National University
Of Computer and Emerging Sciences

Assignment-02

In partial
fulfillment of the requirements
for the course of

FA2024-SS2007

Technical and Business Writing

By:

Maryam Masood
22i-1169
BSCS-C

Resume

Maryam Masood
Email: i221169@nu.edu.pk | Phone: 923038018095
LinkedIn: www.linkedin.com/in/maryam-masood-694b412a8

Career Objective

Driven and detail-oriented Computer Science student specializing in cybersecurity and ethical hacking. Skilled in conducting vulnerability assessments, penetration testing, and analyzing security systems. Eager to apply hands-on experience with security protocols and tools to protect critical infrastructure at Tier3 Cyber Security Services.

Education

Bachelor of Science in Computer Science
FAST NUCES Islamabad
Expected Graduation: June 2026

ICS
Scholars Science College, Wah Cantt
June 2020 - May 2022

Matriculation
Margalla Grammar School, Wah Cantt
May 2018 - May 2020

Relevant Coursework: Cybersecurity, Ethical Hacking, Network Security, Cryptography, Advanced Programming

---

Technical Skills

- **Security Tools:** Kali Linux, Metasploit, Burp Suite, Wireshark, Nmap
- **Programming Languages:** Python, C++, C#, Bash
- **Network Protocols:** TCP/IP, DNS, HTTP, SSL/TLS
- **Vulnerability Assessment:** OWASP Top 10, SQL Injection, XSS, CSRF
- **Operating Systems:** Linux (Kali, Ubuntu), Windows

Experience

Penetration Tester Intern
Vizz Web Solutions | Islamabad, Pakistan
October 2023 – August 2024

- Conducted penetration tests on web applications and network systems to identify and exploit vulnerabilities.
- Collaborated with IT teams to remediate security risks, improving security posture by 30%.
- Utilized Metasploit and Burp Suite for vulnerability detection and demonstrated remediation strategies.
- Applied knowledge of the OWASP Top 10 security vulnerabilities to perform comprehensive penetration tests on web applications.

Security Analyst Intern
SecureIT Innovations | Remote
January 2023 – September 2023

- Monitored network traffic to detect and analyze potential threats.
- Developed and automated scripts to streamline vulnerability scanning and reporting.
- Assisted in resolving a variety of security incidents, reducing response time by 25%.

Projects

Personal Penetration Testing Lab

- Set up a home lab using Kali Linux and VirtualBox to practice penetration testing techniques, including privilege escalation, SQL injection, and cross-site scripting.

Mock Web Application Security Assessment

- Conducted a full penetration test on a sample web application, identifying vulnerabilities in SQL injection, XSS, and authentication flaws. Provided a detailed report with remediation steps.

Certifications

- CompTIA Security+ (2023)
- Certified Ethical Hacker (CEH) (2024)

References

Available upon request.

Cover Letter

Maryam Masood
House#346 Phase 1 Extension, Wah Model Town, Wah Cantt
i221169@nu.edu.pk
923038018095
November 7, 2024

Hiring Manager
Tier3 Cyber Security Services
Street 26, F-10
Islamabad, Pakistan

Dear Hiring Manager,

I am excited to submit my application for the Penetration Tester position at Tier3 Cyber Security Services, as advertised on your company's career portal. With a solid foundation in cybersecurity and hands-on experience in ethical hacking, I am enthusiastic about the opportunity to contribute to Tier3 Cyber Security Services' mission of securing critical digital assets.

In my recent internship at Vizz Web Solutions, I conducted penetration tests on internal systems and web applications, detecting and mitigating high-impact vulnerabilities. I used tools like Metasploit, Burp Suite, and Wireshark to assess system integrity and collaborated with the IT team to implement security improvements that reduced vulnerabilities by 30%. This experience honed my skills in identifying security gaps and deepened my understanding of effective vulnerability management.

Additionally, I have developed a personal penetration testing lab to continually refine my skills and stay current with evolving cybersecurity threats. This hands-on approach has provided me with expertise in areas such as SQL injection, cross-site scripting, and network scanning. I am confident that my proactive attitude toward learning and commitment to cybersecurity would make me a valuable asset to your team.

Thank you for considering my application. I look forward to the opportunity to discuss how my skills and experiences align with the needs of Tier3 Cyber Security Services. Please feel free to contact me at your convenience.

