IRC (Internet Relay Chat)

IRC (Internet Relay Chat) is **a text-based communication protocol** that allows users to join channels (chat rooms) and communicate in real-time. It was originally developed for group communication but can also support private messaging, file sharing, and multi-channel chats. IRC operates over the internet, typically **using TCP on port 6667**, but can also use **encrypted connections through SSL/TLS (usually on port 6697)**.

How IRC Works

- **Channels**: Users join specific chat rooms called channels (e.g., #channelname), where they can communicate with others in real time.
- **Servers and Clients**: IRC operates using a **client-server model**, where users connect to an IRC server via an IRC client. Multiple servers can be interconnected in networks, allowing for a broad, distributed communication system.
- **Commands**: Users interact with the system using commands such as /join #channel to enter a channel or /msg user to send a private message.

Use by Hackers (Botnets)

IRC has **historically been exploited by hackers for nefarious activities, including the management of botnets**.

1. **Botnets**

- A botnet is **a network of compromised devices (bots) that can be controlled remotely by an attacker**. Hackers infect devices with malware, turning them into bots that can perform coordinated attacks, such as **DDoS (Distributed Denial of Service)** attacks or **spamming campaigns**.
- **IRC-based botnets**: Hackers **use IRC as a command-and-control (C2) channel for managing botnets**. The bot-infected devices connect to a specific IRC server and **join a hidden channel controlled by the attacker**.
- Once connected, the attacker can issue **commands through the IRC channel to all bots simultaneously, instructing them to launch attacks, download additional malware, or steal data**.

2. **Anonymity**

- IRC can be used **over the Tor network or with proxies**, allowing hackers to remain anonymous and making it difficult for authorities to trace their activities.
- IRC's simplicity and the ability to host servers with relative anonymity make it an attractive platform for cybercriminals.

3. Example of IRC Botnet Control

- A hacker creates a malware strain that infects devices, turning them into bots.
- These bots are programmed to automatically connect to an IRC server, join a secret channel, and await commands.
- The hacker, from the IRC server, can issue commands to all connected bots to perform attacks or retrieve stolen data.

Why Hackers Use IRC

- **Real-time Control**: IRC allows for real-time communication, making it efficient for coordinating fast-moving attacks like DDoS.
- **Simple and Lightweight**: The protocol is simple and lightweight, allowing it to operate even on low-resource devices or compromised systems.
- **Widely Available and Easy to Set Up**: IRC servers are easy to deploy, and there are many publicly available IRC networks, providing flexibility for attackers.

Summary

- **IRC is a real-time communication protocol**, originally used for group chats and file sharing.
- Hackers **leverage IRC to manage botnets**, using it as a **command-and-control channel** to coordinate compromised devices for attacks.
- The anonymous nature of IRC, especially when used with tools like Tor, makes it a favored platform for cybercriminal activities.