Introduction to network protocols

Welcome to week 2, Network potocols

Congratulations on the progress you've made so far!
In this section, you'll learn about how
networks operate using tools and protocols.
These are the concepts that you'll use every
day in your work as a security analyst.
The tools and protocols you'll learn in this section of
the program will help you protect
your organization's network from attacks.
Did you know that malicious actors can take advantage of
data moving from one device to another on a network?
Thankfully, there are tools and
protocols to ensure the network
stays protected against this type of threat.
As an example, I once identified an attack
based solely on the fact they were
using the wrong protocol.
The network traffic volumes were right, and it
was coming from a trusted IP,
but it was on the wrong protocol,
which tipped us off enough to shut down
the attack before they caused real damage.
First, we'll discuss some common network protocols.
Then we'll discuss virtual private networks, or VPNs.
And finally, we'll learn about
firewall security zones and proxy servers.
Now that you have an idea of where we're
headed, let's get started.

Network protocols

Networks benefit from having rules.
Rules ensure that data sent over
the network gets to the right place.
These rules are known as network protocols.
Network protocols are a set of
rules used by two or more devices on
a network to describe the order of

delivery and the structure of the data.

Let's use a scenario to demonstrate
a few different types of network protocols
and how they work together on a network.
Say you want to access your favorite recipe website.
You go to the address bar at the top of
your browser and type in the website's address.
For example: www.yummyrecipesforme.org.
Before you gain access to the website,
your device will establish
communications with a web server.
That communication uses a protocol called
the Transmission Control Protocol, or TCP.
TCP is an internet communications protocol that allows
two devices to form a connection and stream data.

TCP also verifies both devices
before allowing any further communications to take place.
This is often referred to as a handshake.
Once communication is established using a TCP handshake,
a request is made to the network.
Using our example, we have requested
data from the Yummy Recipes For Me server.
Their servers will respond to that request and send
data packets back to
your device so that you can view the web page.

As data packets move across the network,
they move between network devices such as routers.
The Address Resolution Protocol, or ARP, is used to
determine the MAC address of
the next router or device on the path.
This ensures that the data gets to the right place.
Now the communication has been
established and the destination device is known,
it's time to access the Yummy Recipes For Me website.

The Hypertext Transfer Protocol Secure, or HTTPS, is
a network protocol that provides a secure method of
communication between client and website servers.
It allows your web browser to securely send a request
for a webpage to the Yummy Recipes For Me server
and receive a webpage as a response.

Next comes a protocol called the
Domain Name System, or DNS,

which is a network protocol that translate
internet domain names into IP addresses.
The DNS protocol sends
the domain name and the web address to
a DNS server that retrieves
the IP address of the website you were trying to access,
in this case, Yummy Recipes For Me.
The IP address is included as a destination address for
the data packets traveling to
the Yummy Recipes For Me web server.
So just by visiting one website,
the device on your networks are
using four different protocols:
TCP, ARP, HTTPS, and DNS.

These are just some of the protocols
used in network communications.
To help you learn more about the different protocols,
we'll discuss them further
in an upcoming course material.

But how do these protocols relate to security?
Well, on the Yummy Recipes For Me website example,
we used HTTPS, which is
a secure protocol that
requests a webpage from a web server.
HTTPS encrypts data using
the Secure Sockets Layer and Transport Layer Security,
otherwise known as SSL/TLS.
This helps keep the information secure from
malicious actors who want to steal valuable information.

That's a lot of information and
a lot of protocols to remember.
Throughout your career as a security analyst,
you'll become more familiar with
network protocols and use them in your daily activities.

Common network protocols

In this section of the course, you learned about network protocols and how they organize communication over a network. This reading will discuss network protocols in more depth and review some basic protocols that you have learned previously. You will also learn new protocols and discuss some of the ways protocols are involved in network security.

Overview of network protocols

A **network protocol** is a set of rules used by two or more devices on a network to describe the order of delivery and the structure of data. Network protocols serve as instructions that come with the information in the data packet. These instructions tell the receiving device what to do with the data. Protocols are like a common language that allows devices all across the world to communicate with and understand each other.

Even though network protocols perform an essential function in network communication, security analysts should still understand their associated security implications. Some protocols have vulnerabilities that malicious actors exploit. For example, a nefarious actor could use the Domain Name System (DNS) protocol, which resolves web addresses to IP addresses, to divert traffic from a legitimate website to a malicious website containing malware. You'll learn more about this topic in upcoming course materials.

