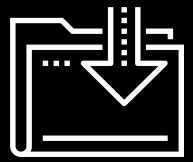
Following Data Through Layers 2, 3, and 4

Cybersecurity

Networking 101, Day 3



© 2022 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.

Class Objectives

By the end of today's class, you will be able to:

- Define enumeration as a set of methods used by security professionals and attackers to determine network vulnerabilities.
- Use `Wireshark` to capture and analyze ARP activity, including ARP spoofing.
- Use `ping` to determine if hosts are reachable.
- Use `traceroute` to troubleshoot networking communication issues between two devices.
- Define and distinguish between TCP and UDP.
- Analyze TCP traffic in Wireshark.
- Analyze SYN scans to determine the availability of ports on a network.


Recap

Recap

Let's briefly review the topics of the previous class:

Protocols are standardized rules that dictate how data is communicated.

Ports assist with where data is transmitted from and to with respect to the server and client.

The seven layers of the OSI model conceptualize how data is communicated across a network.

Wireshark is a powerful utility for in-depth analysis of network packets.

Introduction to Enumeration

Attackers often try to gain unauthorized access into a network.

It’s the job of security professionals to secure networks by identifying vulnerabilities.

Real-world Hacking Example

- An attacker discovers that a server with payroll data accidentally has open port 22, for SSH.
- This lets the attacker gain unauthorized access to the network, allowing the attacker to steal or alter important data, e.g., social security numbers or salary information.
- It is the security professional's job to determine which unauthorized ports are open, and then close them, protecting the integrity of the company.

The methods used by security professionals to find and patch vulnerabilities are often the same ones used by hackers to find and exploit vulnerabilities.

The methods used by hackers to find and exploit vulnerabilities are often the same ones used by security professionals to find and patch vulnerabilities.

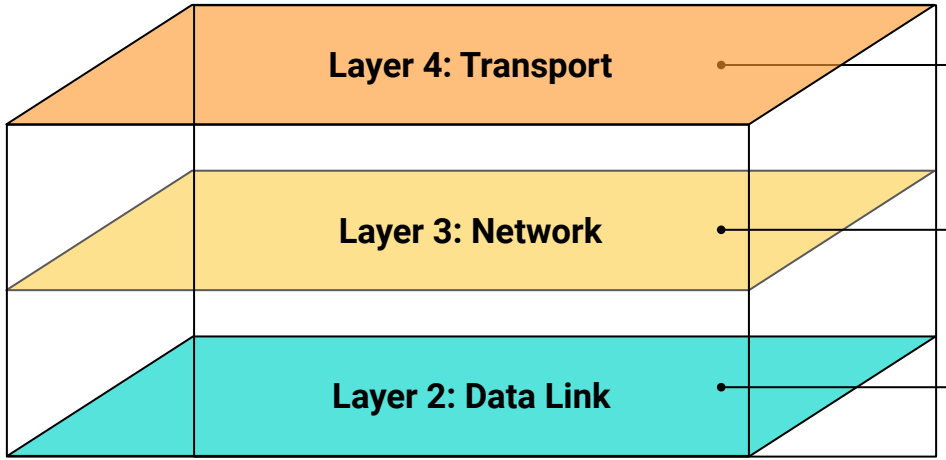
Enumeration is the process of gathering data for a specific network, usually for the purpose of finding ways to gain access into that network.

Enumeration

Enumeration can provide the following information:

Enumeration

Security professionals use protocols and tools that exist in Layers 2, 3, and 4 of the OSI model to enumerate a network:



Transport protocols **TCP** and **UDP** (**TCP** establishes a connection with a three-way handshake).

Network utilities `ping` and `traceroute`, used by network and security professionals to diagnose network issues.

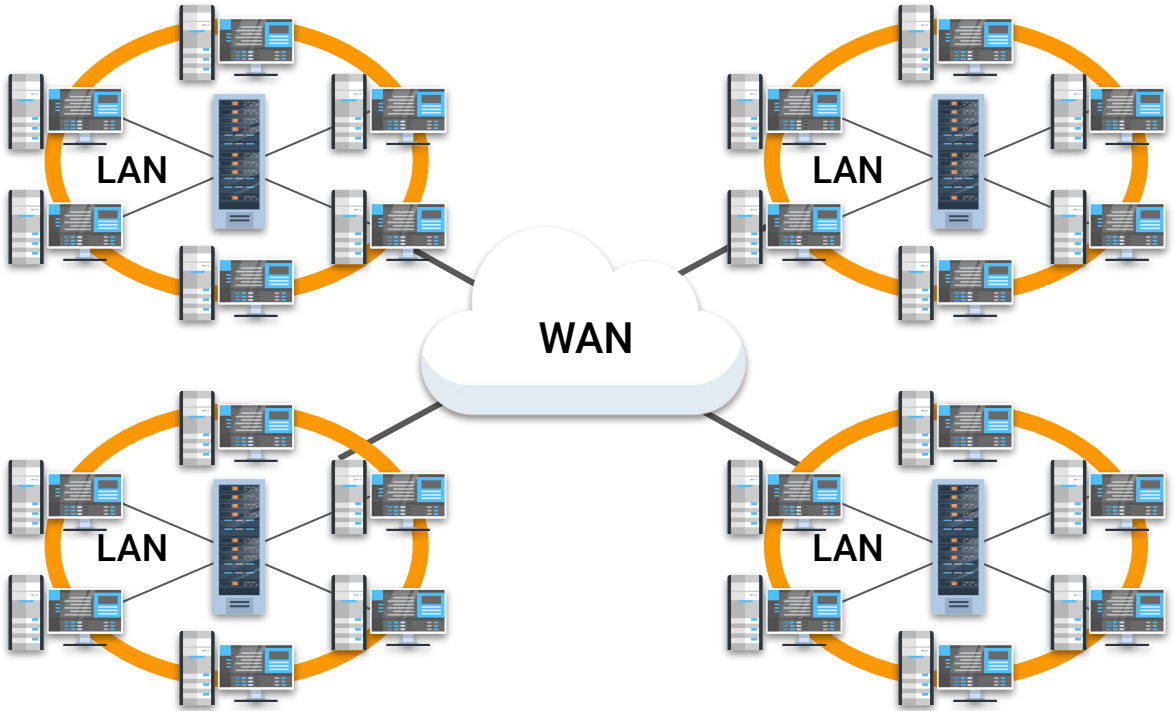
Data link protocol **ARP**, used to transfer network traffic within a local network.

Address Resolution Protocol (ARP)
(Layer 2: Data Link)

Intro to ARP

First, we'll recap the process used by networks to communicate with each other over the internet:

- When devices communicate from one network to another, they often send communications across the internet. This type of network is a **wide area network**, or **WAN**.
- The data then travels across the internet to its destination network, a **local area network**, or **LAN**.
- Once the data reaches the LAN, it still has to be transmitted to its final destination on the LAN.



Media Access Control (MAC)

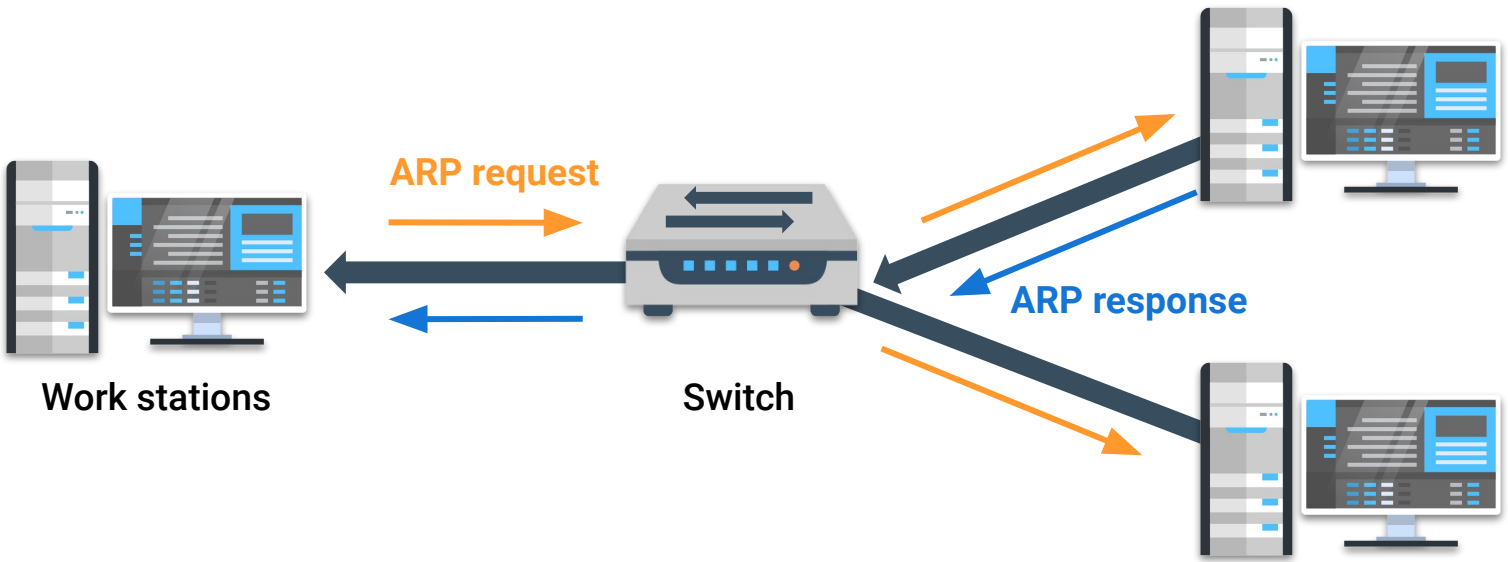
Once on a LAN, the data is routed through network devices called **switches** to a physical machine address.

- The physical address, also referred to as the **media access control** (**MAC) address**, is a sequence of numbers and letters, such as `00:0c:29:0f:71:a3`, that identifies the destination computer's unique hardware number.
- Without a **MAC address**, the data may reach the LAN, but not know where to next transmit the data.

