



Cryptography

Paper Code : MCACS4T15


Unit : 4 - System Security

DoS Attacks

Ms. Sushmita Chakraborty

Assistant Professor

Dept. of MCA, Patna Women's College



With the boom in the e-commerce industry the web server is now prone to attacks and is easy target for the hackers. Hackers usually attempt two types of attacks:

DoS (Deniel-of-Service)

DDoS (Distributed Deniel-of-Service)

DoS (Denial -of-Service) Attacks

- Do to make a nekerack is an attempt by hackers to make a network resource unavailable . It usually interrupts the host, temporary or indefinitely, which is conncted to the internet.
- These attacks typically target services hostedon mission ceitical web services such as banks, credit card, payment gateways.

Symptoms of Dos attacks

- Usually slow network performance
- If there is an unavailability of a particular website
- Inability to access any website
- If there is an increase in the number of spam emails received.
- Long-term denial of access to the web or any internet services.

Types of Dos Attacks

- Buffer Overflow: name itself clear the things.
- Ping of death: ping request larger than 65536 bytes
- Smurf attacks :A security breach for flooding
- TCP SYN Attack: really easy to understand and interesting



Buffer Overflow

It can only hold specific amount of data, when that capacity has been reached, data has to flow somewhere else, typically into another buffer which can corrupt the data that already contained in the buffer

Ping of death

A type of Dos attack in which the attacker sends a ping request that is larger than 65,536 bytes, which is the maximum size that IP allows. While a ping larger than 65,536bytes is too larger to fit in one packet that can be transmitted.

TCP/IP allows a packet to be fragmented, essentially splitting the packet into smaller segments that are eventually reassembled.

Ping of death (cont.)

Attacks too advantage of this flaw by fragmenting packets that when received would total more than the allowed number of bytes and would effectively cause a buffer overload on the operating system at the receiving end, crashing the system

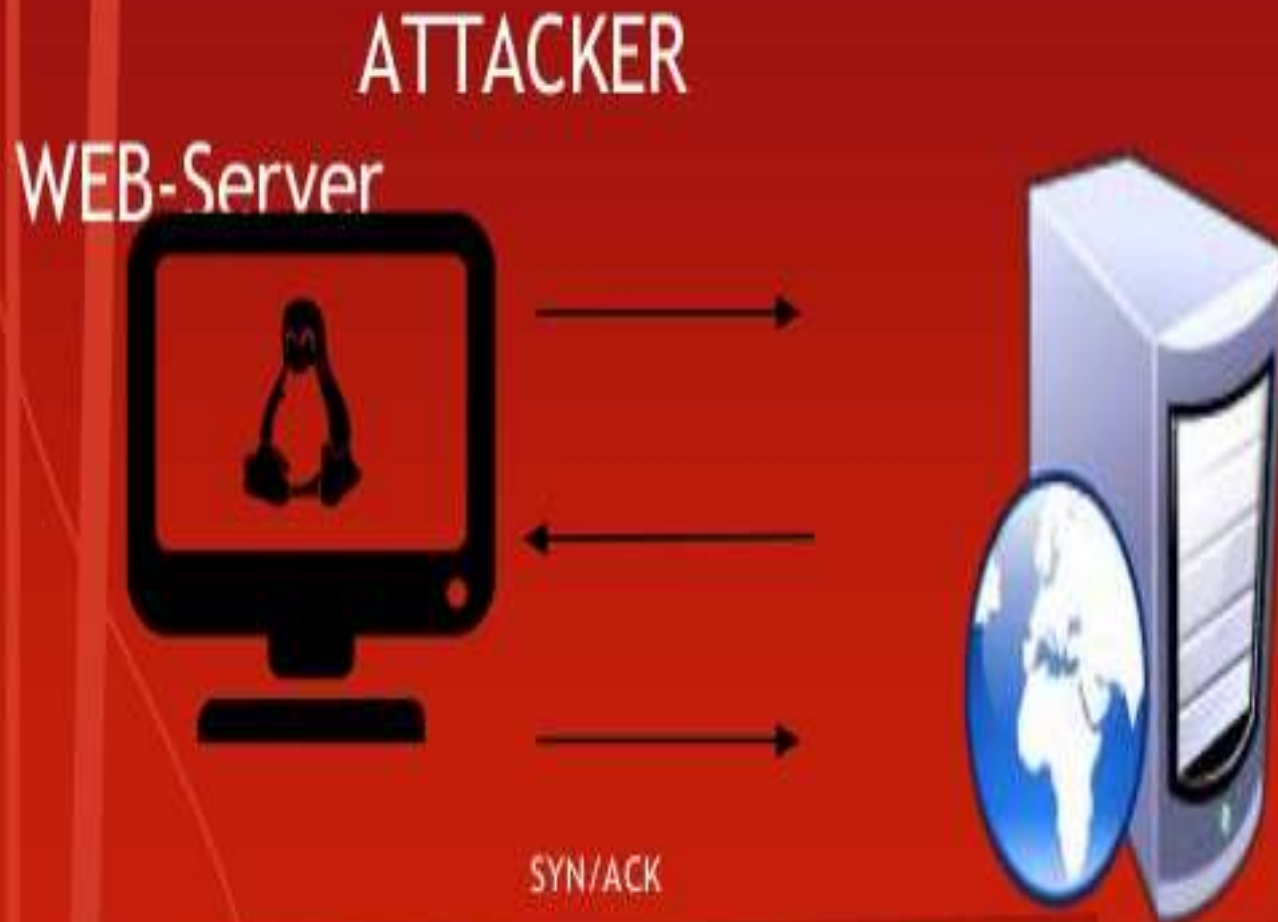
Smurf Attack

- The smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.

TCP SYN / ACK Attack

This is really easy to understand , this attack send the syn packet to server then wait for syn/ack from server once it got syn/ack it keeps server waiting for ack, This creates DoS or DDoS to server.

★ TCP SYN/ACK Attack (Cont)





Thank You