Three categories of network protocols

Network protocols can be divided into three main categories: communication protocols, management protocols, and security protocols. There are dozens of different network protocols, but you don't need to memorize all of them for an entry-level security analyst role. However, it's important for you to know the ones listed in this reading.

Communication protocols

Communication protocols govern the exchange of information in network transmission. They dictate how the data is transmitted between devices and the timing of the communication. They also include methods to recover data lost in transit. Here are a few of them.

- **Transmission Control Protocol (TCP)** is an internet communication protocol that allows two devices to form a connection and stream data. TCP uses a three-way handshake process. First, the device sends a synchronize (SYN) request to a server. Then the server responds with a SYN/ACK packet to acknowledge receipt of the device's request. Once the server receives the final ACK packet from the device, a TCP connection is established. In the TCP/IP model, TCP occurs at the transport layer.
- **User Datagram Protocol (UDP)** is a connectionless protocol that does not establish a connection between devices before a transmission. This makes it less reliable than TCP. But it also means that it works well for transmissions that need to get to their destination quickly. For example, one use of UDP is for internet gaming transmissions. In the TCP/IP model, UDP occurs at the transport layer.
- **Hypertext Transfer Protocol (HTTP)** is an application layer protocol that provides a method of communication between clients and website servers. HTTP uses port 80. HTTP is considered insecure, so it is being replaced on most websites by a secure version, called HTTPS. However, there are still many websites that use the insecure HTTP protocol. In the TCP/IP model, HTTP occurs at the application layer.
- **Domain Name System (DNS)** is a protocol that translates internet domain names into IP addresses. When a client computer wishes to access a website domain using their internet browser, a query is sent to a dedicated DNS server. The DNS server then looks up the IP address that corresponds to the website domain. DNS normally uses UDP on port 53. However, if the DNS reply to a request is large, it will switch to using the TCP protocol. In the TCP/IP model, DNS occurs at the application layer.

Management Protocols

The next category of network protocols is management protocols. Management protocols are used for monitoring and managing activity on a network. They include protocols for error reporting and optimizing performance on the network.

- **Simple Network Management Protocol (SNMP)** is a network protocol used for monitoring and managing devices on a network. SNMP can reset a password on a network device or change its baseline configuration. It can also send requests to network devices for a report on how much of the network’s bandwidth is being used up. In the TCP/IP model, SNMP occurs at the application layer.
- **Internet Control Message Protocol (ICMP)** is an internet protocol used by devices to tell each other about data transmission errors across the network. ICMP is used by a receiving device to send a report to the sending device about the data transmission. ICMP is commonly used as a quick way to troubleshoot network connectivity and latency by issuing the “ping” command on a Linux operating system. In the TCP/IP model, ICMP occurs at the internet layer.

Security Protocols

Security protocols are network protocols that ensure that data is sent and received securely across a network. Security protocols use encryption algorithms to protect data in transit. Below are some common security protocols.

- **Hypertext Transfer Protocol Secure (HTTPS)** is a network protocol that provides a secure method of communication between clients and website servers. HTTPS is a secure version of HTTP that uses secure sockets layer/transport layer security (SSL/TLS) encryption on all transmissions so that malicious actors cannot read the information contained. HTTPS uses port 443. In the TCP/IP model, HTTPS occurs at the application layer.
- **Secure File Transfer Protocol (SFTP)** is a secure protocol used to transfer files from one device to another over a network. SFTP uses secure shell (SSH), typically through TCP port 22. SSH uses Advanced Encryption Standard (AES) and other types of encryption to ensure that unintended recipients cannot intercept the transmissions. In the TCP/IP model, SFTP occurs at the application layer. SFTP is used often with cloud storage. Every time a user uploads or downloads a file from cloud storage, the file is transferred using the SFTP protocol.

Note: The encryption protocols mentioned do not conceal the source or destination IP address of network traffic. This means a malicious actor can still learn some basic information about the network traffic if they intercept it.

Key takeaways

The protocols you learned about in this reading are basic networking protocols that entry-level cybersecurity analysts should know. Understanding how protocols function on a network is essential. Cybersecurity analysts can leverage their knowledge of protocols to successfully mitigate vulnerabilities on a network and potentially prevent future attacks.

Additional network protocols

In previous readings and videos, you learned how network protocols organize the sending and receiving of data across a network. You also learned that protocols can be divided into three categories: communication protocols, management protocols, and security protocols.

This reading will introduce you to a few additional concepts and protocols that will come up regularly in your work as a security analyst. Some protocols are assigned port numbers by the Internet Assigned Numbers Authority (IANA). These port numbers are included in the description of each protocol, if assigned.

