1.9 Physical interception

Physical interception

In this section, we'll look at how attacks are carried out on layer 1, the physical layer.

To start, let's walk through an example of what happens when we browse the internet. Firstly, once we tell the browser what website we want to see, the browser establishes a TCP connection with the website's server. Then the browser asks for the index web page, the one entered by typing the address in the search bar or by clicking on a link, using the HTTP command GET. Finally the browser displays the page on the screen.

View description

A diagram showing how different protocols encapsulate an HTTP GET request, and how it's demultiplexed at the receiving end. Starting with the GET request on layer 7, it gets passed to encapsulated by TCP protocol on layer 4, IP address on layer 3 and MAC access on layer 2, before being sent physically on layer 1. The demultiplexing happens in reverse order.

Layer 1 refers to the physical aspect of networking, the cabling and infrastructure used by networks to communicate. Layer 1 attacks focus on disrupting this service in any manner possible, resulting in Denial of Service (DoS) attacks. The disruption could be caused by physically cutting cable right through to disrupting wireless signals (jamming). However, layer attacks can be also focused on intercepting the traffic that transits inside the cables, but this is far from being trivial as it is necessary to consider other aspects.

When an attacker wants to intercept traffic, for instance, it has to consider its position relative to the network it wants to attack. The attacker can be already inside the network, making the interception easier but, there might be the chance that the attacker is outside, so it needs to find a way to get access to the network before to intercept the traffic. Another aspect to consider is whether the interception the attacker wants to carry out results in an active interception or a passive one. Let's look at passive interception.

A **passive interception** is characterised by the interception of messages without modification. There is no change to the network data or systems and it is nearly impossible for company IT managers to detect. Here's how it works.

Normally when network cards receive a message, they analyse it and discard it if the message was not meant to be for them. However, network cards have a special mode called 'promiscuous mode' that allows them to get all the traffic without discarding it, so all the messages are read and processed. This works for networks using hubs and Wi-Fi networks, but it does not work for networks using switches. Let's see why.

A **hub** is the least expensive, least intelligent and least complicated. Its job is very simple: anything that comes in one port is sent out to the others. Every computer connected to the hub 'sees' everything every other computer on the hub does.

View description

A diagram showing how a hub works. Any data incoming to the hub are broadcast to all connected devices. Any response sent by one device is also sent to all the other devices.

A **switch** does what a hub does, but more efficiently. By paying attention to the traffic that comes across it, it learns which computers are connected to which port. Initially, a switch knows nothing, and simply sends on incoming messages to all ports. Just by accepting that first message, however, the switch has learned something: it knows on which connection the sender of the message is located.

By processing the response, the switch has also learned something else: it now knows on which connection machine 'A' is located. That means subsequent messages destined for machine 'A' need only be sent to that one port. Switches learn the location of the devices they are connected to almost instantaneously. The result is, most network traffic only goes where it needs to, rather than to every port. On busy networks, this can make the network significantly faster.

View description

A diagram showing how a switch works. Any incoming data are initially sent to all devices like with a hub. However a response by one device is only sent where it needs to go and is not sent to any other device.

Now let's look at **active interception** which actually has two meanings. First, it can mean that the attacker is actually interfering with the normal flow of the traffic. Second, it can also refer to a modification of the information gathered. In other words, there is an attempt to modify the integrity or availability of the information that the attackers have intercepted.

If the attacker is outside of the network, there are many ways to get in. If the infrastructure has a Switch SPAN, typically used in IT companies, there is a specific port that can be used for diagnostics that replicates all the traffic from the other ports to that specific exit. So, if the attacker plugs into the port, they could see all the traffic generated. However, this can be difficult since it requires the attacker to be able to get access physically to the switch.

There are other tools that are used for this purpose. In the next exercise, you will be asked to investigate one of them.