

Connect and Protect: Networks and Network Security

Module 1 - Network Architecture

What are networks?

- A network is a group of connected devices. The devices on a network can communicate with each other over network cables, or wireless connections. Networks in your home and office can communicate with networks in other locations, and the devices on them.
- Devices need to find each other on a network to establish communications. These are called the IP and MAC addresses.
- Devices can communicate on two types of networks: a local area network, also known as a LAN, and a wide area network, also known as a WAN.
- A local area network, or LAN, spans a small area like an office building, a school, or a home. For example, when a personal device like your cell phone or tablet connects to the WIFI in your house, they form a LAN. The LAN then connects to the internet.
- A wide area network or WAN spans a large geographical area like a city, state, or country. You can think of the internet as one big WAN. An employee of a company in San Francisco can communicate and share resources with another employee in Dublin, Ireland over the WAN.

Network tools

- A hub is a network device that broadcasts information to every device on the network.
- A switch makes connections between specific devices on a network by sending and receiving data between them. A switch is more intelligent than a hub. It only passes data to the intended destination. This makes switches more secure than hubs, and enables them to control the flow of traffic and improve network performance.
- A router is a network device that connects multiple networks together. For example, if a computer in one network wants to send information to a tablet on another network, then the information will be transferred as follows: First, the information travels from the computer to the router. Then, the router reads the destination address, and forwards the data to the intended network's router. Finally, the receiving router directs that information to the tablet.
- A modem is a device that connects your router to the internet, and brings internet access to the LAN. For example, if a computer from one network wants to send information to a device on a network in a different geographic location, it would be transferred as follows: The computer would send information to the router, and the router would then transfer the information through the modem to the internet. The intended recipient's modem receives the information, and transfers it to the router. Finally, the recipient's router forwards that information to the destination device.

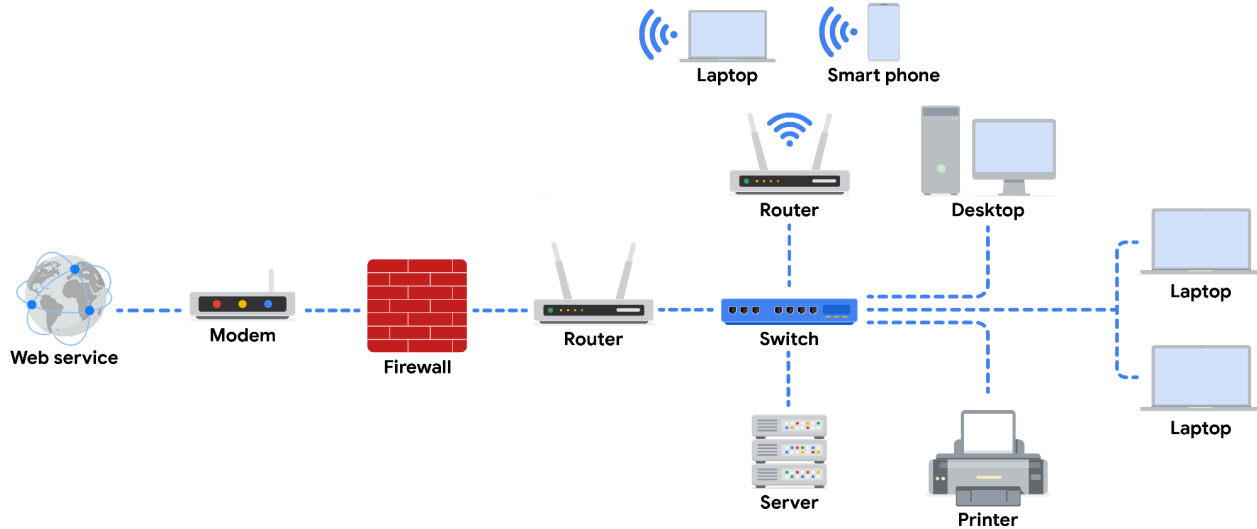
Network tools such as hubs, switches, routers, and modems are physical devices. However, many functions performed by these physical devices can be completed by virtualization tools.

- Virtualization tools are pieces of software that perform network operations. Virtualization tools carry out operations that would normally be completed by a hub, switch, router, or modem, and they are offered by Cloud service providers. These tools provide opportunities for cost savings and scalability.

Once you have a foundational understanding of network architecture, sometimes referred to as network design, you will learn about security vulnerabilities inherent in all networks and how malicious actors attempt to exploit them. In this reading, you will review network devices and connections and investigate a simple network diagram similar to those used every day by network security professionals. Essential tasks of a security analyst include setting up the tools, devices, and protocols used to observe and secure network traffic.

Devices on a network

Network devices are the devices that maintain information and services for users of a network. These devices connect over wired and wireless connections. After establishing a connection to the network, the devices send data packets. The data packets provide information about the source and the destination of the data.



Devices and desktop computers

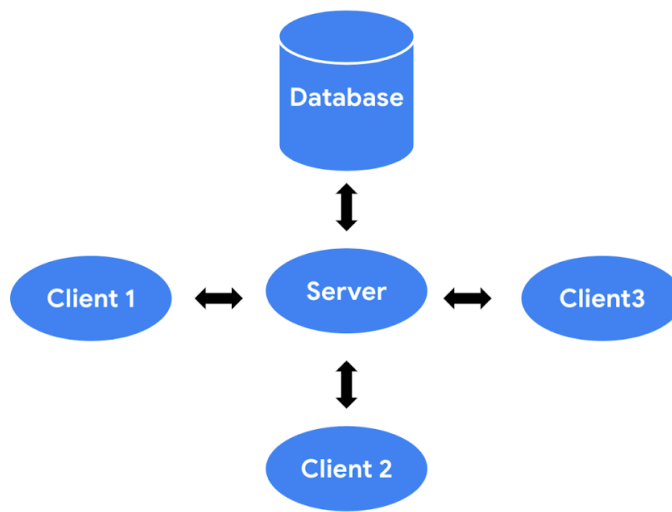
Most internet users are familiar with everyday devices, such as personal computers, laptops, mobile phones, and tablets. Each device and desktop computer has a unique MAC address and IP address, which identify it on the network, and a network interface that sends and receives data packets. These devices can connect to the network via a hard wire or a wireless connection.

Firewalls

A **firewall** is a network security device that monitors traffic to or from your network. Firewalls can also restrict specific incoming and outgoing network traffic. The organization configures the security rules. Firewalls often reside between the secured and controlled internal network and the untrusted network resources outside the organization, such as the internet.

Servers

Servers provide a service for other devices on the network. The devices that connect to a server are called clients. The following graphic outlines this model, which is called the client-server model. In this model, clients send requests to the server for information and services. The server performs the requests for the clients. Common examples include DNS servers that perform domain name lookups for internet sites, file servers that store and retrieve files from a database, and corporate mail servers that organize mail for a company.



Hubs and switches

Hubs and switches both direct traffic on a local network. A hub is a device that provides a common point of connection for all devices directly connected to it. Hubs additionally repeat all information out to all ports. From a security perspective, this makes hubs vulnerable to eavesdropping. For this reason, hubs are not used as often on modern networks; most organizations use switches instead.

A switch forwards packets between devices directly connected to it. It maintains a MAC address table that matches MAC addresses of devices on the network to port numbers on the switch and forwards incoming data packets according to the destination MAC address.

Routers

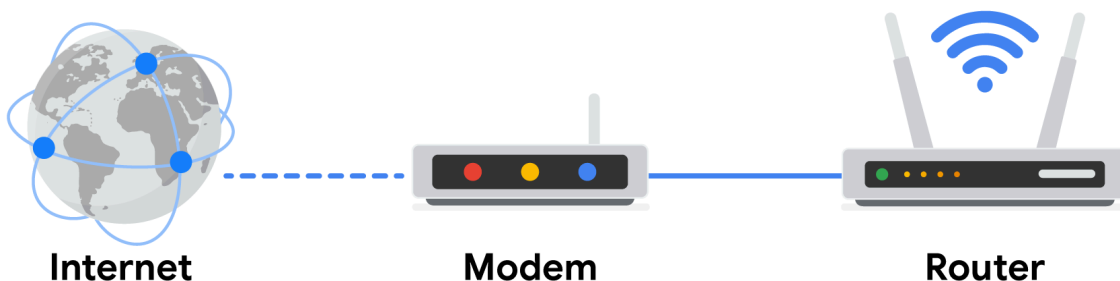
Routers sit between networks and direct traffic, based on the IP address of the destination network. The IP address of the destination network is contained in the IP header. The router reads the header information and forwards the packet to the next router on the path to the destination. This continues until the packet reaches the destination network. Routers can also include a firewall feature that allows or blocks incoming traffic based on information in the transmission. This stops malicious traffic from entering the private network and damaging the local area network.

Modems and wireless access points

Modems

Modems usually interface with an internet service provider (ISP). ISPs provide internet connectivity via telephone lines, coaxial cables, fiber-optic cables, or satellites. Modems receive transmissions from the internet and translate them into digital signals that can be understood by the devices on the network. Usually, modems connect to a router that takes the decoded transmissions and sends them on to the local network.

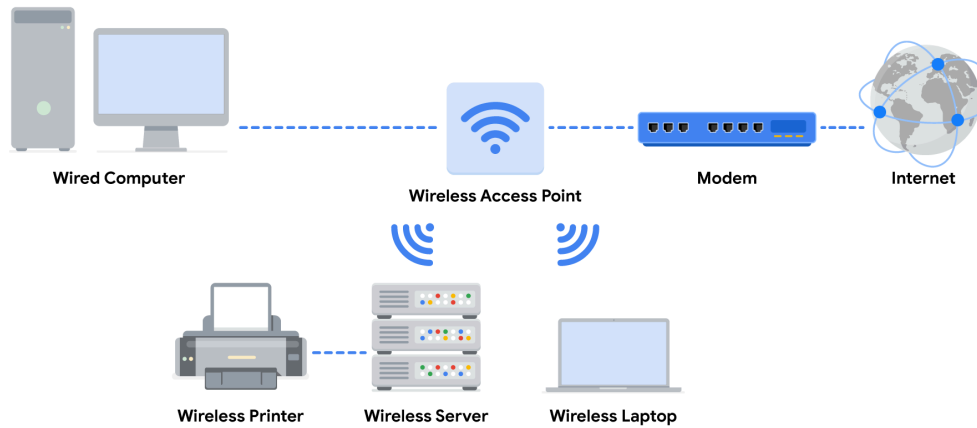
Note: Enterprise networks used by large organizations to connect their users and devices often use other broadband technologies to handle high-volume traffic, instead of using a modem.



Wireless access point

A wireless access point sends and receives digital signals over radio waves creating a wireless network. Devices with wireless adapters connect to the access point using Wi-Fi. Wi-Fi refers to a set of standards that are used by network devices to communicate wirelessly. Wireless access points and the devices connected to them use Wi-Fi

protocols to send data through radio waves where they are sent to routers and switches and directed along the path to their final destination.

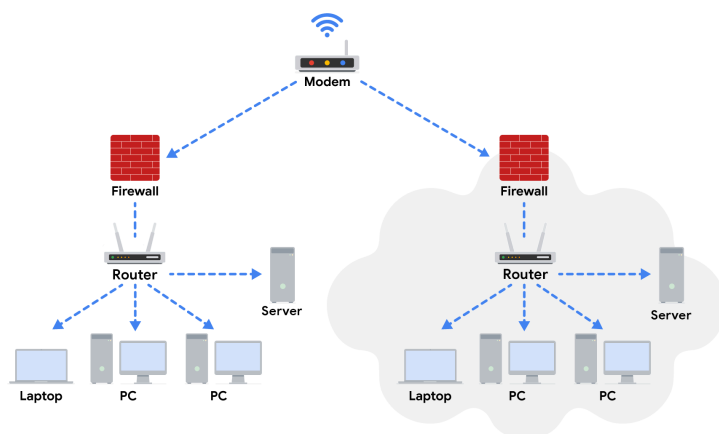


Using network diagrams as a security analyst

Network diagrams allow network administrators and security personnel to imagine the architecture and design of their organization's private network.

Network diagrams are topographical maps that show the devices on the network and how they connect.

Network diagrams use small representative graphics to portray each network device and dotted lines to show how each device connects to the other. Security analysts use network diagrams to learn about network architecture and how to design networks.



Cloud networks

Cloud computing is the practice of using remote servers, applications, and network services that are hosted on the internet instead of on local physical devices.

A cloud network is a collection of servers or computers that stores resources and data in a remote data center that can be accessed via the internet. Because companies don't house the servers at their physical location, these servers are referred to as being "in the cloud".

Traditional networks host web servers from a business in its physical location. However, cloud networks are different from traditional networks because they use remote servers, which allow online services and web applications to be used from any geographic location. Cloud security will become increasingly relevant to many security professionals as more organizations migrate to cloud services.

Cloud service providers offer cloud computing to maintain applications. For example, they provide on-demand storage and processing power that their customers only pay as needed. They also provide business and web analytics that organizations can use to monitor their web traffic and sales.

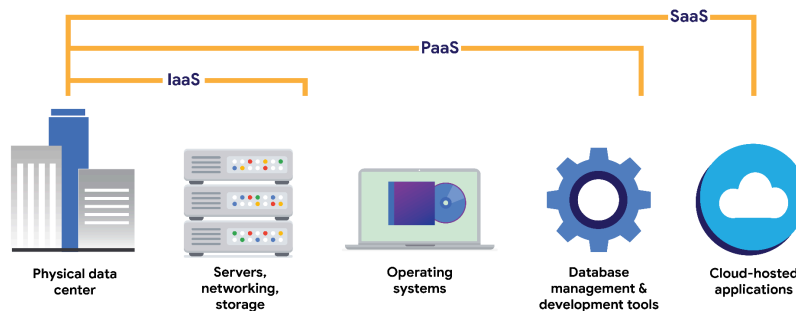
Computing processes in the cloud

Traditional networks are called on-premise networks, which means that all of the devices used for network operations are kept at a physical location owned by the company, like in an office building, for example. **Cloud computing**, however, refers to the practice of using remote servers, applications, and network services that are hosted on the internet instead of at a physical location owned by the company.

A cloud service provider (CSP) is a company that offers cloud computing services. These companies own large data centers in locations around the globe that house millions of servers. Data centers provide technology services, such as storage, and compute at such a large scale that they can sell their services to other companies for a fee. Companies can pay for the storage and services they need and consume them through the CSP's application programming interface (API) or web console.

CSPs provide three main categories of services:

- **Software as a service (SaaS)** refers to software suites operated by the CSP that a company can use remotely without hosting the software.
- **Infrastructure as a service (IaaS)** refers to the use of virtual computer components offered by the CSP. These include virtual containers and storage that are configured remotely through the CSP's API or web console. Cloud-compute and storage services can be used to operate existing applications and other technology workloads without significant modifications. Existing applications can be modified to take advantage of the availability, performance, and security features that are unique to cloud provider services.
- **Platform as a service (PaaS)** refers to tools that application developers can use to design custom applications for their company. Custom applications are designed and accessed in the cloud and used for a company's specific business needs.



Hybrid cloud environments

When organizations use a CSP's services in addition to their on-premise computers, networks, and storage, it is referred to as a hybrid cloud environment. When organizations use more than one CSP, it is called a multi-cloud environment. The vast majority of organizations use hybrid cloud environments to reduce costs and maintain control over network resources.

Software-defined networks

CSPs offer networking tools similar to the physical devices that you have learned about in this section of the course. Next, you'll review software-defined networking in the cloud. Software-defined networks (SDNs) are made up of virtual network devices and services. Just like CSPs provide virtual computers, many SDNs also provide virtual switches, routers, firewalls, and more. Most modern network hardware devices also support network virtualization and software-defined networking. This means that physical switches and routers use software to perform packet routing. In the case of cloud networking, the SDN tools are hosted on servers located at the CSP's data center.

Benefits of cloud computing and software-defined networks

Three of the main reasons that cloud computing is so attractive to businesses are reliability, decreased cost, and increased scalability.

Reliability

Reliability in cloud computing is based on how available cloud services and resources are, how secure connections are, and how often the services are effectively running. Cloud computing allows employees and customers to access the resources they need consistently and with minimal interruption.