Sincerely,
Maryam Masood

Reflection

The Chain of Thought (CoT) process significantly enhanced my ability to logically break down the various tasks involved in crafting my resume and cover letter. By using a structured approach, I was able to align each section of my documents with the specific needs of the job description for the Penetration Tester role at Tier3 Cyber Security Services.

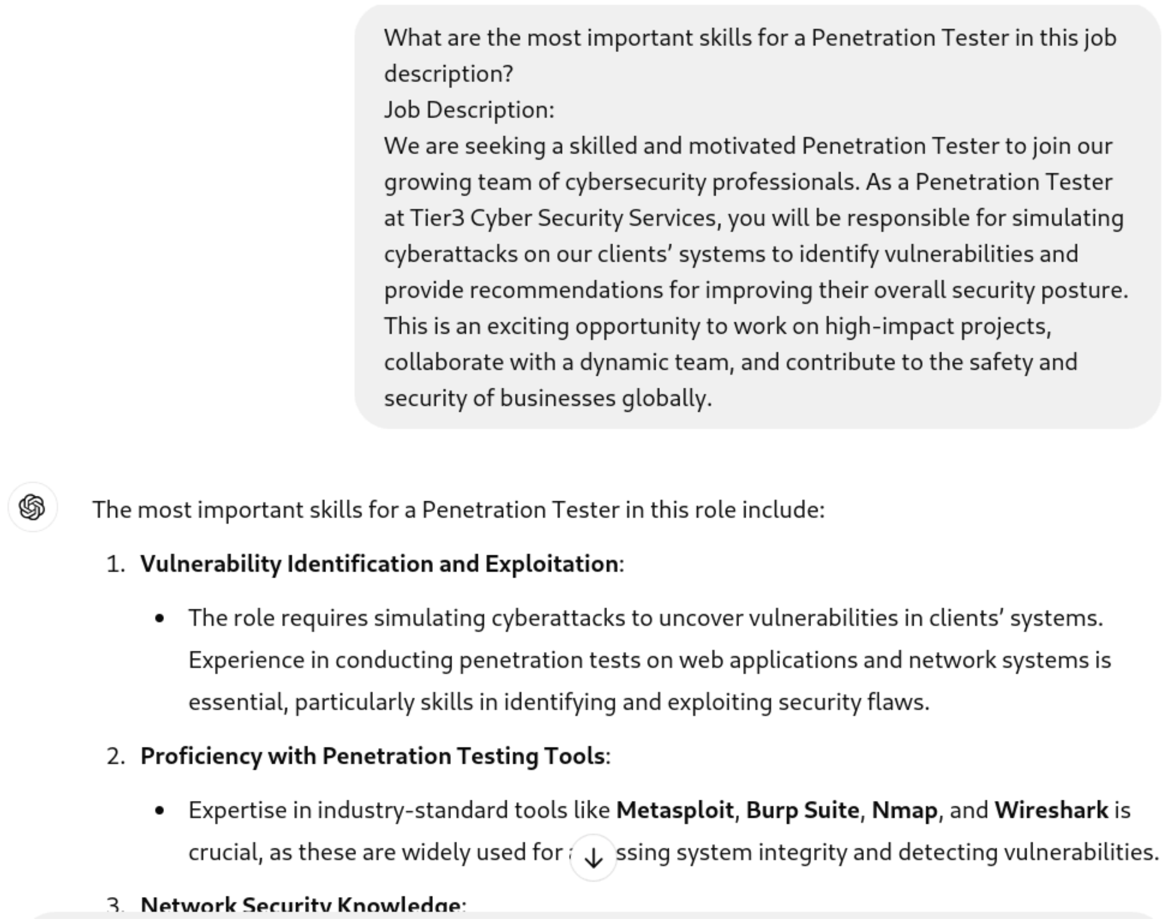
Breaking Down Tasks Logically with CoT: The most valuable lesson I learned from the CoT process was the importance of analyzing each job requirement and how it directly connects to my skills and experiences. For instance, instead of simply listing my skills, I carefully examined how each skill aligned with the responsibilities of the job. This methodical approach ensured that my resume and cover letter were not only comprehensive but also relevant.

