Cybersecurity Careers
Context for Educators

DIGITAL CAREERS TOOLKIT

BY SHARED LANE

DOWNLOADABLE GUIDES

About Careers in Cybersecurity

This guide contains supplemental information for educators who use the Digital Career Toolkit with learners. It includes detailed background information to provide context on cybersecurity careers. Use this alongside the Facilitator Guide which includes lesson planning suggestions.

Business Context for Cybersecurity Careers

Cybersecurity specialists make sure that computer systems and networks perform the way they are supposed to, and that they are safe from attack. They are responsible for making sure that networks and computer systems are up-to-date and not vulnerable to software bugs.

Cybersecurity specialists are also responsible for making sure that other co-workers are kept up-to-date on security best practices (what’s the safe vs. dangerous way to do your work), which means they might take on the role of a trainer or an advisor. Ultimately they are responsible for keeping data safe, and helping everyone else keep data safe as well.

Another aspect of a cybersecurity specialist’s job is the design of security measures, like firewalls, to make sure that information and internal networks adhere to the most recent security standards. Cybersecurity specialists are responsible for constantly monitoring security systems and networks for abnormal traffic or activity and tracking (or recording) those activities in documents and reports.

Social Context for Cybersecurity Careers

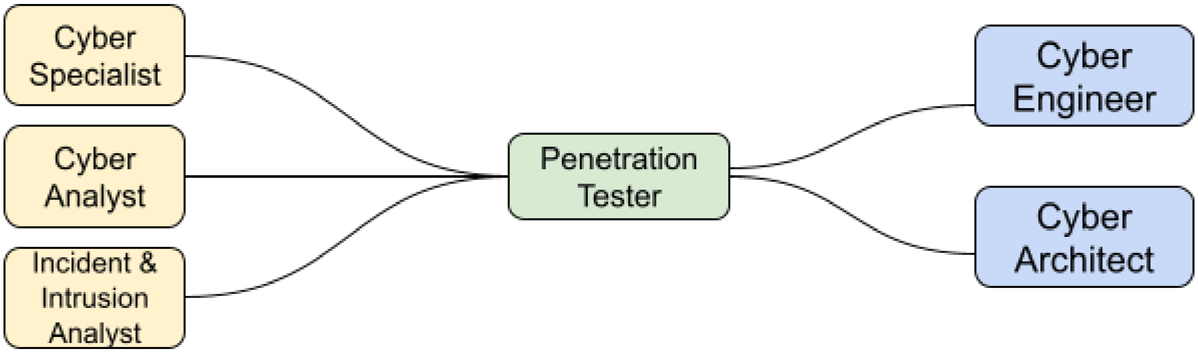
“The gender [and racial] gap that exists in the cybersecurity workforce contributes to the overall cyber workforce shortage that persists in the United States and globally, which ultimately makes us less prepared to deal with the threats of today and tomorrow.” -CISA Director Jen Easterly

Digital Career Toolkit

In the Toolkit we focus on two entry level roles roles:

1. **Cybersecurity Analyst** - junior level role that is fairly easy to access with certifications
2. **Penetration Tester** - high-demand job, accessible with experience and additional training

Career Paths:



Additional Resources:

Cyberseek - career pathway information, links to training providers, job openings, etc.

National Initiative For Cybersecurity Careers And Studies - includes a user guide for a cybersecurity career pathways tool

Life Hackers - a video exploration of cybersecurity careers

More on Penetration Tester Responsibilities

The purpose of penetration testing is to **help companies find out where they are most likely to face an attack and proactively shore up those weaknesses** before they are exploited by hackers.

Main Job Duties of Penetration Testers[1]:

- **Planning Penetration Tests:** Plan and develop tests to find potential security problems. They use existing methods and sometimes make their own tools to launch tests.This requires strong project management and time management skills.

- **Enacting Penetration Tests:** Penetration tests simulate malicious cyberattacks from outside individuals or organizations to detect internal vulnerabilities. This allows organizations to improve their security, stopping data breaches and other cyberattacks before they happen. Penetration testers use the same types of tools and methods as hackers to protect company data.

- **Making Security Recommendations:** Penetration testers can improve security by analyzing what went wrong in their simulations. They can make recommendations to address security weaknesses and suggest security education for employees. They may work with computer engineers or other cybersecurity team members to mitigate identified weaknesses.

- **Writing Reports/Giving Presentations:** After launching a test, penetration testers write reports to present their findings to management. Reports typically include recommendations about how to improve security for the future. Pen testers also sometimes give oral presentations describing the results of their tests.

- **Track New Cybersecurity Developments:** Penetration testers should follow professional publications or complete certifications to remain informed about emerging security threats and malware. It also helps to research general information technology and security trends.

Other Required Skills:

- **Knowledge of Vulnerabilities and Exploits**: Penetration testers need to know various common exploits and techniques, and they need to know how to modify existing exploits to get them to work in specific networks for testing purposes.
- **Secure Web Communications and Technologies**: Testers need to understand everything from how to register a web domain name to applying the domain name to a cloud-IP address to generating secure certificates for the domain, and finally, using those certifications to secure web communication. Penetration testers also need to know how web applications are built, how to identify input fields, and how to gather information that can lead to exploiting the functionality of the web application.
- **Script or Write Code**: The main languages penetration Testers need to maintain a basic proficiency in are Python, Perl, PowerShell, and Bash. Along with knowing these languages, Penetration Testers need to be able to manipulate data in whatever format is required for you to form an operational picture.
- **Public Speaking, Report Writing**: Cybersecurity experts, including Penetration Testers, need to communicate complex ideas in ways even non-technical people can understand.
- **Certifications**: The Offensive Security certifications (OSCP/OSCE), SANS certifications, Red Hat Certified Specialist in Security: Linux, CompTIA PenTest+, CISSP, CISA, and CISM certifications

[1] cyberdegrees.org