getting started & introduction to networks

- Introduction to Course 3 + course 3 overview
- Glossary Cybersecurity
- Welcome to week 1
- Chris: My path to cybersecurity
- What are networks?
- Tina: Working in network security
- Emmanuel: Useful skills for network security
- tech enthusiest reminder
- Network tools
- Network components, devices, and diagrams
- Cloud networks
- Cloud networks

Introduction to Course 3 + course 3 overview

Introduction

You've learned about security domains in previous courses.
Now we'll explore one of those domains further: networks.
It's important to secure networks because network-based attacks are growing in both frequency and complexity.

Hi there! My name is Chris, and I'm the Chief Information Security Officer for Google Fiber.
I'm excited to be your instructor for this course!
I've been working in network security and engineering for over 20 years, and I'm looking forward to sharing some of my knowledge and experience with you.

This course will help you understand the basic structure of a network (also referred to as network architecture) and commonly used network tools.
You'll also learn about network operations and explore some basic network protocols.
Next, you'll learn about common network attacks and how network intrusion tactics can prevent a threat to a network.
Finally, the course will provide an overview of security hardening practices and how you might use them to help secure a network.

There's a lot to learn in securing networks, and I'm excited to go on this journey with you.
Ready to get started?
Let's go!

Course 3 overview

Course 3 welcome banner

Hello and welcome to **Connect and Protect: Networks and Network Security**, the third course in the Google Cybersecurity Certificate. You’re on an exciting journey!

By the end of this course, you will develop a greater understanding of network architecture, operations, intrusion tactics, common types of network vulnerabilities and attacks, and how to secure networks. You'll also be introduced to common network protocols, firewalls, virtual private networks (VPNs), and system hardening practices.

Certificate program progress

The Google Cybersecurity Certificate program has eight courses. **Connect and Protect: Networks and Network Security** is the third course.

The titles of each of the eight courses with course three highlighted

1. **Foundations of Cybersecurity**

- — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.
- **Play It Safe: Manage Security Risks**
- — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.
- **Connect and Protect: Networks and Network Security**
- — *(current course)* Gain an understanding of network-level vulnerabilities and how to secure networks.
- **Tools of the Trade: Linux and SQL**
- — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.
- **Assets, Threats, and Vulnerabilities**
- — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.
- **Sound the Alarm: Detection and Response**
- — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.
- **Automate Cybersecurity Tasks with Python**
- — Explore the Python programming language and write code to automate cybersecurity tasks.
- **Put It to Work: Prepare for Cybersecurity Jobs**

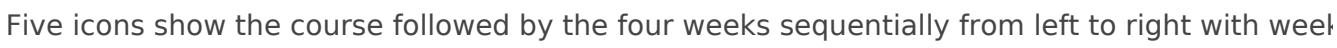
1. — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

Course 3 content

Each course of this certificate program is broken into weeks. You can complete courses at your own pace, but the weekly breakdowns are designed to help you finish the entire Google Cybersecurity Certificate in about six months.

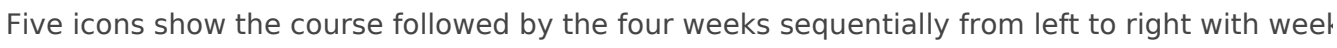
What’s to come? Here’s a quick overview of the skills you’ll learn in each week of this course.

Week 1: Network architecture



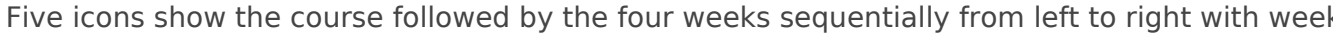
You'll be introduced to network security and explain how it relates to ongoing security threats and vulnerabilities. You will learn about network architecture and mechanisms to secure a network.

Week 2: Network operations



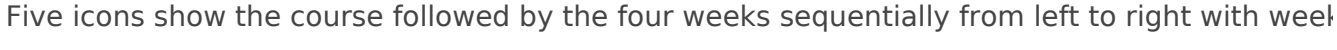
You will explore network protocols and how network communication can introduce vulnerabilities. In addition, you'll learn about common security measures, like firewalls, that help network operations remain safe and reliable.

Week 3: Secure against network intrusions



You will understand types of network attacks and techniques used to secure compromised network systems and devices. You'll explore the many ways that malicious actors exploit vulnerabilities in network infrastructure and how cybersecurity professionals identify and close potential loopholes.

Week 4: Security hardening



You will become familiar with network hardening practices that strengthen network systems. You'll learn how security hardening helps defend against malicious actors and intrusion methods. You'll also learn how to use security hardening to address the unique security challenges posed by cloud infrastructures.

What to expect

Each course offers many types of learning opportunities:

- **Videos** led by Google instructors teach new concepts, introduce the use of relevant tools, offer career support, and provide inspirational personal stories.
- **Readings** build on the topics discussed in the videos, introduce related concepts, share useful resources, and describe case studies.
- **Discussion prompts** explore course topics for better understanding and allow you to chat and exchange ideas with other learners in the **discussion forums**

- .
- **Self-review activities** and **labs** give you hands-on practice in applying the skills you are learning and allow you to assess your own work by comparing it to a completed example.
- **Interactive plug-ins** encourage you to practice specific tasks and help you integrate knowledge you have gained in the course.
- **In-video quizzes** help you check your comprehension as you progress through each video.
- **Practice quizzes** allow you to check your understanding of key concepts and provide valuable feedback.
- **Graded quizzes** demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate, and you can take a graded quiz multiple times to achieve a passing score.

