PREREQUISITE SKILLS

You've got 99 problems but a skill ain't one!

In this chapter, we'll make sure this is true by talking about the skills needed to land your first cybersecurity job.

First, though, I want to be clear that while we can't teach you everything you need to know, we will cover the fundamentals based on a common baseline of knowledge which rests on network and security fundamentals. This type of prereq knowledge can be learned through formal security certifications like CompTIA Network+ and Security+.

Let's get started by going over the concepts you'll need to know to crush an interview, starting with our good ol' reliable friend, networking.

Networking

This section isn't about talking to people; instead, we're covering the basics of the modern TCP/IP stack.

The Transmission Control Protocol and Internet Protocol (TCP/IP) was created in the 1970s by DARPA scientists, Vinton Cerf and Bob Kahn. At that time, no standardized network standard existed, but after a decade of tests and refinement, the TCP/IP stack was launched in 1983.

Soon, the US Department of Defense adopted it, securing TCP/IP as the standard moving forward.

The TCP/IP stack consists of four layers, each one solving a set of problems around data transmission. This is where the magic happens. If you need to send a file or email, the TCP/IP stack goes to work for you.

Alternatively, there's a seven-layer model called the Open Systems Interconnection (OSI) model. OSI is generally used more because it provides a more granular view of the encapsulation process. Moving forward, we'll use the OSI model. Let's take a quick look at both for comparison:

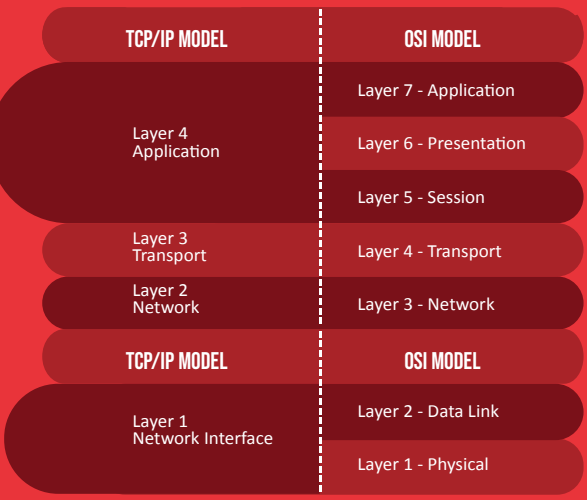

FIGURE 4-1: TCP/IP AND OSI MODEL

If you're curious to learn more, search YouTube for "OSI Model Encapsulation" to discover informative videos breaking down the process through animation for easier understanding.

Let's talk about IP addresses now. There are two types:

- IPv4 (10.0.0.1) is the previous standard of how machines on the internet communicate with each other. While 4 billion addresses seemed like plenty at one time, the increasing Internet landscape means we've started running out of 32-bit IPv4 addresses.
- IPv6 (2001:0db8:85a3:0000:0000:8a2e:0370:7334) is the updated standard for identifying computers on the Internet. It also provides a unique identifier but has been adjusted to 128-bit.

There are also two type of network spaces:

- Public, a network that is accessible to the public internet. Generally leased by an Internet Service Provider (ISP).
- Private, a network that is owned and managed by an individual or organization.

Using networking devices, people typically have one public IP address that is the single point of access to the broader public internet for the many internet connected things in your home. However, organizations typically need many public IP addresses so that people and other organizations on the broader internet can access their services.

ADDRESS SPACE	SUBNET MASK	TOTAL IP ADDRESSES
10.0.0.0 - 10.255.255.255	10.0.0.0/8	16,777,216
192.168.0.0 -192.168.255.255	192.168.0.0/16	1,048,576
172.16.0.0 - 172.31.255.255	172.16.0.0/12	65,536

FIGURE 4-2: RFC 1918 ADDRESSES

Beyond the RFC1918 address space, you'll want to know the common port numbers and differences between TCP and UDP.

- TCP relies on an established connection called a three-way handshake and UDP protocol. If a piece of data is missed in transit, TCP will resend the missed packet and put the packets back in order. TCP connections are used when every bit of data needs to arrive at the destination, like a file transfer. Without all bits and bytes, a file can't run.
- UDP sends messages and doesn't care if they get there or not. We often jokingly call it "Unreliable Dang Protocol" for this reason. UDP is often used for video streaming.

PORT NUMBER	PROTOCOL	APPLICATION
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP,TCP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
443	V	SSL

FIGURE 4-3: COMMON PORT NUMBERS

Another item to address is the three-way handshake. Let's try to break this down in an easy-to-understand way:

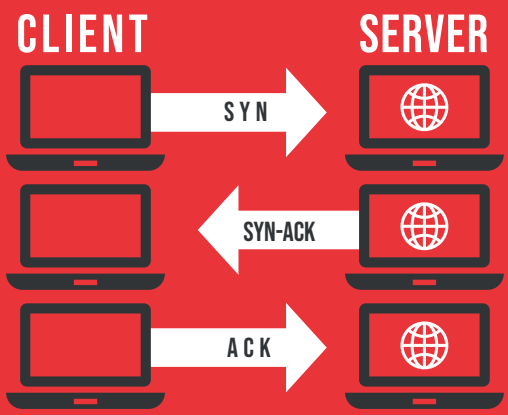

FIGURE 4-4: THREE-WAY HANDSHAKE

- Let's say you're uploading a file to an image hosting website.
- Your computer first establishes a connection to the server by sending an SYN packet.
- The server then sends a SYN and Acknowledge packet back.
- The client sends the Acknowledge packet back.
- The three-way handshake is now complete.

