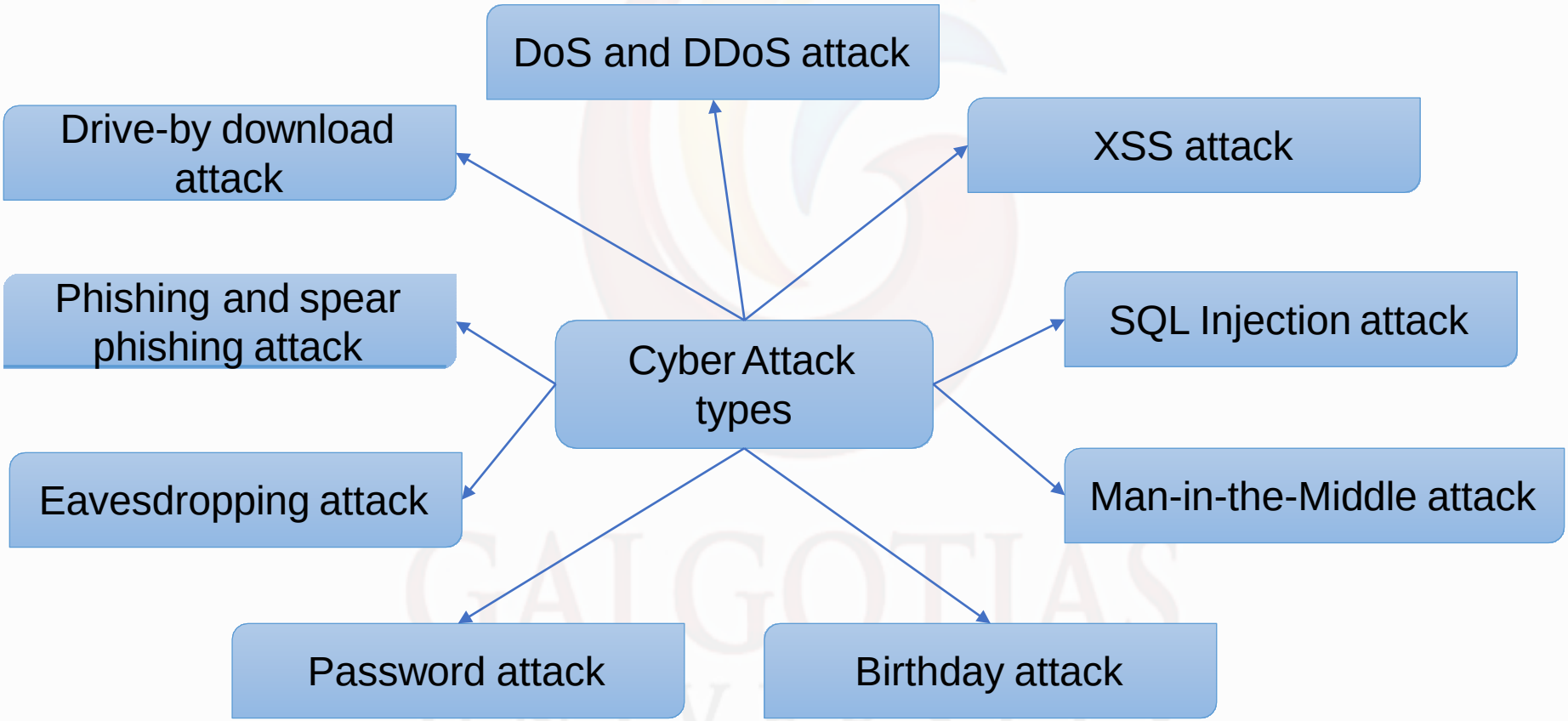
UNIT I

INTRODUCTION TO CYBER ATTACKS

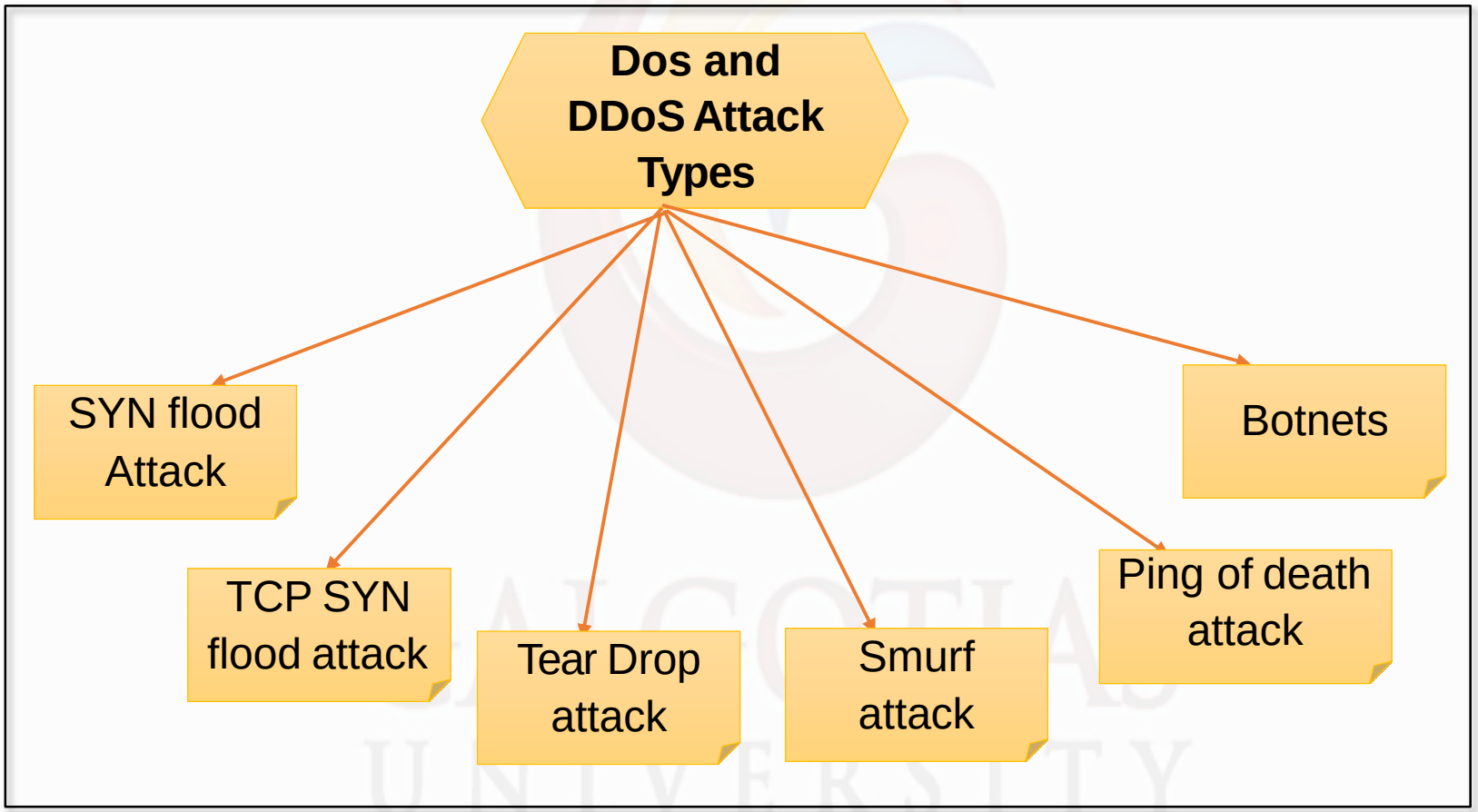
Most Common types of Cyber-attacks



DoS and DDoS Attack

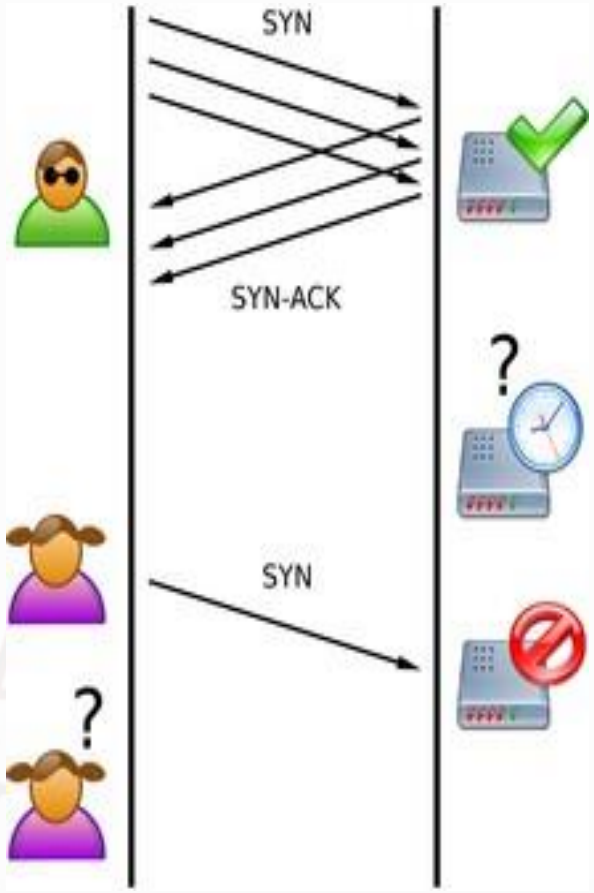
