



Cyber Security: Comprehensive Introductory Course

Certified Ethical Hacking Syllabus — **Course Code: CS-4551**

4.0 CREDIT HOURS | 60 CONTACT HOURS

HYBRID: IN-PERSON & LIVE ONLINE LAB

\$499.95 PER PERSON

Course At a Glance

Instructor

Dr. Robert Steven Owor, Ph.D.
Securetsys Cyber Security Consultant

Terms Offered

Fall / Spring / Summer

Delivery

Hybrid — In-Person & Live Online Lab via Google Classroom

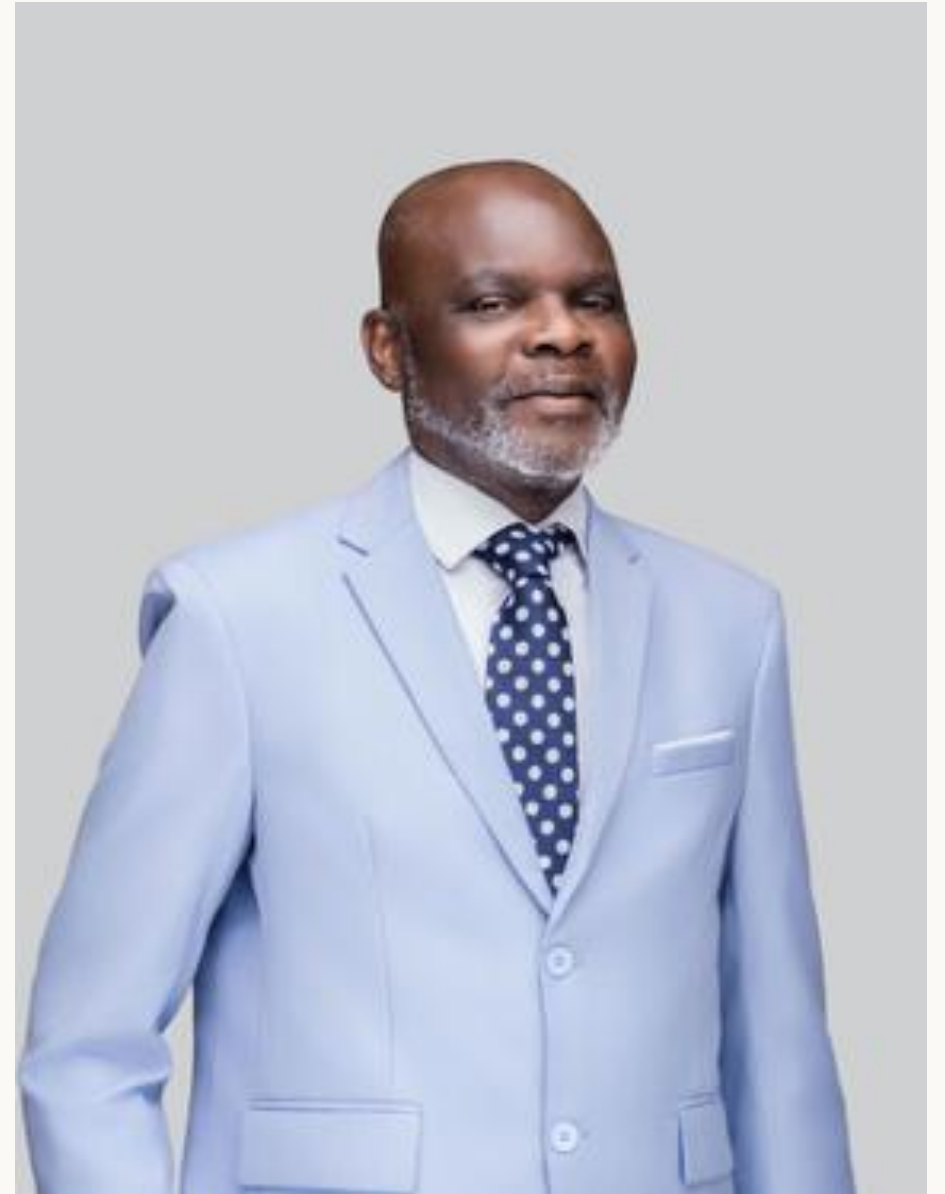
Tuition

\$499.95 per person. Link & Registration code provided upon enrollment.

