Eli Castillo

(216) 555-0184 | eli.castillo.resume@example.com | linkedin.com/example/elicastillo | Cleveland, OH 44109

SUMMARY

Early-career **cybersecurity** candidate ready to support **penetration testing**, **cyber risk analysis**, **technical assessments**, and customer deliverables. Completed supervised security assessments, penetration-testing labs, and a Bachelor of Science in Cybersecurity in 2026. Academic work covered vulnerability analysis, network traffic review, Windows and Linux administration, TCP/IP and DNS troubleshooting, firewall evaluation, access-control testing, threat research, and technical reporting. Used Nmap, Wireshark, Burp Suite, and Nessus in controlled environments, documenting evidence against confidentiality, integrity, and availability principles. Practicum work included simulated alert triage, emerging-threat research, risk escalation, and briefings for faculty reviewers and student teams. Clear writing, careful evidence handling, sound judgment, and collaborative problem solving support dependable service for sensitive cybersecurity missions.

EDUCATION

Bachelor's Degree in Cybersecurity 2026

Cleveland State University GPA: 3.8 *Cleveland, OH*

Coursework: *Penetration Testing, Network Security, Operating Systems, Risk Analysis, Digital Forensics*

TECHNICAL SKILLS

- **Penetration Testing Tools:** Nmap, Burp Suite, Nessus
- **Network Analysis:** Wireshark, TCP/IP, DNS
- **Operating Systems:** Windows, Linux, Windows Server
- **Network Security:** Firewalls, network segmentation, service enumeration
- **Security Principles:** CIA triad, access control, threat concepts
- **Assessment Methods:** Vulnerability assessment, risk analysis, rules of engagement
- **Reporting Tools:** Technical reporting, screenshots, remediation tracking
- **Incident Analysis:** Alert triage, connection tracing, escalation
- **Research References:** NIST guidance, security advisories, threat research
- **Collaboration Platforms:** Git, version control, briefing materials
- **Documentation Practices:** Evidence logs, test plans, scope records
- **Web Security:** Authentication testing, access-control testing, attack-path review

SKILLS

- Penetration Testing
- Vulnerability Assessment
- Risk Analysis
- Technical Reporting
- TCP/IP
- DNS
- Firewalls
- Windows
- Linux
- CIA Triad
- Access Control
- Threat Research
- Incident Triage
- Customer Support
- Documentation

EXPERIENCE

Junior Penetration Tester, Academic Research Assistantship September 2025 - August 2026

University Cybersecurity Lab *Cleveland, OH*

Supported faculty-led security research across isolated Windows and Linux hosts, controlled web applications, network traffic reviews, and assessment **reporting**. Prepared evidence packages, maintained sensitive research records, joined weekly cyber reviews, and translated technical findings into practical remediation guidance for academic stakeholders.

- Executed supervised Nmap and Nessus reviews across isolated hosts, producing prioritized evidence packages for faculty review.
- Investigated **TCP/IP**, **DNS**, and firewall behavior in Wireshark, separating configuration issues from expected traffic.
- Tested web authentication and **access control** with **Burp Suite**, documenting reproducible findings without retaining credentials.
- Converted observations into assessment reports covering scope, severity, assets, screenshots, and practical remediation steps.
- Presented findings during weekly **cyber reviews**, answering methodology questions and revising records after peer feedback.
- Maintained version-controlled logs covering targets, tool settings, test dates, and cleanup actions for repeatability.

Junior Penetration Tester, Supervised Practicum January 2025 - August 2025

Cyber Defense Practicum *Cleveland, OH*

Completed supervised cyber defense work across a simulated small-business network with Windows workstations, a Linux server, DNS services, and a perimeter firewall. Supported threat analysis, incident triage, customer-style reporting, security research, briefing preparation, and escalation decisions within defined rules of engagement.

- Assessed **Windows**, **Linux**, DNS, and firewall exposure across a simulated small-business network under approved rules.
- Mapped services to **threat concepts** and **CIA triad** impacts, separating observations from risks requiring escalation.
- Traced unusual connections with Wireshark and Nmap, producing a documented timeline for response-team review.
- Researched phishing, credential abuse, and exposed-service **techniques** through NIST-aligned advisories and reference material.
- Drafted customer-style **deliverables** translating weaknesses into business concerns, recommended controls, and validation steps.
- Coordinated four-person review scheduling, tracked open questions, and delivered an accurate security briefing.

Junior Penetration Tester, Capstone Team

September 2024 - December 2024

Cybersecurity Capstone Project

Cleveland, OH

Contributed to a supervised capstone assessment involving a six-host virtual environment, network segmentation, Windows and Linux hardening, firewall review, web testing, evidence handling, and faculty presentation. Helped define scope, validate remediation, document residual risk, and communicate findings within ethical testing boundaries.

- Built a six-host virtual environment for segmentation, Windows hardening, Linux hardening, and firewall testing.
- Defined an authorized plan covering discovery, enumeration, credential hygiene, and evidence handling before scans.
- Identified outdated services and broad permissions, then validated fixes through repeat scans and configuration comparisons.
- Inspected a vulnerable web workflow with Burp Suite, documenting approved attack paths and ethical boundaries.
- Produced a twenty-page report with methodology, limitations, risk summaries, screenshots, and remediation priorities.
- Presented residual-risk findings to instructors and classmates, addressing scope, false positives, and testing limits.

PROJECTS

Controlled Web Application Assessment 2025

Created a supervised testing exercise for authentication and access-control scenarios. Used Burp Suite, captured reproducible evidence, protected test data, and presented remediation priorities for faculty review.

Network Threat Review Lab 2025

Built a focused lab for TCP/IP, DNS, firewall, and unusual-connection analysis. Combined Nmap and Wireshark findings into a clear escalation brief for a simulated response team.

Virtual Host Hardening Study 2024

Evaluated segmentation, Windows and Linux hardening, exposed services, and broad permissions across six virtual hosts. Repeat scans confirmed remediation and clarified residual risk.

LEADERSHIP & AWARDS

- Dean's List, Cleveland State University, Fall 2025 and Spring 2026
- Cyber Defense Practicum Excellence Award, 2025
- Capstone Presentation Recognition, Cleveland State University, 2024

CERTIFICATIONS

- Google Cybersecurity Professional Certificate 2025
- Cisco Networking Academy Cybersecurity Essentials 2025

PROFESSIONAL AFFILIATIONS

- Cybersecurity Club, Peer Lab Coordinator, Cleveland State University, 2025-2026
- Student Cyber Defense Team, Training Participant and Briefing Volunteer, 2024-2026

LANGUAGES

- English (Native)
- Spanish (Proficient)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST