SIIMT University College

DIPLOMA IN CYBER SECURITY

COURSE SYLLABUS

Duration - 1 Year

WHY CHOOOSE US ?

PRACTICAL HANDS-ON

BRIDGING KNOWLEDGE WITH EXPERIENCE, SHAPING SKILLS, AND PREPARING FOR REAL-WORLD SUCCESS

INDUSTRY

EXPERTS

STUDENTS LEARN FROM INDUSTRY EXPERTS, SHAPING SKILLS FOR REAL-WORLD SUCCESS AND JOB MARKET.

UPDATED SYLLABUS

OUR SYLLABUS ENRICHES LEARNING, FOSTERING SKILLS, AND PREPARES STUDENTS FOR A BRIGHTER FUTURE

SIIMT

OUR TEACHING STRATEGY

Each module will include a combination of theoretical concepts, practical exercises, and real-world case studies to ensure that students gain a comprehensive understanding of data analysis techniques and tools.

SIIMT

OUR REQUIREMENT

- BASIC UNDERSTAND OF COMPUTER AND ICT

  - For complete beginners we offer ICT course tailored to meet this prerequisite

SIIMT

LAPTOP REQUIRED

- Windows OS
- Minimum i5 processor
- Minimum 8GB RAM
- Sufficient Space

SIIMT

FEES

- **GHC 10,000** for Ghanaians
- **GHC 12,000** for Non-Ghanaians

  - Hostel Facilities availiable

DURATION OF THE COURSE

- 10 -12 MONTHS (APPROXIMATELY)

WEEKDAY EVENING BATCHES

- **BATCH 1 - MONDAY & TUESDAY**
  - 6:00 PM to 8:00 PM
- **BATCH 2 - WEDNESDAY & THURSDAY**
  - 6:00 PM to 8:00 PM

WEEKDAY EVENING BATCH

- **BATCH 1 - SATURDAY**
  - 9:00 AM to 1:00 PM
  - 2:00 PM to 5:00 PM

LEVEL 1

CERTIFIED INFROMATION SECURITY EXPERT

In this module, students will be introduced to the fundamentals of ethical hacking, including its importance, basic concepts, and techniques.

Topics covered will include:

- Module 1: Introduction to Exploit Writing
  - Fundamentals of exploit writing in cybersecurity
  - Importance and basic concepts
  - Essential techniques for vulnerability exploitation
- Module 2: Programming & Basics
  - Overview of programming fundamentals
  - Data types, control structures, functions
  - Foundation for exploit development
- Module 3: Assembly Language
  - Understanding assembly language
  - Role in low-level exploit development
  - System architecture insights
- Module 4: Debugging
  - Techniques for debugging exploits
  - Identifying vulnerabilities
  - Understanding program behavio

SIIMT

- Module 5: Stack Based Buffer Overflow
  - Detection and exploitation techniques
  - Mitigation strategies
  - Impact on program security
- Module 6: Understanding Windows Shellcode
  - Development and execution of Windows shellcode
  - Injecting and executing payloads
  - Malicious payload techniques
- Module 7: Fuzzers
  - Role of fuzzers in exploit development
  - Automated vulnerability discovery
  - Refining exploit techniques
- Module 8: Heap Based Overflow
  - Exploiting heap-based vulnerabilities
  - Manipulating heap structures
  - Techniques for exploitation
- Module 9: Exploiting /GS Canary Protected Programs
  - Bypassing /GS (Stack Cookies) protection
  - Challenges and strategies in exploit development
- Module 10: Exploiting Safe SEH Protected Programs
  - Techniques to bypass SafeSEH protection
  - Exploiting Windows programs with enhanced exception handling
- Module 11: Denial of Service
  - Methods for conducting DoS attacks
  - Exploiting vulnerabilities to overwhelm system resources
- Module 12: Case Studies and Real-world Examples
  - Analysis of notable exploit cases
  - Practical insights into exploit techniques
- Module 13: Career Path & Opportunities
  - Exploration of career paths in exploit development
  - Required skills and job opportunities

LEVEL 2

MODULE 1 - CERTIFIED EXPLOIT WRITING EXPERT

In this module, students will be introduced to the fundamentals of ethical hacking, including its importance, basic concepts, and techniques.

