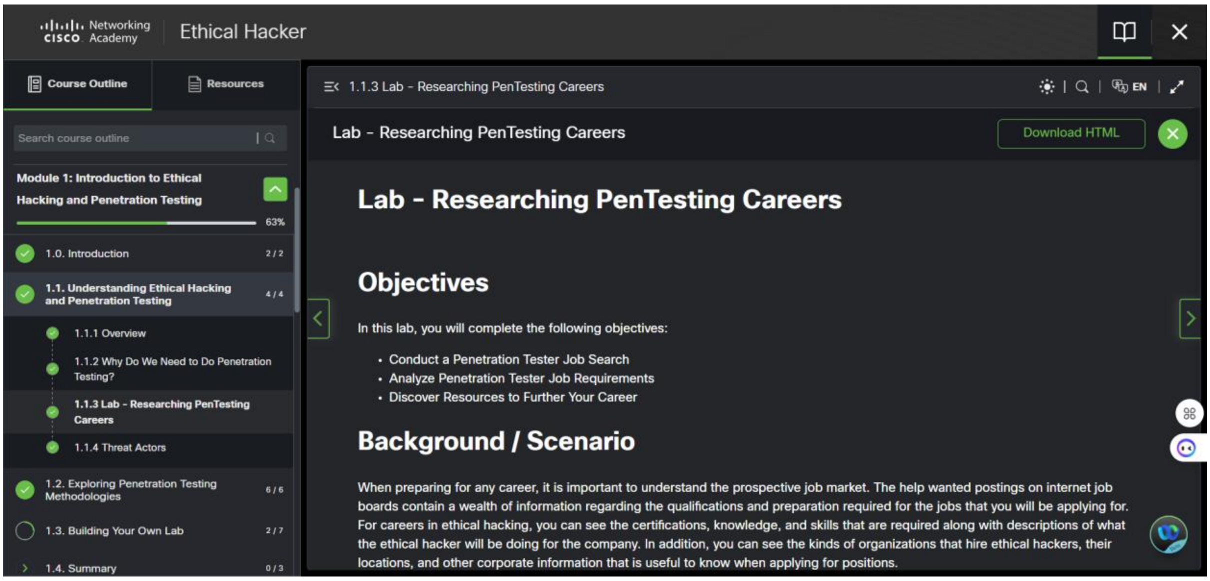
POE for Lab: Researching PenTesting Careers

Lab Title: Researching PenTesting Careers
Learner Name: Motlalepula Jonathan Mojatau
Date: 16/09/2025
Course / Program: Ethical Hacking – Cisco Networking Academy

1. Lab Description & Objectives

This lab focuses on investigating the job market for penetration testers (ethical hackers). The objectives are:

- Conduct a search of current job postings for penetration tester / ethical hacking roles.
- Analyze what employers require in terms of duties, skills, experience, certifications.
- Discover resources (training, certifications, courses) that can help me prepare for those roles.


Networking Academy
Ethical Hacker
Course Outline
Resources
Search course outline
Module 1: Introduction to Ethical Hacking and Penetration Testing
63%
1.0. Introduction 2 / 2
1.1. Understanding Ethical Hacking and Penetration Testing 4 / 4
1.1.1 Overview
1.1.2 Why Do We Need to Do Penetration Testing?
1.1.3 Lab - Researching PenTesting Careers
1.1.4 Threat Actors
1.2. Exploring Penetration Testing Methodologies 6 / 6
1.3. Building Your Own Lab 2 / 7
1.4. Summary 0 / 3
1.1.3 Lab - Researching PenTesting Careers
EN
Lab - Researching PenTesting Careers
Download HTML

Lab - 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.

2. Job Search Findings

I used job boards such as Indeed, Glassdoor, LinkedIn, Pnet, ZipRecruiter to find at least five jobs. Below is a table summarizing five job postings that are entry-level or junior level, or at least ones I found interesting.

