THE OPEN UNIVERSITY OF TANZANIA

ETHICAL HACKING TRAINING

START DATE: 3rd JUNE, 2024

DURATION: 6 WEEKS (3hrs/Day/3days/week)

Course Overview

Ethical hacking, also known as penetration testing or white-hat hacking, is the practice of deliberately testing computer systems, networks, and applications to identify security vulnerabilities that malicious hackers could exploit. Ethical hackers use the same tools and techniques as black-hat hackers, but with the explicit permission of the organization or individual owning the system being tested.

The primary goal of ethical hacking is to improve the security posture of the target system by identifying and remedying vulnerabilities before they can be exploited by malicious actors. This proactive approach helps organizations strengthen their defenses and protect sensitive data from unauthorized access, theft, or manipulation.

Also, ethical hacking plays a crucial role in the cybersecurity ecosystem by helping organizations proactively identify and mitigate security risks. By simulating real-world cyber-attacks in a controlled environment, ethical hackers assist in strengthening defenses, enhancing incident response capabilities, and ultimately safeguarding sensitive information from cyber threats. Additionally, ethical hacking certifications such as Certified Ethical Hacker (CEH) provide professionals with the necessary skills and credentials to perform ethical hacking activities responsibly and effectively.

Course Objectives

- The course is intended to inculcate the importance of ethical hacking & cybersecurity
- Participants should grasp the fundamental concepts and principles of ethical hacking, including its purpose, legal aspects, and ethical considerations.
- Participants should acquire a solid understanding of cybersecurity principles, including network security, system security, cryptography, and information security policies.
- This course should provide practical, hands-on experience with various hacking tools and techniques used by ethical hackers, such as penetration testing tools, vulnerability assessment tools, and network sniffers.

- Attendees should learn how to identify security vulnerabilities in systems, networks, and applications and understand how to mitigate these vulnerabilities effectively.
- Emphasis should be placed on the ethical and legal aspects of hacking, including laws and regulations related to cybersecurity, as well as ethical guidelines and codes of conduct for ethical hackers.
- Participants should learn how to conduct risk assessments, prioritize security risks, and develop risk management strategies to protect organizations from cyber threats.
- This course should cover incident response procedures, including how to detect, analyze, and respond to security incidents effectively.

Learning Outcomes

- Upon completion, each participant will learn the basics of ethical hacking and preventive cybersecurity measures for securing their digital assets
- Participants will learn to think like hackers and be able to leverage that knowledge for digital security
- Proficiency in various hacking tools and techniques, such as penetration testing frameworks network, scanning tools, and vulnerability assessment tools
- Understanding of common vulnerabilities in network protocols, web applications, operating systems, and software.
- Ability to differentiate between ethical hacking and malicious hacking, and to use skills responsibly and lawfully.
- Implementation of risk mitigation strategies, such as patching vulnerabilities, implementing security controls, and conducting security awareness training.
- Analytical thinking and problem-solving skills to identify and exploit vulnerabilities effectively.

Course contents

Topic 1: Introduction to Linux

✓ □Linux Filesystem
✓ □The Linux shell environment
✓ □File Operations
✓ □Choosing a Linux Distribution

Topic 2: Introduction to Computer Networks

✓ □TCP/IP
✓ □OSI Model
✓ □Network Protocols
✓ □Networking Ports and Services

Topic 3: Introduction to Ethical Hacking

- ✓ □Ethical Hacking
- ✓ □Types of Hackers
- ✓ □Red Teaming
- ✓ □Penetration Testing
- ✓ □2015 Tanzania Cybercrime act

Topic 4: Hacker Lab setup

- ✓ □Hypervisor Installation
- ✓ □Installing Kali Linux
- ✓ □Installing Metasploitable2
- ✓ □Installing Metasploitable3
- ✓ □Custom OUT Labs

Topic 5: Reconnaissance and Footprinting

- ✓ □Footprinting Concepts
- ✓ □Attack Surface Expansion
- ✓ □Google Hacking
- ✓ □Footprinting Through Web Services
- ✓ □Website Footprinting
- ✓ □Organization Footprinting
- ✓ □Footprinting People
- ✓ □Email Footprinting
- ✓ □Whois Footprinting
- ✓ □DNS Reconnaissance
- ✓ □Footprinting Through Social Engineering

