IP Spoofing Attack

Dr. Ravi Verma

IP spoofing

- IP spoofing is a technique used to gain unauthorized access to computers, where by the attacker sends messages to a computer with a forging IP address indicating that the message is coming from a trusted host.
- Attacker puts an internal, or trusted, IP address as its source. The access control device sees the IP address as trusted and lets it through.

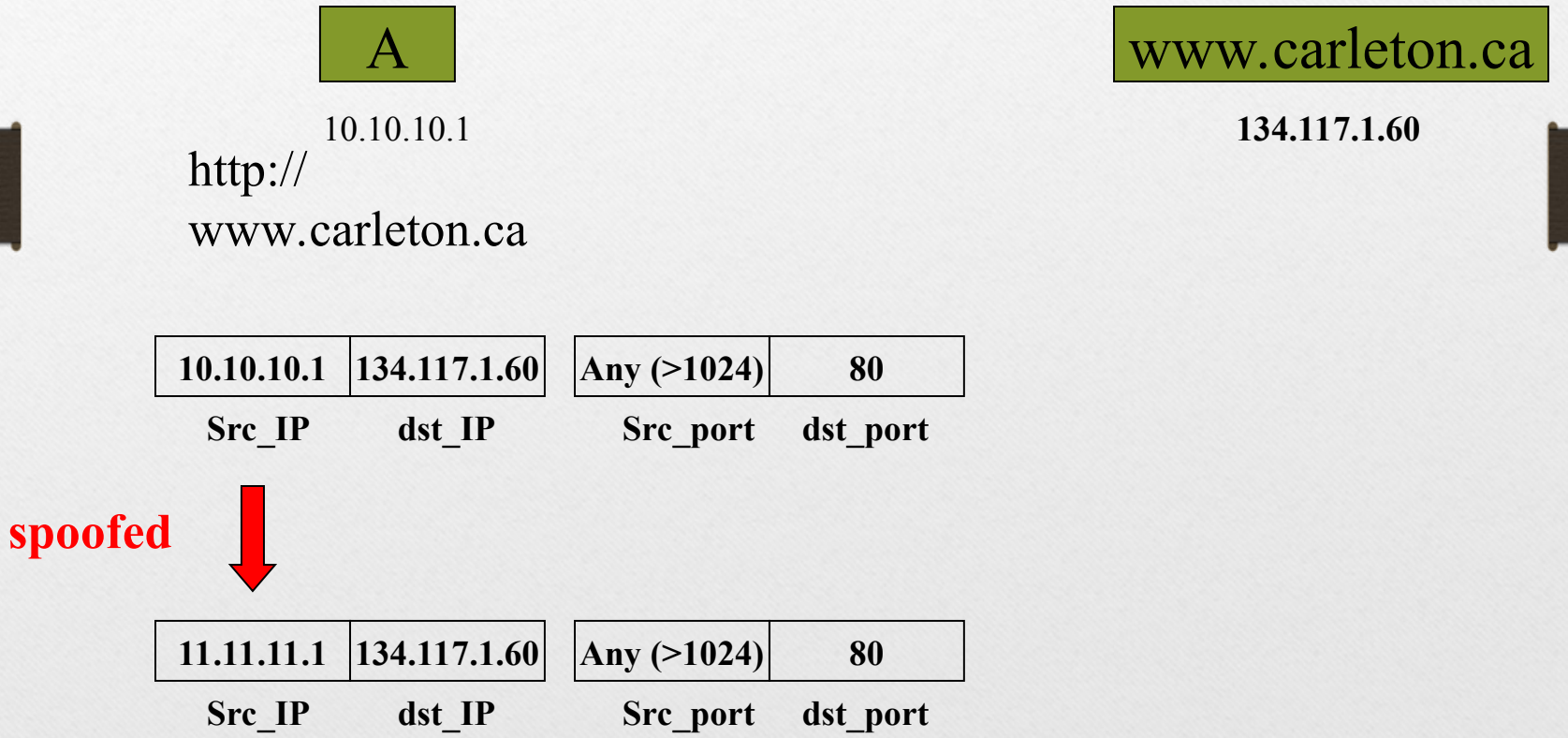
IP Spoofing

IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.

