Course 3 overview

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.

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.
2. **Play It Safe: Manage Security Risks** — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.
3. **Connect and Protect: Networks and Network Security** — *(current course)* Gain an understanding of network-level vulnerabilities and how to secure networks.
4. **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.
5. **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.
6. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.
7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks.
8. **Put It to Work: Prepare for Cybersecurity Jobs** — 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.

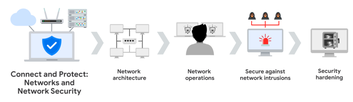
Week 1: Network architecture

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

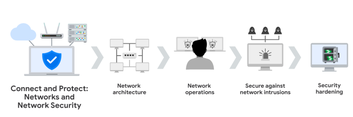
You will explore network protocols and how network communication can introduce vulnerabilities. In addition, you'll learn about common security measures, like firewalls, that help network operations remain safe and reliable.

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.

Mark as completed

Like Dislike Report an issue