Table 1: Jobs Table

#	Job Title	Company / Location	Entry Level / Level	Link / Source
1	Junior Penetration Tester	Job Crystal, Pretoria, Gauteng	Junior Level	Pnet (www.pnet.co.za)
2	Junior Pen Tester / Security Analyst	Mediro ICT Recruitment, Midrand	Junior / Entry Level	Pnet (www.pnet.co.za)
3	Entry-Level Penetration Tester	ZipRecruiter (remote / US-type listing)	Entry Level	ZipRecruiter (ZipRecruiter)
4	Application Security Engineer / Security Consultant	Various firms in South Africa (e.g. DigiCert, etc.)	More toward mid / senior, but interesting job requirements to compare	Glassdoor/Pnet/LinkedIn (Glassdoor)
5	Cyber Security Specialist / IT Security Specialist	European Technology Chamber (Remote SA)	Intermediate / Remote, but some junior tasks inside	Indeed / Glassdoor (Indeed)

3. Duties and Required Training / Certification

Below is a breakdown of the five jobs: their duties, required skills, experience, and certifications.

Table 2: Duties and Required Training and Certification

Job Title	Duties / Responsibilities	Skills Required (Pentesting & General)	Required Experience	Certifications Mentioned / Desirable
Junior Penetration Tester (Job Crystal, Pretoria)	Assist in performing penetration tests on **servers, networks, and applications**; vulnerability assessments; simulating attacks; contributing to labs / proof-of-concept; report findings under senior guidance. (www.pnet.co.za)	Familiarity with scanning tools (Wireshark, Nmap); understanding of network fundamentals (TCP/IP, DNS, DHCP, etc.); passion for cybersecurity; ability to document findings clearly. (www.pnet.co.za)	The posting asks for **3-5 years experience in cybersecurity / related fields** even though title is “Junior”. (www.pnet.co.za)	Nice to have: CEH, Security+, OSCP, scripting skills (Python, Bash, etc.), knowledge of cloud / container environment. (www.pnet.co.za)

Job Title	Duties / Responsibilities	Skills Required (Pentesting & General)	Required Experience	Certifications Mentioned / Desirable
Entry-Level Penetration Tester (ZipRecruiter)	Study penetration techniques; document how systems are breached; vulnerability scanning; basic exploitation; help software teams understand findings. (ZipRecruiter)	Tools such as Metasploit, Burp Suite, Nmap; networking basics; perhaps programming / scripting; problem solving; attention to detail; communication skills. (ZipRecruiter)	Because it's entry level, years of experience may be minimal or 0-1 years; often expecting some IT or cybersecurity fundamentals. (ZipRecruiter)	Certifications like CEH or CompTIA Security+ often expected or advantage. (ZipRecruiter)
Cyber Security / IT Security Specialist (Remote, SA)	Vulnerability assessments; penetration tests; ensuring secure configurations; possibly work with dev teams; monitor systems; risk mitigation. (Indeed)	Strong understanding of pen testing tools; knowledge of network / system / app security; probably scripting / automation; communication; regulatory / compliance knowledge. (Indeed)	3-5 years in cybersecurity / network security / related fields. (Glassdoor)	Certifications often asked: CEH, sometimes OSCP; also vendor certifications. (Glassdoor)
Application Security Engineer / Security Consultant	Review secure code; conduct dynamic & static analysis; help with web-app security; possibly some pen testing but heavier focus on app security. (Glassdoor)	Knowledge of code security; web app vulnerabilities; tools for SAST/DAST; programming or scripting; application frameworks; maybe cloud knowledge. (Glassdoor)	3-5 years or more in application security / cybersecurity. (Glassdoor)	Certifications like CEH, OSCP; sometimes vendor/app security certifications. (Glassdoor)
Cyber Security Specialist (IT Security Specialist, Remote SA)	Conduct regular vulnerability assessments and penetration testing; monitor threats; ensure secure code / secure configurations; work with development / infrastructure teams. (Indeed)	Tools: scanning/Vulnerability tools; knowledge of networks, systems; possibly cloud / containers; communication; regulatory standards; being proactive. (Indeed)	Typically 3 years or more in relevant field. (Indeed)	Certifications like CEH, Security+, OSCP etc. may be requested or seen as advantage. (ZipRecruiter)

4. Resources to Further Your Career

a. Certifications commonly required / mentioned

From the job postings and from career guides:

