

# 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 Security Clearance | Relocatable | United States Air Force Veteran

## Career Summary

---

- Cybersecurity professional with 5+ years of enterprise experience specializing in offensive security, ethical hacking, penetration testing, and red teaming; highly skilled in finding and exploiting security vulnerabilities.
- Credentials include BS in Cybersecurity, 11 certifications (including OSCP, CISSP, eJPT, PenTest+, CEH, CySA+, CCNA, Cloud+, Linux+, Security+, and Network+), and high leaderboard rankings in capture the flags (CTFs).

## Professional Experience

---

### Penetration Tester & Security Consultant – DOD SkillBridge Internship

October 2023 – Present

TrustFoundry – United States (Remote)

- Performed extensive internal and external network penetration tests for two clients using manual and automated techniques to find 38 meaningful and verifiable findings across 429 systems/servers.
- Conducted one thorough web application assessment on two APIs to find 17 findings; performed cross-site scripting (XSS), Structured Query Language (SQL) injection (SQLi), and cross-site request forgery (CSRF) attacks.
- Expertly utilized industry-standard tools and techniques (Kali Linux, Nmap, Burp Suite Professional, Metasploit, Mimikatz, Impacket, Nuclei, Amass, CrackMapExec, Responder, Nessus, Shodan) in all live penetration tests.
- Wrote and delivered two clear and concise timely reports, providing clear insights and actionable mitigation strategies for all clients; peer-reviewed one more penetration test report before delivering to the customer.
- Leveraged automation, programming, and scripting skills (Python, Bash, PowerShell, C, C#, VBA, PHP, JavaScript).
- Identified and exploited vulnerabilities in Windows and Linux systems/servers, enhancing system security.
- Applied comprehensive knowledge of methodologies and frameworks (OWASP, PTES, MITRE ATT&CK, Cyber Kill Chain, NIST, ISO, PCI-DSS) across three penetration tests and web application assessments.
- Developed sophisticated exploits and executed advanced chained/multi-staged attacks for every PenTest.

### Penetration Tester & Security Consultant – Contract

August 2023

TrustFoundry – United States (Remote)

- Led vulnerability assessment of Barracuda and Azure firewalls on a client's production network, identifying 34 vulnerabilities; devised and delivered strategies to enhance and secure network traffic.

### Cyber Defense Operations (1D771) – Active Duty

April 2018 – Present

United States Air Force – Worldwide

- Led comprehensive vulnerability assessment, identifying and remediating 105 security vulnerabilities, reducing security risk by hardening a server supporting 1,500 Air Mobility missions.
- Managed and mitigated six classified message incidents, ensuring prompt sanitization of secret data leaks across 57 systems and contributing to the success of 15,600 Pacific Air Force missions.
- Orchestrated unit (organization) information technology (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 (GATES), providing seamless support to 150 workstations and facilitating secure operations for 183 system users.
- Streamlined security 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

---

<b>Master of Science (MS) in Cybersecurity Management and Policy (WIP)</b> University of Maryland Global Campus (UMGC)	(Projected) February 2025
<b>Bachelor of Science (BS) in Cybersecurity Management and Policy</b> University of Maryland Global Campus (UMGC) Minor in Business Administration   3.873 GPA   Honors: Cum Laude	August 2023

## Professional Certifications

---

<b>OffSec Experienced Penetration Tester (OSEP) (WIP)</b>	(Projected) December 2023
<b>OffSec Certified Professional (OSCP)</b>	May 2023
<b>ISC2 Certified Information Systems Security Professional (CISSP)</b>	October 2022
<b>INE Security 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

## Capture the Flags (CTFs) and Content Creation

---

<b>Hack The Box (HTB)/TryHackMe (THM) Player &amp; HTB Content Engineer</b>	December 2021 – Present
<ul style="list-style-type: none"><li>• Attained "Pro Hacker" rank on HTB, securing a global leaderboard ranking of #265 by compromising 41 machines, showcasing exceptional problem-solving skills and out-of-the-box thinking.</li><li>• Proved rapid resolution abilities during HTB Season 1, achieving 47th place out of 5987 competitors (top 0.8%).</li><li>• Further proved hacking skills and infosec passion during HTB Season 2, ranking 166/7390 (top 2.3%).</li><li>• Authored four machine writeups on personal blog website and created 28 YouTube video walkthroughs, highlighting clear and concise cybersecurity vulnerability documentation and reporting skills.</li><li>• Illustrated expertise in privilege escalation techniques, embracing the "Try Harder" mindset and mantra.</li><li>• Conducted successful web application attacks utilizing SQLMap, Nikto, and other tools to exploit vulnerabilities.</li><li>• Executed password cracking with John the Ripper and Hashcat, displaying competency in post-exploitation tasks.</li><li>• Demonstrated unwavering passion for the field and commitment to continuous learning, maintaining a 365-day hacking streak, completing 216 rooms, and achieving a top 0.2% global ranking on THM leaderboards.</li><li>• Collaborated with virtual teams to tackle multi-faceted HTB machines, displaying strong teamwork, communication, and problem-solving capabilities essential for real-world red teaming engagements.</li><li>• Published author for five captivating and engaging blog articles, showcasing exceptional communication and marketing skills to effectively engage readers and drive meaningful traffic to the HTB website.</li></ul>	