

# Kyser J. Clark – Penetration Tester

---

(330) 575-8005 | [Kyser@KyserClark.com](mailto: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 | Relocatable | United States Air Force Veteran

## Career Summary

---

Cyber Defense Operations leader with 5+ years of active duty U.S. Air Force experience specializing in offensive security, ethical hacking, penetration testing, and red teaming. Possesses the experience, knowledge, and required credentials to make an immediate and valuable contribution to the penetration testing team. Credentials include B.S. in Cybersecurity, 11 certifications (including OSCP, CISSP, eJPT, PenTest+, CEH), and high leaderboard rankings in capture the flags (CTFs).

## Core Competencies & Skills

---

- Experienced in manual and automated network penetration testing and web application assessments.
- Proficient in red team engagements, threat actor emulation, and bypassing cybersecurity defenses.
- Exceptional with industry-standard tools and techniques. (Kali Linux, Nmap, Burp Suite, Metasploit, Mimikatz)
- Clear and concise written and verbal communication skills for reporting actionable mitigation strategies.
- Versed in automation, programming, and scripting. (Python, Bash, PowerShell, C, C#, VBA, PHP, JavaScript)
- Sharp at identifying and exploiting security vulnerabilities in Windows and Linux systems/servers.
- Strong knowledge of methodologies and frameworks. (OWASP, PTES, MITRE ATT&CK, Cyber Kill Chain, NIST).
- Adept in exploit development, leveraging advanced techniques for employing social engineering attacks.

## Professional Experience

---

### **Cyber Defense Operations (1D771) – Active Duty** United States Air Force – Worldwide

April 2018 – Present

- Led comprehensive vulnerability assessment, identifying and remediating 105 security vulnerabilities, reducing security risk, and bolstering system resilience for 1,500 Air Mobility missions.
- Managed and mitigated six classified message incidents, ensuring prompt sanitization of secret data leaks across 57 systems, supporting 15,600 successful sorties.
- Orchestrated Squadron IT Asset program, meticulously inventorying and tracking 400 items valued at \$600,000 across six facilities, ensuring optimal resource utilization and security.
- Acted as the primary administrator for the Global Air Transportation and Execution System, providing seamless support to 150 workstations and facilitating secure operations for 183 system users.
- Demonstrated technical expertise as a technician responsible for maintaining and securing a \$55 million telecommunications network, serving 3,100 joint service personnel.
- Streamlined network operations by effectively coordinating workflow among seven work centers, resulting in the timely resolution of 5,000 trouble tickets within a two-year period.
- Ensured uninterrupted network connectivity for 8,000 network devices supporting 43 F-16 fighter aircraft, playing a pivotal role in bolstering North Korean nuclear deterrence efforts.

## Education

---

**Bachelor of Science (BS) in Cybersecurity Management & Policy** (WIP)  
University of Maryland Global Campus (UMGC)  
Minor in Business Administration | 3.91 GPA

(Projected) August 2023 (114/120 Credits)

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

October 2022

## Professional Certifications

---

<b>OffSec Experienced Penetration Tester (OSEP)</b> (WIP)	(Projected) August 2023
<b>OffSec Certified Professional (OSCP)</b>	May 2023
<b>(ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP)</b>	October 2022
<b>eLearnSecurity Junior Penetration Tester (eJPT)</b>	February 2023
<b>CompTIA Network Security Professional (CNSP)</b> Security+ / PenTest+ / Cybersecurity Analyst (CySA+)	December 2022
<b>EC-Council Certified Ethical Hacker (CEH)</b>	January 2023
<b>Cisco Certified Network Associate (CCNA)</b>	September 2021
<b>CompTIA Secure Cloud Professional (CSCP)</b> Security+ / Cloud+	November 2022
<b>CompTIA Cloud Admin Professional (CCAP)</b> Network+ / Cloud+	November 2022
<b>CompTIA Linux Network Professional (CLNP)</b> Network+ / Linux+	October 2021

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

## Capture the Flags (CTFs) & Projects

---

### Hack The Box

[app.hackthebox.com/profile/766179](https://app.hackthebox.com/profile/766179)

- HTB Rank: Pro Hacker | 17 user & system owns | Global Ranking: #320
- Season 1 Place: 47/5987 (Top 0.8%) - Holo Tier
- Season 2 Place: TBD

### TryHackMe

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

- In the top 0.2% | 215 rooms completed | Level 13 – God (max) | 30 badges
- [Two room writeups](#) | 365-Day Streak Badge

### 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)