TRAINING AND EXERCISE COURSE CATALOG

TRAINING AND EXERCISE COURSE CATALOG

Table of Contents

INTRODUCTION

COURSE LISTINGS

Courses in this catalog are divided into four broad categories:

- Product training from CyberCENTS®, which covers the core functionality of CyberCENTS products and solutions, including deployment, administration, and operation activities
- Cyber security training from CyberCENTS, which covers essential cyber security skills that use free, open-source or existing customer technologies, whether or not they are CyberCENTS solutions
- Self-paced training from InfoSec Learning, which covers practical and abbreviated subjects within multiple cyber work roles
- Cyber security exercises from CyberCENTS, which cover a range of industries and activities

INSTRUCTOR-LED PRODUCT TRAINING

Instructor-led product training is presented by a live instructor, either in-person or via a virtual classroom. Instructor-led training includes hands-on labs designed to accelerate the acquisition of practical skills using Cyberoperations Enhanced Network & Training Simulator (CENTS®) solutions. The duration of a single instructor-led product course can range from a one hour to five days.

INSTRUCTOR-LED CYBER SECURITY TRAINING

CyberCENTS instructors are proven experts with years of experience throughout industry and government. Instructor-led Cyber Security Courses are derived from the National Institute for Science and Technology (NIST) National Initiative for Cybersecurity Education (NICE). The duration of a single instructor-led training course can range from a one day to five days.

SELF-PACED TRAINING COURSES

By Light, in partnership with InfoSec Learning LLC, offers several self-paced training courses that emphasize subject matter expertise for different tasks within the NIST NICE work roles. The duration of a single self-paced training course can range from minutes to hours.

EXERCISE PACKAGES

Exercise packages are pre-defined packages developed to exercise cyber security staff from multiple work roles in a team environment. Exercise playbooks are available for facilitators to use to execute the exercise. The duration of a single exercise can range from 6 hours to two weeks.

BLCC-PROD-001-01 - SLAM-R 3.X RANGE MANAGER

This course will provide the user with information on operating and administering the SLAM-R 3.1 Web Client. The course also covers all CENTS architectures supported, including SLAM-R 2.10 units.

The SLAM-R 3.X Range Manager Course of Instruction (COI) has been created to provide CyberCENTS customers with the information required to manage the Cyberoperations Enhanced Network & Training Simulators® (CENTS®) Sentinel, Legion, Auto build, Myrmidon, & Reconstitution (SLAM-R©) Version 3.X Web Client. Topics include an overview of CENTS environments, administration of the SLAM-R exercise control platform, and exercises in building training using SLAM-R.

LEARNING OBJECTIVES

- Discuss the use and purpose of the CENTS training environments to support normal and abnormal operations.
- Discuss the physical configurations of CENTS Equipment Variants and Rack Components.
- Understand SLAM-R 3.X functionality and operation.
- Discuss the use and purpose of Remote Login Tools.
- Discuss the use and purpose of the SLAM-R 3.X Web Client.
- Discuss the use and purpose of the Device Manager.
- Discuss use and purpose of the Traffic Manager.
- Discuss use and purpose of the Traffic Tracker.
- Discuss the use and purpose of the Attack Manager.
- Discuss the use and purpose of the Network Manager.
- Discuss the management of system permission settings using the Authorization option.
- Discuss Log Management.
- Discuss Infrastructure Management.
- Discuss Image Management.
- Discuss License Management.

WHO SHOULD ATTEND

Clients using the CENTS SLAM-R software performing the Range Manager function

PREREQUISITES

Training and/or experience in administering virtual network environments.

DURATION

3.5 Days

BLCC-PROD-001-02 - SLAM-R 3.X RANGE MANAGER DIFFERENCES COURSE

The SLAM-R 3.X Range Manager Differences Course of Instruction (COI) has been created to provide the differences between the CENTS® SLAM-R Version 2.10 and Version 3.X Web Clients. Topics include an overview of the latest CENTS environments, administration of the SLAM-R exercise control platform, and building training and exercises using SLAM-R.

LEARNING OBJECTIVES

- Discuss the physical configurations of CENTS Equipment Variants and Rack Components.
- Understand SLAM-R 3.X functionality and operation.
- Discuss the management of system permission settings using the Authorization option.
- Discuss Log Management.
- Discuss the Infrastructure Management option.
- Discuss the Image Management option.
- Discuss License Management.
- Discuss the use and purpose of the Web Client.
- Discuss the use and purpose of the Device Manager.
- Discuss use and purpose of the Traffic Manager.
- Discuss the use and purpose of the Attack Manager.

- Discuss the use and purpose of the Network Manager.
- Introduction to Exercises Planning and Execution.
- Perform Exercise Planning in the CENTS Immersive Training Environment.