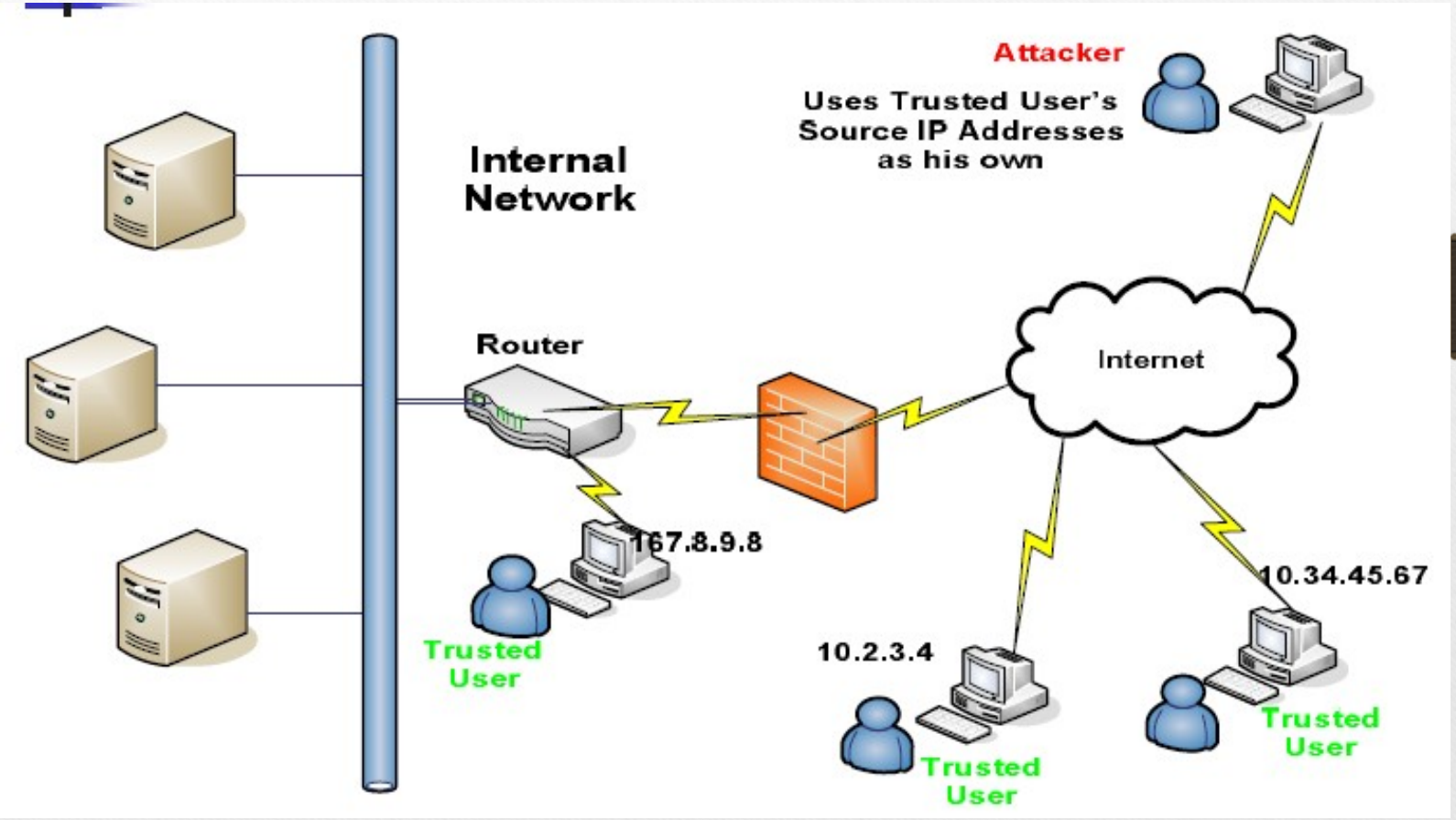
Two general techniques are used during IP spoofing:

- A hacker uses an IP address that is within the range of trusted IP addresses.
- A hacker uses an authorized external IP address that is trusted.