Course Overview

CS-4551 bridges rigorous theoretical frameworks with hands-on labs. Students explore the historical evolution of computer crime, analyze contemporary threat vectors, examine defensive architectures, and navigate professional pathways in cyber security.

The course covers ethical hacking practice, principles, and operations — preparing students to sit and pass the **Certified Ethical Hacker (CEH)** exams.



Dr. Robert Steven Owor

"Cyber security is not merely about blocking malicious hackers; it is about establishing resilient organizational trust, safeguarding human lives in healthcare environments, and preserving democratic stability in the digital age."

— Dr. Robert Steven Owor, Instructor Philosophy

Meet Your Instructor

Dr. Robert Steven Owor, Ph.D.

Principal Consultant, Securetsys Cyber Security
Consultant

Over **two decades** of hands-on experience protecting critical infrastructure, financial institutions, and government networks.

Academic Credentials

- **Ph.D.** — Computer Science & Software Engineering
- **M.Sc.** — Computer Science
- **B.Sc.** — Computer Science

Instructor Certifications Training



CISSP

Certified Information Systems Security Professional



CISM

Certified Information Security Manager



CEH

Certified Ethical Hacker



CompTIA

Security+ & Advanced Security Practitioner (CASP+)

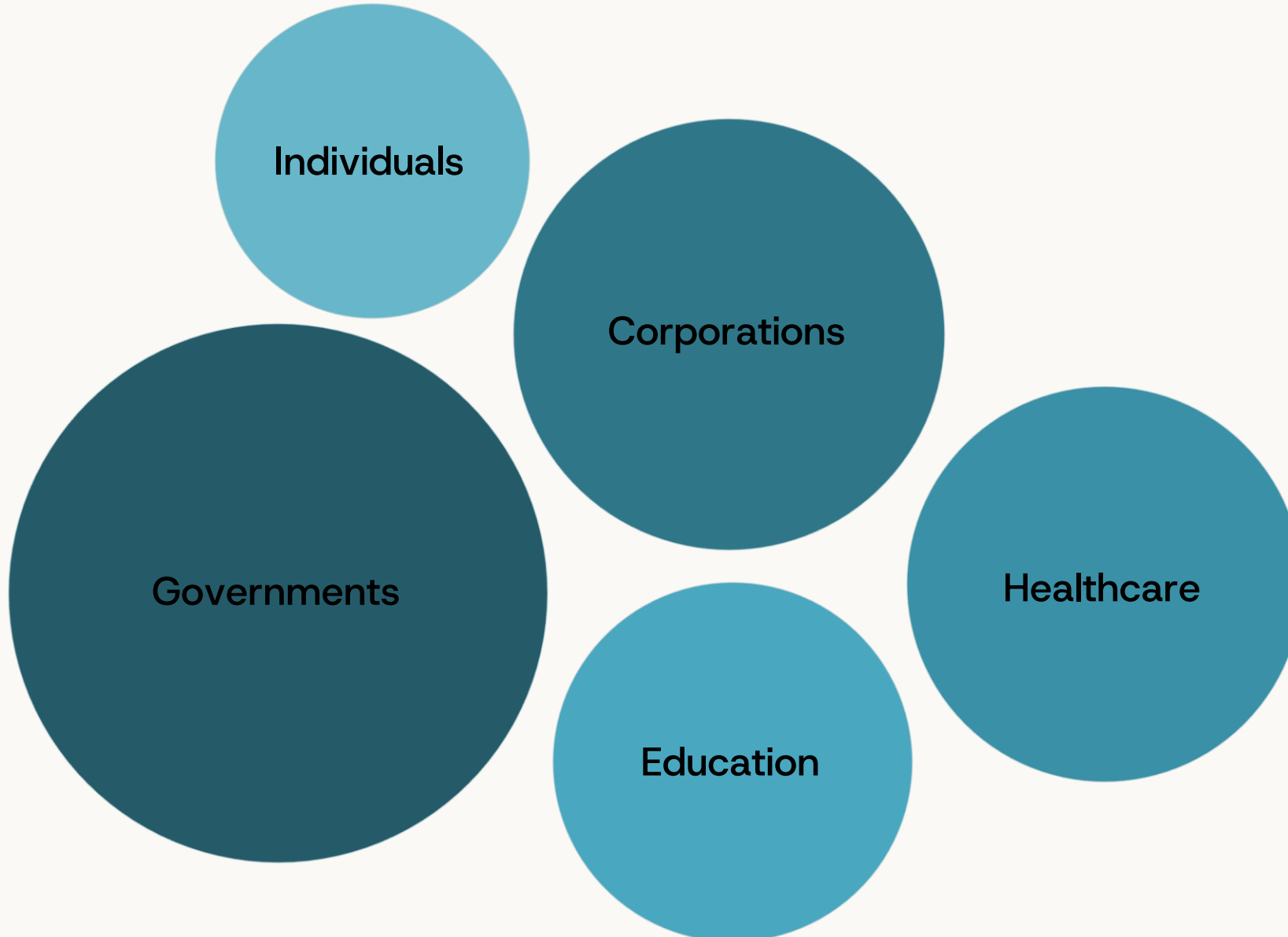
Dr. Owor's Industry Leadership

Dr. Owor has designed and delivered executive security training for **Fortune 500 boardrooms**, federal defense agencies, and major healthcare hospital networks across North America and internationally. His research in cryptographic resilience and zero-trust network architecture has shaped industry standards. He brings real-world incident response narratives directly into the classroom — frontline combat against advanced persistent threats (APTs).



Cyber Security Impacts Every Sector

A core premise of CS-4551 is that cyber security touches every facet of modern society. Students examine sector-specific vulnerabilities, regulatory compliance frameworks, and real-world disaster scenarios across five critical domains.