WHO SHOULD ATTEND

Clients receiving the SLAM-R 2.10 to SLAM-R 3.X upgrade.

PREREQUISITES

Training and/or experience in administering SLAM-R 2.10 environments.

DURATION

1.5 Days

BLCC-PROD-001-03 - CENTS LEARNING MANAGEMENT SYSTEM QUICK START TUTORIAL

Basic overview of the CyberCENTS Learning Management System. Training topics include account management and course creation.

DURATION

1 Hour

BLCC-PROD-001-04 - INSTRUCTIONAL SYSTEM DESIGN USING THE CENTS LEARNING MANAGEMENT SYSTEM (LMS)

The Instructional System Design (ISD) Using the Cyberoperations Enhanced Network & Training Simulators® (CENTS®) Learning Management System (LMS) Course of Instruction (COI) has been created to address gaps in training of personnel who use the CENTS LMS as a training platform. Topics within the course include an overview of, configuration of, and operation of the LMS, and the steps involved in planning a course in the LMS. Some topics within this course are refresher training for topics learned in the Industry certification, college-level IT and Cybersecurity degrees, and military training.

LEARNING OBJECTIVES

- Discuss the functional overview of the CENTS Learning Management System (LMS).
- Discuss the deployment of the CENTS LMS training environments.
- Discuss the initial configuration of the CENTS LMS.
- Discuss navigation and management of courses in the CENTS LMS.
- Discuss the Role-Based Access Controls and enrollments using the CENTS LMS.
- Discuss the course competencies and grading to support training IAW CENTS documentation.
- Discuss the course maintenance and back-up procedures.
- Discuss how to add course feedback within the CENTS LMS.

WHO SHOULD ATTEND

Clients using the CENTS LMS to develop and deliver training and exercises.

PREREQUISITES

Training and/or experience in instructional system design, curriculum development, exercise planning and instruction.

DURATION

1 Day

BLCC-PROD-001-05 - CENTS CAPTURE-THE-FLAG SCORING ENGINE TUTORIAL

Scoring Exercises Using the CENTS® Capture-the-Flag (CTF) Scoring Engine Course of Instruction (COI) has been created to provide CyberCENTS customers with the information required to operate and manage the Cyberoperations Enhanced Network & Training Simulators® (CENTS®) Capture-the-Flag (CTF) Scoring Engine. Topics within the course include an overview of and information on the administration & operation of the Capture-the-Flag (CTF) Scoring Engine.

LEARNING OBJECTIVES

- Discuss the configuration of the CENTS Capture-the-Flag Scoring Engine to support exercise events.
- Discuss the administration of the CENTS Capture-the-Flag Scoring Engine.
- Discuss the participant operation of the CENTS Capture-the-Flag Scoring Engine.

WHO SHOULD ATTEND

Clients using the CENTS Capture-the-Flag scoring engine within SLAM-R to build, distribute and score flags found by exercise participants.

PREREQUISITES

Training and/or experience in exercise planning and CTF-style exercise execution.

DURATION

1 Hour

BLCC-PROD-001-06 - SECURE INFRASTRUCTURE AND COLLABORATION CAPABILITY (SIC-2) VIDYO® DISPLAY SYSTEM

The Secure Infrastructure Collaboration Capability (SIC-2) Vidyo Display Systems Course of Instruction (COI) has been created to provide CyberCENTS customers with the information required to operate and manage the Cyberoperations Enhanced Network & Training Simulators® (CENTS®) Secure Infrastructure Collaboration Capability (SIC-2) Vidyo Display Systems. Topics within the course include an overview of, information on the administration of, and exercises in operating the SIC-2 Display System.

LEARNING OBJECTIVES

- Discuss the purpose and physical layout of the Secure Infrastructure Collaboration Capability (SIC-2) Vidyo® Display Systems.
- Understand the BigNote built-in software features.
- Understand the function and operation of VidyoRoom HD-3.
- Discuss the additional documentation on the hardware used in the Vidyo portfolio.

WHO SHOULD ATTEND

Clients using the SIC-2 Vidyo products to perform cyber operations and collaboration between operational teams.

PREREQUISITES

Training and/or experience in the use of collaboration tools to assist in planning and operations.

DURATION

4 Hours

BLCC-ILC-001-02 CYBER INCIDENT RESPONDER

The Cyber Incident Response (CIR) Course of Instruction provides training on computer network detection and response techniques, tools and supporting systems. This training and exercise follow the NIST Special Publication 800-61 Incident Response Life Cycle. Participants will defend ICS/SCADA devices and organizational systems against an Advanced Persistent Threat. The training is intended for use by local, state, commercial and educational institutions.

