Different Types of Attacks Overview

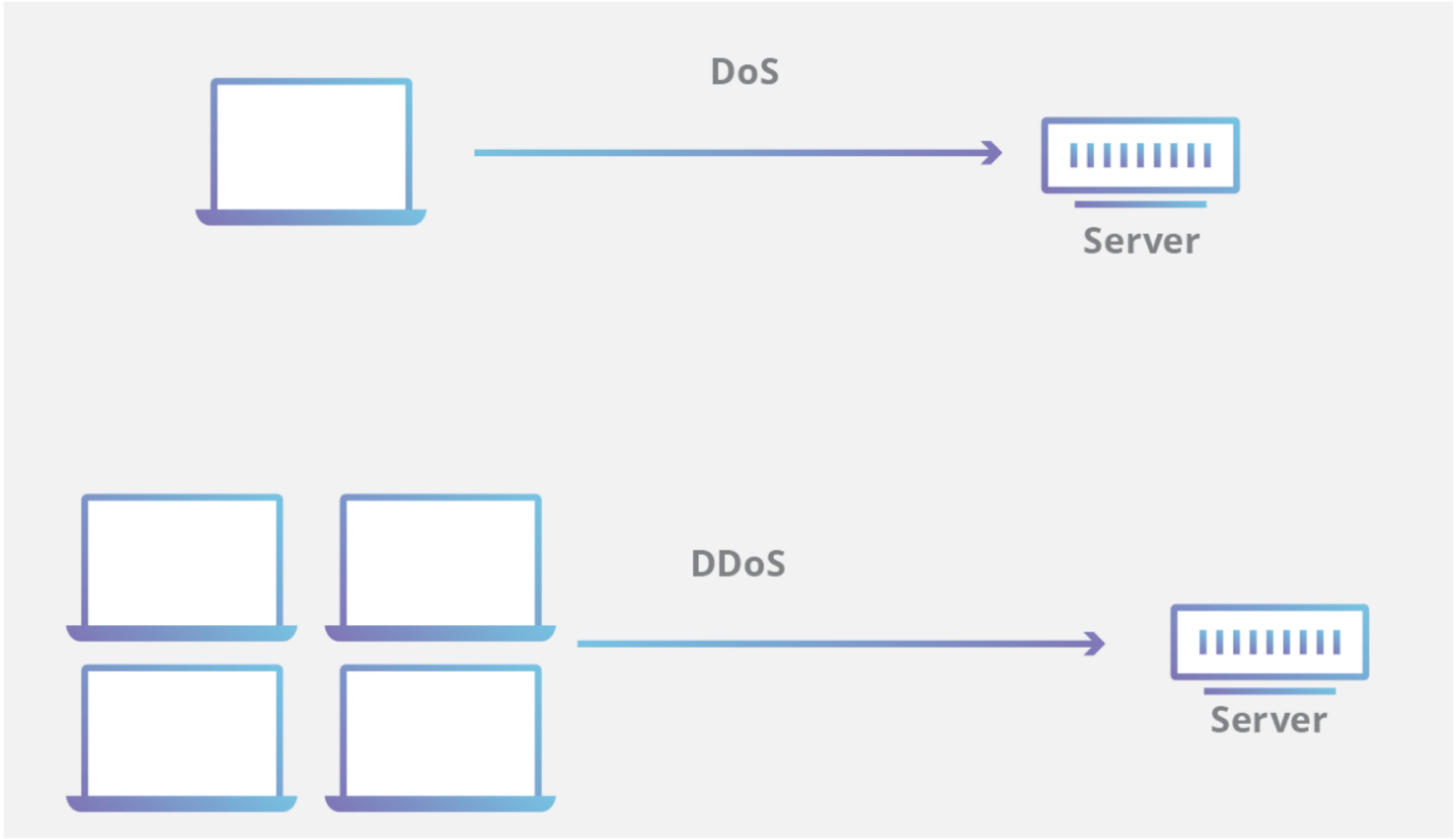
Nazrul Islam

nazrul13@gmail.com

DoS and DDoS

- A denial-of-service (DoS) attack floods a server with traffic, making a website or resource unavailable.
- A distributed denial-of-service (DDoS) attack is a DoS attack that uses multiple computers or machines to flood a targeted resource.
- Both types of attacks overload a server or web application with the goal of interrupting services.

