

# Nicholas B. Anderson

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

✉ nanderson7@gmail.com | 🏠 brewfault.io | 📧 muffins | 📄 nanderson7 | 🐦 @poppyseedplehxr

## Experience

### Apple

PRODUCT SECURITY ENGINEER, ECOSYSTEM INTEGRITY PROTECTION

- Reverse Engineered malware samples affecting the macOS platform
- Developed automation infrastructure of response workflows using AWS
- Developed standardized libraries for analyst and investigator workflows

Seattle, WA

Mar. 2020 - Current

### Facebook

SECURITY ENGINEER, DETECTION INFRASTRUCTURE

- Architected and executed EDR cluster 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
- 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 endpoint detection at scale

Menlo Park, CA

Feb. 2016 - Mar. 2020

### Sandia National Laboratories

CYBER SECURITY R&D SCIENTIST AND ENGINEER

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

Albuquerque, NM

Jan. 2015 - Jan. 2016

### Sandia National Laboratories

GRADUATE STUDENT INTERN

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

Albuquerque, NM

June. 2014 - Aug. 2014

### Trail of Bits

SECURITY INTERN

- Developed platform testing framework for Windows Virtual Machines

New York, NY

Jan. 2014 - Aug. 2014

### Handel IT

SOFTWARE DEVELOPER, SYSTEMS ADMINISTRATOR

- 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

Laramie, WY

Sep. 2012 - Aug. 2013

### University of Wyoming, Mathematics Dept.

ACADEMIC LECTURER

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

Laramie, WY

Dec. 2009 - Apr. 2010

### University of Wyoming

IT TECHNICIAN FOR ACADEMIC SUPPORT UNIT

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

Laramie, WY

Feb. 2008 - July. 2009

## Education

### New York University, Polytechnic

MASTER OF SCIENCE IN CYBERSECURITY, 3.889 GPA

- SFS ASPIRE Fellowship

Brooklyn, NY

Aug. 2013 - Dec. 2014

### University of Wyoming

MASTER OF SCIENCE IN MATHEMATICS, **DID NOT COMPLETE**, 3.42 GPA

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

Laramie, WY

Aug. 2010 - Feb. 2012

## University of Wyoming

BACHELOR OF SCIENCE IN MATHEMATICS, MINOR IN COMPUTER SCIENCE, 3.883 GPA

- 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

Laramie, WY

Aug. 2006 - May 2010

## 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](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

RESEARCHER

Laramie, WY  
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

RESEARCHER

Laramie, WY  
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	<b>Regional Winners</b> , Splunk Boss of the SoC competition	Seattle, Washington, US
2017	<b>Winners</b> , Splunk Boss of the SoC competition	San Jose, California, US
2017	<b>O'Reilly Security Project Defender Award</b> , O'Reilly Security Conference	New York, New York, US
2014, 15, 17	<b>Completed and Honor Roll</b> , FireEye FLARE Reverse Engineering Challenge Competition	flare-on.com

## Skills

<b>Programming</b>	Python, C/C++, x86/x64 Assembly, Powershell, Hacklang, sqlite, R
<b>Security Tools</b>	IDA Pro, BinaryNinja, WinDBG, gdb, Wireshark, tshark, nmap, x64dbg, ollydbg, Metasploit, Empyre
<b>Enterprise Tools</b>	osquery, Chef, Splunk, Graylog, AWS, MD-ATP, Windows Active Directory, GPO, SCCM, pfSense, Carbon Black
<b>Skillsets</b>	Malware Reverse Engineering, Infrastructure, Automation, Digital Forensics, SOAR, Lockpicking, Exploitation, CTFs

## Publications

### Introducing osquery for Windows

Facebook Protect the Graph Blog

[HTTPS://WWW.FACEBOOK.COM/NOTES/PROTECT-THE-GRAPH/INTRODUCING-OSQUERY-FOR-WINDOWS/1775110322729111/](https://www.facebook.com/notes/protect-the-graph/introducing-osquery-for-windows/1775110322729111/)

Sept. 27th, 2016

### Computing the refined stability condition

University of Wyoming

[HTTPS://ARXIV.ORG/ABS/1207.4101](https://arxiv.org/abs/1207.4101)

July 17th, 2012

## Associations

2009 - 2010	<b>Researcher</b> , Cryptography Research Cohort	University of Wyoming Mathematics Dept.
2009	<b>Researcher</b> , NSF EPSCoR Research Fellowship	University of Wyoming Mathematics Dept.
2009 - 2012	<b>Founding Charter Member</b> , Upsilon Pi Epsilon	University of Wyoming Computer Science Dept.
2009 - 2012	<b>Founding Member and Co-Captain</b> , Cyber Defense Action League, University of Wyoming Cybersecurity Team	University of Wyoming