LEARNING OBJECTIVES

- Discuss the use and purpose of the Cyberoperations Enhanced Network & Training Simulators (CENTS) to support training and exercises.
- Review the use and purpose of Remote Login Tools to support normal and maintenance operations in the CENTS environment IAW the SLAM-R Systems Administrator Guide.
- Apply critical thinking and legislation/directives to assist in security the network.
- Identify cybersecurity chains of command and reporting structures.
- Understand compliance with national and international laws, regulations, policies, and ethics as they relate to cybersecurity.
- Discuss cybersecurity principles to support defense-in-depth of the network using systems provided in the CENTS environment.
- Understand information assurance (IA), mission assurance (MA), and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data.
- Understand incident categories, incident responses, and timelines for responses.
- Examine strategies for containing, eradicating, and recovering from an incident.
- Discuss the cyber environment and uses of systems within the cyber environment to support normal and maintenance operations in the CENTS environment.

WHO SHOULD ATTEND

This course is intended for Local, State, Federal and Industry cyber security personnel to network with other geographic partners in team-based exercises using emulations of enterprise networks, Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition equipment cyber intrusions.

PREREQUISITES

Training and/or experience in IT Systems Administration and/or cyber security.

DURATION

3.5 Days

BLCC-ILC-001-01 - CYBER DEFENSE ANALYST

The Cyber Network Defense (CND) course provides trainees with the background knowledge, skills, and abilities to perform cyber operations against an emulated adversary using the Cyberoperations Enhanced Network & Training Systems (CENTS) as the training environment. The course includes a well-rounded approach to the organization's cybersecurity program and its support to cyber incident response. The course will culminate in an exercise that takes trainees through the cyber kill chain prompting them to respond by using tactics, techniques and procedures learned throughout the course. The course provides an overall definition of the organization's cyber security program.

LEARNING OBJECTIVES

- An introduction to the CENTS platforms that support exercises and training.
- Discussion on current events, critical thinking, and the use of Open-Source Research to aid in troubleshooting, research and incident response.
- Knowledge of the organizational reporting structures for cyber incident response and reporting.
- Discussion of how the IT Security Policy Framework of the organization supports compliance with international law and creating a security baseline.
- Identifying risks, threats and vulnerabilities within the network and the use of network management frameworks to bolster the cybersecurity program.
- The fundamentals of cybersecurity and the tactics, techniques and procedures of malicious actors.
- Detecting and analyzing network traffic to identify possible malicious activity.
- Efforts to contain, eradicate and recover from a cyber incident.
- Tools used to remotely log into devices on the network to perform cyber network defense and administration.

- Discussion of the tools and devices housed within the normal enterprise network and the CENTS architecture to be used during the Cyber Network Defense exercises in this course.
- Cyber network defense exercises that train students in the tactics and techniques used by adversarial actors and the defense against those tactics and techniques.

WHO SHOULD ATTEND

This course is intended for cyber security personnel responsible for defending the enterprise network in team-based exercises.

PREREQUISITES

Training and/or experience in Cyber Network Defense.

DURATION

5 Days

BLCC-ILC-001-03 - CYBER OPERATIONS ANALYST

This course provides in depth technical information by having participants defend enterprise enclaves against major attacks.

LEARNING OBJECTIVES

- Discuss the use and purpose of the Cyberoperations Enhanced Network & Training Simulators (CENTS) to support requirements gathering operations.
- Review the use and purpose of Remote Login Tools to support normal and maintenance operations in the CENTS environment IAW the SLAM-R Systems Administrator Guide.
- Apply critical thinking and legislation/directives to assist in security the network.
- Identify the National Cyber Chain of Command, the missions of the Cyber Mission Forces (CMFs), the mission of the Color Teams, and the reporting structure.
- Understand national and international laws, regulations, policies, and ethics as they relate to cybersecurity.
- Discuss the use, purpose, and implementation of cybersecurity principles to support defense-in-depth of the network using systems provided in the CENTS environment.

- Understand information assurance (IA), mission assurance (MA), and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data.
- Understand incident categories, incident responses, and timelines for responses.
- Examine strategies for containing, eradicating, and recovering from an incident.
- Practice network enumeration to become familiar with the Florida Cyber Range (FCR) environment.
- Manage devices by implementing tools in the FCR.
- Perform cybersecurity response actions for a variety of simulated cyber incidents in the FCR and operate as a team to manage a multi-faceted, advanced, persistent, simulated threat.

WHO SHOULD ATTEND

CyberCENTS customers that are required to perform as a Cyber Network Defender using the Cyberoperations Enhanced Network & Training Simulators® (CENTS®).

PREREQUISITES

Advanced training and certification in operating systems, manufacturer systems, security or an IT/Cybersecurity Degree (Associates and 2 years' experience or Bachelors).