Cost

Traditionally, companies have had to provide their own network infrastructure, at least for internet connections. This meant there could be potentially significant upfront costs for companies. However, because CSPs have such large data centers, they are able to offer virtual devices and services at a fraction of the cost required for companies to install, patch, upgrade, and manage the components and software themselves.

Scalability

Another challenge that companies face with traditional computing is scalability. When organizations experience an increase in their business needs, they might be forced to buy more equipment and software to keep up. But what if business decreases shortly after? They might no longer have the business to justify the cost incurred by the upgraded components. CSPs reduce this risk by making it easy to consume services in an elastic utility model as needed. This means that companies only pay for what they need when they need it.

Changes can be made quickly through the CSPs, APIs, or web console—much more quickly than if network technicians had to purchase their own hardware and set it up. For example, if a company needs to protect against a threat to their network, web application firewalls (WAFs), intrusion detection/protection systems (IDS/IPS), or L3/L4 firewalls can be configured quickly whenever necessary, leading to better network performance and security.

Resources for more information

For more information about cloud computing and the services offered, you can review [Google Cloud \(GC\)](#).

Introduction to network communication

- Networks help organizations communicate and connect. But communication makes network attacks more likely because it gives a malicious actor an opportunity to take advantage of vulnerable devices and unprotected networks.
- Communication over a network happens when data is transferred from one point to another. Pieces of data are typically referred to as data packets.
- A data packet is a basic unit of information that travels from one device to another within a network. When data is sent from one device to another across a network, it is sent as a packet that contains information about where the packet is going, where it's coming from, and the content of the message.
- Think about data packets like a piece of physical mail. Imagine you want to send a letter to a friend. The envelope will need to have the address where you want the letter to go and your return address. Inside the envelope is a letter that contains the message that you want your friend to read.
- A data packet is very similar to a physical letter. It contains a header that includes the internet protocol address, the IP address, and the media access control, or MAC, address of the destination device. It also includes a protocol number that tells the receiving device what to do with the information in the packet. Then there's the body of the packet, which contains the message that needs to be transmitted to the receiving device. Finally, at the end of the packet, there's a footer, similar to a signature on a letter, the footer signals to the receiving device that the packet is finished.
- The movement of data packets across a network can provide an indication of how well the network is performing. Network performance can be measured by bandwidth.
- Bandwidth refers to the amount of data a device receives every second. You can calculate bandwidth by dividing the quantity of data by the time in seconds. Speed refers to the rate at which data packets are received or downloaded. Security personnel are interested in network bandwidth and speed because if

either are irregular, it could be an indication of an attack. Packet sniffing is the practice of capturing and inspecting data packets across the network.

- Communication on the network is important for sharing resources and data because it allows organizations to function effectively.

The TCP/IP model

- TCP/IP stands for Transmission Control Protocol and Internet Protocol. TCP/IP is the standard model used for network communication
- First, TCP, or Transmission Control Protocol, is an internet communication protocol that allows two devices to form a connection and stream data. The protocol includes a set of instructions to organize data, so it can be sent across a network. It also establishes a connection between two devices and makes sure that packets reach their appropriate destination.
- The IP in TCP/IP stands for Internet Protocol. IP has a set of standards used for routing and addressing data packets as they travel between devices on a network. Included in the Internet Protocol (IP) is the IP address that functions as an address for each private network. When data packets are sent and received across a network, they are assigned a port.
- Within the operating system of a network device, a port is a software-based location that organizes the sending and receiving of data between devices on a network. Ports divide network traffic into segments based on the service they will perform between two devices. The computers sending and receiving these data segments know how to prioritize and process these segments based on their port number.
- This is like sending a letter to a friend who lives in an apartment building. The mail delivery person not only knows how to find the building, but they also know exactly where to go in the building to find the apartment number where your friend lives.
- Data packets include instructions that tell the receiving device what to do with the information. These instructions come in the form of a port number. Port numbers allow computers to split the network traffic and prioritize the operations they will perform with the data. Some common port numbers are: port 25, which is used for email, port 443, which is used for secure internet communication, and port 20, for large file transfers.

The four layers of the TCP/IP model

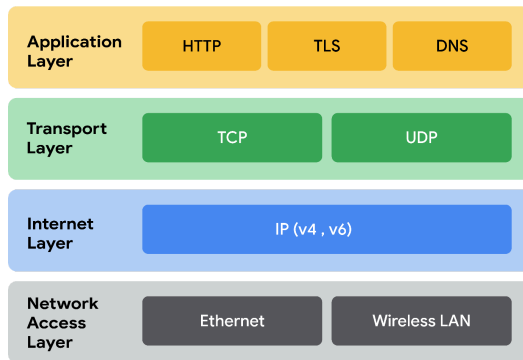
The four layers are: the network access layer, the internet layer, the transport layer, and the application layer.

- Layer one is the network access layer. The network access layer deals with creation of data packets and their transmission across a network. This includes hardware devices connected to physical cables and switches that direct data to its destination.
- Layer two is the internet layer. The internet layer is where IP addresses are attached to data packets to indicate the location of the sender and receiver. The internet layer also focuses on how networks connect to each other. For example, data packets containing information that determine whether they will stay on the LAN or will be sent to a remote network, like the internet.
- The transport layer includes protocols to control the flow of traffic across a network. These protocols permit or deny communication with other devices and include information about the status of the connection. Activities of this layer include error control, which ensures data is flowing smoothly across the network.
- Finally, at the application layer, protocols determine how the data packets will interact with receiving devices. Functions that are organized at the application layer include file transfers and email services.

The TCP/IP model

The **TCP/IP model** is a framework used to visualize how data is organized and transmitted across a network. This model helps network engineers and network security analysts conceptualize processes on the network and communicate where disruptions or security threats occur.

The TCP/IP model has four layers: network access layer, internet layer, transport layer, and application layer. When troubleshooting issues on the network, security professionals can analyze and deduce which layer or layers an attack occurred based on what processes were involved in an incident.



Network access layer

The network access layer, sometimes called the data link layer, deals with the creation of data packets and their transmission across a network. This layer corresponds to the physical hardware involved in network transmission. Hubs, modems, cables, and wiring are all considered part of this layer. The address resolution protocol (ARP) is part of the network access layer. ARP assists IP with directing data packets on the same physical network by mapping IP addresses to MAC addresses on the same physical network.

Internet layer

The internet layer, sometimes referred to as the network layer, is responsible for ensuring the delivery to the destination host, which potentially resides on a different network. It ensures IP addresses are attached to data packets to indicate the location of the sender and receiver. The internet layer also determines which protocol is responsible for delivering the data packets and ensures the delivery to the destination host. Here are some of the common protocols that operate at the internet layer:

- **Internet Protocol (IP).** IP sends the data packets to the correct destination and relies on the Transmission Control Protocol/User Datagram Protocol (TCP/UDP) to deliver them to the corresponding service. IP packets allow communication between two networks. They are routed from the sending network to the receiving network. The TCP/UDP retransmits any data that is lost or corrupt.
- **Internet Control Message Protocol (ICMP).** The ICMP shares error information and status updates of data packets. This is useful for detecting and troubleshooting network errors. The ICMP reports information about packets that were dropped or that disappeared in transit, issues with network connectivity, and packets redirected to other routers.

Transport layer

The transport layer is responsible for delivering data between two systems or networks and includes protocols to control the flow of traffic across a network. TCP and UDP are the two transport protocols that occur at this layer.

Transmission Control Protocol

The **Transmission Control Protocol (TCP)** is an internet communication protocol that allows two devices to form a connection and stream data. It ensures that data is reliably transmitted to the destination service. TCP contains the port number of the intended destination service, which resides in the TCP header of a TCP/IP packet.

User Datagram Protocol

The **User Datagram Protocol (UDP)** is a connectionless protocol that does not establish a connection between devices before transmissions. It is used by applications that are not concerned with the reliability of the transmission. Data sent over UDP is not tracked as extensively as data sent using TCP. Because UDP does not

establish network connections, it is used mostly for performance sensitive applications that operate in real time, such as video streaming.

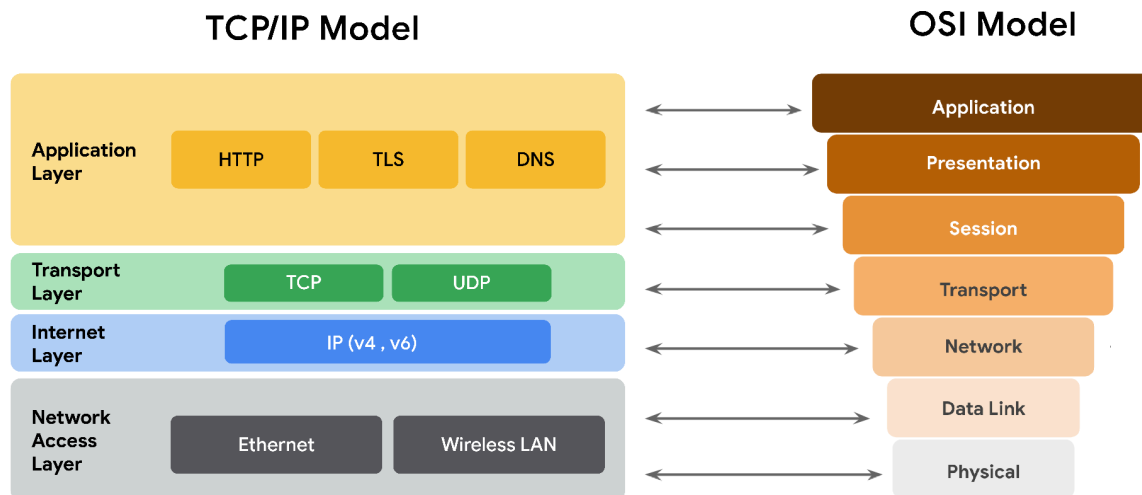
Application layer

The application layer in the TCP/IP model is similar to the application, presentation, and session layers of the OSI model. The application layer is responsible for making network requests or responding to requests. This layer defines which internet services and applications any user can access. Protocols in the application layer determine how the data packets will interact with receiving devices. Some common protocols used on this layer are:

- Hypertext transfer protocol (HTTP)
- Simple mail transfer protocol (SMTP)
- Secure shell (SSH)
- File transfer protocol (FTP)
- Domain name system (DNS)

Application layer protocols rely on underlying layers to transfer the data across the network.

TCP/IP model versus OSI model



The **OSI** visually organizes network protocols into different layers. Network professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.

The TCP/IP model combines multiple layers of the OSI model. There are many similarities between the two models. Both models define standards for networking and divide the network communication process into different layers. The TCP/IP model is a simplified version of the OSI model.

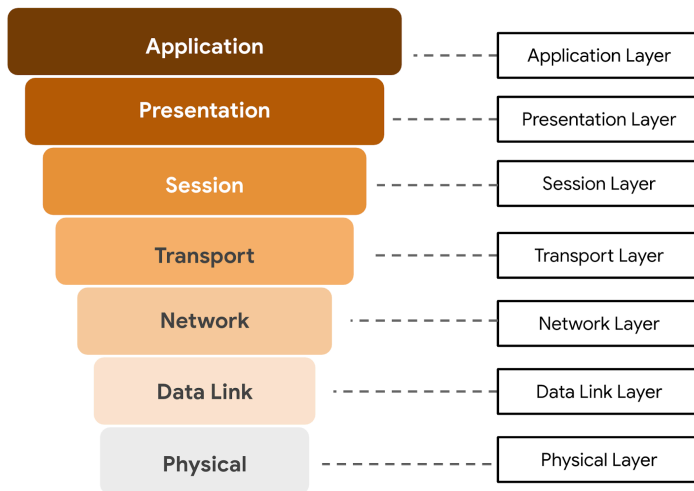
The TCP/IP model vs. the OSI model

The **TCP/IP model** is a framework used to visualize how data is organized and transmitted across a network. This model helps network engineers and network security analysts design the data network and conceptualize processes on the network and communicate where disruptions or security threats occur.

The TCP/IP model has four layers: network access layer, internet layer, transport layer, and application layer. When analyzing network events, security professionals can determine what layer or layers an attack occurred in based on what processes were involved in the incident.

The **OSI model** is a standardized concept that describes the seven layers computers use to communicate and send data over the network. Network and security professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.

OSI Model



Some organizations rely heavily on the TCP/IP model, while others prefer to use the OSI model. As a security analyst, it's important to be familiar with both models. Both the TCP/IP and OSI models are useful for understanding how networks work.

Layer 7: Application layer

The application layer includes processes that directly involve the everyday user. This layer includes all of the networking protocols that software applications use to connect a user to the internet. This characteristic is the identifying feature of the application layer—user connection to the network via applications and requests. An example of a type of communication that happens at the application layer is using a web browser. The internet browser uses HTTP or HTTPS to send and receive information from the website server. The email application uses simple mail transfer protocol (SMTP) to send and receive email information. Also, web browsers use the domain name system (DNS) protocol to translate website domain names into IP addresses which identify the web server that hosts the information for the website.

Layer 6: Presentation layer

Functions at the presentation layer involve data translation and encryption for the network. This layer adds to and replaces data with formats that can be understood by applications (layer 7) on both sending and receiving systems. Formats at the user end may be different from those of the receiving system. Processes at the presentation layer require the use of a standardized format.

Some formatting functions that occur at layer 6 include encryption, compression, and confirmation that the character code set can be interpreted on the receiving system. One example of encryption that takes place at this layer is SSL, which encrypts data between web servers and browsers as part of websites with HTTPS.

Layer 5: Session layer

A session describes when a connection is established between two devices. An open session allows the devices to communicate with each other. Session layer protocols occur to keep the session open while data is being transferred and terminate the session once the transmission is complete.

The session layer is also responsible for activities such as authentication, reconnection, and setting checkpoints during a data transfer. If a session is interrupted, checkpoints ensure that the transmission picks up at the last session checkpoint when the connection resumes. Sessions include a request and response between applications. Functions in the session layer respond to requests for service from processes in the presentation layer (layer 6) and send requests for services to the transport layer (layer 4).

Layer 4: Transport layer

The transport layer is responsible for delivering data between devices. This layer also handles the speed of data transfer, flow of the transfer, and breaking data down into smaller segments to make them easier to transport. Segmentation is the process of dividing up a large data transmission into smaller pieces that can be processed by the receiving system. These segments need to be reassembled at their destination so they can be processed at the session layer (layer 5). The speed and rate of the transmission also has to match the connection speed of the destination system. TCP and UDP are transport layer protocols.

Layer 3: Network layer

The network layer oversees receiving the frames from the data link layer (layer 2) and delivers them to the intended destination. The intended destination can be found based on the address that resides in the frame of the data packets. Data packets allow communication between two networks. These packets include IP addresses that tell routers where to send them. They are routed from the sending network to the receiving network.

Layer 2: Data link layer

The data link layer organizes sending and receiving data packets within a single network. The data link layer is home to switches on the local network and network interface cards on local devices.

Protocols like network control protocol (NCP), high-level data link control (HDLC), and synchronous data link control protocol (SDLC) are used at the data link layer.

Layer 1: Physical layer

As the name suggests, the physical layer corresponds to the physical hardware involved in network transmission. Hubs, modems, and the cables and wiring that connect them are all considered part of the physical layer. To travel across an ethernet or coaxial cable, a data packet needs to be translated into a stream of 0s and 1s. The stream of 0s and 1s are sent across the physical wiring and cables, received, and then passed on to higher levels of the OSI model.

IP addresses and network communication

- IP addresses are used to communicate over a network. IP stands for internet protocol. An internet protocol address, or IP address, is a unique string of characters that identifies a location of a device on the internet. Each device on the internet has a unique IP address, just like every house on a street has its own mailing address.
- There are two types of IP addresses: IP version 4, or IPv4, and IP version 6, or IPv6. Let's look at examples of an IPv4 address.
- IPv4 addresses are written as four, 1, 2, or 3-digit numbers separated by a decimal point. In the early days of the internet, IP addresses were all IPV4. But as the use of the internet grew, all the IPV4 addresses started to get used up, so IPV6 was developed.
- IPv6 addresses are made up of 32 characters. The length of the IPV6 address will allow for more devices to be connected to the internet without running out of addresses as quickly as IPV4.
- IP addresses can be either public or private. Your internet service provider assigns a public IP address that is connected to your geographic location. When network communications goes out from your device on the internet, they all have the same public-facing address. Just like all the roommates in one home share the same mailing address, all the devices on a network share the same public-facing IP address.
- Private IP addresses are only seen by other devices on the same local network. This means that all the devices on your home network can communicate with each other using unique IP addresses that the rest of the internet can't see.

