

Nicholas B. Anderson

SECURITY ENGINEER · HOST BASED SECURITY DETECTION AND RESPONSE

✉ 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

- 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 TECHNICIAN FOR ACADEMIC SUPPORT UNIT

Feb. 2008 - July. 2009

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

Skills

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

Presentations

OSDFcon

Herndon, VA, USA

THE OSQUERY FILE CARVER

Oct. 2018

- Introduced the osquery file "carving" capability, it's goals, and non-goals

QueryCon

San Francisco, CA, USA

KEYNOTE - EVOLVING OUR OPEN SOURCE COMMUNITY

June 2018

- Covered basic concepts of Secure and Trusted boot technologies, <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-CAPTAIN 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 asymmetric 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

2017 **O'Reilly Security Project Defender Award**, O'Reilly Security Conference

New York, NY, U.S.A

2014, 15, 17 **FLARE-ON Honor Roll**, FireEye FLARE Lab RE Competition

flare-on.com