Tips for success

- It is strongly recommended that you go through the items in each lesson in the order they appear because new information and concepts build on previous knowledge.
- Participate in all learning opportunities to gain as much knowledge and experience as possible.
- If something is confusing, don’t hesitate to replay a video, review a reading, or repeat a self-review activity.
- Use the additional resources that are referenced in this course. They are designed to support your learning. You can find all of these resources in the **Resources**
- tab.
- When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review.
- Understand and follow the Coursera Code of Conduct

- to ensure that the learning community remains a welcoming, friendly, and supportive

place for all members.

Helpful resources and tips

As a learner, you can choose to complete one or multiple courses in this program. However, to obtain the Google Cybersecurity Certificate, you must complete all the courses. This reading describes what is required to obtain a certificate and best practices for you to have a good learning experience on Coursera.

Course completion to obtain a certificate

To submit graded assignments and be eligible to receive a Google Cybersecurity Certificate, you must:

- Pay the course certificate fee or apply and be approved for a Coursera scholarship.
- Pass all graded quizzes in the eight courses with a score of at least 80%. Each graded quiz in a course is part of a cumulative grade for that course.

Healthy habits for course completion

Here is a list of best practices that will help you complete the courses in the program in a timely manner:

- **Plan your time:** Setting regular study times and following them each week can help you make learning a part of your routine. Use a calendar or timetable to create a schedule, and list what you plan to do each day in order to set achievable goals. Find a space that allows you to focus when you watch the videos, review the readings, and complete the activities.
- **Work at your own pace:** Everyone learns differently, so this program has been designed to let you work at your own pace. Although your personalized deadlines start when you enroll, feel free to move through the program at the speed that works best for you. There is no penalty for late assignments; to earn your certificate, all you have to do is complete all of the

work. You can extend your deadlines at any time by going to **Overview** in the navigation panel and selecting **Switch Sessions**. If you have already missed previous deadlines, select **Reset my deadlines** instead.

- **Be curious:** If you find an idea that gets you excited, act on it! Ask questions, search for more details online, explore the links that interest you, and take notes on your discoveries. The steps you take to support your learning along the way will advance your knowledge, create more opportunities in this high-growth field, and help you qualify for jobs.

- **Take notes:** Notes will help you remember important information in the future, especially as you're preparing to enter a new job field. In addition, taking notes is an effective way to make connections between topics and gain a better understanding of those topics.

- **Review exemplars:** Exemplars are completed assignments that fully meet an activity's criteria. Many activities in this program have exemplars for you to validate your work or check for errors. Although there are often many ways to complete an assignment, exemplars offer guidance and inspiration about how to complete the activity.

- **Chat (responsibly) with other learners:** If you have a question, chances are, you're not alone. Use the discussion forums to ask for help from other learners taking this program. You can also visit Coursera's Global Online Community. Other important things to know while learning with others can be found in the Coursera Honor Code and Code of Conduct.

- **Update your profile:** Consider updating your profile on Coursera. When other learners find you in the discussion forums, they can click on your name to access your profile and get to know you better.

Documents, spreadsheets, presentations, and labs for course activities

To complete certain activities in the program, you will need to use digital documents, spreadsheets, presentations, and/or labs. Security professionals use these software tools to collaborate within their teams and organizations. If you need more information about using a particular tool, refer to these resources:

- Microsoft Word: Help and learning: Microsoft Support page for Word
- Google Docs: Help Center page for Google Docs
- Microsoft Excel: Help and learning: Microsoft Support page for Excel
- Google Sheets: Help Center page for Google Sheets
- Microsoft PowerPoint: Help and learning: Microsoft Support page for PowerPoint
- How to use Google Slides: Help Center page for Google Slides
- Common problems with labs: Troubleshooting help for Qwiklabs activities

Weekly, course, and certificate glossaries

This program covers a lot of terms and concepts, some of which you may already know and some of which may be unfamiliar to you. To review terms and help you prepare for graded quizzes, refer to the following glossaries:

- **Weekly glossaries**: At the end of each week's content, you can review a glossary of terms from that week. Each week's glossary builds upon the terms from the previous weeks in that course. The weekly glossaries are not downloadable; however, all of the terms and definitions are included in the course and certificate glossaries, which are downloadable.
- **Course glossaries**: At the end of each course, you can access and download a glossary that covers all of the terms in that course.
-

Certificate glossary: The certificate glossary includes all of the terms in the entire certificate program and is a helpful resource that you can reference throughout the program or at any time in the future.

You can access and download the certificate glossaries and save them on your computer.

You can always find the course and certificate glossaries through the course's Resources section. To access the **Cybersecurity Certificate glossary**, click the link below and select *Use Template*.

- Cybersecurity Certificate glossary

OR

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

Google Cybersecurity Certificate glossary
DOCX File

Course feedback

Providing feedback on videos, readings, and other materials is easy. With the resource open in your browser, you can find the thumbs-up and thumbs-down symbols.

- Click **thumbs-up** for materials that are helpful.
-

Click **thumbs-down** for materials that are not helpful.

If you want to flag a specific issue with an item, click the flag icon, select a category, and enter an explanation in the text box. This feedback goes back to the course development team and isn’t visible to other learners. All feedback received helps to create even better certificate programs in the future.

For technical help, visit the Learner Help Center.