Now Entering Layer 2: Data Link

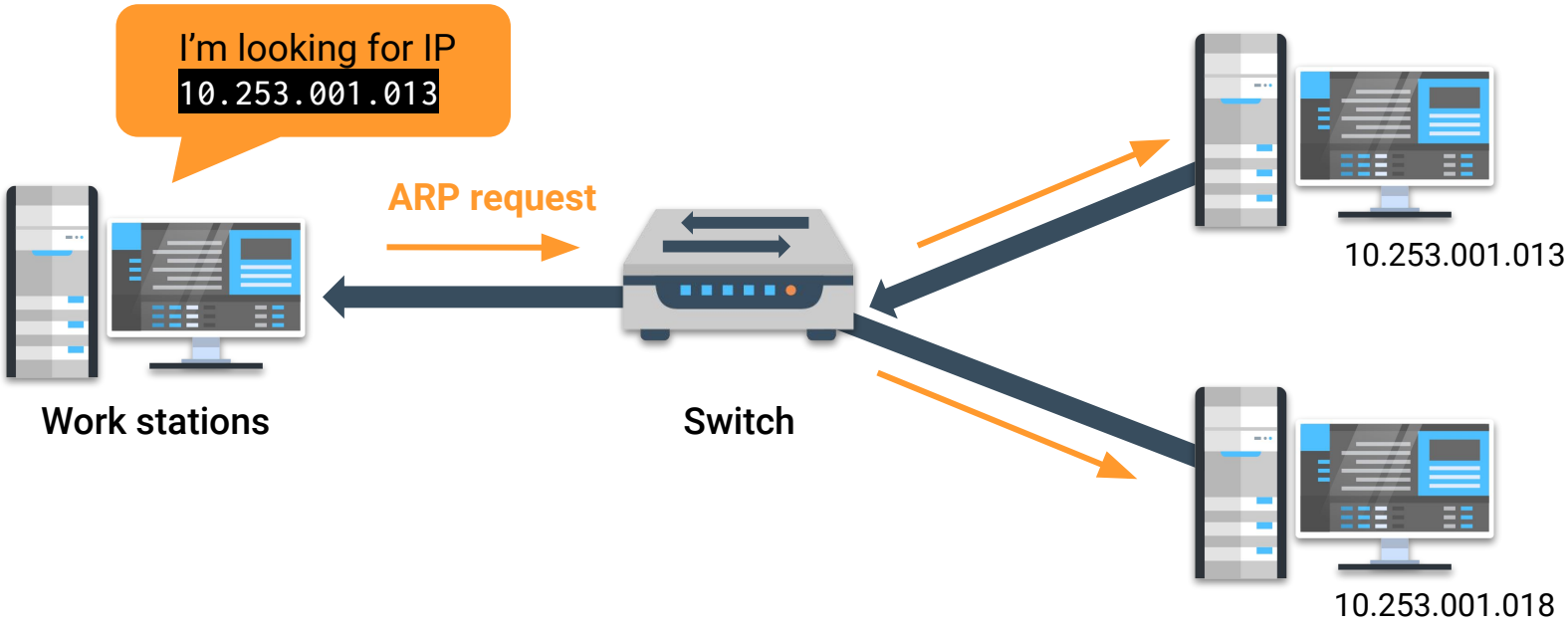
To ensure data gets from the LAN to the machine, the **Address Resolution Protocol (ARP)** maps the MAC address to an IP address within the LAN.

This mapping is done through an **ARP request and response** process.



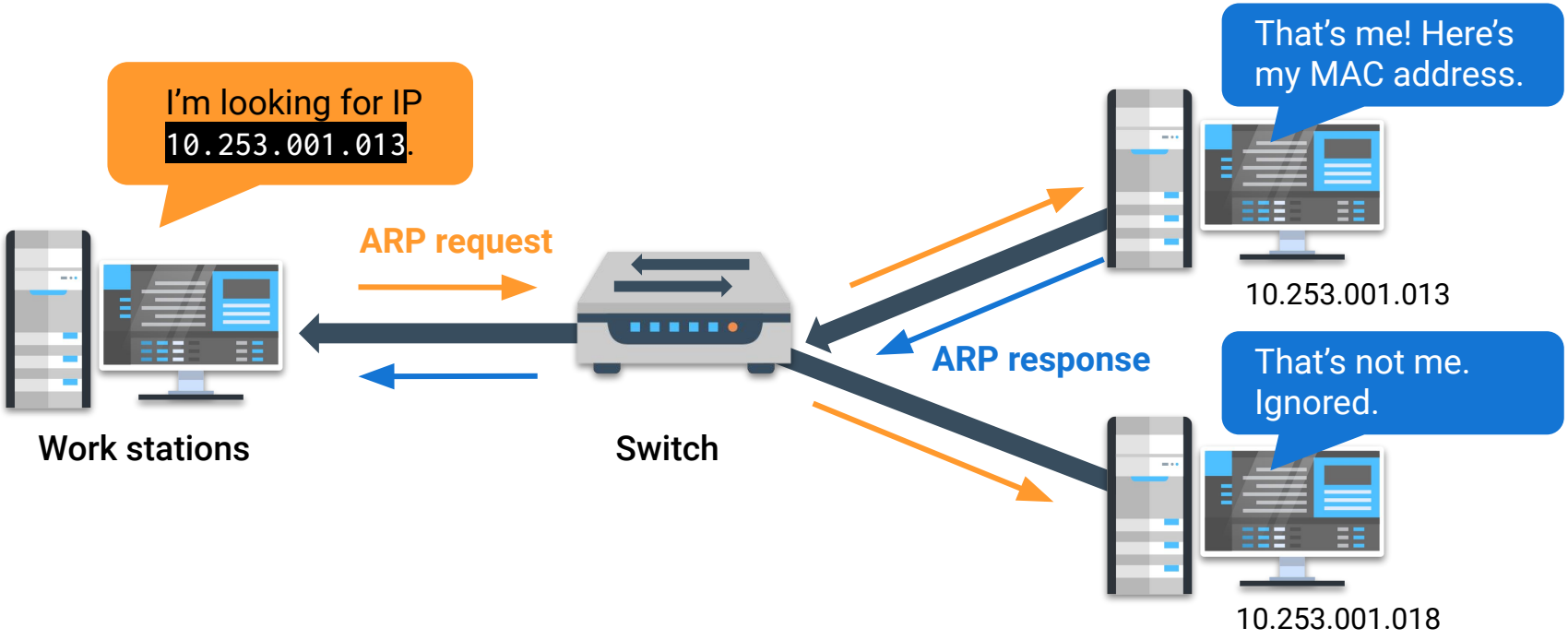
Now Entering Layer 2: Data Link

The network device transmitting the data broadcasts an **ARP request** to all devices in its network to find the physical address matching the IP address.



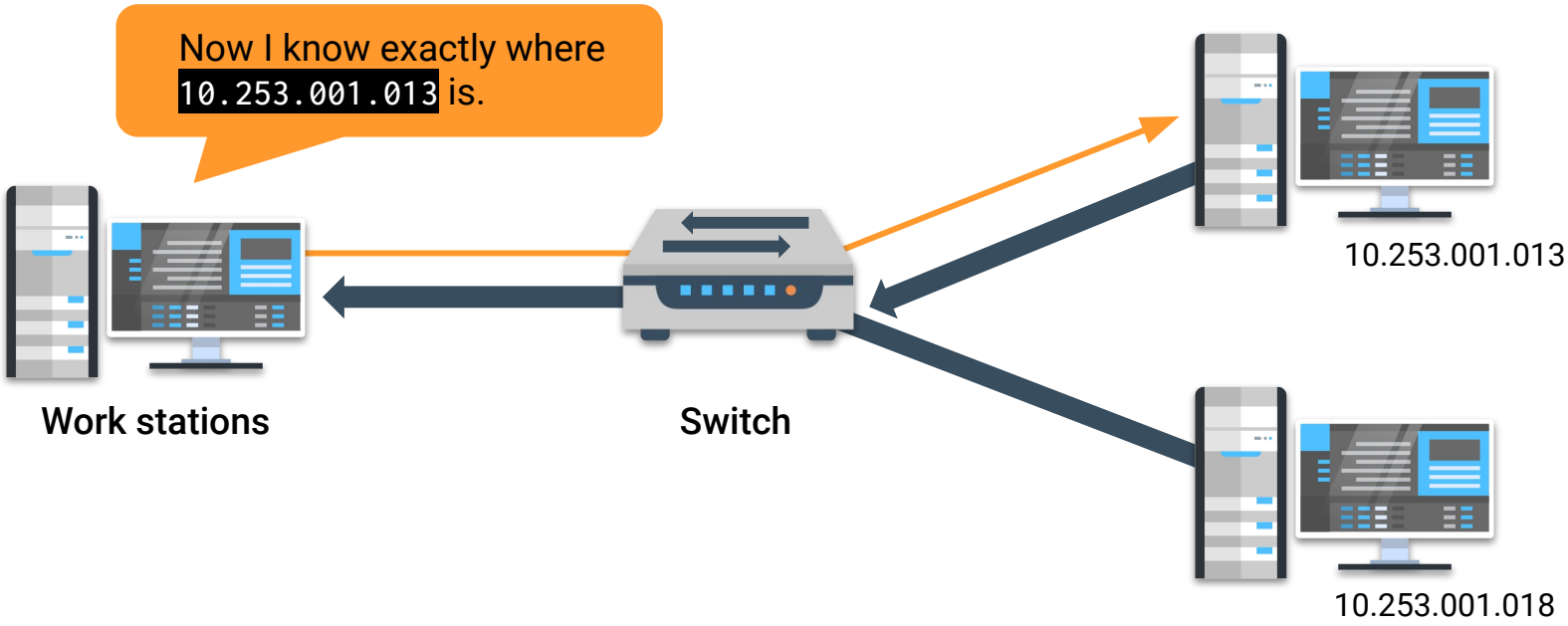
Now Entering Layer 2: Data Link

The device that owns that IP address recognizes its IP in the ARP request. It sends an **ARP reply** with its **MAC address**, so the network knows where to route the data.



Now Entering Layer 2: Data Link

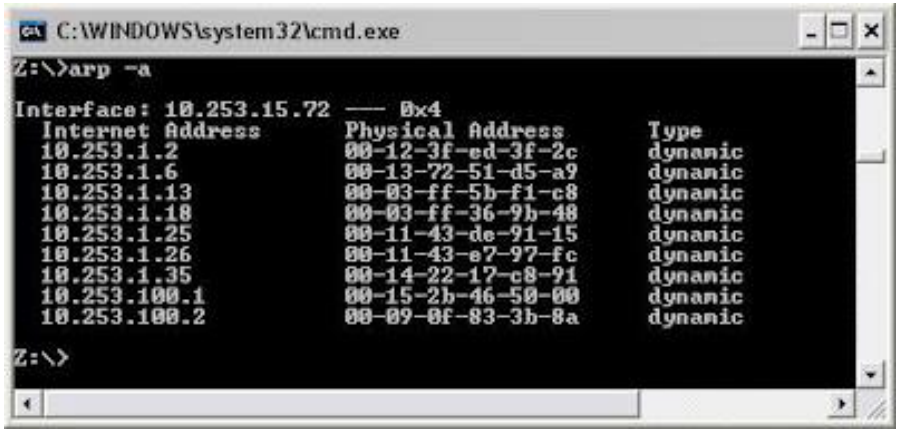
The mapping of the MAC address to the IP address is added into the **ARP cache**. The next time data comes in for this specific destination, it won't need to broadcast an ARP request. The network has the record in its cache and can automatically route the data.



ARP Cache Timeout

Entries added to the ARP cache are called **dynamic ARP entries**, meaning they can be changed with future ARP replies.

- Dynamic ARP entries will only stay in the ARP cache for a limited period of time, known as the **ARP cache timeout**.
- When the ARP cache timeout expires, the record is removed from the ARP cache, and any future requests for the host require a new ARP request.



Source

ARP and Wireshark Setup

Wireshark allows us to visualize ARP requests and responses.

In the next demo:

- We will filter for all ARP packets in a .pcap file.
- This filter will show us the request from the source host, which will include a MAC address, associated with a specific IP address, that the data needs to be transmitted to.
- If the request can be successfully answered, we'll see a response from the owner of the IP address that contains the device's MAC address.