How AI Supported or Clarified My Thinking: AI played a critical role in helping me organize my thoughts and refine the language in my resume and cover letter. For example, when reflecting on how to phrase my achievement in reducing security vulnerabilities by 30%, AI helped me craft a concise bullet point that effectively communicated the impact of my work. Additionally, AI assisted in framing my skills and experiences in a way that was clear and professional, especially when it came to describing my proactive learning approach, such as setting up a personal penetration testing lab. By prompting me to think through each section, AI provided clarity in terms of both content and structure.

CoT Prompting's Role in Creating a More Targeted Resume and Cover Letter: The CoT prompting process allowed me to craft a more targeted resume and cover letter by ensuring every element was tailored to the job. It made me consider not just what I had done but how it specifically matched the role’s requirements. This led to the creation of more compelling, purpose-driven statements. For example, in my cover letter, I used CoT to reflect on the company’s values and mission and how my skills in ethical hacking align with their commitment to securing critical assets. I also emphasized my hands-on experience with penetration testing tools and my proactive approach to learning, both of which are central to the role.

Overall, the CoT process helped me develop a more focused and impactful application package. By breaking down each requirement logically, seeking clarity through AI, and aligning my qualifications with the job’s needs, I was able to present myself as a highly suitable candidate for the Penetration Tester role.

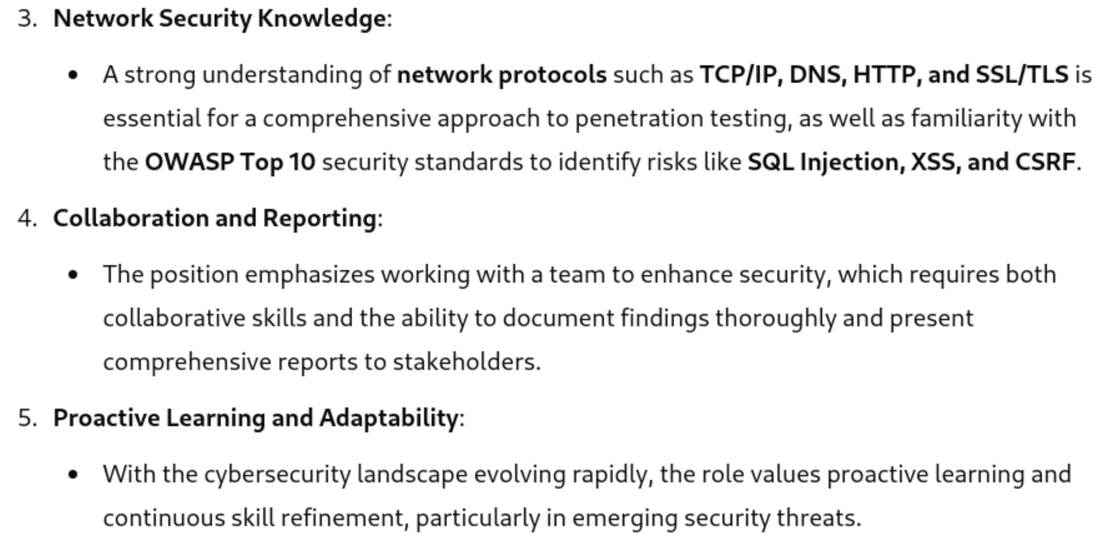
Chain of Thought Prompting



What are the most important skills for a Penetration Tester in this job description?
Job Description:
We are seeking a skilled and motivated Penetration Tester to join our growing team of cybersecurity professionals. As a Penetration Tester at Tier3 Cyber Security Services, you will be responsible for simulating cyberattacks on our clients' systems to identify vulnerabilities and provide recommendations for improving their overall security posture. This is an exciting opportunity to work on high-impact projects, collaborate with a dynamic team, and contribute to the safety and security of businesses globally.

