CYBERSECURITY COURSE CONTENT

Location: Virtual/ Physical

Date: 11/03/2024

Facilitator: Micheal Itegbe

Course Content

Month 1: Introduction			
	Week 1 (Classes 1-3):	Introduction to Cybersecurity Historical overview of cybersecurity evolution Key cybersecurity concepts (CIA Triad, access management, incident response) Introduction to malicious software types (viruses, worms, trojans, etc.) Overview of cybersecurity tools (firewalls, antivirus, encryption)	
	Week 2 (Classes 1-3):	Operating System Security Introduction to operating systems (Windows, macOS, Linux, Mobile) Understanding basic OS architecture, file systems, and commands Introduction to virtualization in cybersecurity Hands-on practice with common operating system tasks	[Location]
	Week 3 (Classes 1-3)	Cybersecurity Roles & Malicious Software Understanding cybersecurity roles within organizations (security analyst, penetration tester, etc.) Key cybersecurity processes and common scenarios In-depth exploration of different malicious software types and their impact	[Location]

		Exploring techniques for mitigating malware threats	
	Week 4 (Classes 1-3)	Network Fundamentals & Security Tools Introduction to networking concepts (TCP/IP model, OSI model) Understanding core network components (DNS, DHCP, switching, routing) Familiarization with IP addressing basics (subnetting, NAT) Introduction to basic network security tools (firewalls, intrusion detection/prevention systems)	[Location]
Month 2: Deep Dive & Compliance			
	Week 5 (Classes 1-3):	Network Security & Compliance Basics Exploring network security principles (defense in depth, least privilege) Understanding network security vulnerabilities (denial-of-service attacks, man-in-the-middle) Introduction to cybersecurity compliance (NIST, GDPR, HIPAA) Analyzing compliance requirements and their impact on security practices	[Location]
	Week 6 (Classes 1-3):	System Administration & Cryptography Introduction to server and user administration concepts Importance of patching and endpoint protection in system administration Essential concepts of cryptography: encryption, encoding, hashing, digital certificates Hands-on practice with basic encryption and decryption techniques	[Location]
	Week 7 (Classes 1-3):	Database Security & Penetration Testing Fundamentals Understanding common database structures (SQL, CouchDB, etc.) Exploring common database vulnerabilities (SQL injection, cross-site scripting)	[Location]

		Introduction to penetration testing methodology and ethical hacking principles Exploring basic penetration testing tools and techniques	
	Week 8 (Classes 1-3)	Introduction to Incident Response & Scripting Introduction to the incident response process (preparation, identification, containment, eradication, recovery) Importance of documentation and forensic evidence collection during incident response Introduction to scripting languages commonly used in cybersecurity (Python, Bash) Hands-on practice with basic scripting for security automation tasks	[Location]
		Month 3: Advanced Skills & Cloud Security	
	Week 9 (Classes 1-3):	Advanced Penetration Testing Techniques & Case Studies Deep dive into specific penetration testing techniques (footprinting, scanning, exploitation) Analyzing real-world penetration testing case studies for practical understanding Applying learned techniques through hands-on labs or simulations	[Location]
	Week 10 (Classes 1-3)	Digital Forensics & Introduction to Cloud Security Introduction to digital forensics methodologies and evidence analysis techniques Understanding the importance of digital forensics in incident response Introduction to cloud security principles and shared responsibility model Exploring basic cloud security concepts (IAM, encryption, logging)	[Location]
	Week 11 (Classes 1-3)	Application Security & Threat Intelligence Exploring common application security vulnerabilities (injection attacks, broken authentication) Introduction to threat intelligence concepts and methodologies Understanding the role of threat intelligence in proactive security posture	[Location]

		Analyzing security alert information and identifying potential threats	
	Week 12 (Classes 1-3):	Capstone Project & Cybersecurity Breach Response Develop a capstone project applying learned concepts in a practical scenario (e.g., securing a web application) Research and analyze real-world cybersecurity breach case studies Understanding cyber attack trends and their consequences Applying incident response methodologies through case study analysis	[Location]
	Week 13 (Classes 1-3):	Advanced Topics Exploration (student-driven) Students choose an advanced topic of interest within cybersecurity (e.g., web security, mobile security, etc.) Utilize online resources, books, and tutorials for self-directed learning Class time dedicated to sharing discoveries, asking questions, and peer discussion	[Location]
	Week 14 (Classes 1-3)	Capstone Project Development and Presentation Students dedicate time to further develop their capstone projects Class time is used for peer discussions, troubleshooting, and feedback Students can present their completed projects and receive feedback	[Location]
	Week 15 (Classes 1-3)	Examination, Evaluation and Certification	[Location]

Signed
Micheal Itegbe

Head Training & Research