Instructor Demonstration

ARP and Wireshark Setup

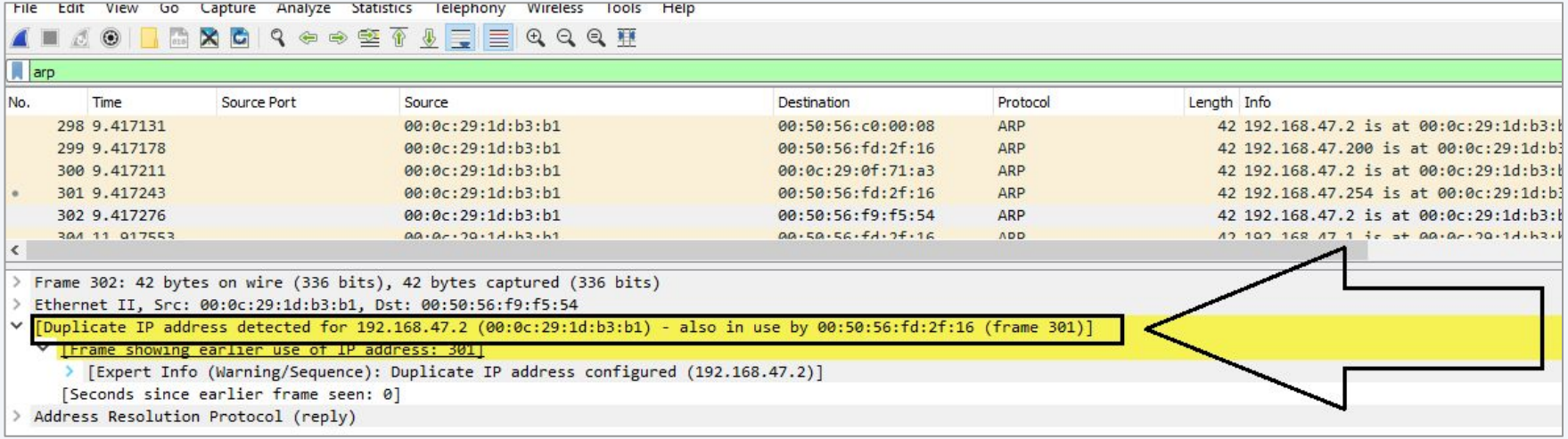
Now that we know how ARP assists with routing data within a LAN, we will look at the security vulnerabilities associated with the protocol.

ARP and Security

If an attacker has access to a LAN, they can intercept traffic on its way to the correct destination (“the good host”).

ARP Spoofing

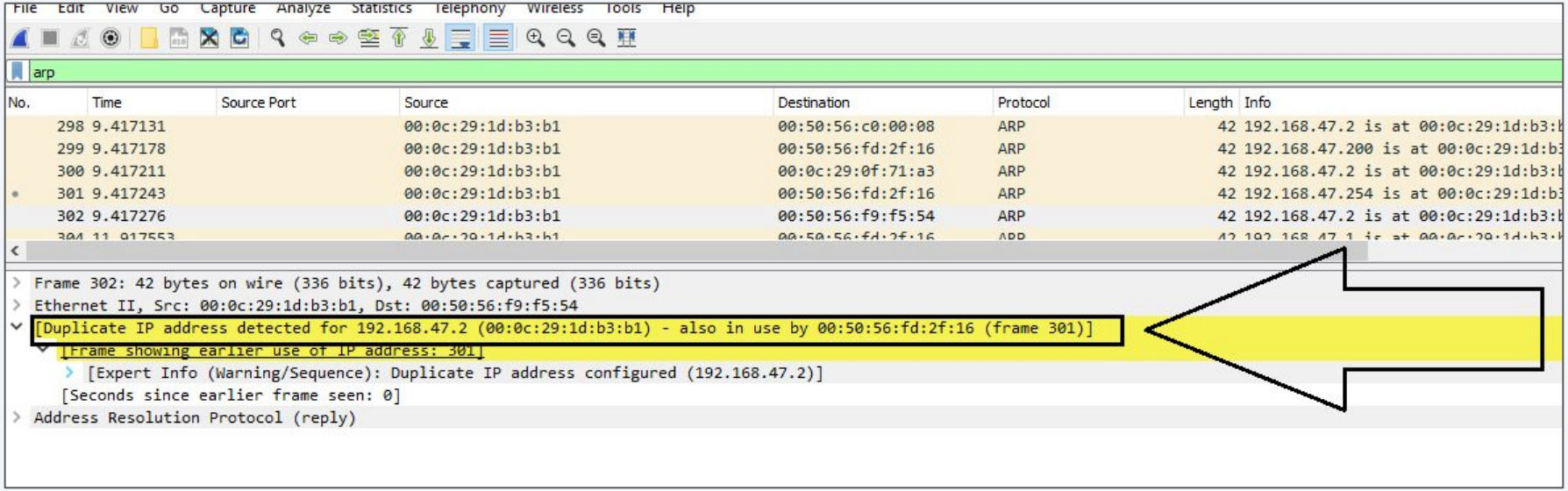
- The attacker can send a spoof ARP message to the LAN, directing all traffic intended for the good host to the attacker's MAC address.
- After the attacker sends the spoof ARP message, all traffic originally destined for the good host is intercepted by the attacker's device with the malicious MAC address.
- This attack is known as **ARP cache poisoning** or **ARP spoofing**.



This vulnerability has significant consequences, since it can be used to intercept classified or sensitive data such as usernames and passwords.

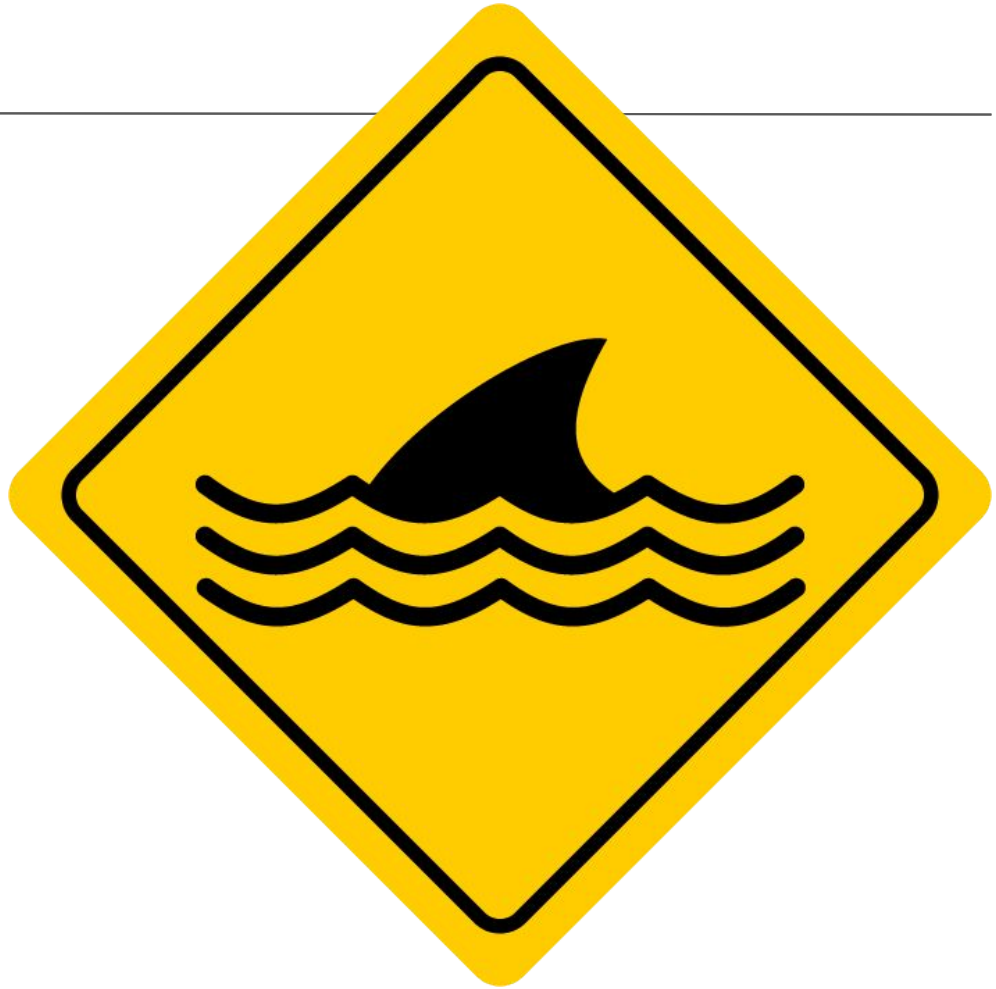
ARP Spoofing

- The good host is **`192.168.47.2`**; the correct MAC address is **`00:50:56:fd:2f:16`**.
- The attacker's MAC address is **`00:0c:29:1d:b3:b1.`** A spoof ARP message directs traffic intended for the good MAC address to the attacker's MAC address.
- The spoof ARP message can be understood as **`192.168.47.2 is at 00:0c:29:1d:b3:b1.`**



But There's a Solution!

Wireshark can detect and alert multiple MAC addresses associated with a single IP address, but it will not take any action on its own.



Static ARP Entries

To protect against an ARP poisoning attack, a network administrator can create **static ARP entries**, rather than dynamic ARP entries.

- Static ARP entries create permanent IP-to-MAC-address mappings in the ARP cache.
- Unlike the dynamic ARP entries, these cannot be changed.
- However, it is time-consuming to manually enter and edit each IP-to-MAC mapping in the ARP cache as they are added and changed.
- Additionally, ARP spoofing detection software programs can be installed to identify and block ARP poisoning attempts. These can be expensive and often require time to install, maintain, and update.

Activity: Analyze ARP Activity

In this activity, you will play the role of a security analyst at Acme Corp. CompuCom, a software company, has hired Acme Corp to do a security assessment of its network.

You will analyze ARP activity from a CompuCom packet capture to determine whether any vulnerabilities exist.

Suggested Time:

15 Minutes

Time’s Up! Let’s Review.

Questions?

ping

(Packet Inter-network Groper)

When enumerating, it’s important to check if an external host is reachable.

`ping` Example

Company X wants to make sure its new intranet is accessible from its offices in the United States and Japan.

