WOTMERS TECHNOLOGIES LTD

Cybersecurity

Defend Networks, Protect Data, Secure the Digital World

Duration	Level	Course Fee	Delivery
12 Weeks (Full-Time) / 24 Weeks (Part-Time)	Beginner to Intermediate	NGN 120,000	In-Person | Abuja & Kaduna

Course Overview

This comprehensive Cybersecurity programme equips students with the knowledge and practical skills required to protect computer systems, networks, and sensitive data from modern digital threats. Beginning with foundational IT concepts and progressing through ethical hacking, incident response, and cloud security, graduates are prepared for entry-level to mid-level cybersecurity roles across industries. The curriculum aligns with globally recognised frameworks including CompTIA Security+ and the NIST Cybersecurity Framework.

Course Curriculum

Week	Topic	What You Will Learn
Wk 1	**Foundations of IT & Networking**	OSI model, TCP/IP, DNS, DHCP, HTTP/S, subnetting, network topologies and protocols
Wk 2	**Introduction to Cybersecurity**	CIA Triad, threat actors, attack vectors, vulnerabilities vs exploits, security governance
Wk 3	**Operating Systems Security**	Windows and Linux hardening, user permissions, file system security, process monitoring
Wk 4	**Cryptography**	Symmetric/asymmetric encryption, hashing, PKI, SSL/TLS, digital certificates and signatures
Wk 5	**Network Security**	Firewalls, IDS/IPS, VPNs, DMZ, network segmentation, traffic analysis with Wireshark
Wk 6	**Ethical Hacking & Penetration Testing**	Phases of pen testing, reconnaissance (OSINT), scanning with Nmap, vulnerability assessment
Wk 7	**Exploitation Techniques**	Metasploit framework, web app attacks (SQL injection, XSS, CSRF), password cracking
Wk 8	**Web Application Security**	OWASP Top 10, Burp Suite, input validation, authentication flaws, security headers

Wk 9	**Incident Response & Forensics**	Incident lifecycle, evidence collection, log analysis, memory forensics, chain of custody
Wk 10	**Security Operations Centre (SOC)**	SIEM tools, threat intelligence, alert triage, Splunk basics, monitoring dashboards
Wk 11	**Cloud & Mobile Security**	AWS/Azure security basics, shared responsibility model, mobile threat landscape, MDM
Wk 12	**Capstone Project & Career Prep**	Full pen test simulation, vulnerability report writing, certification roadmap, interview prep

Learning Outcomes

By the end of this course, students will be able to:

- ✓ Identify, analyse, and mitigate cybersecurity threats
- ✓ Configure firewalls, IDS/IPS, and VPN systems
- ✓ Analyse network traffic to detect anomalies and attacks
- ✓ Write professional security assessment reports
- ✓ Perform basic penetration testing and vulnerability assessments
- ✓ Implement cryptographic controls to protect data
- ✓ Respond to security incidents using industry frameworks
- ✓ Understand compliance standards (ISO 27001, GDPR, NDPR)

Tools & Technologies Covered

Kali Linux	**Metasploit**	**Wireshark**	**Nmap**
Burp Suite	**Splunk**	**Nessus/OpenVAS**	**John the Ripper**

Career Opportunities

➤ SOC Analyst	➤ Penetration Tester	➤ Network Security Engineer
➤ Information Security Analyst	➤ Cybersecurity Consultant	➤ Digital Forensics Analyst

Ready to enrol? Visit wotmerstechnologies.com/register.html | Email: wotmersinfo@gmail.com | WhatsApp: +234 8125604035