Nicholas B. **Anderson**

SECURITY ENGINEER · HOST BASED SECURITY DETECTION AND RESPONSE · MALWARE REVERSE ENGINEERING

nanderson7@gmail.com | brewfault.io | muffins | nanderson7 | @poppyseedplehzr

Experience

Meta *Security Engineer, Malware Analysis* *Seattle, WA* *Nov. 2020 - Current*

- Reverse Engineering of Malware for various platforms (Windows, iOS, Android, macOS) to generate reports and signatures which prevented the spread of malware on Facebook platforms
- Reverse Engineering of mobile SDKs to detect Ads fraud and abuse
- Reverse Engineering mobile and native applications for vulnerability assessments to harden Meta owned client fleet and Oculus applications
- Re-architected internal Dynamic Analysis infrastructure used for identifying malicious applications at scale
- Developed automation libraries and toolkits for malware analysis workflows and report generation

Apple *Product Security Engineer, Ecosystem Integrity Protection* *Seattle, WA* *Mar. 2020 - Nov. 2020*

- Reverse Engineered malware samples affecting macOS and published protective signatures deployed to endpoints
- Architected framework using AWS and WWDR to revoke certificates used by fraudulent developers publishing malware
- Unified analyst libraries and brought CI/CD and testing suites to code repository to enhance reliability of tooling

Facebook *Security Engineer, Detection Infrastructure* *Menlo Park, CA* *Feb. 2016 - Mar. 2020*

- Architected and executed Endpoint Detection and Response infrastructure on-prem to cloud migration
- Purchase and integration of third-party Detection-as-a-Service capabilities
- Core developer and maintainer of osquery project - https://osquery.io
- Developed and maintained host-based endpoint monitoring agents, logging infrastructure, and deployment mechanisms
- Administered and orchestrated Carbon Black backend infrastructure and endpoint deployment
- Built endpoint detections leveraging host-based telemetry
- Mentor university students internationally for the Facebook Open Source Mentorship program
- Rearchitected corporate DNS deny-listing capability, increasing reliability and reducing operational overhead
- Developed security education curriculum for lockpicking and CTF challenges used in Hacktober security awareness month
- Developed and delivered osquery workshop curriculum for conferences to teach endpoint detection at scale

Sandia National Laboratories *Cyber Security R&D Scientist and Engineer* *Albuquerque, NM* *Jan. 2015 - Jan. 2016*

- Malware Reverse Engineer on Security Incident Response Teams
- Reverse Engineered and developed C2 generation script for detection of Hammertoss malware
- Mentored Albuquerque High School CyberPatriot team

Sandia National Laboratories *Graduate Student Intern, Center for Cyber Defenders (CCD)* *Albuquerque, NM* *June 2014 - Aug. 2014*

- Developed fuzzing framework for email detection engine to test corporate detection rules
- Researched automated vulnerability discovery methods for Windows binary files

Trail of Bits *Security Intern* *New York, NY* *Jan. 2014 - Aug. 2014*

- Developed platform testing framework for iterated Windows versions using Virtual Machine APIs

Handel IT *Software Developer, Systems Administrator* *Laramie, WY* *Sept. 2012 - Aug. 2013*

- C# and .NET software developer for RiteTrack5 software suite
- Systems Administrator for Windows 2003, 7, 2008, 2012, and FreeBSD(pfSense) Operating Systems
- Deployed and Administered Nagios Core to enterprise endpoints
- Administered Windows SCCM server for software deployments and endpoint compliances

University of Wyoming, Mathematics Dept. *Academic Lecturer* *Laramie, WY* *Dec. 2009 - Apr. 2010*

- Responsible for lectures, student grades, and preparing and issuing class quizzes

University of Wyoming *IT Technicianfor Academic Support Unit* *Laramie, WY* *Feb. 2008 - July. 2009*

- Troubleshooting computer issues, maintaining computer labs, and tech support

Education

New York University, Polytechnic *Master of Science in Cybersecurity, 3.889 GPA* *Brooklyn, NY*

- SFS ASPIRE Fellowship

University of Wyoming *Master of Science in Mathematics, **Did Not Complete**, 3.42 GPA* *Laramie, WY*

- Computing the refined stability condition, Quarterly of Applied Mathematics
- Upsilon Pi Epsilon Special Recognition Scholarship Recipient, Fall 2012

University of Wyoming *Bachelor of Science in Mathematics, Minor in Computer Science, 3.883 GPA* *Laramie, WY*