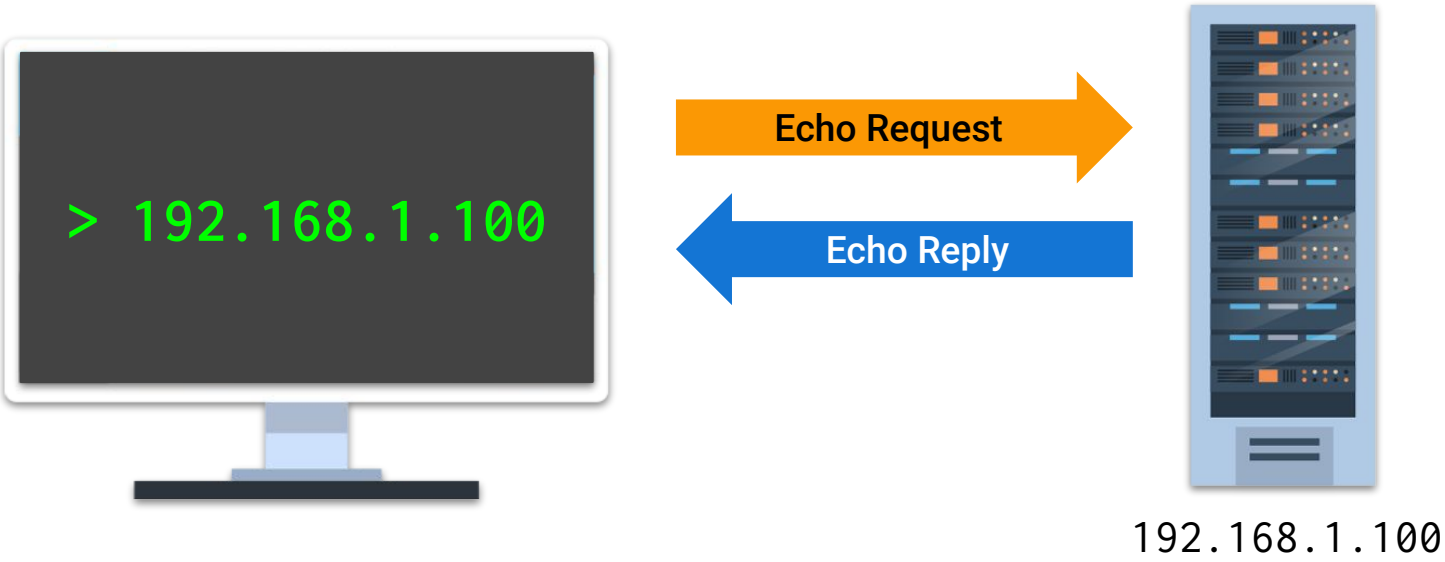
- The intranet is used for daily employee tasks and to access employee contact information. So intranet **availability** is critical for all employees.
- To test the intranet's accessibility, Company X has employees from the United States and Japan each send a `ping` request from their location, validating that the intranet is **available** and **accessible** from each location.

ping (Packet Inter-network Groper) is a utility used to determine whether a host is operating and responding to echo requests.

Internet Control Message Protocol

When we ping a host, it sends an **Internet Control Message Protocol (ICMP) echo request** to a specific IP address and waits on a reply.

ICMP is a protocol that network devices use to send error messages and operational information about whether a requested service or host can be reached.



`ping` Demo Scenario

In the following demonstration, we'll use `ping` on the command line with the following scenario:

- You are a restaurant looking to purchase commercial beverages online.
- You need to check if Pepsi.com is working and accepting requests.

Instructor Demonstration

`ping`

Activity: Enumerating with `ping`

In this activity, you will continue to play the role of a security analyst at Acme Corp.

You must use `ping` to determine which of CompuCom's host IP addresses are accepting connections.

Suggested Time:

15 Minutes

Time’s Up! Let’s Review.

Questions?

Countdown timer

15:00

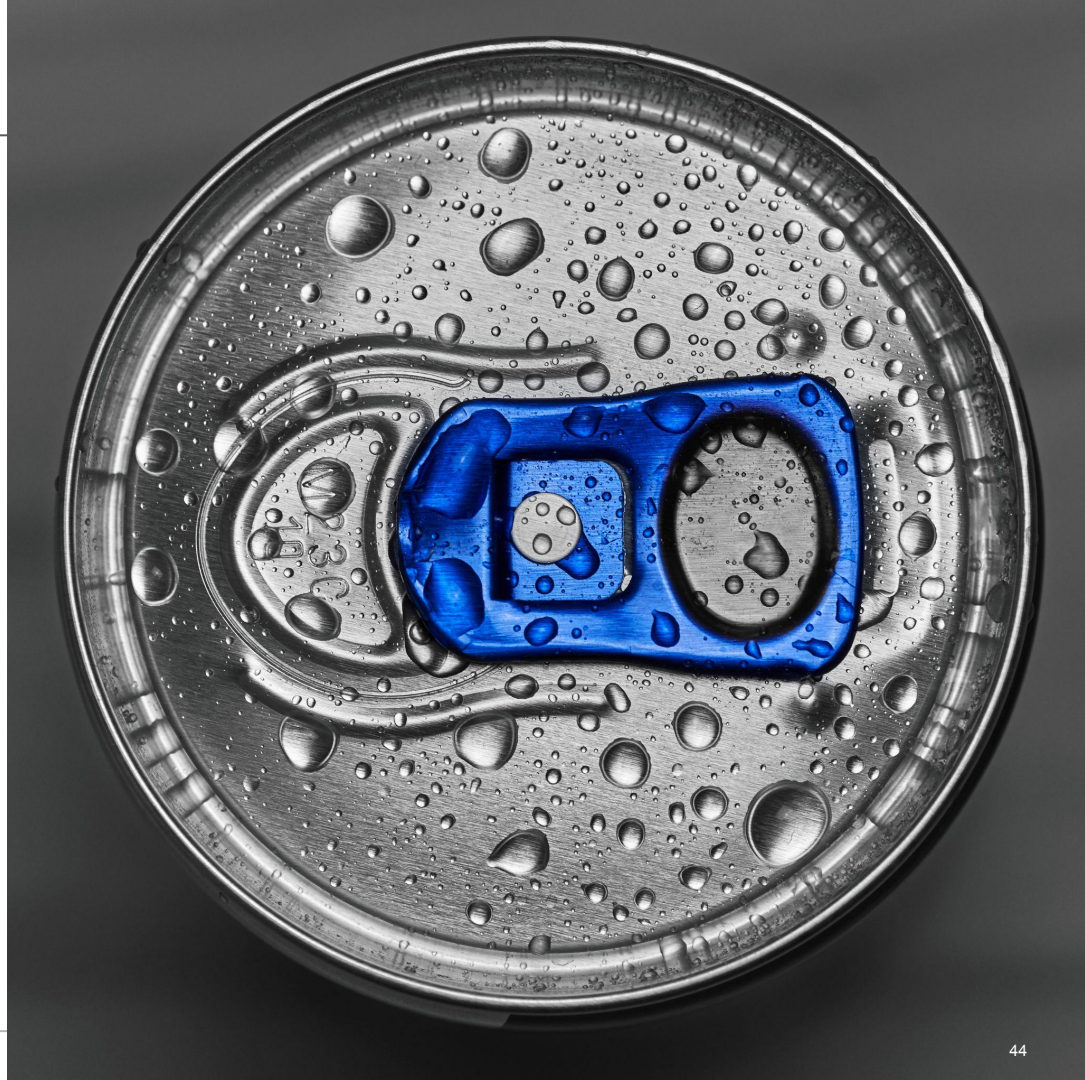
(with alarm)

Introduction to `traceroute`

`traceroute` Demo

In the previous demonstration, we discovered that redbull.com did not respond to our ping.

Now we'll find out why.



While `ping` indicates if a host is up or down, security professionals often need more info to determine why.

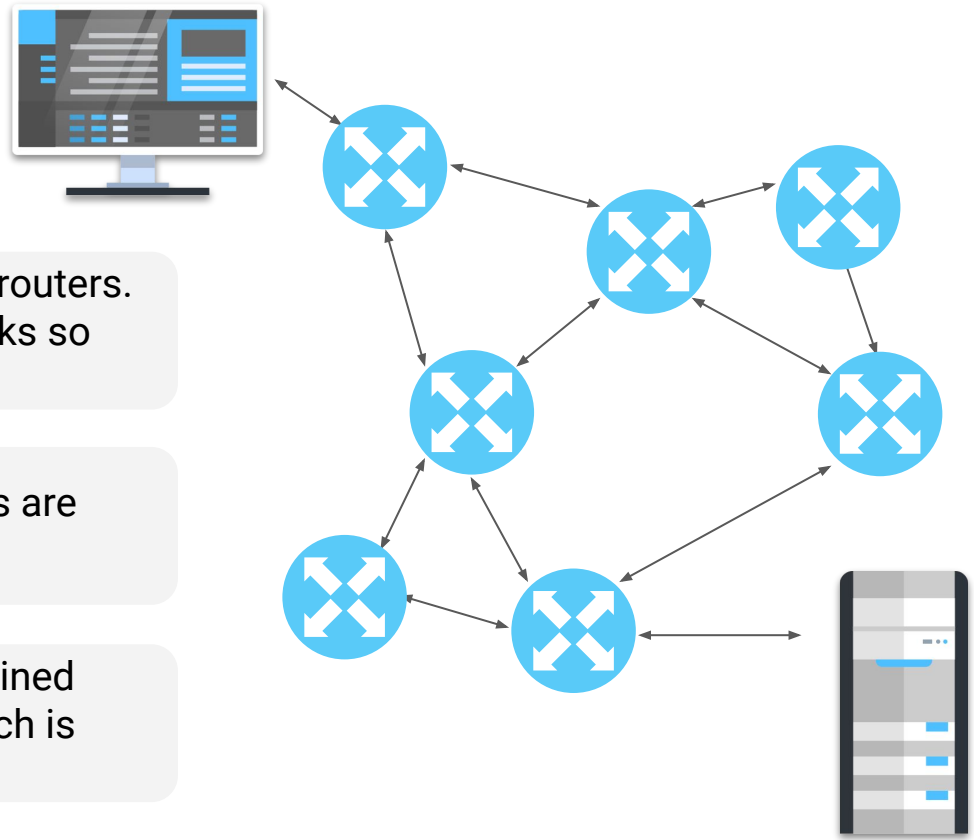
For Example:

Company X's employees were able to successfully ping their intranet from the United States office, but unable to ping the exact same address from the Japan office.

- More information is needed to understand why the intranet is not accessible from Japan.
- Company X can better understand the issue by finding out where in the request the failure occurred.

Routing and Redirections

When data travels from a source to a destination, it typically does not follow a straight path.