Basic Concept of IP Spoofing



IP Spoofing


Attacker
Uses Trusted User's Source IP Addresses as his own
Internal Network
Router
Internet
167.8.9.8
Trusted User
10.2.3.4
Trusted User
10.34.45.67
Trusted User

Why IP Spoofing is easy?

- Problem with the Routers.
- Routers look at Destination addresses only.
- Authentication based on Source addresses only.
- To change source address field in IP header field is easy.

Spoofing Attacks:

There are a few variations on the types of attacks that using IP spoofing.

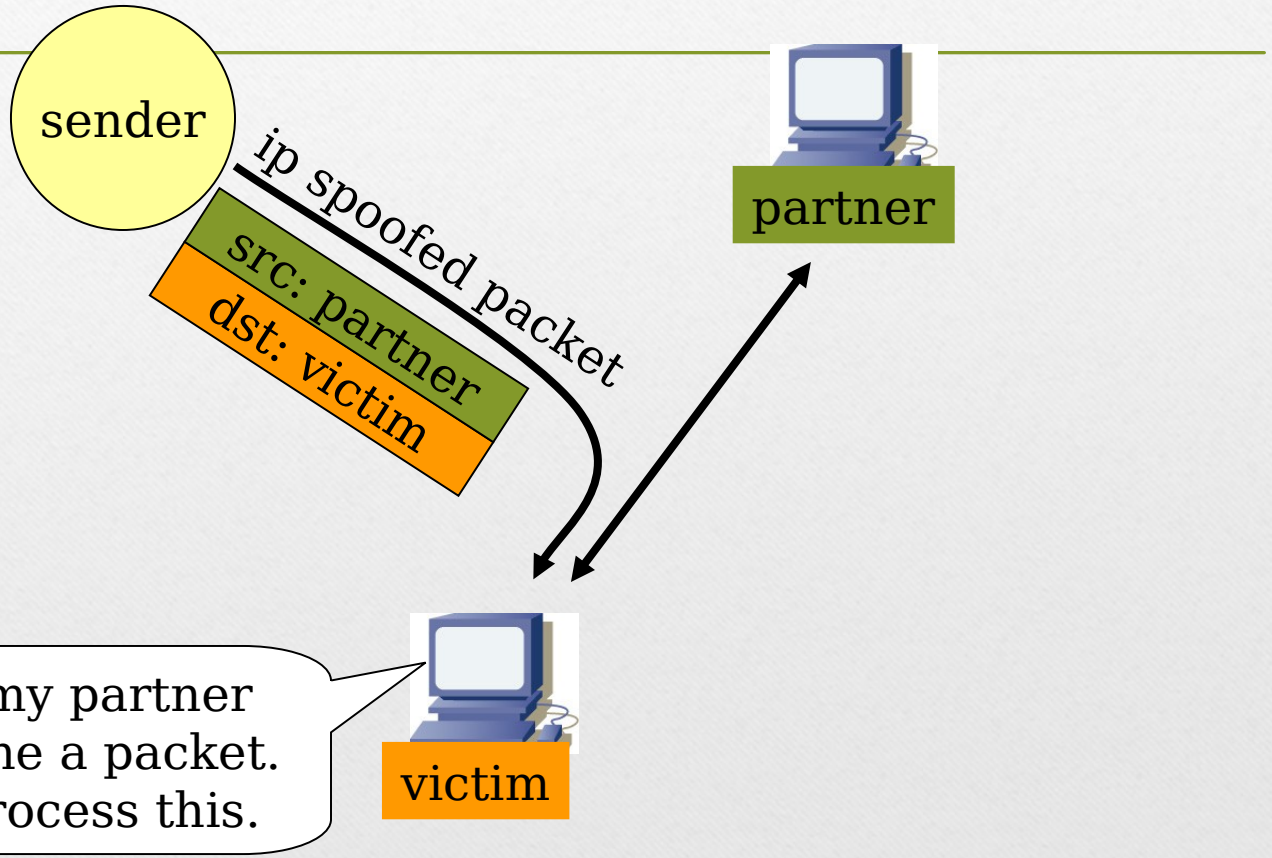
Spoofing is classified into :-

1. **non-blind spoofing**
   This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets.

