Training course outline

ITU and Naif Arab University for Security Sciences (NAUSS)

Title	Cybersecurity Foundations
Modality	Online Instructor led
Dates	19-20 January 2022
Duration	2 days
Registration deadline	12 January 2022
Training fees	0 USD
Description	This training will enable the participants to understand cybersecurity foundations principles, encryption, and decryption mechanisms. Also, to differentiate between threat, vulnerability and risk in cybersecurity. Furthermore, to gain practical skills related to cyberattacks and its trends. This course also provides hands-on practice with a virtual machine and cyberattacks simulation.
Code	22OI28030ARB-E

1. LEARNING OBJECTIVES

To understand the principles of cybersecurity and to perform practical skills in simulating a phishing attack.

2. LEARNING OUTCOMES

- Knowledge of the main elements of cybersecurity and describe their importance.
- Knowledge of the trends of cyber-attacks and differentiate between the types of these cyberattacks.
- Knowledge of differentiating between threat, vulnerability and risk in cybersecurity domain.
- Skills to conduct of Demonstrate the practical steps of cyber-attacks simulation.
- Skills in Perform the steps of vulnerabilities scanning
- Skills in using virtual machine and simulating cyberattacks.

3.TARGET POPULATION

This training is providing a great value for network administrators, system administrators, security operation centre employees as well as individuals who are interested in gaining more knowledge in cybersecurity.

4.ENTRY REQUIREMENTS

There is not mandatory prerequisite course to attend this course, but the following knowledge and skills preferred.

- Have a background of computer science and IT related experience.
- Basic level experience in Linux Operating System.

5.TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Contact details
Dr. Meryem AMMI	mammi@nauss.edu.sa

6.TRAINING COURSE CONTENTS

Topic	Description
Cybersecurity Fundamentals	This topic covers the fundamentals of cybersecurity
Introduction to cyberattacks and threats	Types of cyberattacks and threats, and the difference between vulnerability, risk and threat.
Virtualization and virtual machines/Kali Linux OS	Principles of virtualization, Practical steps to install a Kali Linux virtual machine.
Simulation of a phishing attack on VM	Practical steps on simulating a phishing attack using Kali Linux VM

7.TRAINING COURSE SCHEDULE (Riyadh Time)

Day / Session	Topic	Exercises and interactions
Day 1: 19 Jan.	Cybersecurity Fundamentals Introduction to cyberattacks and threats	Case studies on how to defend cyberattacks and threats

Day 2: 20 Jan.	Virtualization and virtual machines/Kali Linux OS	Hands on simulating a phishing attack
	Simulation of a phishing attack on VM	

8.METHODOLOGY (Didactic approach)

The course will include Instructor-led presentations, case studies, group exercises and assignments.

9.EVALUATION AND GRADING

The training will be concluded with the final test with passing score of 70 percent.

10.TRAINING COURSE COORDINATION

Training Coordinator:	ITU Coordinator:
Dr. Abdulrazaq Al-Morjan Director of Centre of Excellence in Cyber Crimes and Digital Forensics, at NAUSS Mobile: +966 54 470 05 53 Email: t-aalmargan@nauss.edu.sa	**Mr. Ahmed El Raghy** Senior Advisor ITU Arab Regional Office Tel: +202 3537 1777 Mobile: +201005281908 Fax: +202 3537 1888 Email: ahmed.elraghy@itu.int