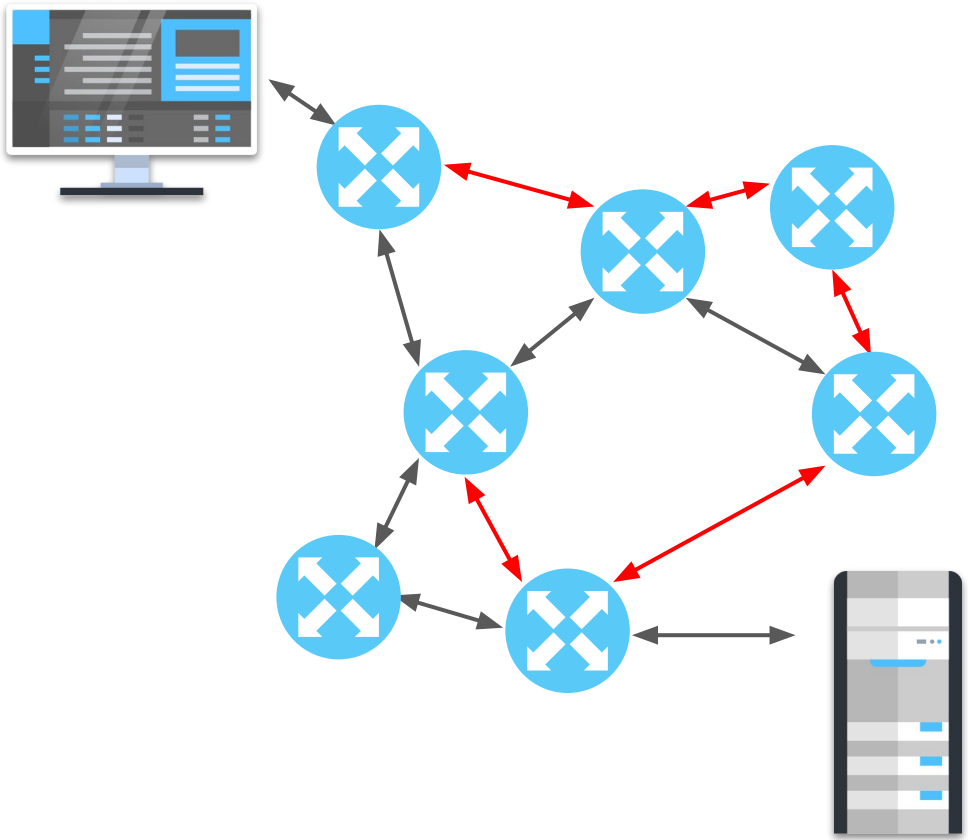


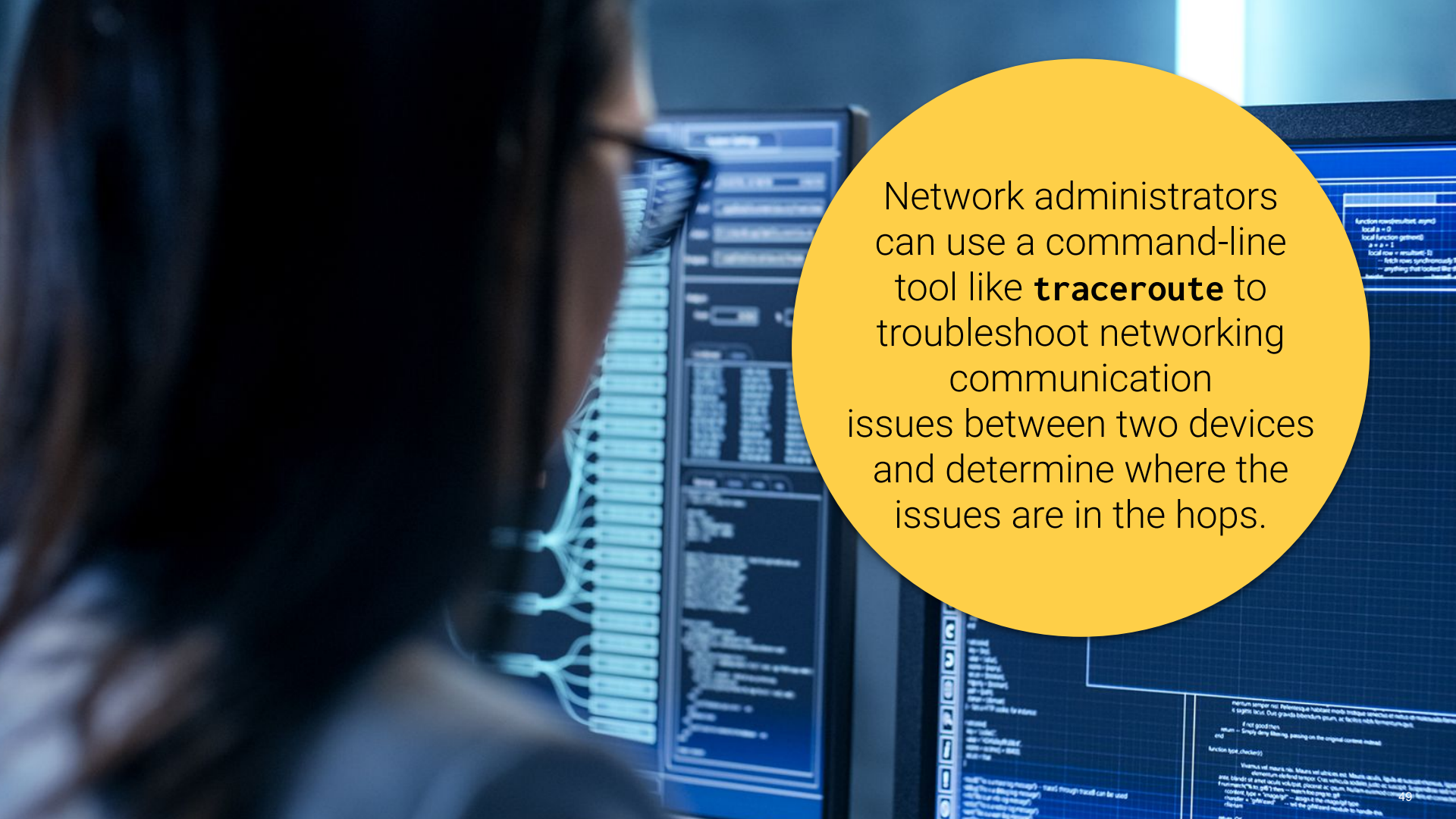
- Data is often redirected by many routers. Routers connect different networks so their hosts can communicate.
- Redirection of data transmissions are called **hops**.
- Optimal routing paths are determined based on the “shortest path,” which is influenced by network topology.

Routing and Redirections

Despite using the “shortest path,” communication between two devices can sometimes fail, leaving network administrators unsure where a communication problem is located.

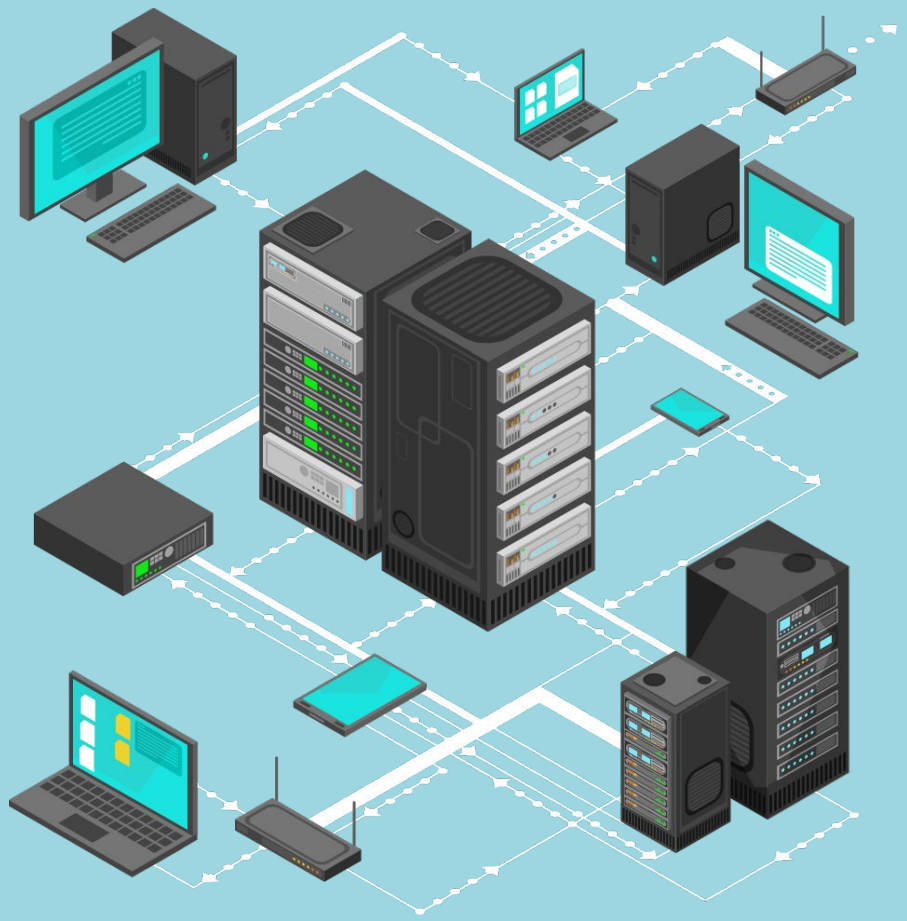
Poor connectivity and latency issues are often due to packets being dropped along their routing paths.




Network administrators can use a command-line tool like **traceroute** to troubleshoot networking communication issues between two devices and determine where the issues are in the hops.

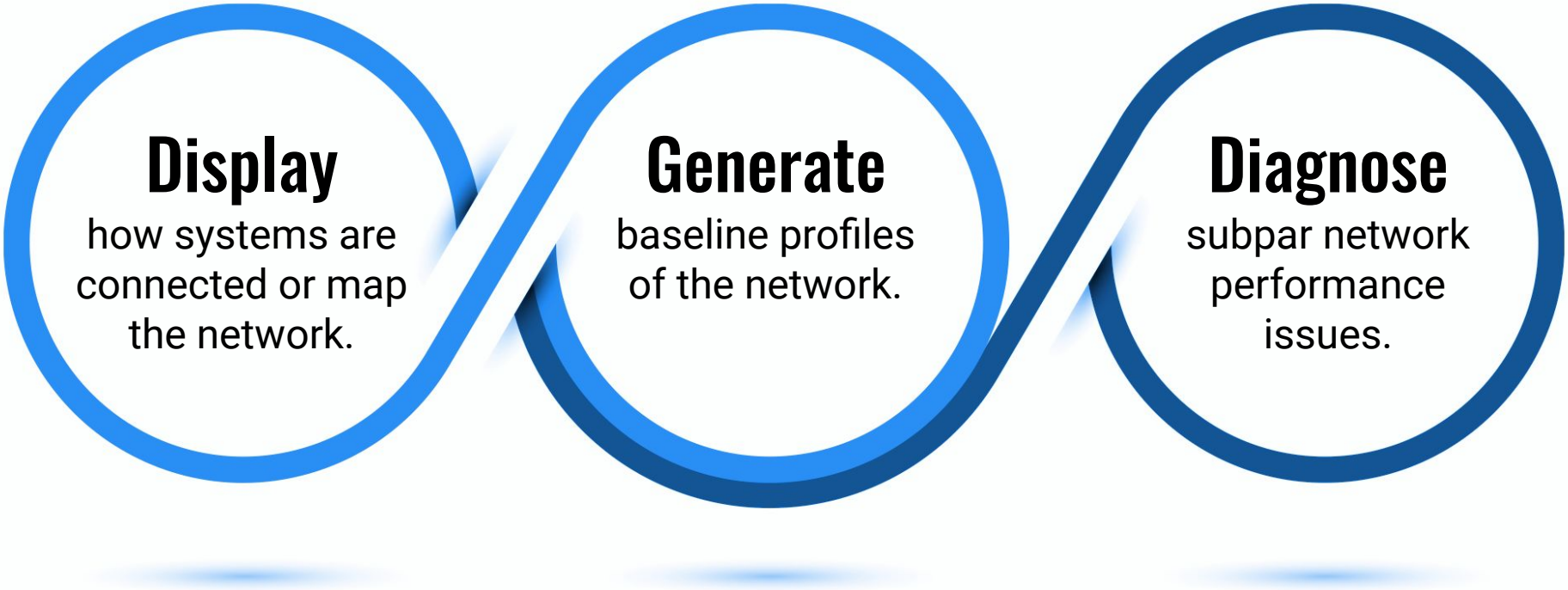
Introduction to `traceroute`

- **`traceroute`** shows the route taken between two systems across a network.
- It lists all routers (hops) the connection must pass through to get to the destination.
- Network administrators can use **`traceroute`** to identify precisely where connectivity problems occur.



