Aman Raj

7274017051 | iamanraj28@gmail.com | linkedin.com/in/amanraj28 | iamanraj.com

Cybersecurity professional with hands-on experience in web and network penetration testing, source code review, and security tool development. Skilled in automating SOC workflows and orchestrating incident response using XSOAR. Proven ability to identify, assess, and remediate vulnerabilities using industry-standard tools and methodologies. Seeking to leverage strong technical and analytical expertise in a challenging Security Analyst role.

EXPERIENCE

CyberSecurity Consultant Feb 2024 – Present

Altisec Technologies Pvt. Ltd. *Pune, Maharashtra*

*Results-driven **Cyber Security Consultant** specializing in **Vulnerability Assessment and Penetration Testing (VAPT)** with deep expertise in **Web, Network, and Application Security**. Proven experience in **SOC operations, SIEM monitoring, incident response automation, and source code review**, with a strong focus on reducing **MTTD/MTTR** and enhancing enterprise security posture.*
*Skilled in tools such as **IBM QRadar, SIEM++, CrowdStrike, IBM Guardium, FireEye (NX, EX, CM, SMG), Arbor DDoS, Trend Micro Deep Security, Imperva WAF, Zscaler, Smokescreen, SEPM, TippingPoint NIPS, and Forcepoint Proxy**. Adept at building **automation workflows and playbooks in XSOAR and Tines**, improving SOC efficiency and response accuracy.*

- **SOC Automation & Playbook Development (XSOAR & Tines):**
  Designed and automated **end-to-end incident response workflows** in **Palo Alto XSOAR** and **Tines**, significantly reducing manual effort and improving consistency in SOC processes.
  Created custom **playbooks** for alerts such as **malware detection, phishing analysis, suspicious login activity, DLP violations, IOC enrichment, and automated triage**, improving SOC operational efficiency.
  Integrated multiple tools and APIs including **CrowdStrike, VirusTotal, IBM QRadar, Cortex XDR, AbuseIPDB, OTX, FireEye, Wazuh**, and email gateways to enable **automated enrichment, correlation, and response actions**.
  Automated repetitive SOC tasks such as **IOC blocking, user isolation, WAF rule creation, URL detonation, and log retrieval**, reducing **MTTD/MTTR** and lowering analyst workload.
  Developed **error-handled**, scalable automation workflows ensuring reliable execution, detailed reporting, and audit-ready documentation.
  Enhanced threat detection and response accuracy through **behavior-based automation**, reducing false positives and improving alert quality.

- **Web VAPT:**
  Performed comprehensive penetration testing on web applications using **Burp Suite, OWASP ZAP, and Nikto**, identifying and exploiting vulnerabilities such as **SQLi, XSS, CSRF, authentication flaws, insecure session management, and access control weaknesses**.
  Delivered detailed **risk assessment reports**, remediation recommendations, and secure architecture suggestions aligned with **OWASP Top 10 and industry best practices**.

- **Network VAPT:**
  Led **end-to-end network vulnerability assessments**, leveraging **Nmap, Nessus, and Metasploit** to enumerate networks, detect misconfigurations, identify open ports, and exploit weaknesses including **weak encryption, privilege escalation paths, and unpatched services**.
  Simulated real-world attack scenarios to evaluate network resilience and recommended mitigation strategies to improve security posture.

- **Source Code Review:**
  Conducted **static code analysis** using **SonarQube** to identify security issues such as **hardcoded secrets, unsafe API usage, improper error handling, injection risks, and insecure cryptographic implementations**.
  Collaborated with development teams to strengthen **secure coding practices**, reduce vulnerability density, and implement robust security controls.

- **Additional Responsibilities:**
  Led internal SOC automation initiatives to reduce MTTD/MTTR, developed an in-house threat intelligence platform, and contributed to building custom VAPT tools to enhance detection efficiency and offensive security capabilities.
  Monitored and investigated security alerts using **QRadar and SIEM++**, handling incidents involving **malware, email threats, anomalous web traffic, and compromised hosts**.
  Analyzed attacker behavior and TTPs to improve **threat detection logic** and enhance correlation rules.
  Monitored **DDoS traffic**, blocked malicious IOCs on firewalls, and ensured optimal network health.
  Performed **file integrity monitoring (FIM)** on critical system files to detect unauthorized access or modifications.
  Managed and monitored **honeypots, deception systems (network/email decoys), and threat intelligence integrations**.
  Conducted continuous monitoring and behavioral analysis of **malicious URLs and domains** across servers and endpoints.

