KRISHNENDU BHATTACHERJEE

Kolkata, West Bengal, 700060, India | bhattacherjeekrishnendu1@gmail.com | +918240020174
linkedin.com/in/krishnendu-bhattacharjee | medium.com/@bhattacherjeekrishnendu1

PROFESSIONAL SUMMARY

Highly analytical and detail-oriented Security Operations Center (SOC) Analyst trainee with extensive hands-on laboratory experience in alert triage, continuous monitoring, and incident response. Proficient in executing high-fidelity threat detection across Security Information and Event Management (SIEM) platforms, including Splunk and Elastic Stack (ELK). Possesses deep technical expertise in Digital Forensics and Incident Response (DFIR), with published investigations detailing Network Traffic Analysis (NTA) and memory forensics. Adept at leveraging the MITRE ATT&CK framework and the Cyber Kill Chain to contextualize endpoint telemetry, reduce false positive rates, and document actionable Indicators of Compromise (IOCs).

CORE COMPETENCIES & TECHNICAL SKILLS

Security Operations (SOC): Alert Triage, Continuous Monitoring, False Positive Reduction, Root Cause Analysis, Phishing Analysis, Incident Ticket Documentation, Log Aggregation.

Digital Forensics & Incident Response (DFIR): Network Traffic Analysis (NTA), Packet Capture (PCAP) Analysis, Memory Forensics, Data Exfiltration Detection, Malware Behavioral Analysis.

Frameworks & Threat Intelligence: MITRE ATT&CK Matrix, NIST Cybersecurity Framework (CSF), Incident Response Lifecycle (NIST SP 800-61), Cyber Kill Chain, Open Source Intelligence (OSINT).

Core Security Tooling: SIEM (Splunk, Elastic Stack/ELK), Wireshark, Volatility, NetworkMiner, Autopsy, FTK Imager, Wazuh, Endpoint Detection and Response (EDR) telemetry.

Systems & Scripting: Linux Administration, Windows Event Logs (Sysmon), Python, C/C++, Java, OWASP Top 10 Vulnerabilities.

SIMULATED PROFESSIONAL EXPERIENCE & SECURITY OPERATIONS

CyberDefenders - Blue Team & DFIR Operations **Jan 2023 - Present**

Digital Forensics & Incident Response (DFIR) Analyst (Global Rank #2,584) | Remote

- Executed end-to-end network forensics investigations (PacketMaze scenario), utilizing Wireshark to filter and analyze complex PCAP files, isolating unauthorized UDP exfiltration traffic and Command and Control (C2) communications.
- Extracted deeply embedded Indicators of Compromise (IOCs) from network traffic, including plaintext FTP credentials, IPv6 DNS server configurations, and TLS 1.3 client randoms to reconstruct adversary network traversal.
- Conducted advanced memory forensics (Szechuan Sauce scenario) on compromised endpoint memory dumps (.mem) utilizing the Volatility framework.
- Deployed Volatility plugins including windows.pstree to identify anomalous parent-child process relationships and windows.malfind to detect injected code, successfully tracking malware process migration and process hollowing techniques.
- Authored and published comprehensive Incident Response reports detailing adversary Tactics, Techniques, and Procedures (TTPs), demonstrating the ability to translate highly technical forensic data into clear, actionable executive summaries.

TryHackMe - Security Operations Center (SOC) Track **Jan 2023 - Present**

SOC Analyst Trainee (Top 3% Global Rank) | Remote

- Operated within simulated enterprise SOC environments, utilizing Splunk and Elastic Stack (ELK) SIEMs to ingest, parse, and analyze Windows Event Logs, firewall traffic, and web server logs.
- Triaged incoming security alerts, distinguishing between benign anomalous activity and true positive threats, effectively reducing false positive rates through rigorous log correlation.
- Applied the NIST SP 800-61 Incident Response Lifecycle to contain simulated threats, mapping identified adversary behaviors directly to the MITRE ATT&CK framework to ensure comprehensive threat intelligence gathering.
- Performed deep-dive phishing analysis by evaluating malicious email headers, detonating suspicious payloads in secure sandbox environments, and extracting malicious domains and file hashes for SIEM blacklisting.

FEATURED PUBLICATION

Digital Forensic and Incident Response (DFIR) Case Study:

Medium Publication | Link: medium.com/@bhattacherjeekrishnendu1/digital-forensic-and-incident-response-dfir-case-study-cyberdefender-szechuan-sauce-lab-6cc6ad0db2a5

- Published a detailed walkthrough of a memory forensics investigation. Documented the step-by-step extraction of malicious artifacts from a compromised Windows host using Volatility, showcasing practical proficiency in memory analysis, malware identification, and system process auditing.

Network Forensics Investigation Report: PacketMaze

Medium Publication | Link: medium.com/@bhattacherjeekrishnendu1/network-forensics-investigation-report-packetmaze-a-multi-protocol-traffic-analysiscase-9494cfdcfeec

- Authored a comprehensive technical breakdown of a multi-protocol network intrusion. Demonstrated advanced Wireshark filtering techniques to isolate FTP command channels, map unauthorized external DNS resolution, and trace data exfiltration vectors.

Memory Driven Threat Hunting in Linux Envionments: Deconstructing EXIM4 & CVE-2010-4344

Medium Publication | Link: https://medium.com/@bhattacherjeekrishnendu1/-9888d7ac34c1

- Analyzing memory dumps, network traffic, and system artifacts to trace an attack from the initial access vector through to lateral movement and Domain Controller compromise. The investigation culminated in a published technical report outlining the breach timeline, isolation of malicious payloads (such as Meterpreter), and strategic remediation recommendations..

EDUCATION

Bachelor in Computer Application (BCA) **2019 – 2022**

Meghnad Saha Institute of Technology, Kolkata, India

PROFESSIONAL CERTIFICATIONS

- SOC Level 1 Certification – **TryHackMe**
- Certified Network Security Specialist (CNSS) – **ICSI DefensityOne**
- Networks and Communication Security – **(ISC)²**
- Introduction to Cybersecurity – **Cisco Networking Academy**
- Usable Security – **University of Maryland**
- Introduction to Cybersecurity Tools and Cyberattacks – **IBM**
- The Bits and Bytes of Computer Networking – **Google**
- Computer Forensics Investigations Training – **CIP Cyber**