Jefferson T. Yarbah

[**LinkedIn**](https://www.linkedin.com/in/rennie-wendell/) | +91 8050732672 | wendellej9@gmail.com | [**GitHub**](https://github.com/ChroNiCle23/)

**07/31/2024**

# **Professional Summary\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Dedicated cybersecurity professional with a Bachelor's degree in Cybersecurity and 10 months of internship experience. Passionate about leveraging cutting-edge security technologies and best practices to protect organizations from evolving cyber threats. Skilled in network monitoring, vulnerability assessment, and incident response procedures. Adept at collaborating with cross-functional teams to develop and implement robust security policies. Eager to apply academic knowledge and practical skills to a full-time cybersecurity role and contribute to the mission of safeguarding critical systems and data.

# **Technical Skills\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Burp Suite | Postman API | Python | Zeek | Splunk | Object-Oriented Programming (OOP) | Networking Fundamentals (Cisco CLI) | Bash Scripting | Active Directory Penetration Testing | Wireless Attacks (WPA2) | Legal Documentation and Report Writing

# **Experience\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Security Analysts** [**SecIQ**](https://seciqtech.com) **06/2023 – 10/2023**

* Spearheaded risk assessments on company websites to identify potential vulnerabilities
  + Analyzed findings and reported on them to relevant stakeholders. Implemented continuous monitoring strategies to detect emerging vulnerabilities.
  + Developed proactive remediation plans to address identified vulnerabilities. Resulted in a 30% reduction in cybersecurity incidents within the organization
* Conducted network, application, system, and mobile penetration testing across the company's product suite
  + Utilized a variety of tools and techniques to simulate real-world cyber-attacks. Identified weaknesses and potential entry points for malicious actors, provided actionable recommendations for improving security posture
* Completed Practical Ethical Hacking course, gaining proficiency in various areas:
  + Mastered networking fundamentals using Cisco CLI, Acquired introductory knowledge of Linux and Bash scripting.
  + Learned introductory Python 3 for ethical hacking purposes and developed a deep understanding of hacking methodology, reconnaissance, and information gathering techniques
  + Became proficient in scanning, enumeration, and basic exploitation using Metasploit framework

# **Cyber Security Analysts** [**Black Innovations**](https://blackinnovations.ae/) **03/2024 – 06/2024**

* Monitoring and Analysis:
  + Assist in monitoring network traffic and security events using tools such as
  + Splunk, Wireshark, SIEM, IDS/IPS and QRadar. Analyze alerts and logs to identify potential security incidents.
* Incident Response and Vulnerability Assessment:
  + Support the investigation of security incidents and breaches. Participate in the incident response process, helping to mitigate threats and document actions taken.
  + Conduct vulnerability assessments using tools like Nessus and OpenVAS. Assist in performing penetration testing with Metasploit and Burp Suite.
* Completed Practical Ethical Hacking course from:
  + Tryhackme laps
  + Portswigger Laps

# **Cyber Security Specialist** [**Center for Cyber Security Studies & Research**](https://cfcs2r.com/) **04/2024 – 07/2024**

* Windows and Linux Forensics:
  + Disk Imaging, Memory Analysis, Log Analysis, Registry Analysis, File System Analysis, Network Forensics, Rootkit Detection.
  + Tools: FTK Imager, EnCase, Volatility, RegRipper, dd, Log2Timeline, Chkrootkit, rkhunter etc.
* Network Analysis and File hardening:
  + Packet Capture and Analysis, Traffic Flow Analysis, Network Scanning, Intrusion Detection and Prevention, Log Analysis, Performance Monitoring, Behavioral Analysis, File Permissions, Access Control Lists (ACLs), File Encryption, File Integrity Monitoring, Security Policies.
  + Tools: Wireshark, tcpdump, Nmap, NetFlow, Zeek, Snort, Tripwire, SELinux OSSEC and FIM etc.
* Report Findings and Documentation:
  + Creating a detailed report and documentation for findings from network analysis and file hardening is essential for communicating the results, recommendations, and actions to stakeholders.

# **Projects\_\_\_\_­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* **SubScan: (04/2024)**
  + This tool is designed to help with reconnaissance tasks related to discovering subdomains of a given target and checking if the status (live or not) of those subdomains. It provides fast, flexible, and accurate live subdomain identification
  + This tool efficiently fetches subdomains from various sources including Wayback Machine, VirusTotal, URLScan, crt.sh, and HackerTarget.
  + This tool has been created to help Bug bounty hunter, Penetration tester and Ethical hacker in the reconnaissance.
  + View project on [**GitHub**](https://github.com/ChroNiCle23/SubScan)
* **Remote File Integrity Monitoring: (04/2024)**
  + This project contributes to cybersecurity integrity efforts by enabling file integrity monitoring and remote execution capabilities.
  + By proactively monitoring file integrity and facilitating remote management, the script enhances security posture, supports incident detection and response, and assists organizations in meeting compliance requirements in the ever-evolving landscape of cybersecurity threats.
  + It can be used by blue teamers, SOC analysts, and Forensic experts during investigation when comparing the hashes
  + View project on [**GitHub**](https://github.com/ChroNiCle23/Remote-File-Integrity-Monitoring)
* **SecureGuard Keylogger Sentry: (06/2024)**
  + This project "SecureGuard Keylogger Sentry" is a comprehensive security tool tailored for network administrators, system administrators, forensic analysts, and cybersecurity analysts.
  + It offers a suite of features to bolster system defenses, including monitoring keylogging activities, scanning network traffic, tracking system resources, and assessing vulnerabilities.
  + With its ability to provide real-time alerts, detailed logs, and proactive threat detection, SecureGuard enables users to identify and respond to security threats effectively, ensuring the integrity and security of networked environments.
  + View project on [**GitHub**](https://github.com/ChroNiCle23/SecureGuard-Keylogger-Sentry)

# 

# 





# 

# **Certifications\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* [Cisco Certified Support Technician (CCST)](https://www.credly.com/earner/earned/badge/c81b3d50-876f-48dc-b166-c3d12da0b199) | Pearson | 2023
* [IT Specialist - Cybersecurity](https://www.credly.com/earner/earned/badge/ff8bf7d7-a1d8-456b-8bf0-fedb8f836d83) | Cisco | 2023
* [Ethical Hacking Associate | EHA](https://www.credly.com/earner/earned/badge/b79cbe78-3598-487b-aa49-e5f2aec229b7) | EC – Council | 2023
* [Google Cybersecurity](https://coursera.org/verify/professional-cert/9699P2WZYM8Y) | Coursera | 2024

**Education\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Bachelor of Science REVA UNIVERSITY Bengaluru, INDIA 08/2021 – 07/2024**

* **B.Sc in Cybersecurity — GPA : 3.33 / 4**