Common Network Conversations & Their Protocols

Reading

30 minutes

✓ Status | Incomplete

Introduction

Currently, there may be thousands of protocols used to communicate applications over a single network. In this reading, you will be introduced to some of the most well-known and most influential basic network protocols.

Reading

Important Protocols Over the Network

Address Resolution Protocol (ARP)

ARP is a TCP/IP stack protocol to map Layer 2 physical MAC addresses into IP addresses. These MAC addresses provide exclusive identification over a network. ARP is used when information sent to a network arrives at the gateway, which serves as the entry point to the network. The gateway uses ARP to find the computer's MAC address based on the IP address to which data is being sent. ARP typically looks up this information in a table called the **ARP cache**. If the address is found, the information will be relayed to the gateway, sending the received data to the appropriate machine. It can also convert the data to the correct network format if needed.

If the address is not found, ARP will broadcast a **request packet** to other machines on the network to verify that the IP address belongs to a device not listed in the ARP cache. If a valid system is found, the information will be relayed to the gateway, and the ARP cache will be updated with the new information. Updating the ARP cache will make future requests to that IP address much faster. While this seems like a complex process, it usually only takes a second to complete.

TCP/IP

TCP/IP is fundamental to the Internet network. These two protocols ensure that information packets reach their destination correctly and securely. This way, we can process and define the data between devices before going to their destinations.

TCP defines how applications can create communication channels across the network. It is the Transport layer that establishes a reliable, ordered connection between two devices for the exchange of data. It also assists in breaking a message into pieces that will later be reconstructed before reaching its destination. The IP is what defines the address and path of the data packet. It ensures that the information reaches its correct destination.

HTTP (Hypertext Transfer Protocol)

HTTP is a protocol that specifies how the communication between a browser and a web server will occur. It enables communication by sending and receiving messages in the form of requests and responses. It is the foundation of the **World Wide Web (www)** and it is used for communication between clients and servers.

This protocol works through a computational model known as client-server, where a browser (client) establishes communication with a server, and both begin exchanging information. HTTP is part of the Application layer, closest to the end user and usually works together with another transfer protocol: TCP/IP which is part of the Transport layer, and the IP on the Network layer.

Simple Mail Transfer Protocol (SMTP)

SMTP is a protocol that only sends e-mails, which means that the user is not allowed to download messages from the server. Using an e-mail client that supports **POP3** or **IMAP** protocols is necessary. Most applications like Gmail support the use of SMTP for sending emails.

Secure Shell (SSH)

Like the VM?

SSH is a protocol that allows you to connect and access a server as if you were in a terminal. It provides a secure way to access a remote device by encrypting all communications between the client and the server. The risk of someone tampering with your work on the server is virtually zero.

When a user connects via SSH to another computer, the user can log into the remote device and execute commands as if they were sitting at the device's console. A common example of this will be a web developer connecting to the company web server from their local machine. To do so they can use a command like `ssh dev@192.73.8.101` from the terminal on their local machine. They will then be prompted to enter a password and then the terminal session will connect to the web server. This means any command the user types now runs on that remote computer, not on their PC.

Internet Control Message Protocol (ICMP)

ICMP is a protocol to troubleshoot network connectivity or data transfer problems between devices. It assists in sending, receiving, and processing ICMP messages to report connectivity issues to source network devices. Therefore, the primary purpose of the ICMP is to report errors at the Network layer. For example, this protocol is used whenever you use the ***ping*** command. This is used to test your ability to contact another machine. If the packets are lost this commonly signifies an issue in connectivity, but if the machine replies to the ping this signifies that you are able to reach that machine with no issues.

DNS (Domain Name System)

DNS is a record that contains website names and their associated IP addresses. This correlation favours the transfer of data between computers and allows access to the Internet. The request is sent to your ISP and forwarded to DNS. Friendly to humans, the DNS works to connect that URL to the real server's IP address and is called DNS name resolution. It involves a DNS resource that queries multiple nameservers to find a server's actual IP address. For example, when you enter the name www.google.com into a web browser, DNS is used to convert that into an IP Address that allows your machine to contact the web server and give you the website that you see. If DNS didn't exist you would have to memorize the Google web server IP Address everytime you wanted to visit the website.

Dynamic Host Configuration Protocol (DHCP)

DHCP is a relevant tool for data network infrastructure; that is how computers automatically get an IP address. When a **DHCP** server receives a request, the addresses and settings are available to the client machine. It can operate in three ways: automatic, dynamic, and manual. In automatic DHCP, you define an IP amount in a range for use on the network. Whenever a computer requests a connection, another workstation assigns an IP that is not in use.

In the dynamic configuration, the computer's connection to the IP has a time limit predetermined by the network administrator. Regardless of the MAC address, a free IP address is assigned. In manual DHCP, IPs are allocated according to the MAC of the network interfaces.

> ? Why do you think is it important for security professionals to know about these different protocols?
>
> **Your Answer**
>
> Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.
>
> Toggle Answer

Conclusion

Understanding the use and purpose of some of the common protocols and how they are used in network communications will help you be prepared for upcoming exercises in this course, as well as your future Cyber Security professional activities.

✓ Mark Completed

← Previous
Network Administration

Next
Network Administration Quiz →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W01D4

Thu Jun 27

Lectures (1)

Work (7)

4 hrs

- Common Network Conversations & Their Protocols
- ? Network Administration Quiz ✓
- Windows Logging
- Linux Logging: Syslog and Log Collection
- Centralized Logging
- ? Logs
- Troubleshooting Approaches

W01D4 Schedule »

Powered by Lighthouse Labs.