Assignment 1 - Researching PenTesting Careers

Objectives

In this lab, you will complete the following objectives:

- Conduct a Penetration Tester Job Search
- Analyze Penetration Tester Job Requirements
- Discover Resources to Further Your Career

Background / Scenario

When preparing for any career, it is important to understand the prospective job market. The help wanted postings on internet job boards contain a wealth of information regarding the qualifications and preparation required for the jobs that you will be applying for. For careers in ethical hacking, you can see the certifications, knowledge, and skills that are required along with descriptions of what the ethical hacker will be doing for the company. In addition, you can see the kinds of organizations that hire ethical hackers, their locations, and other corporate information that is useful to know when applying for positions.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

Instructions

Part 1: Conduct a Penetration Tester Job Search

In this part of the lab, you will conduct a search for ethical hacker/penetration tester jobs on various internet employment sites.

Step 1: Search internet job boards.

- Open a browser and search for jobs related to ethical hacking and penetration testing. Use employment sites such as **indeed.com**, **glassdoor.com**, **linkedin.com**, **monster.com**, etc.
- Consult at least three different employment sites. Search specifically for entry-level postings, although feel free to look at more senior positions. Find some jobs that look interesting to you.

Assignment 1 - Researching PenTesting Careers

- Complete **Table 1: Jobs Table** with at least five jobs that you have found from different employment sites. You can complete the tables in this document, or recreate the tables in another file or on a piece of paper.
- Bookmark these jobs or open each job in a new tab. Keep the sites available for the next part of the lab.

Table 1: Jobs Table

1 - Job Title	2 - Company Name	3 - Level (Entry, Mid, Senior)	4 – Location	5 – Internet Job Board Source
Ethical Hacker	SecureTech Inc.	Mid	San Francisco, CA	LinkedIn
Cybersecurity Penetration Tester	Cintel Inc	Entry	Eglin AFB, FL	Glassdoor
Penetration Tester	WarCollar Industries	Entry	Reston, VA	Indeed
Cyber Security Defense Analyst	Lockheed Martin	Entry	Atlanta, IL	Digitalhire
Red Team Security Consultant	Mandiant, Google Cloud	Mid	New York, NY, USA	Glassdoor
Cybersecurity Intern	Washington, DC, United States	Conference of State Bank Supervisors (CSBS)	Entry-Level (Internship)	ZipRecruiter

Part 2: Analyze Penetration Tester Job Requirements

Now that you have collected some jobs that are interesting to you, go through and complete **Table 2: Duties and Required Training and Certification**.

Step 1: Complete the table.

Assignment 1 - Researching PenTesting Careers

- Copy the five jobs from Table 1 into the **Job Title** column in **Table 2: Duties and Required Training and Certification**.
- Read through the job postings and summarize the duties that you would be responsible for in the position. Focus on the diversity of duties that are required by the different positions.
- What skills are required? Focus on the pentesting-related skills, but also any general skills that are required.
- Explore the postings further and complete the Required Experience column. What kind of experience is required for each job? How many years of experience do they require? If the employment site interface permits, filter or search for entry-level positions that require no experience. There are some out there !
- Finally, what certifications are mentioned as required or desirable?

Table 2: Duties and Required Training and Certification

Job Title	Duties	Required Sklls	Required Experience	Required Training and Certification
Ethical Hacker	Identify security flaws, conduct security testing, and provide remediation strategies.	•Knowledge in cybersecurity, network security, application infrastructure, and software development lifecycle •Experience with network security monitoring tools •Experience with Data Loss Prevention	2-4 years	CompTIA Security+, CEH

		(DLP) technology •Strong work ethic and organizational skills •Ability to analyze risks and make security recommendations		
Cybersecurity Penetration Tester	• Conduct penetration testing and cybersecurity assessments on DoD systems. • Develop and manage cyber test strategies for military and government systems. • Analyze vulnerabilities in aircraft, weapons, cloud, and IP system architectures. • Work with the 48th Cyberspace Test Squadron to perform	• Penetration testing and vulnerability assessment expertise. • Knowledge of cybersecurity testing methodologies (scanning, exploitation, reporting). • Familiarity with	1-3 years	OSCP, GPEN, CEH

	security evaluations. • Prepare reports and communicate findings to technical and non-technical audiences. • Ensure compliance with NIST, ISO 27001, and DoD cybersecurity frameworks. • Travel 15-20 weeks per year for cybersecurity test events.	NIST, ISO 27001, and SOC 2 cybersecurity frameworks. • Strong problem-solving and analytical thinking skills. • Ability to work independently and in small or large team settings. • Excellent communication		

		skills (written and verbal). • Project management and ability to prioritize multiple projects.		
Penetration Tester	• Conduct penetration testing and vulnerability assessments on networks, systems, and applications. • Identify and analyze security risks and provide recommendations for mitigation. • Develop detailed reports outlining findings,	Proficiency in penetration testing tools like Metasploit, Burp Suite..	1 Year	CompTIA PenTest+, GPEN,CEH, CPT