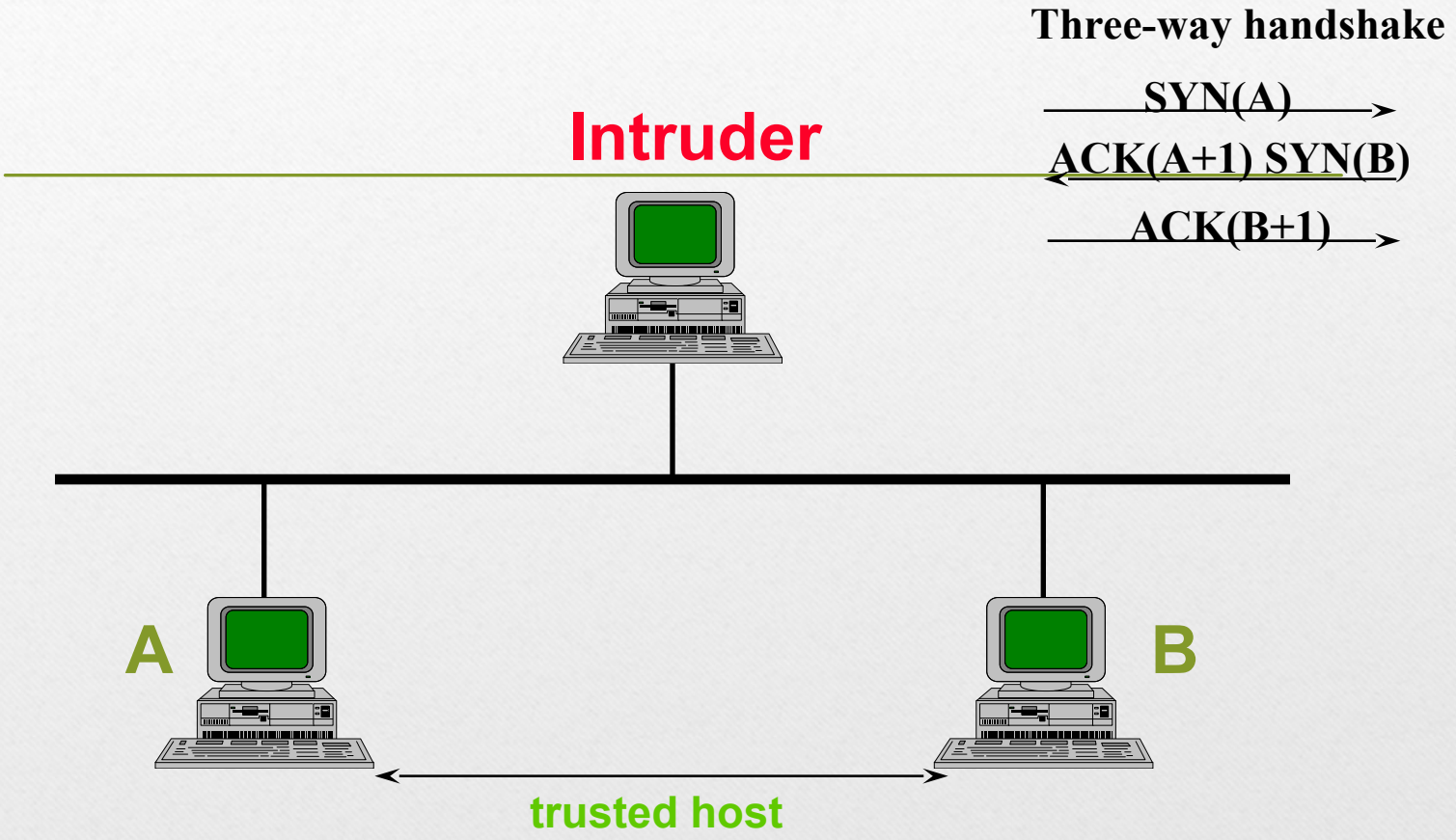
- Using the spoofing to interfere with a connection that sends packets along your subnet.

