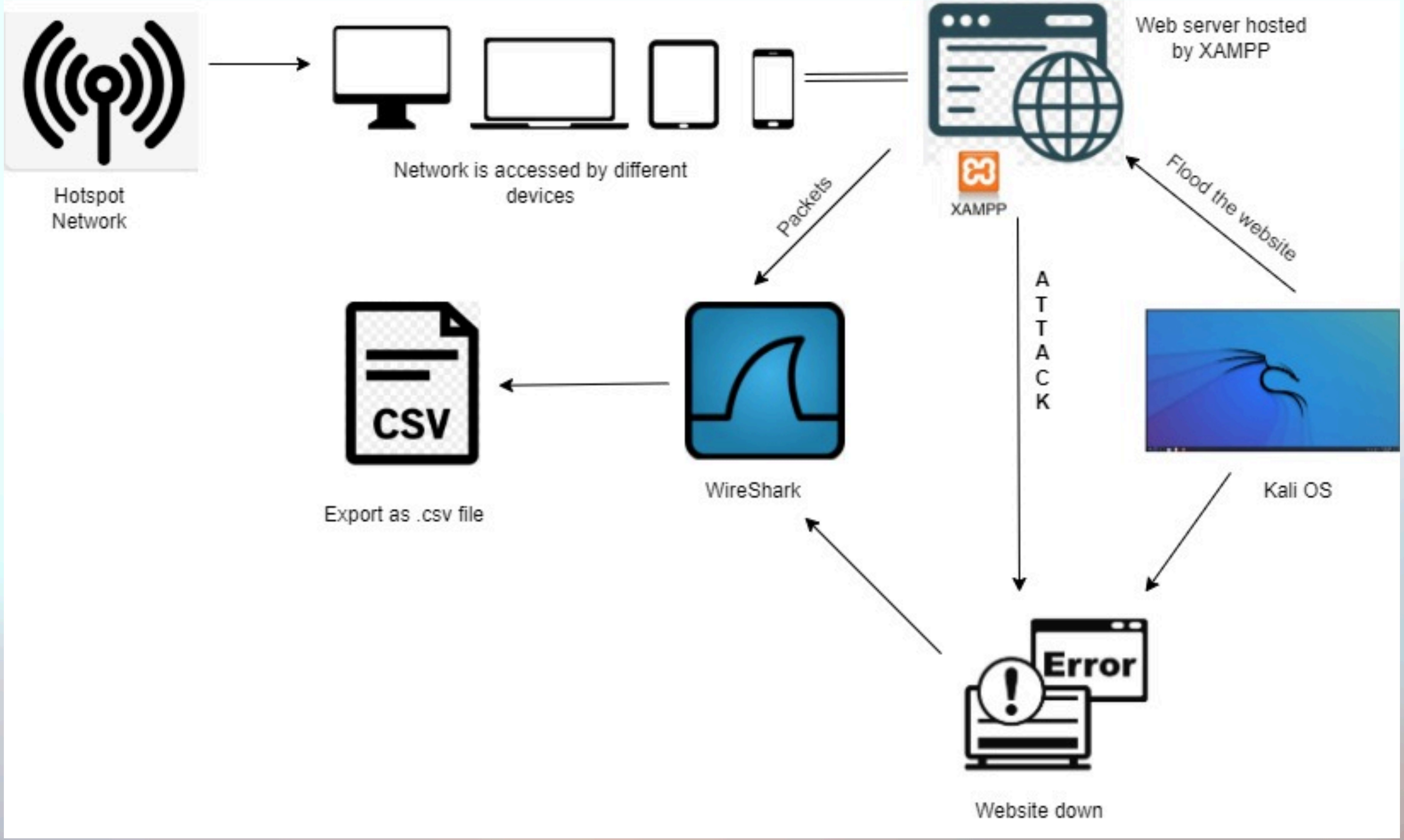
AI Threat Analysis System: Safeguarding businesses through dynamic cybersecurity insights.

