Emmanuel Mberu 658546

Lab - Researching PenTesting Careers

Answers Written in Red

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.

a. 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.
b. 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.

c. 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.

d. 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
Manual Ethical Hacker	Bank of America	Mid	Seattle, WA	www.indeed.com
Lead Penetration Tester	AutoRoboto	Senior	Mountain View, CA	www.glassdoor.com
Junior Penetration Tester	Black Lantern Security	Entry	Remote	www.indeed.com
Penetration Tester	Booz Allen	Senior	Washington, DC	www.glassdoor.com
CMMC Cybersecurity Technical Writer	Sev1Tech	Mid	Colorado	www.indeed.com
Red Team Operator (Cooperative Red/Blue Team Operations)	KBR	Entry	Pearl City, HI	www.glassdoor.com

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.

a. Copy the five jobs from Table 1 into the **Job Title** column in **Table 2: Duties and Required Training and Certification**.

b. 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.

c. What skills are required? Focus on the pentesting-related skills, but also any general skills that are required.

d. 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 !

e. Finally, what certifications are mentioned as required or desirable?

Table 2: Duties and Required Training and Certification

1. **Manual Ethical Hacker**

Duties:

Perform application security assessments on internal technologies and applications.

Analyze internal and external cyber threats and anticipate future threat behavior.

Incorporate threat actors' tactics, techniques, and procedures (TTPs) into offensive security testing.

Assess the effectiveness and security posture of multiple technology systems.

Conduct manual code reviews and simulate real-world hacking scenarios.

Prepare technical reports, documents, and risk advisory notices.

Provide practical advice on managing cybersecurity risks.

Mentor junior assessors in both technical and soft skills.

Continuously research evolving threats and adapt testing methods accordingly.

Required Skills:

Penetration Testing (manual preferred)

Application Security and ethical hacking

Manual web app assessments (e.g., simulating attacks like XSS/SQLi without automated tools)

Manual code review for security vulnerabilities

Scripting/coding proficiency

Experience with SAST tools

Familiarity with vulnerability assessment tools (e.g., IBM AppScan, Burp Suite, SQLMap)

Understanding of network and web protocols (e.g., TCP/IP, UNIX/Linux, Cookies)

Technical writing and reporting

Innovative problem-solving

Threat analysis and security advisory

Emmanuel Mberu 658546

Required Experience:
Minimum 4 years of professional experience in:
-Penetration testing
-Application security
-Ethical hacking

Demonstrated expertise in at least 3 of the following:
-Security engineering
-Application architecture
-Security/authentication protocols
-Session management
-Applied cryptography
-RESTful APIs
-Mobile frameworks
-SSO technologies
-Exploit automation

Required Training and Certification:
No explicit requirement, but strong preference for:
-OSWE (Offensive Security Web Exper)
-OSCP, CEH, CISSP, GPEN, PenTest+

2. Lead Penetration Tester
Duties:
Lead and manage a team of penetration testers.

Design and perform penetration tests targeting biometric systems.

Develop and maintain methodologies for penetration testing.

Document penetration test actions, processes, and findings.

Produce both technical and executive-level reports.

Automate repetitive penetration testing tasks to improve team efficiency.

Identify potential attack vectors and entry points into systems.

Evaluate and improve existing security and testing processes.
Required Skills:
Strong command of the Linux command line.

Leadership or mentorship capabilities.

Strong analytical and problem-solving skills.

Excellent communication and documentation skills.

Ability to think offensively i.e., like a hacker to identify potential exploits.

Research and/or work experience in facial recognition technologies.

Required Experience:
Experience managing or mentoring penetration testing teams.

Research or work related to facial recognition.

Strong hands-on background in:
-Penetration testing
-Vulnerability assessment
-Exploit development

No explicit year requirement, but leadership and specialized testing experience is expected.

Required Training and Certification:
2+ years experience in:
-Mobile security testing
-Scientific lab environments
-Deep debugging tasks

1+ year experience in:
-Animation or game development

Proficiency in:
-Photoshop
-Photography

Experience with:
-3D printers and maker tools
-Automation scripting/tools

Certified Ethical Hacker (CEH) or similar credentials

3. **Junior Penetration Tester**
Duties:
Design and execute test strategies to attack and assess complex systems.

Simulate TTPs (tactics, techniques, and procedures) used by various threat actors (opportunistic to advanced).

Emmanuel Mberu 658546

Prepare situation reports and activity summaries for clients and leadership.

Perform verification and validation testing on client defenses and mitigations.

Develop and deliver:
-Walkthroughs
-Proofs of Concept (PoCs)
-Technical articles
-Formal presentations

Attend and/or present at professional cybersecurity events.

