Daniel Irving

✉ danielirving028@gmail.com ☎ +1 (876) 834-0392 📍 Westmoreland, Jamaica

Professional Summary

Cybersecurity student with hands-on experience in penetration testing and vulnerability assessment, seeking an internship to gain practical industry experience. Skilled in identifying vulnerabilities, exploiting and securing systems, and delivering actionable remediation strategies. Proficient with tools such as Metasploit, Nmap, Burp Suite, Nessus, and Wireshark, with a strong academic foundation in ethical hacking and network security.

Education

Bachelor of Science – Computer Networking and Security, 09/2022 – Present
University of Technology, Jamaica
Relevant Coursework: Ethical Hacking, Security Testing & Detection, Enterprise Security, Cyber Security, Computer Security, Network Administration & Technical Support
Network Operating Systems Administration

Technical Skills

Penetration Testing & Offensive Security
Metasploit Framework, Password Cracking (Hydra), Privilege Escalation, CTF Methodologies

Network Security & Firewall Configuration
pfSense, iptables, Cisco Packet Tracer, VLAN Segmentation, Network Traffic Analysis (Wireshark), Intrusion Detection Systems (Snort)

Operating Systems & Services
Linux Administration (Kali, Ubuntu), Windows Server & Active Directory, FTP/SSH/SMB/MySQL Exploitation

Vulnerability Assessment & Risk Analysis
Nessus, OpenVAS, Nmap, Nikto, Vulnerability Scanning

Reconnaissance & Enumeration
Nmap, Dirb, Gobuster, Enum4linux, Google Dorking (GHDB), WHOIS Lookups, SSL/TLS Testing (Testssl.sh)

Web Application Security
SQL Injection, Phishing Simulation, Directory Enumeration, Security Header Analysis

Cybersecurity Projects & Hands-On Labs

Advanced Vulnerability Assessment

- Conducted a comprehensive vulnerability assessment using Nmap, Nessus, Nikto, Dirb, Enum4linux, and testssl.sh.
- Identified critical vulnerabilities including Samba remote code execution (RCE), SSH misconfigurations, and SSL/TLS weaknesses.
- Performed cross-tool validation to confirm findings and reduce false positives.
- Developed detailed remediation recommendations, prioritizing risks using CVSS scoring.

Penetration Testing Lab exercises

- Performed network reconnaissance and enumeration using fast, stealth, and full Nmap scans, identifying exposed services.
- Utilized ExploitDB to identify known vulnerabilities and corresponding exploits for FTP, SMB, and SSH services during lab-based penetration testing.
- Exploited FTP, SSH, VNC, and Samba services using Metasploit and credential brute-forcing techniques.
- Conducted user enumeration via SMB, SMTP, and null session exploitation.
- Achieved privilege escalation from standard user to root access through service misconfigurations and known vulnerabilities.

Web Application Security & OSINT

- Conducted passive reconnaissance and OSINT using WHOIS, ARIN/RIPE databases, and geolocation services.
- Performed Google Dorking to uncover exposed credentials, administrative portals, and sensitive files.
- Utilized TheHarvester, HTTrack, and CeWL for in-depth website footprinting and intelligence gathering.

- Scanned web applications using Nikto and OpenVAS to identify outdated software, insecure configurations, and common web vulnerabilities.

Network Security Infrastructure

- Configured and managed pfSense and iptables firewalls to enforce security policies and traffic filtering.
- Designed a hierarchical network topology using Cisco Packet Tracer, implementing routing and VLAN segmentation.
- Deployed Snort IDS for intrusion detection and analyzed network traffic using Wireshark.
- Implemented a Windows Server environment with Active Directory, user management, shared resources, and access controls.
- Simulated phishing, SQL injection, Credential Bruteforce attack and DDoS attacks in controlled lab environments to evaluate defensive readiness