DURATION

5 Days

BLCC-ILC-001-05 - EXERCISE PLANNING USING CENTS IMMERSIVE TRAINING ENVIRONMENTS

The Planning Exercises Using the CENTS® SLAM-R© 3.X Immersive Training Environments Course of Instruction (COI) has been created to provide Metova CyberCENTS customers with the information required to plan and execute exercises using the Cyberoperations Enhanced Network & Training Simulators® (CENTS®) Sentinel, Legion, Auto build, Myrmidon, & Reconstitution (SLAM-R©) Version 3.X Web Client. Topics within the course include an overview of the exercise planning process. This course is meant to be a .5-day add-on component with the SLAM-R 3.X Range Manager course of instruction and uses the Department of Defense Joint Event Life Cycle method of building exercises as an example.

LEARNING OBJECTIVES

- Analyze mission goals and identify mission essential tasks in accordance with (IAW) the CJCSI 3500.01, Joint Training Policy for the Armed Forces of the United States and the Joint Mission Essential Task List (JMETL) Development Handbook, dated September 2002.
- Discuss the Joint Event Life Cycle (JELC) for exercise planning, execution and after-action reporting IAW the CJCSM 3500.03E, Joint Training Manual for the Armed Forces of the United States, Enclosure E, dated 20 April 2015.
- Perform the processes and procedures for planning, executing and de-briefing a Cyber Network Defense exercise IAW CJCSM 3500.03E, JMETL Development Handbook, AFI 36-2251, and the SLAM-R 2.10 User's Guide.

WHO SHOULD ATTEND

This course is intended for exercise planners who use the CENTS family of products to plan and execute cyber exercises.

PREREQUISITES

Training and/or experience in cyber security and network defense.

DURATION

4 Hours

BLCC-ILC-001-04 - CURRICULUM DEVELOPMENT USING CENTS IMMERSIVE TRAINING ENVIRONMENTS

The Enhancing Curriculum Using the CENTS® SLAM-R© 3.X Immersive Training Environments Course of Instruction (COI) has been created to provide CyberCENTS customers with the information required to perform curriculum development using the Cyberoperations Enhanced Network & Training Simulators® (CENTS®) Sentinel, Legion, Auto build, Myrmidon, & Reconstitution (SLAM-R©) Version 3.X Web Client. Topics within the course include an overview of the curriculum development process. This course is meant to be a 1-day add-on component with the SLAM-R 3.X Range Manager course of instruction.

LEARNING OBJECTIVES

- Understand educational psychology of adult learners and how the adult learner applies training objectives to job tasks using best practice, instructional techniques and educational psychology models.
- Discuss the steps required to perform a Training Needs Assessment (TNA).
- Discuss the System Training Plan (STP).
- Discuss Training Course Control Documents (TCCDs) and Resource Requirements.
- Analyze business goals and identify business essential knowledge, skills, abilities (KSAs) and Tasks for education tasks identified during the Planning Phase of PADDIE.
- Discuss design and development of education courses.
- Discuss the implementation and evaluation of classroom.

WHO SHOULD ATTEND

This course is intended for personnel responsible for developing training and education courses.

PREREQUISITES

Training and/or experience in Instructional System Design, Curriculum Development and/or Instruction.

DURATION

3 Days

CYBER EXERCISES

BLCC-CEX-001-01- EXECUTIVE-LEVEL CYBER SEMINAR

This presentation provides an overview of current events and cyber tactics and techniques being used by malicious actors.

LEARNING OBJECTIVES

- Define the C-Suites roles and responsibilities.
- Define terms related to Cybersecurity.
- Understand security-related laws, guidelines, and policies that mandate some of the tasks and responsibilities of management.
- Accepting risk.

WHO SHOULD ATTEND

Executive Cyber Leadership.

PREREQUISITES

Associates and 2 years' experience or Bachelors

DURATION

1 Hour

BLCC-CEX-001-02 - C-SUITE CYBER TRAINING AND TABLE-TOP EXERCISE

This presentation is a follow-on to the Executive Leadership Cyber Seminar, and exercises management on responding to cyber breaches in a table-top exercise environment. Training audience should react and respond according to the organization's IT Security Policy Framework and Pre-Planned Responses.

LEARNING OBJECTIVES

- Discuss current events in Cybersecurity, and how they affect your organization.
- Apply concepts and terms of management and IT security frameworks.

- Identify laws, regulations, policies, and procedures that guide the organization.
- Identify responsibilities of the cybersecurity team.
- Exercise organizational policy base for continual improvement of the organization's IT Security Policy Framework.

WHO SHOULD ATTEND

Cybersecurity Management

Customer Service and Technical Support

Executive Cyber Leadership

PREREQUISITES

Associates and 2 years' experience or Bachelors

DURATION

1 Day

BLCC-CEX-001-03 - SECURITY OPERATIONS CENTER TRAINING AND EXERCISE

This exercise will exercise the Security Operations Center in responding to several cyber incidents.

LEARNING OBJECTIVES

- Perform Cyber Operations throughout the anatomy of an attack.
- Employ Protect, Detect, Respond and Recover techniques as needed.

