الأكاديمية العربية الدولية
Arab International Academy

Subject Name: cyber security- owasp10

Presenter name: Zainab ali

الأكاديمية العربية الدولية – منصة أعد

About me

Zainab Ali ,Bachelor of Computer Science ,graduate 2021

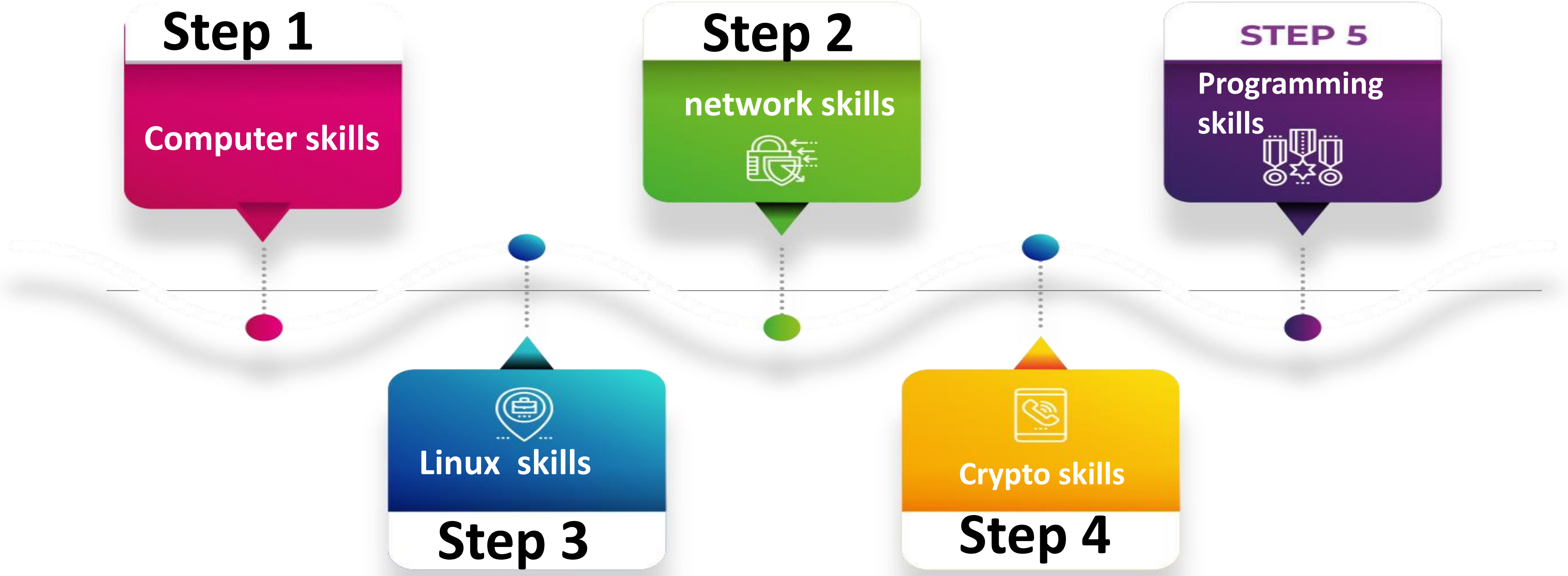
Certified international trainer

I have 8000 trainees on Udemy

4 years experience in cyber security

الأكاديمية العربية الدولية
Arab International Academy

RoudMap



Step 1

Computer skills

Step 2

network skills

Step 3

Linux skills

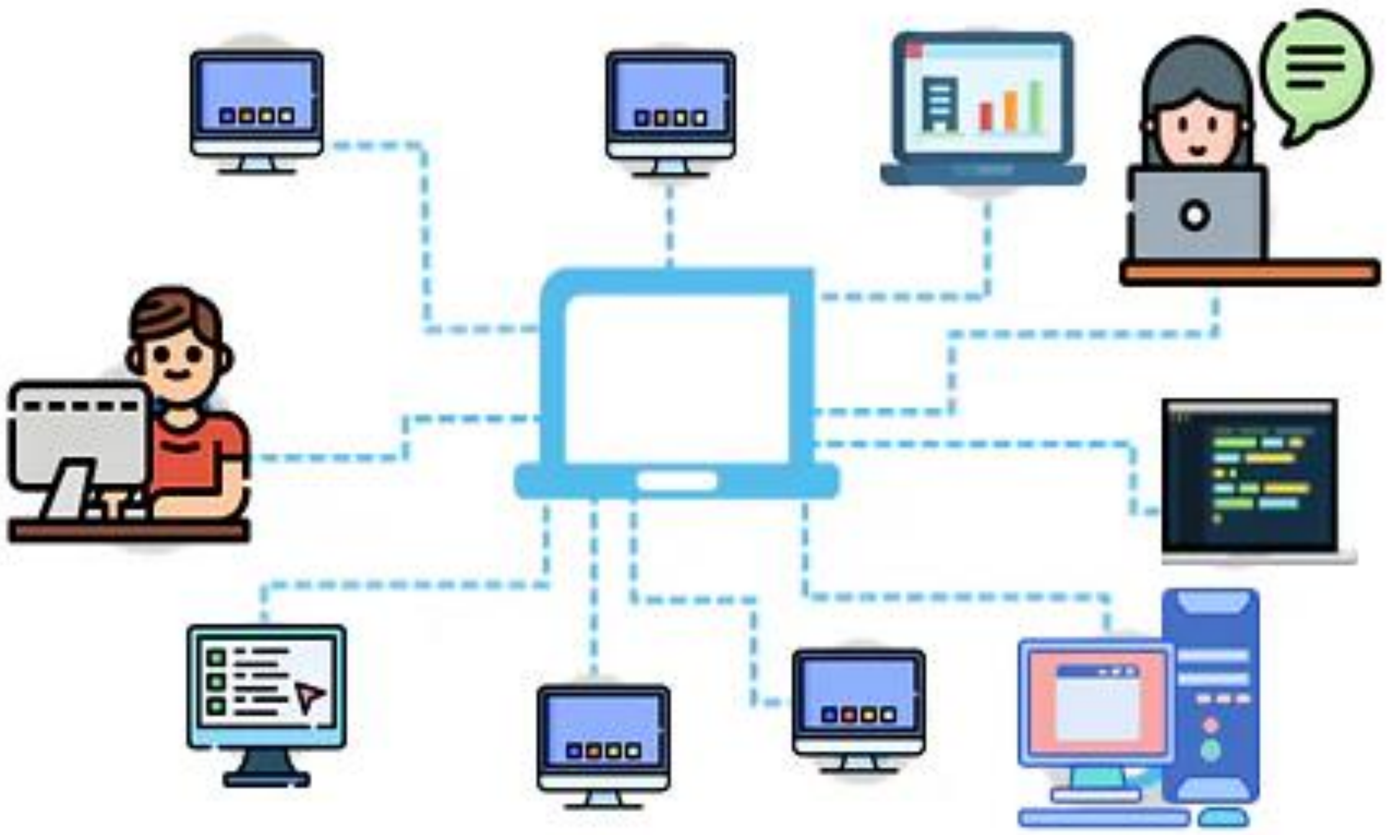
Step 4

Crypto skills

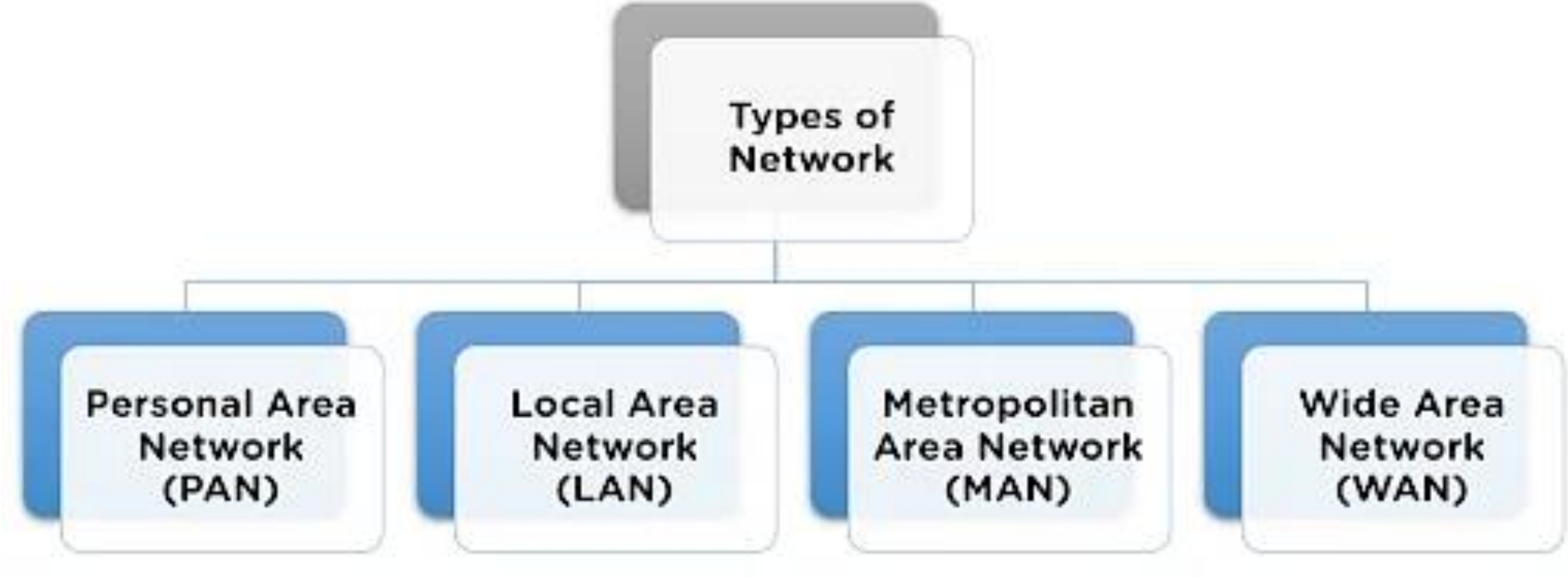
STEP 5

Programming skills

Network



Network



Types of Network

Personal Area Network (PAN)

Local Area Network (LAN)

Metropolitan Area Network (MAN)

Wide Area Network (WAN)

الأكاديمية العربية الدولية
Arab International Academy

Network

Cyber security- owsap 10

OWASP (Open Web Application Security Project)

1. Injection Attacks
2. Broken Authentication and Session Management))
3. insecure direct object reference
4. Insufficient Cryptography
5. Security Misconfiguration
6. (Injection Flaws)
7. (Insecure Communication)
