Nathan Burns

nburns.tech | nburns9922@gmail.com | Nathan Burns | AlbinoGazelle | 425-737-0347

Experience

AutoDesk Inc. — **Bellingham, WA**
Threat Hunter - Threat Intelligence — *June 2022 - Present*
- Incoming Threat Hunter at AutoDesk Inc.

Naval Underwater Warfare Center — **Bellingham, WA**
Matryoshka Honeypot Project - WWU Cyber Security Department — *September 2021 - Present*
- Currently working with a group of 3 other WWU students in partnership with the Navy's Underwater Warfare Center to develop a framework on the proper implementation and deployment of honeypots.
- Deliverables include a research paper, presentation, and a honeynet for demonstration purposes.

Western Washington University — **Bellingham, WA**
Student Security Analyst - PISCES — *January 2022 - Present*
- Worked alongside 3 other students to monitor the network traffic of Covington, WA.
- We successfully notified the city of numerous anomalies, misconfigurations, and potential malicious activity utilizing an ELK stack and ticketing system
- Documented findings/tasks in a wiki.js page.

Western Washington University — **Bellingham, WA**
Webmaster/Secretary - Cybersecurity Club — *August 2021 - Present*
- Responsible for developing and maintaining the club website and organizing club resources, growing the club to over 100 members.
- Utilized public speaking, teamwork, and research skills to deliver weekly meetings to club members.

Western Washington University — **Bellingham, WA**
Co-Captain - Collegiate Cyber Defense Competition — *January 2022 - April 2022*
- Responsible for deploying and hardening Linux systems and preparing relevant technical documentation.

Education

Western Washington University — **Bellingham, WA**
BS in Cyber Security; GPA: 3.5; NSA CAE-CD Certified — *September 2020 - December 2022*
- Computer Security, Database Concepts, Secure Software Development, and Technical Writing.

Lake Washington Institute of Technology — **Kirkland, WA**
AAS in Computer Security; GPA: 3.6; Graduated Cum Laude — *March 2017 - June 2020*
- Computer and Network Security, Network Administration, and Computer Science (Java).

Personal Projects

Personal Website and Blog - React.js, Docusaurus, Github Pages, Cloudflare — *nburns.tech*
- Used to host technical posts relating to malware analysis, network defense, and CTF reports.

Discord Shell - Python, Bash, PowerShell — *GitHub Repo*
- Discord API-powered C2 designed to infect Windows and Linux hosts while evading AV engines.
- Developed in partnership with a fellow student. Created for educational purposes only.

ToolBox - Python — *GitHub Repo*
- Utility Discord bot created for the WWU Cybersecurity club. Written in Python using Discord.py.
- Logs numerous Discord actions, allows users to upload links to VirusTotal's API, and gives users the ability to download malware samples for analysis using virus.exchange.

Signature Based Detection - Zeek — *Available Upon Request*
- Zeek rules to detect DNS exfiltration and malicious MQTT usage. This involved manual deconstruction and analysis of the MQTT packet structure to detect a subscribe all topic attack.

Research

Deconstructing WhisperGate — *nburns.tech*
- Blog post on a destructive malware sample being used to target Ukrainian systems. Includes Indicators of Compromise, Yara rules to detect activity, and MITRE ATT&CK techniques used.
- Tools Used: Sysmon, YARA, Ghidra, and VirusTotal.

Mirai Analysis — *nburns.tech*
- Research into witnessed Mirai activity targeting my honeypot. Includes Indicators of Compromise, timeline of the attack, and analysis on the payload.
- Tools Used: TPOT Honeypot Framework, VirusTotal, and Ghidra.

The Dangerous Impact of the Rise of Cyberstalking — *nburns.tech*
- Academic paper detailing the rise of cyberstalking and its impacts on victims.