Topics covered will include:

- Module 1: Introduction to Exploit Writing Students will be introduced to the fundamentals of exploit writing, covering its significance in cybersecurity, basic concepts, and essential techniques.
- Module 2: Programming & Basics This module will provide an overview of programming fundamentals essential for exploit development, including data types, control structures, and functions.
- Module 3: Assembly Language An in-depth exploration of assembly language will be conducted, focusing on its role in understanding system architecture and crafting low-level exploits.
- Module 4: Debugging Students will learn debugging techniques crucial for identifying vulnerabilities and understanding program behavior to facilitate successful exploit development

SIIMT

- Module 5: Stack Based Buffer Overflow This module will delve into the mechanics of stack-based buffer overflow vulnerabilities, including detection, exploitation, and mitigation strategies.
- Module 6: Understanding Windows Shellcode Participants will gain insights into Windows shellcode development, emphasizing techniques for injecting and executing malicious payloads.
- Module 7: Fuzzers The use of fuzzers in exploit development will be covered, exploring their role in automated vulnerability discovery and exploit refinement.
- Module 8: Heap Based Overflow Students will explore heap-based overflow vulnerabilities, learning techniques to manipulate heap structures for exploit purposes
    - Module 9: Exploiting /GS Canary Protected Programs This module will focus on bypassing stack protection mechanisms like /GS (Stack Cookies), addressing challenges and strategies in exploit development.
    - Module 10: Exploiting Safe SEH Protected Programs Participants will study SafeSEH (Safe Structured Exception Handling) bypass techniques, essential for exploiting Windows programs with enhanced exception handling.
    - Module 11: Denial of Service An examination of denial-of-service (DoS) attacks will be conducted, including techniques to exploit vulnerabilities and overwhelm system resources.
    - Module 12: Case Studies and Real-world Examples Real-world case studies and examples of notable exploits will be analyzed, providing practical insights into exploit techniques and their impact.

LEVEL 2

MODULE 2 - CERTIFIED EXPLOIT WRITING EXPERT

In this module, students will be introduced to the fundamentals of ethical hacking, including its importance, basic concepts, and techniques.

Topics covered will include:

- Module 1: Network Topology
  - Overview of network topologies: Bus, Star, Ring, Mesh, Hybrid
  - Applications and considerations in network design
  - Importance of choosing the right topology for different scenarios
- Module 2: Open Systems Interconnectivity Model
  - Understanding OSI model layers and their functions
  - Interactions between OSI layers in network communication
  - Role in standardizing network protocols
- Module 3: TCP/IP In-depth
  - Detailed examination of TCP/IP protocol suite
  - TCP vs UDP: characteristics and use cases
  - IP addressing, subnetting, and basic routing concepts
- Module 4: WAP, NAT, DNS and ICMP
  - Wireless Access Points (WAP) and their security implications
  - Network Address Translation (NAT) principles and configurations
  - Domain Name System (DNS) functionality and vulnerabilities
  - Internet Control Message Protocol (ICMP) overview and utilitie

SIIMT

- Module 5: Internet Routing
  - Overview of routing protocols: OSPF, BGP, RIP
  - Routing tables and their role in directing traffic
  - Structure of the Internet backbone and Autonomous Systems (AS)
- Module 6: Advanced Port Scanning
  - Techniques for port scanning: SYN, ACK, FIN, XMAS
  - Nmap tool features and capabilities
  - Detection and evasion methods for port scanning
- Module 7: Sniffing Attacks
  - Packet sniffing methods and tools
  - Passive vs active sniffing techniques
  - Application of protocol analyzers in network monitoring
- Module 8: Masquerading Attacks
  - IP spoofing and masquerading techniques
  - Measures to detect and prevent masquerading attacks
  - Examples and case studies of masquerading incidents
- Module 9: Advanced DOS and DDOS
  - Understanding Denial of Service (DoS) and Distributed DoS (DDoS) attacks
  - Techniques like amplification and reflection attacks
  - Countermeasures and mitigation strategies against DoS/DDoS
    - Securing sessions through encryption and tokenization
  - Module 11: Network Operations Centre – Security
    - Security considerations for Network Operations Centers (NOC)
    - Incident response procedures and protocols
    - Monitoring tools and their role in maintaining network security
  - Module 12: Network Traffic Analysis
    - Techniques for analyzing network traffic patterns
    - Intrusion detection through traffic analysis
    - Use of tools like Wireshark for deep packet inspection
  - Module 13: Network Vulnerability Assessment
    - Conducting comprehensive vulnerability assessments
    - Tools such as Nessus and OpenVAS for scanning vulnerabilities
    - Prioritizing and reporting vulnerabilities for remediation
  - Module 14: Network Penetration Testing
    - Methodologies for penetration testing: black box, white box, gray box
    - Exploitation techniques and ethical considerations
    - Delivering actionable recommendations based on test findings
  - Module 15: Intrusion Detection System
    - Overview of Intrusion Detection Systems (IDS) vs Intrusion Prevention Systems (IPS)
    - Signature-based vs anomaly-based detection methods
    - Implementation and configuration of IDS/IPS systems
-

