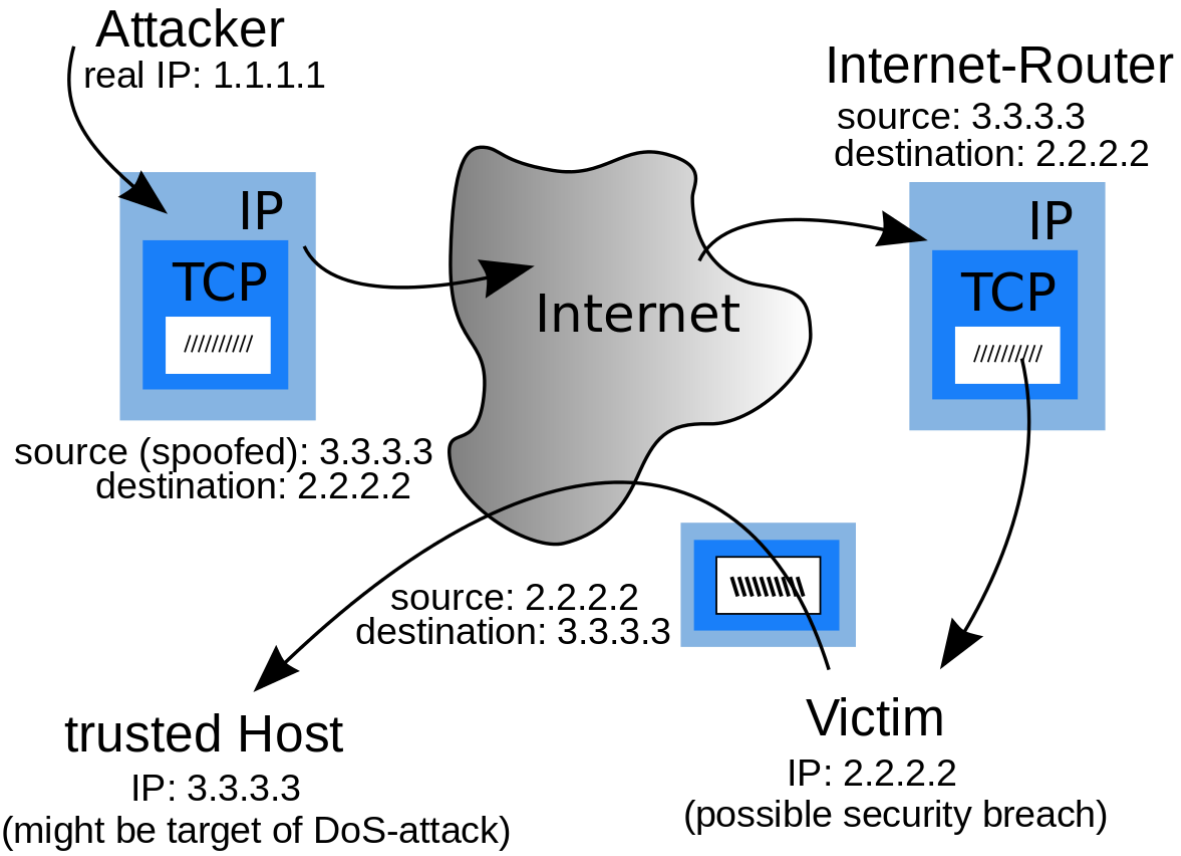
Lab Assignment – 1

1. **What is IP spoofing?**



Example scenario of IP address 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.

2. How to protect from IP Spoofing?

While detecting an IP spoofing attack early on can prove challenging, there are several steps you can take to protect from the dangers of IP spoofing.

i. Packet Filtering

Packet filtering examines the IP packets for every device or user trying to connect to a network (this can be ingress to monitoring incoming communications or egress to monitor outgoing communications). This practice looks particularly closely at each IP packet's header, which contains the IP address, to confirm it matches the source and everything looks as it should. If anything looks amiss, the packet will not be able to complete the connection as intended.

ii. Authentication via Public Key Infrastructure

Public key infrastructure (PKI) is a common method for authenticating users and devices that relies on a public and private key pair. The private key can encrypt communications and verify a user/device's authenticity, while the public key can decrypt these communications.

Importantly, these authentication methods use asymmetric encryption, meaning that each key is different from the other in its pair. This method makes it extremely difficult for hackers to determine the private key and is highly effective for preventing common types of IP spoofing attacks, like the man in the middle attack.

iii. Network Monitoring and Firewalls

Network monitoring is the practice of closely tracking network activity to look out for anything suspicious. While this can prove a bit difficult in preventing hackers from gaining access via IP spoofing since that approach should disguise their presence, it can help catch any malicious activity earlier on to stem the flow of damage. Meanwhile, setting up a network firewall is another way to authenticate IP addresses and filter out any traffic that appears sketchy and potentially subject to IP spoofing.

iv. Security Training

Finally, security training for legitimate network users can also help protect against damages due to IP spoofing. For example, this might involve instructing users to never respond to emails that ask them to click on a link to change their login information. Instead, go directly to the sender's website to take any action. While this type of training can certainly help, it's important to keep in mind that it's just another layer of protection against damages. This training is not a prevention tactic since by the time this training comes in handy, a hacker has already led a successful IP spoofing effort and gained access to certain systems.