- DoS makes the system unresponsive to the actual service requests
- It does so by overpowering the system resources
- DDoS attack is similar to the DoS attack
- Difference is that the attack is launched from a series of host machines

DoS and DDoS Attack types



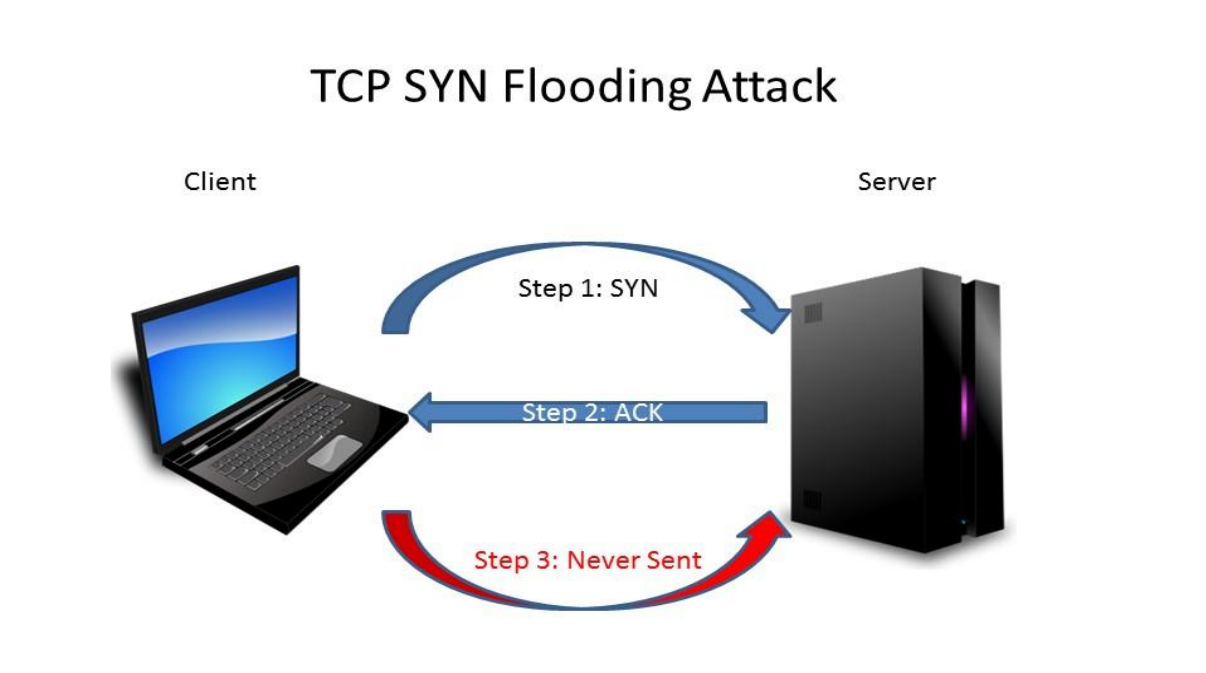
SYN flood attack

- This attack compromises the initial handshake process
- It makes the server unavailable for the actual traffic
- It sends SYN packets repeatedly and eventually overwhelms the targeted server