Conduct independent research into:
-New attack methods
-Undisclosed or zero-day vulnerabilities
Required Skills:
Penetration testing

Computer Network Attack (CNA)

Computer Network Defense (CND)

Basic scripting with bash and/or PowerShell

Programming experience in at least one OOP language (e.g., Python, Ruby, Java)

familiarity with:
-Windows and Unix systems
-TCP/IP
-IDS/IPS systems
-Web content filtering

Strong critical thinking and risk assessment skills

Ability to go beyond automated tools

Required Experience:
Hands-on experience with:
-Cybersecurity technical work
-Penetration testing
-CNA/CND roles

Understanding of:
-Regulatory frameworks (HIPAA, PCI-DSS, GLBA)
-Security standards (PTES, MITRE ATT&CK)

Experience writing or using:
-Custom tools/utilities for red or blue teaming

Required Training and Certification:
No specific certification listed as required.

4.Penetration Tester
Duties:
Conduct penetration tests, red team operations, and adversary emulation across cloud, on-premise, and hybrid federal systems.

Emulate real-world attacker TTPs to identify vulnerabilities and assess system weaknesses.

Work closely with SOC analysts, engineers, and incident responders to:
-Validate defensive capabilities
-Provide threat-informed feedback
-Develop and maintain custom tools/scripts for testing and automation (Python, PowerShell, etc.).

Produce detailed technical reports that include:
-Risk analysis
-Exploitation paths
-Remediation recommendations

Lead projects and mentor junior penetration testers.

Stay updated on emerging threats, attack vectors, and security trends.
Required Skills:
Proficient in offensive security tools:
-Metasploit
-Cobalt Strike
-Burp Suite
-Nmap
-Kali Linux
-Nessus

Scripting and automation with:
-Python
-PowerShell

Familiarity with:
-MITRE ATT&CK framework
-OWASP Top 10
-CVE analysis
-Post-exploitation techniques

Emmanuel Mberu 658546

Technical writing:
-strong report writing and documentation skills

Strong verbal communication skills for stakeholder engagement
Required Experience:
10+ years in:
-Penetration testing
-Red teaming
-Adversary emulation
-Ethical hacking

Previous work in:
-Cyber operations
-Security Operations Centers (SOC)

Understanding of:
-Federal cybersecurity standards (NIST 800-53)
-Cloud and hybrid system security
Required Training and Certification:
Minimum Education: High School Diploma or GED

Preferred: Bachelor's in CS, IT, or InfoSec

CEH – Certified Ethical Hacker

CompTIA PenTest+

CISSP

OSWP, GPEN, GWAPT

5. CMMC Cybersecurity Technical Writer
Duties:
Develop and maintain CMMC-related cybersecurity documentation including:
-System Security Plans (SSPs)
-Incident Response Plans (IRPs)
-Access Control Policies (ACPs)
-Risk Management Plans (RMPs)
-Shared Responsibility Matrices (SRMs)
-Plans of Action and Milestones (POA&Ms)

Collaborate with technical teams to document:
-System configurations
-Control implementations
-Evidence for compliance

Emmanuel Mberu 658546

Ensure documentation aligns with:
-CMMC Level 2
-NIST 800-171/172
-DFARS

Prepare monthly compliance reports for the Change Control Board.

Maintain an organized evidence library for self and third-party (C3PAO) audits.

Support mock assessments and audit readiness efforts.

Use the Vertasyn™ compliance platform to:
-Centralize compliance evidence
-Generate audit-ready packets
-Monitor documentation health

Align documentation with realities across AWS GovCloud, Azure Gov, GCC High, and on-prem environments.
Required Skills:
Strong technical writing abilities, especially in cybersecurity or compliance contexts

Understanding of cybersecurity compliance frameworks:
-CMMC Level 2
-NIST 800-171/172
-DFARS

Familiarity with:
-Documentation types: SSP, POA&M, IRP
-Regulatory compliance requirements

Proficiency in Microsoft 365 tools (Word, Excel, SharePoint, Teams)

Excellent attention to detail and communication skills

Ability to work both independently and collaboratively
Required Experience:
3+ years experience in technical writing (preferably cybersecurity or federal IT context)

Practical experience working with:
-Cybersecurity documentation
-Compliance audits and evidence collection

Bachelor’s degree in:
-Cybersecurity
-IT

Emmanuel Mberu 658546

Technical Communication
Required Training and Certification:
No mandatory certifications

Preferred/Bonus certifications:
-CompTIA Security+
-CISSP
-Certified Technical Writer (CTW)

6. Red Team Operator (Cooperative Red/Blue Team Operations)
Duties:
Simulate cyber attacks to assess network and system defenses.

Penetration testing of networks and web applications using both manual and automated methods.

Develop custom attack tools, scripts, and payloads to simulate APT-style threats.

Leverage social engineering tactics like phishing and spear-phishing.

Exploit vulnerabilities in cloud, network, and endpoint environments.

Test and evaluate Blue Team detection and incident response capabilities.