Glossary Cybersecurity

Terms and definitions from the certificate

A

Absolute file path: The full file path, which starts from the root

Access controls: Security controls that manage access, authorization, and accountability of information

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

Address Resolution Protocol (ARP): A network protocol used to determine the MAC address of the next router or device on the path

Advanced persistent threat (APT): An instance when a threat actor maintains unauthorized access to a system for an extended period of time

Adversarial artificial intelligence (AI): A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently

Adware: A type of legitimate software that is sometimes used to display digital advertisements in applications

Algorithm: A set of rules used to solve a problem

Analysis: The investigation and validation of alerts

Angler phishing: A technique where attackers impersonate customer service representatives on social media

Anomaly-based analysis: A detection method that identifies abnormal behavior

Antivirus software: A software program used to prevent, detect, and eliminate malware and viruses

Application: A program that performs a specific task

Application programming interface (API) token: A small block of encrypted code that contains information about a user

Argument (Linux): Specific information needed by a command

Argument (Python): The data brought into a function when it is called

Array: A data type that stores data in a comma-separated ordered list

Assess: The fifth step of the NIST RMF that means to determine if established controls are implemented correctly

Asset: An item perceived as having value to an organization

Asset classification: The practice of labeling assets based on sensitivity and importance to an organization

Asset inventory: A catalog of assets that need to be protected

Asset management: The process of tracking assets and the risks that affect them

Asymmetric encryption: The use of a public and private key pair for encryption and decryption of data

Attack surface: All the potential vulnerabilities that a threat actor could exploit

Attack tree: A diagram that maps threats to assets

Attack vectors: The pathways attackers use to penetrate security defenses

Authentication: The process of verifying who someone is
Authorization: The concept of granting access to specific resources in a system
Authorize: The sixth step of the NIST RMF that refers to being accountable for the security and privacy risks that might exist in an organization
Automation: The use of technology to reduce human and manual effort to perform common and repetitive tasks
Availability: The idea that data is accessible to those who are authorized to access it

B
Baiting: A social engineering tactic that tempts people into compromising their security
Bandwidth: The maximum data transmission capacity over a network, measured by bits per second
Baseline configuration (baseline image): A documented set of specifications within a system that is used as a basis for future builds, releases, and updates
Bash: The default shell in most Linux distributions
Basic auth: The technology used to establish a user’s request to access a server
Basic Input/Output System (BIOS): A microchip that contains loading instructions for the computer and is prevalent in older systems
Biometrics: The unique physical characteristics that can be used to verify a person’s identity
Bit: The smallest unit of data measurement on a computer
Boolean data: Data that can only be one of two values: either True or False
Bootloader: A software program that boots the operating system
Botnet: A collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder"
Bracket notation: The indices placed in square brackets
Broken chain of custody: Inconsistencies in the collection and logging of evidence in the chain of custody
Brute force attack: The trial and error process of discovering private information
Bug bounty: Programs that encourage freelance hackers to find and report vulnerabilities
Built-in function: A function that exists within Python and can be called directly

Business continuity: An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans
Business continuity plan (BCP): A document that outlines the procedures to sustain business operations during and after a significant disruption
Business Email Compromise (BEC): A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage
C
Categorize: The second step of the NIST RMF that is used to develop risk management processes and tasks
CentOS: An open-source distribution that is closely related to Red Hat
Central Processing Unit (CPU): A computer’s main processor, which is used to perform general computing tasks on a computer

Chain of custody: The process of documenting evidence possession and control during an incident lifecycle
Chronicle: A cloud-native tool designed to retain, analyze, and search data
Cipher: An algorithm that encrypts information
Cloud-based firewalls: Software firewalls that are hosted by the cloud service provider
Cloud computing: The practice of using remote servers, applications, 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
Cloud security: The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorized users
Command: An instruction telling the computer to do something
Command and control (C2): The techniques used by malicious actors to maintain communications with compromised systems

Command-line interface (CLI): A text-based user interface that uses commands to interact with the computer
Comment: A note programmers make about the intention behind their code
Common Event Format (CEF): A log format that uses key-value pairs to structure data and identify fields and their corresponding values
Common Vulnerabilities and Exposures (CVE®) list: An openly accessible dictionary of known vulnerabilities and exposures
Common Vulnerability Scoring System (CVSS): A measurement system that scores the severity of a vulnerability
Compliance: The process of adhering to internal standards and external regulations
Computer security incident response teams (CSIRT): A specialized group of security professionals that are trained in incident management and response
Computer virus: Malicious code written to interfere with computer operations and cause damage to data and software
Conditional statement: A statement that evaluates code to determine if it meets a specified set of conditions
Confidentiality: The idea that only authorized users can access specific assets or data
Confidential data: Data that often has limits on the number of people who have access to it
Confidentiality, integrity, availability (CIA) triad: A model that helps inform how organizations consider risk when setting up systems and security policies
Configuration file: A file used to configure the settings of an application
Containment: The act of limiting and preventing additional damage caused by an incident
Controlled zone: A subnet that protects the internal network from the uncontrolled zone
Cross-site scripting (XSS): An injection attack that inserts code into a vulnerable website or web application

Crowdsourcing: The practice of gathering information using public input and collaboration
Cryptographic attack: An attack that affects secure forms of communication between a sender and intended recipient
Cryptographic key: A mechanism that decrypts ciphertext
Cryptography: The process of transforming information into a form that unintended readers can’t understand
Cryptojacking: A form of malware that installs software to illegally mine cryptocurrencies
CVE Numbering Authority (CNA): An organization that volunteers to analyze and distribute information on eligible CVEs
Cybersecurity (or security): The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation
D
Data: Information that is translated, processed, or stored by a computer
Data at rest: Data not currently being accessed
Database: An organized collection of information or data
Data controller: A person that determines the procedure and purpose for processing data
Data custodian: Anyone or anything that’s responsible for the safe handling, transport, and storage of information
Data exfiltration: Unauthorized transmission of data from a system
Data in transit: Data traveling from one point to another
Data in use: Data being accessed by one or more users
Data owner: The person who decides who can access, edit, use, or destroy their information

Data packet: A basic unit of information that travels from one device to another within a network
Data point: A specific piece of information
Data processor: A person that is responsible for processing data on behalf of the data controller
Data protection officer (DPO): An individual that is responsible for monitoring the compliance of an organization's data protection procedures
Data type: A category for a particular type of data item
Date and time data: Data representing a date and/or time
Debugger: A software tool that helps to locate the source of an error and assess its causes
Debugging: The practice of identifying and fixing errors in code
Defense in depth: A layered approach to vulnerability management that reduces risk
Denial of service (DoS) attack: An attack that targets a network or server and floods it with network traffic
Detect: A NIST core function related to identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections
Detection: The prompt discovery of security events