Governments & National Security

Nation-state actors engage in continuous cyber espionage, infrastructure disruption, and electoral interference. Governments must secure classified intelligence, defense supply chains, voter databases, and municipal utilities — including water treatment grids, power grids, and traffic systems.



A breach at the national level can cripple national defense and destabilize geopolitical stability.

Corporations & Financial Institutions

Corporate Threats

- Intellectual property theft
- Ransomware attacks
- Customer data breaches
- Catastrophic financial loss & brand erosion

Financial Institution Threats

- Sophisticated fraud schemes
- SWIFT network attacks
- DDoS extortion attempts
- Requires 24/7 SOC monitoring

Hospitals & Healthcare Systems

Healthcare cyber security is literally a matter of life and death. Ransomware locking electronic health records (EHRs), tampering with infusion pumps, or compromising biomedical IoT devices — pacemakers, MRI scanners — can directly delay critical patient care, resulting in patient morbidity and mortality.

- ❌ Healthcare is one of the most targeted sectors due to the high monetary value of Protected Health Information (PHI).



Education & Individual Citizens

Educational Institutions (K-12 & Universities)

Schools hold sensitive data including student Social Security numbers, faculty research grants, and medical histories.

Universities are prime targets for foreign intelligence agencies seeking proprietary research in quantum computing, aerospace, and biotechnology.

Individual Citizens

Everyday individuals face phishing scams, identity theft, ransomware, stalkerware on mobile devices, and financial fraud.

Individual cyber hygiene forms the **human firewall** that prevents broader enterprise infiltration.

Anatomy of Cyber Attacks

Understanding how adversaries operate is essential to building effective defenses. This module provides a deep taxonomy of cyber attacks illustrated through famous historical case studies.



