CYBERSECURITY ATTACKS DEFENSE FUNDAMENTALS HANDS-ON TRAINING

Course Description

This course provides a comprehensive overview of cybersecurity attacks and defense strategies, focusing on fundamental concepts, techniques, and best practices for protecting against cyber threats. Participants will gain an understanding of various types of cyber attacks, including malware, phishing, ransomware, denial-of-service (DoS), and advanced persistent threats (APTs), as well as defensive measures such as intrusion detection, incident response, threat intelligence, and security awareness training. Through a combination of theoretical instruction, hands-on exercises, case studies, and simulations, participants will develop the skills and knowledge necessary to identify, mitigate, and respond to cyber threats effectively.

I.T.LLECTUAL MANILA

ITELLEQQ TRAINING AND CONSULTANCY

A Comprehensive two (2) day hands-on training for Network Administrators and Network Security Specialist!

—

Conducted by one of best Cybersecurity Expert in the Philippines!

—

Full packed with real-world case studies, threat analysis, defensive measures cyber attacks simulations!

—

Guaranteed learning as we always do hands-on!

—

ITLLECTUAL MANILA
Suite 210 FMSG Bldg.
1823 E. Rodriguez Sr. Ave.
Brgy. Immaculate Conception
Cubao, Quezon City
Philippines 1111

www.itelleqq.com
0915-4885708 | 0919-5618888

Course Objectives:

Upon completion of this training, participants will be able to:

- ✓ Define fundamental concepts of cybersecurity attacks and defense strategies.
- ✓ Identify common cyber attack vectors, including malware, phishing, ransomware, and social engineering.
- ✓ Understand the motivations and tactics used by cyber attackers to compromise systems and networks.
- ✓ Recognize signs of cyber attacks and indicators of compromise (IOCs) within network traffic and system logs.
- ✓ Implement defensive measures, including intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM) solutions.
- ✓ Develop incident response plans and procedures for detecting, containing, and mitigating cyber security incidents.
- ✓ Utilize threat intelligence sources and tools to enhance proactive cyber threat detection and response capabilities.
- ✓ Conduct security awareness training programs to educate end users on best practices for preventing and responding to cyber attacks.
- ✓ Analyze real-world cyber attack scenarios and case studies to understand attack methodologies and defensive strategies.
- ✓ Participate in hands-on exercises and simulations to simulate cyber attack scenarios and practice defensive responses.

Course outline:

Module 1: Introduction to Cybersecurity Attacks and Defense Fundamentals

- ✓ Overview of cybersecurity landscape
- ✓ Importance of cybersecurity defense strategies

Module 2: Common Cyber Attack Vectors

- ✓ Malware attacks: Types and characteristics
- ✓ Phishing attacks: Techniques and prevention
- ✓ Ransomware attacks: Impact and mitigation
- ✓ Social engineering attacks: Tactics and red flags

Module 3: Defensive Measures

- ✓ Intrusion detection systems (IDS)
- ✓ Intrusion prevention systems (IPS)
- ✓ Security information and event management (SIEM)
- ✓ Network segmentation and access controls

Module 4: Incident Response Planning and Procedures

- ✓ Developing incident response plans
- ✓ Incident detection and analysis
- ✓ Incident containment and mitigation
- ✓ Incident recovery and post-incident analysis

Module 5: Threat Intelligence and Proactive Defense

- ✓ Sources of threat intelligence
- ✓ Threat intelligence analysis and utilization
- ✓ Implementing threat intelligence-driven defense strategies

Module 6: Security Awareness Training

- ✓ Importance of security awareness
- ✓ Designing and delivering effective security awareness training programs
- ✓ Best practices for end user education and training

Course outline, continued:

Module 7: Real-World Cyber Attack Scenarios and Case Studies

- ✓ Analysis of real-world cyber attacks
- ✓ Understanding attack methodologies and tactics
- ✓ Defensive strategies and lessons learned from case studies

Hands-on Exercises and Simulations

- ✓ Simulated cyber attack scenarios
- ✓ Incident response simulations
- ✓ Defensive response exercises

Target Audience:

This course is suitable for cybersecurity professionals, IT professionals, system administrators, network administrators, incident responders, and anyone interested in learning fundamental concepts and strategies for defending against cyber attacks.

Prerequisites:

Basic understanding of networking concepts and familiarity with cybersecurity fundamentals is recommended.

Duration:

2-Days | 14-hours (Customizable based on specific training needs)

Delivery Method:

Instructor-led training with a combination of lectures, case studies, group discussions, actual demonstration, and hands-on exercises.

Certification:

Upon successful completion of the training program and assessment, participants will receive a Certificate of Completion in Cybersecurity Attacks and Defense Fundamentals Training.

Training Investment:

Per head Investment – **Php22,400.00 (VAT-Inc)**

Exclusive/Group Training – **Php 224,000.00 (VAT-Inc),** maximum of 10 participants

Outside Manila or Provincial Training – Subject to verification and customized costing.

Securing the training slot:

Upon settling the training investment, send the proof of payment, full name, mobile number, and email address to itllectualmanila@gmail.com.

Where to pay:

Bank Name: LANDBANK OF THE PHILIPPINES

Account Name: ITELLEQQ TRAINING AND CONSULTANCY

Account Number: 5462-0024-42

Bank Name: BANCO DE ORO

Account Name: VANESA CEZAR

Account Number: 001100-205134

GCASH

Account Name: VANESA CEZAR

Gcash Number: 09154655700

Other concerns? Contact our Hotline:

0915-4885708 | 0919-5168888 | itllectualmanila@gmail.com

"Anyone who stops learning is old, whether 20 or 80, anyone who keeps learning stays young. The greatest thing in life is to keep your mind young."

– Henry Ford -