Prakash Nadakuditi

Cybersecurity Engineer

Texas, USA | prakash.nadakuditi@gmail.com | cyberboy.net | (813)-869-4142

PROFESSIONAL SUMMARY

Security Engineer with 5+ years of experience in vulnerability management, red teaming, and penetration testing, specializing in cloud environments like AWS. Skilled in identifying security risks through data analytics, developing scalable remediation solutions, and automating vulnerability management processes. Proven expertise in tools like Cobalt Strike, Burp Suite, and AWS Inspector, coupled with advanced programming in Python and C++ for security automation.

TECHNICAL SKILLS

Red Teaming & Penetration Testing Tools: Cobalt Strike, Nmap, Burp Suite, Metasploit, OWASP ZAP, SQLMap.
Programming & Scripting: Python, C++, JavaScript, Bash, PowerShell.
Cloud Security: AWS, GCP, Azure, Prisma Cloud, Terraform, CSPM (Cloud Security Posture Management), Cloud Workload Protection, AWS Inspector, Azure Security Center
Security Processes: Threat modeling, lateral movement analysis, post-exploitation reporting, custom offensive tool development.
Network Security Tools: Wireshark, Nessus, Netcat, TCPDump, OSSEC, OpenVAS, Shodan, Sysmon, DNS Enumeration Tools, ARP Spoofing Detection
Web Security: OWASP Top 10, XSS, CSRF, SSRF, CORS Misconfigurations, Injection Attacks (SQLi, NoSQLi), Broken Access Control, API Security Testing, WebSocket Analysis
Operating Systems Expertise: Windows, Linux, MacOS.

WORK EXPERIENCE

Security Engineer (R&D) **October 2024–Present**
Caspia Technologies, Remote, USA

- Spearheaded ransomware detection research, leveraging hardware performance counters (HPC) to develop real-time prevention mechanisms, reducing malicious activity impact by 60%.
- Designed and optimized Python and Bash tools to automate data extraction and analysis of hardware-level activities, enhancing detection accuracy.
- Conducted threat modeling for ransomware behavior, developing techniques for real-time anomaly detection that strengthened post-exploitation safeguards.
- Collaborated with cross-functional teams to integrate machine learning models for malware detection into live environments, reducing incident response time by 40%.

Cybersecurity Project manager **May 2024–October 2024**
Resilience Inc, Texas, USA

- Conducted end-to-end penetration tests on financial applications, uncovering high-risk vulnerabilities (e.g., injection attacks) using tools like Burp Suite, resulting in a 50% reduction in exploitable attack surfaces.
- Implemented secure coding practices and remediation plans for OWASP vulnerabilities, reducing issues by 40%.
- Integrated advanced SIEM tools (Splunk, ELK Stack) into monitoring workflows, improving detection rates by 25% and minimizing false positives.
- Designed Python-based automation scripts for vulnerability assessment, increasing assessment frequency and saving 30+ hours per cycle.

Security Engineer/Penetration Tester **April 2021–August 2022**
Tata Consultancy Services, Karnataka, India

- Performed red team exercises and threat modeling on AWS cloud environments, identifying 30+ misconfigurations (e.g., IAM policy gaps, exposed S3 buckets), improving compliance by 50%.

- Built Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP) frameworks, reducing attack surfaces in financial systems by 40%.
- Leveraged Prisma Cloud to monitor and prevent 15+ critical security incidents, ensuring real-time threat mitigation in financial applications.
- Automated vulnerability remediation workflows, reducing manual testing efforts by 40% while enhancing the efficiency of penetration testing processes.

External Penetration Tester **March 2018–June 2024**

Independent Bug Bounty Hunter, Florida, USA

- Investigated and responsibly disclosed over 100 vulnerabilities, including critical flaws like remote code execution and SSRF, across more than 30 organizations, safeguarding sensitive assets and improving trust.
- Engineered a suite of Bash-based automation tools to enhance vulnerability scanning capabilities, increasing scan coverage by 50% and reducing manual effort by 40%.
- Conducted in-depth manual penetration tests on complex web applications, revealing vulnerabilities undetected by automated scanners and contributing to enhanced application security.
- Designed comprehensive threat models for targeted applications, enabling stakeholders to prioritize the remediation of high-impact vulnerabilities with an 80% improvement in remediation efficiency.
- Authored detailed technical reports outlining exploitation techniques, potential risks, and tailored remediation strategies, directly leading to a 70% improvement in incident resolution timelines.
- Partnered with a network of cybersecurity experts to create and publish five technical write-ups, driving a 15% increase in community engagement and sharing industry best practices.

EDUCATION

Master of Science in Cybersecurity

The University of Tampa, Florida, USA *August 2022–May 2024* (GPA: 3.9)

Bachelor of Technology in Information Technology

PVP Siddhartha Institute of Technology, Andhra Pradesh, India *March 2017–April 2022* (GPA: 3.21)

CERTIFICATIONS

- Certified Ethical Hacker (CEH Master) — EC-Council
- CompTIA Pentest+ — CompTIA
- Certified Web Application Security Professional — EC-Council

ACHIEVEMENTS

- **1st Place Winner in the BSides Tampa 2023 Capture the Flag (CTF) competition:** Designed and executed custom payloads to exploit vulnerabilities in simulated enterprise environments, mastering advanced lateral movement techniques.
- **Champion of the OWASP Tampa Chapter Q2 CTF Event:** Demonstrated expertise in exploit development and vulnerability chaining to bypass layered defenses, simulating real-world penetration testing scenarios.
- **1st Place Winner in Spartans CTF 2024:** Leveraged advanced cryptographic techniques and reverse engineering to uncover sensitive data, contributing to enhanced understanding of post-exploitation tactics.