Introduction to Network Tools and Protocols

In this section, you will explore various tools and protocols essential for maintaining network security. These concepts will be crucial in your role as a security analyst, helping to protect your organization's network from potential attacks.

Key Learning Areas:

1. Network Protocols: Learn about the protocols that govern how data is transferred across networks and how malicious actors can exploit these protocols. Understanding these protocols will help you spot any irregularities in network traffic.
   * Example: Identifying an attack based on the use of an incorrect protocol, even when other traffic patterns seemed normal.
2. Virtual Private Networks (VPNs): VPNs are used to secure communications across the internet by encrypting data and hiding a user’s IP address. You'll learn how VPNs protect sensitive information during transmission.
3. Firewalls, Security Zones, and Proxy Servers: These tools help monitor and control incoming and outgoing network traffic.
   * Firewalls: Serve as a barrier to protect against unauthorized access.
   * Security Zones: Dividing the network into different zones allows for better control and segmentation.
   * Proxy Servers: Act as intermediaries between users and the internet, improving security and anonymity.

By the end of this section, you’ll understand how to use these tools and protocols to monitor, secure, and protect your organization's network against potential security threats.

Understanding Network Protocols and Their Role in Communication

Network protocols are essential for ensuring that data sent across a network reaches its correct destination. They provide the rules and structure for how devices communicate, ensuring smooth and accurate data transmission.

Example: Accessing a Website When you access a website, several protocols work together to ensure that your request is fulfilled securely and accurately:

1. Transmission Control Protocol (TCP): Establishes a connection between your device and the web server through a handshake. This verifies both devices before allowing communication.
2. Address Resolution Protocol (ARP): Helps determine the MAC address of the next device (router) in the path of the data packet, ensuring it reaches the correct destination.
3. Hypertext Transfer Protocol Secure (HTTPS): Secures communication between your device and the server, using encryption (SSL/TLS) to protect sensitive data from malicious actors.
4. Domain Name System (DNS): Translates the website’s domain name (like [www.yummyrecipesforme.org](http://www.yummyrecipesforme.org)) into an IP address so that your device can locate the server hosting the website.

In this example, just by visiting a website, your device uses four key protocols—TCP, ARP, HTTPS, and DNS—to establish a secure and efficient communication path.

Connection to Security

* HTTPS ensures that data exchanged with websites is encrypted, protecting against interception and malicious attacks.
* Security protocols like SSL/TLS (Secure Sockets Layer / Transport Layer Security) are part of HTTPS, securing the communication by encrypting the data.

By understanding these protocols, you'll be better prepared to secure communications and monitor network traffic as a security analyst.

Common network protocols

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

Overview of network protocols

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

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

Three categories of network protocols

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

Communication protocols

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

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

Management Protocols

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

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

Security Protocols

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

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

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

Key takeaways

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

Additional network protocols

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

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

Network Address Translation

The devices on your local home or office network each have a private IP address that they use to communicate directly with each other. However, in order for the devices with private IP addresses to communicate with the public internet, they need to have a single public IP address that represents all devices on the LAN to the public. For outgoing messages, the router can replace a private source IP address with its public IP address and perform the reverse operation for responses. This process is known as Network Address Translation (NAT) and it generally requires a router or firewall to be specifically configured to perform NAT. NAT is a part of layer 2 (internet layer) and layer 3 (transport layer) of the TCP/IP model.

| Private IP Addresses | Public IP Addresses |
| --- | --- |
| * Assigned by the router * Unique only within private network * No cost to use * Address ranges:   + 10.0.0.0-10.255.255.255   + 172.16.0.0-172.31.255.255   + 192.168.0.0-192.168.255.255 | * Assigned by ISP and IANA * Unique address in global internet * Costs to lease a public IP address * Assignable 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 works with the router to assign a unique IP address to each device and provide 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 a public IP address, a private IP address, and a MAC address that identify it on the network. A device’s IP address may change over time, but its MAC address is permanent because it is unique to a device's network interface card. The MAC address is used to communicate with devices within the same network, but sometimes, the MAC address is unknown. This is why the Address Resolution Protocol (ARP) is needed. 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 since it is a layer 2 protocol and port numbers are associated with the layer 7 application layer.

Telnet

Telnet is an application layer protocol that is used to connect with a remote system. 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. POP3 is the most commonly used version of POP. 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. After downloading, the mail may or may not be deleted from the mail server, so it does not guarantee that a user can sync the same email across multiple devices.

Internet Message Access Protocol (IMAP)

IMAP is used for incoming email. It downloads the headers of emails and the message content. The content also 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. Since the mail is kept on the mail server, it allows a user to sync emails across multiple devices.

Simple Mail Transfer Protocol

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

Protocols and port numbers

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

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

Key takeaways

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

| Protocol | Port |
| --- | --- |
| DHCP | UDP port 67 (servers)  UDP port 68 (clients) |
| ARP | none |
| Telnet | TCP port 23 |
| SSH | TCP port 22 |
| POP3 | TCP/UDP port 110 (unencrypted)  TCP/UDP port 995 (encrypted, SSL/TLS) |
| IMAP | TCP port 143 (unencrypted)  TCP port 993 (encrypted, SSL/TLS) |
| SMTP | TCP/UDP Port 25 (unencrypted) |
| SMTPS | TCP/UDP port 587 (encrypted, TLS) |