6.1.2 Network Threats Facts

The main component of secure network architecture concepts is network segmentation. The idea behind proper network segmentation is that if a system or systems were compromised, the damage would be limited to that network segment. Also, network segmentation makes it much easier to identify suspicious network traffic since the network traffic is broken into manageable chunks.

For example, if your network has static systems, such as IoT devices, then you probably want to have them on their own network segment. This minimizes the damage they can cause to a single network segment and makes identifying issues with them much easier. You also probably need to segment the wireless network from the wired network, as wireless networks are inherently less secure. Segmenting workstations from authentication servers, SQL servers, or DNS servers is also essential. The most common way to segment networks is to create multiple VLANs for each network zone. These zones can also be separated by firewalls to ensure only specific traffic is allowed.

One way to segment a network is to categorize systems into different zones (for example, a no-trust zone, low-trust zone, medium-trust zone, high-trust zone, and highest-trust zone). The no-trust zone is the zone that you have no control over. It is where everything but your network resides—in other words, it is the internet. The low-trust zone is where publicly available information resides. You do have control over the security of this zone, but it is still exposed to the internet. For example, a web server might reside in this zone. This kind of zone is also referred to as a DMZ, or demilitarized zone.

Network attacks are classified as follows:

Technique	Description
Active Attack	Active attacks are when perpetrators attempt to compromise or affect the operations of a system in some way. For example, trying to brute force the root password on a web server is considered an active attack. A distributed denial of service (DDoS) attack is also an active attack.
Passive Attack	Passive attacks occur when perpetrators attempt to gather information without affecting the flow of that information from the targeted network. For example, sniffing network packets or performing a port scan are both types of passive attacks. The goal isn't to immediately compromise a system, but to learn about that system.
External Attack	External attacks are when unauthorized individuals try to breach a network from off-site. It's key to remember with external attacks that the perpetrator is unauthorized for any level of access to the network.
Inside Attack	Inside attacks, on the other hand, are initiated by authorized individuals inside the network's security perimeter who attempt to access systems or resources to which they're not authorized. For example, an inside attack is a disgruntled employee accessing unauthorized company documents and leaking them to the public.

User education and training is the most important aspect of maintaining a secure network environment. Attackers often send phishing emails to organizations in an attempt to compromise an employee workstation. The workstation is used as a pivot point to gain access to more sensitive systems. Another attack strategy is to compromise an employee's personal device that connects to the company's Wi-Fi. The personal device is then used as a pivot point. Because of this threat, it's imperative to educate users so they are security-aware.

As a security professional, you need to understand your network on multiple levels. You should focus on the following:

Areas of Focus	Description
Entry Points	Recognize all vulnerabilities and entry points for possible attacks. This includes public-facing servers, workstations, Wi-Fi networks, and personal devices. Primarily, you must account for anything that connects to the network as a possible entry point.
Inherent Vulnerabilities	Identify inherent vulnerabilities or systems that lack proper security controls. For example, if your organization needs to use an older version of Windows for a particular application, then you need to identify that system as a vulnerability. IoT and SCADA devices are both systems that lack proper security controls, and therefore must be dealt with appropriately.
Documentation	Document all network assets in your organization and create a suitable network diagram that you can use as a reference. This is probably one of the most important components of knowing your system. If you don't know the underlying infrastructure of your network, then you can't adequately secure it. Proper network documentation and diagrams will not only help you identify a weak network architecture or design, but protect against system sprawl and unknown systems.
Network Baseline	Identify a network baseline. This means that you need to know your systems' normal activity, such as its regular traffic patterns, data usage, network activity, server load, et cetera. Mainly, you need to know what your network looks like in normal day-to-day usage. Knowing this allows you to identify unusual or atypical activity that can indicate an attack in progress or a compromised network. To identify a network baseline, you can use network tools that monitor network traffic and create a graphical representation of the collected data, such as Cisco's NetFlow tool.