Kingston Banks

Entry-Level Penetration Tester

(614) 555-0186 kingston.banks@example.com
linkedin.com/example/kingstonbanks Columbus, Ohio 43215

STRENGTHS

Evidence-Based Analysis
Compared automated results with manual checks, then gave reviewers findings they could reproduce and trust.

Ethical Testing
Set clear boundaries before lab assessments; peers valued careful handling of authorized systems and sensitive evidence.

Technical Writing
Turned complex test results into concise reports with assets, steps, impact, and practical remediation guidance.

Collaborative Learning
Worked with faculty and student security teams, sharing lessons from CTF exercises and assessment reviews.

Persistent Problem Solving
When scanner output looked uncertain, repeated tests manually until evidence separated real weaknesses from noise.

SKILLS

Penetration Testing

Network Reconnaissance

Service Enumeration

Vulnerability Assessment

Web Application Security

OWASP Top 10 CVE CVSS

TCP/IP DNS HTTP/HTTPS

Authentication Testing Linux

Python Security Reporting

SUMMARY

Entry-level penetration tester and recent Cybersecurity graduate with supervised experience assessing networks, systems, and web applications in university labs, Capture the Flag exercises, and intentionally vulnerable environments. Conducted reconnaissance, **service enumeration**, **vulnerability scanning**, **manual validation**, and remediation retesting with Nmap, Burp Suite, Wireshark, Nessus, OpenVAS, Metasploit, Linux, Windows, Python, Bash, and PowerShell. Applied OWASP Top 10, CVE, CVSS, authentication, authorization, session management, input validation, and **rules of engagement** during authorized assessments. Documented affected assets, evidence, reproduction steps, impact, and remediation guidance in clear reports. Worked closely with faculty reviewers and student security teams, presenting findings with ethical judgment and practical recommendations. Ready to support careful security assessments and keep building offensive-security capability.

EDUCATION

Bachelor's Degree in Cybersecurity

Ohio University GPA: 3.8 2026 Athens, Ohio

Coursework: *Network security, ethical hacking, web application security, digital forensics*

TECHNICAL SKILLS

- **Reconnaissance Tools:** Nmap, Wireshark, Burp Suite
- **Vulnerability Scanners:** Nessus, OpenVAS, Metasploit
- **Operating Systems:** Linux, Windows, Kali Linux
- **Scripting Languages:** Python, Bash, PowerShell
- **Network Protocols:** TCP/IP, DNS, HTTP/HTTPS
- **Web Security Testing:** Burp Suite, OWASP Top 10, input validation
- **Identity Testing:** Authentication, authorization, session management
- **Vulnerability Standards:** CVE, CVSS, OWASP Top 10
- **Assessment Methods:** Reconnaissance, enumeration, manual validation
- **Reporting Practices:** Evidence capture, reproduction steps, remediation retesting

EXPERIENCE

Cybersecurity Penetration Testing Practicum

Midwest Cyber Range University Lab September 2025 - May 2026 Columbus, Ohio

Supported supervised penetration tests across segmented Linux and Windows lab networks, web applications, and authorized services. Established scope, followed rules of engagement, gathered evidence, reviewed findings, and presented remediation priorities to faculty reviewers.

- Established assessment scope and **rules of engagement** before testing authorized Linux and Windows hosts.
- Mapped **TCP/IP** services with Nmap, Wireshark, and Nessus across segmented laboratory **networks**.
- Compared scanner output with manual checks, separating outdated software findings from **false positives**.
- Validated **authentication**, authorization, session, and input weaknesses through Burp Suite web testing.
- Documented assets, evidence, **reproduction steps**, CVE references, CVSS factors, impact, and remediation guidance.
- Retested corrected findings after configuration changes and presented unresolved risks to faculty reviewers.

LANGUAGES

English — Native

Spanish — Beginner

MY CAREER

- Cybersecurity Penetration Testing Practicum at Midwest Cyber Range University Lab (8 Months)
- Web Application Security Researcher at Ohio State Cyber Range Project (7 Months)
- Offensive Security Lab Analyst at University CTF and Home Lab Program (3 Months)

Web Application Security Researcher

Ohio State Cyber Range Project | January 2025 - August 2025 | Columbus, Ohio

Researched web application weaknesses in a sandboxed e-commerce environment, creating repeatable tests and clear technical documentation. Coordinated controlled demonstrations, mapped findings to practical fixes, and helped faculty reviewers improve vulnerability prioritization.

- Evaluated selected **OWASP Top 10** categories across a sandboxed e-commerce application.
- Built Python and Bash utilities for HTTP data normalization and repeatable test cases.
- Discovered endpoints with **Burp Suite** and command-line tools during authorized **reconnaissance**.
- Reproduced confirmed issues with controlled payloads and captured request-response **evidence** safely.
- Mapped findings to **input validation**, session expiration, least-privilege **authorization**, and secure configuration fixes.
- Delivered a technical demonstration that earned faculty approval for repeatable testing procedures.

Offensive Security Lab Analyst

University CTF and Home Lab Program | September 2024 - December 2024 | Athens, Ohio

Completed guided offensive-security labs using isolated virtual machines and intentionally vulnerable **applications**. Practiced network enumeration, web testing, scripting, packet inspection, and vulnerability prioritization while maintaining clear ethical boundaries.

- Completed **Capture the Flag** challenges covering Linux, Windows, **network enumeration**, and web vulnerabilities.
- Configured isolated virtual machines with Nmap, Metasploit, Burp Suite, and Wireshark workflows.
- Wrote Python, Bash, and **PowerShell** scripts for banner collection and service checks.
- Investigated exposed services, weak credentials, outdated packages, and insecure configurations within lab authorization.
- Applied CVE terminology and CVSS factors to rank findings by exposure and **potential impact**.
- Presented six challenge findings to a campus security club with **remediation** lessons.

PROJECTS

Authorized Web Security Assessment Lab | 2026

Built a repeatable assessment workflow for an intentionally vulnerable application, combining reconnaissance, Burp Suite testing, evidence capture, OWASP Top 10 mapping, and remediation retesting.

Network Enumeration and Validation Lab | 2025

Practiced authorized host discovery and service analysis with Nmap, Nessus, Wireshark, and Linux command-line tools, then documented findings with CVE, CVSS, and remediation context.

LEADERSHIP & AWARDS

- Dean's List, Ohio University, Fall 2024 and Spring 2025
- Outstanding Technical Report, Ohio University Cyber Range Project, 2025
- Finalist, Midwest Collegiate Capture the Flag Challenge, 2025
- Cybersecurity Academic Scholarship, Ohio University, 2024-2026

CERTIFICATIONS

- Google Cybersecurity Professional Certificate | 2025
- CompTIA Security+ Preparation Certificate | 2026
- Cisco Networking Academy Introduction to Cybersecurity | 2024

PROFESSIONAL AFFILIATIONS

- Security Club Lab Coordinator, Ohio University, 2025-2026
- Capture the Flag Practice Team Member, Ohio University, 2024-2026
- Peer Presenter, Cyber Range Project Showcase, 2025

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST