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

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**

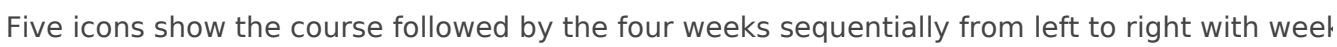
1. — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

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.

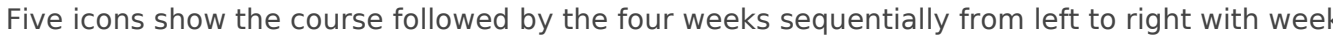
What’s to come? Here’s a quick overview of the skills you’ll learn in each week of this course.

Week 1: Network architecture



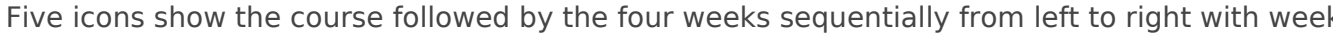
You'll be introduced to network security and explain how it relates to ongoing security threats and vulnerabilities. You will learn about network architecture and mechanisms to secure a network.

Week 2: Network operations



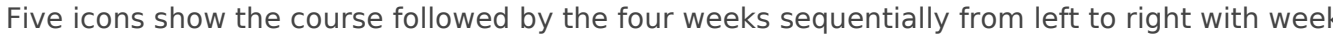
You will explore network protocols and how network communication can introduce vulnerabilities. In addition, you'll learn about common security measures, like firewalls, that help network operations remain safe and reliable.

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.

Revision #3
Created 2023-06-25 16:29:49 UTC by naruzkurai
Updated 2023-07-03 10:29:21 UTC by naruzkurai