Anees Ahmad

linkedin.com/in/aneesahmad | aneesahmed2859@gmail.com | +44.7507.834.357

Summary

Cybersecurity graduate with expertise in network security, digital forensics, and penetration testing. Experienced in vulnerability assessments, incident response, and regulatory compliance (PCI DSS, ISO 27001, NIST CSF). Proficient in Windows/Linux systems.

Work Experience

Freelancer Aug 2022 - Oct 2024

As a freelancer, I delivered over 65 successful cybersecurity projects with a 4.9/5 client rating and 90 percent success rate. My work covered vulnerability management, penetration testing, digital forensics, compliance, and incident response, consistently helping clients strengthen defenses and reduce exposure to cyber threats.

I have extensive experience in conducting vulnerability assessments using CVSS 3.0, delivering detailed reports to help organizations understand and prioritize risks. My penetration testing engagements followed a hybrid approach of manual testing combined with automated scanning tools, leveraging technologies such as Tenable Nessus, OWASP ZAP, Wireshark, Metasploit, Hydra, SQLmap, and Nmap to uncover and validate security gaps.

In digital forensics, I analyzed compromised systems with Autopsy and FTK Toolkit, uncovering attacker activity, user behavior, and file metadata. These investigations improved incident resolution times by an average of 30 percent. I also performed OSINT investigations with Maltego and audio forensics with Audacity, providing reliable evidence for clients.

I guided organizations through compliance with PCI DSS, ISO 27001, NIST CSF, SOC 2, and OSFI, creating tailored roadmaps that accelerated audit readiness and closed gaps in security controls. My work helped clients achieve regulatory alignment more efficiently while building sustainable security practices.

I managed log analysis and incident response for hosting providers under large-scale bot attacks. By implementing defensive strategies and traffic controls, I reduced downtime by over 50 percent, restored critical services, and deployed preventive measures that safeguarded future operations.

Cyber Security Internship 06-weeks July 2023 - Aug 2023

During my cybersecurity internship, I gained hands-on experience in firewall management, including creating and applying security policies to control and filter network traffic. I also worked with Active Directory and Group Policy Objects (GPOs), implementing access management and security controls to enforce cybersecurity best practices across users and systems.

My role involved exposure to server and network administration through virtualization platforms such as VMware ESXi and Microsoft Hyper-V, where I learned to manage server resources and handle network traffic effectively. I also worked with Kaspersky Small Business Security and CPanel, gaining practical skills in endpoint protection, account management, and server control.

This internship provided me with a solid foundation in network security, system administration, and access management, while reinforcing key concepts in cybersecurity governance and best practices.

Projects

IoT Based Intelligent Honeypot
I developed an IoT-based intelligent honeypot to detect DDoS and brute-force attacks using a Random Forest classifier with 78.54 percent accuracy. The system was deployed as a single IoT node using three sensors (humidity, temperature, and smoke) connected to an Arduino Uno, with a light alert to simulate real-world device behavior. The honeypot attracted attacker activity and captured critical information, including IP addresses, timestamps, request counts, usernames, password attempts, and other access patterns.
The machine learning model was implemented in Python, with feature selection applied to optimize detection accuracy. This project demonstrated practical threat detection in resource-constrained IoT environments, providing actionable insights into attacker behavior and IoT security vulnerabilities
For real time Attacks i have used tools like LOIC and Slowloris for DDoS attack and hydra for brute force attack from kali Linux on honeypot and honeypot shared logs real-time on the web based front end..

Bots Traffic Analysis and Mitigation on Server
I worked on a project where a client reported that their website was down and believed they were under a Distributed Denial of Service (DDoS) attack. After analyzing the server logs, I discovered that the issue was not a traditional DDoS but rather a massive influx of automated bot traffic coming from multiple sources, including Googlebot, Bingbot, OpenAIBot, YandexBot, and others. These bots were aggressively scraping data, likely for purposes such as search indexing and AI models training, which caused the server to become overloaded and the website unavailable.
To resolve the issue, I conducted a detailed investigation, differentiated between legitimate crawlers and harmful automated activity, and recommended effective mitigation strategies. This included applying rate limiting, configuring robots.txt to manage bot access, and implementing Web Application Firewall (WAF) rules to control traffic without blocking essential search engine crawlers.

Vulnerability Assessment and Penetration Testing (VAPT) - NAQDE.NET
Conducted a comprehensive vulnerability assessment and penetration test on two production servers to evaluate the organization's IT security posture. The assessment combined automated scanning and manual testing techniques following OWASP, CVSS 3.0, and PCI-DSS standards. Tools used included Nmap, Nessus, OWASP ZAP, Metasploit, Wireshark, SQLMap, and Hydra.
The engagement identified one high-risk vulnerability involving PII exposure, several medium-risk issues (e.g., missing CSRF tokens, weak Content Security Policy, outdated jQuery library, TLS 1.1 support, and certificate misconfigurations), and multiple low-risk misconfigurations (e.g., insecure cookies, error disclosures, private IP exposure). Exploitation testing verified the potential impact of these findings in a safe and controlled manner.
Delivered a detailed report with prioritized recommendations, including implementing anti-CSRF protections, enforcing HTTPS, upgrading libraries, hardening SSL/TLS configurations, and securing sensitive data handling. The overall risk level was classified as Medium, and the remediation roadmap provided the client with clear steps to reduce attack surface, strengthen compliance posture, and prevent data leakage.

DDoS Attack Incident Analysis and Mitigation – BACT Consultation
During my project with BACT Consultation, I assisted in investigating a Denial-of-Service (DoS) attack that targeted the company website from 5 February 2024 to 6 February 2024, causing an outage of approximately 34 hours. I helped analyze server logs and traffic patterns to identify the attack vectors, which involved a massive influx of HTTP requests that overwhelmed server resources and blocked legitimate user access.
As part of the recovery process, I helped implement mitigation measures, including removing malicious code, performing thorough malware scans, and verifying server functionality to restore normal operations. I also contributed to developing strategic recommendations to enhance the company's cybersecurity posture, such as deploying Web Application Firewalls (WAF), implementing application layer security, enabling two-factor authentication (2FA), IP whitelisting and maintaining regular backups.

Education

2025 - present	MS in Computer Science and Technology at **Ulster University**	(GPA: in-progress)
2020 - 2024	Bachelor's Degree in Cyber Security **Air university**	(GPA: 2.8/4.0)
2018 - 2020	Class 12th Punjab Group of colleges	(A)
2016 - 2018	Class 10th The Punjab School	(A+)

Certifications

Networking	Cisco Networking Academy, 2025.
Ethical Hacker	Cisco Networking Academy, 2025.
Hacking and Penetration Testing Lab	EC-Council, 2025.
Ethical Hacking Essentials	EC-Council, 2024.
Digital Forensics Essentials	EC-Council, 2024.
Cyber Security Internship	Pakistan Aeronautical Complex Kamra, 2023.

Skills

Vulnerability Assessment
Penetration Testing
Network Security
Networking
Cryptography
Digital Forensics
Incident Response
Python
C++
C
Logs Analysis
Information Security
Windows
Linux
Microsoft 365