Cybersecurity Certificate Course

Instructor: Nimshan Bandara (Cybersecurity Analyst, BSc in Information Technology – Cyber Security)

Orientation Program

- What a SOC does (monitoring, triage, escalation, reporting)
- SIEM basics: log sources, alerts, correlation (high-level)
- Log analysis workflow + triage mindset
- What pentesting is (scope, permissions, Rules of Engagement)
- Engagement phases (recon → scanning → validation → reporting)
- What "exploitation" means in a *training* context: understanding risk + mitigation
- Professional reporting structure
- Governance vs Risk vs Compliance (who owns what)
- Risk terminology and what employers expect (risk register, control mapping)
- Framework overview and evidence mindset

Cybersecurity Foundations + Environment Setup

- Networking basics
- Introduction to cybersecurity
- Environment configuration
- Information & information security terminology
- Core security concepts
- User security principles

Ethernet & LAN Switching + VLAN Concepts

- Ethernet LAN devices
- Switching concepts
- VLAN segmentation: purpose and real business value
- Types of VLANs + benefits
- VLAN configuration concepts

IPv4 Addressing + Subnetting for Real Networks

- Address classes
- IPv4 fundamentals
- IPv4 subnetting
- Ports: how services expose risk

TCP/IP Model + Connection Behavior

- TCP/IP model
- Three-way handshake
- TCP vs UDP
- TCP states

- TCP header basics

CS Foundations Used in Security + Vulnerability Concepts

- Algorithms overview
- String matching
- Data structures: queues, stacks; pop/push methods
- Deadlock concept
- Buffer overflow overview

Availability Attacks + Linux Basics

- DoS (Denial of Service) concepts + business impact
- DDoS concepts + resilience controls
- Linux basics

Web Fundamentals + Secure Web Controls

- HTTP/HTTPS fundamentals
- Web cookies and sessions
- SSL/TLS overview
- Security headers overview
- Website hack demo

SOC In-Depth + Operating Model

- SOC workflow: alert → triage → escalate → close
- Severity vs priority + false positives
- SIEM role in SOC

Log Analysis + Triage Execution

- Log sources
- Log analysis workflow
- Triage decision

Threat Intelligence + Malware Sandboxing + Credential Abuse Case Study

- Threat intelligence: IOCs vs TTPs
- Malware sandboxing workflow
- Credential abuse case study – mimikatz demo
    - What credential dumping is
    - What defenders look for
    - Hardening controls

Cryptography Part 1

- Cryptography fundamentals
- Encryption vs decryption
- Where encryption is used in real systems

Cryptography Part 2 + Access Controls

- Hashing vs encryption
- Access controls
- Steganography

PKI & Key Architecture + SSO

- PKI
- Key architecture basics

- SSO concepts and common security pitfalls

Pentesting Introduction

- Pentesting vs vulnerability assessment
- Scope, permissions, Rules of Engagement
- Reporting: business impact and remediation guidance

Reconnaissance

- Recon concepts
- Target profiling
- Documenting findings professionally

Scanning

- Scanning concepts and how defenders use results
- Prioritization: severity vs exploitability vs business impact
- Turning scan results into a remediation plan

Exploitation & post-exploitation + Reporting

- Exploitation concepts
- Post-exploitation concepts
- Finalization and reporting (professional pentest report format)

SQL, SQL Injection + XSS

- SQL fundamentals
- SQL Injection: concept, impact, prevention
- XSS overview: concept, impact, prevention

- XSS Live Hack demo

Introduction to GRC + Risk Management

- GRC fundamentals (governance, risk, compliance)
- Risk terminology and real-world usage
- Risk management process end-to-end
- NIST overview (framework mindset)

Risk Frameworks + ISO 27001

- QRA concepts (qualitative risk assessment)
- OCTAVE framework overview
- ISO 27001 overview (ISMS basics)

Introduction to Cyber Forensics

- What forensics is and when it's used
- Case workflow
- Forensic reporting mindset

Data Acquisition

- Acquisition concepts (what is collected and why)
- Integrity concept
- Avoiding evidence contamination

Digital Evidence + Analysis

- Computer crimes overview
- Digital evidence types and handling

- Analysis Part 1 + Part 2
- Writing findings clearly

Final Evaluation + Cybersecurity Interview question Practise