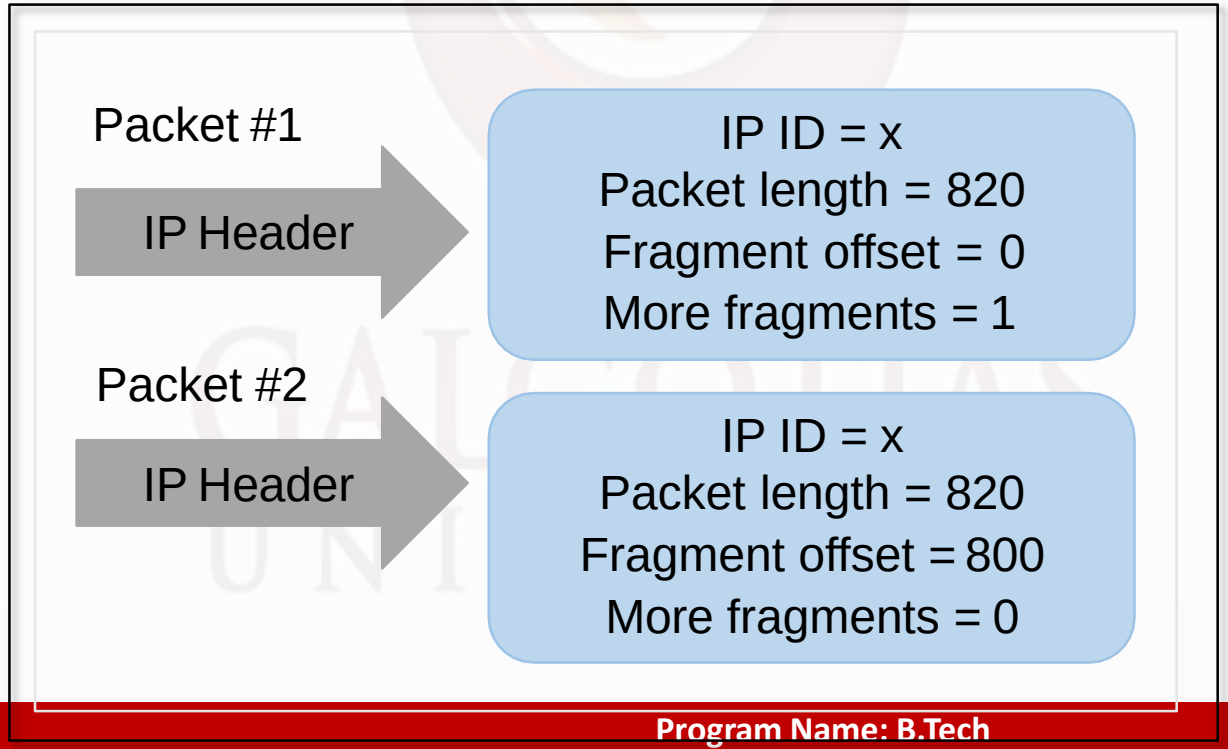
TCP SYN flood attack

- During TCP connection establishment the attacker fills up the target machine with multiple connection requests
- It makes target machine to timeout, awaiting for permission to connect from the server



