€TRAINING

Information Security Management (Cyber Security)

Information Security Management (Cyber Security)

Introduction

This course covers prerequisite topics introducing you to information security, programming, and pentesting it also builds strong foundations by giving theoretical lessons reinforced with practical exercises, covering topics like system, network, web app, and Wi-Fi security by the end of this course you will become a professional IT Security personnel and it will increase your ability to defend and assist an organization in assessing and mitigating infrastructure and the risks within the cyberspace

Course Objectives

At the end of this course, the participants will be able to:

 Understand the fundamentals of IT security
 More than interesting theories and lecture
 Gain the required skills of a professional IT Security personnel
 Understand Web Application security and exploit them
 Understanding vulnerabilities and exploits - how to find them and use them
 Understand network exploitation in Linux and windows operating systems
 Discussing some technologies such as DNS/TCPIP/HTTP and some useful techniques such as OSINT
 Understand WIFI Networks Security

Targeted Audience:

- IT professionals and managers responsible for implementing and maintaining an organization's information security program
- Network administrators and engineers
- Security analysts and consultants
- Compliance and risk management professionals
- Auditors and compliance officers
- Business continuity and disaster recovery professionals
- System administrators
- IT managers and executives
- anyone who is interested in information security management.

Course Outlines

Unit 1: Penetration Testing Basics and Web Applications

- Penetration Testing Basics and Process
- TCP/IP - Network Protocols
- Routing and Firewalls
- Wireshark Introduction
- Web Applications Introduction
- HTTP Protocol
- Sessions and Cookies
- Web Applications Information Gathering

- Web Applications Enumeration and Crawling
- Cross Site Scripting XSS

Unit 2: Web Applications and Network basics

- SQL Injections
- Cross-Site Request Forgery
- Web Applications Authentication and Authorization
- Remote Code execution on web apps
- CMS Security
- Understanding Web Services
- Network Penetration Testing Basics
- Network Information Gathering
- Network scanning
- Service and OS Detection

Unit 3: Network Security

- Null Sessions
- SNMP Enumeration
- Basics of ARP
- Traffic Sniffing
- MiTM Attacks
- Cryptography and Password Cracking
- Password Attacks
- Brute-forcing
- Windows Authentication

Unit 4: Network Security

- Metasploit Basics
- Exploitation with Metasploit
- Bypassing antivirus
- Windows Privilege Escalation
- Windows Maintaining Access
- Linux Information Gathering
- Linux Exploitation
- Linux Maintaining Access

Unit 5: Social Engineering and WIFI-Security

- OSINT
- Social Engineering
- Client-Side Exploitation - Spear phishing
- WIFI Standards
- Discover Wi-Fi Networks
- Attacking Wi-Fi Networks
- WPA Capture Attacks
- Rogue Access Point - Evil Twin
- How to write a security assessment Report

info@euro-training.net
+447447999485 - +447492882996