DoS and DDoS



DoS attacks categories

- **DoS attacks typically fall in 2 categories-**
  - **Buffer overflow attacks**
    - An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time.
  - **Flood attacks**
    - By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service.

Historic DoS attacks

- Smurf attack

  - A previously exploited DoS attack in which a malicious actor utilizes the broadcast address of vulnerable network by sending spoofed packets, resulting in the flooding of a targeted IP address.

- Ping flood

  - This simple denial-of-service attack is based on overwhelming a target with ICMP (ping) packets. By inundating a target with more pings than it is able to respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack.

- Ping of Death

  - Often conflated with a ping flood attack, a ping of death attack involves sending a malformed packet to a targeted machine, resulting in deleterious behavior such as system crashes.

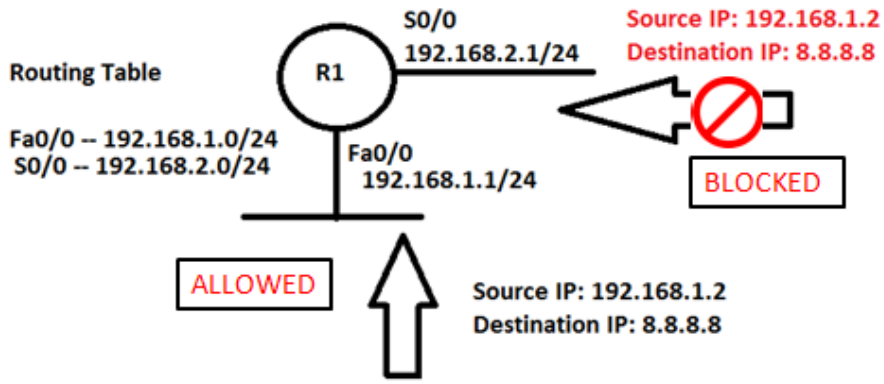
Unicast RPF

- uRPF is a security feature that prevents these spoofing attacks. Whenever your router receives an IP packet it will check if it has a **matching entry in the routing table for the source IP address**.

- uRPF has two modes:
  - **Strict mode**
  - **Loose mode**

Strict Mode

- Strict mode means that that router will perform **two checks** for all incoming packets on a certain interface-
  - Source Matching in the **routing table**
  - **Same interface to reach this source**

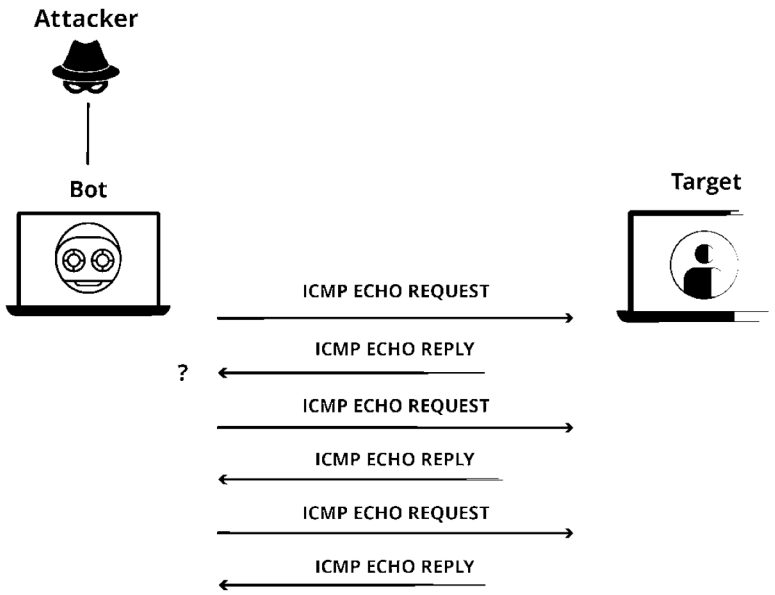


Loose Mode

- Loose mode means that the router will perform only a **single check** when it receives an IP packet on an interface:
  - If the source address in the **routing table it will forward the packet.**