Tear Drop attack

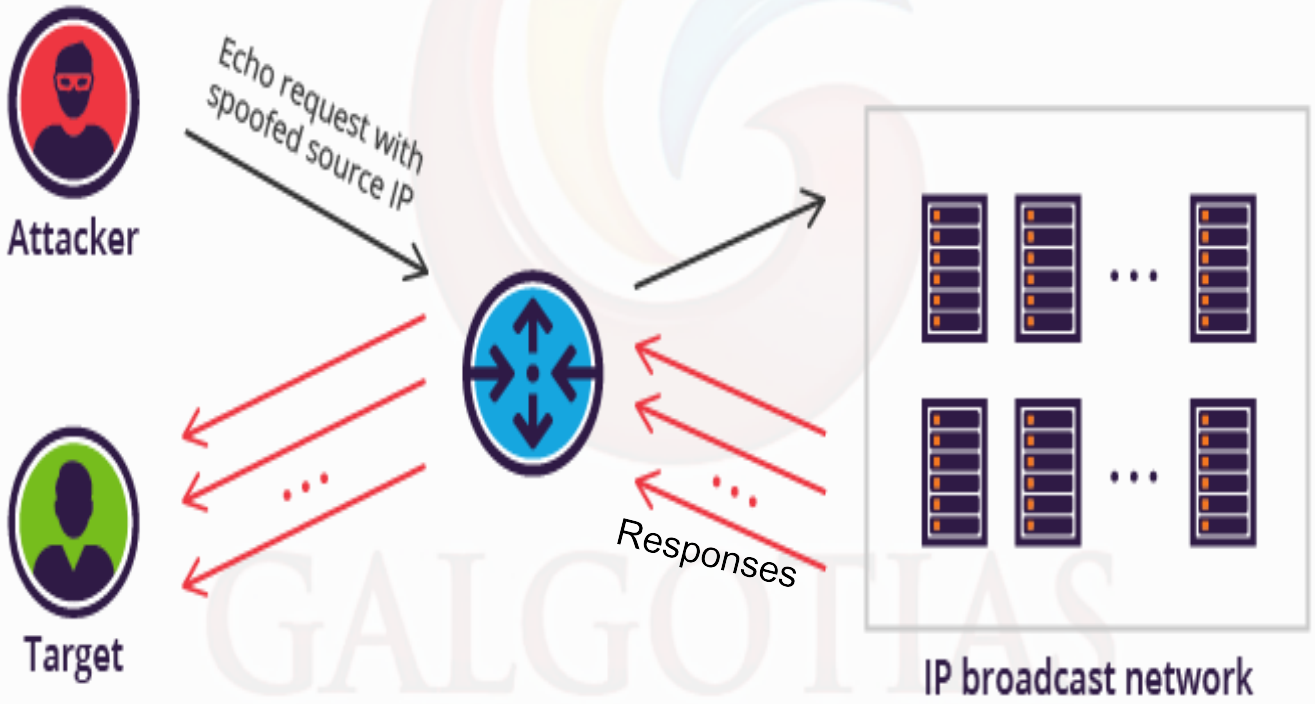
- It is a DoS attack where fragmented packets are sent to a target machine
- This makes the victim's computer to crash overwhelming with packets



Smurf attack

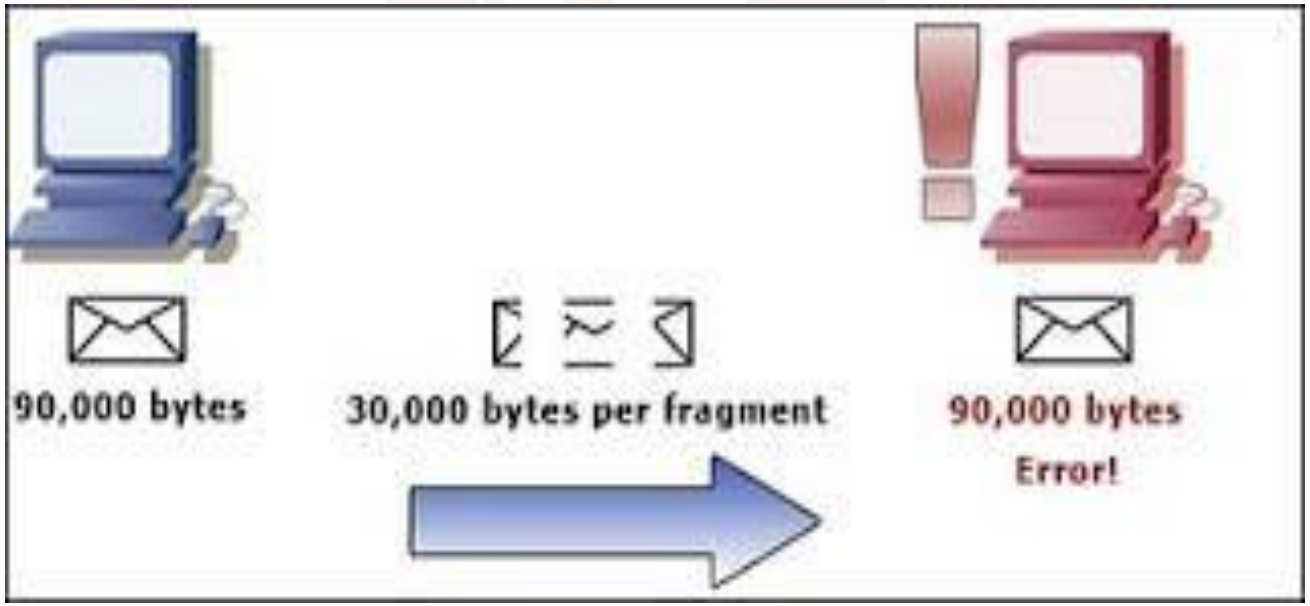
- It is a DoS attack which involves IP spoofing
- A Ping is issued to the entire IP Broadcast addresses
- It stimulates response to the ping packet and the target computer
- The process is repeated and automated to generate large amount of network congestion