Dictionary data: Data that consists of one or more key-value pairs
Digital certificate: A file that verifies the identity of a public key holder
Digital forensics: The practice of collecting and analyzing data to determine what has happened after an attack
Directory: A file that organizes where other files are stored
Disaster recovery plan: A plan that allows an organization’s security team to outline the steps needed to minimize the impact of a security incident

Distributed denial of service (DDoS) attack: A type of denial or service attack that uses multiple devices or servers located in different locations to flood the target network with unwanted traffic
Distributions: The different versions of Linux
Documentation: Any form of recorded content that is used for a specific purpose
DOM-based XSS attack: An instance when malicious script exists in the webpage a browser loads
Domain Name System (DNS): A networking protocol that translates internet domain names into IP addresses
Dropper: A type of malware that comes packed with malicious code which is delivered and installed onto a target system
E
Elevator pitch: A brief summary of your experience, skills, and background
Encapsulation: A process performed by a VPN service that protects your data by wrapping sensitive data in other data packets
Encryption: The process of converting data from a readable format to an encoded format
Endpoint: Any device connected on a network
Endpoint detection and response (EDR): An application that monitors an endpoint for malicious activity
Eradication: The complete removal of the incident elements from all affected systems
Escalation policy: A set of actions that outline who should be notified when an incident alert occurs and how that incident should be handled
Event: An observable occurrence on a network, system, or device
Exception: An error that involves code that cannot be executed even though it is syntactically correct
Exclusive operator: An operator that does not include the value of comparison

Exploit: A way of taking advantage of a vulnerability
Exposure: A mistake that can be exploited by a threat
External threat: Anything outside the organization that has the potential to harm organizational assets
F
False negative: A state where the presence of a threat is not detected
False positive: An alert that incorrectly detects the presence of a threat
Fileless malware: Malware that does not need to be installed by the user because it uses legitimate programs that are already installed to infect a computer
File path: The location of a file or directory

Filesystem Hierarchy Standard (FHS): The component of the Linux OS that organizes data
Filtering: Selecting data that match a certain condition
Final report: Documentation that provides a comprehensive review of an incident
Firewall: A network security device that monitors traffic to or from a network
Float data: Data consisting of a number with a decimal point
Foreign key: A column in a table that is a primary key in another table
Forward proxy server: A server that regulates and restricts a person’s access to the internet
Function: A section of code that can be reused in a program

G

Global variable: A variable that is available through the entire program
Graphical user interface (GUI): A user interface that uses icons on the screen to manage different tasks on the computer

H

Hacker: Any person who uses computers to gain access to computer systems, networks, or data
Hacktivist: A person who uses hacking to achieve a political goal
Hard drive: A hardware component used for long-term memory
Hardware: The physical components of a computer
Hash collision: An instance when different inputs produce the same hash value
Hash function: An algorithm that produces a code that can’t be decrypted
Hash table: A data structure that's used to store and reference hash values
Health Insurance Portability and Accountability Act (HIPAA): A U.S. federal law established to protect patients’ health information
Honeypot: A system or resource created as a decoy vulnerable to attacks with the purpose of attracting potential intruders
Host-based intrusion detection system (HIDS): An application that monitors the activity of the host on which it’s installed
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 website servers

I

Identify: A NIST core function related to management of cybersecurity risk and its effect on an organization’s people and assets
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

Immutable: An object that cannot be changed after it is created and assigned a value
Implement: The fourth step of the NIST RMF that means to implement security and privacy plans for an organization
Improper usage: An incident type that occurs when an employee of an organization

violates the organization’s acceptable use policies
Incident: An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies
Incident escalation: The process of identifying a potential security incident, triaging it, and handing it off to a more experienced team member
Incident handler’s journal: A form of documentation used in incident response
Incident response: An organization’s quick attempt to identify an attack, contain the damage, and correct the effects of a security breach
Incident response plan: A document that outlines the procedures to take in each step of incident response
Inclusive operator: An operator that includes the value of comparison
Indentation: Space added at the beginning of a line of code
Index: A number assigned to every element in a sequence that indicates its position
Indicators of attack (IoA): The series of observed events that indicate a real-time incident
Indicators of compromise (IoC): Observable evidence that suggests signs of a potential security incident
Information privacy: The protection of unauthorized access and distribution of data
Information security (InfoSec): The practice of keeping data in all states away from unauthorized users
Injection attack: Malicious code inserted into a vulnerable application
Input validation: Programming that validates inputs from users and other programs

Integer data: Data consisting of a number that does not include a decimal point
Integrated development environment (IDE): A software application for writing code that provides editing assistance and error correction tools
Integrity: The idea that the data is correct, authentic, and reliable
Internal hardware: The components required to run the computer
Internal threat: A current or former employee, external vendor, or trusted partner who poses a security risk
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 flood (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
Interpreter: A computer program that translates Python code into runnable instructions line by line
Intrusion detection system (IDS): An application that monitors system activity and alerts on possible intrusions
Intrusion prevention system (IPS): An application that monitors system activity for

intrusive activity and takes action to stop the activity
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
Iterative statement: Code that repeatedly executes a set of instructions
K