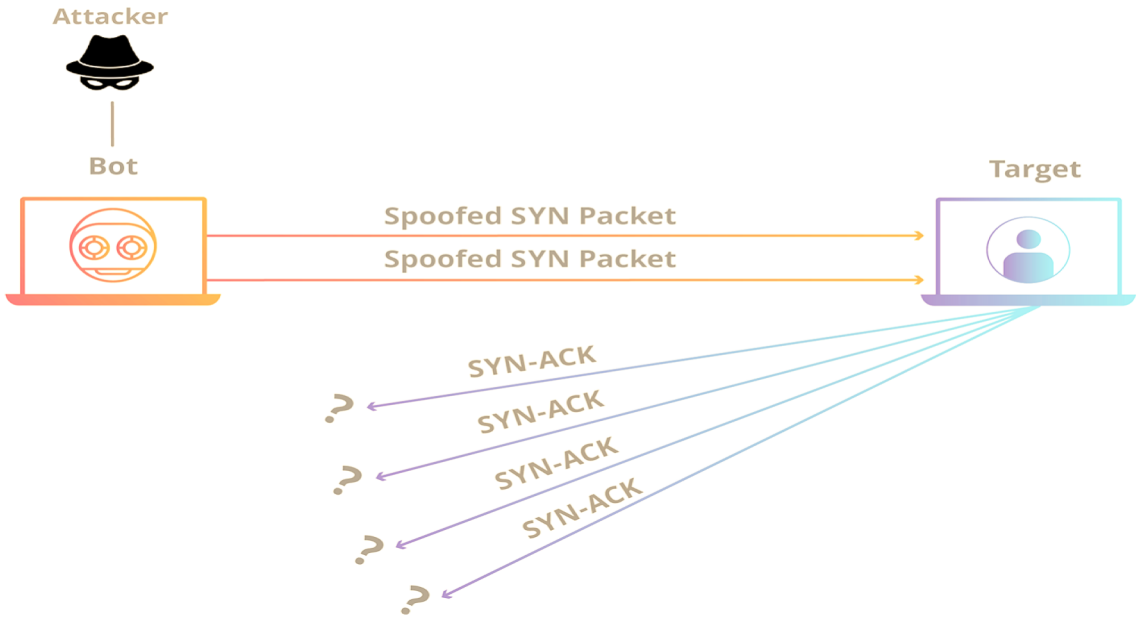
Ping (ICMP) flood attack

- A ping flood is a denial-of-service attack in which the attacker attempts to overwhelm a targeted device with ICMP echo-request packets, causing the target to become inaccessible to normal traffic.
  - When the attack traffic comes from multiple devices, the attack becomes a DDoS or distributed denial-of-service attack.



TCP Attack

- TCP SYN floods are one of the oldest yet still very popular Denial of Service (DoS) attacks. The most common attack involves sending numerous SYN packets to the victim.
  - The attack in many cases will spoof the SRC IP meaning that the reply (SYN+ACK packet) will not come back to it.



UDP Attack

- A UDP flood is a form of volumetric Denial-of-Service (DoS) attack where the attacker targets and overwhelms random ports on the host with IP packets containing User Datagram Protocol (UDP) packets.
  - In this type of attack, the host looks for applications associated with these datagrams. When none are found, the host issues a “Destination Unreachable” packet back to the sender.