# SCOTT HANSEN

FRIDLEY, MN 55432 651-357-5757 S.HANSEN18@GMAIL.COM

## WEBSITE, PORTFOLIO, PROFILES

- https://www.linkedin.com/in/scott-hansen-cybersecurity-specialist/
- https://github.com/shansen18/BootCamp/blob/main/Readme.md

## PROFESSIONAL SUMMARY

Ambitious, career-focused job seeker, anxious to obtain an entry-level Cybersecurity Analyst position to help launch career while achieving company goals.
Currently attending a Cybersecurity Bootcamp, put on by the University of Minnesota.
This class has been exposed to many tools, such as; Docker, and container, Linux, Terminal, bash and basic scripting, wireshark, Autopsy, Elks Stack, Kali Linux, Metasploit and many others.
This class has 3 project as well as weekly homework. Seeing how this class is currently in session, and ends in December 2021, only 2 projects have been completed.
Project 1.
A trial version of Microsoft Azure was used to setup a small network. This network started with a Resource group, then a firewall rule was used to secure this network, then 4 virtual machines were added to the network. The first machine was a jumpbox, that was used to remote connect into the jumpbox using SSH, and from there connect to the other machines. Two more virtual machines were then added, that ran the DVWA website using Ansible and Containers. Then a load balancing machine was created, to control the previous two machines hosting the DVWA webpage. What this did was to create redundancy so if machine 1 would fail machine 2 would take over. Elk stack server was added to the network to monitor the network. Then Ansible, and Docker to deploy this server, as well as deploy Filebeat and Metricbeat.
Project2.
An Azure machine with 3 computer in Hyper-V, networked together. A virtual network in a virtual machine. One computer was a Kali Linux machine used as an attacker. The second Hyper-V machine was setup to be a web server, that was setup to be the victim. The third Hyper-V machine was an ELK server, used to identify the attack.
The first part of this project, the class acted as the Red Team, and analyzed the web server for vulnerabilities, and exploit them. This was done by using Metasploit to create payload which allowed for reverse shell connection that was used to exfiltrate data off that server.
The second half, The class acted as the Blue team to analyze the signature of the attack. From there advise was given on what could be done to mitigate this type of attack from happening again.

## SKILLS

- Penetration testing [Metasploit, NMAP, Legion, Wireshark, Hydra, John the ripper, netcat.]
- Help Desk Support
- Network Security
- Analytical and Critical Thinking

- Wireshark software
- Verbal and Written Communication
- Troubleshooting Network Issues
- Technical Troubleshooting
- User Support

## PROFESSIONAL EXPERIENCE

MARCH 2015-APRIL 2021

**Broadband Technician** | CenturyLink\Lumen | Brooklyn, Mn

- At CenturyLink I was working as a broadband technician, installing DSL, Fiber, and Pots into residential, and small businesses.
- I also troubleshot and repaired copper and fiber lines used in providing internet and phone services.
- Depending on the job, this may have included rewiring or installation of phone jacks.
- Running new cat5/6 wire and terminating them with rj45/rj11 ends, depending on the use.
- Finding damaged copper and fiber line and repairing it, either on premise or in the field.
- This career allows me to work independently from other technicians and with little contact from supervisors.
- Every day I have multiple face to face contacts with our customers, in order to resolve any issues, or to install services, this requires me to translate technical terms and processes to customers who may not know the terms or processes.
- This part of the job focused mainly on soft skills.

MARCH 2010-SEPTEMBER 2014

**Technical Support** | Yada Systems Inc | Roseville

- I worked as a help desk technician providing phone support for Axalta's ColorNet Automotive Paint retrieval system software, as well as Axalta's ProfitNet Body Shop management system software and effectively logging the calls.
- Other support includes hardware troubleshooting of CPU's, printers and custom equipment such as paint scale, and the X-Pert Pour system, and diagnosing any defective hardware.
- I also directed customers on how to Peer to Peer networks, and install our software in server and client machines (in both a peer to peer setup and domain setup).
- Logging the calls, and following up on any unresolved issues.
- Between calls I worked on setting up an internal help web-page and installing it in a Server 2008 IIS7 environment, learning HTML, Java, CSS, and WIKI syntax as I created the page.

JULY 2001-JULY 2009

**Blackhawk Helicopter Technician** | Army National Guard

- Rank: E4 MOS: 15-T.
- Deployed from 2002-2004

## EDUCATION

DECEMBER 2021

**No Degree**: Cyber Security Bootcamp

University of Minnesota - Twin Cities, Minneapolis, MN
I am currently enrolled in the UofMN Cybersecurity bootcamp. During this course, I have further developed my networking knowledge as well as gained skills in cyber security. I have been exposed to numerous concepts, applications, and operating systems.

SEPTEMBER 2009

**A.A. degree**: Network Development
Brown College, Mendota Heights, MN
Graduated with distinction, GPA: 3.75