Malware

Viruses, Worms, Trojans, Ransomware, Spyware, Rootkits



Network Exploits

MitM, DDoS, ARP Spoofing, DNS Hijacking



Social Engineering

Phishing, Spear Phishing, Whaling, Vishing, Smishing, Pretexting



Web App Flaws

SQL Injection, XSS, Remote Code Execution (RCE)



Advanced Persistent Threats & Zero-Days

Advanced Persistent Threats (APTs) represent the most sophisticated tier of cyber attack — nation-state or well-funded adversaries conducting long-term, targeted espionage campaigns. Zero-day exploits leverage unknown vulnerabilities before patches exist, making them extraordinarily dangerous and valuable on the black market.

CASE STUDIES

Landmark Attacks: Forensic Post-Mortems

Stuxnet Worm

Industrial control system sabotage targeting Iranian nuclear centrifuges — a watershed moment in nation-state cyber warfare.

WannaCry Ransomware

Global outbreak causing massive healthcare disruption, locking hospitals out of critical patient records.

Equifax Breach

Corporate governance failure exposing 147 million Americans' personal data — a cautionary tale in patch management.

SolarWinds Compromise

Sophisticated supply chain attack enabling nation-state espionage across U.S. federal agencies and Fortune 500 companies.

CAREER PATHWAYS

Professional Roles in Cyber Security

The cyber security job market offers diverse, high-paying career tracks suited to various technical and analytical skill sets. Students will explore specific roles, daily responsibilities, and core competency requirements.



SOC Analyst & Penetration Tester

SOC Analyst (Tier 1–3)

Continuous monitoring of security alerts, triaging incidents, analyzing log files via SIEM, and executing initial containment protocols.

Penetration Tester / Ethical Hacker

Simulating real-world cyber attacks against corporate networks and web apps to discover vulnerabilities before malicious actors exploit them.

Security Engineering, Forensics & GRC

Security Engineer & Architect

Designing secure enterprise network architectures, firewalls, VPNs, zero-trust access controls, and cloud security configurations.

DFIR Specialist

Investigating digital crime scenes, preserving chain of custody, recovering deleted artifacts, and testifying in legal proceedings.

GRC Analyst / Security Manager

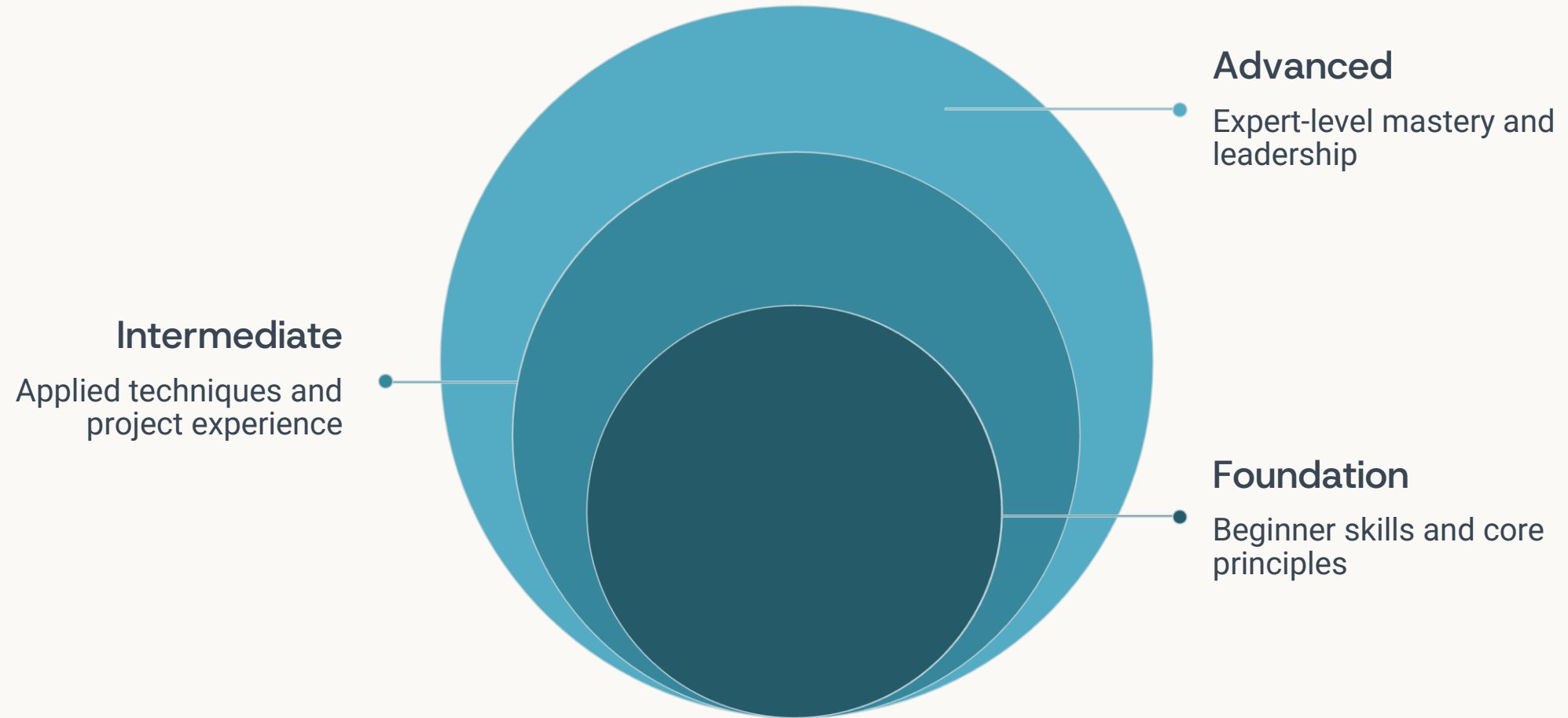
Designing corporate security policies, ensuring compliance with ISO 27001, HIPAA, GDPR, and NIST, and conducting risk assessments.

Cryptographer & Security Researcher

Designing advanced cryptographic algorithms, PKI, and quantum-resistant encryption protocols.

Your Certification Roadmap

Industry certifications serve as gold-standard validations of professional competence. Dr. Owor guides students through the exact roadmap required to accelerate their careers — from beginner to expert level.



Foundation Level Certifications

CompTIA Security+

Validates baseline knowledge of network security, compliance, threats, and vulnerabilities. Ideal starting point for newcomers (0–2 years experience).

AWS / Azure Fundamentals

Foundational cloud concepts, deployment models, and basic shared responsibility security models across AWS, Azure, and GCP.

Cisco CCNA

Core networking principles, IP addressing, routing, switching, and basic perimeter defense configuration.

Intermediate Level Certifications

1

CEH — EC-Council

Globally recognized credential for hands-on penetration testing and ethical hacking methodologies.

2

CISSP — (ISC)²

Vendor-neutral certification covering security architecture, risk management, and asset security. Requires 5 years experience.

3

CISM — ISACA

Enterprise security management, governance, program development, and incident management.

4

CompTIA CySA+ & PenTest+

Intermediate-to-advanced cybersecurity skills across multiple domains via hands-on performance-based testing.

Advanced & Expert Level Certifications

OSCP

Offensive Security Certified Professional — advanced penetration testing, exploit writing, and binary analysis in enterprise environments.

CISSP-ISSAP / ISSEP

Premier expert-level certification covering complex network security architecture and enterprise-wide defense design.

GCFA / GCIH — GIAC

Rigorous practical examination of elite incident response and digital forensics capabilities.

Certification Preparation Strategy

1 Blueprint Mastery

Master official exam blueprints and domain weightings from (ISC)², CompTIA, ISACA, and EC-Council.

2 Multi-Modal Study

Combine authoritative textbooks, video masterclasses (Professor Messer, Pluralsight, Cybrary), and practice question banks (Boson, Transcender).

3 Hands-On Lab Practice

Home labs using VirtualBox, VMware, Kali Linux, Hack The Box, and TryHackMe for practical muscle memory.

4 Exam Registration

Navigate Pearson VUE or PSI testing centers, leverage student discounts, and master exam-day time management.



JOB MARKET

A Field With 3.5 Million Unfilled Jobs

The global cyber security deficit remains at over **3.5 million unfilled positions**, guaranteeing exceptional career stability and lucrative compensation. This module examines macroeconomic employment trends and salary expectations across all experience levels.



Cyber Security Salary Ranges

Job Role / Title	Experience Level	Avg. Annual Salary (US)
SOC Analyst (Tier 1–2)	Entry-Level (0–2 Years)	\$75,000 – \$95,000
Penetration Tester / Ethical Hacker	Mid-Level (3–5 Years)	\$110,000 – \$145,000
Security Engineer / Architect	Senior-Level (5+ Years)	\$135,000 – \$185,000
CISO	Executive (10+ Years)	\$200,000 – \$350,000+

Resume Building & Career Coaching

What You'll Build

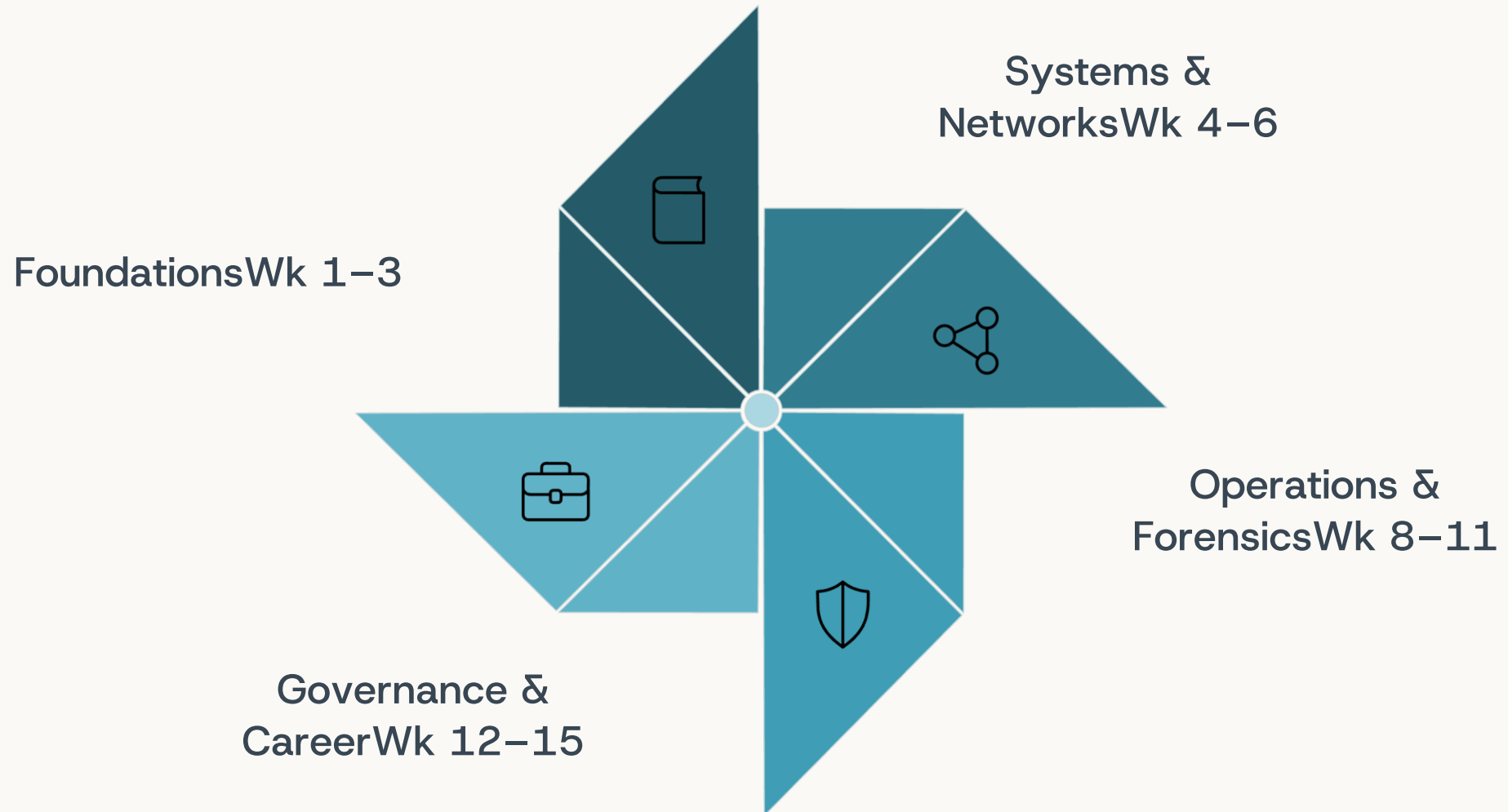
- ATS-optimized cyber security resume
- Compelling LinkedIn profile
- Mock technical interview skills

