Charanpreet Singh

India | charanpreet@charanpreet.dev | charanpreet.dev | GitHub

Professional Summary

Cybersecurity Practitioner with extensive coursework in Computer Science and certifications in **CompTIA CySA+, Security+, AWS CCP & ISC2 CC**. Proficient in **Vulnerability Management, Threat Intelligence Gathering, Log Analysis** & **Digital Forensics** using tools such as **Nessus, Elastic, Wireshark, FTK & Eric Zimmerman Tools**. Dedicated to safeguarding digital environments through **continuous learning** and **practical application** of advanced cybersecurity and networking principles.

Certifications

- **CompTIA Security+**
- **CompTIA CySA+ (Cybersecurity Analyst)**
- **AWS CCP (Certified Cloud Practitioner)**

Education

- **Chitkara University**
  Coursework in **Computer Science** (105 credits completed) | GPA 3.73
  Web Development | Computer Networking | Cybersecurity | Cloud Computing

Technical Skills

- **Log Analysis**: Skilled in reviewing and analyzing logs to detect anomalies, track unauthorized access, and identify potential threats using SIEM solutions such as Splunk and ELK stack.
- **Threat Intelligence**: Knowledge of leveraging threat intelligence sources to proactively mitigate risks. Used tools like OpenCTI and VirusTotal to cross-check IPs, domains, and embedded URLs for malicious indicators.
- **Network Monitoring and Troubleshooting**: Proficient in tools like Network Miner and Wireshark for analyzing any suspicious connections being made to endpoint.
- **System Administration**: Skilled in Linux and Windows system administration, including Group Policy management and secure system configurations. Experience in setting up VMs (Flare + REMnux) for malware analysis using VMware, and Hyper-V.
- **Endpoint Security**: Can configure and manage endpoint protection solutions to safeguard devices against malware and unauthorized activities.

Programming and Tools

- **Languages**: Python, Bash, SQL, HTML, CSS, JavaScript

- **Tools**: Nmap, Wireshark, Nessus, Splunk, Elastic, REMnux, Flare-VM, Sysinternals Suite, VirusTotal, Volatility, Autopsy, FTK, Eric Zimmerman Tools
- **Other Skills**: Effective report writing, and documentation for SOC teams

Projects

- **Secure Malware Analysis Lab Setup**
  - Setup an **isolated** and secure environment for malware analysis using **Flare-VM** and **REMnux**, ensuring protection against unintended exposure.
  - Performed **static and dynamic malware analysis** to examine malicious code behavior, leveraging tools to identify critical artifacts and system interactions.
- **Network Traffic Monitoring with Wireshark**
  - Analyzed network packets to detect abnormal patterns and potential threats using Wireshark.
  - Configured and monitored TCP/IP protocols to troubleshoot connectivity issues and ensure secure data transmission.
- **Digital Evidence Acquisition and Analysis**
  - Collected and analyzed forensic artifacts such as disk images, memory dumps, and log files using tools like **FTK**, **Autopsy**, and **Volatility**, ensuring proper evidence handling and chain of custody.
- **Incident Investigation and Timeline Reconstruction**
  - Investigated security incidents by correlating system artifacts, event logs, and user activities to reconstruct attack timelines and identify indicators of compromise.
- **Firewall Management**
  - Configured and maintained firewalls using OPNsense and PFsense, enhancing perimeter security and improving overall network security

Relevant Coursework

- **Network Security**
  Explored principles of network defense, including threat modeling, firewall configurations, and secure protocol implementation. Gained hands-on experience with network vulnerability assessment tools and secure network architecture.
- **Malware Analysis and DFIR**
  - Learned malware identification techniques, analysis tools, and reverse engineering.
  - Completed many real life simulated digital forensics hands on labs on CyberDefenders
- **Web Application Security**
  Covered the OWASP Top 10 vulnerabilities and best practices for securing web applications. Gained proficiency in identifying and mitigating risks associated with web-based applications, ensuring protection against common threats.