Topic 6: Network Scanning and Exploitation

- ✓ Network Scanning Concepts
- ✓ Network Scanning Tools
- ✓ Host Discovery
- ✓ Port Scanning and Services Discovery
- ✓ OS Discovery
- ✓ Banner Grabbing and OS Fingerprinting
- ✓ Version Identification
- ✓ One day Exploits
- ✓ Attacking Network Protocols
- ✓ Firewall Evasion Techniques

Topic 7: Web Application Scanning and Exploitation

- ✓ Technology stack identification
- ✓ Web server scanning
- ✓ Web server attacks
- ✓ API scanning and attacks
- ✓ Automated vulnerability scanning
- ✓ Java Spring Boot Log4J exploitation
- ✓ Web Frameworks Security Auditing
- ✓ NoSQL Injection (NodeJS)
- ✓ CMS Security Auditing (WordPress, Joomla)
- ✓ SQL Injection Vulnerabilities
- ✓ Cross Site Scripting (Cookie theft with BeEF)
- ✓ File upload and Remote Code Execution
- ✓ Denial of Service Attacks

Topic 8: System Hacking

- ✓ SQL Injections
- ✓ File Upload Attacks
- ✓ Password Attacks
- ✓ Attacking Network Protocols
- ✓ Zero-Day Exploits
- ✓ One-Day Exploits
- ✓ Initial access brokers (IAB)

Topic 9: Social Engineering

- ✓ Social Engineering the Art of Human Hacking
- ✓ Why Social Engineering is So Effective
- ✓ Types of Social Engineering Attacks
- ✓ Spear Phishing Attack
- ✓ Smishing
- ✓ Vishing
- ✓ Business Email Compromise
- ✓ Generative AI and Social Engineering

Topic 9: Introduction to Malware Threats

- ✓ Malware Concepts
- ✓ Antivirus Concepts
- ✓ Malware Infection Lifecycle
- ✓ Trojan and Remote Access Tools (RAT)
- ✓ Viruses and Worms
- ✓ Ransomware
- ✓ Malware Delivery Techniques
- ✓ Command and control (C2)
- ✓ Viruses
- ✓ Worm
- ✓ Trojan

- Keylogger
- Ransomware
- Backdoors
- APT Groups and State Sponsored Threat Actors
- APT Malware (GoRAT)
- Generative AI and Malware Threats (WormGPT, FraudGPT)
- Uncensored LLMs
- Malware Writing 1
- Malware Writing 2
- Living off the land
- Malware Analysis Basics

Topic 10: Cryptography

- Introduction to Cryptography
- Symmetric Encryption
- AES
- Public Key Cryptography
- RSA
- Data Hashing
- Hashing Algorithms
- Message Digest Algorithm Number 5 (MD5)
- SHA-128
- SHA-256
- SHA-512
- Bcrypt (Blowfish)
- Cracking Encryptions with Hashcat
- Secured Networking Protocols

Topic 11: Steganography

- Introduction to Steganography
- Binary files structures
- Metadata Extraction
- Hiding a message in a file
- Retrieving a message from a file

Targeted group:

This course targets individuals who are interested in learning about Ethical Hacking including;

- ✓ Information Security Professionals.
- ✓ Information Technology Professionals (System Administrators, Network Administrators, Application Programmers).
- ✓ Process Automation – Control Systems and IT Engineers.
- ✓ Ethical Hackers and Cyber Security Professionals.
- ✓ All public servants and private sectors personnel's who work in various sections of IT

Training Mode

The course will be offered through F2F mode at HQ and online mode depending on course content and topic.

Teaching mode will include 30% theory and 70% practices using computer laboratories.

Course fee: Tshs 500,000

To paid through

BANK NAME: NBC

BANK Account no. 011103033713,

ACCOUNT NAME: OCB

NB: Only 40 Students Required for this class to start and all fees amount to be paid before class commences.

How to Register

https://forms.gle/P4Wiy51Xb3kWBWU59

To register please contact us through the following details

Email: richlaizer.96@gmail.com, mwanuzi@gmail.com

Telephone: 0687063988/0753000102/0719454547