COURSE CATEGORY: CYBER DEFENCE
COURSE LEVEL: ESSENTIALS
COURSE CODE: IFIS CDE/02
COURSE NAME: : I.T SECURITY ESSENTIAL TRAINING

Institute of Forensics & ICT Security
Forensics. Security. Training

With practical skills, You succeed

Institute of Forensics & ICT Security
Forensics. Security. Training

With practical skills, You succeed

About this Course

This course is the first step to learn the most effective steps to prevent cybercrime occurrences and identify threats with hands on techniques that you can directly apply when you get back to work. You will learn from practical sessions delivered by professionals in the field with many years of experience. The knowledge attained will help you and your company that you can win the battle against the wide range of cyber adversaries that want to harm your environment. This course aims to enable students to understand properly how to secure and defend a network.

Prerequisites

This course covers all of the core areas of security and assumes a basic understanding of technology, networks, and security

Learning Outcomes

In this course, you will learn;

(i) Causes of system data losses and breaches
(ii) How to identify compromised systems on your network.
(iii) The value of each security device and their accurate configuration.
(iv) Setting up suitable security metrics

Course Outline

Topic 1: Network Security Essentials

a) Network Essentials
b) Network Architecture
c) Cloud security and Virtualization
d) Device and Network Security
e) Internet protocols and Networking
f) Wireless networks security
g) Online communication security

Topic 2: Defence-In-Depth and Attacks

a) Introduction
b) Access control and password management
c) Security Privacy
d) Security controls
e) Advanced Persistent Threat (APT)

Topic 3: Threat Management

a) Introduction to threat management
b) Vulnerability Scanning
c) Penetration testing
d) Network security devices
e) End point security
f) Active defence

Topic 4: Risk management and response

a) Incident handling foundations
b) Contingency planning – BCP/DRP
c) Risk management

Topic 5: Windows Security

a) The windows security infrastructure
b) Service packs, hot fixes and backups
c) Windows access controls
d) Security policy enforcement
e) Securing network services
f) Automation, Auditing and forensics

Requirements

- System running Windows 64-bit version
- At least 8 GB RAM
- 50 GB of available disk space (more space is recommended)
- Administrator access to the operating system and all security software installed.
- Anti-virus software will need to be disabled in order to install some of the tools.
- An available USB port.
- Machines should NOT contain any personal or company data.
- Verify that under BIOS, Virtual Support is ENABLED.

Target Audience

- Security professionals
- Managers
- Operations personnel
- IT engineers and supervisors
- Administrators
- Forensic analysts, penetration testers, and auditors
- Anyone new to information security

with some background in information systems and networking.
formal training and certification

Applications/ Relevance to the economy

- Apply what you learned directly to your job when you go back to work
- Design and build a network architecture using VLANs, NAC, and 802.1x based on advanced persistent threat indicators of compromise
- Run Windows command line tools to analyse the system looking for high-risk items
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Create an effective policy that can be enforced within an organization and design a checklist to validate security and create metrics to tie into training and awareness
- Identify visible weaknesses of a system using various tools and, once vulnerabilities are discovered, cover ways to configure the system to be more secure
- Build a network visibility map that can be used for hardening of a network validating the attack surface and covering ways to reduce that surface by hardening and patching
- Sniff open protocols like telnet, ftp, and determine the content, passwords, and vulnerabilities using Wireshark.

Duration and fees

Duration: 5 days
Pricing: $400

For Inquiries, booking and more information,

Call Admissions on 0393517236/0783517236 or
Email: admissions@forensicsinstitute.org