The most important skills for a Penetration Tester in this role include:

1. **Vulnerability Identification and Exploitation**:
    - The role requires simulating cyberattacks to uncover vulnerabilities in clients' systems. Experience in conducting penetration tests on web applications and network systems is essential, particularly skills in identifying and exploiting security flaws.
2. **Proficiency with Penetration Testing Tools**:
    - Expertise in industry-standard tools like **Metasploit**, **Burp Suite**, **Nmap**, and **Wireshark** is crucial, as these are widely used for a ssing system integrity and detecting vulnerabilities.
3. **Network Security Knowledge**:



3. **Network Security Knowledge**:
    - A strong understanding of **network protocols** such as **TCP/IP, DNS, HTTP, and SSL/TLS** is essential for a comprehensive approach to penetration testing, as well as familiarity with the **OWASP Top 10** security standards to identify risks like **SQL Injection, XSS, and CSRF**.
4. **Collaboration and Reporting**:
    - The position emphasizes working with a team to enhance security, which requires both collaborative skills and the ability to document findings thoroughly and present comprehensive reports to stakeholders.
5. **Proactive Learning and Adaptability**:
    - With the cybersecurity landscape evolving rapidly, the role values proactive learning and continuous skill refinement, particularly in emerging security threats.

In my resume, how can I describe my experience with Metasploit to show my effectiveness in penetration testing?

To describe your experience with **Metasploit** in a way that highlights your effectiveness in penetration testing, you can structure your bullet point to demonstrate the impact of using the tool, your proficiency with it, and the results of your actions. Here's an example based on your experience:

- **Utilized Metasploit during penetration tests to identify, exploit, and remediate vulnerabilities in web applications and network systems, resulting in a 30% improvement in the security posture of the organization.**

This bullet point effectively shows that you used Metasploit to find and exploit vulnerabilities while quantifying the positive outcome of your actions.

What's a powerful way to phrase my achievement in reducing security vulnerabilities by 30% during my internship? (in a bullet point)

A powerful way to phrase your achievement in reducing security vulnerabilities by 30% during your internship could be:

- **Collaborated with the IT team to conduct penetration tests, identify critical vulnerabilities, and implement remediation strategies, resulting in a 30% reduction in security risks across internal systems and web applications.**

This bullet point emphasizes your teamwork, the proactive measures you took, and the measurable outcome of your efforts.

What’s a good way to highlight my knowledge of the OWASP Top 10 in a resume bullet?

To highlight your knowledge of the **OWASP Top 10** in a resume bullet, focus on how you applied that knowledge in real-world scenarios, such as identifying and mitigating vulnerabilities. Here’s an example:

- **Applied knowledge of the OWASP Top 10 security vulnerabilities (e.g., SQL Injection, XSS) to perform comprehensive penetration tests on web applications, identifying critical flaws and providing actionable recommendations for remediation.**

This bullet clearly shows your understanding of the OWASP Top 10 and how it was used to improve security in practical situations.

How can I open my cover letter to show enthusiasm for a cybersecurity role with Tier3 cyber security services?

Here’s a strong way to open your cover letter to express enthusiasm for the cybersecurity role with Tier3 Cyber Security Services:

"I am excited to apply for the Penetration Tester position at Tier3 Cyber Security Services, as advertised on your career portal. With a strong foundation in cybersecurity and hands-on experience in penetration testing, I am eager to contribute to your mission of protecting critical digital assets. Your company's commitment to innovation and security aligns perfectly with my passion for ethical hacking and my drive to safeguard businesses against evolving cyber threats."

This opening effectively conveys your enthusiasm for the role, aligns your passion with the company’s values, and sets the tone for a focused, engaging cover letter.

How can I highlight my proactive learning approach, like creating a personal penetration testing lab, in my cover letter?

Here’s a way to highlight your proactive learning approach and your personal penetration testing lab in your cover letter:

"In addition to my formal education and internships, I have taken the initiative to build a personal penetration testing lab using Kali Linux and VirtualBox. This hands-on lab allows me to practice and refine my skills in areas like privilege escalation, SQL injection, and cross-site scripting. By continually challenging myself with new security scenarios, I ensure that I stay up-to-date with the latest threats and tools in cybersecurity, demonstrating my commitment to constant learning and improvement."

What’s a good way to summarize my motivation and unique strengths for this role in the closing paragraph of my cover letter?

Here’s a strong way to summarize your motivation and unique strengths in the closing paragraph of your cover letter:

"I am confident that my hands-on experience with penetration testing, coupled with my proactive learning approach and passion for cybersecurity, would make me a valuable asset to Tier3 Cyber Security Services. I am excited about the opportunity to contribute to your team and help safeguard the digital assets of your clients. I look forward to the opportunity to discuss how my skills and experiences align with your needs, and I am eager to bring my expertise in ethical hacking to your organization."