Lab - Becoming a Defender

Objectives

Research and analyze what it takes to become a network defender.

Part 1: Conduct search of Certifications.

Part 2: Investigate positions available within cybersecurity

Background / Scenario

In our technology-centric world, as the world gets more connected, it also gets less safe. Cybersecurity is one of the fastest growing and most in-demand professions. Individuals in this field perform a wide variety of jobs including, but not limited to, consultation, investigation, and program management services to mitigate risks from both internal and external sources. Cybersecurity professionals are required to evaluate, design and implement security plans, conduct in-depth fraud investigation, perform security research and risk assessment, and propose solutions to potential security breaches.

Individuals with good security skills have a great earning potential. To be considered for one of these high paying jobs, it is very important to have the proper qualifications. Because of this, it is important to consider the industry certifications available for this career path. There are many certifications to choose from. Selecting the right certification(s) for you requires careful consideration.

Note: You can use the web browser in the virtual machine that was installed in a previous lab to research security-related issues. By using the virtual machine, you may prevent malware from being installed on your computer.

Required Resources

- PC or mobile device with internet access and virtual machine (optional).

Instructions

Step 1: Conduct search of Certifications.

a. Use your favorite search engine to conduct a search for the most popular cybersecurity-related certifications. List them below with the organization that provides the certification.

Certified Information Systems Security Professional (CISSP) – (ISC)²

Certified Ethical Hacker (CEH) – EC-Council

Certified Information Security Manager (CISM) – ISACA

CompTIA Security+ – CompTIA

GIAC Security Essentials (GSEC) – GIAC

b. Pick three certifications from the list above and provide more detail about the certification requirements and knowledge gained i.e.: vendor specific or neutral, number of exams to gain certification, exam requirements, topics covered etc.

CISSP: Organization: $(ISC)^2$

Requirements: 5 years of full-time security experience in at least two of the eight CISSP domains.

Exams: 1

Topics: Security and risk management, asset security, security architecture, etc.

CEH: Organization: EC-Council

Requirements: Two years of work experience in security or completion of EC-Council's training.

Exams: 1

Topics: Penetration testing, hacking tools, vulnerability assessments, etc.

CompTIA Security+: Organization: CompTIA

Requirements: No formal prerequisites, though two years of experience recommended.

Exams: 1

Topics: Network security, cryptography, identity management, and more.

Step 2: Investigate positions available within cybersecurity

Glassdoor is one of the largest job sites worldwide. Using your browser of choice, access glassdoor.com and search to find cybersecurity jobs available that were posted within the last two weeks. Adjust the search as you would like. You can search for jobs in your area or an area that you would like to live and work in.

a. How many new job listings were posted within the last two weeks?

For Cybersecurity analyst, 32 job listings were posted in the last 2 weeks.

b. What is the salary range for the top 10 listings?

40K-100K

c. What are the most common qualifications required by employers?

- **Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field.**
- **Basic understanding of network security principles, malware analysis, and threat intelligence.**
- **Strong understanding of security concepts, principles, and best practices.**
- **Experience with security technologies such as firewalls, intrusion detection/prevention systems, and endpoint protection**
- **Experience with security incident response and management**

d. What industry certifications are required by these employers?

CompTIA Security+, CEH, SANS GCFA (GIAC Certified Forensic Analyst), GNFA (GIAC Network Forensic Analyst), GCFE (GIAC Certified Forensic Examiner)

e. Do any of the certifications match the ones that you found in Step 1a?

Yes.

f. Investigate online resources that allow you to legally test your hacking skills. These tools allow a novice with limited cyber security experience to sharpen their penetration testing skills. One such site is Google Gruyere (Web Application Exploits and Defenses). What kinds of challenges can you find?

Google Gruyere: Offers challenges related to web application exploits and defenses.

Hack The Box: Provides virtual labs and real-world penetration testing scenarios.

TryHackMe: Beginner-friendly with guided labs for learning cybersecurity concepts.