Spoofing Attacks:

impersonation



IP Spoofing


Three-way handshake
SYN(A)
ACK(A+1) SYN(B)
ACK(B+1)
Intruder
A
B
trusted host

Spoofing Attacks:

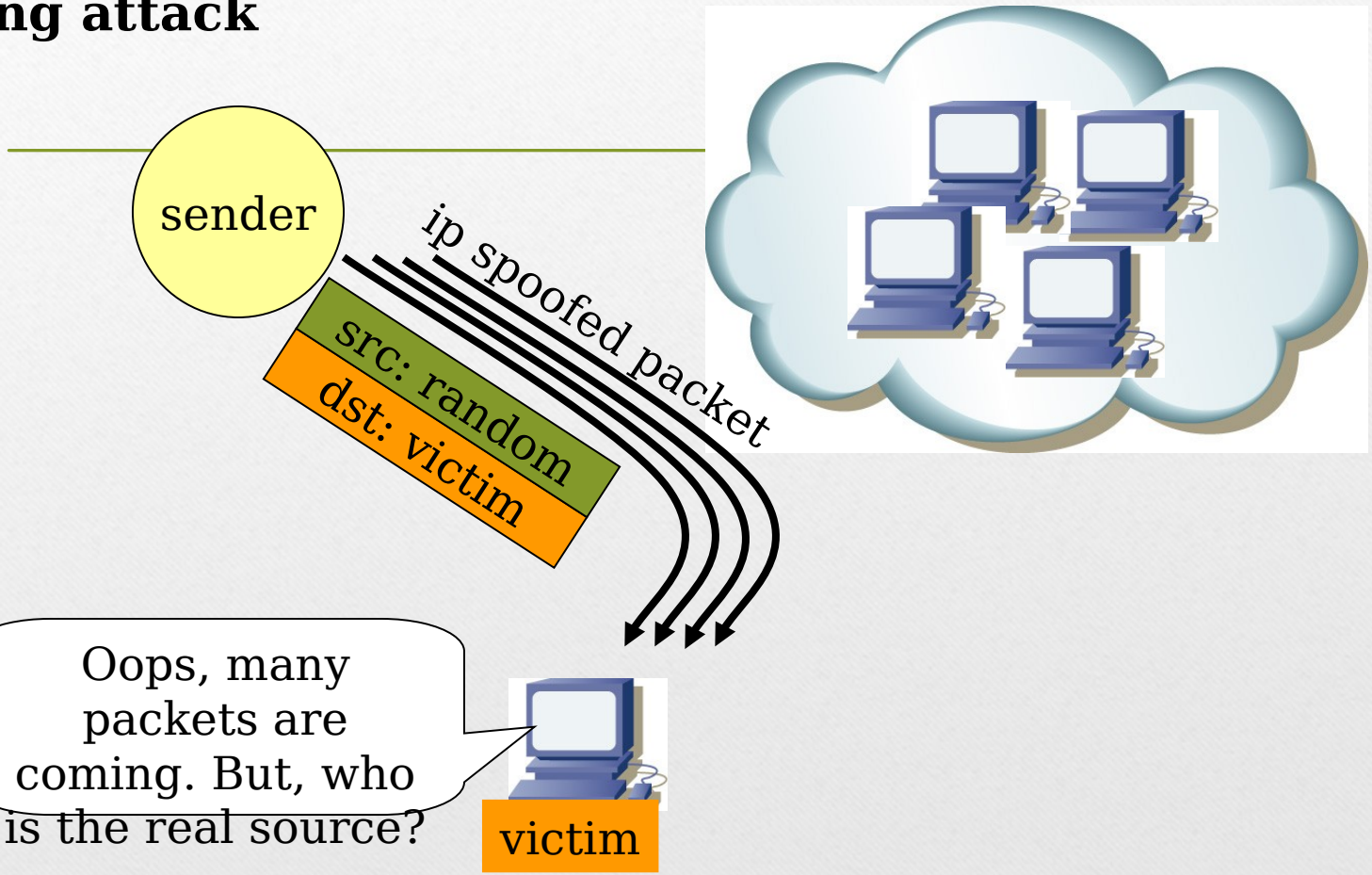
2. Blind spoofing

This attack may take place from outside where sequence and acknowledgement numbers are unreachable. Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days .

- Using the spoofing to interfere with a connection (or creating one), that does not send packets along your cable.

Spoofing Attacks:

flooding attack



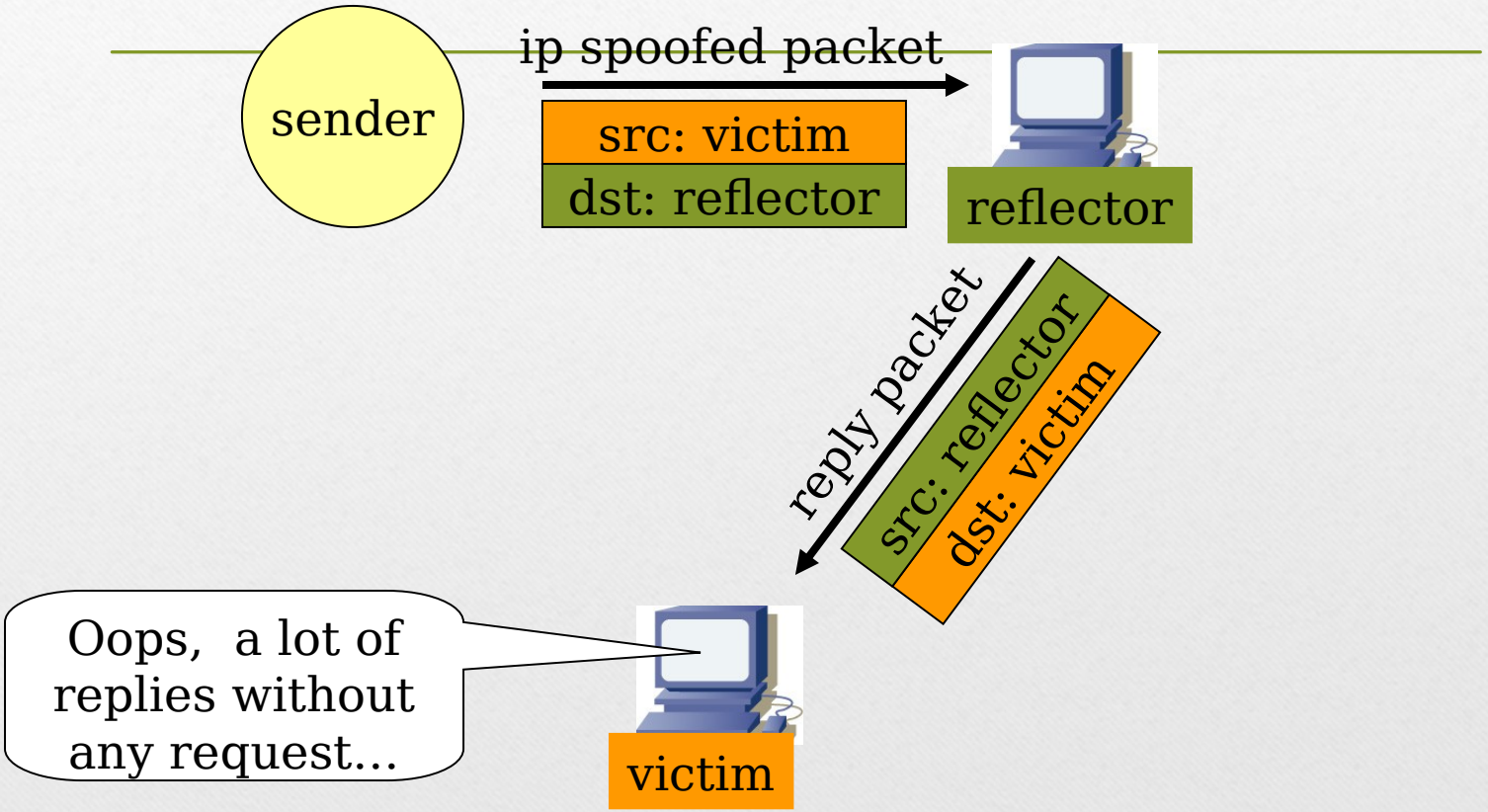
Spoofing Attacks:

