

# DAISY ADELINE HARRIS

Freetown, Sierra Leone • daisyharris566@gmail.com  
LinkedIn • GitHub • Portfolio

## SUMMARY

---

Cybersecurity student (GPA 3.94) at Old Dominion University with hands-on experience in network scanning, packet analysis, web application testing, and firewall configuration. Comfortable in Linux and virtualized lab environments using industry tools like Nmap, Wireshark, and Burp Suite. Seeking an internship or entry-level role where I can contribute to defensive and offensive security operations while continuing to grow technically.

## EDUCATION

---

Old Dominion University — Norfolk, VA

*B.S. in Cybersecurity, Minor in Risk Management & Insurance | GPA: 3.93 | Expected May 2027 | Dean's List*

**Relevant coursework:** Ethical Hacking & Penetration Testing, Networked Systems Security, Cybersecurity Techniques & Operations, Linux Systems for Cybersecurity, Networking & Security, Cybersecurity Programming, Cyber Law, Cybersecurity Ethics.

## SKILLS

---

- **Networking:** TCP/IP, subnetting, DNS, DHCP, common ports & protocols
- **Security concepts:** CIA triad, authentication, access control, basic threat modeling
- **Tools:** Nmap, Wireshark, Burp Suite, OpenVAS
- **Operating Systems:** Linux (Kali, Ubuntu), Windows
- **Virtualization:** UTM, VirtualBox-style lab environments
- **Programming:** Python (scripting), Bash (basics)

## PROJECTS

---

### Linux User, Group & Permission Management

- Managed Linux users, groups, and file permissions.
- Configured shared directories with controlled access using group ownership and permission settings (rwx, umask).
- Investigated permission behavior and group ownership changes after deletion events.

### Network Security and Traffic Analysis with Wireshark

- Captured and analyzed network traffic using Wireshark to examine ICMP, DNS, FTP, and TCP communications.
- Applied protocol filters to isolate and investigate specific network activity and DNS resolution behavior
- Identified security risks by intercepting plaintext FTP credentials and reconstructing transferred files from packet captures.

### Web Application Security Testing

- Assessed intentionally vulnerable web apps for OWASP-style flaws including injection, broken authentication, and input validation weaknesses.
- Proposed mitigations such as input sanitization, parameterized queries, and stricter session handling.

### Network Scanning & Firewall Configuration

- Authored and implemented pfSense firewall rule sets to allow or deny traffic based on port, protocol, and source/destination IP addresses.
- Validated firewall effectiveness through Nmap scanning and traffic testing, refining policies based on observed results.

### Active & Passive Reconnaissance

- Performed active reconnaissance using Nmap for ICMP sweeps, TCP port scanning, service detection, and OS fingerprinting in controlled environments.
- Conducted DNS enumeration and zone transfer testing using dnsenum to evaluate DNS security posture.
- Used Shodan and WHOIS for passive reconnaissance to identify exposed services and internet-facing infrastructure.
- Mapped findings to CVEs and MITRE ATT&CK framework to analyze potential attack vectors and system exposure.

## LEADERSHIP & INVOLVEMENT

---

### Vice President — Interact Club

- Led planning and execution of community service initiatives and campus events.
- Coordinated cross-functional volunteer teams and grew member engagement through regular outreach.
- Built project management, public speaking, and interpersonal communication skills.