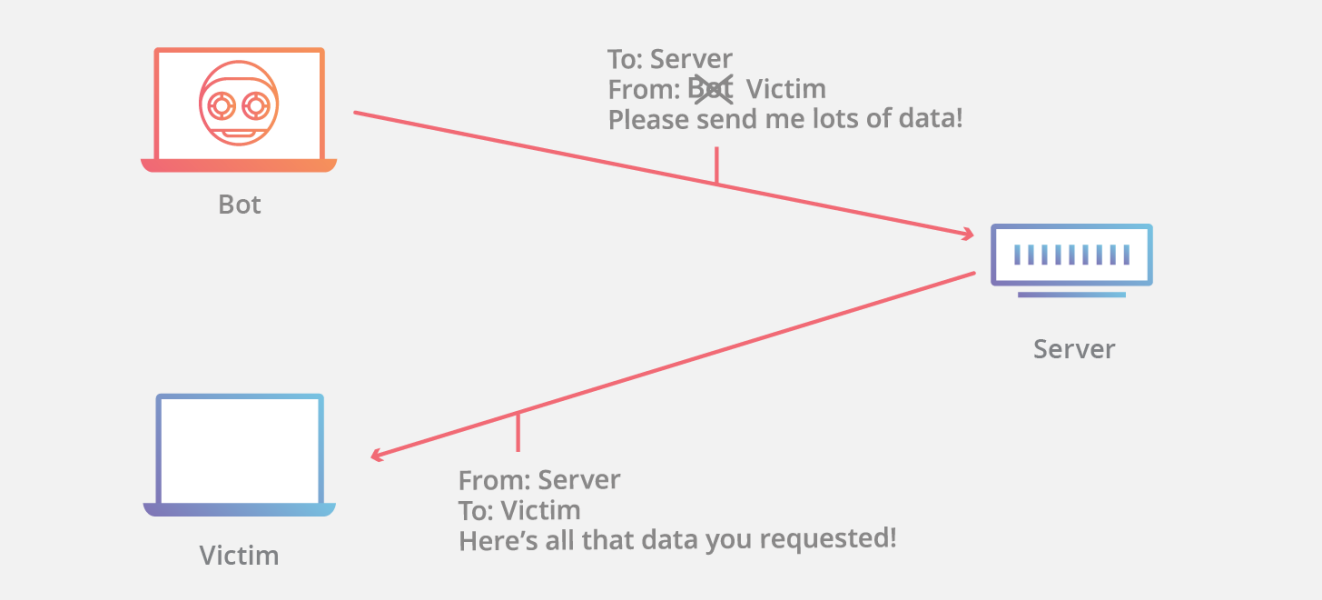
IP Spoofing

What is IP spoofing?

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.

Sending and receiving IP packets is a primary way in which networked computers and other devices communicate, and constitutes the basis of the modern internet. All IP packets contain a header which precedes the body of the packet and contains important routing information, including the source address. In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.



IP Spoofing is analogous to an attacker sending a package to someone with the wrong return address listed. If the person receiving the package wants to stop the sender from sending packages, blocking all packages from the bogus address will do little good, as the return address is easily changed. Relatedly, if the receiver wants to respond to the return address, their response package will go somewhere other than to the real sender. The ability to spoof the addresses of packets is a core vulnerability exploited by many DDoS attacks.

DDoS attacks will often utilize spoofing with a goal of overwhelming a target with traffic while masking the identity of the malicious source, preventing mitigation efforts. If the source IP address is falsified and continuously randomized, blocking malicious requests becomes difficult. IP spoofing also makes it tough for law enforcement and cyber security teams to track down the perpetrator of the attack.

spoofing is also used to masquerade as another device so that responses are sent to that targeted device instead. Volumetric attacks such as NTP Amplification and DNS amplification make use of this vulnerability. The ability to modify the source IP is inherent to the design of TCP/IP, making it an ongoing security concern.

Tangential to DDoS attacks, spoofing can also be done with the aim of masquerading as another device in order to sidestep authentication and gain access to or “hijack” a user’s session.

How to protect against IP spoofing (packet filtering) ?

While IP spoofing can’t be prevented, measures can be taken to stop spoofed packets from infiltrating a network. A very common defense against spoofing is ingress filtering, outlined in BCP38 (a Best Common Practice document). Ingress filtering is a form of packet filtering usually implemented on a network edge device which examines incoming IP packets and looks at their source headers. If the source headers on those packets don’t match their origin or they otherwise look fishy, the packets are rejected. Some networks will also implement egress filtering, which looks at IP packets exiting the network, ensuring that those packets have legitimate source headers to prevent someone within the network from launching an outbound malicious attack using IP spoofing.