Network Address Translation

The devices on your local home or office network each have a private IP address that they use to communicate directly with each other. In order for the devices with private IP addresses to communicate with the public internet, they need to have a public IP address. Otherwise, responses will not be routed correctly. Instead of having a dedicated public IP address for each of the devices on the local network, the router can replace a private source IP address with its public IP address and perform the reverse operation for responses. This process is known as Network Address Translation (NAT) and it generally requires a router or firewall to be specifically configured to perform NAT. NAT is a part of layer 2 (internet layer) and layer 3 (transport layer) of the TCP/IP model.

Private IP Addresses	Public IP Addresses

• Assigned by network admins
• Unique only within private network
• No cost to use
• Address ranges:
  ◦ 10.0.0.0-10.255.255.255
  ◦ 172.16.0.0-172.31.255.255
  ◦ 192.168.0.0-192.168.255.255
	• Assigned by ISP and IANA
	• Unique address in global internet
	• Costs to lease a public IP address
	• Address ranges:
	  ◦ 1.0.0.0-9.255.255.255
	  ◦ 11.0.0.0-126.255.255.255
	  ◦ 128.0.0.0-172.15.255.255
	  ◦ 172.32.0.0-192.167.255.255
	  ◦ 192.169.0.0-233.255.255.255

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is in the management family of network protocols. DHCP is an application layer protocol used on a network to configure devices. It assigns a unique IP address and provides the addresses of the appropriate DNS server and default gateway for each device. DHCP servers operate on UDP port 67 while DHCP clients operate on UDP port 68.

Address Resolution Protocol

By now, you are familiar with IP and MAC addresses. You've learned that each device on a network has both an IP address that identifies it on the network and a MAC address that is unique to that network interface. A device's IP address may change over time, but its MAC address is permanent. Address Resolution Protocol (ARP) is an internet layer protocol in the TCP/IP model used to translate the IP addresses that are found in data packets into the MAC address of the hardware device.

Each device on the network performs ARP and keeps track of matching IP and MAC addresses in an ARP cache. ARP does not have a specific port number.

Telnet

Telnet is an application layer protocol that allows a device to communicate with another device or server. Telnet sends all information in clear text. It uses command line prompts to control another device similar to secure shell (SSH), but Telnet is not as secure as SSH. Telnet can be used to connect to local or remote devices and uses TCP port 23.

Secure shell

Secure shell protocol (SSH) is used to create a secure connection with a remote system. This application layer protocol provides an alternative for secure authentication and encrypted communication. SSH operates over the TCP port 22 and is a replacement for less secure protocols, such as Telnet.

Post office protocol

Post office protocol (POP) is an application layer (layer 4 of the TCP/IP model) protocol used to manage and retrieve email from a mail server. Many organizations have a dedicated mail server on the network that handles incoming and outgoing mail for users on the network. User devices will send requests to the remote mail server and download email messages locally. If you have ever refreshed your email application and had new emails populate in your inbox, you are experiencing POP and internet message access protocol (IMAP) in action. Unencrypted, plaintext authentication uses TCP/UDP port 110 and encrypted emails use Secure Sockets Layer/Transport Layer Security (SSL/TLS) over TCP/UDP port 995. When using POP, mail has to finish downloading on a local device before it can be read and it does not allow a user to sync emails.

Internet Message Access Protocol (IMAP)

IMAP is used for incoming email. It downloads the headers of emails, but not the content. The content remains on the email server, which allows users to access their email from multiple devices. IMAP uses TCP port 143 for unencrypted email and TCP port 993 over the TLS protocol. Using IMAP allows users to partially read email before it is finished downloading and to sync emails. However, IMAP is slower than POP3.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is used to transmit and route email from the sender to the recipient’s address. SMTP works with Message Transfer Agent (MTA) software, which searches DNS servers to resolve email addresses to IP addresses, to ensure emails reach their intended destination. SMTP uses TCP/UDP port 25 for unencrypted emails and TCP/UDP port 587 using TLS for encrypted emails. The TCP port 25 is often used by high-volume spam. SMTP helps to filter out spam by regulating how many emails a source can send at a time.

Protocols and port numbers

Remember that port numbers are used by network devices to determine what should be done with the information contained in each data packet once they reach their destination. Firewalls can filter out unwanted traffic based on port numbers. For example, an organization may configure a firewall to only allow access to TCP port 995 (POP3) by IP addresses belonging to the organization.

As a security analyst, you will need to know about many of the protocols and port numbers mentioned in this course. They may be used to determine your technical knowledge in interviews, so it’s a good idea to memorize them. You will also learn about new protocols on the job in a security position.