WHO SHOULD ATTEND

Cybersecurity Management

Vulnerability Assessment and Management

PREREQUISITES

Associates and 2 years' experience or Bachelors

DURATION

3 Day

BLCC-CEX-001-04 - SMALL TO MEDIUM-SIZED HIPAA/HITECH TABLE-TOP AND DISCUSSION

This exercise consists of several video injects of HIPAA/HITECH and other cyber security practice violations. It is a one-day, table-top exercise.

DURATION

1 Day

CYBER DEFENSE ANALYST TRACK (SELF-PACED)

This training track provides information aligned with the National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) Knowledge, Skills, Abilities (KSAs) and Tasks for Cyber Defense Analyst, PR-CDA-001, and Cyber Defense Infrastructure Support Specialist, PR-INF-001.

BLCC-CDA-001-00 - NIST CYBER DEFENSE ANALYST (CDA) USING CENTS – INTRODUCTION

This topic is an overview of how the courses within this track satisfy the NICE Work Role KSAs and Tasks required for the Cyber Defense Analyst and Cyber Defense Infrastructure Support Specialist Work Roles.

DURATION

15 Minutes

BLCC-CDA-001-01 - INFORMATION OPERATIONS

This topic reviews one of our most important tools, Information!! In the topic, we'll discuss current events in the cybersecurity realm. We'll then discuss resources that are available for doing open-source research, or intelligence. Lastly, we'll display how the bad guy uses this same tool to enumerate a target.

DURATION

45 Minutes

BLCC-CDA-001-02 - CYBER FUNDAMENTALS

This topic provides a foundational understanding of cybersecurity tactics, techniques and procedures (TTPs). In the topic, we'll review fundamental information about types of attacks and attackers.

DURATION

25 Minutes

BLCC-CDA-001-03 - DEFENSE-IN-DEPTH & RISK

This topic provides an understanding of security through defense-in-depth and defines risks to our enterprise from breaches.

DURATION

45 Minutes

BLCC-CDA-001-04 - LAW, COMPLIANCE AND THE CYBERSECURITY POLICY FRAMEWORK

This topic is an overview of National and International regulations that drive our organization's cybersecurity policy framework.

DURATION

30 Minutes

BLCC-CDA-001-05 -NETWORK, SECURITY & INCIDENT MANAGEMENT FRAMEWORKS

In this topic, we discuss several management frameworks that will assist you in performing security operations.

DURATION

30 Minutes

BLCC-CDA-001-06 -REMOTE LOGIN TOOLS

This topic steps you through the operation of tools to communicate remotely with the VNC, RDP, NoVNC, and SSH protocols. Students use the actual tools to remote around the CENTS Immersive Training Environment.

DURATION

15 Minutes

BLCC-CDA-002-01 - NETWORKING 200-LEVEL

This course reviews network fundamentals and discusses intermediate networking concepts.

LEARNING OBJECTIVES

- The TCP/IP Model, LANS, WANS, and IP Networks
- TCP/IP Network, Transport & Application Layers
- IP Subnetting
- IP Routing with Connected, Static, and RIP-2 Routes
- IP Troubleshooting and EIGRP
- Subnet Design
- Advanced IP Routing and OSPF
- Troubleshooting Routing Protocols and IP Version 6
- Troubleshooting LANs
- Troubleshooting WANs

DURATION

4 Hours

BLCC-CDA-003-01 - INTRODUCTION TO PACKET ANALYSIS

This course introduces you to the basic operation of the Internet, the key protocols, their uses, how they are typically exploited and how you can protect a network that requires the protocol.

We begin with a short discussion about how packets are structured in encapsulated layers on the Internet and what normal protocols look like in the protocol analysis tool Wireshark.

LEARNING OBJECTIVES

- Introduction to Packet Analysis
- How the Internet Works
- Introduction to Wireshark
- Using Wireshark to Understand the OSI Layers and TCP Header
- Understanding Key Protocols through Packet Analysis
- Deep Dive Packet Analysis to Support Intrusion Detection

DURATION

2 Hours

BLCC-CDA-001-07 - PROXY & NAT FUNCTIONALITY

Some security is provided by limiting our public-facing IP space. By using NAT and/or proxy server techniques, we can mask the IP of our internal user. This topic is a deep-dive in the Network Address Translation, Port Address Translation and Proxying.

DURATION

15 Minutes

BLCC-CDA-001-08 - INTRUSION DETECTION & INTRUSION PREVENTION

Recognizing an attack is in progress is critical to our job as a cyber defense analyst. This topic will review tools we use to provide intrusion detection and prevention.

DURATION

30 Minutes

BLCC-CDA-004-01 - STRUCTURED QUERY LANGUAGE (SQL) & SQL INJECTION (SQLI)

This topic provides basic and intermediate training in the Structured Query Language (SQL), as well as the use of SQL injection (SQLi) as a means to break through defenses.

