**Kyser J. Clark – Penetration Tester**

(330) 575-8005 | Kyser@KyserClark.com | [linkedin.com/in/KyserClark](https://www.linkedin.com/in/kyserclark/) | [KyserClark.com](https://www.KyserClark.com) | [github.com/KyserClark](https://github.com/KyserClark)  
Secret Clearance | Available: April 23, 2024 | Current Location: Anchorage, Alaska | Highly Relocatable

**Career Summary**

I am a passionate cybersecurity professional with more than four years of active duty U.S. Air Force cyber defense operations experience specializing in offensive security, ethical hacking, penetration testing, and red teaming. I want to transition out of the military and into the private sector. My mission is to make cyberspace better & safer for everyone by committing to lifelong learning, sharing knowledge with the community, and inspiring others to do the same.

* B.S. Cybersecurity (WIP)
* CISSP
* OSCP (WIP)
* eJPT
* CEH
* PenTest+
* CySA+ (Results Pending)
* CCNA
* Cloud+
* Linux+
* Security+
* Network+
* Top 0.4% TryHackMe
* Home Lab & Self-Learner

**Core Competencies & Skills**

* Security Assessment Tools & Techniques
* System, Network, & Web App Exploitation
* Threat & Vulnerability Analysis
* Frameworks & Methodologies
* Governance, Risk, & Compliance (GRC)
* Cloud Computing & Virtualization
* Automation, Programming, & Scripting
* Architecture & Infrastructure Security
* Troubleshooting & Problem Solving
* Reporting & Communication Skills

**Professional Experience**

**Cyber Defense Operations (1D771) – Active Duty** April 2018 – PresentUnited States Air Force **–** Worldwide

* Led network inspection; identified 105 errors to harden system security, enabling 1,500 Air Mobility missions.
* Managed six classified message incidents; sanitized secret data leaks for 57 systems generating 15,600 sorties.
* Managed Squadron IT Asset program; inventoried/tracked 400 items valued at $600,000 across six facilities.
* Admin for Global Air Transportation and Execution System; supported 150 workstations & 183 system users.
* Technician for 3,100 joint service personnel with access to a telecommunications network worth $55 million.
* Coordinated workflow by synchronizing seven work centers and completed 5,000 trouble tickets in two years.
* Sustained 8,000 network devices enabling 43 F-16 fighter aircraft furthering North Korean nuclear deterrence.

**Construction Laborer – Full Time** August 2013 – April 2018  
Apache Industrial Services – Canton, Ohio

* Painting, sandblasting, fireproofing, asbestos abatement, and lead abatement in oil refineries & chemical plants.

**Education**

**Bachelor of Science (BS) in Cybersecurity Management & Policy** Projected August 2023 (114/120 Credits)University of Maryland Global Campus (UMGC)  
Minor in Business Administration | 3.95 GPA

**Associate of Science (AS) in Information Systems Technology** October 2022Community College of the Air Force (CCAF)

**Professional Certifications**

**(ISC)2 Certified Information Systems Security Professional (CISSP)** October 2022

**Offensive Security Certified Professional (OSCP)** Projected May 2023

**eLearnSecurity Junior Penetration Tester (eJPT)**  February 2023

**CompTIA Network Security Professional (CNSP)** Projected May 2023   
Security+ / PenTest+ / Cybersecurity Analyst (CySA+)

**CompTIA Network Vulnerability Assessment Professional (CNVP)** December 2022  
Security+ / PenTest+

**EC-Council Certified Ethical Hacker (CEH)** January 2023

**Cisco Certified Network Associate (CCNA)** September 2021

**CompTIA Secure Cloud Professional (CSCP)** November 2022   
Security+ / Cloud+

**CompTIA Cloud Admin Professional (CCAP)** November 2022Network+ / Cloud+

**CompTIA Linux Network Professional (CLNP)** October 2021  
Network+ / Linux+

You can get certification verification links at [KyserClark.com/resume](https://www.kyserclark.com/resume) or [linkedin.com/in/KyserClark](https://www.linkedin.com/in/kyserclark/).

**Home Labs, Self-Learning, & Projects**

**TryHackMe** [tryhackme.com/p/KyserClark](https://tryhackme.com/p/KyserClark)

* In the top 0.4%
* 161 rooms completed
* Level 13 – God (max)
* 22 badges
* Eight learning path certs
* 267-day ongoing streak
* Two room writeups

**100 Days of Code** **(Python)** [kyserclark.com/blog/categories/100-days-of-code](https://kyserclark.com/blog/categories/100-days-of-code)

* 240 hours
* Four video courses
* Read 2.2 books
* Five larger projects
* 176 small programs
* Network automation lab

**Additional**

* Cybersecurity content creator
* Avid infosec podcast listener
* Packet Tracer & Active Directory Labs
* [github.com/KyserClark/Hacking-Notes](https://github.com/KyserClark/Hacking-Notes)