Securetsys Network

Students leverage Securetsys industry hiring partner networks for internships and full-time job placements — working directly with Dr. Owor throughout the process.

Weekly Course Schedule Overview

The course is structured as a 15-week semester, progressing from foundational concepts through advanced operations, culminating in a Red Team vs. Blue Team capstone simulation.



Weeks 1–3: Foundations

01

Week 1 — Information Security Concepts

CIA Triad (Confidentiality, Integrity, Availability) and Risk Management Frameworks.

02

Week 2 — The Human Element

Social Engineering, Phishing, Insider Threats, and Security Awareness Training.

03

Week 3 — Cryptography Fundamentals

Symmetric vs. Asymmetric Encryption, Hashing, Digital Signatures, and PKI.

Weeks 4–6: Systems, Networks & Web Security

01

Week 4 — OS & Endpoint Security

Hardening Windows, Linux, and macOS endpoints against malware and privilege escalation.

02

Week 5 — Network Security Architecture

Firewalls, IDS/IPS, VPNs, VLANs, Zero Trust Architecture, and Perimeter Defenses.

03

Week 6 — Web Application Vulnerabilities

OWASP Top 10, SQL Injection, XSS, and Secure Coding Practices.



Week 7: Midterm Examination

Week 7 is dedicated to a **Comprehensive Midterm Examination & Practical Lab Assessment** — a full evaluation of both theoretical knowledge and applied concepts covered in Weeks 1 through 6.

Weeks 8–10: Threat Intelligence, SOC & DFIR

01

Week 8 — Threat Intelligence & Vulnerability Management

CVE databases, Nessus scanning, patching cycles, and risk scoring (CVSS).

02

Week 9 — Security Operations Centers (SOC)

SIEM log analysis, alert triage, incident detection, and SOAR automation.

03

Week 10 — Digital Forensics & Incident Response

Chain of custody, volatile memory capture, disk forensics, and containment.

Weeks 11–12: Cloud Security & Compliance

Week 11 — Cloud Security & Virtualization

- Securing AWS, Azure, and GCP environments
- Containerization: Docker & Kubernetes
- IAM policies and cloud-native controls

Week 12 — Governance, Risk & Compliance (GRC)

- ISO 27001 & NIST SP 800-53
- HIPAA & GDPR
- PCI-DSS regulatory standards

Weeks 13–14: Certifications & Career Development

Week 13 — Certification Roadmap Deep Dive

Study plans, exam strategies, and registration guidance for CompTIA, CEH, and CISSP certifications.

Week 14 — Career Development

Resume workshops, job market analysis, salary negotiation strategies, and mock technical interviews with Dr. Owor.

Week 15: Final Capstone Project

The course culminates in a **Red Team vs. Blue Team Simulation** — students apply every skill developed throughout the semester in a live adversarial exercise, followed by a comprehensive course review and final presentations.



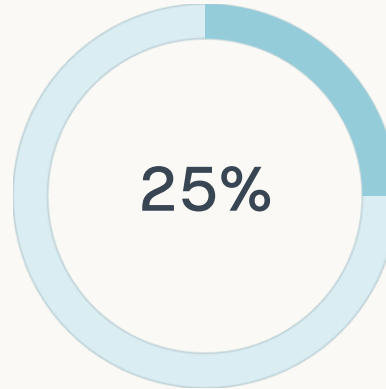
Grading & Evaluation Matrix

Student performance is evaluated through a balanced matrix of quizzes, hands-on lab reports, examinations, and a capstone team project.



