IP Spoofing

Next, let's learn about
another kind of network attack called IP spoofing.
IP spoofing is a network attack
performed when an attacker changes the source IP of
a data packet to impersonate
an authorized system and gain access to a network.
In this kind of attack,
the hacker is pretending to be someone they are
not so they can communicate over
the network with the target computer and get
past firewall rules that may prevent outside traffic.
Some common IP spoofing attacks are on-path attacks,
replay attacks, and smurf attacks.
Let's discuss these one at a time.

An on-path attack is
an attack where the malicious actor places themselves in
the middle of an authorized connection
and intercepts or alters the data in transit.
On-path attackers gain access to
the network and put themselves between two devices,
like a web browser and a web server.
Then they sniff the packet
information to learn the IP and
MAC addresses to devices
that are communicating with each other.
After they have this information,
they can pretend to be either of these devices.

Another type of attack is a replay attack.
A replay attack is
a network attack performed when
a malicious actor intercepts
a data packet in transit and delays
it or repeats it at another time.
A delayed packet can cause
connection issues between target computers,
or a malicious actor may take
a network transmission that was sent by
an authorized user and repeat it at
a later time to impersonate the authorized user.

A smurf attack is a combination of
a DDoS attack and an IP spoofing attack.
The attacker sniffs an authorized user's IP address
and floods it with packets.
This overwhelms the target computer and can
bring down a server or the entire network.

Now that you've learned about
different kinds of IP spoofing,
let's talk about how you can protect
the network from this kind of attack.
As you previously learned,
encryption should always be implemented so that the data
in your network transfers can't
be read by malicious actors.
Firewalls can be configured
to protect against IP spoofing.
IP spoofing makes it seem like
the malicious actor is an authorized user
by changing the sender's address of
the data packet to match the target network's address.
So if a firewall receives a data packet from the internet
where the sender's IP address
is the same as the private network,
then the firewall will deny the transmission
since all the devices with that IP address
should already be on the local network.
You can make sure that your firewalls
configure correctly by creating a rule to
reject all incoming traffic that has
the same IP address as the local network.

That's it for IP spoofing.
You've learned how IP spoofing is used in
some common attacks like on-path attacks,
replay attacks, and smurf attacks.

Revision #1
Created 2023-07-02 05:52:02 UTC by naruzkurai
Updated 2023-07-03 10:29:21 UTC by naruzkurai