Title : The Water Coolers

Project Name : DOS,DDOS & Botnet

Abstract :

In the landscape of cybersecurity threats, botnets stand out as formidable weapons wielded by malicious actors to compromise network integrity, steal data, launch denial of service(Dos), distributed denial-of-service (DDoS) attacks, and wreak havoc on unsuspecting systems. Among the various targets susceptible to these assaults, Internet of Things (IoT) networks emerge as particularly vulnerable due to their distributed nature and often lax security protocols. The ability to swiftly detect and mitigate these botnet intrusions is paramount to preserving the integrity and functionality of IoT ecosystems. A botnet is a Malicious network of computers used for hostile cyberattacks that is remotely controlled by a third party. Botnets can be used for spamming, data theft, distributed denial-of-service (DDOS) attacks, and gaining access to the target device and network.With command and control (C&C) software, the owner can take charge of the botnet.The devices which are compromised with these attack are “Bots / Zombie Devices” and the Owner who controls these Bots known as “Bot Master”. IOT networks are vulnerable to all of these assaults, which can also negatively impact the network's performance.

Traditional methods for identifying botnet activities in IoT networks have proven to be both resource-intensive and less accurate, especially when faced with the challenges of handling large volumes of network traffic data. Our Aim is to Detect the presence of Botnet in Devices/Network using Network Traffic Analysis with Network tools and Python

Team Members:

P. Harshitha (218T5A1203)

A. Vijaya Prajwala (208T1A1202)

G. Madhu Babu (208T1A1216)

M. Trivani (208T1A1232)

U. Dhanalakshmi (208T1A1261)

N.Viharika (20NN1A1245)

B. Geethika Sai (218T5A1201)