ASHLEY SKELTON

CYBER SECURITY STUDENT

702.285.0662 | Las Vegas, NV | askelton@email.arizona.edu | https://www.linkedin.com/in/ash-lianne-skelton/

QUALIFICATIONS

Analytical professional with hands-on project experience configuring network security, analyzing threats and infrastructure testing. Currently pursuing a BAS degree in Cyber Operations with University of Arizona. Exhibiting over ten years of experience in customer service, leadership, compliance and inventory control. Accelerated understanding of new concepts and effective implementation of new skills. Vibrant and joyful demeanor that strengthens company culture and drives company vision. Works above and beyond to finish projects thoroughly by the assigned deadlines. Efficient and productive, works well individually and with teams. Encourages and empowers colleagues while collaborating on group projects.

TECHNICAL STACK

SOFTWARE: Active Directory, AWS, Linux, NSM, Security Onion, Splunk, Nessus, Snort, Kibana, AlienVault, Wireshark, NMAP, VPNs, Firewalls, ACL, CVSS, CVE, Keyloggers, IPSec

SKILLS

- Threat Analysis
- Cryptography
- Network Security
- Packet Inspection
- Indicators of Compromise
- Infrastructure Testing
- Network Mapping

- Cyber Kill Chain
- Certificate Management
- Encryption
- Incident Response
- Endpoint Security
- Network Hardening
- Protocols & Services

- VPNs
- RDP
- DHCP
- IDS/IPS
- DNS
- OSI Model
- TCP/IP

HANDS-ON INDUSTRY PROJECTS

Completed during NexGenT's accelerated training program (01/2021 to 08/2021)

Disable Botnet - Red Team

Core Competencies: Network Protocols, Reconnaissance/Enumeration, Password Cracking and Exploration, Remote Administration

- Identify remote C2 server that is controlling a botnet
- Use Hydra to crack C2 server password
- Disable Apache httpd service

Stop Malicious Processes - Blue Team

Core Competencies: Application layer networking, Linux command line interface, packet capture, process analysis, and containment and eradication of malware

- Analyze network traffic attacking a financial institution
- Stop data exfiltration
- Remove artifacts and exfiltration process to prevent reinfection

Intercept Attack Plans (Russia / USA) - Red Team

Core Competencies: Offensive Red Team processes, Linux command line interface, systems administration, privilege escalation, MSFVenom

- Infiltrate Russian commanders workstation
- Escalate privileges through buffer overflow exploitation
- Obtain mission objectives file without detection

WORK HISTORY

NETWORK VULNERABILITY ASSESSMENT
Jan 2019 - Pres
Freelance | Remote
- Analyze network structure
- Device / OS / Software troubleshooting
- Network hardening
- Vulnerability assessments completed for 5 SOHO businesses

INVENTORY CONTROL SPECIALIST
Apr 2019 - Dec 2019
Bite One's Lip, LLC | Portland, OR
- Work directly with local law enforcement and the OLCC to correct non-compliance issues
- METRC administration
- Analyze inventory levels and adjustments made by the inventory managers
- Developed SOPs for company structure to minimize profit loss

INVENTORY MANAGER
Sep 2017 - Mar 2019
The Green Planet | Portland, OR
- Develop and nurture vendor relations
- Purchasing and buying for 3 high volume locations
- Worked directly with District Manager to lead meetings and ensure compliance
- POS integration

EDUCATION

University of Arizona | BAS in Cyber Operations: Defense and Forensics (NSA accredited CAE-CO and CAE-CD)
(Graduation in Dec 2022) Aug 2020 – Present
- Cyber warfare strategies
- Cyber Ethics, law and policy
- Vulnerability assessments / Incident response
- Penetration testing

NexGenT | Intensive 24-week military-grade engineering program
Cybersecurity Specialist Program Jan 2021 – Aug 2021
- 480 hours of training, education, and hands-on project experience
- Network Architectures and Networking for Cybersecurity
- Cyber Range Testing, Hacker Week, Labs / Skill Qualification Checks

---

CERTIFICATIONS

NexGenT Cyber Security Associate (NCSA) Apr 2021
NexGenT Cyber Security Professional (NCSP*)* Jun 2021
CompTIA Security+ *IN PROGRESS* --