- **CEH (Certified Ethical Hacker)** – frequently mentioned or desirable. (ZipRecruiter)
- **CompTIA Security+** – considered a good foundation as entry-level. (ZipRecruiter)
- **OSCP (Offensive Security Certified Professional)** – more advanced, but often the "gold standard" for technical credibility. (Coursera)
- Some job descriptions list vendor / product / cloud certifications or "nice to have" certifications.
- Entry level / junior roles sometimes ask for or favour **eJPT** for hands-on early skills. (INE)

b. Training options for those certifications

- **INE's eJPT** (Junior Penetration Tester) by INE Security: entry level, hands-on. (INE)
- Online platforms: Coursera, TryHackMe, TryHackMe's career paths; cybersecurity bootcamps. (TryHackMe)
- Self-study / labs: use tools like Kali Linux, virtual labs, capture-the-flag (CTF) challenges, Hack The Box, etc.
- Formal education: Degrees in Computer Science, Information Security, Networking often help. (CyberDegrees)

---

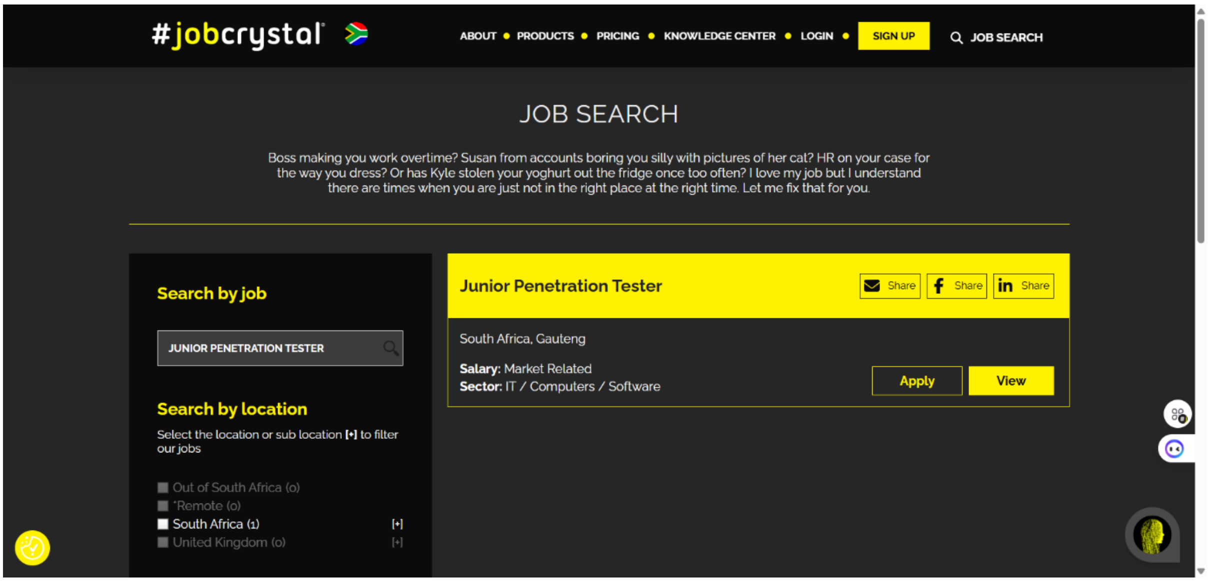
5. Reflection & Analysis

Reflection Questions

1. **Do you find that jobs are concentrated in any one area, or are they distributed?**
   - Many job postings that require penetration testing are concentrated in major cities (Johannesburg, Pretoria, Cape Town) in South Africa. Also a number are remote or allow remote work. (www.pnet.co.za)
   - Some roles are with consulting / security firms; others are in-house for companies. So, there is some distribution by employer type.
   - The level of required experience tends to skew toward intermediate (3-5 years), even for roles labeled "junior" or "entry level," which suggests that many companies expect prior relevant experience or demonstrable skills.
2. **What are the most common duties mentioned?**
   Some recurring duties across job postings include:
   - Performing vulnerability assessments / penetration testing of networks, applications, servers.
   - Using tools for scanning / exploitation (e.g. Nmap, Wireshark, Burp Suite, Metasploit).
   - Reconnaissance / information gathering.
   - Reporting findings clearly (both technically and to management).
   - Working under guidance of senior pentesters.
   - Keeping up with threat intelligence, security tools, and new vulnerabilities.

6. Screenshots Evidence

- Junior Penetration Tester



JOB SEARCH

Boss making you work overtime? Susan from accounts boring you silly with pictures of her cat? HR on your case for the way you dress? Or has Kyle stolen your yoghurt out the fridge once too often? I love my job but I understand there are times when you are just not in the right place at the right time. Let me fix that for you.

Search by job

JUNIOR PENETRATION TESTER

Search by location

Select the location or sub location [+] to filter our jobs

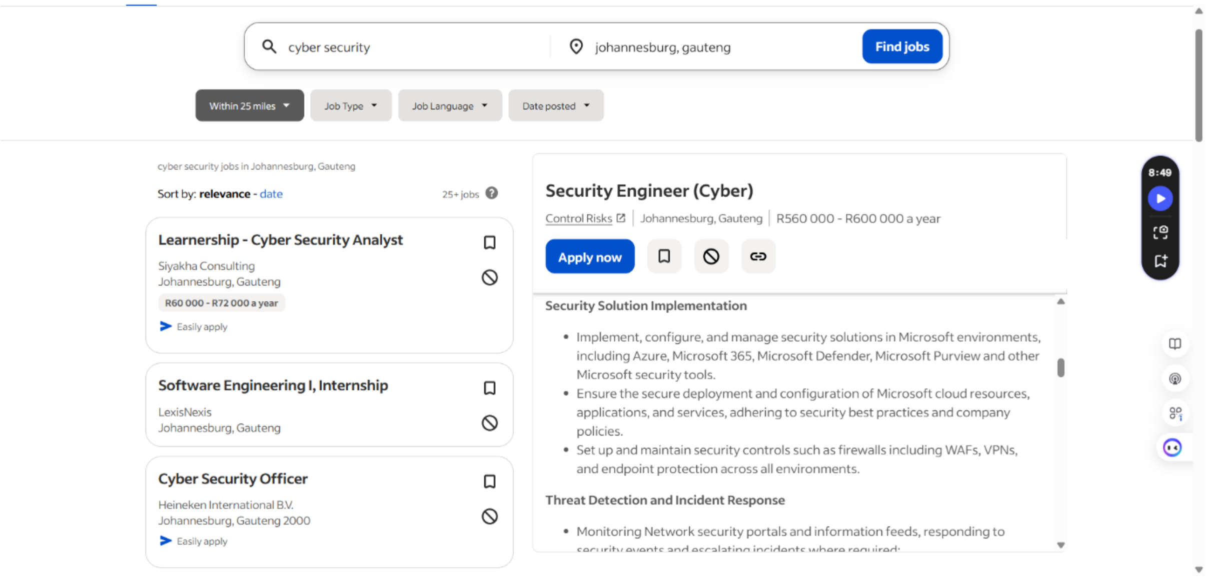
□ Out of South Africa (0)
□ *Remote (0)
□ South Africa (1) [+]
□ United Kingdom (0) [+]

Junior Penetration Tester

South Africa, Gauteng

Salary: Market Related
Sector: IT / Computers / Software

- Screenshot of job board showing “Cyber Security Specialist” role in SA.



cyber security jobs in Johannesburg, Gauteng

Sort by: **relevance** - date 25+ jobs

Learnership - Cyber Security Analyst
Siyakha Consulting
Johannesburg, Gauteng
R60 000 - R72 000 a year
Easily apply

Software Engineering I, Internship
LexisNexis
Johannesburg, Gauteng

Cyber Security Officer
Heineken International B.V.
Johannesburg, Gauteng 2000
Easily apply

Security Engineer (Cyber)

Control Risks | Johannesburg, Gauteng | R560 000 - R600 000 a year

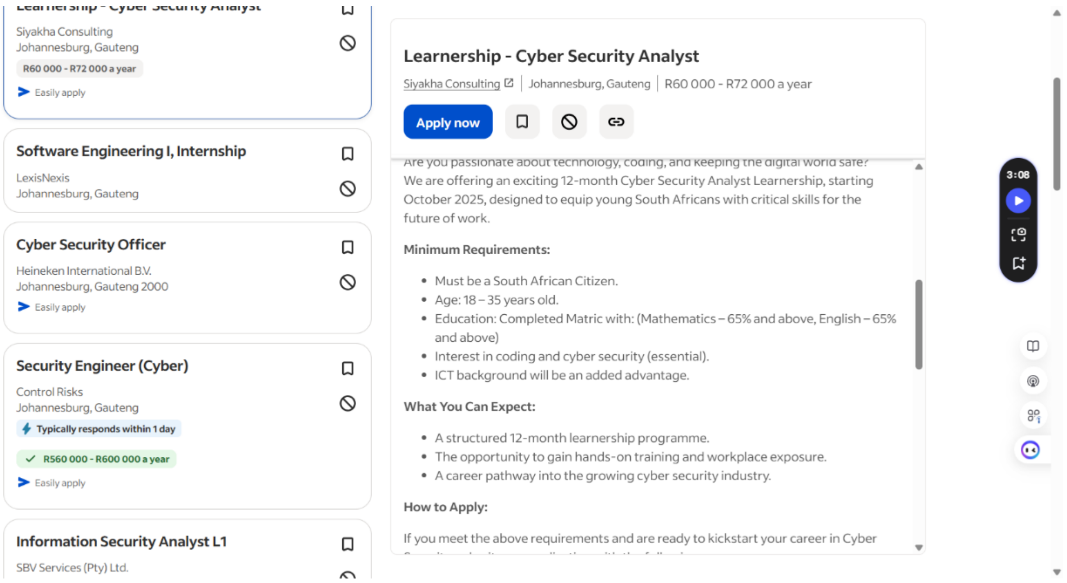
Security Solution Implementation

- Implement, configure, and manage security solutions in Microsoft environments, including Azure, Microsoft 365, Microsoft Defender, Microsoft Purview and other Microsoft security tools.
- Ensure the secure deployment and configuration of Microsoft cloud resources, applications, and services, adhering to security best practices and company policies.
- Set up and maintain security controls such as firewalls including WAFs, VPNs, and endpoint protection across all environments.

Threat Detection and Incident Response

- Monitoring Network security portals and information feeds, responding to security events and escalating incidents where required:

- Screenshot of requirements for learnship programs for Cyber



Learnership - Cyber Security Analyst
Siyakha Consulting
Johannesburg, Gauteng
R60 000 - R72 000 a year
Easily apply

Software Engineering I, Internship
LexisNexis
Johannesburg, Gauteng

Cyber Security Officer
Heineken International B.V.
Johannesburg, Gauteng 2000
Easily apply

Security Engineer (Cyber)
Control Risks
Johannesburg, Gauteng
Typically responds within 1 day
✓ R560 000 - R600 000 a year
Easily apply

Information Security Analyst L1
SBV Services (Pty) Ltd.

Learnership - Cyber Security Analyst

Siyakha Consulting | Johannesburg, Gauteng | R60 000 - R72 000 a year

Apply now

Are you passionate about technology, coding, and keeping the digital world safe? We are offering an exciting 12-month Cyber Security Analyst Learnership, starting October 2025, designed to equip young South Africans with critical skills for the future of work.

Minimum Requirements:

- Must be a South African Citizen.
- Age: 18 – 35 years old.
- Education: Completed Matric with: (Mathematics – 65% and above, English – 65% and above)
- Interest in coding and cyber security (essential).
- ICT background will be an added advantage.

What You Can Expect:

- A structured 12-month learnership programme.
- The opportunity to gain hands-on training and workplace exposure.
- A career pathway into the growing cyber security industry.

How to Apply:

If you meet the above requirements and are ready to kickstart your career in Cyber

7. References

- Indeed, Glassdoor, LinkedIn, Pnet job-boards (various job posts) (Indeed)
- Coursera "How to Become a Penetration Tester: 2025 Career Guide" (Coursera)
- TryHackMe "Becoming a Penetration Tester" career path (TryHackMe)
- INE eJPT Certification page (INE)
- Infosec Institute's "Degree vs Certification" guide (Infosec Institute)