KALI LINUX TM: An open-source distribution of Linux that is widely used in the security industry
Kernel: The component of the Linux OS that manages processes and memory
Key-value pair: A set of data that represents two linked items: a key, and its corresponding value
L
Legacy operating system: An operating system that is outdated but still being used
Lessons learned meeting: A meeting that includes all involved parties after a major incident
Library: A collection of modules that provide code users can access in their programs
Linux: An open-source operating system
List concatenation: The concept of combining two lists into one by placing the elements of the second list directly after the elements of the first list
List data: Data structure that consists of a collection of data in sequential form
Loader: A type of malware that downloads strains of malicious code from an external source and installs them onto a target system
Local Area Network (LAN): A network that spans small areas like an office building, a school, or a home
Local variable: A variable assigned within a function
Log: A record of events that occur within an organization’s systems
Log analysis: The process of examining logs to identify events of interest
Logging: The recording of events occurring on computer systems and networks
Logic error: An error that results when the logic used in code produces unintended results
Log management: The process of collecting, storing, analyzing, and disposing of log data

Loop condition: The part of a loop that determines when the loop terminates
Loop variable: A variable that is used to control the iterations of a loop
M
Malware: Software designed to harm devices or networks
Malware infection: An incident type that occurs when malicious software designed to disrupt a system infiltrates an organization’s computers or network
Media Access Control (MAC) address: A unique alphanumeric identifier that is assigned to each physical device on a network
Method: A function that belongs to a specific data type
Metrics: Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application
MITRE: A collection of non-profit research and development centers
Modem: A device that connects your router to the internet and brings internet access

to the LAN
Module: A Python file that contains additional functions, variables, classes, and any kind of runnable code
Monitor: The seventh step of the NIST RMF that means be aware of how systems are operating
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
nano: A command-line file editor that is available by default in many Linux distributions
National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk
National Institute of Standards and Technology (NIST) Incident Response Lifecycle: A framework for incident response consisting of four phases: Preparation;

Detection and Analysis; Containment, Eradication and Recovery, and Post-incident activity
National Institute of Standards and Technology (NIST) Special Publication (S.P.) 800-53: A unified framework for protecting the security of information systems within the U.S. federal government
Network: A group of connected devices
Network-based intrusion detection system (NIDS): An application that collects and monitors network traffic and network data
Network data: The data that’s transmitted between devices on a network
Network Interface Card (NIC): Hardware that connects computers to a network
Network log analysis: The process of examining network logs to identify events of interest
Network protocol analyzer (packet sniffer): A tool designed to capture and analyze data traffic within a network
Network protocols: 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 security: The practice of keeping an organization's network infrastructure secure from unauthorized access
Network segmentation: A security technique that divides the network into segments
Network traffic: The amount of data that moves across a network
Non-repudiation: The concept that the authenticity of information can’t be denied
Notebook: An online interface for writing, storing, and running code
Numeric data: Data consisting of numbers
O
OAuth: An open-standard authorization protocol that shares designated access between applications

Object: A data type that stores data in a comma-separated list of key-value pairs
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
Open-source intelligence (OSINT): The collection and analysis of information from

publicly available sources to generate usable intelligence
Open systems interconnection (OSI) model: A standardized concept that describes the seven layers computers use to communicate and send data over the network
Open Web Application Security Project/Open Worldwide Application Security Project (OWASP): A non-profit organization focused on improving software security
Operating system (OS): The interface between computer hardware and the user
Operator: A symbol or keyword that represents an operation
Options: Input that modifies the behavior of a command
Order of volatility: A sequence outlining the order of data that must be preserved from first to last
OWASP Top 10: A globally recognized standard awareness document that lists the top 10 most critical security risks to web applications
P
Package: A piece of software that can be combined with other packages to form an application
Package manager: A tool that helps users install, manage, and remove packages or applications
Packet capture (P-cap): A file containing data packets intercepted from an interface or network
Packet sniffing: The practice of capturing and inspecting data packets across a network
Parameter (Python): An object that is included in a function definition for use in that function

Parrot: An open-source distribution that is commonly used for security
Parsing: The process of converting data into a more readable format
Passive packet sniffing: A type of attack where a malicious actor connects to a network hub and looks at all traffic on the network
Password attack: An attempt to access password secured devices, systems, networks, or data
Patch update: A software and operating system update that addresses security vulnerabilities within a program or product
Payment Card Industry Data Security Standards (PCI DSS): Any cardholder data that an organization accepts, transmits, or stores
Penetration test (pen test): A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes
PEP 8 style guide: A resource that provides stylistic guidelines for programmers working in Python
Peripheral devices: Hardware components that are attached and controlled by the computer system
Permissions: The type of access granted for a file or directory
Personally identifiable information (PII): Any information used to infer an individual's identity
Phishing: The use of digital communications to trick people into revealing sensitive data or deploying malicious software
Phishing kit: A collection of software tools needed to launch a phishing campaign

Physical attack: A security incident that affects not only digital but also physical environments where the incident is deployed
Physical social engineering: An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location
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
Playbook: A manual that provides details about any operational action

Policy: A set of rules that reduce risk and protect information
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
Post-incident activity: The process of reviewing an incident to identify areas for improvement during incident handling
Potentially unwanted application (PUA): A type of unwanted software that is bundled in with legitimate programs which might display ads, cause device slowdown, or install other software
Private data: Information that should be kept from the public
Prepare: The first step of the NIST RMF related to activities that are necessary to manage security and privacy risks before a breach occurs
Prepared statement: A coding technique that executes SQL statements before passing them on to a database
Primary key: A column where every row has a unique entry
Principle of least privilege: The concept of granting only the minimal access and authorization required to complete a task or function
Privacy protection: The act of safeguarding personal information from unauthorized use
Procedures: Step-by-step instructions to perform a specific security task
Process of Attack Simulation and Threat Analysis (PASTA): A popular threat modeling framework that’s used across many industries
Programming: A process that can be used to create a specific set of instructions for a computer to execute tasks
Protect: A NIST core function used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats

Protected health information (PHI): Information that relates to the past, present, or future physical or mental health or condition of an individual
Protecting and preserving evidence: The process of properly working with fragile and volatile digital evidence
Proxy server: A server that fulfills the requests of its clients by forwarding them to other servers
Public data: Data that is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others
Public key infrastructure (PKI): An encryption framework that secures the exchange

of online information
Python Standard Library: An extensive collection of Python code that often comes packaged with Python
Q
Query: A request for data from a database table or a combination of tables
Quid pro quo: A type of baiting used to trick someone into believing that they'll be rewarded in return for sharing access, information, or money
R
Rainbow table: A file of pre-generated hash values and their associated plaintext
Random Access Memory (RAM): A hardware component used for short-term memory
Ransomware: A malicious attack where threat actors encrypt an organization's data and demand payment to restore access
Rapport: A friendly relationship in which the people involved understand each other's ideas and communicate well with each other
Recover: A NIST core function related to returning affected systems back to normal operation

Recovery: The process of returning affected systems back to normal operations
Red Hat® Enterprise Linux® (also referred to simply as Red Hat in this course): A subscription-based distribution of Linux built for enterprise use
Reflected XSS attack: An instance when malicious script is sent to a server and activated during the server's response
Regular expression (regex): A sequence of characters that forms a pattern
Regulations: Rules set by a government or other authority to control the way something is done
Relational database: A structured database containing tables that are related to each other
Relative file path: A file path that starts from the user's current directory
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
Resiliency: The ability to prepare for, respond to, and recover from disruptions
Respond: A NIST core function related to making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process
Return statement: A Python statement that executes inside a function and sends information back to the function call
Reverse proxy server: A server that regulates and restricts the internet's access to an internal server
Risk: Anything that can impact the confidentiality, integrity, or availability of an asset
Risk mitigation: The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach
Root directory: The highest-level directory in Linux
Rootkit: Malware that provides remote, administrative access to a computer
Root user (or superuser): A user with elevated privileges to modify the system
Router: A network device that connects multiple networks together

S
Salting: An additional safeguard that’s used to strengthen hash functions
Scareware: Malware that employs tactics to frighten users into infecting their device
Search Processing Language (SPL): Splunk’s query language
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 architecture: A type of security design composed of multiple components, such as tools and processes, that are used to protect an organization from risks and external threats
Security audit: A review of an organization's security controls, policies, and procedures against a set of expectations
Security controls: Safeguards designed to reduce specific security risks
Security ethics: Guidelines for making appropriate decisions as a security professional
Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy
Security governance: Practices that help support, define, and direct security efforts of an organization
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 in an organization
Security mindset: The ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, application, or data
Security operations center (SOC): An organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks

Security orchestration, automation, and response (SOAR): A collection of applications, tools, and workflows that use automation to respond to security events
Security posture: An organization’s ability to manage its defense of critical assets and data and react to change
Security zone: A segment of a company’s network that protects the internal network from the internet
Select: The third step of the NIST RMF that means to choose, customize, and capture documentation of the controls that protect an organization
Sensitive data: A type of data that includes personally identifiable information (PII), sensitive personally identifiable information (SPII), or protected health information (PHI)
Sensitive personally identifiable information (SPII): A specific type of PII that falls under stricter handling guidelines
Separation of duties: The principle that users should not be given levels of authorization that would allow them to misuse a system
Session: a sequence of network HTTP requests and responses associated with the same user
Session cookie: A token that websites use to validate a session and determine how

long that session should last
Session hijacking: An event when attackers obtain a legitimate user’s session ID
Session ID: A unique token that identifies a user and their device while accessing a system
Set data: Data that consists of an unordered collection of unique values
Shared responsibility: The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security
Shell: The command-line interpreter
Signature: A pattern that is associated with malicious activity
Signature analysis: A detection method used to find events of interest

Simple Network Management Protocol (SNMP): A network protocol used for monitoring and managing devices on a network
Single sign-on (SSO): A technology that combines several different logins into one
Smishing: The use of text messages to trick users to obtain sensitive information or to impersonate a known source
Smurf attack: A network attack performed when an attacker sniffs an authorized user’s IP address and floods it with ICMP packets
Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables
Social media phishing: A type of attack where a threat actor collects detailed information about their target on social media sites before initiating the attack
Spear phishing: A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source
Speed: The rate at which a device sends and receives data, measured by bits per second
Splunk Cloud: A cloud-hosted tool used to collect, search, and monitor log data
Splunk Enterprise: A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time
Spyware: Malware that’s used to gather and sell information without consent
SQL (Structured Query Language): A programming language used to create, interact with, and request information from a database
SQL injection: An attack that executes unexpected queries on a database
Stakeholder: An individual or group that has an interest in any decision or activity of an organization
Standard error: An error message returned by the OS through the shell
Standard input: Information received by the OS via the command line
Standard output: Information returned by the OS through the shell
Standards: References that inform how to set policies

STAR method: An interview technique used to answer behavioral and situational questions
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

Stored XSS attack: An instance when malicious script is injected directly on the server
String concatenation: The process of joining two strings together
String data: Data consisting of an ordered sequence of characters
Style guide: A manual that informs the writing, formatting, and design of documents
Subnetting: The subdivision of a network into logical groups called subnets
Substring: A continuous sequence of characters within a string
Sudo: A command that temporarily grants elevated permissions to specific users
Supply-chain attack: An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed
Suricata: An open-source intrusion detection system, intrusion prevention system, and network analysis tool
Switch: A device that makes connections between specific devices on a network by sending and receiving data between them
Symmetric encryption: The use of a single secret key to exchange information
Synchronize (SYN) flood attack: A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets
Syntax: The rules that determine what is correctly structured in a computing language
Syntax error: An error that involves invalid usage of a programming language
T
Tailgating: A social engineering tactic in which unauthorized people follow an authorized person into a restricted area