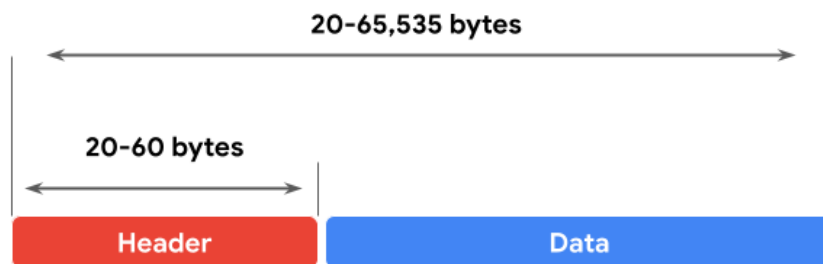
- Another kind of address used in network communications is called a MAC address. A MAC address is a unique alphanumeric identifier that is assigned to each physical device on a network. When a switch receives a data packet, it reads the MAC address of the destination device and maps it to a port. It then keeps this information in a MAC address table. Think of the MAC address table like an address book that the switch uses to direct data packets to the appropriate device.

Operations at the network layer

Functions at the network layer organize the addressing and delivery of data packets across the network and internet from the host device to the destination device. This includes directing the packets from one router to another router across the internet, based on the internet protocol (IP) address of the destination network. The destination IP address is contained within the header of each data packet. This address will be stored for future routing purposes in routing tables along the packet's path to its destination.

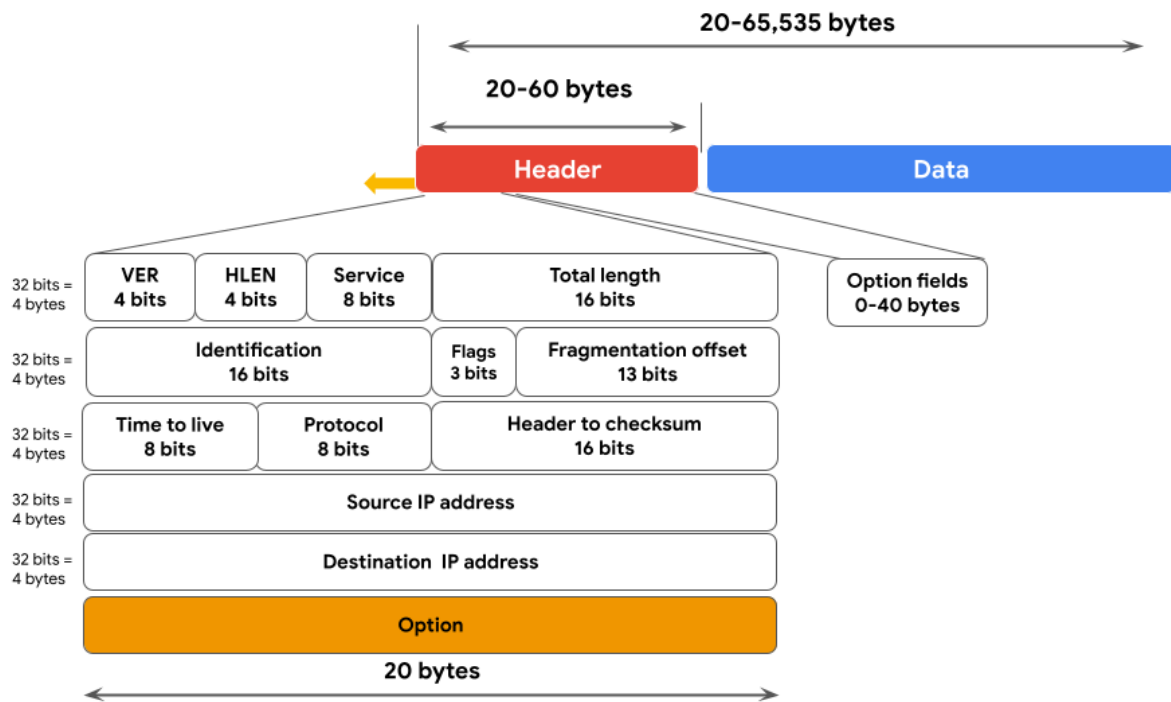
All data packets include an IP address; this is referred to as an IP packet or datagram. A router uses the IP address to route packets from network to network based on information contained in the IP header of a data packet. Header information communicates more than just the address of the destination. It also includes information such as the source IP address, the size of the packet, and which protocol will be used for the data portion of the packet.

Format of an IPv4 packet



Next, you can review the format of an IP version 4 (IPv4) packet and review a detailed graphic of the packet header. An IPv4 packet is made up of two sections, the header and the data:

- An IPv4 header format is determined by the IPv4 protocol and includes the IP routing information that devices use to direct the packet. The size of the IPv4 header ranges from 20 to 60 bytes. The first 20 bytes are a fixed set of information containing data such as the source and destination IP address, header length, and total length of the packet. The last set of bytes can range from 0 to 40 and consists of the options field.
- The length of the data section of an IPv4 packet can vary greatly in size. However, the maximum possible size of an IPv4 packet is 65,535 bytes. It contains the message being transferred over the internet, like website information or email text.



There are 13 fields within the header of an IPv4 packet:

- **Version (VER):** This 4 bit component tells receiving devices what protocol the packet is using. The packet used in the illustration above is an IPv4 packet.
- **IP Header Length (HLEN or IHL):** HLEN is the packet's header length. This value indicates where the packet header ends and the data segment begins.
- **Type of Service (ToS):** Routers prioritize packets for delivery to maintain quality of service on the network. The ToS field provides the router with this information.
- **Total Length:** This field communicates the total length of the entire IP packet, including the header and data. The maximum size of an IPv4 packet is 65,535 bytes.
- **Identification:** For IPv4 packets that are larger than 65,535 bytes, the packets are divided, or fragmented, into smaller IP packets. The identification field provides a unique identifier for all the fragments of the original IP packet so that they can be reassembled once they reach their destination.
- **Flags:** This field provides the routing device with more information about whether the original packet has been fragmented and if there are more fragments in transit.
- **Fragmentation Offset:** The fragment offset field tells routing devices where in the original packet the fragment belongs.
- **Time to Live (TTL):** TTL prevents data packets from being forwarded by routers indefinitely. It contains a counter that is set by the source. The counter is decremented by one as it passes through each router along its path. When the TTL counter reaches zero, the router currently holding the packet will discard the packet and return an ICMP Time Exceeded error message to the sender.
- **Protocol:** The protocol field tells the receiving device which protocol will be used for the data portion of the packet.
- **Header Checksum:** The header checksum field contains a checksum that can be used to detect corruption of the IP header in transit. Corrupted packets are discarded.
- **Source IP Address:** The source IP address is the IPv4 address of the sending device.
- **Destination IP Address:** The destination IP address is the IPv4 address of the destination device.
- **Options:** The options field allows for security options to be applied to the packet if the HLEN value is greater than five. The field communicates these options to the routing devices.

Difference between IPv4 and IPv6

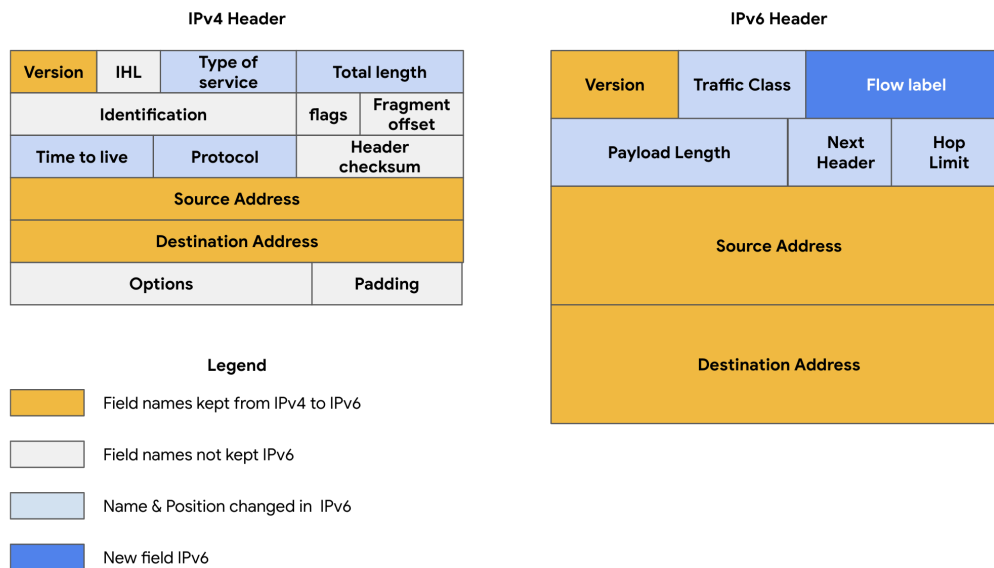
In an earlier part of this course, you learned about the history of IP addressing. As the internet grew, it became clear that all of the IPv4 addresses would eventually be depleted; this is called IPv4 address exhaustion. At the

time, no one had anticipated how many computing devices would need an IP address. IPv6 was developed to mitigate IPv4 address exhaustion and other related concerns.

One of the key differences between IPv4 and IPv6 is the length of the addresses. IPv4 addresses are made of four decimal numbers, each ranging from 0 to 255. Together they span numeric, made of 4 bytes, and allow for up to 4.3 billion possible addresses. IPv4 addresses are made up of four strings and the numbers range from 0 to 255. An example of an IPv4 address would be: 198.51.100.0. IPv6 addresses are made of eight hexadecimal numbers consisting of four hexadecimal digits. Together, they span made up of 16 bytes, and allow for up to 340 undecillion addresses (340 followed by 36 zeros). An example of an IPv6 address would be:

2002:0db8:0000:0000:0000:ff21:0023:1234.

There are also some differences in the layout of an IPv6 packet header. The IPv6 header format is much simpler than IPv4. For example, the IPv4 Header includes the IHL, Identification, and Flags fields, whereas the IPv6 does not. The IPv6 header only introduces the Flow Label field, where the Flow Label identifies a packet as requiring special handling by other IPv6 routers.



There are some important security differences between IPv4 and IPv6. IPv6 offers more efficient routing and eliminates private address collisions that can occur on IPv4 when two devices on the same network are attempting to use the same address.

Terms and definitions from Course 3, Module 1

- **Bandwidth:** The maximum data transmission capacity over a network, measured by bits per second
- **Cloud computing:** The practice of using remote servers, application, and network services that are hosted on the internet instead of on local physical devices
- **Cloud network:** A collection of servers or computers that stores resources and data in remote data centers that can be accessed via the internet
- **Data packet:** A basic unit of information that travels from one device to another within a network
- **Hub:** A network device that broadcasts information to every device on the network
- **Internet Protocol (IP):** A set of standards used for routing and addressing data packets as they travel between devices on a network
- **Internet Protocol (IP) address:** A unique string of characters that identifies the location of a device on the internet
- **Local Area Network (LAN):** A network that spans small areas like an office building, a school, or a home
- **Media Access Control (MAC) address:** A unique alphanumeric identifier that is assigned to each physical device on a network
- **Modem:** A device that connects your router to the internet and brings internet access to the LAN
- **Network:** A group of connected devices

- **Open systems interconnection (OSI) model:** A standardized concept that describes the seven layers computers use to communicate and send data over the network
- **Packet sniffing:** The practice of capturing and inspecting data packets across a network
- **Port:** A software-based location that organizes the sending and receiving of data between devices on a network
- **Router:** A network device that connects multiple networks together
- **Speed:** The rate at which a device sends and receives data, measured by bits per second
- **Switch:** A device that makes connections between specific devices on a network by sending and receiving data between them
- **TCP/IP model:** A framework used to visualize how data is organized and transmitted across a network
- **Transmission Control Protocol (TCP):** An internet communication protocol that allows two devices to form a connection and stream data
- **User Datagram Protocol (UDP):** A connectionless protocol that does not establish a connection between devices before transmissions
- **Wide Area Network (WAN):** A network that spans a large geographic area like a city, state, or country

Module 2 - Network Operations

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.

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 web page 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 translates 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 devices 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.

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.

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

- 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

Public IP Addresses

- 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 mainly a network access 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.

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)

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.

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.

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.

Firewalls and network security measures

- A firewall is a network security device that monitors traffic to and from your network. It either allows traffic or it blocks it based on a defined set of security rules. A firewall can use port filtering, which blocks or allows certain port numbers to limit unwanted communication. For example, it could have a rule that only allows communications on port 443 for HTTPS or port 25 for email and blocks everything else. These firewall settings will be determined by the organization's security policy.
- A hardware firewall is considered the most basic way to defend against threats to a network. A hardware firewall inspects each data packet before it's allowed to enter the network. A software firewall performs the same functions as a hardware firewall, but it's not a physical device. Instead, it's a software program installed on a computer or on a server. If the software firewall is installed on a computer, it will analyze all the traffic received by that computer. If the software firewall is installed on a server, it will protect all the devices connected to the server. A software firewall typically costs less than purchasing a separate physical device, and it doesn't take up any extra space. But because it is a software program, it will add some processing burden to the individual devices.
- Organizations may choose to use a cloud-based firewall. Cloud service providers offer firewalls as a service, or FaaS, for organizations. Cloud-based firewalls are software firewalls hosted by a cloud service provider. Organizations can configure the firewall rules on the cloud service provider's interface, and the firewall will perform security operations on all incoming traffic before it reaches the organization's onsite network. Cloud-based firewalls also protect any assets or processes that an organization might be using in the cloud.
- All the firewalls we have discussed can be either stateful or stateless. The terms "stateful" and "stateless" refer to how the firewall operates. Stateful refers to a class of firewall that keeps track of information passing through it and proactively filters out threats. A stateful firewall analyzes network traffic for characteristics and behavior that appear suspicious and stops them from entering the network. Stateless refers to a class of firewall that operates based on predefined rules and does not keep track of information from data packets. A stateless firewall only acts according to preconfigured rules set by the firewall administrator. The rules programmed by the firewall administrator tell the device what to accept and what to reject. A stateless firewall doesn't store analyzed information. It also doesn't discover

suspicious trends like a stateful firewall does. For this reason, stateless firewalls are considered less secure than stateful firewalls.

- A next generation firewall, or NGFW, provides even more security than a stateful firewall. Not only does an NGFW provide stateful inspection of incoming and outgoing traffic, but it also performs more in-depth security functions like deep packet inspection and intrusion protection. Some NGFWs connect to cloud-based threat intelligence services so they can quickly update to protect against emerging cyber threats.

Virtual private networks (VPNs)

- ◆ When you connect to the internet, your internet service provider receives your network's requests and forwards it to the correct destination server.
- ◆ But your internet requests include your private information.
- ◆ This includes some information that you want to keep private, like bank accounts and credit card numbers.
- ◆ A virtual private network, also known as a VPN, is a network security service that changes your public IP address and hides your virtual location so that you can keep your data private when you're using a public network like the internet.
- ◆ VPNs also encrypt your data as it travels across the internet to preserve confidentiality. A VPN service performs encapsulation on your data in transit.
- ◆ Encapsulation is a process performed by a VPN service that protects your data by wrapping sensitive data in other data packets.
- ◆ This is a security threat because it shows the IP and virtual location of your private network. This means you won't be able to connect to the internet site or the service that you want.
- ◆ Encapsulation solves this problem while still maintaining your privacy. VPN services encrypt your data packets and encapsulate them in other data packets that the routers can read.
- ◆ This allows your network requests to reach their destination, but still encrypts your personal data so it's unreadable while in transit.
- ◆ A VPN also uses an encrypted tunnel between your device and the VPN server. The encryption is unhackable without a cryptographic key, so no one can access your data.