8. Insufficient Logging and Monitoring))
9. Server-Side Request Forgery)
10. Sensitive Data Exposure

اعلان

Cyber security- owsap 10

OWASP (Open Web Application Security Project)

Injection Attacks

Injection attacks are a type of security attack in which an attacker injects malicious code or data into an application or system with the intent of causing it to perform unintended actions or divulge sensitive information. Injection attacks can target various types of systems, including databases, web applications, and operating systems.
There are several types of injection attacks, including SQL injection, command injection, and cross-site scripting (XSS) injection. SQL injection attacks involve injecting malicious SQL code into a database query, which can result in unauthorized access to sensitive data. Command injection attacks involve injecting malicious code into a command executed by an application or operating system

Sql injection

Lab

SELECT * FROM users WHERE username='$username' AND password='$password'

https://portswigger.net/web-security/sql-injection/lab-login-bypass

Os command injection

OS Command Injection is a type of security vulnerability that occurs when an attacker is able to inject malicious code into a system command that is executed by the operating system. The vulnerability arises when a web application takes user input as part of a command or script that is then executed by the operating system without appropriate validation and sanitation.

Os command injection

Purpose of command	Linux	Windows
Name of current user	whoami	whoami
Operating system	uname -a	ver
Network configuration	ifconfig	ipconfig /all
Network connections	netstat -an	netstat -an
Running processes	ps -ef	tasklist

Lab
https://portswigger.net/web-security/os-command-injection/lab-simple

Cyber security- owsap 10

Insecure direct object references(idor)

is a type of security vulnerability that occurs when an application exposes internal object references, such as file names, record IDs or database keys, as part of a user-accessible interface without appropriate access control checks. As a result, an attacker can modify or access unauthorized data by manipulating the object references.

Lab:
https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references