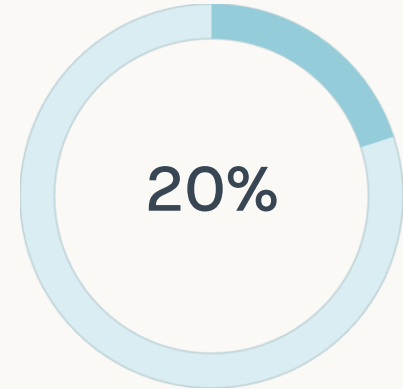
Weekly Quizzes

Knowledge checks throughout the semester



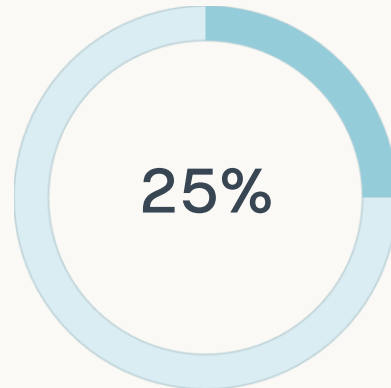
Lab Reports

Hands-on virtual lab reports & practical exercises



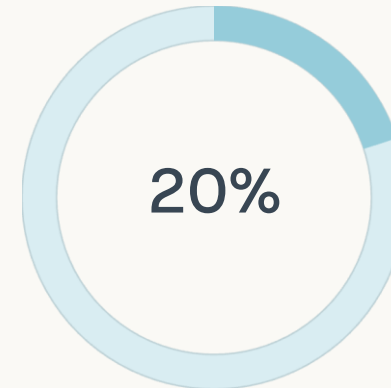
Midterm Exam

Theoretical & practical examination



Capstone Project

Red/Blue Team simulation & final presentation



Participation

Class participation, professionalism & discussion forums

Hands-On Lab Environment

Students build practical muscle memory through virtual lab environments using **VirtualBox**, **VMware**, and **Kali Linux**. Platforms such as **Hack The Box** and **TryHackMe** provide real-world attack-and-defend scenarios that reinforce every lecture topic – from network exploitation to digital forensics.



Google Classroom Delivery

How to Access

The course is delivered via **Google Classroom**. The enrollment link and Registration code will be provided upon registration.

Hybrid Format

The hybrid delivery model combines in-person instruction with live online lab sessions, ensuring flexibility without sacrificing the hands-on experience essential to ethical hacking training.

WHY CS-4551

What Sets This Course Apart



Expert Instruction

Led by a Ph.D.-credentialed, multiply-certified practitioner with 20+ years of real-world experience.



CEH Exam Ready

Fully prepares students to sit and pass the Certified Ethical Hacker (CEH) examination.



Career Placement

Resume coaching, mock interviews, and access to Securetsys hiring partner networks for internships and jobs.



Hands-On Labs

Real-world lab exercises, Red/Blue Team capstone, and industry-standard tooling throughout the semester.

Enrollment Details

Course Fee

\$499.95 per person

Credit Hours

4.0 Units — 60 Contact Hours

Terms Available

Fall / Spring / Summer

Platform

Google Classroom — link & registration code provided upon enrollment



Contact Securetsys Cyber Security Consultant to register and receive your Google Classroom access credentials.



Begin Your Cyber Security Journey

CS-4551 is your gateway to one of the most in-demand, highest-paying, and most impactful professions in the modern world. With expert instruction from Dr. Robert Steven Owor, hands-on labs, CEH exam preparation, and career coaching — you will graduate ready to defend the digital world.

"Cyber security is a fundamental pillar of national security, economic vitality, corporate governance, and personal privacy."

ENROLL TODAY — \$499.95

CS-4551 | SECURETSYS CYBER SECURITY CONSULTANT