`traceroute` Uses

In addition to troubleshooting connectivity issues, **`traceroute`** can be used to:



ICMP and Time to Live (TTL)

Like `ping`, `traceroute` also uses the ICMP protocol. It also shows the time taken to travel across each of these hops from source to destination.

The ICMP header contains a field called **TTL**.

TTL indicates how long a data packet can exist in a network.

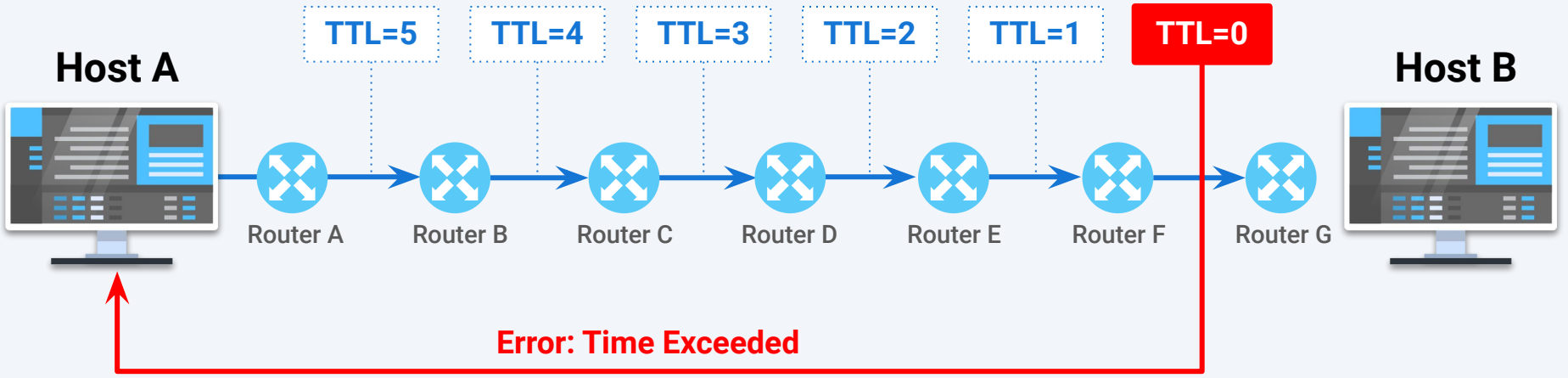
TTL is utilized as a decrementing hop counter.

Every router that forwards the packet decrements (reduces) the TTL value by one.

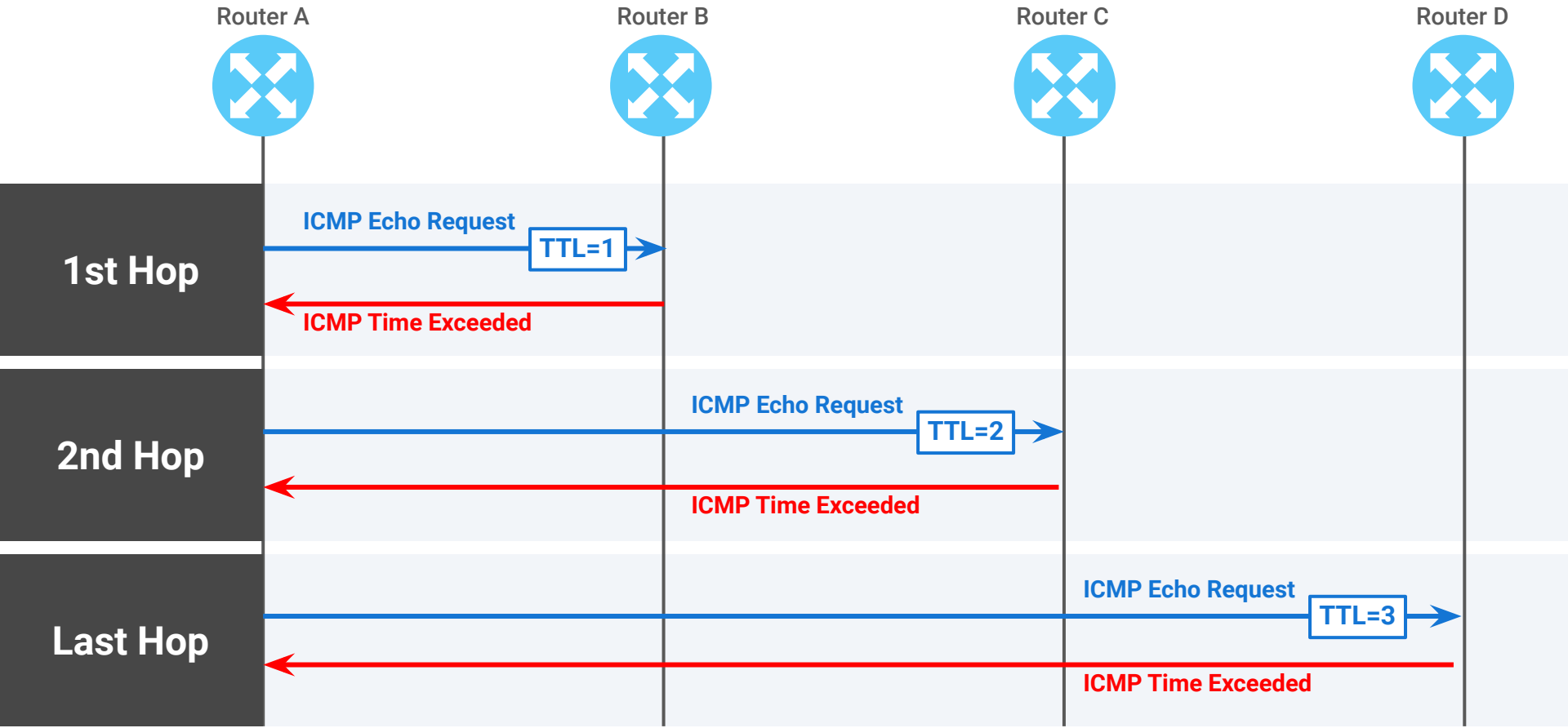
TTL

If the starting TTL value of a data packet is five and the data travels across two routers, the TTL will drop to three.

When the TTL count reaches zero, it sends a time exceeded error message back to the source address. This prevents data from being stuck in an infinite loop if it cannot be delivered to the destination.



User Datagram Protocol (UDP) Datagrams



Next, we'll use `traceroute` on the command line to further investigate why redbull.com isn't responding.

Instructor Demonstration

`traceroute`

[Optional] Activity: Enumerate with `traceroute`

In this activity, you will continue to play the role of a security analyst at Acme Corp.

You've been tasked with further analyzing the IPs rejected in the last activity to determine where in their path the connection is being dropped.

Suggested Time:

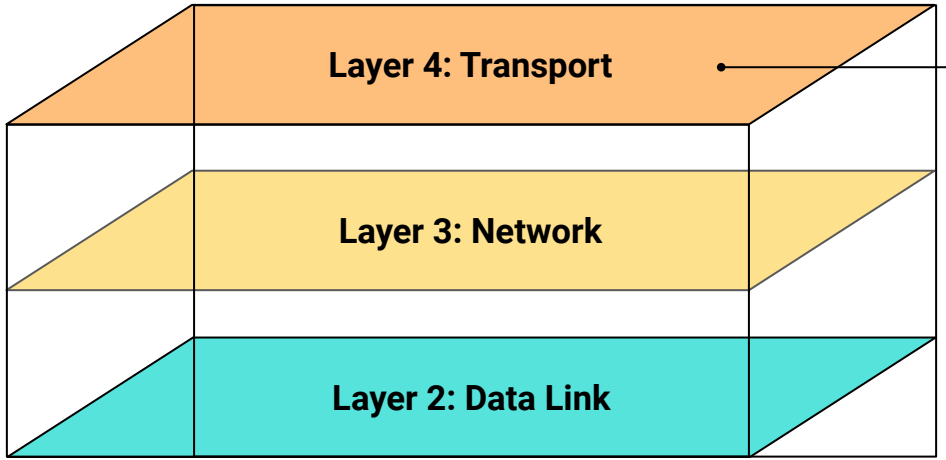
Complete if class falls on a Saturday

Time's Up! Let's Review.

Questions?

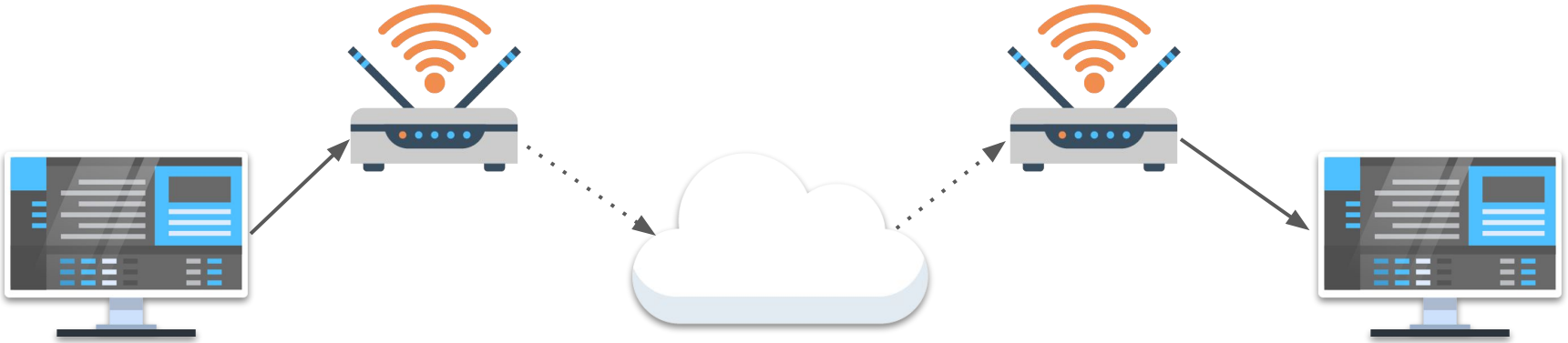
Checkpoint

So far, we've studied the ARP on Layer 2 and the `ping` and `traceroute` utilities from Layer 3.



Now, we'll move onto Layer 4 protocols TCP and UDP.

Layer 4: Transport



The **transport** layer is responsible for end-to-end communication over a network.

The data from the above layers is broken into **smaller packets** and transported to the destination.

The recipient **reassembles** these packets into a complete message.

