Lab - Becoming a Defender
Objectives
Research and analyze what it takes to become a network defender.

Part 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.

- CompTIA Security+ - CompTIA
- CISSP (Certified Information Systems Security Professional) - (ISC)²
- CEH (Certified Ethical Hacker) - EC-Council
- CCSP (Certified Cloud Security Professional) - (ISC)²
- CISM (Certified Information Security Manager) - ISACA
- GSEC (GIAC Security Essentials Certification) - SANS Institute

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.

CompTIA Security+ - provided by CompTIA The CompTIA Security+ certification is a vendor-neutral certification that validates an individual's knowledge and skills in the field of IT security. To obtain the Security+ certification, candidates must pass a single exam that covers topics such as network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control and identity management, and cryptography

CISSP (Certified Information Systems Security Professional) - provided by (ISC)² The CISSP certification is a vendor-neutral certification and is widely recognized as one of the most respected certifications in the information security industry. To obtain the CISSP certification, candidates must have a minimum of five years of professional work experience in the information security field, with at least three of those years in a security management role.

CEH (Certified Ethical Hacker) - provided by EC-Council The CEH certification is a vendor-neutral certification that demonstrates an individual's ability to identify vulnerabilities and weaknesses in target systems and to use the same tools and techniques as a malicious hacker to test the security of those systems. To obtain the CEH certification, candidates must pass a single exam that covers topics such as network scanning, enumeration, vulnerability analysis, system hacking, and social engineering.

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?

Within last two weeks there are more than 35 new job listing

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

15-20L,10-15L,6-9L,3-5L

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

A bachelor’s/master’s degree in Computer Science background,Experience needed for higher roles and related major Security certification

d. What industry certifications are required by these employers?

- Fundamental knowledge and experience on IT Infrastructure and Endpoints management.
- 2-3 years on IT delivery experience.
- Technical knowledge and experience managing teams across various domains involved in Workplace, Data center, Networking,security, compliance is required.

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

Yes CISSP, Comptia Security+ etc

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 penetest skills. What kinds of challenges can you find

Cross-site scripting (XSS) attacks: Injecting malicious code into a web page, which can then be executed by unsuspecting users who visit that page.

Cross-site request forgery (CSRF) attacks: Tricking a user into performing an action on a website without their knowledge or consent, often by using social engineering techniques.

SQL injection attacks: This type of attack involves inserting malicious SQL code into a web page in order to gain access to a website's database.