O-RANGE CYBERSECURITY

TRAINING & SERVICES LTD

COURSE OUTLINE BROCHURE

Cybersecurity & Ethical Hacking • Bug Bounty Hunting • GRC • VAPT • OSINT

CYBERSECURITY	BUG BOUNTY	VAPT	OSINT	GRC
6 Months	5 Weeks	4 Weeks	4 Weeks	Flexible

info@o-rangecybersecurity.com | 09034847995 | **www.o-rangecybersecurity.com** | 23 Taiwo Akinsanya, Oshodi/Isolo, Lagos, Nigeria

ABOUT OUR SCHOOL

O-Range Cybersecurity Training & Services Ltd is a Lagos-based cybersecurity training institution committed to equipping individuals with practical, industry-relevant skills. Our programmes are designed and delivered by certified ethical hackers and security professionals with real-world experience, ensuring every learner gains hands-on proficiency and career-ready competencies.

WHY STUDY WITH US?

- Hands-on practical learning approach
- Real-world cybersecurity simulations
- Mentorship from industry professionals
- Career guidance and interview preparation
- Access to recorded classes and lab environments

LEARNING FORMATS

- Beginner-friendly learning structure
- Physical classroom training
- Online live classes
- Weekend and weekday learning options
- Practical, hands-on sessions
- Continuous assessments and assignments

PROGRAMME 1 — CYBERSECURITY & ETHICAL HACKING 6 MONTHS

A 6-Month Comprehensive Training Programme

This intensive programme takes students from foundational concepts through to advanced offensive and defensive security techniques. Delivered through guided instruction, hands-on labs, and real-world simulations, graduates will be equipped to pursue careers as penetration testers, SOC analysts, and security consultants.

COURSE MODULES

01	Introduction to Cybersecurity & Threat Landscape
02	Networking Fundamentals for Security (TCP/IP, OSI, DNS)
03	Operating Systems Security (Windows & Linux)
04	Cybersecurity Tools & Environment Setup
05	Web Technologies Basics
06	Web Application Security (OWASP Top 10)
07	Introduction to Cryptography
08	Identity & Access Management (IAM)
09	Governance, Risk and Compliance
10	Security Operations Center (SOC) Fundamentals
11	Log Analysis & SIEM Tools (e.g., Splunk)
12	Incident Detection & Response
13	Threat Intelligence & Threat Hunting
14	Vulnerability Assessment & Management
15	Penetration Testing Methodology
16	Exploitation Techniques & Tools (Burp Suite, Metasploit)
17	Cloud Security Fundamentals (AWS, Azure basics)
18	Digital Forensics & Malware Analysis
19	AI & Cybersecurity
20	Capstone Project / Real-World Simulation

LEARNING OUTCOMES

By the completion of this programme, students will be able to:

1. Understand core cybersecurity concepts, threats, and defense mechanisms
2. Analyse network traffic and identify suspicious activities
3. Perform vulnerability assessments and basic penetration testing
4. Use industry tools such as SIEMs, Burp Suite, and scanners effectively
5. Detect, respond to, and report security incidents
6. Apply security best practices across systems, networks, and applications
7. Understand compliance standards and risk management principles
8. Build a foundational cybersecurity home lab for continuous practice

LEARNING PATHWAYS / CAREER ALIGNMENT

Students will be prepared for entry-level roles such as:

1. Security Operations Center (SOC) Analyst
2. Junior Penetration Tester
3. Cybersecurity Analyst
4. IT Security Support Specialist
5. Vulnerability Assessment Analyst
6. Threat Intelligence Analyst (Junior Level)

TRAINING MATERIALS

Type of materials provided

1. Instructor-led slides and presentations
2. Recorded video sessions for each class
3. Hands-on lab environments (TryHackMe, Hack The Box, custom labs)
4. Practical assignments and real-world scenarios
5. Tool walkthroughs and guided exercises

Access to recorded sessions

All online sessions will be recorded and shared with students for revision.

Additional resources

- Cheat sheets and playbooks
- Practice questions and assessments
- Recommended reading materials and documentation

PROGRAMME 2 — BUG BOUNTY HUNTING 5 WEEKS

A 5-Week Intensive Bug Bounty Hunting Practical Programme

This beginner-to-advanced programme equips participants with the real-world skills needed to legally hack websites, discover vulnerabilities, and earn rewards through bug bounty platforms — no prior hacking experience required. The course is delivered by Coy Emerald, a certified ethical hacker with verified bounties from Apple, Google, Facebook, and other global companies.