TCP

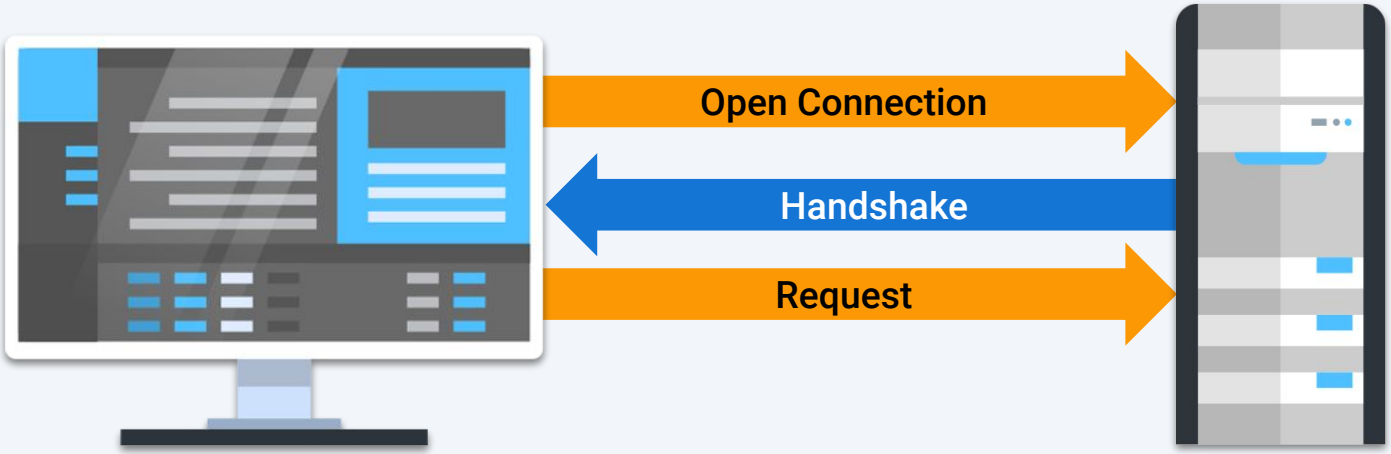
TCP (Transmission Control Protocol) is one of the most widely used protocols for data transmission.

- It is a “connection-oriented” protocol, meaning the server must acknowledge it has received the request from the client.
- If the recipient doesn’t acknowledge the request, the sender assumes the request has not been received and will attempt to resend.
- This connection-oriented acknowledgment is known as the **TCP handshake.**

TCP in the Real World

TCP also ensures that all data is transmitted without errors in the correct order.

TCP is used with familiar protocols such as HTTP, HTTPS, FTP, SSH, and SMTP.



TCP in the Real World

For example:

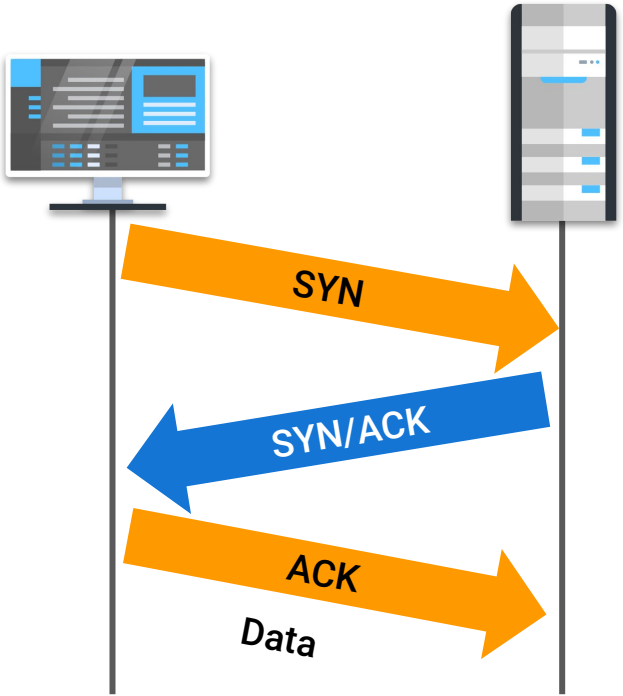
We want to check our transaction history on an online banking website.

- We would use HTTPS, a protocol that runs over TCP. It ensures that all the requested data from our banking transaction history has been transmitted from the bank's web server.
- Banking customers need to trust the integrity of the data they are viewing. It's critical that banking data is complete and error-free.

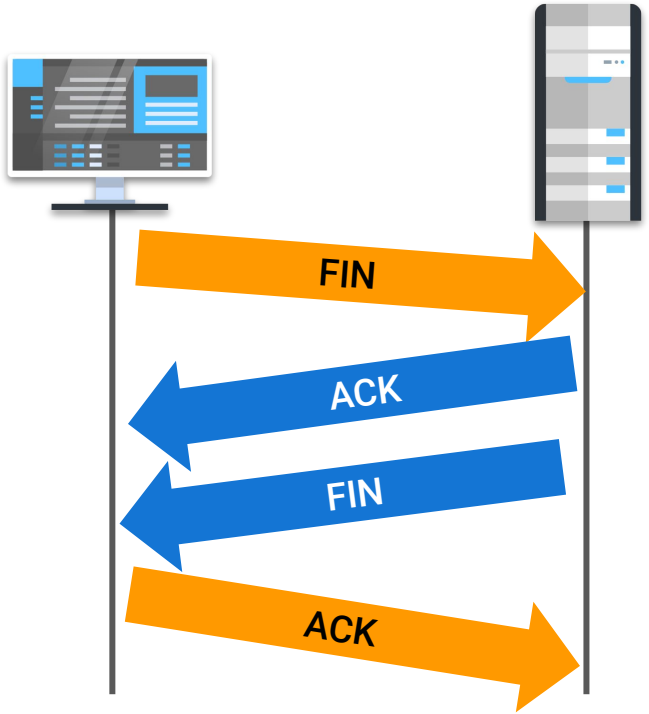
The **TCP three-way handshake** is the process of establishing a reliable connection to transmit data between devices.

Three-way Handshake

Setup:
SYN, SYN/ACK, ACK

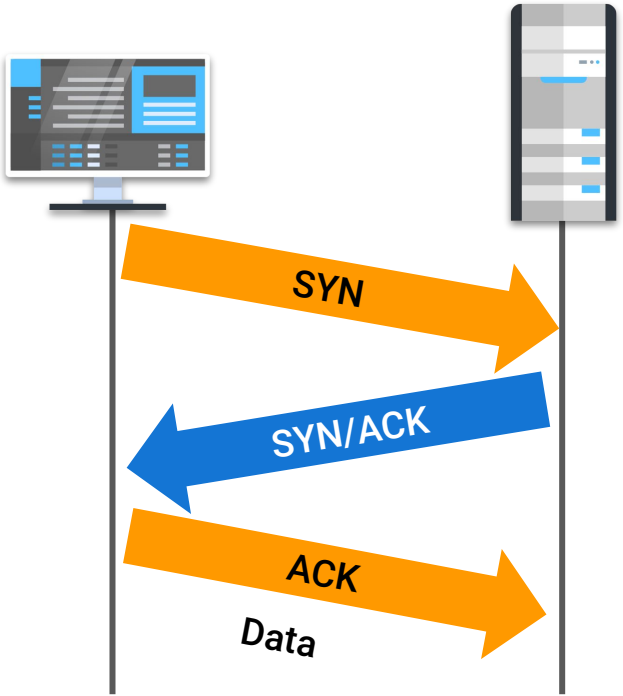


Termination:
FIN, ACK, FIN, ACK



Three-way Handshake: Step by Step

Setup:
SYN, SYN/ACK, ACK



SYN (*synchronize*):

From client to server

Client sends a SYN data packet to the server to determine if it is ready to open a connection.

SYN/ACK (*synchronize/acknowledge*):

From server to client

The server acknowledges or confirms receipt of the SYN packet.

ACK (*acknowledge*):

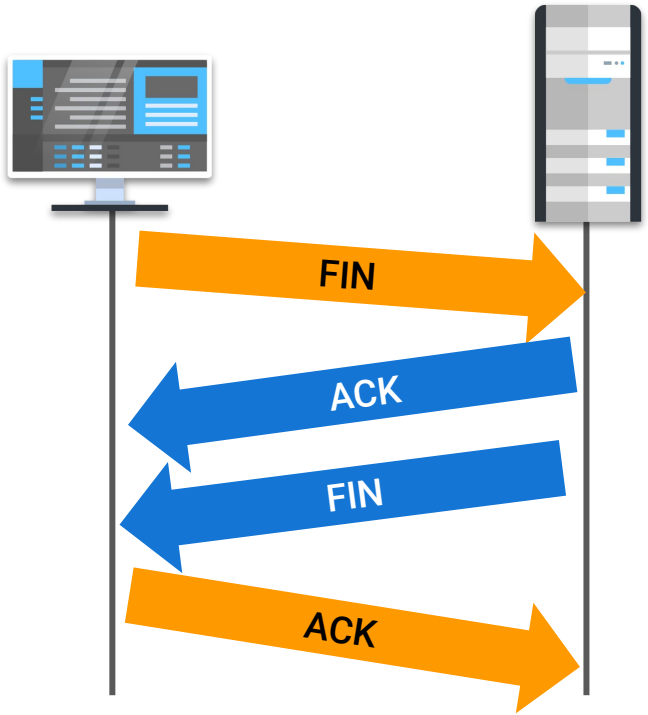
From client to server

Client confirms receipt of the SYN/ACK packet.

Once the handshake is successfully completed, the data transmission can begin.

Three-way Handshake: Step by Step

Termination:
FIN, ACK, FIN, ACK



FIN (*finish*):

From client to server
The client sends a FIN data packet to the server to close the connection.

ACK:

From server to client
The server acknowledges receipt of the FIN packet.

FIN:

From server to client
After the server terminates the connection, it sends a FIN packet.

ACK:

From client to server
The client acknowledges it has received the server's FIN packet. The TCP termination process is complete.

TCP Downsides

TCP also has disadvantages.

Retransmissions (when the server resends packets because the client does not acknowledge receipt) and the ordering of packets can cause delays during data transmissions.

