Malicious packet sniffing

In this video, we'll discuss
packet sniffing, with a focus on how
threat actors may use this technique to
gain unauthorized access to information.
Previously, you learned about
the information and data packets
that travel across the network.
Packets include a header which contains
the sender's and receiver's IP addresses.
Packets also contain a body, which
may contain valuable information like names,
date of birth, personal messages,
financial information, and credit card numbers.

Packet sniffing is the practice of using
software tools to observe
data as it moves across a network.
As a security analyst,
you may use packet sniffing to analyze and capture
packets when investigating ongoing incidents
or debugging network issues.
Later in this certificate program,
you'll gain hands-on practice
with some packet sniffing software.
However, malicious actors may also use
packet sniffing to look at
data that has not been sent to them.
This is a little bit like opening somebody else's mail.
It's important for you to learn about how
threat actors use packet sniffing
with harmful intent so you can be
prepared to protect against these malicious acts.
Malicious actors may insert themselves in the middle of
an authorized connection between two devices.
Then they can use packet sniffing to spy on
every data packet as it comes across their device.
The goal is to find valuable information in
the data packets that they can
then use to their advantage.
Attackers can use software applications
or a hardware device to look into data packets.
Malicious actors can access a network packet with

a packet sniffer and make changes to the data.
They may change the information
in the body of the packet,
like altering a recipient's bank account number.

Packet sniffing can be passive or active.
Passive packet sniffing is a type of
attack where data packets are read in transit.
Since all the traffic on a network
is visible to any host on the hub,
malicious actors can view
all the information going
in and out of the device they are targeting.
Thinking back to the example of a letter being delivered,
we can compare a passive packet sniffing
attack to a postal delivery person
maliciously reading somebody's mail.
The postal worker, or packet
sniffer, has the right to deliver the mail,
but not the right to read the information inside.
Active packet sniffing is a type of
attack where data packets are manipulated in transit.
This may include injecting
internet protocols to redirect the packets to
an unintended port or
changing the information the packet contains.
Active packet sniffing attack would
be like a neighbor telling the delivery person
"I'll deliver that mail for you," and then reading the mail
or changing the letter before putting it in your mailbox.
Even though your neighbor knows you
and even if they deliver it to the correct house,
they are actively going out of
their way to engage in malicious behavior.

The good news is that
malicious packet sniffing can be prevented.
Let's look at a few ways
the network security professional
can prevent these attacks.
One way to protect against
malicious packet sniffing is to use
a VPN to encrypt and protect
data as it travels across the network.
If you don't remember how VPNs work,
you can revisit the video about
this topic in the previous section of the program.

When you use a VPN,
hackers might interfere with your traffic,
but they won't be able to decode it
to read it and read your private information.
Another way to add a layer of
protection against packet sniffing is to make sure
that websites you have use
HTTPS at the beginning of the domain address.
Previously, we discussed how HTTPS uses SSL/TLS to
encrypt data and prevent eavesdropping
when malicious actors spy on network transmissions.
One final way to help protect yourself against
malicious packet sniffing is to
avoid using unprotected WiFi.
You usually find unprotected WiFi in
public places like coffee shops,
restaurants, or airports.
These networks don't use encryption.
This means that anyone on the network can access
all of the data traveling to and from your device.
One precaution you can take is avoiding
free public WiFi unless you have
a VPN service already installed on your device.

Now you know how threat actors may use
packet sniffing and how to
protect a network from these attacks.
Let's move on to discuss other network intrusions.

Revision #1
Created 2 July 2023 05:47:31 by naruzkurai
Updated 3 July 2023 10:29:21 by naruzkurai