Denial of Service Attack(DoS)

Winter Training Project by Ankur Karmakar

What is DoS and DDoS Attack?

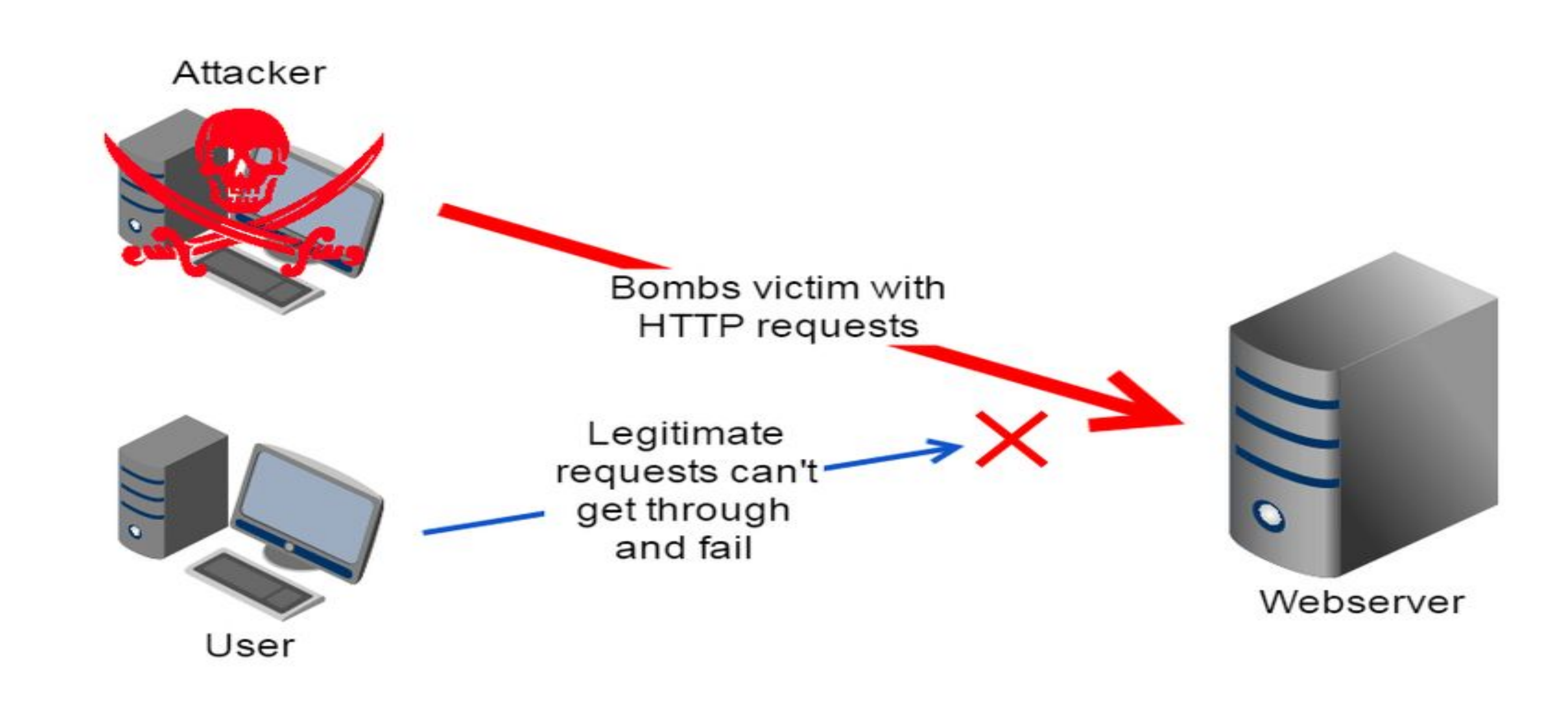
A **denial-of-service attack** (**DoS attack**) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a **distributed denial-of-service attack** (**DDoS attack**), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.
A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, disrupting trade.

Where is it used?

Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail and activism can motivate these attacks.

How does it work?


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

Tools Required:

- Xerxes (The most powerful DoS tool)

Thank You