Use offensive security tools:
-Cobalt Strike
-Metasploit
-Empire
-Covenant
-BloodHound
-Mimikatz
-Burp Suite
-Kali Linux

Document and refine Red Team TTPs (Tactics, Techniques, Procedures) aligned with MITRE ATT&CK.

Create after-action reports and remediation guidance for stakeholders.

Maintain a Persistent Penetration Testing Network (PPTN) for continuous assessments.

Participate in joint Red/Blue/Purple team exercises to improve detection and collaboration.

Train and mentor junior team members.
Required Skills:
Ethical hacking and attack simulation

Emmanuel Mberu 658546

Manual and automated penetration testing

Tool proficiency in:
-Kali Linux
-Burp Suite
-Metasploit
-Cobalt Strike
-Empire
-Mimikatz
-BloodHound

Social engineering tactics (phishing, pretexting)

Scripting and exploit development

Familiarity with:
-MITRE ATT&CK
-Red/Blue/Purple Team operations

Strong documentation and communication skills
Required Experience:
Multiple Experience Levels:
Level I:
-2+ years practical cybersecurity experience
-Education: HS Diploma/GED

Level II:
-3+ years practical experience
-Education: HS Diploma/GED

Level III:
-5+ years with a Bachelor's degree
-OR 7+ years with HS/GED in Cybersecurity or related experience
Required Training and Certification:
8570 Compliant IAT Level 2 or 3 certifications required such as:
-Security+ CE
-GSEC
-SSCP
-CASP+
-CISSP

DoD 8140 Role-Specific Certifications such as:
-CND Auditor
-CND Analyst
-CNDSP Manager

Emmanuel Mberu 658546

-CND IR
-IASAE I or II

Part 3: Discover Resources to Further Your Career

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?
Based on the job listing I have gone through the most commonly required certifications are:

-OSCP (Offensive Security Certified Professional) which is provides hands-on offensive security and is widely respected in Red Teaming/Pen Testing.

-CEH (Certified Ethical Hacker) which is a recognized entry-level ethical hacking certification.

-Security+ (CompTIA) which provides baseline cybersecurity knowledge, and is DoD 8570 compliant.

-GPEN (GIAC Penetration Tester) which provides advanced pen testing and exploit knowledge.

-OSWE (Offensive Security Web Expert) which provides specialization in manual web application exploitation.

-PenTest+ (CompTIA) which covers network and web pen testing.

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?
For OSCP (Offensive Security Certified Professional) you can use the official course by Offensive Security, which including 90 days lab access and one exam attempt,

For CEH (Certified Ethical Hacker) you can use EC-Council Official CEH v13 Training which includes 20 learning modules and 221 hands-on labs

For CompTIA Security+ you can use CompTIA CertMaster Learn which is a self-paced interactive course that is aligned with Security+

For CISSP (Certified Information Systems Security Professional) you can use their Official ISC² Self-Paced & Instructor-Led Training which adaptive for both online or live classes.

For OSWE (Offensive Security Web Expert) you can use OffSec WEB-300 which is the official training course that provides hands-on experience.

Emmanuel Mberu 658546

Reflection

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?

From both the job listings I found and a broader internet search, it's clear that cybersecurity and penetration testing jobs are widely distributed, but some areas have a higher concentration due to industry demand and government presence. While specific regions like Washington D.C. and California remain hotspots due to government and tech industry presence, the job market is increasingly distributed thanks to the growth in remote opportunities and the global demand for cybersecurity talent.

2. What are the most common duties mentioned?
Most Common Duties are:

Conducting Penetration Tests (Manual & Automated)
-Simulating real-world cyberattacks on web apps, networks, mobile systems, and cloud environments.
-Using tools like Burp Suite, Metasploit, Nmap, Cobalt Strike, etc.

Adversary Emulation & Red Team Exercises
-Emulating tactics, techniques, and procedures (TTPs) of real attackers (e.g., based on MITRE ATT&CK).
-Coordinating red and blue team operations to test and improve defenses.

Vulnerability Identification & Exploitation
-Discovering, validating, and exploiting system or application vulnerabilities.
-Developing proof-of-concept (PoC) exploits or attack chains.

Reporting & Documentation
-Writing detailed technical and executive-level reports.
-Clearly outlining findings, risk assessments, and actionable remediation guidance.

Security Assessments & Compliance Support
-Performing assessments aligned with standards like NIST 800-171/172, CMMC, or OWASP.
-Mapping vulnerabilities to compliance frameworks and supporting audit readiness.

Developing or Using Custom Tools and Scripts
-Writing or modifying tools (often in Python, PowerShell, Bash) to automate testing or simulate threats.

Collaboration with Security Teams

-Working with SOC analysts, incident responders, system engineers, or developers to fix identified issues.

-Engaging in tabletop exercises and threat modeling.

Mentoring and Knowledge Sharing

For senior roles: mentoring junior team members or contributing to internal R&D.

Sharing expertise through documentation, walkthroughs, and mock assessments.