Nicholas B. **Anderson**

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

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

Experience

Apple - Product Security Engineer, Ecosystem Integrity Protection

- Reverse Engineered malware samples aff
- Developed automation infrastructure of r
- Deveopled standardized libraries for anal

Facebook - Security Engineer, Detection Infrastructure

- Architected and executed EDR cluster infr
- Purchase and integration of third-party D
- Core developer and maintainer of osquer
- Developed and maintained host-based en
- Administered and orchestrated Carbon B
- Built endpoint detections leveraging host
- Mentor for Facebook Open Source Mento
- Rearchitected corporate DNS blacklisting
- Developed security education curriculum
- Developed osquery workshop curriculum

Sandia National Laboratories - Cyber Security R&D Scientist and Engineer

- Malware Reverse Engineer on Security Inc
- Reverse Engineered and developed C2 ge
- Mentored Albuquerque High School Cybe

Sandia National Laboratories - Graduate Student Intern

- Member of the TITANS Center for Cyber D
- Developed fuzzing framework for email d

Trail of Bits - Security Intern

- Developed platform testing framework fo

Handel IT - Software Developer, Systems Administrator

- C# and .NET software development of Rit
- Systems Administrator for Windows 2003,
- Deployed and Administered Nagios Core,
- Administered Windows SCCM server for a

Education

New York University, Polytechnic - Master of Science in Cybersecurity, 3.889 GPA

- SFS ASPIRE Fellowship

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

- Computing the refined stability condition
- Upsilon Pi Epsilon Special Recognition So

University of Wyoming - Bachelor of Science in Mathematics, Minor in Computer Science, 3.883 GPA

- Outstanding Graduate, College of Arts & S
- Honor Roll, U.W. President's List, 4.0 Seme
- Varineau Memorial Math Scholarship Rec

Conference Talks and Workshops

OSDFcon - The osquery file carver

OSDFcon - Docker Detection and Forensics, 'Gotta catch them all'!

QueryCon - Keynote - Evolving Our Open Source Community

BlueHat - Detecting compromise on Windows endpoints with osquery

Brucon 0x8 - Hunting Malware at Scale with osquery

Structure Security - Open Source Security Panel

DEFCON 24 - Hunting Malware at Scale with osquery

DEFCON 23 - Hardware and Trust Security: Explain it like I'm 5

Skills

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

Publications

Introducing osquery for Windows -
https://www.facebook.com/notes/protect-the-graph/introducing-osquery-for-windows/1775110322729111/

Computing the refined stability condition - https://arxiv.org/abs/1207.4101