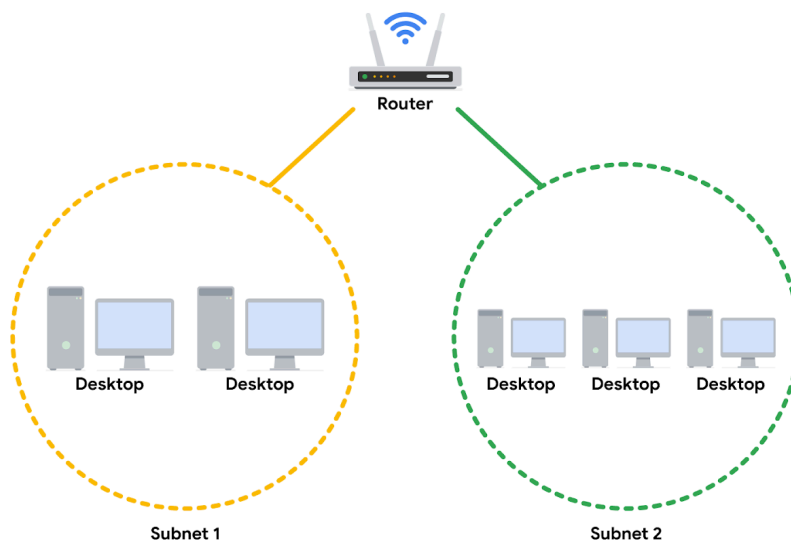
Security zones

- ❖ Security zones are a segment of a network that protects the internal network from the internet.
 - They are a part of a security technique called network segmentation that divides the network into segments. Each network segment has its own access permissions and security rules. Security zones control who can access different segments of a network. Security zones act as a barrier to internal networks, maintain privacy within corporate groups, and prevent issues from spreading to the whole network.
 - One example of network segmentation is a hotel that offers free public Wi-Fi. The unsecured guest network is kept separate from another encrypted network used by the hotel staff.
- ❖ Additionally, an organization's network can be divided into subnetworks, or subnets, to maintain privacy for each department in an organization.
 - For instance, at a university, there may be a faculty subnet and a separate students subnet. If there is contamination on the student's subnet, network administrators can isolate it and keep the rest of the network free from contamination.
- ❖ An organization's network is classified into two types of security zones.
 - First, there's the uncontrolled zone, which is any network outside of the organization's control, like the internet. Then, there's the controlled zone, which is a subnet that protects the internal network from the uncontrolled zone. There are several types of networks within the controlled

- zone. On the outer layer is the demilitarized zone, or DMZ, which contains public-facing services that can access the internet.
 - This includes web servers, proxy servers that host websites for the public, and DNS servers that provide IP addresses for internet users. It also includes email and file servers that handle external communications.
 - The DMZ acts as a network perimeter to the internal network. The internal network contains private servers and data that the organization needs to protect. Inside the internal network is another zone called the restricted zone. The restricted zone protects highly confidential information that is only accessible to employees with certain privileges.
- ❖ Now, let's try to picture these security zones. Ideally, the DMZ is situated between two firewalls. One of them filters traffic outside the DMZ, and one of them filters traffic entering the internal network.
 - This protects the internal network with several lines of defense. If there's a restricted zone, that too would be protected with another firewall.
 - This way, attacks that penetrate into the DMZ network cannot spread to the internal network, and attacks that penetrate the internal network cannot access the restricted zone.
 - As a security analyst, you may be responsible for regulating access control policies on these firewalls. Security teams can control traffic reaching the DMZ and the internal network by restricting IPs and ports.
 - For example, an analyst may ensure that only HTTPS traffic is allowed to access web servers in the DMZ.

Overview of subnetting

- **Subnetting** is the subdivision of a network into logical groups called subnets. It works like a network inside a network. Subnetting divides up a network address range into smaller subnets within the network. These smaller subnets form based on the IP addresses and network mask of the devices on the network. Subnetting creates a network of devices to function as their own network. This makes the network more efficient and can also be used to create security zones. If devices on the same subnet communicate with each other, the switch changes the transmissions to stay on the same subnet, improving speed and efficiency of the communications.



Classless Inter-Domain Routing notation for subnetting

- Classless Inter-Domain Routing (CIDR) is a method of assigning subnet masks to IP addresses to create a subnet. Classless addressing replaces classful addressing. Classful addressing was used in

the 1980s as a system of grouping IP addresses into classes (Class A to Class E). Each class included a limited number of IP addresses, which were depleted as the number of devices connecting to the internet outgrew the classful range in the 1990s. Classless CIDR addressing expanded the number of available IPv4 addresses.

- CIDR allows cybersecurity professionals to segment classful networks into smaller chunks. CIDR IP addresses are formatted like IPv4 addresses, but they include a slash ("/") followed by a number at the end of the address. This extra number is called the IP network prefix. For example, a regular IPv4 address uses the 198.51.100.0 format, whereas a CIDR IP address would include the IP network prefix at the end of the address, 198.51.100.0/24. This CIDR address encompasses all IP addresses between 198.51.100.0 and 198.51.100.255. The system of CIDR addressing reduces the number of entries in routing tables and provides more available IP addresses within networks. You can try converting CIDR to IPv4 addresses and vice versa through an online conversion tool, like [IPAddressGuide](#), for practice and to better understand this concept.
- **Note:** You may learn more about CIDR during your career, but it won't be covered in any additional depth in this certificate program. For now, you only need a basic understanding of this concept.

Security benefits of subnetting

Subnetting allows network professionals and analysts to create a network within their own network without requesting another network IP address from their internet service provider. This process uses network bandwidth more efficiently and improves network performance. Subnetting is one component of creating isolated subnetworks through physical isolation, routing configuration, and firewalls.

Common network protocols

Network protocols are used to direct traffic to the correct device and service depending on the kind of communication being performed by the devices on the network. Protocols are the rules used by all network devices that provide a mutually agreed upon foundation for how to transfer data across a network.

There are three main categories of network protocols: communication protocols, management protocols, and security protocols.

1. Communication protocols are used to establish connections between servers. Examples include TCP, UDP, and Simple Mail Transfer Protocol (SMTP), which provides a framework for email communication.
2. Management protocols are used to troubleshoot network issues. One example is the Internet Control Message Protocol (ICMP).
3. Security protocols provide encryption for data in transit. Examples include IPsec and SSL/TLS.

Some other commonly used protocols are:

- HyperText Transfer Protocol (HTTP). HTTP is an application layer communication protocol. This allows the browser and the web server to communicate with one another.
- Domain Name System (DNS). DNS is an application layer protocol that translates, or maps, host names to IP addresses.
- Address Resolution Protocol (ARP). ARP is a network layer communication protocol that maps IP addresses to physical machines or a MAC address recognized on the local area network.

Wi-Fi

This section of the course also introduced various wireless security protocols, including WEP, WPA, WPA2, and WPA3. WPA3 encrypts traffic with the Advanced Encryption Standard (AES) cipher as it travels from your device to the wireless access point. WPA2 and WPA3 offer two modes: personal and enterprise. Personal mode is best suited for home networks while enterprise mode is generally utilized for business networks and applications.

Network security tools and practices

Firewalls

Previously, you learned that firewalls are network virtual appliances (NVAs) or hardware devices that inspect and can filter network traffic before it's permitted to enter the private network. Traditional firewalls are configured with rules that tell it what types of data packets are allowed based on the port number and IP address of the data packet.

There are two main categories of firewalls.

- **Stateless:** A class of firewall that operates based on predefined rules and does not keep track of information from data packets
- **Stateful:** A class of firewall that keeps track of information passing through it and proactively filters out threats. Unlike stateless firewalls, which require rules to be configured in two directions, a stateful firewall only requires a rule in one direction. This is because it uses a "state table" to track connections, so it can match return traffic to an existing session

Next generation firewalls (NGFWs) are the most technologically advanced firewall protection. They exceed the security offered by stateful firewalls because they include deep packet inspection (a kind of packet sniffing that examines data packets and takes actions if threats exist) and intrusion prevention features that detect security threats and notify firewall administrators. NGFWs can inspect traffic at the application layer of the TCP/IP model and are typically application aware. Unlike traditional firewalls that block traffic based on IP address and ports, NGFWs rules can be configured to block or allow traffic based on the application. Some NGFWs have additional features like Malware Sandboxing, Network Anti-Virus, and URL and DNS Filtering.

Proxy servers

A proxy server is another way to add security to your private network. Proxy servers utilize network address translation (NAT) to serve as a barrier between clients on the network and external threats. Forward proxies handle queries from internal clients when they access resources external to the network. Reverse proxies function opposite of forward proxies; they handle requests from external systems to services on the internal network. Some proxy servers can also be configured with rules, like a firewall. For example, you can create filters to block websites identified as containing malware.

Virtual Private Networks (VPN)

A VPN is a service that encrypts data in transit and disguises your IP address. VPNs use a process called encapsulation. Encapsulation wraps your encrypted data in an unencrypted data packet, which allows your data to be sent across the public network while remaining anonymous. Enterprises and other organizations use VPNs to help protect communications from users' devices to corporate resources. Some of these resources include servers or virtual machines that host business applications. Individuals also use VPNs to increase personal privacy. VPNs protect user privacy by concealing personal information, including IP addresses, from external servers. A reputable VPN also minimizes its own access to user internet activity by using strong encryption and other security measures. Organizations are increasingly using a combination of VPN and SD-WAN capabilities to secure their networks. A software-defined wide area network (SD-WAN) is a virtual WAN service that allows organizations to securely connect users to applications across multiple locations and over large geographical distances.

Remote access and site-to-site VPNs

Individual users use remote access VPNs to establish a connection between a personal device and a VPN server. Remote access VPNs encrypt data sent or received through a personal device. The connection between the user and the remote access VPN is established through the internet.

Enterprises use site-to-site VPNs largely to extend their network to other networks and locations. This is particularly useful for organizations that have many offices across the globe. IPSec is commonly used in site-to-site VPNs to create an encrypted tunnel between the primary network and the remote network. One disadvantage of site-to-site VPNs is how complex they can be to configure and manage compared to remote VPNs.

WireGuard VPN vs. IPSec VPN

WireGuard and IPSec are two different VPN protocols used to encrypt traffic over a secure network tunnel. The majority of VPN providers offer a variety of options for VPN protocols, such as WireGuard or IPSec. Ultimately, choosing between IPSec and WireGuard depends on many factors, including connection speeds, compatibility with existing network infrastructure, and business or individual needs.

WireGuard VPN

WireGuard is a high-speed VPN protocol, with advanced encryption, to protect users when they are accessing the internet. It's designed to be simple to set up and maintain. WireGuard can be used for both site-to-site connection and client-server connections. WireGuard is relatively newer than IPSec, and is used by many people due to the fact that its download speed is enhanced by using fewer lines of code. WireGuard is also open source, which makes it easier for users to deploy and debug. This protocol is useful for processes that require faster download speeds, such as streaming video content or downloading large files.

IPSec VPN

IPSec is another VPN protocol that may be used to set up VPNs. Most VPN providers use IPSec to encrypt and authenticate data packets in order to establish secure, encrypted connections. Since IPSec is one of the earlier VPN protocols, many operating systems support IPSec from VPN providers. Although IPSec and WireGuard are both VPN protocols, IPSec is older and more complex than WireGuard. Some clients may prefer IPSec due to its longer history of use, extensive security testing, and widespread adoption. However, others may prefer WireGuard because of its potential for better performance and simpler configuration.

Proxy servers

Proxy servers are another system that helps secure networks. The definition of a proxy server is a server that fulfills the request of a client by forwarding them on to other servers. The proxy server is a dedicated server that sits between the internet and the rest of the network. When a request to connect to the network comes in from the internet, the proxy server will determine if the connection request is safe. The proxy server is a public IP address that is different from the rest of the private network. This hides the private network's IP address from malicious actors on the internet and adds a layer of security.

Let's examine how this will work with an example. When a client receives an HTTPS response, they will notice a distorted IP address or no IP address rather than the real IP address of the organization's web server. A proxy server can also be used to block unsafe websites that users aren't allowed to access on an organization's network. A proxy server uses temporary memory to store data that's regularly requested by external servers. This way, it doesn't have to fetch data from an organization's internal servers every time. This enhances security by reducing contact with the internal server.

There are different types of proxy servers that support network security. This is important for security analysts who monitor traffic from various proxy servers and may need to know what purpose they serve. Let's explore some different types of proxy servers. A forward proxy server regulates and restricts a person with access to the internet. The goal is to hide a user's IP address and approve all outgoing requests. In the context of an

organization, a forward proxy server receives outgoing traffic from an employee, approves it, and then forwards it on to the destination on the internet. A reverse proxy server regulates and restricts the internet access to an internal server. The goal is to accept traffic from external parties, approve it, and forward it to the internal servers. This setup is useful for protecting internal web servers containing confidential data from exposing their IP address to external parties. An email proxy server is another valuable security tool. It filters spam email by verifying whether a sender's address was forged. This reduces the risk of phishing attacks that impersonate people known to the organization.

Let's talk about a real world example of an email proxy. Several years ago when I was working at a large U.S. broadband ISP, we used a proxy server to implement multiple layers of anti-spam filtering before a message was allowed in for delivery. It ended up tagging around 95% of messages as spam. The proxy servers would've allowed us to filter and then scale those filters without impacting the underlying email platform.

The case for securing networks

Attackers can infiltrate networks via malware, spoofing, or packet sniffing. Network operations can also be disrupted by attacks such as packet flooding. As we go along, you're going to learn about these and other common network intrusion attacks in more detail.

Protecting a network from these types of attacks is important. If even one of them happens, it could have a catastrophic impact on an organization. Attacks can harm an organization by leaking valuable or confidential information. They can also be damaging to an organization's reputation and impact customer retention. Mitigating attacks may also cost the organization money and time.

Over the last few years, there have been a number of examples of damage that cyber attacks can cause. One notorious example was an attack against the American home-improvement chain, Home Depot, in 2014. A group of hackers compromised and infected Home Depot servers with malware. By the time network administrators shut down the attack, the hackers had already taken the credit and debit card information for over 56 million customers.

Attackers could have varying motivations for attacking your organization's network. They may have financial, personal, or political motivations, or they may be a disgruntled employee or an activist who disagrees with the company's values and wants to harm an organization's operations. Malicious actors can target any network. Security analysts must be constantly alert to potential vulnerabilities in their organization's network and take quick action to mitigate them.

In this reading, you'll learn about network interception attacks and backdoor attacks, and the possible impacts these attacks could have on an organization.

Network interception attacks

Network interception attacks work by intercepting network traffic and stealing valuable information or interfering with the transmission in some way.

Malicious actors can use hardware or software tools to capture and inspect data in transit. This is referred to as **packet sniffing**. In addition to seeing information that they are not entitled to, malicious actors can also intercept network traffic and alter it. These attacks can cause damage to an organization's network by inserting malicious code modifications or altering the message and interrupting network operations. For example, an attacker can intercept a bank transfer and change the account receiving the funds to one that the attacker controls.

Later in this course you will learn more about malicious packet sniffing, and other types of network interception attacks: on-path attacks and replay attacks.

Backdoor attacks

A **backdoor attack** is another type of attack you will need to be aware of as a security analyst. An organization may have a lot of security measures in place, including cameras, biometric scans and access codes to keep employees from entering and exiting without being seen. However, an employee might work around the security measures by finding a backdoor to the building that is not as heavily monitored, allowing them to sneak out for the afternoon without being seen.

In cybersecurity, backdoors are weaknesses intentionally left by programmers or system and network administrators that bypass normal access control mechanisms. Backdoors are intended to help programmers conduct troubleshooting or administrative tasks. However, backdoors can also be installed by attackers after they've compromised an organization to ensure they have persistent access.

Once the hacker has entered an insecure network through a backdoor, they can cause extensive damage: installing malware, performing a denial of service (DoS) attack, stealing private information or changing other security settings that leaves the system vulnerable to other attacks. A **DoS attack** is an attack that targets a network or server and floods it with network traffic.

Possible impacts on an organization

As you've learned already, network attacks can have a significant negative impact on an organization. Let's examine some potential consequences.

