Raheem Moore

Arlington, Texas| 214-436-9667|Codeheem@gmail.com| LinkedIn | https://github.com/Dokkaem

Holder of CompTIA Pentest certificate and Google IT Support Professional Certificate with practical experience from TryHackMe. Knowledgeable in various data structures and algorithms, combined with exemplary understanding of cybersecurity framework. Demonstrated ability to analyze vulnerabilities, mitigate risks, and troubleshoot technical issues. Ready to contribute to cybersecurity, IT, or pentesting teams with strong problem-solving skills and a passion for continuous learning.

RELEVANT SKILLS & EXPERTISE

Tools/Languages: Linux, SQL (BigQuery), Splunk, WireShark, Tcpdump, Suricata, Python, C++, Java, Go, HTML
Security Practices: Information Security, Network Security, Vulnerability Assessment, Threat Analysis, Log Analysis, Security Frameworks and Controls, Packet Analysis, Network Penetration Testing
Software Platforms: Google Workspace, Slack,Zendesk, WireShark, Greenbone, VMware, Metasploit, Burpsuite
Strengths: Problem-Solving, Collaboration, Attention to Detail, Calmness Under Pressure, Customer Service, Operational Efficiency

CYBERSECURITY PROJECTS

TryHackMe Rooms: Utilized interactive, gamified virtual environment to enhance practical knowledge and hands-on skills:

- **Linux Fundamentals** (1, 2, & 3) and **Linux Strength Training** - Navigated directories and files, adjusted permissions, analyzed logs, explored common utilities
- **Intro to Logs** and **Log Analysis** - Identified log types, located logs, employed regular expressions (RegEx), and utilized command line and CyberChef for effective log analysis
- **Wireshark Basics** and **Wireshark 101** - Gained proficiency in packet dissection, navigation, and filtering techniques; analyzed ARP, ICMP, TCP, DNS, HTTP, and HTTPS traffic for network troubleshooting and security analysis
- **Windows Fundamentals** (1, 2, & 3) and **Windows Forensics** (1 & 2) - Acquired fundamental understanding of Windows, including file systems, user account control (UAC), control panel, system configuration, security, firewall, registry, and FAT/NTFS file systems; developed skills in accessing hives, utilizing registry explorer, and recovering files
- **Splunk Basics**, **Incident Handling with Splunk**, and **Splunk** (2 & 3) - Developed skills in navigating Splunk; conducting incident handling using Splunk; participated in the Boss of the SOC investigation for security analysis

Raspberry Pi Zero: Is a small computer that is used for various projects and applications:

- **Installing Kali linux to communicate ssh** - Developed skills on how to install kali linux onto a device. Then effectively applied appropriate security measures to allow communication via ssh from the Raspberry to a mobile device (like a smartphone) with applications like juiceSSH
- **Created homebrewed scripts** - Applied knowledge with Python and GO to write various scripts to automate task and create programs ie keyloggers, TCP scanner ,MD5/SHA-256 cracker, and building middleware
- **Database miner** - Using GO created a program that could extract information from SQL and NoSQL databases, core functionality of the program was its ability to connect and interact with these databases

RELEVANT TECHNOLOGY EXPERIENCE

Regency Technology -Arlington, Texas **09/2022 - 04/2023**

- Tasked with servicing and repairing various electronics, including PCs and cell phones, to resolve software errors, fix damaged hardware, and upgrade outdated components.
- Repaired damaged hardware components, such as screens, keyboards, batteries, and motherboards, ensuring devices were restored to full functionality.
- Maintained detailed records of repairs, upgrades, and diagnostics performed on each device, ensuring accurate tracking and reporting for clients.
- Resolved hardware issues for 30+ workstations, achieving a 95% success rate in restoring functionality and minimizing downtime, showcasing adeptness in hardware troubleshooting and repair.
- Collaborated with senior technicians to execute system upgrades, contributing to a 20% enhancement in system performance and user experience, displaying willingness to learn and adapt to new technologies.