TCP/IP model: A framework used to visualize how data is organized and transmitted across a network
tcpdump: A command-line network protocol analyzer
Technical skills: Skills that require knowledge of specific tools, procedures, and policies
Telemetry: The collection and transmission of data for analysis
Threat: Any circumstance or event that can negatively impact assets
Threat actor: Any person or group who presents a security risk
Threat hunting: The proactive search for threats on a network
Threat intelligence: Evidence-based threat information that provides context about existing or emerging threats
Threat modeling: The process of identifying assets, their vulnerabilities, and how each is exposed to threats
Transferable skills: Skills from other areas that can apply to different careers
Transmission Control Protocol (TCP): An internet communication protocol that allows two devices to form a connection and stream data
Triage: The prioritizing of incidents according to their level of importance or urgency
Trojan horse: Malware that looks like a legitimate file or program
True negative: A state where there is no detection of malicious activity
True positive An alert that correctly detects the presence of an attack
Tuple data: Data structure that consists of a collection of data that cannot be changed
Type error: An error that results from using the wrong data type
U
Ubuntu: An open-source, user-friendly distribution that is widely used in security and

other industries

Unauthorized access: An incident type that occurs when an individual gains digital or physical access to a system or application without permission
Uncontrolled zone: Any network outside your organization's control
Unified Extensible Firmware Interface (UEFI): A microchip that contains loading instructions for the computer and replaces BIOS on more modern systems
USB baiting: An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network
User: The person interacting with a computer
User Datagram Protocol (UDP): A connectionless protocol that does not establish a connection between devices before transmissions
User-defined function: A function that programmers design for their specific needs
User interface: A program that allows the user to control the functions of the operating system
User provisioning: The process of creating and maintaining a user's digital identity
V
Variable: A container that stores data
Virtual machine (VM): A virtual version of a physical computer
Virtual Private Network (VPN): 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 are using a public network like the internet
Virus: Malicious code written to interfere with computer operations and cause damage to data and software
VirusTotal: A service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content
Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source
Visual dashboard: A way of displaying various types of data quickly in one place

Vulnerability: A weakness that can be exploited by a threat
Vulnerability assessment: The internal review process of an organization's security systems
Vulnerability management: The process of finding and patching vulnerabilities
Vulnerability scanner: Software that automatically compares existing common vulnerabilities and exposures against the technologies on the network
W
Watering hole attack: A type of attack when a threat actor compromises a website frequently visited by a specific group of users
Web-based exploits: Malicious code or behavior that’s used to take advantage of coding flaws in a web application
Whaling: A category of spear phishing attempts that are aimed at high-ranking executives in an organization
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
Wildcard: A special character that can be substituted with any other character
Wireshark: An open-source network protocol analyzer
World-writable file: A file that can be altered by anyone in the world
Worm: Malware that can duplicate and spread itself across systems on its own
Y
YARA-L: A computer language used to create rules for searching through ingested log data
Z

Zero-day: An exploit that was previously unknown

Welcome to week 1

Before securing a network, you need to understand the basic design of a network and how it functions.

In this section of the course, you will learn about the structure of a network, standard networking tools, cloud networks, and the basic framework for organizing communications across a network called the TCP/IP model.

Securing networks is a big part of a security analyst's responsibilities, so I'm excited to help you understand how to secure your organization's network from threats, risks, and vulnerabilities.

Let's get going!

Chris: My path to cybersecurity

My name is Chris and I'm the Chief Information Security Officer at Google Fiber. We provide high speed Internet to customers across the United States. As the chief information security officer, I'm responsible for making sure that the network stays safe, our customers' data stays safe and that we are supporting law enforcement and others as required. The career path was a long and winding one. My actual first job was working as a butcher at the family grocery store. I eventually ended up with a job in the computer center at college, which is where I learned a lot of my initial computer skills. Then when I graduated from college, I started off as a software developer, designing accounting software for a consulting company supporting the Department of Agriculture. Then I moved on from that to other roles, eventually ending up in one of the first Internet over cable companies. I ran several of their services, email, web services, etc. My stuff kept getting attacked. I fell into cybersecurity because I had to defend the things that I was building. I realized it was fun. I realized that it was a great career opportunity. I've just stuck with that ever since then. When I got into this field, other than a couple of books, there wasn't a lot of training material out there. There were some other people out there that I could ask questions of, and I could get some mentoring from. But as a general rule of thumb, I was on my own. Despite this being a fairly technical field, the most important thing you're going to learn are the connections you're going to make to other people. I made a conscious decision to become actively involved in some of the outside work organizations, the trade associations, the non profits, the meet ups, and other cybersecurity organizations. This enabled me to build the reputation and the relationships so that as my career moved along, people were reaching out to me saying, hey Chris, we have this opportunity, are you interested? Because the cybersecurity industry is so varied, it can seem like there is a tremendous amount you have to learn that there is this huge step that you have to take in order to get into the industry. That can be daunting. But the thing to remember is, once you have that fundamental level of skills and fundamental level of background, there are so many different directions you can go and there's so much opportunity out there. There's this continuous education and curiosity aspect of the job that is so much fun. It means that you are always having the opportunity to learn something new, to change directions and go in new ways because cybersecurity is going to be constantly changing. And that's part of the fun.

What are networks?

Welcome! Before you can understand the importance of securing a network, you need to know what a network is.

A network is a group of connected devices. At home, the devices connected to your network might be your laptop, cell phones, and smart devices, like your refrigerator or air conditioner. In an office, devices like workstations, printers, and servers all connect to the network. 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 devices will use unique addresses, or identifiers, to locate each other. The addresses will ensure that communications happens with the right device. 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.

Now that you've learned about the structure and types of networks, meet me in an upcoming video to learn about the devices that connect to them.