- **Financial:** When a system is taken offline with a DoS attack, or business operations are halted or slowed down by some other tactic, they prevent a company from performing the tasks that generate revenue. Depending on the size of an organization, interrupted operations can cost millions of dollars. In addition, if a malicious actor gets access to the personal information of the company's clients or customers, the company may face heavy litigation and settlement costs if customers seek legal recourse.
- **Reputation:** Attacks can also have a negative impact on the reputation of an organization. If it becomes public knowledge that a company has experienced a cyber attack, the public may become concerned about the security practices of the organization. They may stop trusting the company with their personal information and choose a competitor to fulfill their needs.
- **Public safety:** If an attack occurs on a government network, this can potentially impact the safety and welfare of the citizens of a country. In recent years, defense agencies across the globe are investing heavily in combating cyber warfare tactics. If a malicious actor gained access to a power grid, a public water system, or even a military defense communication system, the public could face physical harm due to a network intrusion attack.

Module 3 - Secure against network intrusions

Denial of Service (DoS) attacks

A denial of service attack is an attack that targets a network or server and floods it with network traffic. The objective of a denial of service attack, or a DoS attack, is to disrupt normal business operations by overloading an organization's network. The goal of the attack is to send so much information to a network device that it crashes or is unable to respond to legitimate users. This means that the organization won't be able to conduct their normal business operations, which can cost them money and time. A network crash can also leave them vulnerable to other security threats and attacks.

A distributed denial of service attack, or DDoS, is a kind of DoS attack that uses multiple devices or servers in different locations to flood the target network with unwanted traffic. Use of numerous devices makes it more likely that the total amount of traffic sent will overwhelm the target server. Remember, DoS stands for denial of service. So it doesn't matter what part of the network the attacker overloads; if they overload anything, they win. An unfortunate example I've seen is an attacker who crafted a very careful packet that caused a router to

spend extra time processing the request. The overall traffic volume didn't overload the router; the specifics within the packet did.

Now we'll discuss network level DoS attacks that target network bandwidth to slow traffic. Let's learn about three common network level DoS attacks. The first is called a SYN flood attack. A SYN flood attack is a type of DoS attack that simulates the TCP connection and floods the server with SYN packets. Let's break this definition down a bit more by taking a closer look at the handshake process that is used to establish a TCP connection between a device and a server. The first step in the handshake is for the device to send a SYN, or synchronize, request to the server. Then, the server responds with a SYN/ACK packet to acknowledge the receipt of the device's request and leaves a port open for the final step of the handshake. Once the server receives the final ACK packet from the device, a TCP connection is established. Malicious actors can take advantage of the protocol by flooding a server with SYN packet requests for the first part of the handshake. But if the number of SYN requests is larger than the number of available ports on the server, then the server will be overwhelmed and become unable to function.

Let's discuss two other common DoS attacks that use another protocol called ICMP. ICMP stands for Internet Control Message Protocol. ICMP is an internet protocol used by devices to tell each other about data transmission errors across the network. Think of ICMP like a request for a status update from a device. The device will return error messages if there is a network concern. You can think of this like the ICMP request checking in with the device to make sure that all is well. An ICMP flood attack is a type of DoS attack performed by an attacker repeatedly sending ICMP packets to a network server. This forces the server to send an ICMP packet. This eventually uses up all the bandwidth for incoming and outgoing traffic and causes the server to crash. Both of the attacks we've discussed so far, SYN flood and ICMP flood, take advantage of communication protocols by sending an overwhelming number of requests. There are also attacks that can overwhelm the server with one big request. One example that we'll discuss is called the ping of death.

A ping of death attack is a type of DoS attack that is caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64 kilobytes, the maximum size for a correctly formed ICMP packet. Pinging a vulnerable network server with an oversized ICMP packet will overload the system and cause it to crash. Think of this like dropping a rock on a small anthill. Each individual ant can carry a certain amount of weight while transporting food to and from the anthill. But if a large rock is dropped on the anthill, then many ants will be crushed, and the colony is unable to function until it rebuilds its operations elsewhere.

A **network protocol analyzer**, sometimes called a packet sniffer or a packet analyzer, is a tool designed to capture and analyze data traffic within a network. They are commonly used as investigative tools to monitor networks and identify suspicious activity. There are a wide variety of network protocol analyzers available, but some of the most common analyzers include:

- SolarWinds NetFlow Traffic Analyzer
- ManageEngine OpManager
- Azure Network Watcher
- Wireshark
- tcpdump

This reading will focus exclusively on tcpdump, though you can apply what you learn here to many of the other network protocol analyzers you'll use as a cybersecurity analyst to defend against any network intrusions. In an upcoming activity, you'll review a tcpdump data traffic log and identify a DoS attack to practice these skills.

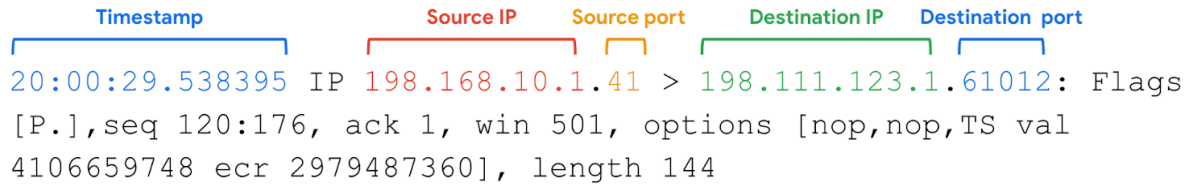
tcpdump

tcpdump is a command-line network protocol analyzer. It is popular, lightweight—meaning it uses little memory and has a low CPU usage—and uses the open-source libpcap library. tcpdump is text based, meaning all commands in tcpdump are executed in the terminal. It can also be installed on other Unix-based operating systems, such as macOS®. It is preinstalled on many Linux distributions.

tcpdump provides a brief packet analysis and converts key information about network traffic into formats easily read by humans. It prints information about each packet directly into your terminal. tcpdump also displays the source IP address, destination IP addresses, and the port numbers being used in the communications.

Interpreting output

tcpdump prints the output of the command as the sniffed packets in the command line, and optionally to a log file, after a command is executed. The output of a packet capture contains many pieces of important information about the network traffic.



```
20:00:29.538395 IP 198.168.10.1.41 > 198.111.123.1.61012: Flags  
[P.], seq 120:176, ack 1, win 501, options [nop,nop,TS val  
4106659748 ecr 2979487360], length 144
```

Some information you receive from a packet capture includes:

- **Timestamp:** The output begins with the timestamp, formatted as hours, minutes, seconds, and fractions of a second.
- **Source IP:** The packet's origin is provided by its source IP address.
- **Source port:** This port number is where the packet originated.
- **Destination IP:** The destination IP address is where the packet is being transmitted to.
- **Destination port:** This port number is where the packet is being transmitted to.

Note: By default, tcpdump will attempt to resolve host addresses to hostnames. It'll also replace port numbers with commonly associated services that use these ports.

Common uses

tcpdump and other network protocol analyzers are commonly used to capture and view network communications and to collect statistics about the network, such as troubleshooting network performance issues. They can also be used to:

- Establish a baseline for network traffic patterns and network utilization metrics.
- Detect and identify malicious traffic
- Create customized alerts to send the right notifications when network issues or security threats arise.
- Locate unauthorized instant messaging (IM), traffic, or wireless access points.

However, attackers can also use network protocol analyzers maliciously to gain information about a specific network. For example, attackers can capture data packets that contain sensitive information, such as account usernames and passwords. As a cybersecurity analyst, It's important to understand the purpose and uses of network protocol analyzers.

A DDoS targeting a widely used DNS server

In previous videos, you learned about the function of a DNS server. As a review, DNS servers translate website domain names into the IP address of the system that contains the information for the website. For instance, if a user were to type in a website URL, a DNS server would translate that into a numeric IP address that directs network traffic to the location of the website's server.

On the day of the DDoS attack we are studying, many large companies were using a DNS service provider. The service provider was hosting the DNS system for these companies. This meant that when internet users typed in the URL of the website they wanted to access, their devices would be directed to the right place. On October 21, 2016, the service provider was the victim of a DDoS attack.

Leading up to the attack

Before the attack on the service provider, a group of university students created a botnet with the intention to attack various gaming servers and networks. A **botnet** is a collection of computers infected by malware that are under the control of a single threat actor, known as the "bot-herder." Each computer in the botnet can be remotely controlled to send a data packet to a target system. In a botnet attack, cyber criminals instruct all the bots on the botnet to send data packets to the target system at the same time, resulting in a DDoS attack.

The group of university students posted the code for the botnet online so that it would be accessible to thousands of internet users and authorities wouldn't be able to trace the botnet back to the students. In doing so, they made it possible for other malicious actors to learn the code to the botnet and control it remotely. This included the cyber criminals who attacked the DNS service provider.

The day of attack

At 7:00 a.m. on the day of the attack, the botnet sent tens of millions of DNS requests to the service provider. This overwhelmed the system and the DNS service shut down. This meant that all of the websites that used the service provider could not be reached. When users tried to access various websites that used the service provider, they were not directed to the website they typed in their browser. Outages for each web service occurred all over North America and Europe.

The service provider's systems were restored after only two hours of downtime. Although the cyber criminals sent subsequent waves of botnet attacks, the DNS company was prepared and able to mitigate the impact.

Malicious packet sniffing

Packets include a header which contains the sender's and receiver's IP addresses. Packets also contain a body, which may contain valuable information like names, date of birth, personal messages, financial information, and credit card numbers.

Packet sniffing is the practice of using software tools to observe data as it moves across a network. As a security analyst, you may use packet sniffing to analyze and capture packets when investigating ongoing incidents or debugging network issues. Later in this certificate program, you'll gain hands-on practice with some packet sniffing software. However, malicious actors may also use packet sniffing to look at data that has not been sent to them. This is a little bit like opening somebody else's mail. It's important for you to learn about how threat actors use packet sniffing with harmful intent so you can be prepared to protect against these malicious acts. Malicious actors may insert themselves in the middle of an authorized connection between two devices. Then they can use packet sniffing to spy on every data packet as it comes across their device. The goal is to find valuable information in the data packets that they can then use to their advantage. Attackers can use software applications or a hardware device to look into data packets. Malicious actors can access a network packet with a packet sniffer and make changes to the data. They may change the information in the body of the packet, like altering a recipient's bank account number.

Packet sniffing can be passive or active. Passive packet sniffing is a type of attack where data packets are read in transit. Since all the traffic on a network is visible to any host on the hub, malicious actors can view all the information going in and out of the device they are targeting. Thinking back to the example of a letter being delivered, we can compare a passive packet sniffing attack to a postal delivery person maliciously reading somebody's mail. The postal worker, or packet sniffer, has the right to deliver the mail, but not the right to read the information inside. Active packet sniffing is a type of attack where data packets are manipulated in transit. This may include injecting internet protocols to redirect the packets to an unintended port or changing the information the packet contains. Active packet sniffing attack would be like a neighbor telling the delivery person "I'll deliver that mail for you," and then reading the mail or changing the letter before putting it in your mailbox. Even though your neighbor knows you and even if they deliver it to the correct house, they are actively going out of their way to engage in malicious behavior.

The good news is that malicious packet sniffing can be prevented. Let's look at a few ways the network security professional can prevent these attacks. One way to protect against malicious packet sniffing is to use a VPN to encrypt and protect data as it travels across the network. If you don't remember how VPNs work, you can

revisit the video about this topic in the previous section of the program. When you use a VPN, hackers might interfere with your traffic, but they won't be able to decode it to read it and read your private information. Another way to add a layer of protection against packet sniffing is to make sure that websites you have use HTTPS at the beginning of the domain address. Previously, we discussed how HTTPS uses SSL/TLS to encrypt data and prevent eavesdropping when malicious actors spy on network transmissions. One final way to help protect yourself against malicious packet sniffing is to avoid using unprotected WiFi. You usually find unprotected WiFi in public places like coffee shops, restaurants, or airports. These networks don't use encryption. This means that anyone on the network can access all of the data traveling to and from your device. One precaution you can take is avoiding free public WiFi unless you have a VPN service already installed on your device.

IP Spoofing

IP spoofing is a network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network. In this kind of attack, the hacker is pretending to be someone they are not so they can communicate over the network with the target computer and get past firewall rules that may prevent outside traffic. Some common IP spoofing attacks are on-path attacks, replay attacks, and smurf attacks. Let's discuss these one at a time.

An on-path attack is an attack where the malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit. On-path attackers gain access to the network and put themselves between two devices, like a web browser and a web server. Then they sniff the packet information to learn the IP and MAC addresses to devices that are communicating with each other. After they have this information, they can pretend to be either of these devices.

Another type of attack is a replay attack. A replay attack is a network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time. A delayed packet can cause connection issues between target computers, or a malicious actor may take a network transmission that was sent by an authorized user and repeat it at a later time to impersonate the authorized user.

A smurf attack is a combination of a DDoS attack and an IP spoofing attack. The attacker sniffs an authorized user's IP address and floods it with packets. This overwhelms the target computer and can bring down a server or the entire network.

Now that you've learned about different kinds of IP spoofing, let's talk about how you can protect the network from this kind of attack. As you previously learned, encryption should always be implemented so that the data in your network transfers can't be read by malicious actors. Firewalls can be configured to protect against IP spoofing. IP spoofing makes it seem like the malicious actor is an authorized user by changing the sender's address of the data packet to match the target network's address. So if a firewall receives a data packet from the internet where the sender's IP address is the same as the private network, then the firewall will deny the transmission since all the devices with that IP address should already be on the local network. You can make sure that your firewalls configure correctly by creating a rule to reject all incoming traffic that has the same IP address as the local network.

A closer review of packet sniffing

As you learned in a previous video, **packet sniffing** is the practice of capturing and inspecting data packets across a network. On a private network, data packets are directed to the matching destination device on the network.

The device's Network Interface Card (NIC) is a piece of hardware that connects the device to a network. The NIC reads the data transmission, and if it contains the device's MAC address, it accepts the packet and sends it to the device to process the information based on the protocol. This occurs in all standard network operations. However, a NIC can be set to promiscuous mode, which means that it accepts all traffic on the network, even the packets that aren't addressed to the NIC's device. You'll learn more about NIC's later in the program. Malicious actors might use software like Wireshark to capture the data on a private network and store it for later use. They can then use the personal information to their own advantage. Alternatively, they might use the IP and MAC addresses of authorized users of the private network to perform IP spoofing.

A closer review of IP spoofing

After a malicious actor has sniffed packets on the network, they can impersonate the IP and MAC addresses of authorized devices to perform an IP spoofing attack. Firewalls can prevent IP spoofing attacks by configuring it to refuse unauthorized IP packets and suspicious traffic. Next, you'll examine a few common IP spoofing attacks that are important to be familiar with as a security analyst.

On-path attack

An **on-path attack** happens when a hacker intercepts the communication between two devices or servers that have a trusted relationship. The transmission between these two trusted network devices could contain valuable information like usernames and passwords that the malicious actor can collect. An on-path attack is sometimes referred to as a **meddler-in-the middle attack** because the hacker is hiding in the middle of communications between two trusted parties.

Or, it could be that the intercepted transmission contains a DNS system look-up. You'll recall from an earlier video that a DNS server translates website domain names into IP addresses. If a malicious actor intercepts a transmission containing a DNS lookup, they could spoof the DNS response from the server and redirect a domain name to a different IP address, perhaps one that contains malicious code or other threats. The most important way to protect against an on-path attack is to encrypt your data in transit, e.g. using TLS.

Smurf attack

A **smurf attack** is a network attack that is performed when an attacker sniffs an authorized user's IP address and floods it with packets. Once the spoofed packet reaches the broadcast address, it is sent to all of the devices and servers on the network.

In a smurf attack, IP spoofing is combined with another denial of service (DoS) technique to flood the network with unwanted traffic. For example, the spoofed packet could include an Internet Control Message Protocol (ICMP) ping. As you learned earlier, ICMP is used to troubleshoot a network. But if too many ICMP messages are transmitted, the ICMP echo responses overwhelm the servers on the network and they shut down. This creates a denial of service and can bring an organization's operations to a halt.

An important way to protect against a smurf attack is to use an advanced firewall that can monitor any unusual traffic on the network. Most next generation firewalls (NGFW) include features that detect network anomalies to ensure that oversized broadcasts are detected before they have a chance to bring down the network.