- Outstanding Graduate, College of Arts & Sciences Top 20 in Class, Spring 2010
- Honor Roll, U.W. President's List, 4.0 Semester GPA, Spring 2007, 08, 09
- Varineau Memorial Math Scholarship Recipient, Spring 2009

Conference Talks & Workshops

Oct. 2018	**OSDFcon**, The osquery file carver	*Herndon, VA, USA*
Oct. 2018	**OSDFcon**, Docker Detection and Forensics, ‘Gotta catch them all’!	*Herndon, VA, USA*
June 2018	**QueryCon**, Keynote - Evolving Our Open Source Community	*San Francisco, CA, USA*
Nov. 2018	**BlueHat**, Detecting compromise on Windows endpoints with osquery	*Redmond, WA, USA*
Oct. 2016	**Brucon 0x8**, Hunting Malware at Scale with osquery	*Ghent, Belgium*
Sept. 2016	**Structure Security**, Open Source Security Panel	*San Francisco, CA, USA*
Aug. 2016	**DEFCON 24**, Hunting Malware at Scale with osquery	*Las Vegas, NV, USA*
Aug. 2015	**DEFCON 23**, Hardware and Trust Security: Explain it like I’m 5	*Las Vegas, NV, USA*

Publications

Introducing osquery for Windows *Protect the Graph* *Sept. 27th, 2016*
https://www.facebook.com/notes/protect-the-graph/introducing-osquery-for-windows/1775110322729111/

Computing the refined stability condition *https://arxiv.org/abs/1207.4101* *University of Wyoming* *July 17th, 2012*

Skills

Programming Python, C, C++, Intel x86/x64 Assembly, Powershell, Hacklang, sqlite, R

Security Tools IDA Pro, BinaryNinja, WinDBG, gdb, Wireshark, nmap, x64dbg, ollydbg, Metasploit, Empyre

Enterprise Tools osquery, Chef, Splunk, Graylog, AWS (EC2, Lambda, SQS SNS, ECS, CloudFormation), MD-ATP, Windows Active Directory, pfSense, Carbon Black

Fields of Interest Malware Reverse Engineering, Digital Forensics, Cloud Infrastructure for Detection and Response, Exploitation, Lockpicking, CTFs

Honors & Awards

2017, 2019	**Splunk Boss of the SoC**, Regional Winners	*Seattle, WA, US*
2017	**O’Reilly Security Conference**, O’Reilly Security Project Defender Award	*New York, NY, US*
2014, 15, 17	**FireEye flare-on Reverse Engineering CTF**, Completed and Honor Roll	*flare-on.com*

Associations

2009 - 2010	**Researcher**, Cryptography Research Cohort	*University of Wyoming*
2009	**Researcher**, NSF EPSCoR Research Fellowship	*University of Wyoming*
2009 - 2012	**Founding Charter Member**, Upsilon Pi Epsilon	*University of Wyoming*
2009 - 2012	**Founding Member and Co-Captain**, Cyber Defense Action League, University of Wyoming Cybersecurity Team	*University of Wyoming*

Extracurricular Activity

Brooklynt Overflow, NYU OSIRIS Lab *Co-Captian and Team Lead* *Brooklyn, NY* *2013 - 2015*

- Curator of educational program Hack Night, teaching new students about security
- Organizer of CSAW Security Conference
- CTF Challenge author for DHS Forensics competition

Cyber Defense Action League, Univ of Wyo Cyber Security team *Core and Founding Member* *Laramie, WY* *2009 - 2012*

- Helped found and establish the University of Wyoming Cybersecurity team
- Awarded $15,271.26 for grant proposal to construct Cyber Security Lab
- 1st Place Winner of the North Central Collegiate Cyber Defense Competition in Spring 2011, 12
- Competed in CTF competitions such as CSAW, ASIS, Plaid, and ruCTF
- Gave educational demos around exploitation and malware reverse engineering

Upsilon Pi Epsilon *Founding Charter Member* *Laramie, WY* *2009 - 2012*

- Helped found and establish the University of Upsilon Pi Epsilon (Computer Science Honor Society) chapter

University of Wyoming Cryptography Research Cohort *Researcher* *Laramie, WY* *Academic year 2009 - 2010*

- Worked with cohort on deep dives into asymetric crypto routines and co-prime primitives
- Wrote R code for running numerical analysis of research work

NSF EPSCoR Research Fellowship *Researcher* *Laramie, WY* *Spring 2009*

- Senior research project the analysis of eigenvalues of different wave forms