Key takeaways

As a cybersecurity analyst, you will encounter various common protocols in your everyday work. The protocols covered in this reading include NAT, DHCP, ARP, Telnet, SSH, POP3, IMAP, and SMTP. It is equally important to understand where each protocol is structured in the TCP/IP model and which ports they occupy.

Protocol	Port
DHCP	UDP port 67 (servers) UDP port 68 (clients)
ARP	none
Telnet	TCP port 23
SSH	TCP port 22
POP3	TCP/UDP port 110 (unencrypted) TCP/UDP port 995 (encrypted, SSL/TLS)
IMAP	TCP port 143 (unencrypted) TCP port 993 (encrypted, SSL/TLS)
SMTP	TCP/UDP port 587 (encrypted, TLS)

Co

Antara: Working in network security

My name is Antara,
I work on the Enterprise Infrastructure Protection Team at Google.
And our main job responsibility is to protect
the infrastructure that all the amazing Google products run on.
I didn't start with a background in computers, and I did my undergrad
in electronics and communication, which is far away from computers.
I took up the challenge to actually pivot into computers with my first job.
That actually led me to explore the security world even more.
And that's how it led to doing my masters in security, getting expertise in that
area and then come to Google as a security engineer.
A typical day in the life of an entry-level network security engineer
would start with solving a problem.
Maybe you're trying to debug, why is this particular endpoint flooded with so
much traffic?
Or why is this endpoint actually slowing down?
And you would start with, okay, let me get to the endpoint.
Let me capture some traffic on the endpoint and
see what kind of traffic is coming in and going out through this endpoint.
So I would typically go back, think about the problem during lunch.
Sometimes things would click.
When you're thinking you might not have thought about a problem from a different
perspective, you might want to actually see how it looks like.
So you would go about maybe doing a lab recreate.
Let me connect these endpoints and let me try to reproduce the issue.
You might see some things in the lab recreate that you might have not
thought of.
And you might need to actually consult with experts from different domains who
might know better about this area.
Get their view on what the problem is, analyze,
show them everything that you have done.
You might get your solution just by talking to people.
It's a pretty busy day, but it's also a very fun day.
It's like solving puzzles all the time, which is pretty exciting.
Some of the best practices in network security that I've learned are,
don't try to always reinvent the wheel.
There are certain protocols,

there are certain algorithms that have been tried, tested,
analyzed, and they have been deemed secure for being used in network security.
The time that you spend on reinventing the wheel is not going to give you
the benefits that you need.
So it's always good to think about the unsolved challenges instead of
trying to solve the same problem in a different way.
I feel cybersecurity is actually a great field to get into right now, because,
as you see, we are in this information age where tech is exponentially growing.
Just getting into this field is just going to be exciting because there
are amazing new challenges coming up in this field.

Wireless protocols, The evolution of wireless security protocols

So far, you've learned about
a variety of network protocols,
including communication protocols like TCP/IP.
Now we're going to go more in depth
into a class of communication protocols
called the IEEE802.11.
IEEE802.11, commonly known as Wi-Fi,
is a set of standards that define
communications for wireless LANs.
IEEE stands for
the Institute of Electrical and Electronics Engineers,
which is an organization that maintains Wi-Fi standards,
and 802.11 is a suite of
protocols used in wireless communications.
Wi-Fi protocols have adapted
over the years to become more secure and reliable
to provide the same level of
security as a wired connection.
In 2004,
a security protocol called the Wi-Fi Protected Access,
or WPA, was introduced.
WPA is a wireless security protocol
for devices to connect to the internet.
Since then, WPA has evolved
into newer versions, like WPA2 and WPA3,
which include further security improvements,
like more advanced encryption.
As a security analyst,
you might be responsible for making sure that
the wireless connections in your organization are secure.
Let's learn more about security measures.

The evolution of wireless security protocols

In the early days of the internet, all internet communication happened across physical cables. It wasn’t until the mid-1980s that authorities in the United States designated a spectrum of radio wave frequencies that could be used without a license, so there was more opportunity for the internet to expand.

In the late 1990s and early 2000s, technologies were developed to send and receive data over radio. Today, users access wireless internet through laptops, smart phones, tablets, and desktops. Smart devices, like thermostats, door locks, and security cameras, also use wireless internet to communicate with each other and with services on the internet.

Wireless router with antenna connected to WEP, WPA, WPA2, and WPA3 protocols

Introduction to wireless communication protocols

Many people today refer to wireless internet as Wi-Fi. **Wi-Fi** refers to a set of standards that define communication for wireless LANs. Wi-Fi is a marketing term commissioned by the Wireless Ethernet Compatibility Alliance (WECA). WECA has since renamed their organization Wi-Fi Alliance.