DoS attack

As you've learned, once the malicious actor has sniffed the network traffic, they can impersonate an authorized user. A **Denial of Service attack** is a class of attacks where the attacker prevents the compromised system from performing legitimate activity or responding to legitimate traffic. Unlike IP spoofing, however, the attacker will not receive a response from the targeted host. Everything about the data packet is authorized including the IP address in the header of the packet. In IP spoofing attacks, the malicious actor uses IP packets containing fake IP addresses. The attackers keep sending IP packets containing fake IP addresses until the network server crashes.

Pro Tip: Remember the principle of defense-in-depth. There isn't one perfect strategy for stopping each kind of attack. You can layer your defense by using multiple strategies. In this case, using industry standard encryption will strengthen your security and help you defend from DoS attacks on more than one level.

Terms and definitions from Course 3, Module 3

- **Active packet sniffing:** A type of attack where data packets are manipulated in transit
- **Botnet:** A collection of computers infected by malware that are under the control of a single threat actor, known as the "bot-herder"
- **Denial of service (DoS) attack:** An attack that targets a network or server and floods it with network traffic

- **Distributed denial of service (DDoS) attack:** A type of denial of service attack that uses multiple devices or servers located in different locations to flood the target network with unwanted traffic
- **Internet Control Message Protocol (ICMP):** An internet protocol used by devices to tell each other about data transmission errors across the network
- **Internet Control Message Protocol (ICMP) flood:** A type of DoS attack performed by an attacker repeatedly sending ICMP request packets to a network server
- **IP spoofing:** A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network
- **On-path attack:** An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit
- **Packet sniffing:** The practice of capturing and inspecting data packets across a network
- **Passive packet sniffing:** A type of attack where a malicious actor connects to a network hub and looks at all traffic on the network
- **Ping of death:** A type of DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB
- **Replay attack:** A network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time
- **Smurf attack:** A network attack performed when an attacker sniffs an authorized user's IP address and floods it with ICMP packets
- **Synchronize (SYN) flood attack:** A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets

Module 4 - Security Hardening

Security hardening

- Security hardening is the process of strengthening a system to reduce its vulnerability and attack surface. All the potential vulnerabilities that a threat actor could exploit are referred to as a system's attack surface.
- Example : compares a network to a house. The attack surface would be all the doors and windows that a robber could use to gain access to that house. Just like putting locks on all the doors and windows in the house, security hardening involves minimizing the attack surface or potential vulnerabilities and keeping a network as secure as possible.
- As part of security hardening, security analysts perform regular maintenance procedures to keep network devices and systems functioning securely and optimally. Security hardening can be conducted on any device or system that can be compromised, such as hardware, operating systems, applications, computer networks, and databases. Physical security is also a part of security hardening. This may include securing a physical space with security cameras and security guards.
- Some common types of hardening procedures include software updates, also called patches, and device application configuration changes. These updates and changes are done to increase security and fix security vulnerabilities on a network. An example of a security configuration change would be requiring longer passwords or more frequent password changes. This makes it harder for a malicious actor to gain login credentials. An example of a configuration check is updating the encryption standards for data that is stored in a database. Keeping encryption up to date makes it harder for malicious actors to access the database.
- Other examples of security hardening include removing or disabling unused applications and services, disabling unused ports, and reducing access permissions across devices and network. Minimizing the number of applications, devices, ports, and access permissions makes network and device monitoring more efficient and reduces the overall attack surface, which is one of the best ways to secure an organization.

- Another important strategy for security hardening is to conduct regular penetration testing. A penetration test, also called a pen test, is a simulated attack that helps identify vulnerabilities in a system, network, website, application, and process. Penetration testers document their findings in a report. Depending on where the test fails, security teams can determine the type of security vulnerabilities that require fixing. Organizations can then review these vulnerabilities and come up with a plan to fix them.

OS hardening practices

- The operating system is the interface between computer hardware and the user.
 - The OS is the first program loaded when a computer turns on.
 - The OS acts as an intermediary between software applications and the computer hardware.
 - It's important to secure the OS in each system because one insecure OS can lead to a whole network being compromised.
 - There are many types of operating systems, and they all share similar security hardening practices.
 - Some OS hardening tasks are performed at regular intervals, like updates, backups, and keeping an up-to-date list of devices and authorized users.
 - Other tasks are performed only once as part of preliminary safety measures.
 - One example would be configuring a device setting to fit a secure encryption standard.
-
- A patch update is a software and operating system, or OS, update that addresses security vulnerabilities within a program or product.
 - With patch updates, the OS should be upgraded to its latest software version. Sometimes patches are released to fix a security vulnerability in the software.
 - As soon as OS vendors publish a patch and the vulnerability fix, malicious actors know exactly where the vulnerability is in systems running the out-of-date OS.
 - This is why it's important for organizations to run patch updates as soon as they are released.
 - For example, my team had to perform an emergency patch to address a recent vulnerability found in a commonly used programming library.
-
- The library is used almost everywhere, so we had to quickly patch most of our servers and applications to fix the vulnerability.
 - The newly updated OS should be added to the baseline configuration, also called the baseline image.
 - A baseline configuration is a documented set of specifications within a system that is used as a basis for future builds, releases, and updates.
 - For example, a baseline may contain a firewall rule with a list of allowed and disallowed network ports.
-
- If a security team suspects unusual activity affecting the OS, they can compare the current configuration to the baseline and make sure that nothing has been changed.
 - Another hardening task performed regularly is hardware and software disposal.
 - This ensures that all old hardware is properly wiped and disposed of.
 - It's also a good idea to delete any unused software applications since some popular programming languages have known vulnerabilities.
 - Removing unused software makes sure that there aren't any unnecessary vulnerabilities connected with the programs that the software uses.
-
- The final OS hardening technique that we'll discuss is implementing a strong password policy.
 - Strong password policies require that passwords follow specific rules.
 - For example, an organization may set a password policy that requires a minimum of eight characters, a capital letter, a number, and a symbol.

- To discourage malicious actors, a password policy usually states that a user will lose access to the network after entering the wrong password a certain number of times in a row. Some systems also require multi-factor authentication, or MFA. MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network.
- Ways of identifying yourself include something you know, like a password, something you have like an ID card, or something unique about you, like your fingerprint.

Brute force attacks and OS hardening

Implementing various OS hardening tasks can help prevent brute force attacks. An attacker can use a brute force attack to gain access and compromise a network.

Username and passwords are among the most common and important security controls in place today. They are used and enforced on everything that stores or accesses sensitive or private information, like personal phones, computers, and restricted applications within an organization. However, a major issue with relying on login credentials as a critical line of defense is that they're vulnerable to being stolen and guessed by malicious actors.

Brute force attacks

A **brute force attack** is a trial-and-error process of discovering private information. There are different types of brute force attacks that malicious actors use to guess passwords, including:

- *Simple brute force attacks.* When attackers try to guess a user's login credentials, it's considered a simple brute force attack. They might do this by entering any combination of usernames and passwords that they can think of until they find the one that works.
- *Dictionary attacks* use a similar technique. In dictionary attacks, attackers use a list of commonly used passwords and stolen credentials from previous breaches to access a system. These are called "dictionary" attacks because attackers originally used a list of words from the dictionary to guess the passwords, before complex password rules became a common security practice.

Using brute force to access a system can be a tedious and time consuming process, especially when it's done manually. There are a range of tools attackers use to conduct their attacks.

Assessing vulnerabilities

Before a brute force attack or other cybersecurity incident occurs, companies can run a series of tests on their network or web applications to assess vulnerabilities. Analysts can use virtual machines and sandboxes to test suspicious files, check for vulnerabilities before an event occurs, or to simulate a cybersecurity incident.

Virtual machines (VMs)

Virtual machines (VMs) are software versions of physical computers. VMs provide an additional layer of security for an organization because they can be used to run code in an isolated environment, preventing malicious code from affecting the rest of the computer or system. VMs can also be deleted and replaced by a pristine image after testing malware.

VMs are useful when investigating potentially infected machines or running malware in a constrained environment. Using a VM may prevent damage to your system in the event its tools are used improperly. VMs also give you the ability to revert to a previous state. However, there are still some risks involved with VMs. There's still a small risk that a malicious program can escape virtualization and access the host machine.

You can test and explore applications easily with VMs, and it's easy to switch between different VMs from your computer. This can also help in streamlining many security tasks.

Sandbox environments

A sandbox is a type of testing environment that allows you to execute software or programs separate from your network. They are commonly used for testing patches, identifying and addressing bugs, or detecting cybersecurity vulnerabilities. Sandboxes can also be used to evaluate suspicious software, evaluate files containing malicious code, and simulate attack scenarios.

Sandboxes can be stand-alone physical computers that are not connected to a network; however, it is often more time- and cost-effective to use software or cloud-based virtual machines as sandbox environments.

Note that some malware authors know how to write code to detect if the malware is executed in a VM or sandbox environment. Attackers can program their malware to behave as harmless software when run inside these types of testing environments.

Prevention measures

Some common measures organizations use to prevent brute force attacks and similar attacks from occurring include:

- **Salting and hashing:** Hashing converts information into a unique value that can then be used to determine its integrity. It is a one-way function, meaning it is impossible to decrypt and obtain the original text. Salting adds random characters to hashed passwords. This increases the length and complexity of hash values, making them more secure.
- **Multi-factor authentication (MFA) and two-factor authentication (2FA):** MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. This verification happens using a combination of authentication factors: a username and password, fingerprints, facial recognition, or a one-time password (OTP) sent to a phone number or email. 2FA is similar to MFA, except it uses only two forms of verification.
- **CAPTCHA and reCAPTCHA:** CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It asks users to complete a simple test that proves they are human. This helps prevent software from trying to brute force a password. reCAPTCHA is a free CAPTCHA service from Google that helps protect websites from bots and malicious software.
- **Password policies:** Organizations use password policies to standardize good password practices throughout the business. Policies can include guidelines on how complex a password should be, how often users need to update passwords, and if there are limits to how many times a user can attempt to log in before their account is suspended.

Activity Exemplar: Apply OS hardening techniques

To review the exemplar for this course item, click the link below and select *Use Template*.

- [Security incident report exemplar](#)
- [The exemplar explained: Security incident report](#)

OR

If you don't have a Google account, you can download the exemplar and incident report directly from the attachment below.

[Security incident report exemplar](#)

[DOCX File](#)

[The Exemplar Explained - Security incident report exemplar](#)

[DOCX File](#)

Assessment of Exemplar

Note: The exemplar represents one possible explanation for the issues that the end users are facing. Yours will likely differ in certain ways. What's important is that you identified the network protocols involved and created a report. In your role as a security analyst, you and your team would document any issue that occurs on the network and come up with solutions to help prevent the same issues from occurring in the future. Good quality documentation can save you and your organization time and potentially manage the attack early on.

First, analyze the DNS & HTTP traffic log to identify a network protocol. Then, document the cybersecurity incident. Finally, recommend one security measure your organization could implement to prevent brute force attacks in the future. Creating this process will, in turn, help improve the organization's security posture.

The exemplar is accompanied by the activity, and presents a professional documentation example to include the following:

- One network protocol identified during the investigation
- Documentation of the incident
- A recommended security measure

Activity Overview

- In this activity, you will take on the role of a cybersecurity analyst working for a company that hosts the cooking website, yummyrecipesforme.com. Visitors to the website experience a security issue when loading the main webpage. Your job is to investigate, identify, document, and recommend a solution to the security problem.
- When investigating the security event, you will review a tcpdump log. You will need to identify the network protocols used to establish the connection between the user and the website. Network protocols are the communication rules and standards networked devices use to transmit data. Unfortunately, malicious actors can also use network protocols to invade and attack private networks. Knowing how to identify the protocols commonly used in attacks will help you protect your organization's network against these types of security events.
- To complete the assignment, you will also need to document what occurred during the security incident. Then, you will recommend one security measure to implement to prevent similar security problems in the future.
- Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the scenario below. Then complete the step-by-step instructions.

-
- You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A disgruntled baker has decided to publish the website's best-selling recipes for the public to access for free.
- The baker executed a brute force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one. After they obtained the login credentials, they were able to access the admin panel and change the website's

source code. They embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After running the downloaded file, the customers are redirected to a fake version of the website where the seller's recipes are now available for free.

- Several hours after the attack, multiple customers emailed yummyrecipesforme's helpdesk. They complained that the company's website had prompted them to download a file to update their browsers. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly.
- In response to this incident, the website owner tries to log in to the admin panel but is unable to, so they reach out to the website hosting provider. You and other cybersecurity analysts are tasked with investigating this security event.
- To address the incident, you create a sandbox environment to observe the suspicious website behavior. You run the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, you are prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then observe that your browser redirects you to a different URL, greatrecipesforme.com, which is designed to look like the original site. However, the recipes your company sells are now posted for free on the new website.

The logs show the following process:

1. The browser requests a DNS resolution of the yummyrecipesforme.com URL.
 2. The DNS replies with the correct IP address.
 3. The browser initiates an HTTP request for the webpage.
 4. The browser initiates the download of the malware.
 5. The browser requests another DNS resolution for greatrecipesforme.com.
 6. The DNS server responds with the new IP address.
 7. The browser initiates an HTTP request to the new IP address.
-
- A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. They notice that javascript code had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com.
 - The cybersecurity team reports that the web server was impacted by a brute force attack. The disgruntled baker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack.
 - Your job is to document the incident in detail, including identifying the network protocols used to establish the connection between the user and the website. You should also recommend a security action to take to prevent brute force attacks in the future.

Step-By-Step Instructions

Step 1: Access the template

To use the template for this course item, click the link below and select *Use Template*.

Link to template:

- [Security incident report template](#)

OR

If you don't have a Google account, you can download the template directly from the attachment below.

[Security incident report template](#)

Step 2: Access supporting materials

To use the supporting materials for this course item, click the link below and select *Use Template*.

Links to supporting materials:

- [DNS & HTTP traffic log](#)
- [How to read the DNS & HTTP log](#)

OR

If you don't have a Google account, you can download the supporting materials directly from the attachment below.

[DNS & HTTP traffic log](#)

[DOCX File](#)

[How to read the DNS & HTTP traffic log](#)

[DOCX File](#)

Step 3: Identify the network protocol involved in the incident

Imagine that you are one of the cybersecurity analysts in this scenario and you are tasked with writing an incident report for this security event. Using the DNS & HTTP log file you produced with tcpdump, determine which network protocol is identified in the packet captures during the investigation. You will use what you learned about the four layers of the TCP/IP model and which protocols happen at each layer. If needed, you can review [the video](#) and [reading about the TCP/IP model](#) to use as guides for your response. Then review the DNS & HTTP traffic log and record which protocol you identified in the first section of the security incident report template.

Step 4: Document the incident

Summarize the incident in the second section of the report. Provide as many details and facts as possible in your documentation. When writing the documentation, be sure to:

- Avoid using strong emotional language (good, terrible, awful, etc.).
- Include as many facts about the issue as you can, including where the incident occurred, how it happened, whether anyone witnessed it, how it was discovered, etc.
- Indicate your sources for information and evidence.

Writing accurate and detailed documentation for cybersecurity incidents can serve as a reference point for other cybersecurity analysts. Additionally, quality documentation can be used to educate other employees about cybersecurity measures taken within the company when incidents occur and can help businesses comply with various security audits.

Step 5: Recommend one remediation for brute force attacks

After documenting the incident, write one recommendation to help your organization prevent brute force attacks in the future.

Some of the common security methods used to prevent brute force attacks include:

- Requiring strong passwords
- Enforcing two-factor authentication (2FA)
- Monitoring login attempts
- Limiting the number of login attempts

Select one security measure, and explain why it is effective in section three of the security incident report template. The more safety measures that are in place, the less likely a malicious actor will be able to access sensitive information.