Intern/Associate Consultant Oct 2023 – Feb 2024

CyberFrat *Dehradun, Uttarakhand*

- Assisted in developing a phishing simulation tool to create realistic attack scenarios for security awareness training
- Conducted testing and quality assurance, identifying bugs and ensuring tool functionality.
- Executed phishing campaigns targeting fellow students to assess awareness and improve phishing defense strategies

Cyber Security Trainee Aug 2023 – Feb 2024

Cyber Shikshaa *Dehradun, Uttarakhand*

- Assisted in conducting network and web app assessments using tools like Nmap, Nessus, and OpenVAS to identify vulnerabilities.
- Supported penetration testing efforts using Metasploit and Burp Suite to exploit vulnerabilities in test environments.
- Helped design and execute phishing campaigns using GoPhish to evaluate user awareness and security practices.
- Configured security tools for vulnerability scanning, reporting, and risk analysis.
- Participated in exploiting vulnerabilities and assessing risk severity to provide actionable recommendations.
- Contributed to generating detailed technical reports with findings, risk levels, and remediation steps.

PROJECTS

Multi-Customer SOC Automation & Orchestration | *Tines* Nov 2024 – Present

- Developed automated SOC workflows in **Tines** for more than **10 enterprise customers**, streamlining alert triage, phishing analysis, and IOC enrichment to reduce manual investigation effort and improve detection accuracy.
- Integrated multiple security tools and APIs (VirusTotal, OTX, AbuseIPDB, CrowdStrike, SIEM platforms) to create **end-to-end automated incident response pipelines** tailored to each customer environment.
- Built scalable, logic-driven automation stories that significantly reduced **MTTD/MTTR**, standardized incident handling, and enhanced SOC operational efficiency across diverse customer deployments.

Malware Development | *Batchfile* July 2024 – Present

- Developed malware leveraging socat to bypass various solutions by establishing secure, encrypted communication channels for data exfiltration and reverse shell access.
- Employed evasion techniques such as dynamic payload delivery and traffic obfuscation using socat to avoid detection by traditional antivirus and security monitoring systems.
- Tested and refined the malware under controlled environments to ensure successful evasion of signature-based and behavioral detection methods, enhancing stealth capabilities against security tools.

Personal multitool | *Python, Batchfile* May 2024 – Present

- Developed a multifunctional tool for malware development, reverse shell creation, and network listening, streamlining penetration testing and exploitation tasks.
- Integrated reverse shell functionality to enable remote system control and facilitate post-exploitation activities in controlled testing environments.

PCST - Phishing Control Simulation Tool | *Go, JavaScript, HTML* Oct 2023 – Feb 2024

- Built a phishing simulation tool to replicate various phishing attacks (email spoofing, URL redirection, fake login pages) for testing security awareness.
- Developed automated reporting features to track user responses, identify vulnerabilities, and generate detailed analytics for improvement.
- Created customizable scenarios for different phishing techniques, enabling organizations to assess and strengthen their security defenses.

CERTIFICATIONS

- Certified Red Team Analyst [CRTA] – Cyberwarfare Labs
- Ethical hacking Essentials (EHE) Certified by EC-Council.
- CISCO Networkings.
- SQL Injection Attacks by EC-Council.
- VAPT : Importance & Benefits for Securing Organizations from Cyberattacks by CyberFrat.
- Cybersecurity Workshop by Slog Solutions.

EDUCATION

Shivalik College of Engineering Dehradun, Uttarakhand

Bachelors of Technology in Computer Science

2020 – 2024

TECHNICAL SKILLS

Penetration Testing Tools: Burp Suite, OWASP ZAP, Nikto, Metasploit, Acunetix, Kali Linux
Networks Scanning and Exploitation: Nmap, Nessus, OpenVAS, Wireshark, Netcat, Hydra, Aircrack-ng, tcpdump, Ettercap, Hping3
Web Application Security: OWASP Top 10, SQL Injection, XSS, CSRF, IDOR, Insecure Deserialization
Security Testing Methodologies: Black-box testing, White-box testing, Gray-box testing, Social Engineering