DURATION

4 Hours

BLCC-CDA-001-09 - EMAIL ANALYSIS

This topic provides an understanding of email log and header analysis, and it provides an overview of the use of DNS with email.

DURATION

30 Minutes

BLCC-CDA-005-01 - CROSS-SITE SCRIPTING (XSS) ATTACKS

This course introduces you to basic concepts in a Cross-Site Scripting (XSS) attack. This is a very common and dangerous class of attacks involving web site vulnerabilities using malicious code injection in a web page or application.

When you complete this course, you will understand the different types of XSS attacks, how they are used and what they are designed to achieve from an attacker's viewpoint. The course also provides a discussion on detection and mitigation strategies.

LEARNING OBJECTIVES

- Introduction to Cross-Site Scripting
- Interacting with Web Application

- Web Languages
- Impact of Successful XSS Attacks
- Types of XSS Attacks
- Preventing and Detecting XSS Attacks
- Analyzing XSS Attacks

DURATION

4 Hours

BLCC-CDA-001-10 - MALWARE ANALYSIS, ANTI-VIRUS AND FORENSICS TOOLS

This topic is an introductory course in Malware Analysis and Monitoring. Discussions in the topic include the definition of different types of malware, the use of anti-virus, and what to do when under attack by malware.

DURATION

15 Minutes

SELF-PACED TRAINING COURSES

Self-paced courses are available from InfoSec Learning in partnership with By Light Professional IT Services. Multiple tracks are available from which trainers can assemble training plans. The tracks include:

- Information Security Fundamentals
- Ethical Hacking & Systems Defense
- Networking Fundamentals
- Digital Forensics
- Linux Server I: Linux Fundamentals
- Linux Server II: System Administration
- Scripting Fundamentals
- Network Security Fundamentals
- Linux-based Security+
- Pentesting and Understanding Vulnerabilities
- Hadoop Administration
- PC Maintenance and Repair
- Introduction to Operating Systems

INFOSEC LEARNING TRAINING TRACK BREAK-DOWN

INFOSEC LEARNING LIST OF LABS AND CORRESPONDING CERTIFICATIONS

INFORMATION SECURITY FUNDAMENTALS | PREPARE FOR COMPTIA SECURITY +

Securing the pfSense Firewall
Implementing NAT and Allowing Remote Access
Implementing Common Protocols and Services
Examining Wireless Networks
Implementing Security Policies on Windows and Linux
Data Backups in Windows, BSD, and Linux
Incident Response Procedures, Forensics, and Forensic Analysis
Crafting & Deploying Malware Using a Remote Access Trojan (RAT)
Social Engineering Using SET

