TRENT MILLER

Madison, WI | trentmiller25@protonmail.com
linkedin.com/in/azureadtrent | github.com/AzureADTrent | azureadtrent.github.io

PROFESSIONAL SUMMARY

Offensive security consultant and OSCP-certified penetration tester with 5+ years of experience in network, web application, and infrastructure security assessments. Skilled in Active Directory exploitation, vulnerability research, digital forensics and incident response (DFIR), and adversary simulation. Builds custom offensive tooling and automation to support engagements. Passionate about mentoring the security community and continuously advancing red team tradecraft.

CERTIFICATIONS

OSCP – Offensive Security Certified Professional (2023)
CRTO – Certified Red Team Operator, Zero-Point Security (In Progress)

TECHNICAL SKILLS

Offensive Testing: Burp Suite, Metasploit, BloodHound, Sliver C2, Cobalt Strike, Nessus, Nmap, Hashcat, Responder, Impacket, CrackMapExec
Active Directory: Kerberoasting, AS-REP Roasting, RBCD, DCSync, ADCS Abuse, NTLM Relay, Constrained/Unconstrained Delegation, Shadow Credentials
Web Application: OWASP Top 10, XSS, SQLi, IDOR, SSRF, File Upload Exploitation, API Testing
DFIR: Incident Response, Log Analysis, Forensic Triage, Threat Hunting
Infrastructure: Linux, Windows Server, Docker, Proxmox, Cloud Security, Network Segmentation, Firewall Configuration
Programming: Python, Bash, PowerShell, JavaScript
Platforms: Splunk, JIRA, Wireshark, Git

PROFESSIONAL EXPERIENCE

Security Consultant & Penetration Tester

Ghostscale | Madison, WI — July 2024 – Present

- Lead penetration testing engagements across network, web application, and desktop application environments, identifying critical vulnerabilities and delivering actionable remediation guidance.
- Execute Active Directory and Windows network attack path assessments, identifying misconfigurations in delegation, group policy, and certificate services that expose domain compromise.
- Perform web application and thick-client application security assessments, covering OWASP Top 10 vulnerabilities, API security, and business logic flaws.
- Conduct digital forensics and incident response (DFIR) engagements, supporting clients through containment, evidence collection, root cause analysis, and recovery.
- Manage vulnerability assessment programs, performing scheduled scans, validating findings, and guiding clients through risk-based remediation prioritization.
- Advise clients on security posture improvements, risk prioritization, and hardening strategies across on-premise and cloud environments.
- Develop custom offensive tooling and automation frameworks to improve engagement efficiency and expand test coverage.

Information Security Engineer

Tenable | Madison, WI — July 2023 – July 2024

- Documented vulnerability findings and communicated remediation strategies to over 12 internal teams.
- Monitored and assessed findings within Tenable's FedRAMP environment for compliance and risk.

- Performed vulnerability assessments and delivered results with prioritized recommendations to senior management.
- Developed, implemented, and documented security programs and policies; monitored ongoing compliance.
- Conducted remediation validation testing against findings from external penetration tests.

Technical Support Engineer

Tenable | Madison, WI August 2022 – July 2023

- Managed approximately 20 troubleshooting cases per day across Tenable Cloud and Nessus product lines.
- Performed advanced troubleshooting through log analysis, environment replication, and configuration testing.
- Monitored the vulnerability landscape to proactively assist customers and escalated product defects to development.
- Provided remote guidance on product installation, configuration, and deployment to enterprise customers.

Systems Engineer

ITX Tech Group | Middleton, WI June 2020 – August 2022

- Implemented multi-factor authentication and intrusion detection systems to strengthen network defenses across client environments.
- Coordinated incident response efforts across multiple clients, driving resolution of complex security issues.
- Managed software configurations, patching, and updates for over 1,000 systems across 30 businesses.
- Proactively deployed patches to mitigate known vulnerabilities and reduce attack surface.

EDUCATION

Bachelor of Science: Information Technology, Network Management

Herzing University, Madison, WI | 2015 – 2018

COMMUNITY INVOLVEMENT

DC608 – Treasurer

- Host monthly in-person cybersecurity meetups in Madison, WI.
- Mentor DC608 members in both red and blue team skills, covering platforms such as Hack The Box, TryHackMe, and Blue Team Labs Online.
- Teach monthly online training sessions on offensive and defensive security techniques.