3.Man in the Middle Attack

This is also called connection hijacking. In this attacks, a malicious party intercepts a legitimate communication between two hosts to controls the flow of communication and to eliminate or alter the information sent by one of the original participants without their knowledge.

Spoofing Attacks:

reflection



Spoofing Attacks:

4.Denial of Service Attack

- conducting the attack, attackers spoof source IP addresses to make tracing and stopping the DoS as difficult as possible. When multiple compromised hosts are participating in the attack, all sending spoofed traffic, it is very challenging to quickly block the traffic.

- IP spoofing is almost always used in denial of service attacks (DoS), in which attackers are concerned with consuming bandwidth and resources by flooding the target with as many packets as possible in a short amount of time. To effectively

Spoofing Attacks:

- IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be extremely difficult, as it involves modifying thousands of packets at a time. This type of attack is most effective where trust relationships exist between machines.
- For example, it is common on some corporate networks to have internal systems trust each other, so that a user can log in without a username or password provided they are connecting from another machine on the internal network (and so must already be logged in). By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without authenticating.

SMURF ATTACK

- Send ICMP ping packet with spoofed IP source address to a LAN which will broadcast to all hosts on the LAN
- Each host will send a reply packet to the spoofed IP address leading to denial of service

Misconception of IP Spoofing:

A common misconception is that "IP Spoofing" can be used to hide your IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth.

This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection. However, IP spoofing is an integral part of many networks that do not need to see responses.

Impact

Current intruder activity in spoofing source IP addresses can lead to unauthorized remote root access to systems behind a filtering-router firewall. After gaining root access and taking over existing terminal and login connections, intruders can gain access to remote hosts.

Detection of IP Spoofing:

1. If you monitor packets using network-monitoring software such as netlog, look for a packet on your external interface that has both its source and destination IP addresses in your local domain. If you find one, you are currently under attack.

Detection of IP Spoofing:

2. Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access.

Detection of IP Spoofing:

Source Address Validation :

- Check the source IP address of IP packets
  - filter invalid source address
  - filter close to the packets origin as possible
  - filter precisely as possible
- If no networks allow IP spoofing, we can eliminate these kinds of attacks

Prevention IP spoofing

The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network in order to prevent a source IP spoofing attack originating from your site.

Prevention IP spoofing

If your vendor’s router does not support filtering on the inbound side of the interface or if there will be a delay in incorporating the feature into your system, you may filter the spoofed IP packets by using a second router between your external interface and your outside connection. Configure this router to block, on the outgoing interface connected to your original router, all packets that have a source address in your internal network.

Prevention of IP Spoofing:

To prevent IP spoofing happen in your network, the following are some common practices:

1- Avoid using the source address authentication. Implement cryptographic authentication system-wide.

2- Configuring your network to reject packets from the Net that claim to originate from a local address.

3- Implementing ingress and egress filtering on the border routers and implement an ACL (access control list) that blocks private IP addresses on your downstream interface.

If you allow outside connections from trusted hosts, enable encryption sessions at the router.

Conclusion

- Presentation defines about Spoofing and its tools used to perform spoofing activities over the network or on any local or remote machine.

- Session describes How a local system can capture the network interface activities through Wireshark tools .

Question