Tina: Working in network security

My name is Tina and I'm a software engineer at Google. As a software engineer, I work on an internal tool that serves the security engineers and network engineers at Google. Network security is important because we want to make sure that our network systems are safe and resilient to be able to defend against malicious hackers, and that we have the ability to protect our user data. Working with network security allows to see the overview of the whole company's network systems, which is super cool. My favorite part of my job is the impact I get to have on the community that I serve at Google. I would say most of my day is a lot of coding, design, talking to security teams and network teams on their priorities and their blockers and being able to come up with a solution. There are often going to be requests that come from network teams and security teams that have specific requirements on certain platforms or on a feature that they need in one of the network policies, and usually we would escalate that and try to work on a fix for that. One piece of advice I would give for someone who wants to take on the cybersecurity journey is to be able to always keep learning and be curious about how things work. Because security is an ever changing field, cybersecurity is definitely a team sport. Everybody has something to contribute, and especially on cybersecurity problems, there can be a lot of possibilities and a lot of different solutions to one problem. It's always great to be able to have people to brainstorm with and to track down issues together because things can get very complex sometimes, but it's also a fun process to be able to work on things together.

Emmanuel: Useful skills for network security

My name is Emmanuel and I am an offensive security engineer at Google. For offensive security, my job is to simulate adversaries and threats that are targeting various companies and I look at defending how we can protect Google's infrastructure. I make it harder to hack Google by actually hacking Google. The technical skills that I use is a lot of programming, as well as learning about operational and platform security. Knowing how these computers work, what is under the hood, and understanding the components that create this infrastructure. An entry-level cybersecurity analyst would look at using command lines, log parsing, and network traffic analysis in their everyday scope of work. Command line allows you to interact with various levels of your operating system, whether it's the low-level things like the memory and the kernel, or if it's high-level things like the applications and the programs that you're running on your computer. With log parsing, they're going to be times where you may need to figure out and debug what is going on in your program or application and these logs are there to help you and support you in finding the root issue and then resolve it from there. With this network traffic analysis, there may be times where you need to figure out why is my Internet going slow? Why is traffic not being routed to the appropriate destination? What can I do to ensure that my network is up and running? Network traffic analysis is looking at network across various application and network layers and seeing what that traffic is doing, how we can secure that traffic, as well as identify any vulnerabilities and concerns. In the contexts for me, for security, I look at: are passwords being leaked in the traffic that's being sent across the network? Are infrastructures being secured? Are firewalls being readily configured and configured safely? One skill that has continued to grow with me in my current role has been communicating effectively to product teams, engineers, and identifying an issue that is influencing or affecting the business, and communicating to those teams effectively to fix it. Being able to take on these many hats and explain things with the right business approach to things to ensure that the issues that I do find in my work are identified but there are also fixed. My advice to folks who are taking this certificate would take things apart, feel uncomfortable, learn and grow and find opportunities to learn and understand how things work and that skill set will benefit you for the remainder of your journey.

tech enthusiest reminder

A hub is a network device that broadcasts information to every device on the network.

Network tools

In this video, you'll learn about the common devices that make up a network. Let's get started.

A hub is a network device that broadcasts information to every device on the network. Think of a hub like a radio tower that broadcasts a signal to any radio tuned to the correct frequency.

Another network device is a switch. 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.

Another device that we'll discuss is a router. 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.

Finally, let's discuss modems. 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. You'll learn more about them later in the certificate program.

Now you've explored some common devices that make up a network. Coming up, you're going to learn more about cloud computing, and how networks can be designed using cloud services.

Network components, devices, and diagrams

In this section of the course, you will learn about network architecture.

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.

A network diagram displaying how different devices are connected to an internal network

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.

A client server model showing three client devices sending requests and receiving responses from a database ser

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 or coaxial cables. 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.

A modem converting data from the internet, connecting to a Wi-Fi router

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.

A wireless access point connected to wired and wireless devices on a network

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.

A router connecting to two firewalls and creating two separate security zones

Key takeaways

In the client-server model, the client requests information and services from the server, and the server performs the requests for the clients. Network devices include routers, workstations, servers, hubs, switches, and modems. Security analysts use network diagrams to visualize network architecture.

Cloud networks

Companies have traditionally owned their network devices, and kept them in their own office buildings. But now, a lot of companies are using third-party providers to manage their networks.

Why? Well, this model helps companies save money while giving them access to more network resources. The growth of cloud computing is helping many companies reduce costs and streamline their network operations.

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.

Today, the number of businesses that use cloud computing is increasing every year, so it's important to understand how cloud networks function and how to secure them.

Cloud providers offer an alternative to traditional on-premise networks, and allow organizations to have the benefits of the traditional network without storing the devices and managing the network on their own.

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.

With the transition to cloud networking, I have witnessed an overlap of identity-based security on top of the more traditional network-based solutions. This meant that my focus needed to be on verifying both where the traffic is coming from and the identity that is coming with it.

More organizations are moving their network services to the cloud to save money and simplify their operations. As this trend has grown, cloud security has become a significant aspect of network security.

Cloud networks

Companies have traditionally owned their network devices, and kept them in their own office buildings. But now, a lot of companies are using third-party providers to manage their networks.

Why? Well, this model helps companies save money while giving them access to more network resources. The growth of cloud computing is helping many companies reduce costs and streamline their network operations.

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.

Today, the number of businesses that use cloud computing is increasing every year, so it's important to understand how cloud networks function and how to secure them.

Cloud providers offer an alternative to traditional on-premise networks, and allow organizations to have the benefits of the traditional network without storing the devices and managing the network on their own.

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.

With the transition to cloud networking, I have witnessed an overlap of identity-based security on top of the more traditional network-based solutions. This meant that my focus needed to be on verifying both where the traffic is coming from and the identity that is coming with it.

More organizations are moving their network services to the cloud to save money and simplify their operations. As this trend has grown, cloud security has become a significant aspect of network security.