Pro tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

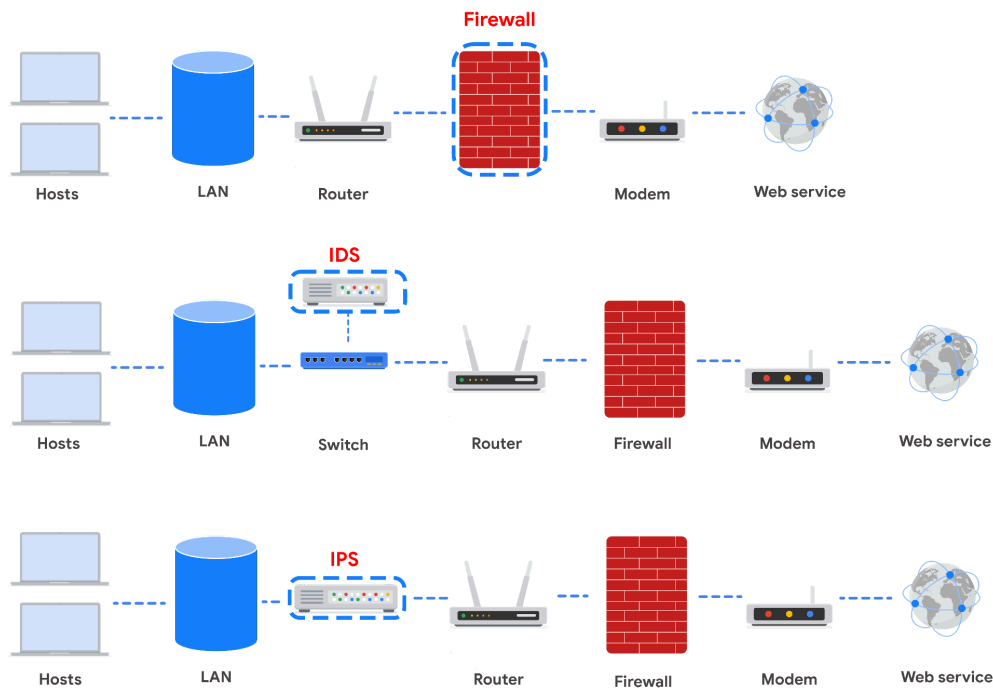
Be sure to address the following criteria in your completed activity:

- Name one network protocol identified during the investigation
- Document the incident
- Recommend one security measure

Network hardening practices

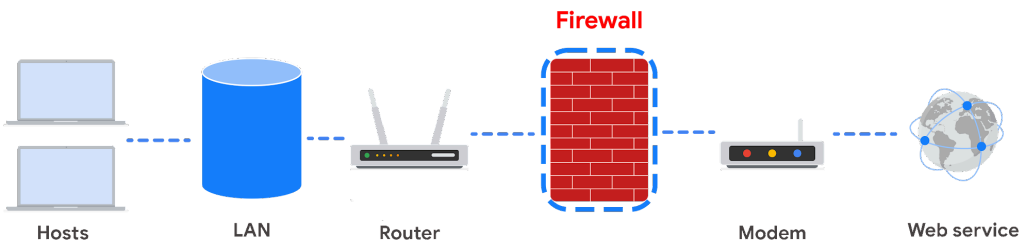
- Network hardening focuses on network-related security hardening, like port filtering, network access privileges, and encryption over networks. Certain network hardening tasks are performed regularly, while others are performed once and then updated as needed.
- Some tasks that are regularly performed are firewall rules maintenance, network log analysis, patch updates, and server backups.
- Network log analysis is the process of examining network logs to identify events of interest. Security teams use a log analyzer tool or a security information and event management tool, also known as a SIEM, to conduct network log analysis.
- A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization.
- It gathers security data from a network and presents that data on a single dashboard. The dashboard interface is sometimes called a single pane of glass.
- A SIEM helps analysts to inspect, analyze, and react to security events across the network based on their priority.
- Reports from the SIEM provide a list of new or ongoing network vulnerabilities and list them on a scale of priority from high to low, where high priority vulnerabilities have a much shorter deadline for mitigation.
- These tasks include port filtering on firewalls, network access privileges, and encryption for communication, among many things.
- Port filtering can be formed over the network. Port filtering is a firewall function that blocks or allows certain port numbers to limit unwanted communication. A basic principle is that the only ports that are needed are the ones that are allowed. Any port that isn't being used by the normal network operations should be disallowed.
- This protects against port vulnerabilities. Networks should be set up with the most up-to-date wireless protocols available and older wireless protocols should be disabled.
- Security analysts also use network segmentation to create isolated subnets for different departments in an organization. For example, they might make one for the marketing department and one for the finance department.
- This is done so the issues in each subnet don't spread across the whole company and only specific users are given access to the part of the network that they require for their role. Network segmentation may also be used to separate different security zones.
- Any restricted zone on a network containing highly classified or confidential data should be separate from the rest of the network.
- Encryption standards are rules or methods used to conceal outgoing data and uncover or decrypt incoming data. Data in restricted zones should have much higher encryption standards, which makes them more difficult to access.

Network security applications



Firewall

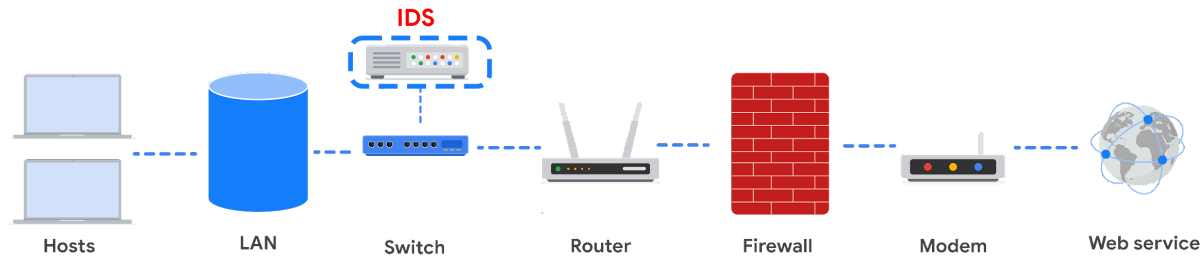
- Most firewalls are similar in their basic functions.
- Firewalls allow or block traffic based on a set of rules.
- As data packets enter a network, the packet header is inspected and allowed or denied based on its port number. NGFWs are also able to inspect packet payloads.
- Each system should have its own firewall, regardless of the network firewall.



Intrusion Detection System

- An **intrusion detection system** (IDS) is an application that monitors system activity and alerts on possible intrusions. An IDS alerts administrators based on the signature of malicious traffic.
- The IDS is configured to detect known attacks.
- IDS systems often sniff data packets as they move across the network and analyze them for the characteristics of known attacks.
- Some IDS systems review not only for signatures of known attacks, but also for anomalies that could be the sign of malicious activity.
- When the IDS discovers an anomaly, it sends an alert to the network administrator who can then investigate further.
- The limitations to IDS systems are that they can only scan for known attacks or obvious anomalies. New and sophisticated attacks might not be caught.

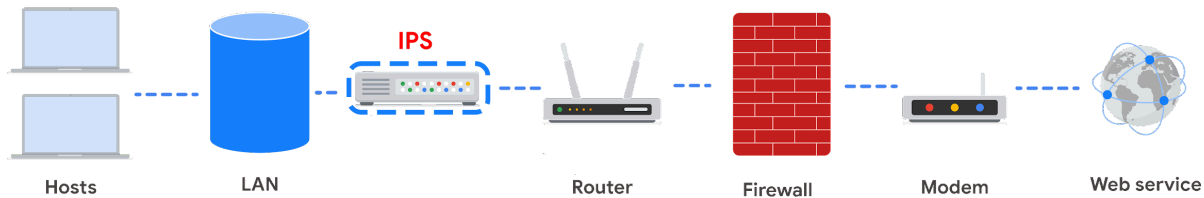
- The other limitation is that the IDS doesn't actually stop the incoming traffic if it detects something awry. It's up to the network administrator to catch the malicious activity before it does anything damaging to the network.



- When combined with a firewall, an IDS adds another layer of defense. The IDS is placed behind the firewall and before entering the LAN, which allows the IDS to analyze data streams after network traffic that is disallowed by the firewall has been filtered out. This is done to reduce noise in IDS alerts, also referred to as false positives.

Intrusion Prevention System

- An **intrusion prevention system (IPS)** is an application that monitors system activity for intrusive activity and takes action to stop the activity. It offers even more protection than an IDS because it actively stops anomalies when they are detected, unlike the IDS that simply reports the anomaly to a network administrator.
- An IPS searches for signatures of known attacks and data anomalies. An IPS reports the anomaly to security analysts and blocks a specific sender or drops network packets that seem suspect.



- The IPS (like an IDS) sits behind the firewall in the network architecture. This offers a high level of security because risky data streams are disrupted before they even reach sensitive parts of the network. However, one potential limitation is that it is inline: If it breaks, the connection between the private network and the internet breaks. Another limitation of IPS is the possibility of false positives, which can result in legitimate traffic getting dropped.

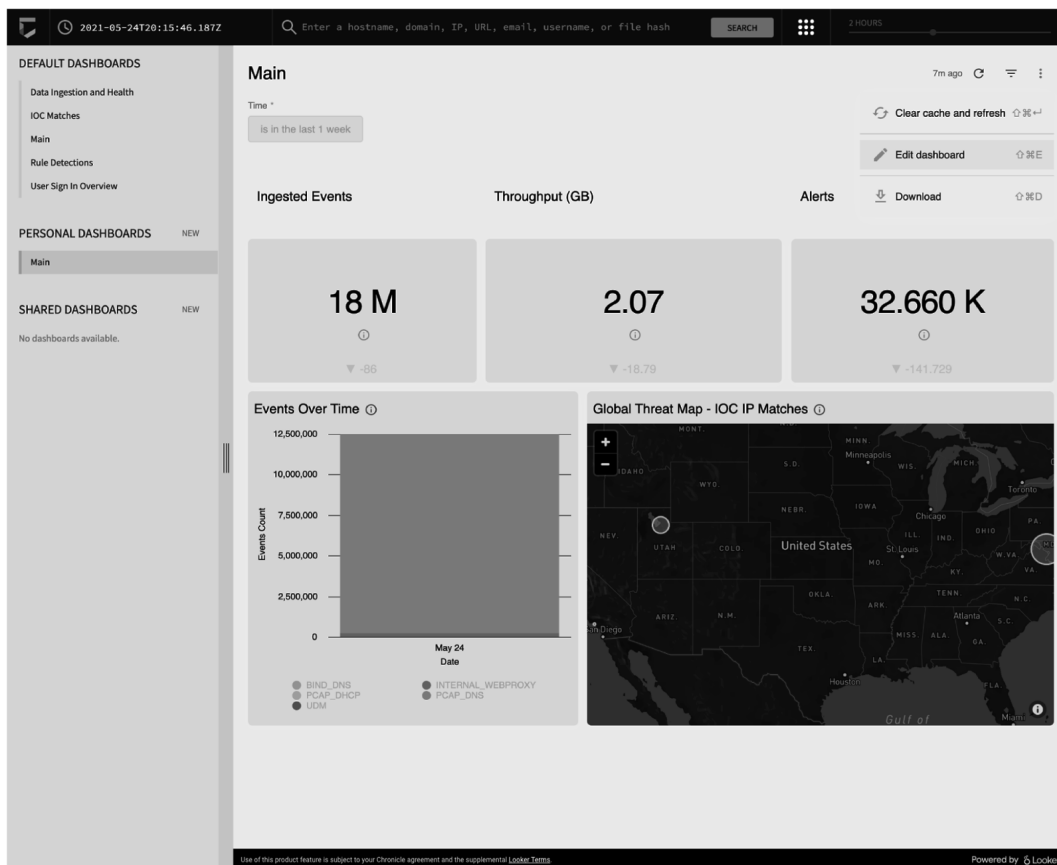
Full packet capture devices

Full packet capture devices can be incredibly useful for network administrators and security professionals. These devices allow you to record and analyze all of the data that is transmitted over your network. They also aid in investigating alerts created by an IDS.

Security Information and Event Management

A **security information and event management system (SIEM)** is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools work in real time to report suspicious activity in a centralized dashboard. SIEM tools additionally analyze network log data sourced from IDSs, IPSs, firewalls, VPNs, proxies, and DNS logs. SIEM tools are a way to aggregate security event data so that it all appears in one place for security analysts to analyze. This is referred to as a single pane of glass.

Chronicle is a cloud-native tool designed to retain, analyze, and search data.



Splunk is another common SIEM tool. Splunk offers different SIEM tool options: Splunk Enterprise and Splunk Cloud. Both options include detailed dashboards which help security professionals to review and analyze an organization's data. There are also other similar SIEM tools available, and it's important for security professionals to research the different tools to determine which one is most beneficial to the organization.

Key takeaways

Devices / Tools	Advantages	Disadvantages
Firewall	A firewall allows or blocks traffic based on a set of rules.	A firewall is only able to filter packets based on information provided in the header of the packets.
Intrusion Detection System (IDS)	An IDS detects and alerts admins about possible intrusions, attacks, and other malicious traffic.	An IDS can only scan for known attacks or obvious anomalies; new and sophisticated attacks might not be caught. It doesn't actually stop the incoming traffic.
Intrusion Prevention System (IPS)	An IPS monitors system activity for intrusions and anomalies and takes action to stop them.	An IPS is an inline appliance. If it fails, the connection between the private network and the internet breaks. It might detect false positives and block legitimate traffic.

Security Information
and Event
Management (SIEM)

A SIEM tool collects and analyzes log data from multiple network machines. It aggregates security events for monitoring in a central dashboard.

A SIEM tool only reports on possible security issues. It does not take any actions to stop or prevent suspicious events.

Completed Exemplar

To review the exemplar for this course item, click the link below and select *Use Template*.

[Security risk assessment report exemplar](#)

OR

If you don't have a Google account, you can download the exemplar directly from the attachment below.

[Security risk assessment report exemplar](#)

[DOCX File](#)

Assessment of Exemplar

The exemplar focuses on the vulnerability of an outdated software for an on-premises database. One potential solution to the vulnerability is identified and included in the report for the direct supervisors. The report explains how the company might be compromised in the future if the database is not patched and if employees continue to share passwords.

In the section about the organization's information security policy, the report includes information about adding general security hardening practices, a recommendation for how often the hardening practices should be performed, and an explanation of what the potential consequences are if the policy is not followed.

This is one example of how a security risk assessment report can be analyzed and how an information security policy might be written.

Cloud Hardening

Network security in the cloud

A cloud network is a collection of servers or computers that stores resources and data in a remote data center that can be accessed via the internet. They can host company data and applications using cloud computing to provide on-demand storage, processing power, and data analytics. Just like regular web servers, cloud servers also require proper maintenance done through various security hardening procedures. Although cloud servers are hosted by a cloud service provider, these providers cannot prevent intrusions in the cloud—especially intrusions from malicious actors, both internal and external to an organization.

One distinction between cloud network hardening and traditional network hardening is the use of a server baseline image for all server instances stored in the cloud. This allows you to compare data in the cloud servers to the baseline image to make sure there haven't been any unverified changes. An unverified change could come from an intrusion in the cloud network. Similar to OS hardening, data and applications on a cloud network are kept separate depending on their service category. For example, older applications should be kept

separate from newer applications, and software that deals with internal functions should be kept separate from front-end applications seen by users.

Even though the cloud service provider has a shared responsibility with the organization using their services, there are still security measures that need to be taken by the organization to make sure their cloud network is safe.

Secure the cloud

Cloud computing is a model for allowing convenient and on-demand network access to a shared pool of configurable computing resources. These resources can be configured and released with minimal management effort or interaction with the service provider.

Just like any other IT infrastructure, a cloud infrastructure needs to be secured. This reading will address some main security considerations that are unique to the cloud and introduce you to the shared responsibility model used for security in the cloud. Many organizations that use cloud resources and infrastructure express concerns about the privacy of their data and resources. This concern is addressed through cryptography and other additional security measures, which will be discussed later in this course.

Cloud security considerations

Many organizations choose to use cloud services because of the ease of deployment, speed of deployment, cost savings, and scalability of these options. Cloud computing presents unique security challenges that cybersecurity analysts need to be aware of.

Identity access management

Identity access management (IAM) is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can use different cloud resources. A common problem that organizations face when using the cloud is the loose configuration of cloud user roles. An improperly configured user role increases risk by allowing unauthorized users to have access to critical cloud operations.

Configuration

The number of available cloud services adds complexity to the network. Each service must be carefully configured to meet security and compliance requirements. This presents a particular challenge when organizations perform an initial migration into the cloud. When this change occurs on their network, they must ensure that every process moved into the cloud has been configured correctly. If network administrators and architects are not meticulous in correctly configuring the organization's cloud services, they could leave the network open to compromise. Misconfigured cloud services are a common source of cloud security issues.

