Ian C Norden

Greater Atlanta Area
Iancnorden@gmail.com
https://iancnorden.com

Employment History

May 2017 – Present | Intercontinental Exchange
Sr. Security Engineer — Red Team

- Builds reports and leads read outs from internal and external Red Team engagements.
- Build, maintain, and enhance vulnerability scanning, social engineering, and Red Team supporting infrastructure.
- Executes penetration tests against wide portfolio of critical applications and networks.
- Improve processes via automation engineering and coding, including creating the InfoSec automation dashboard.
- Build and maintain internal virtual pentest practice range of vulnerable VM's.
- Teach and guide new InfoSec team members through brown bag's and pentest workshops.
- Develop applicable POC exploits from frameworks such as Mitre's ATT&CK Matrix.

May 2016 – May 2017 | Intercontinental Exchange
Security Engineer — Red Team

- Challenged as initial member of Red Team to build out the team and capability playbooks.
- Assess and build the Red Team testing platforms, tools, and infrastructure.
- Executes penetration tests against wide portfolio of critical applications and networks.
- Improve processes via automation engineering and coding.
- Maintain and improve upon the current Bug Bounty program.
- Engineer, maintain, and manage the Nexpose infrastructure vulnerability scanning platforms.

Mar 2016 – May 2016 | Intercontinental Exchange
Security Engineer — Application Security

- Architect and implement AppSec tool sets including out of band assessment implementations.
- Manages and executes annual penetration tests against wide portfolio of critical applications.
- Subject matter expertise in configuration and built automation around TLS / SSL assessments.
- Subject matter expert and primary engineer for Nexpose vulnerability scanning infrastructure.
- Produces company standards and guidelines documentation leveraging proven expertise.

Mar 2015 – Mar 2016 | Intercontinental Exchange
Security Analyst — Application Security

- Manages and executes annual penetration tests against wide portfolio of critical applications.
- Improve and maintain the groups testing methodology and metrics.
- Overhaul documentation practices to provide robust knowledgebase previously lacking.
- Provide subject matter expertise showcasing proof of concept exploits against found vulnerabilities.
- Assess and build from ground up the vulnerability scanning infrastructure and platform.

Nov 2014 – Mar 2015 | EarthLink Inc.
Sr. Security Engineer — Professional Services

- Rose to lead the Security arm of EarthLink's Pro Services offering, moving from Engineer to Sr Engineer.
- Lead and execute vulnerability assessments and penetration testing customer engagements.

- Provides mitigation guidance based on technical architectural analysis, threat modeling, and research.
- Created EarthLink's attack and penetration testing methodology standards.
- Architects and engineers Professional Service's team's tools and infrastructure.

Jan 2012 – Nov 2014 | EarthLink Inc.
Security Analyst I & II — Enterprise Information Security

- Manage and engineer infrastructure vulnerability assessment program, subject matter expert Tripwire IP360.
- Primary resource for annual penetration testing services coordination.
- Built and maintained the risk assessment processes for new infrastructure builds.
- SIEM investigation and leveraging Q1Radar implementation.
- Primary incident response escalation point and forensics coordination.
- Regular mentoring and training of new analysts within the Security Operations team.

Education

Dec 2011 | Georgia Southern University
Bachelor's Degree, Information Technology

- Specialization: Networking and Data Center Administration
- Minor: Information Systems

HomeLab

- PFSense Firewall deployment controlling ingress / egress.
- Snort deployed and sniffing ingress / egress.
- Segregated networking for wifi, firing range, automation, and desktop IP space.
- OSSIM deployed as a test bed for attacks and infrastructure.
- Pentest Lab housing a number of vulnerable virtual machines to prepare for OSCP against.
- Security onion sniffing traffic in and out of the Pentest lab.

Coding + Open Source Contributions

- Discover Scripts - https://github.com/leebaird/discover - **Trusted contributor** to this OSINT and Pentest automation resource.
- Distroseed - http://distroseed.github.io/distroseed/" - I co-founded this open source project which is an automated assistant for finding, downloading, and managing Linux Distributions, with a beautiful dashboard.
- Awesome Security Talks - https://github.com/PaulSec/awesome-sec-talks" I regularly contribute to this well-maintained security talks and conferences reference.
- SSLDash - Not yet open source - Beautiful dashboard for automated scanning, grading, and reporting on SSL / TLS strength for websites. Provides guidance to end users for hardening and configuration as well.

Organizations

- OWASP Lifetime Member – Atlanta Chapter
- Linux Foundation Member
- InfraGard Atlanta Member