An Example for Smurf Attack



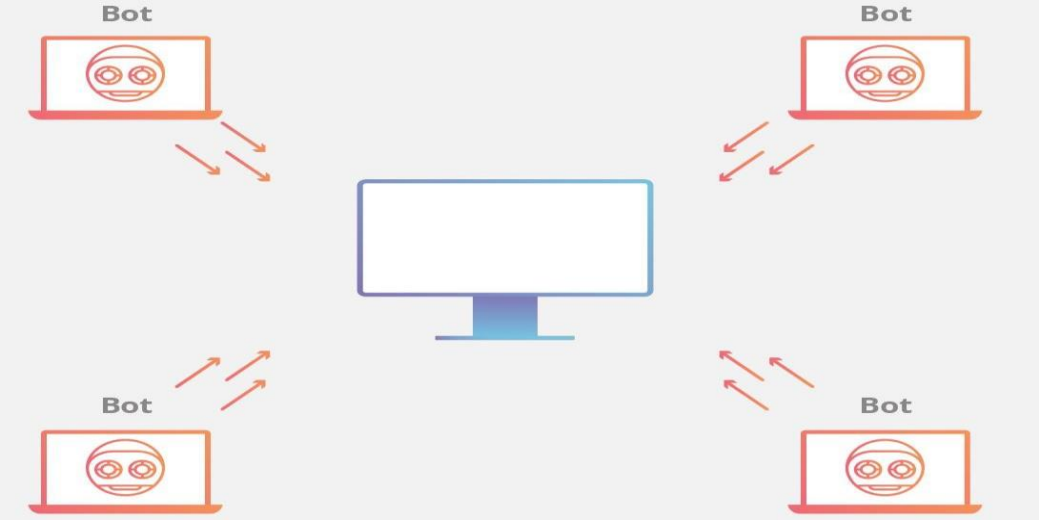
Ping of death attack

- It happens when the network packets are used to ping the target machine with large packet size



Botnets

- Botnets are millions of computers compromised with viruses by the hacker who is under control of DDoS attacks
- As these bots can be located anywhere, they are generally very difficult to identify



Cross-site scripting attack (XSS Attack)

Website

2 The Attacker injects a payload in the website's database with malicious JavaScript that steals cookies.

3 The website transmits the victim's browser the page with the attacker's payload. The victim's browser executes the malicious scripts.

5 The attacker extracts victim's cookie, after which he use it for session hijacking.

Attacker

Website Visitor

1 Attacker discovers a website for having script injection vulnerabilities.

4 After script execution victim sends his cookie to the attacker.

SQL injection attack

- This attack is most common in database-driven websites
- Here SQL query is executed to the database as the input from the client and the server
- It mostly works if a website uses dynamic SQL

References

- Michael Gregg. 2008. Build Your Own Security Lab: A Field Guide for Network Testing. Wiley Publishing.
- Steven DeFino and Larry Greenblatt. 2012. Official Certified Ethical Hacker Review Guide: For Version 7.1 - EC-Council Certified Ethical Hacker (Ceh (1st. ed.). Course Technology Press, Boston, MA, USA.
- David H. Ramirez-IPTV Security Protecting High-Value Digital Contents-Wiley(2008)


Thank You