

Steven Owen

Rockhill SC | 253-590-7941 | Srgowen2@gmail.com

Summary:

Versatile and skilled cybersecurity professional with a strong foundation in Linux and Windows administration, network security, cryptography, scripting, and cloud computing. A quick learner with the ability to adapt to rapidly evolving security challenges. Expertise in setting up Azure labs, recognizing and mitigating attacks, utilizing SIEM solutions, securing web applications with SSL certifications, and using OSINT to stay ahead of potential threats. Passionate about enhancing organizational security and reducing risk.

Technical Skills:

- Operating Systems: Linux, Windows, CentOS
- Scripting Languages: Bash, PowerShell, PHP, XML, Windows
- Network Security: IPS, IDS, Routing, Firewalls, SNORT Rules
- Cryptography: Asymmetric and Symmetric Cryptography
- Web Applications: HTTP/s Sessions and Cookies, SSL Certifications
- Cloud Computing: Azure
- Tools: Splunk, DVWA, Metasploit, Nessus, SIEM, Wazuh, OPNsense, Snort, Suricata, Zenarmor
- Experience using virtual box and oracle. Hosted entire security networks and configured them on virtual box.

Professional Experience:

Southern Methodist University Cybersecurity Bootcamp 24 weeks

- Completed an intensive 24-week program focused on cybersecurity and gained practical experience in Linux and Windows administration, network security, scripting, and cloud computing.
- Set up an Azure lab with a load balancer, jump boxes, firewall, and configured containers to host a website.
- Recognized and mitigated attacks on the Damn Vulnerable Web Application (DVWA) and used OSINT to recognize upcoming threats.
- Used Splunk to create reports and dashboards to gain insight into potential security threats.

Technical Skills Project

- Worked on a team to develop a project focused on building a secure network infrastructure.
- Conducted research on network security, cryptography, and firewalls to determine best practices and implemented those practices in a project.
- Configured network devices, set up a firewall, and implemented load balancing to improve network performance.
- Set up an OPNsense and PfSense firewall complete with a NGFW component with a redundant firewall (including IDS IPS configuration). Wrote and uploaded custom IDS, IPS, and snort rules.
- Configured a Wazuh SIEM that compiled logs by a SNMP trap that was used with the OPNsense NGFW and acted as a HIDS and limited HIPS solution.
- Wrote custom rules and alerts based on behavior with the Wazuh SIEM as well as on Splunk.
- experience using docker for hosting websites and running programs.
- Utilized HTTPS and SSL certifications to secure web applications and protect sensitive data.
- Link to Wazuh and OPNsense firewall project.
- <https://youtu.be/rzXCd87-i3g>

Education:

SMU Cyber Security bootcamp, Southern Methodist University, 6/14/2023

SMU Coding bootcamp, Southern Methodist University, 8/28/23-02/28/23

Certifications:

- CompTIA Security+

Employment History:

IT & RF technician 07/20/2023-current, Buytwowayradios.com

- Maintaining the company's domain network

- Conducting cybersecurity awareness training for employees
- Troubleshooting Windows and Domain connectivity issues
- Screening untrusted files and attachments received by the company
- Leading or assisting in responding to cybersecurity incidents and breaches, including identifying and mitigating vulnerabilities
- Providing remote technical support to employees, efficiently resolving IT issues to minimize disruptions

Transportation Security Officer 06/2022-09/2022 Transportation Security Administration (TSA) Seatac, WA

- Operated various screening equipment and technology to identify dangerous objects in baggage, cargo, and on passengers, and preventing those objects from being transported onto aircraft
- Conducted searches and screenings, which may include physical interaction with passengers (e.g., patdowns, search of property, etc.), conducting bag searches, and lifting/carrying bags, bins, and property weighing up to 50lbs
- Controlled terminal entry and exit points
- Interacted with the public, gave directions, and responded to inquiries.
- Maintained focus and awareness while working in a high-stress environment, in order to identify and locate potentially life-threatening or mass destruction devices, and to make effective decisions in both crisis and routine situations
- Engaged in continuous development of critical thinking skills to mitigate actual and potential security threats, by identifying, evaluating, and applying appropriate situational options and approaches

Security Guard 12/2021 – 03/2022 Naval Base Kitsap Police Department Bremerton, WA

- Receive, authenticate, and vet visitors entering an installation.
- Respond to and/or contain crisis or urgent situations including accidents; man-made, biological, chemical, radiological, or natural disasters; or other incidents that could result in harm to people, property, or the environment.
- Control access to the installation/Federal property and restricted areas, identify security risks, and provide traffic management.
- Apply requirements for equipping and securing government and contractor facilities to guard against unauthorized access, identify suspicious activities, and ensure continuity of operations.
- Operate security-related equipment (both manual and automated) or devices.

- Maintained a secret clearance in between the TSA and corrections.

Correctional Deputy 02/2018 – 08/2020 Pierce County Sheriff's Department Tacoma, WA

- Entered and updated arrestees' information into a secure central database.
- Written over 600 legally binding reports, several of which were charging arrestees of crimes committed in the facility.
- Controlled access of civilians and inmates in a secure facility.
- Properly utilized de-escalation techniques to reduce the need for physical interventions.
- Maintained accurate logs of all pertinent events in my charge.
- Maintained composure and awareness in extremely stressful situations.

11B, Infantryman- Honorable Discharge 01/2014 – 02/2018 United States Army Joint Base Lewis McChord, WA

- Stryker vehicle commander in charge of 2+ million dollars' worth of equipment.
- Safeguarded secret and sensitive equipment.
- Maintained a secret clearance.
- Supervised and led a team of soldiers through high-stress situations and live-fire exercises.
- Section leader of a sniper team in charge of reconnaissance and fire support for a rifle company.

Education:

- Southern Methodist University, 24-week Cybersecurity Bootcamp

- Pierce Community College, Puyallup, WA

Associate of Science in Biology 2021-2022

24 semester hours completed, 3.5 GPA

- Minnesota State Technical and Community Colleges, Moorhead, MN

Associate of Science in Biology, 2020-2021

32 semester hours completed, 3.6 GPA

- El Molino High School, Forestville, CA

High School Diploma, 2013

References available upon request.