Breaking WEP and WPA and Decrypting the Traffic

Deep Dive in Packet Analysis - Using Wireshark and Network Miner

Remote and Local Exploitation

Patching, Securing Systems, and Configuring Anti-Virus

Using Active Directory in the Enterprise

Using Public Key Encryption to Secure Messages

Securing the pfSense Firewall

ETHICAL HACKING & SYSTEMS DEFENSE | PREPARE FOR EC COUNCIL C|EH

Performing Reconnaissance from the WAN

Scanning the Network on the LAN

Enumerating Hosts using Wireshark, Windows, and Linux Commands

Remote and Local Exploitation***

Crafting and Deploying Malware Using a Remote Access Trojan (RAT)***

Capturing and Analyzing Network Traffic Using a Sniffer

Social Engineering Using SET***

Performing a Denial of Service Attack from the WAN

Using Browser Exploitation to Take Over a Host's Computer

Attacking Webservers from the WAN

Exploiting a Vulnerable Web Application

Performing SQL Injection to Manipulate Tables in a Database

Breaking WEP and WPA and Decrypting the Traffic***

Attacking the Firewall and Stealing Data over an Encrypted Channel

Using Public Key Encryption to Secure Messages***

***** Lab used in multiple sets**

NETWORKING FUNDAMENTALS | PREPARE FOR COMPTIA NET +

Configuring Port Redirection

Implementing NAT and Allowing Remote Access***

IPv4 vs IPv6 – Calculating, Configuring and Testing

Network Management

Business Continuity - Disaster Recovery

Breaking WEP and WPA and Decrypting the Traffic***

Closing Ports and Unnecessary Services

Implementing Security Policies on Windows and Linux

Network Security - Firewalls

Network Troubleshooting

TCP/IP Utilities

The OSI Model

TCP/IP Protocols - The Core Protocols

TCP/IP Protocols - Other Key Protocols

Types of Networks

Remote Access - RDP

***** Lab used in multiple sets**

DIGITAL FORENSICS | PREPARE FOR GIAC FORENSIC EXAMINER

Introduction to File Systems

Common Locations of Windows Artifacts

Hashing Data Sets

Drive Letter Assignments in Linux

The Imaging Process

Introduction to Single Purpose Forensic Tools

Introduction to Autopsy Forensic Browser

FAT File System

The NTFS File System

Browser Artifact Analysis

Communication Artifacts

User Profiles and the Windows Registry

Log Analysis

Memory Analysis

Forensic Case Capstone

LINUX SERVER I: LINUX FUNDAMENTALS | PREPARE FOR COMPTIA LINUX +, LPIC 1

CentOS Server Linux Installation

Ubuntu Desktop Linux Installation

Installing Packages and Shared Libraries on Fedora and Ubuntu

Displaying Hardware

Adding a New Partition

Managing Filesystem Quotas

Booting and Restarting the System

Using the BASH Shell - 1

Using the BASH Shell - 2

Using the BASH Shell - 3

Using the BASH Shell - 4

Monitoring Processes

Working with Files

Managing Text Files - 1

Managing Text Files - 2

Managing Text Files - 3

LINUX SERVER II: SYSTEM ADMINISTRATION | PREPARE FOR COMPTIA LINUX +, LPIC 1

Configuring X Windows in CentOS and Fedora Desktop

Accessibility Technologies

User and Group Accounts

System Administration Tasks - 1

System Administration Tasks - 2

System Administration Tasks - 3

crontab and at

Configuring Locale and Time Zone Settings

Working with Email - 1

Working with Email - 2

Basic Network Configuration

Basic Security Administration

Securing Data with Encryption on a Linux System

Host Security

BASH shell features

BASH Scripting

Working with a SQL Database

SCRIPTING FUNDAMENTALS

Advanced Data Structure Usage

File I/O, String Parsing and Data Structures

Tuples(Arrays), Error handling and Secure Programming

Loops

Math in Python

Getting Started with Python on Ubuntu - Running from the Command Line

Introduction to Control Structures and Data Types

Getting Started with Python on Ubuntu - Writing Your First Program

Verifying a File Type with its Extention

Creating a Ping Scanner

Data Visualization

Pattern Matching

Extracting and Cleaning Data Using Python

Analysis with Kmeans

Inheritance

NETWORK SECURITY FUNDAMENTALS

Configuring a Windows based Firewall to Allow Incoming Traffic

Configuring a Linux based Firewall to Allow Incoming and Outgoing Traffic

Implementing Secure DHCP and DNS

Configuring a Linux based Firewall to Allow Outgoing Traffic

Configuring Access Control Lists on a Linux Based Firewall

Configuring a Virtual Private Network with PPTP

Configuring a Virtual Private Network with OpenVPN

Implementing RIP, RIPv2, and Securing RIP

Intrusion Detection using Snort

Writing Custom Rules

Host-Based Firewalls

Configuring RADIUS

Domain Security

Configuring a Site to Branch a Virtual Private Network

Closing Security Holes

LINUX BASED SECURITY + | PREPARE FOR COMPTIA SECURITY +

Configuring a VPN tunnel using the pfSense Firewall

Comparing and Contrasting using Clear Text Protocols

Linux Attack and Response

Log Analysis of Linux Systems with Grep and Gawk

Attacking and Defending Linux

Cracking Passwords on Linux Systems

Identifying & Analyzing Network Host Intrusion Detection System

Exploiting Shellshock

Vulnerability Scanning of a Linux Target

Encrypting Data using TrueCrypt and Attacking the TrueCrypt password using TrueCrack

Injection Attacks using WebGoat

Permissions, Users, and Groups in Linux

Creating a Proxy Server and an SSL Certificate using the pfSense Firewall

Steganography

PENTESTING AND UNDERSTANDING VULNERABILITIES

Provisioning a Web Server

Exploring HTML

Provisioning a MySQL Database

Provisioning PHP

Dissecting the Login Process

SQL Injections (SQLi)

SQLi Vulnerability and Pentesting Steps

HTML Injections (HTMLi)

HTMLi Vulnerability and Mitigation

Reflected XSS

Reflected XSS Mitigation and URL Encoding

PHP Sessions and Cookies

Additional SCRIPT Elements

Session Stealing (Remote Reflected XSS)

Remote Reflected XSS Mitigation and URL Encoding

Vulnerable Forum

Pentesting the Forum

Session Stealing (Stored XSS)