Why choose this programme

- No prior coding or hacking experience required
- Works on any basic laptop — no expensive equipment needed
- Practical, proven techniques used in real-world bounty hunting
- Directly taught by a professional who has earned bounties from Apple and other global companies

WEEKLY CURRICULUM

WEEK 1 — Introduction & Foundation

- What is Bug Bounty Hunting?
- Overview of bug bounty and vulnerability disclosure programmes
- Introduction to penetration testing concepts
- Choosing Bug Bounty as a career path

WEEK 2 — Getting Started with Web Application Hacking

- How to ethically hack websites and web applications
- Platforms for finding and enrolling in bug bounty programmes
- Scoping, legal boundaries, and ethical guidelines
- Knowing when to escalate or stop

WEEK 3 — Real-World Hacking Techniques

- Information disclosure & directory listing
- Cross-site scripting (XSS) & HTML injection
- Open redirect & broken link hijacking
- Remote code execution (RCE)
- Content & email spoofing
- Improper access control, IDOR/UDOR
- Business logic errors & authentication flaws
- File upload vulnerabilities & WordPress testing
- Must-have tools for efficient bug bounty hunting

WEEK 4 — Advanced Case Studies & Reporting

- Live case study: hacking Google using Google
- Live case study: four Apple bounties in one month
- Live case study: Facebook vulnerability in under five minutes
- Bypassing two-factor authentication (2FA) techniques
- How to write effective, actionable vulnerability reports
- Submitting findings for maximum programme impact and payout

WEEK 5 — Assessment & Certification

- Practical assessment on a controlled target environment
- Vulnerability report submission and review

PROGRAMME 3 — GOVERNANCE, RISK & COMPLIANCE (GRC)

A Practical Introduction to GRC for Security Professionals

GOVERNANCE, RISK, AND COMPLIANCE (GRC)

- Introduction to GRC
- Understanding the role of a GRC professional
- Importance of GRC in organizations
- Exploring some free, open-source GRC and organizational tools

REGULATORY COMPLIANCE

- Introduction to regulatory compliance requirements (e.g., NDPR, GDPR, HIPAA, PCI DSS)
- Compliance assessment methodologies

STANDARDS AND FRAMEWORKS

- Overview of GRC frameworks and standards (e.g., ISO 27001, NIST RMF, COBIT, ISO 42001, COSO, CIS, etc.)
- ISO 27001 implementation

SECURITY AWARENESS AND TRAINING

- Importance of security awareness and training programs
- Designing and delivering an effective training module
- Assessing training effectiveness

INFORMATION SECURITY POLICY DEVELOPMENT

- Policy, standards, and procedures
- Types of policy (system-specific, enterprise, and issue-specific)

RISK MANAGEMENT

- Risk identification, assessment, and mitigation strategies
- Risk appetite and tolerance levels
- Risk monitoring and reporting
- Business impact analysis / business continuity management
- Understanding threats (STRIDE, PASTA) and vulnerabilities

THIRD-PARTY RISK MANAGEMENT (VENDOR, CONTRACTOR, SUPPLIER)

- Vendor selection and assessment
- Contractual and legal considerations
- Third-party risk management / enterprise risk management

AUDIT

- Internal and external audit processes

EMERGING TECHNOLOGY

- AI governance, GRC technologies, and latest trends

TUITION & PAYMENT OPTIONS

1. Cybersecurity Full Programme (6 Months)

Physical	**₦1,500,000**
Online	**₦1,000,000**

2. Bug Bounty Hunting Programme (5 Weeks)

Physical	**₦1,000,000**
Online	**₦500,000**

3. Vulnerability Assessment & Penetration Testing (VAPT)

Physical	**₦1,000,000**
Online	**₦500,000**

4. Open Source Intelligence (OSINT)

Physical	**₦1,000,000**
Online	**₦500,000**

5. Governance, Risk & Compliance (GRC)

Physical	**₦600,000**
Virtual	**₦500,000**

SIWES Students

6-Month Fixed Rate (Physical Cybersecurity classes)	**₦500,000**

Students on SIWES pay a discounted, fixed training fee of ₦500,000 for the full six-month period, which gives them access to our physical cybersecurity classes.

CONSULTATIONS

If you are seeking personalised guidance, we offer a Cybersecurity Clarity Session at a fee of ₦20,000 for 30 minutes. The session can be conducted via Google Meet or WhatsApp Call, depending on your preference.

During this session, we can discuss your cybersecurity career path, learning roadmap, technical challenges, skill development strategy, certification goals, or any other cybersecurity-related concerns you may have. The objective is to provide you with practical guidance, clarity, and actionable next steps tailored to your specific goals.

CERTIFICATION

Students who successfully complete the programme and assessments will receive an O-Range Cybersecurity Training Certificate of Completion.

Top-performing students may also receive recommendation opportunities for internships and advanced mentorship.

ENROL & CONTACT US

LOCATION

23 Taiwo Akinsanya, Oshodi/Isolo, Lagos, Nigeria

GET IN TOUCH

info@o-rangecybersecurity.com

09034847995 • 09169593829

www.o-rangecybersecurity.com