Assignment 1 - Researching PenTesting Careers

	risks, and recommendations. • Collaborate with IT and security teams to enhance cybersecurity defenses. • Stay updated on the latest cybersecurity trends, tools, and best practices.			
Cyber Security Defense Analyst	• Perform cyber threat intelligence analysis and correlate actionable security events. • Network traffic analysis using raw packet data, net flow, IDS, IPS, and custom sensor output. • Participate in incident response efforts and	• Must hold at least one of the DoD-8570 baseline certifications (IAT Level 2): Security+, CEH, CYSA+, or CISSP. • Active US DoD	• Experience in network traffic analysis, cyber threat intelligence, and incident response. • Experience in cybersec	Security+, CEH, CYSA+, CISSP, OSCP

	coordinate resources. • Support communications networks security as part of a team protecting US Government customers. • Engage with cybersecurity experts to prevent and protect against cyber threats in real-world environments.	Secret clearance required. • Practical experience with cyber security analysis tools. • Understanding of intrusion detection and incident response. • Experience with TCP/IP networking, common networking ports/	urity defense and familiar with cybersecurity systems.	

Assignment 1 - Researching PenTesting Careers

		protocols, and network traffic flow. - Willingness to perform shift work. - Ability to work onsite full-time at designated Lockheed Martin facilities.		
Red Team Security Consultant	- Perform Red Team and Purple Team assessments, adversarial emulation of cyberattacks. - Conduct external	Expertise in red teaming, network security, and threat hunting.	3+ years	OSCP, OSCE, OSEP

	and internal network assessments and assumed breach assessments. • Perform ransomware readiness reviews and social engineering assessments. • Engage in threat hunting, forensic analysis, and malware triage. • Develop detailed technical and executive-level reports on findings and mitigation strategies. • Communicate cybersecurity threats and strategies to executive			

	leadership, legal counsel, and technical teams. • Research, develop, and enhance offensive security tools and techniques.			
Cybersecurity Intern	• Research and analyze national and global cybersecurity threats affecting the financial sector. • Review cybersecurity incidents in financial entities and extract lessons from after-action reports. • Attend cybersecurity briefings, CSBS Bankers Electronic Crimes	• Working knowledge of network security concepts. • Knowledge of cybersecurity in the financial sector. • Technical inclination in	No experience required	Security+ (Preferred)

	Task Force meetings, and other relevant events. • Assist in developing fact sheets and materials for the 2025 CSBS Cyber Hygiene Awareness campaign. • Contribute to cybersecurity and IT conference presentations and narratives. • Ensure the confidentiality, integrity, and availability of CSBS information systems.	cyber security operations.		

Part 3: Discover Resources to Further Your Career

Assignment 1 - Researching PenTesting Careers

You likely noticed several certification and training requirements that were mentioned in the job postings. In this part of the lab, you will investigate pathways to gain the level of training and the certifications that are suitable for the type of job that you are looking for.

a. Which certifications are most commonly required?

Answer: I am listing down from the job postings analyzed, the most common required cybersecurity certifications are:

- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- GIAC Penetration Tester (GPEN)
- CompTIA Security+
- Certified Information Systems Security Professional (CISSP)

b. Investigate training options for the certifications that you identified as being appropriate to the prospective positions. Where can you take courses to prepare you for those certifications?

Answer:

- CompTIA Security+ – Available via CompTIA, Coursera, Udemy.
- Certified Ethical Hacker (CEH) – Offered by EC-Council, Cybrary.
- Offensive Security Certified Professional (OSCP) – Provided by Offensive Security.
- GIAC Penetration Tester (GPEN) – Available through SANS Institute.
- CISSP – Provided by (ISC)², SANS, Udemy.

Reflection

Assignment 1 - Researching PenTesting Careers

From your internet search results, please answer the following questions.

1. Do you find that jobs are concentrated in any one area, or are they distributed?

Answer: Jobs are available across the USA but concentrated in major tech hubs. However, remote opportunities are increasing nowadays.

2. What are the most common duties mentioned?

Answer:

- ❖ Conducting penetration testing and vulnerability assessments.
- ❖ Performing penetration tests(network, web applications, cloud environments, databases)
- ❖ Staying updates on cybersecurity trends and emerging threats.
- ❖ Identifying security weaknesses and providing remediation strategies.
- ❖ Ensuring compliance with security frameworks, including NIST and ISO 27001.
- ❖ Documenting security findings and reporting them to stakeholders.
- ❖ Using penetration testing tools such as Metasploit and Burp Suite.