LEVEL 2

MODULE 3- CERTIFIED WEB APPLICATION SECURITY EXPERT

In this module, students will be introduced to the fundamentals of ethical hacking, including its importance, basic concepts, and techniques.

Topics covered will include:

- Module 1: Web Architectures & Web Application Introduction
  - Overview of web architectures and their importance in web application development
  - Introduction to web applications, their components, and functionalities
- Module 2: PHP Basics & Sessions / Cookies
  - Fundamentals of PHP programming language
  - Handling sessions and cookies in web applications for user interaction
- Module 3: XSS Attacks & Advanced SQL Injection (SQLI)
  - Understanding Cross-Site Scripting (XSS) vulnerabilities and exploits
  - Advanced techniques in SQL Injection (SQLI) for manipulating databases
  - Module 4: Cross-Site Request Forgery (CSRF) & Session Hijacking
  - CSRF attacks and prevention mechanisms in web applications
  - Techniques and prevention of session hijacking incidents

SIIMT

- Module 6: PHP Injection & Web-based Worms
  - Exploiting PHP injection vulnerabilities in web applications
  - Understanding and mitigating the spread of web-based worms
- Module 7: Flash-based Web Attacks & I-Frame-based Web Attacks
  - Security threats posed by Flash-based content in web applications
  - Risks associated with I-Frame usage and prevention measures
- Module 8: Clickjacking & Attack Frameworks (AttackAPI & BeEF)
  - Clickjacking techniques and prevention strategies
  - Overview and application of AttackAPI and BeEF frameworks in web security
- Module 9: Penetration Testing on DVWA & Honeytokens
  - Hands-on penetration testing using Damn Vulnerable Web Application (DVWA)
  - Implementing honeytokens for detecting and responding to web attack
- Module 10: OWASP Top 10 & Metasploit in Web Application Security
  - Overview of OWASP Top 10 vulnerabilities and mitigation strategies
  - Utilizing Metasploit framework for web application penetration testing
- Module 11: PHP Curl & Automated Bots
  - Using PHP Curl for web data retrieval and manipulation
  - Detection and mitigation of automated bot attacks targeting web applications
- Module 12: Phishing 2.0 & Brute Forcing Web Applications
  - Advanced phishing techniques and defense mechanisms (Phishing 2.0)
  - Brute forcing methods to exploit weak authentication in web applications
- Module 13: Compliance Methodologies and Legalities & Capture the Flag Exercise
  - Understanding compliance requirements and legal considerations in web security
  - Practical application of skills through Capture the Flag (CTF) exercises

TO REGISTER FOR
DIPLOMA IN CYBER SECURITY

CLICK HERE

OR

Visit www.siimtuni.edu.gh to apply now

SIIMT University College

SIIMT UNIVERSITY COLLEGE

OUR GOAL

We aim to provide high-quality education with practical hands-on training, preparing students for leadership roles and employment opportunities.

EXCELLENCE

INNOVATION

PRACTICALITY

INTEGRITY

ABOUT US

- The SIIMT is an Indian-based Ghanaian University College established in 2013 at Labone, Accra before relocating to its current premises near the Nima Police Station at the foot of the Nima-Kanda overpass, Accra in 2018

- The SIIMT was accredited by the **Ghana Tertiary Education Commission (GTEC**) in 2019 to run the Undergraduate Programmes affiliated to University of Cape Coast. It was also accredited by the **Council for Technical and Vocational Education and Training (CTVET)**, to run technical and vocational courses.

SIIMT University College

CONTACT US

ACCRA BRANCH

Nima Kanda Overhead
057 080 1631
030 226 9885

SPINTEX BRANCH

18 Junction, Spintex
057 6444 457
057 6444 458

KASOA BRANCH

DATUS COMPLEX
057 080 1631
030 226 9885

Visit us on **www.siimtuni.edu.gh**