Wi-Fi standards and protocols are based on the 802.11 family of internet communication standards determined by the Institute of Electrical and Electronics Engineers (IEEE). So, as a security analyst, you might also see Wi-Fi referred to as IEEE 802.11.

Wi-Fi communications are secured by wireless networking protocols. Wireless security protocols have evolved over the years, helping to identify and resolve vulnerabilities with more advanced wireless technologies.

In this reading, you will learn about the evolution of wireless security protocols from WEP to WPA, WPA2, and WPA3. You’ll also learn how the Wireless Application Protocol was used for mobile internet communications.

Wired Equivalent Privacy

Wired equivalent privacy (WEP) is a wireless security protocol designed to provide users with the same level of privacy on wireless network connections as they have on wired network connections. WEP was developed in 1999 and is the oldest of the wireless security standards.

WEP is largely out of use today, but security analysts should still understand WEP in case they encounter it. For example, a network router might have used WEP as the default security protocol and the network administrator never changed it. Or, devices on a network might be too old to support newer Wi-Fi security protocols. Nevertheless, a malicious actor could potentially break the WEP encryption, so it’s now considered a high-risk security protocol.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) was developed in 2003 to improve upon WEP, address the security issues that it presented, and replace it. WPA was always intended to be a transitional measure so backwards compatibility could be established with older hardware.

The flaws with WEP were in the protocol itself and how the encryption was used. WPA addressed this weakness by using a protocol called Temporal Key Integrity Protocol (TKIP). WPA encryption algorithm uses larger secret keys than WEPs, making it more difficult to guess the key by trial and error.

WPA also includes a message integrity check that includes a message authentication tag with each transmission. If a malicious actor attempts to alter the transmission in any way or resend at another time, WPA’s message integrity check will identify the attack and reject the transmission.

Despite the security improvements of WPA, it still has vulnerabilities. Malicious actors can use a key reinstallation attack (or KRACK attack) to decrypt transmissions using WPA. Attackers can insert themselves in the WPA authentication handshake process and insert a new encryption key instead of the dynamic one assigned by WPA. If they set the new key to all zeros, it is as if the transmission is not encrypted at all.

Because of this significant vulnerability, WPA was replaced with an updated version of the protocol called WPA2.

WPA2 & WPA3

WPA2

The second version of Wi-Fi Protected Access—known as WPA2—was released in 2004. WPA2 improves upon WPA by using the Advanced Encryption Standard (AES). WPA2 also improves upon WPA’s use of TKIP. WPA2 uses the Counter Mode Cipher Block Chain Message Authentication Code Protocol (CCMP), which provides encapsulation and ensures message authentication and integrity. Because of the strength of WPA2, it is considered the security standard for all Wi-Fi transmissions today. WPA2, like its predecessor, is vulnerable to KRACK attacks. This led to the development of

WPA3 in 2018.

Personal

WPA2 personal mode is best suited for home networks for a variety of reasons. It is easy to implement, initial setup takes less time for personal than enterprise version. The global passphrase for WPA2 personal version needs to be applied to each individual computer and access point in a network. This makes it ideal for home networks, but unmanageable for organizations.

Enterprise

WPA2 enterprise mode works best for business applications. It provides the necessary security for wireless networks in business settings. The initial setup is more complicated than WPA2 personal mode, but enterprise mode offers individualized and centralized control over the Wi-Fi access to a business network. This means that network administrators can grant or remove user access to a network at any time. Users never have access to encryption keys, this prevents potential attackers from recovering network keys on individual computers.

WPA3

WPA3 is a secure Wi-Fi protocol and is growing in usage as more WPA3 compatible devices are released. These are the key differences between WPA2 and WPA3:

- WPA3 addresses the authentication handshake vulnerability to KRACK attacks, which is present in WPA2.
- WPA3 uses Simultaneous Authentication of Equals (SAE), a password-authenticated, cipher-key-sharing agreement. This prevents attackers from downloading data from wireless network connections to their systems to attempt to decode it.
- WPA3 has increased encryption to make passwords more secure by using 128-bit encryption, with WPA3-Enterprise mode offering optional 192-bit encryption.

Key takeaways

As a security analyst, knowing the history of how Wi-Fi security protocols developed helps you to better understand what to consider when protecting wireless networks. It’s important that you understand the vulnerabilities of each protocol and how important it is that devices on your network use the most up-to-date security technologies.