
- Wifiphisher listens for probe requests from devices searching for known Wi-Fi networks.

Fake Access Points:
- It sets up rogue access points with the same name (SSID) as the target network, exploiting the fact that many devices will automatically connect to a familiar SSID.

Deauthentication:
- Wifiphisher may use deauthentication attacks to force devices to disconnect from their legitimate Wi-Fi connections, making them more likely to connect to the rogue access point.

Captive Portal:
- Once a device connects to the rogue access point, Wifiphisher deploys a captive portal that mimics the login page of the legitimate network, capturing login credentials.

Credentials Harvesting:
- Wifiphisher collects the entered credentials and may redirect the user to the actual Wi-Fi network to avoid suspicion.

Phishing:
- It may employ phishing techniques to trick users into entering sensitive information or performing actions they wouldn't normally do.

!!!(TELL SAUBHAGYA TO ADD HIS SCREENSHOTS ONCE HE IS DONE WITH WIFIPHISHER)!!!

Understanding:

Wifiphisher is an attack tool that exploits human behavior and the tendency of devices to connect automatically to known networks. It demonstrates the vulnerability of Wi-Fi networks to social engineering attacks and highlights the importance of user awareness in securing wireless connections.

Explanation:

Wifiphisher is a tool used for penetration testing and security assessments. It leverages social engineering techniques to trick users into connecting to a rogue Wi-Fi access point. By imitating the characteristics of a legitimate Wi-Fi network, Wifiphisher aims to capture sensitive information, such as login credentials.

The tool automates several steps of the attack, making it easier for security professionals to assess the vulnerability of a network to such social engineering tactics. It serves as a reminder for individuals and organizations to be cautious about connecting to unknown Wi-Fi networks and to use secure practices to protect their credentials.

It's important to note that using Wifiphisher for unauthorized access to networks is illegal and unethical. The tool should only be used in controlled environments for legitimate security testing purposes with proper authorization.