Networks

Alexander Lemos's GenCyber outreach project
What is a Network?

A network is a number of interconnected computers, machines, or operations.

The typical home network can consist of:

- A modem
- Router
- Switch(s)
- Access point(s)
- Powerline adapter(s)
- Repeater(s)
- Printer(s)
- Wireless Devices (Laptops, tablets, phones, etc...)
- Desktop Computers
How it works

The router is responsible for most of the work. It assigns each device a unique number called an IP address. This allows other devices on the network to know it exists and communicate to it (this works the other way around as well). Another requirement to be able to communicate on a network is a MAC address. It is made up of six groups of two hexadecimal digits, separated by hyphens which is built in to devices by the manufacturer. This is also a unique code that represents the device, however cannot be changed by the router.
How it works (part 2)

Network devices can transmit/receive data in 1 of two ways. Through a cable, or through WiFi. It transmit/receive data through packets. A packet is a piece of information which was broken down to be able to be sent over a network, or the internet. The size limitation on TCP packet is 64K (65535 bytes). However a packet of this size is quite rare because of network layers that restrict the size of packets. For example the MTU (Maximum Transmission Unit) for Ethernet is 1500 bytes.

<table>
<thead>
<tr>
<th>Packet - E-mail Example</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Header</td>
<td><strong>Sender's IP address</strong>&lt;br&gt;<strong>Receiver's IP address</strong>&lt;br&gt;<strong>Protocol</strong>&lt;br&gt;<strong>Packet number</strong></td>
</tr>
<tr>
<td>Payload</td>
<td><strong>Data</strong></td>
</tr>
<tr>
<td>Trailer</td>
<td><strong>Data to show end of packet</strong>&lt;br&gt;<strong>Error correction</strong></td>
</tr>
</tbody>
</table>
Packet Transmission

When packets are sent wirelessly through WiFi, anyone nearby can capture them. Wireshark is a common tool used for this.
Packets sent from a client to a AP (Access Point) on an encrypted network (such as wpa2) are encrypted using the same key as the network. This means that even if you are on an encrypted network, people who also know the password can decrypt the packets. Intern they could possibly see password that you submit to unencrypted websites, the ones that don't use https. If the AP is not encrypted then the passwords are also visible in the packets. To sum it up, make sure your router/AP uses some type of encryption and only give the password to people you can trust.
4-way handshake

When a device connect wirelessly to a router or access point there is a 4-way handshake. This is how the router/access point can verify with the client that the password is correct. These phases is also responsible for setting up encryption between the two devices.
4-way handshake (part 2)

Hackers can take advantage of this 4-way handshake by capturing the packets with the encrypted keys. It is typically not much use to the hacker right away because it is encrypted. However hackers can try word lists full of common, predefined passwords and compare it to the packets to see if they match, and if they do, they have the password. The hackers can also try to bruteforce the password by having the computer try every combination of letters, numbers, and symbols you tell it. This is typically impractical since it takes a long time.
Now for the demonstration!