**DDOS Attack Presentation**

**What is DDOS Attack ?**

 In a DoS attack, **a hacker uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests**—usually in an attempt to exhaust server resource

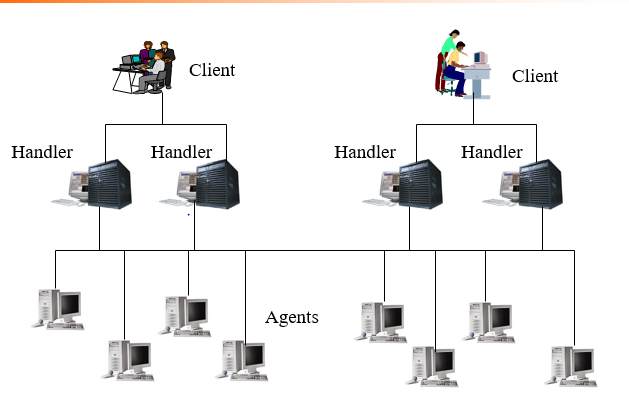
**Background Information: Denial of Service Attacks**

* **Denial of Service Attack:** an attack on a computer or network that prevents legitimate use of its resources.[1]
* DoS Attacks Affect:
  + Software Systems
  + Network Routers/Equipment/Servers
  + Servers and End-User PCs

**Distributed Denial of Service Attacks**

A distributed denial-of-service (DDoS) attack **occurs when multiple machines are operating together to attack one target**. DDoS attackers often leverage the use of a botnet—a group of hijacked internet-connected devices to carry out large scale attacks.

DDOS Architecture

****

**Widely Used DDoS Programs**

* Trinoo
* Tribe Flood Network
* TFN2K
* stacheldraht (barbed wire)

**DDoS Protection Environment**

* Linux Kernal (immune to TARGA & teardrop
* Firewall – packet filtering
* Traffic Monitor
* IP Tunneling