Nicholas B. **Anderson**

Security Engineer · Host Based Security Detection and Response · Malware Reverse Engineering

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

Education

New York University, Polytechnic
Brooklyn, NY

Master of Science in Cybersecurity, 3.889 GPA — *Aug. 2013 - Dec. 2014*

- SFS ASPIRE Fellowship

University of Wyoming
Laramie, WY

Master of Science in Mathematics, **Did Not Complete**, 3.42 GPA — *Aug. 2010 - Feb. 2012*

- Computing the refined stability condition, Quarterly of Applied Mathematics - https://goo.gl/A4LCgP
- Upsilon Pi Epsilon Special Recognition Scholarship Recipient, Fall 2012

University of Wyoming
Laramie, WY

Bachelor of Science in Mathematics, Minor in Computer Science, 3.883 GPA — *Aug. 2006 - May 2010*

- 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

Experience

Facebook
Menlo Park, CA

Security Engineer, Detection Infrastructure — *Feb. 2016 - Current*

- Architected and executed EDR cluster infrastructre 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
- Built endpoint detections leveraging host-based endpoint telemetry
- Mentor for Facebook Open Source Mentorship program
- Rearchitected corporate DNS blacklisting capability
- Developed security education curriculum for lockpicking and CTF challenges for use in Hacktober security awareness month
- Developed osquery workshop curriculum delivered at conferences to teach scaling endpoint detection

Sandia National Laboratories
Albuquerque, NM

Cyber Security R&D Scientist and Engineer — *Jan. 2015 - Jan. 2016*

- Malware Reverse Engineer on Security Incident Response Teams
- Reverse Engineered and developed C2 generation script for detection of Hammertoss malware

Sandia National Laboratories
Albuquerque, NM

Graduate Student Intern — *June. 2014 - Aug. 2014*

- Member of the TITANS Center for Cyber Defenders (CCD) Program
- Developed fuzzing framework for email detection engine to test detection rulesets

Trail of Bits
New York, NY

Security Intern — *Jan. 2014 - Aug. 2014*

- Developed platform testing framework for Windows Virtual Machines

Handel IT
Laramie, WY

Software Developer, Systems Administrator — *Sep. 2012 - Aug. 2013*

- C# and .NET software development of RiteTrack5 software suite
- Systems Administrator for Windows 2003, 7, 2008, 2012, and FreeBSD(pfSense) Operating Systems
- Deployed and Administered Nagios Core, monitoring and alerting engine
- Administered Windows SCCM server for agent and software deployments

University of Wyoming, Mathematics Dept.
Laramie, WY

Academic Lecturer — *Dec. 2009 - Apr. 2010*

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

University of Wyoming
Laramie, WY

IT Technicianfor Academic Support Unit — *Feb. 2008 - July. 2009*

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

Skills

Programming	Python, C/C++, Powershell, Ruby, Hacklang, Golang, C#, Haskell, sqlite, R
Security Tools	IDA Pro, WinDBG, gdb, Wireshark, tshark, nmap, x64dbg, ollydbg, Metasploit, Empyre
Enterprise Tools	osquery, Chef, Splunk, MD-ATP, Windows Active Directory, GPO, and SCCM, pfSense, Carbon Black
Skillsets	Malware Reverse Engineering, Forensics, SOAR, Lockpicking, Exploitation, CTFs

Conference Talks and Workshops

OSDFcon — *Herndon, VA, USA*

The osquery file carver — *Oct. 2018*

- Introduced the osquery file ”carving” capability, it’s goals, and non-goals

OSDFcon — *Herndon, VA, USA*

Docker Detection and Forensics, ‘Gotta catch them all’! — *Oct. 2018*

- Detection and response workshop focused on leveraging osquery to secure Docker containers

QueryCon — *San Francisco, CA, USA*

Keynote - Evolving Our Open Source Community — *June 2018*

- Addressed the challenges of scaling an Open Source project and community, https://www.youtube.com/watch?v=RVNEUqgwv5A

BlueHat — *Redmond, WA, USA*

Detecting compromise on Windows endpoints with osquery — *Nov. 2018*

- Discussed how to scale osquery to detect compromise at enterprise levels, as well as use-cases and success stories from the field. https://www.slideshare.net/MSbluehat/bluehat-v17-detecting-compromise-on-windows-endpoints-with-osquery-84024735

Brucon 0x8 — *Ghent, Belgium*

Hunting Malware at Scale with osquery — *Oct. 2016*

- Same workshop as DEFCON 24
- https://brucon0x082016.sched.com/event/8YCB/hunting-malware-with-osquery-at-scale

Structure Security — *San Francisco, CA, USA*

Open Source Security Panel — *Sep. 2016*

- Organized and took part in a panel discussion about open source security tooling
- Fortune Article - http://fortune.com/2016/09/27/facebook-uber-slack-pandora-open-source-security
- Guardian Article - https://www.theregister.co.uk/2016/09/28/oh_all_right_says_facebook_well_let_windows_admins_run_osquery
- Facebook Graph Blog - https://www.facebook.com/notes/protect-the-graph/introducing-osquery-for-windows/1775110322729111/

DEFCON 24 — *Las Vegas, Nevada, USA*

Hunting Malware at Scale with osquery — *Aug. 2016*

- 4 hour workshop focused on using osquery to scale host based detections
- Covered standing up a SIEM, configuring an endpoint EDR, and building detections around host based security telemetry
- https://brucon0x082016.sched.com/event/8YCB/hunting-malware-with-osquery-at-scale

DEFCON 23 — *Las Vegas, Nevada, USA*

Hardware and Trust Security: Explain it like I’m 5 — *Aug. 2015*

- Covered basic concepts of Secure and Trusted boot technologies, https://www.youtube.com/watch?v=2gbooa3tO5o

Extracurricular Activity

Brooklynt Overflow, NYU OSIRIS Lab — *Brooklyn, NY*

Co-Captian and Team Lead — *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 — *Laramie, WY*

Core and Founding Member — *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 — *Laramie, WY*

Founding Charter Member — *2009 - 2012*

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

University of Wyoming Cryptography Research Cohort — *Laramie, WY*

Researcher — *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 — *Laramie, WY*

Researcher — *Spring 2009*

- Senior research project on the question ”can you hear the shape of a drum?”, analysis of eigen values of wave forms

Honors & Awards

2019	**Regional Winners**, Splunk Boss of the SoC competition	*Seattle, Washington, US*
2017	**Winners**, Splunk Boss of the SoC competition	*San Jose, California, US*
2017	**O’Reilly Security Project Defender Award**, O’Reilly Security Conference	*New York, New York, US*
2014, 15, 17	**Completed and Honor Roll**, FireEye FLARE RE Challenge Competition	*flare-on.com*