Attack surface

Cloud service providers (CSPs) offer numerous applications and services for organizations at a low cost. Every service or application on a network carries its own set of risks and vulnerabilities and increases an organization's overall attack surface. An increased attack surface must be compensated for with increased security measures.

Cloud networks that utilize many services introduce lots of entry points into an organization's network. However, if the network is designed correctly, utilizing several services does not introduce more entry points into an organization's network design. These entry points can be used to introduce malware onto the network and pose other security vulnerabilities. It is important to note that CSPs often defer to more secure options, and have undergone more scrutiny than a traditional on-premises network.

Zero-day attacks

Zero-day attacks are an important security consideration for organizations using cloud or traditional on-premise network solutions. A **zero day** attack is an exploit that was previously unknown. CSPs are more likely to know about a zero day attack occurring before a traditional IT organization does. CSPs have ways of patching hypervisors and migrating workloads to other virtual machines. These methods ensure the customers are not impacted by the attack. There are also several tools available for patching at the operating system level that organizations can use.

Visibility and tracking

Network administrators have access to every data packet crossing the network with both on-premise and cloud networks. They can sniff and inspect data packets to learn about network performance or to check for possible threats and attacks.

This kind of visibility is also offered in the cloud through flow logs and tools, such as packet mirroring. CSPs take responsibility for security in the cloud, but they do not allow the organizations that use their infrastructure to monitor traffic on the CSP's servers. Many CSPs offer strong security measures to protect their infrastructure. Still, this situation might be a concern for organizations that are accustomed to having full access to their network and operations. CSPs pay for third-party audits to verify how secure a cloud network is and identify potential vulnerabilities. The audits can help organizations identify whether any vulnerabilities originate from on-premise infrastructure and if there are any compliance lapses from their CSP.

Things change fast in the cloud

CSPs are large organizations that work hard to stay up-to-date with technology advancements. For organizations that are used to being in control of any adjustments made to their network, this can be a potential challenge to keep up with. Cloud service updates can affect security considerations for the organizations using them. For example, connection configurations might need to be changed based on the CSP's updates.

Organizations that use CSPs usually have to update their IT processes. It is possible for organizations to continue following established best practices for changes, configurations, and other security considerations. However, an organization might have to adopt a different approach in a way that aligns with changes made by the CSP.

Cloud networking offers various options that might appear attractive to a small company—options that they could never afford to build on their own premises. However, it is important to consider that each service adds complexity to the security profile of the organization, and they will need security personnel to monitor all of the cloud services.

Shared responsibility model

A commonly accepted cloud security principle is the shared responsibility model. The **shared responsibility model** states that the CSP must take responsibility for security involving the cloud infrastructure, including physical data centers, hypervisors, and host operating systems. The company using the cloud service is responsible for the assets and processes that they store or operate in the cloud.

The shared responsibility model ensures that both the CSP and the users agree about where their responsibility for security begins and ends. A problem occurs when organizations assume that the CSP is taking care of security that they have not taken responsibility for. One example of this is cloud applications and configurations. The CSP takes responsibility for securing the cloud, but it is the organization's responsibility to ensure that services are configured properly according to the security requirements of their organization.

Cryptography and cloud security

Cloud security hardening

There are various techniques and tools that can be used to secure cloud network infrastructure and resources. Some common cloud security hardening techniques include incorporating IAM, hypervisors, baselining, cryptography, and cryptographic erasure.

Identity access management (IAM)

Identity access management (IAM) is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can leverage different cloud resources.

Hypervisors

A **hypervisor** abstracts the host's hardware from the operating software environment. There are two types of hypervisors. Type one hypervisors run on the hardware of the host computer. An example of a type one hypervisor is VMware®'s ESXi. Type two hypervisors operate on the software of the host computer. An example of a type two hypervisor is VirtualBox. Cloud service providers (CSPs) commonly use type one hypervisors. CSPs are responsible for managing the hypervisor and other virtualization components. The CSP ensures that cloud resources and cloud environments are available, and it provides regular patches and updates. Vulnerabilities in hypervisors or misconfigurations can lead to virtual machine escapes (VM escapes). A VM escape is an exploit where a malicious actor gains access to the primary hypervisor, potentially the host computer and other VMs. As a CSP customer, you will rarely deal with hypervisors directly.

Baselining

Baselining for cloud networks and operations cover how the cloud environment is configured and set up. A baseline is a fixed reference point. This reference point can be used to compare changes made to a cloud environment. Proper configuration and setup can greatly improve the security and performance of a cloud environment. Examples of establishing a baseline in a cloud environment include: restricting access to the admin portal of the cloud environment, enabling password management, enabling file encryption, and enabling threat detection services for SQL databases.

Cryptography in the cloud

Cryptography can be applied to secure data that is processed and stored in a cloud environment. Cryptography uses encryption and secure key management systems to provide data integrity and confidentiality. Cryptographic encryption is one of the key ways to secure sensitive data and information in the cloud.

Encryption is the process of scrambling information into ciphertext, which is not readable to anyone without the encryption key. Encryption primarily originated from manually encoding messages and information using an algorithm to convert any given letter or number to a new value. Modern encryption relies on the secrecy of a key, rather than the secrecy of an algorithm. Cryptography is an important tool that helps secure cloud networks and data at rest to prevent unauthorized access. You'll learn more about cryptography in-depth in an upcoming course.

Cryptographic erasure

Cryptographic erasure is a method of erasing the encryption key for the encrypted data. When destroying data in the cloud, more traditional methods of data destruction are not as effective. Crypto-shredding is a newer technique where the cryptographic keys used for decrypting the data are destroyed. This makes the data undecipherable and prevents anyone from decrypting the data. When crypto-shredding, all copies of the key need to be destroyed so no one has any opportunity to access the data in the future.

Key Management

Modern encryption relies on keeping the encryption keys secure. Below are the measures you can take to further protect your data when using cloud applications:

- **Trusted platform module (TPM).** TPM is a computer chip that can securely store passwords, certificates, and encryption keys.
- **Cloud hardware security module (CloudHSM).** CloudHSM is a computing device that provides secure storage for cryptographic keys and processes cryptographic operations, such as encryption and decryption.

Organizations and customers do not have access to the cloud service provider (CSP) directly, but they can request audits and security reports by contacting the CSP. Customers typically do not have access to the specific encryption keys that CSPs use to encrypt the customers' data. However, almost all CSPs allow customers to provide their own encryption keys, depending on the service the customer is accessing. In turn, the customer is responsible for their encryption keys and ensuring the keys remain confidential. The CSP is limited in how they can help the customer if the customer's keys are compromised or destroyed. One key benefit of the shared responsibility model is that the customer is not entirely responsible for maintenance of the cryptographic infrastructure. Organizations can assess and monitor the risk involved with allowing the CSP to manage the infrastructure by reviewing a CSPs audit and security controls. For federal contractors, FEDRAMP provides a list of verified CSPs.

Terms and definitions from Course 3, Module 4

- **Baseline configuration (baseline image):** A documented set of specifications within a system that is used as a basis for future builds, releases, and updates
- **Hardware:** The physical components of a computer
- **Multi-factor authentication (MFA):** A security measure which requires a user to verify their identity in two or more ways to access a system or network
- **Network log analysis:** The process of examining network logs to identify events of interest
- **Operating system (OS):** The interface between computer hardware and the user
- **Patch update:** A software and operating system update that addresses security vulnerabilities within a program or product
- **Penetration testing (pen test):** A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes
- **Security hardening:** The process of strengthening a system to reduce its vulnerabilities and attack surface
- **Security information and event management (SIEM):** An application that collects and analyzes log data to monitor critical activities for an organization
- **World-writable file:** A file that can be altered by anyone in the world

To review the exemplar for this course item, click the following link:
Link to exemplar:

- [Incident report analysis](#)

OR

If you don't have a Google account, you can download the exemplar directly from the following attachment.

[Incident report analysis exemplar](#)
[DOCX File](#)

Terms and definitions from Course 3

A

Active packet sniffing: A type of attack where data packets are manipulated in transit

Address Resolution Protocol (ARP): Used to determine the MAC address of the next router or device to traverse

B

Bandwidth: The maximum data transmission capacity over a network, measured by bits per second

Baseline configuration: A documented set of specifications within a system that is used as a basis for future builds, releases, and updates

Bluetooth: Used for wireless communication with nearby physical devices

Botnet: A collection of computers infected by malware that are under the control of a single threat actor, known as the "bot herder"

C

Cloud-based firewalls: Software firewalls that are hosted by the cloud service provider

Cloud computing: The practice of using remote servers, application, and network services that are hosted on the internet instead of on local physical devices

Cloud network: A collection of servers or computers that stores resources and data in remote data centers that can be accessed via the internet

Controlled zone: A subnet that protects the internal network from the uncontrolled zone

D

Data packet: A basic unit of information that travels from one device to another within a network

Denial of service (DoS) attack: An attack that targets a network or server and floods it with network traffic

Distributed denial of service (DDoS) attack: A type of denial of service attack that uses multiple devices or servers located in different locations to flood the target network with unwanted traffic

Domain Name System (DNS): A networking protocol that translates internet domain names into IP addresses

E

Encapsulation: A process performed by a VPN service that protects your data by wrapping sensitive data in other data packets

F

File Transfer Protocol (FTP): Used to transfer files from one device to another over a network

Firewall: A network security device that monitors traffic to or from your network

Forward proxy server: A server that regulates and restricts a person's access to the internet

H

Hardware: The physical components of a computer

Hub: A network device that broadcasts information to every device on the network

Hypertext Transfer Protocol (HTTP): An application layer protocol that provides a method of communication between clients and website servers

Hypertext Transfer Protocol Secure (HTTPS): A network protocol that provides a secure method of communication between clients and servers

I

Identity and access management (IAM): A collection of processes and technologies that helps organizations manage digital identities in their environment

IEEE 802.11 (Wi-Fi): A set of standards that define communication for wireless LANs

Internet Control Message Protocol (ICMP): An internet protocol used by devices to tell each other about data transmission errors across the network

Internet Control Message Protocol (ICMP) flood: A type of DoS attack performed by an attacker repeatedly sending ICMP request packets to a network server

Internet Protocol (IP): A set of standards used for routing and addressing data packets as they travel between devices on a network

Internet Protocol (IP) address: A unique string of characters that identifies the location of a device on the internet

IP spoofing: A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network

L

Local area network (LAN): A network that spans small areas like an office building, a school, or a home

M

Media Access Control (MAC) address: A unique alphanumeric identifier that is assigned to each physical device on a network

Modem: A device that connects your router to the internet and brings internet access to the LAN

Multi-factor authentication (MFA): A security measure that requires a user to verify their identity in two or more ways to access a system or network

N

Network: A group of connected devices

Network log analysis: The process of examining network logs to identify events of interest

Network protocols: A set of rules used by two or more devices on a network to describe the order of delivery of data and the structure of data

Network segmentation: A security technique that divides the network into segments

O

Operating system (OS): The interface between computer hardware and the user

Open systems interconnection (OSI) model: A standardized concept that describes the seven layers computers use to communicate and send data over the network

On-path attack: An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit

P

Packet sniffing: The practice of capturing and inspecting data packets across a network

Passive packet sniffing: A type of attack where a malicious actor connects to a network hub and looks at all traffic on the network

Patch update: A software and operating system update that addresses security vulnerabilities within a program or product

Penetration testing: A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes

Ping of death: A type of DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB

Port: A software-based location that organizes the sending and receiving of data between devices on a network

Port filtering: A firewall function that blocks or allows certain port numbers to limit unwanted communication

Proxy server: A server that fulfills the requests of its clients by forwarding them to other servers

R

Replay attack: A network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time

Reverse proxy server: A server that regulates and restricts the Internet's access to an internal server

Router: A network device that connects multiple networks together

S

Secure File Transfer Protocol (SFTP): A secure protocol used to transfer files from one device to another over a network

Secure shell (SSH): A security protocol used to create a shell with a remote system

Security hardening: The process of strengthening a system to reduce its vulnerabilities and attack surface

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities for an organization

Security zone: A segment of a company's network that protects the internal network from the internet

Simple Network Management Protocol (SNMP): A network protocol used for monitoring and managing devices on a network

Smurf attack: A network attack performed when an attacker sniffs an authorized user's IP address and floods it with ICMP packets

Speed: The rate at which a device sends and receives data, measured by bits per second

Stateful: A class of firewall that keeps track of information passing through it and proactively filters out threats

Stateless: A class of firewall that operates based on predefined rules and that does not keep track of information from data packets

Subnetting: The subdivision of a network into logical groups called subnets

Switch: A device that makes connections between specific devices on a network by sending and receiving data between them

Synchronize (SYN) flood attack: A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets

T

TCP/IP model: A framework used to visualize how data is organized and transmitted across a network

Transmission Control Protocol (TCP): An internet communication protocol that allows two devices to form a connection and stream data

Transmission control protocol (TCP) 3-way handshake: A three-step process used to establish an authenticated connection between two devices on a network

U

Uncontrolled zone: The portion of the network outside the organization

User Datagram Protocol (UDP): A connectionless protocol that does not establish a connection between devices before transmissions

V

Virtual Private Network (VPN): A network security service that changes your public IP address and masks your virtual location so that you can keep your data private when you are using a public network like the internet

W

Wide Area Network (WAN): A network that spans a large geographic area like a city, state, or country

Wi-Fi Protected Access (WPA): A wireless security protocol for devices to connect to the internet

Scenario

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

To address this security event, the network security team implemented:

A new firewall rule to limit the rate of incoming ICMP packets

Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets

Network monitoring software to detect abnormal traffic patterns

An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity incident and integrate your analysis into a general security strategy:

Identify security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.

Protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.

Detect potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.

Respond to contain, neutralize, and analyze security incidents; implement improvements to the security process.

Recover affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.

Step-By-Step Instructions

Step 1: Access the incident report analysis template

To access template for this course item, click the following link and select *Use Template*.

Link to template: [Incident report analysis](#)

Link to supporting materials:

[Applying the NIST CSF](#)

[Example of an incident report analysis](#)

OR If you don't have a Google account, you can download the template directly from the following attachment.

[Incident report analysis DOCX File](#)

[Applying the NIST CSF DOCX File](#)

[Completed Example of an Incident report analysis DOCX File](#)

Step 2: Identify the type of attack and the systems affected

Think about all of the concepts covered in the course so far and reflect on the scenario to determine what type of attack occurred and which systems were affected. List this information in the incident report analysis worksheet in the section titled "Identify."

Step 3: Protect the assets in your organization from being compromised

Next, you will assess where the organization can improve to further protect its assets. In this step, you will focus on creating an immediate action plan to respond to the cybersecurity incident. When creating this plan, reflect on the following question:

- What systems or procedures need to be updated or changed to further secure the organization's assets?

Write your response in the incident report analysis template in the "Protect" section.

Step 4: Determine how to detect similar incidents in the future

It is important to continuously monitor network traffic on network devices to check for suspicious activity, such as incoming external ICMP packets from non-trusted IP addresses attempting to pass through the organization's network firewall.

For this step, consider ways you and your team can monitor and analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Write your response in the incident response analysis worksheet in the "Detect" section.

Step 5: Create a response plan for future cybersecurity incidents

After identifying the tools and methods you and your organization have in place for detecting potential vulnerabilities and threats, create a response plan in the event of a future incident. This typically happens after the incident occurred and has been resolved by you and your team. In this case, you will create a response plan for future cybersecurity incidents. Some items to consider when creating a response plan to any cybersecurity incident:

- How can you and your team contain cybersecurity incidents and affected devices?
- What procedures are in place to help you and your team neutralize cybersecurity incidents?
- What data or information can be used to analyze this incident?
- How can your organization's recovery process be improved to better handle future cybersecurity incidents?

Write your response in the incident report analysis template under the "respond" section.

Step 6: Help your organization recover from the incident

Consider what steps need to be taken to help the organization recover from the cybersecurity incident. Reflect on all the information you gathered about the incident in the previous steps to consider which devices, systems, and processes need to be restored and recovered.

Consider the following questions:

- What information do you need to be able to recover immediately?
- What processes are in place to help the organization recover from the incident?

Write your response in the "recover" portion of the worksheet.