Tomiwa Oladejo

Milton Keynes, Buckinghamshire | +44 7342897651 | tommdej@gmail.com

Profile

A recent graduate with a robust academic foundation and hands-on expertise in information systems, network security, and threat mitigation strategies. Demonstrates proficiency in diverse operating systems, state-of-the-art security tools, and sophisticated incident response protocols. Adept at identifying vulnerabilities and implementing strategic remediations, with a methodical and detail-oriented approach. Exceptional communication and collaborative skills which complement a commitment to continuous professional development and innovation in cybersecurity practices.

Education

Nottingham trent university, Nottingham| September 2020 – July 2023

- BSc (Hons) Computer Systems (Cyber Security) – Graduated with a 2:1

Project Experience

Email spam filter (Final year project)

- Engineered a deep learning-based email spam filter using TensorFlow and Keras, implementing a neural network with embedding, flatten, and dense layers to classify spam and non-spam messages with high accuracy.
- Applied advanced NLP techniques including tokenization, stop-word removal, and punctuation stripping to pre-process text data, ensuring optimized input for the model and improved classification performance.
- Evaluated model performance using accuracy and AUC metrics; demonstrated the model's ability to generalize by successfully predicting spam in previously unseen data, highlighting practical application for real-world email security systems.

Vulnerability assessment and penetration testing

- Conducted in-depth vulnerability assessments using tools such as OpenVAS, Nmap, and Metasploit to identify and exploit network weaknesses including UnrealIRCd backdoors, weak PostgreSQL credentials and Java RMI misconfigurations.
- Collaborated effectively within a team to set up a secure virtual network environment using Kali Linux and Metasploitable, ensuring consistent communication and smooth task delegation through strategy.
- Proposed and documented comprehensive network security improvements, including firewall configurations and the deployment of SNORT IDS/IPS, demonstrating a strong understanding of practical defence mechanisms and incident response.

Information security management system portfolio

- Designed and implemented an ISMS in response to Alibaba's 2019–2020 data breach, addressing vulnerabilities from malicious web scraping of 1.1 billion records. Proposed layered technical, procedural, and physical safeguards.
- Developed cybersecurity strategies including IDS deployment, data classification policies, and encryption protocols, ensuring compliance with China's PIPL and enabling real-time threat monitoring.

- Translated technical risks into business impacts for stakeholders, highlighting reputational and financial consequences. Delivered tailored solutions that strengthened Alibaba's long-term security posture.

Denial of service attacks with mitigations

- Conducted a comprehensive study on Distributed Denial of Service (DDoS) attacks targeting the OSI model's transport (Layer 4) and application (Layer 7) layers, including SYN flood, UDP flood, HTTP flood, and Slowloris attacks.
- Analysed and compared advanced mitigation techniques such as TCP SYN cookies, ingress/egress filtering, web application firewalls, and reverse firewall mechanisms to evaluate their effectiveness against various attack vectors.
- Performed a structured literature review using reputable databases (IEEE Xplore, Google Scholar, ScienceDirect) to synthesize current academic perspectives, assess threats to research validity, and support evidence-based cybersecurity recommendations.

Computer Forensics and Investigation

- Conducted a smartphone forensic investigation using Cellebrite Physical Analyzer, extracting physical and logical images to uncover evidence of premeditated theft.
- Analyzed communications, search history, and geolocation metadata to confirm suspect's intent, presence at the scene, and behavioral motives tied to financial stress.
- Recovered hidden data via hex analysis, built a detailed activity timeline, and compiled a court-admissible forensic report linking digital evidence to criminal planning.

Skills & Abilities

- Security Tools: Nmap, Firewalls, IDS/IPS.
- Networking: Network Protocol Analysis, Traffic Monitoring and Incident Response Coordination.
- Cybersecurity Expertise: Threat Detection, Comprehensive Vulnerability Management, Structured Incident Handling
- Programming & Scripting: Python and Java
- Tools and Platforms: Linux (Kali, Ubuntu), VMWare, Metasploit, Wireshark, Autopsy, Cellebrite.
- Professional Attributes: Exceptional communication, critical problem-solving, efficient time management, and meticulous attention to detail.

Additional Information

- Engaged in ongoing research to remain at the forefront of emerging cybersecurity threats and mitigation techniques.
- Working towards Certification in CompTIA Security+