This process will matter in your new SOC analyst job if, say, a host on the public Internet attacks your network's perimeter. You may only see a SYN packet, which sometimes occurs if firewalls drop it because it's not approved traffic.

But if you suspect a computer on your network is communicating with a malicious host and the handshake process has been completed, it's likely they have actively communicated, and some data may have been transferred.

With the basics of networking established, let's move on to related security.

Network Security

When we refer to CIA related to cybersecurity, we are talking about Confidentiality, Integrity, and Availability. All security can be broken down from these three high-level categories:

1. Confidentiality refers to the secrecy of information, making sure that only the intended people can see the information.
2. Integrity refers to the correctness of the data, ensuring you're only consuming data that you intend to, and that the data is complete and unaltered.
3. Availability ensures the data can be used when needed.

Other vital terms related to the basic tenets of security include:

- Firewalls ensure that network resources are only accessed by approved individuals.
- Access control lists (ACLs) ensure the general internet can't access private networks. ACLs act as confidentiality controls and availability controls.
- Network perimeters are boundaries between public Internet space and RPC1918 private Internet space. Perimeters are set by networking appliances.
- Least privilege is a concept related to access control models that says no one needs more access than the absolute minimum needed.
- Separation of duties refers to important duties being separated to provide less opportunity for fraud.

Cryptography

When we say cryptography, we're referring to a method of storing and transmitting data so that only the audience it's intended for can read and process it.

Cryptography principles require you to know the difference between encryption and hashing:

- Encryption refers to changing data in a way that makes it unreadable with the intent that the data will be changed back to a readable state.
- Hashing takes a set of data and creates a unique fingerprint from it.

The main difference between encryption and hashing is that a hash is one way; there's no viable way to turn the unique string of characters, or the fingerprint, back into the original characters.

Endpoint Security

90% of all malware infections come from emails. Networking and network security are important, but the front lines of the cybersecurity war are fought at your network endpoints.

Targeted devices include laptops, smartphones, and printers, to name a few. Because there are so many devices on the market, endpoint security is a challenge.

The most valuable skill here will be understanding how each operating system can be exploited or compromised. The three most common are Windows, Unix, and MacOS.

- Our first OS, Windows, is the global market leader for user endpoints. In fact, 87% of all companies run some version of Windows. Even though newer iterations exist, many older versions are still used. Unfortunately, older Windows OSs aren't maintained when newer ones are released, meaning zero security patches or help desk support. In fact, about 30% of all Windows users are using a version that's no longer supported, opening up many targetable systems for cyber criminals and script kiddies around the world. Windows is often targeted in the following ways:

    1. Phishing: users unknowingly open fraudulent links or attachments that reveal personal and sensitive information.

    2. Weak passwords: users choosing passwords that are easy to guess is the culprit here. Don't use passwords that could be guessed by googling your name or business. Also, using words in password makes them easier to guess. Instead, create longer passwords with a diversified character set to deter hackers.

        To learn to crack passwords as a cybersecurity professional, consider learning tools like John the Ripper and Hashcat, but do not steal or attempt to log in to services with other people's passwords. You may not attempt any hacking activity without expressed or written permission.

    3. User permissions: most at-home users act as the local administrator of their endpoint, which is acceptable in a home setup. In a company, though, allowing the workforce to operate as the local administrator for their endpoints means the risk of malware infection is significantly higher.

- Our next OS, MacOS, is being adopted by more and more companies as their endpoints of choice, making it the second most popular OS in the world. MacOS is a proprietary flavor of Unix, allowing the OS to operate on lower system resources and provide greater user control. Apple owns around 10% of the OS market share, which doesn't sound like a lot but translates to millions and millions of users.

Apple is more secure because it's taken endpoint security to the hardware layer with built-in security chips on the motherboard. These chips encrypt the file storage, ensure a secure boot of the OS every time, and provide application runtime security. Apple's proprietary operating system means that malware authors must tailor their attacks specifically for apple devices which is becoming more common, but overall MacOS has less malware attempts.

Apple's MacOS is a great option for increased security in an enterprise environment, but it usually calls for a high level of IT support and can be expensive.

- Our third OS, Unix/Linux, continues to grow in popularity, owning around 2% of the market share and possessing many different versions. With the advent of the Internet of Things or IoT (which refers to a networking capability that allows information to be sent from objects and devices using the Internet, like a kitchen appliance or fixture in your home), Unix/Linux has infiltrated their way into just about every home and office in some way.

Most Unix/Linux Oss are compromised through misconfigurations in either the OS or the applications hosted on the system rather than malware, which does exist but isn't widespread.

When it comes to endpoints, Unix/Linux users haven't adopted it as a personal OS because of the difficulty in managing it. Linux is used more often as an endpoint OS in cybersecurity and software development communities.

- Other Endpoints we should cover include mobile devices, tablets, and cars with built-in Wi-Fi hotspots. For these operating systems, Android, iOS, and Linux are popular.

  Next, as we discussed earlier, IoT devices include many smart devices you may already have in your home. This biggest risk for these devices is an attack called "credential stuffing" which

a threat actor reuses old passwords found in leaked databases from previous hacks to access your IOT management portal.

Finally, the Chromebook by Google is a low-cost solution for a laptop and touts itself as the most secure OS on the market. Remember, though, that a system is only as secure as the apps it has installed. Google does try to limit these, but there are methods that can circumvent these protections.