Team Name: Access Denied
Team Code:HFC03
College : GSSSIETW, Mysuru

20 February,2024

Step 1: Collection of dataset

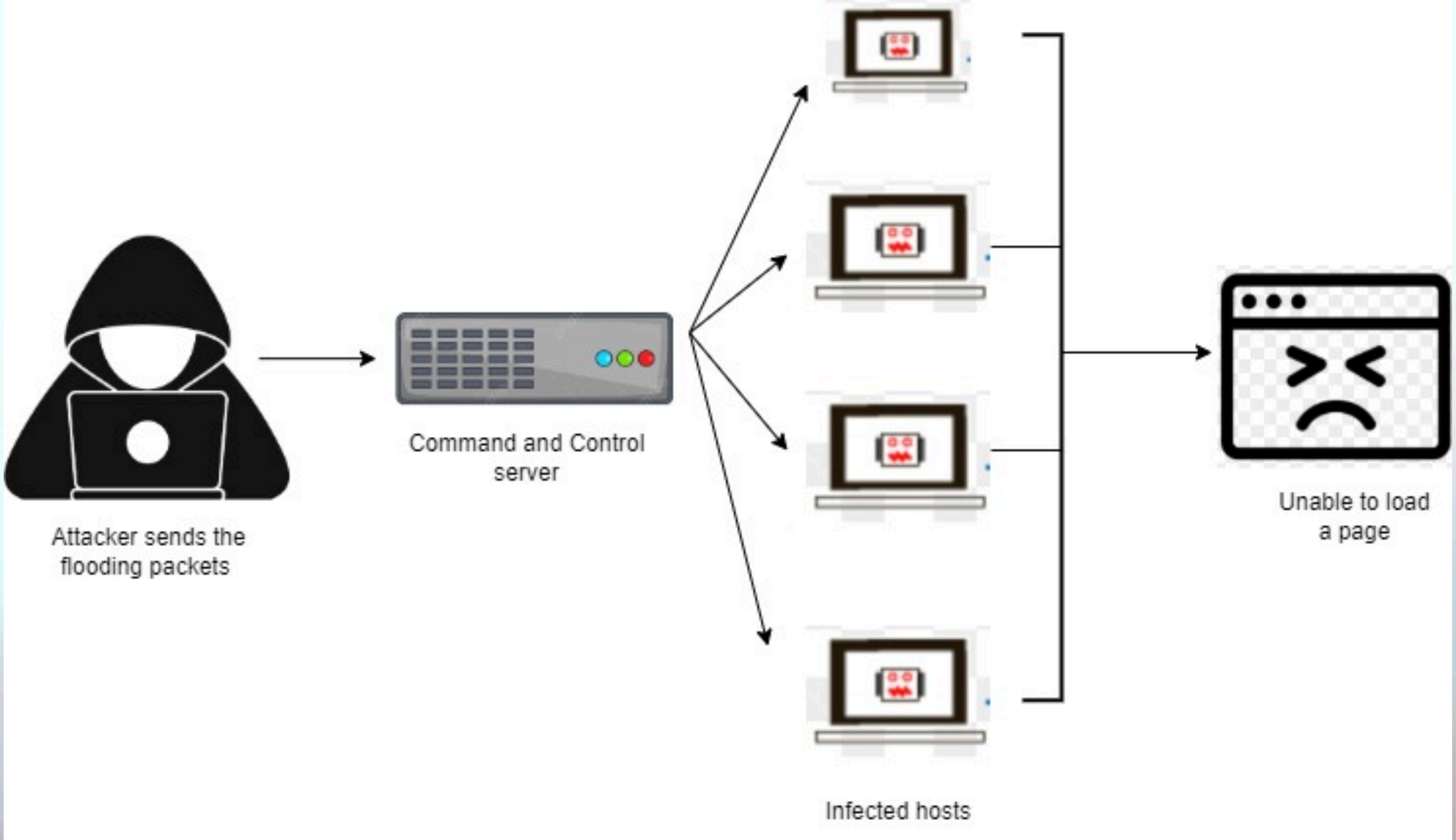


Following steps to collect data:

(This data is collected based on the requirements for the project.)

- **Wireshark:** To trace connections, view the contents of suspect network transactions and identify bursts of network traffic.
- **Kali OS:**Kali includes hacking tools that can be used to carry out and defend against brute-force attacks, wireless attacks, IP spoofing attacks.
- **hping3:** It is a tool ,we can use for DDOS attack and can use it for scanning like Nmap. It is the packet count that we want to send it to the victim.
- **Nmap:**It is used to discover hosts and services on a computer network by sending packets and analysing the responses.
- **XAMPP:** It is an open source software package which provides a local web server environment for testing and development.
- **Flooding(DDOS Attack):**In a flood attack, attackers send a very high volume of traffic to a system so that it cannot examine and allow permitted network traffic.
- ***Through wireshark, we extracted 7 different attributes in which, we are adding one extra attribute and name it as "Target ".***

Working Procedure of Attack


Attacker sends the flooding packets
Command and Control server
Infected hosts
Unable to load a page