Command Injection

Stateless Firewall

Abusing a Stateless Firewall

Stateful Firewall

Abusing a Stateful Firewall

IDS, SYSLOG, and NTP

Signature Detection and Alerting an Admin

IPS, SYSLOG, and NTP

Signature Detection and Remote Shells

Remote Shell: Embedding Client-side Code into a Package

Remote Shell Extracting Data

Incident Response

HADOOP ADMINISTRATION

Hadoop 1.2.1

Map Reduce

Hadoop 1.2.1 Cluster

Name Node Failover

Hadoop 2.7.3

Hadoop 2.7.3 Cluster

PC MAINTENANCE AND REPAIR | PREPARE FOR COMPTIA A +

Examining PC Hardware

PC Operating Systems

Networking Essentials

Printers

Security Practices

Troubleshooting

Disk Maintenance and Data Recovery

Command Prompt Tools

Remote Access

Control Panel

Desktop Customization

Using Active Directory in the Enterprise ***

Data Backups in Windows, BSD, and Linux ***

Ubuntu Desktop Linux Installation ***

Domain Security ***

*** Lab used in multiple sets

INTRODUCTION TO OPERATING SYSTEMS | MAPPED TO MCGRAW-HILL BOOK "SURVEY OF OPERATING SYSTEMS"

Introduction to Operating Systems

Computer Security Basics

Desktop Virtualization

Introduction to Windows 7

Introduction to Windows 8.1

Introduction to Windows 10

Supporting and Troubleshooting Windows

Linux on the Desktop

Connecting Desktops and Laptops to Networks

Mobile Operating Systems

File Management in the Cloud

EXERCISE PACKAGES

HIPAA/HITECH MEDICAL TABLE-TOP

This exercise is a scenario-based exercise program to assess the cyber security response preparedness of healthcare organizations. The exercise is driven by several video scenarios that provide hints to either HIPAA/HITECH violations, illegal activities, non-use of best practices, and/or policy violations. The exercise is a Table-Top exercise designed to drive discussions and test/exercise policies and procedures within your organization.

EXERCISE OBJECTIVES

- Assess your incident response preparedness and crisis management capabilities in response to realistic and relevant cyber threats and events
- Improve the maturity of your cyber security program by identifying lessons learned from the simulation exercises
- Increase cyber security awareness across your organization
- Engage and educate executives on cyber security
- Engage and educate healthcare personnel at all levels on cyber security
- Establish/broaden partnerships and relationships across the healthcare industry to increase collaboration on cyber security challenges
- Assess your incident response preparedness and crisis management capabilities in response to realistic and relevant cyber threats and events

WHO SHOULD ATTEND

This exercise is intended for small to medium-sized medical facilities.

PREREQUISITES

None.

DURATION

1 Day

SECURITY OPERATIONS CENTER EXERCISE (SOCEX)

This exercise is a scenario-based exercise program to assess the cyber security incident response. The exercise is driven by scenario events that exercise the MITRE Cyber Kill Chain and the NIST SP 800-61 Incident Response Life Cycle. The exercise is a 3-day scenario-driven exercise designed to drive actions of the Security Operations Center Team and to test/exercise policies and procedures within your organization.

EXERCISE OBJECTIVES

- Perform steps to prepare system baselines and incident response activities.
- Detect and identify cyber events using tools, techniques and procedures within the CENTS immersive training environments.
- Analyze and report cyber events taking place within the network.
- Contain cyber incidents to keep organizational resources safe from ongoing cyber incidents.
- Eradicate and mitigate system security events to continue business or mission.
- Restore the network to 100% usability after eradication of a cyber intrusion.
- Perform post-incident activities in accordance with organizational plans and procedures.

WHO SHOULD ATTEND

This exercise is intended for established Security Operations Centers (SOCs).

PREREQUISITES

Participants should be members or training to be members of the organization's SOC.

DURATION

3 Days

EXECUTIVE LEADERSHIP CYBER SEMINAR AND TABLE-TOP EXERCISE

The Executive Leadership track is offered in two offerings. They are as follows:

- Cyber Seminar (Only) – An executive overview of current cyber events and techniques being used against industry sectors.
- Cyber Seminar, Training and Table-Top Exercise – A management level cyber response course that begins with the Cyber Seminar discussed above, followed by training for cyber managers and a table-top exercise to assess organizational policies, procedures and pre-planned responses.

EXERCISE OBJECTIVES

- Review current malicious cyber actors and techniques being used within industry sectors.
- Respond to various cyber events using organizational policies, procedures and pre-planned responses
- Assess policies, procedures and pre-planned responses for accuracy and efficiency.
- Use organizational incident response and disaster recovery techniques.
- Eradicate and mitigate system security events to continue business or mission.
- Restore the network to 100% usability after eradication of a cyber intrusion.
- Perform post-incident activities in accordance with organizational plans and procedures.

WHO SHOULD ATTEND

This exercise is intended for executive and management-level personnel within the organization.

PREREQUISITES

None.

DURATION

Cyber Seminar (Only) – 1 Hour

Cyber Training and Table-Top – 7 Hours

Contact Us: 618.624.7800

CyberCENTS

8484 Westpark Drive

Suite 600

McLean, VA 22102

cybercents.sales@metova.com