How to Become a Cybersecurity Professional?

Cybersecurity professionals deliver security across the development process of software systems and networks. They are expected to find risks and vulnerabilities in the security posture of an organization. They manage and monitor various attacks and unlawful intrusions. The cybersecurity professional can recognize any breaches and security violations that need to be resolved, develop rules and regulations to assure the company's systems stay as safe as possible, in addition to developing security measures for all employees. Cybersecurity specialists are experts in finding loopholes in databases, networks, hardware, firewalls, and encryption. A cybersecurity professional's primary role is to avoid attacks by fixing critical issues before malicious hackers can exploit them. Also, cybersecurity professionals manage to clean up after security breaches and cyber-attacks.

Roles and responsibilities:

There are various roles and responsibilities of cybersecurity professionals. Some of them are as follows:

- Manage organizational resources to support security goals and policies
- Create and execute approaches to improve IT project's reliability and security
- Perform and maintain corporate security policies and procedures

- Maintain computer networks, hardware, software, and other related systems, protecting data by implementing network security measures, preserving data from attacks, and replacing damaged network hardware components when required
- Identify possible issues and fix existing problems
- Develop a set of security standards and practices, conducting scans of networks to find vulnerabilities and penetration testing

Tools and technical skills required to become a Cybersecurity professional

A cyber specialist must have an understanding of the following tools:

1) Nmap: Nmap stands for network mapper. Nmap is an information-gathering tool used for reconnaissance. It is an open-source network scanner. It sends packets and analyzes the responses; from these responses, you can find a vulnerable host on a particular network, open ports, operating system version, and other vulnerabilities.

2) Metasploit: Metasploit is an exploitation framework, which means it is a group of tools and utilities put together to make an exploit development. Basically, Metasploit is a penetration testing platform that allows us to use different modules and find, exploit, and validate vulnerabilities.

3) Social Engineering Toolkit: The Social-Engineer Toolkit is an open-source penetration testing framework for social engineering. It is a unique tool that identifies the attacks that are targeted at the human element. It is also an open-source framework.

4) SQLMap: SQLMap is a tool that is used to test SQL injection vulnerabilities. If SQL injection is present, it can also help speed up exploiting the vulnerabilities, assisting the tester in getting results faster, and assisting customers in understanding the code's weakness to address the code.

5) Nessus: Nessus is an open-source and remote security scanner tool that scans network tools and then creates a report listing all the discovered vulnerabilities. This tool allows you to watch your WiFi network's security by capturing data packets and transporting them to text files for further analysis.

A Path to become a cybersecurity professional
There are three steps to become a cybersecurity specialist:

- **Get qualified**: Bachelor or master's degree in IT fields such as computer engineering, information security, computer science, programming, or any relevant field that offers cybersecurity specialization.
- **Skill Development:**Some specific skills for cybersecurity professionals include:
- Penetration and vulnerability and IDS/IPS testing
- Windows, UNIX, and Linux operating systems
- Computer networking, routing, TCP/IP, and switching
- Ethical hacking and threat modeling
- **Get certified:** Having a certification is always an advantage over other applicants so, get certified in at least one of the following cybersecurity certifications.
- CEHv11 (Certified Ethical Hacker v11)
- CompTIA Security+
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)
- Cisco Certified Network Associate (CCNA)

How can InfosecTrain help you?

Infosec Train provides certification training and necessary preparation for all Information Security certification exams. It is one of the best consulting organizations, focusing on a range of IT security training. Well qualified instructors with years of industry experience delivering interactive training sessions thatwill help you hone your cybersecurity skills. You can visit the following link to prepare for the certification exam:
https://www.infosectrain.com