A. Customized Security Track

Course Code: CT-SCT	Duration:	6 days
	Delivery Type:	Classroom (Hands-on labs)

Overview

This is one of advance Infrastructure security *course* with the most current security domains any professional will ever want to know when they are planning to beef up the information security posture of their organization. The goal of this course is to help you master security methodology that can be used in a penetration testing or security of infrastructure. You walk out the door with skills that are highly in demand, as well as the internationally recognized

Audience

Course will significantly benefit those who are in the field of Systems/ Network Administration and wish to enhance their knowledge of computer security.

Prerequisites

- Good Knowledge of networking fundamentals.
- Comfort with client server infrastructure.
- Good knowledge of windows and Linux architecture

Course Objective

- Comprehend your IT infrastructure, network (configuration and topology), network traffic and communication system
- Prepare a security policy, processes, procedures, and their implementation plan
- Implement the above policies and plans
- Periodically test and audit the entire network security (Internet, Intranet and Extranet), update it regularly, and maintain an audit trail of all changes
- Undertake preventive measures, before corrective measures become necessary
-
-
- Gain skills to secure latest mobile network platforms.
- Utilize iLabs - a cloud lab based environment for Windows 7/8 and Server 2012.
- Get practical exposure as well as classroom training to understand the underlying concepts of hacking.

Course Outline

Duration: - 6 Days

Day-1

1. **Security Fundamentals**
   - The Information Security Cycle
   - Information Security Controls
   - Authentication Methods
   - Cryptography Fundamentals
   - Security Policy Fundamentals
2. **Security Threats and Vulnerabilities**
   - Social Engineering
   - Physical Threats and Vulnerabilities
   - Network-Based Threats
   - Wireless Threats and Vulnerabilities
   - Software Based Threats

Day-2

Parameter Defense security systems

Introduction to Firewall

Firewall rules and policies.

Router introduction

Hardening and security of Router

Proxy server functioning

Security Concerns of Proxy

Case Study.

Day 3

Control and monitor Filter Configuration

Configure antivirus software for real time scanning at the gateway

OS and Application Server Security System

OS Security

Linux and Windows System Hardening

Application Servers

Web Servers

Mail Server

Day-4

HOST Protection

User Access Policy

Patches, Hot Fixes for workstation

Antivirus

Backup for workstation

Logging and monitoring host

Day-5

Data and Information Protection

Data encryption

Data Storage practices

System best practices.

Physical Security Controls

Mantrap

Biometric implementation

Logging