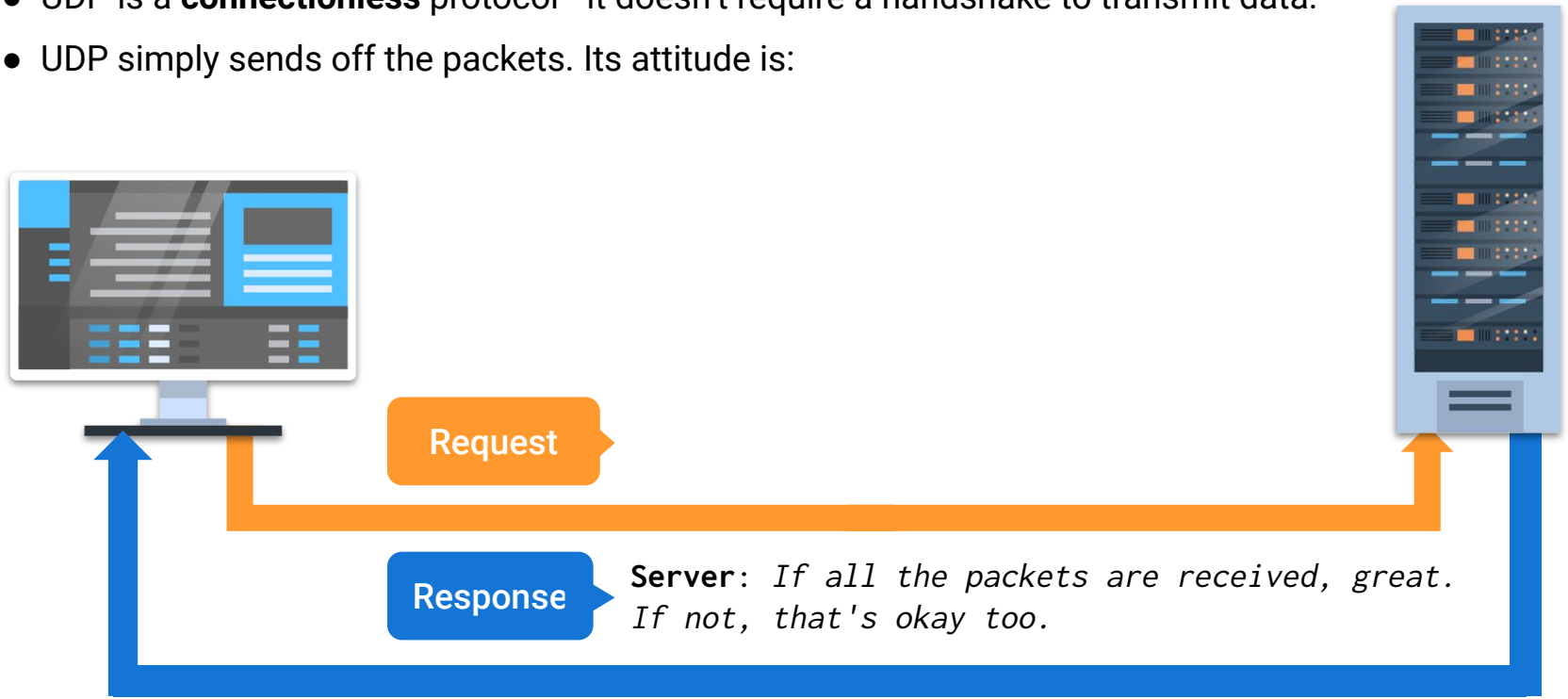
In cases when every single packet of data does not need to be transmitted, TCP is not used. For example, streaming live video.

For situations when it’s not necessary for all data to reach the destination, there is the **User Datagram Protocol (UDP)**.

UDP

UDP is better for reducing latency versus transmitting all data.

- UDP is a **connectionless** protocol—it doesn't require a handshake to transmit data.
- UDP simply sends off the packets. Its attitude is:



Instructor Demonstration

TCP

Time's Up! Let's Review.

Questions?

Introduction to SYN Scan

In the previous lesson, we discussed that ports are like the “doors” to a network.

It’s critical for security professionals to be sure that these doors are not open to unauthorized users.

Activity: Analyze TCP Traffic

In this activity, you will continue to play the role of a security analyst at Acme Corp.

Your task is to analyze a new employee's TCP traffic to determine what they worked on in their first week.

Suggested Time:

15 Minutes

Ports

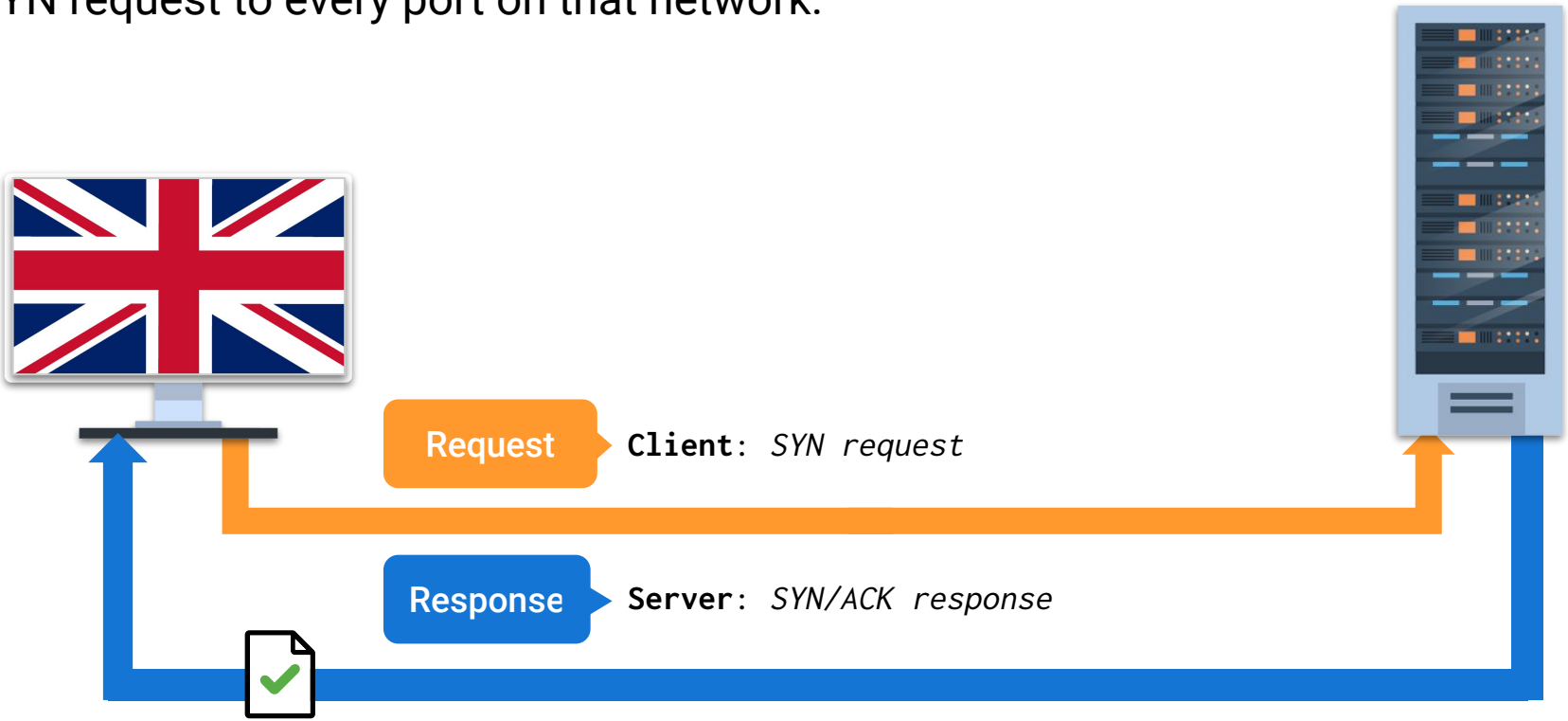
Consider the following scenario:

- Company X recently set up a new network in its London office.
- A security administrator needs to ensure the only ports open on the machines are 80 (HTTP) and 443 (HTTPS), since incoming and outgoing web traffic is allowed for their employees.
- If ports other than HTTP and HTTPS are open, there's a risk an attacker could access the network and view confidential info or impact the availability of the network.

Ports

We can check for open ports on a network by sending a SYN request to every port on that network.

If we receive a SYN/ACK response, we know the port is open.



Introduction to SYN Scan

This enumeration process of sending SYN requests to many ports on a network is called a SYN scan.

A SYN scan is typically run by a software program that automates the sending of the SYN requests.

If a server responds with a SYN/ACK response, the client will not complete the three-way handshake with an ACK response.

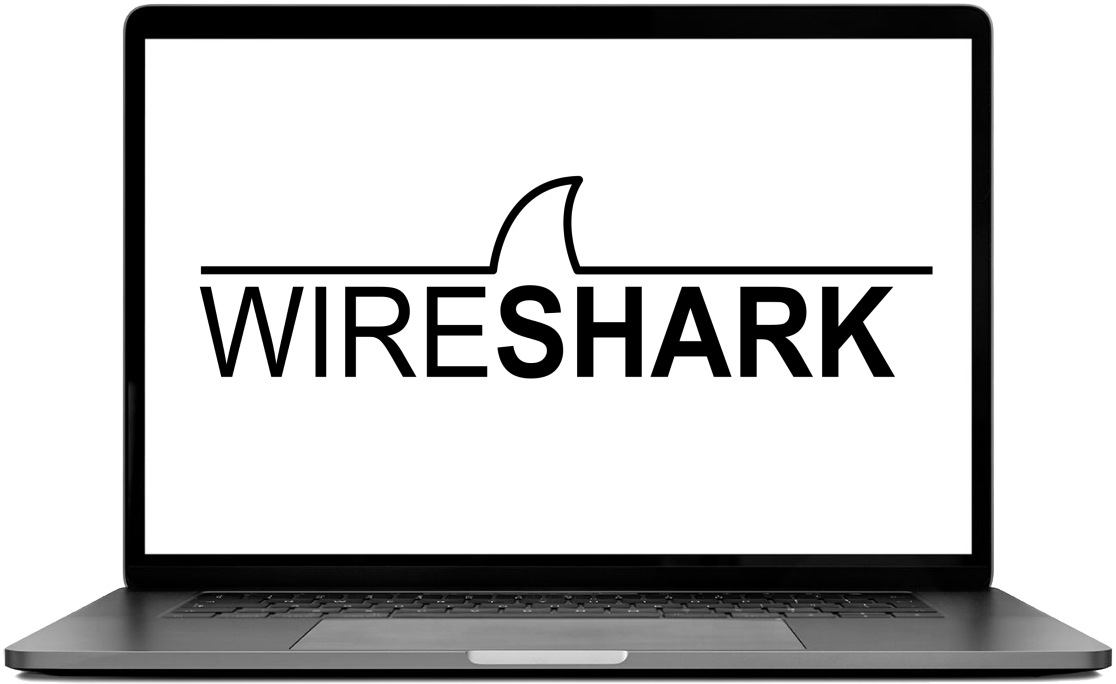
The purpose of the SYN scan is to determine the states of the ports on a network.

Port States

There are three main port states:

Open	The port is accepting connections.
Closed	The port is not accepting connections.
Filtered	The port may be open, but a firewall or another network device is likely blocking it.

We can use Wireshark to display request and response conversations in order to determine if ports are open, closed, or filtered.



SYN Scan Demo

In the upcoming demonstration:

- As security analysts at Company X, we have to analyze the ports from the machine recently set up in London.
- Company X is concerned that the networking team left ports open, putting the company at risk of unauthorized access.
- The security manager ran a SYN scan against the machine.
- We'll analyze the results to see which open ports put the company at risk.

Instructor Demonstration

SYN Scan

SYN Scan Demo Summary

All of the SYN requests going from port to port was expected. We knew a SYN scan had been run by the security manager.

If a SYN scan wasn’t planned, it is unusual network activity that should be looked into.

If a security professional saw this activity, they’d consider using a firewall to block the source IP from scanning the network.

An attacker can use the same SYN scan process for malicious reasons.

Activity: Analyze a SYN Scan

CompuCom hires you to do a security assessment of Its network.

You will analyze a packet capture of a SYN scan CompuCom ran against one of its hosts. You must determine what ports are open, closed, and filtered.

Suggested Time:

12 Minutes

Time's Up! Let's Review.

Questions?


The End