Quickstart Cybersecurity Bootcamp **01/2022 - 07/2022**

- Conducted research on emerging cyber threats and trends, analyzing industry reports and case studies, staying abreast of the latest developments in the cybersecurity landscape and enhancing knowledge base.
- Collaborated with peers on simulated cyber attack scenarios, participating in threat analysis and mitigation exercises, contributing to team success, and fostering a collaborative learning environment.
- Implemented security protocols and best practices on personal projects, reducing vulnerabilities by 30% and ensuring data integrity and confidentiality, showcasing practical application of cybersecurity principles.
- Led cross-functional teams in the design and implementation of access control policies, achieving 100% compliance with industry standards and regulations.

PLR Electronics-Fort Worth, Texas **03/2020 - 07/2022**

- Diagnosed and resolved complex technical issues for diverse electronic systems, demonstrating adept problem-solving skills and attention to detail
- Collaborated with engineers to execute comprehensive maintenance plans, ensuring optimal performance and minimizing system failures.
- Provided tailored technical support to customers, delivering clear and concise instructions to facilitate problem resolution and enhance user experience.

PROFESSIONAL EXPERIENCE

Sprouts-GrandPrairie, Texas **12/2023 - Present time**

- Implemented inventory management strategies, reducing waste by 20% through meticulous tracking and forecasting techniques, optimizing resource allocation and cost-effectiveness
- Spearheaded customer service initiatives, cultivating a welcoming environment and resolving escalated customer inquiries and complaints with professionalism and empathy, maintaining a satisfaction rating of 95%.
- Utilized analytical skills to assess sales trends and customer preferences, informing product placement strategies and promotional campaigns, leading to a 15% increase in deli department sales

EDUCATION, CERTIFICATES, & CERTIFICATIONS

Bachelor Computer Science • *University of Texas Arlington 3.5 GPA* ***Graduation date: 08/26***

- Included Courses[Programming I-III, CCNA 1-3,Database Programming, Fundamentals of Information Security]
- Programmers write & test code that makes computers and software function correctly.
- Acquired practical skills for understanding and deploying various programming languages in **C, Python, HTML, and Java**
- Experienced various hands on project, on when to apply different data structures for **Trees, Maps, Graphs,** and **Sets**
- Learned core skills through their CCNA courses to build simple LANs, perform basic configurations for routers and switches, and implement IPv4 and IPv6 addressing schemes

Google Cybersecurity Professional Certificate • *Merit America, Virtual* **04/2024**

- Cultivated holistic understanding of cybersecurity's critical role in organizational security, privacy, and success, including how to systematically identify and mitigate risks, threats, and vulnerabilities
- Gained practical experience with **Linux**, **SQL**, **Python** and utilized **SIEM tools**, **IDS**, and **network protocol analyzers** for proactive threat management
- Applied knowledge to real-world scenarios, developing skills in proactive **threat detection** and **response** through completion of dynamic hands-on projects, including: conducting a simulated **security audit**, responding to a **cyber incident**, analyzing **vulnerable systems**, and completing an **incident handler's journal**

Quickstart Cybersecurity Bootcamp • *Virtual* *06/2022*

- Aim to gain foundational and advanced cybersecurity knowledge, hands-on experience, and industry-recognized certifications.
- Performed regular vulnerability assessments using tools like Nessus and OpenVAS to identify and remediate security weaknesses in simulated environments.
- Executed penetration testing using tools such as Metasploit and Burp Suite, identifying critical vulnerabilities and documenting findings.
- Participated in incident response drills, developing skills in threat detection, analysis, and mitigation using SIEM tools like Splunk and ELK Stack.
- Configured and secured networks with firewalls, VPNs, and intrusion detection/prevention systems (IDS/IPS).
- Applied NIST, ISO 27001, and other cybersecurity frameworks to develop and implement security policies and procedures.