Ed-Tech
AFRICA

CYBER SECURITY

3 Months | 6 Month Courses

www.ed-techafrica.com

Ed-Tech AFRICA

Transforming education through technology

Course Aims & Objectives

You will have an introduction to Cyber Security and it's aspects as well as basic terms and nomenclature involved with it. Moving further, you will have all the basic requirements at your fingertips to have a vast understanding of Cyber Security as a whole.

This course will provide you with an overview of the cybersecurity landscape as well as national and international views. We'll go through the legislative landscape that affects cybersecurity, as well as the most common threat actors.
To assess the learning level and progress with continuous and rigorous ways to ensure highest level of knowledge and professional exposure ensuring a practical approach.

Learn about the evolution of cybersecurity as a field, as well as the standards, regulations, and frameworks that arose to respond to evolving cyber threats.

Define and apply essential concepts and words in the realm of cybersecurity.

Gain an advanced level of understanding for future prospects and professional level requirement.

Curriculum Index

PRE REQUISITES

PROGRAMMING LANGUAGE FUNDAMENTALS (PYTHON)

*Python basics

2 WEEKS

INTERNET & NETWORKING BASICS (OPTIONAL)

*Learn about basics & essential protocols TCP/IP, UDP), Components, traceroute, ipconfig, HTTP, components (browser, server,DNS etc)

0 WEEKS

INFORMATION SECURITY & APPLIED CRYPTOGRAPHY

INTRODUCTION TO CYBER SECURITY CRYPTOGRAPHY AND ENCRYPTION

*Get introduced by Cyber Security.

1 WEEK

OS FUNDAMENTALS & SECURITY

*Linux CLI, Hardening, Bash Scripting and Security in LInux.

2 WEEKS

CRYPTOGRAPHY & ENCRYPTION

*Get introduced to Cybersecurity. Basic Information Protection: Data Secrecy/Confidentiality and Integrity - Requirements. Encryption as a Solution for Secrecy. Encryption vs Encryption as a computationally difficult to invert function, Symmetric and Asymmetric encryption techniques.

Encryption vs Encoding. Cryptography - Confusion and Diffusion Properties. Public Key and Private Key Encryption Techniques (RSA and AES as Examples). Password-based Encryption. HSM and PKI.

2 WEEKS

CRYPTOGRAPHIC KEY MANAGEMENT MESSAGE DIGEST & DIGITAL SIGNATURES

*Key Management. Die Helman Key Exchange. Key Stores. Providers. Message Digests. Hashes and Signatures. Keyed Hashing. Digital Signatures. Digital Signatures as Solutions for Sender Identity, Message Integrity and Non-repudiation.

1 WEEK

IDENTITY ACCESS MANAGEMENT

*IDAM lifecycle, User Authentication: Passwords and Limitations. Challenge Response Protocols. Replay and Man-in-the-middle Attacks. Freshness / Currency. CAPTCHAS; Multi-factor Authentication; Oauth and Open Id.

1 WEEK

ASSIGNMENT/ PROJECT - ACCESS CONTROL

*Course Assignment/Project.

NETWORK SECURITY IN ETHICAL HACKING

INTRODUCTION TO NETWORK SECURITY & SPOOFING

Local Area Networks - Switched Ethernet. Switches and Security. Addresses: MAC and IP addresses. Address Spoofing. ARP protocol and spoofing, SNMP and IGMP protocols.

1 WEEK

SECURED NETWORKS SYSTEM WITH FIREWALL

Broadcast Domains and Isolation; Virtual LANs. Private vs. Public Addresses. Gateways. Network Address Translation. Demilitarized Zones (DMZs). Firewalls, Access Control, and Firewall Rules.

2 WEEKS

PACKET INSPECTION AND ATTACK AGAINST AVAILABILITY

Packet Inspection, Deep Packet Inspection(Intrusions detection system and Intrusion Prevention System), IP Security, ICMP attacks. TCP and UDP Security. Attacking Availability: Denial-of-Service attacks, Distributed DOS attacks, SSL/TLS , IP Table.

1 WEEK

PACKET INSPECTION AND ATTACK AGAINST AVAILABILITY

Course Assignment/Project.

2 WEEKS

DATA AND DATABASE SECURITY

Data and Database Security - SQL Injection Attacks; Data access and Access Control, Access Control on views, Data Privacy and Anonymity.

2 WEEKS

APPLICATION SECURITY IN ETHICAL HACKING AND ADVANCED CONCEPTS IN CYBER SECURITY

INTRODUCTION TO APPLICATION SECURITY

Secure Programming. Information Flow and Security. Buffer Overflow Attacks. Managed Execution - JVM. OWASP top 10.

1 WEEK

WEB-BASED APPLICATIONS AND ASSOCIATED VULNERABILITIES

Web-based applications: Browsers and Browser Security, CSP Policies. JavaScript vulnerabilities and Cross-Site Scripting. XSS and CSRF vulnerabilities.

1 WEEK

COOKIES AND TRACKING

Cookies and Tracking; User Identities and User profiling.

1 WEEK

DATA AND DATABASE SECURITY

Data and Database Security - SQL Injection Attacks; Data access and Access Control, Access Control on views, Data Privacy and Anonymity.

2 WEEK

PHISHING AND OTHER ATTACKS ON IDENTITY

Phishing and other attacks on Identity(Social Engineering)

1 WEEK

CLOUD APPLICATION SECURITY

Cloud application Security: DOS attacks on the cloud; Process security and Data Access - Protection against multi-tenancy; Isolation in VMs and Containers.

OPTIONAL

PENETRATION TESTING, FUZZING

Pen-testing and tools, exploiting OWASP top 10 vulnerabilities in web application

OPTIONAL

REGULATION, COMPLIANCE, & RISK MANAGEMENT

NIST, ISO 27001, GDPR

1 WEEK

What is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- Network security
- Application security
- Information security
- Operational security
- Disaster recovery and business Continuity
- End-user education

It is used by most companies to;

- Protect against phishing schemes
- Ransomware attacks
- Identity theft
- Data breaches
- Financial losses

Examples of Cyber security:

- Antivirus and Antispyware programs
- Firewall that block unauthorized access to a network and VPNs (Virtual Private Networks) used for secure remote access.

JOB OPPORTUNITIES

- ✱ **Chief Information Security officer (CISO)**
- ✱ **Security Architect**
- ✱ **Cybersecurity Engineer**
- ✱ **Malware Analyst**
- ✱ **Penetration Tester**
- ✱ **Computer Forensics Analyst**
- ✱ **Application Security Engineer**
- ✱ **Cloud Security Specialist**

TYPES OF CYBER THREATS

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

MALWARE

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details

Ransomware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Adware: Advertising software which can be used to spread malware.

Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL INJECTION

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

PHISHING

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

MAN-IN-THE-MIDDLE ATTACK

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecured WiFi network, an attacker could intercept data being passed from the victim's device and the network.

DENIAL-OF-SERVICE ATTACK

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Ed-Tech
AFRICA

☎ +267 3914472
+267 75 546 649

ED Tech Africa
@edtech.bw

Ed-Tech Africa
edtechafricabw

www.ed-techafrica.com

www.ed-techafrica.com