6th COMSATS-ISESCO-INIT
International Workshop on "Internet Security: Enhancing Information Exchange Safeguards"

19th to 23rd December 2016
Rabat, Morocco

Program

Day 1 – December 19, 2016 (Monday)	
TIME	**INAUGURAL CEREMONY**
08:30 – 09:00	Arrival of Guests and Registration
09:00 – 09:15	Welcome Address
09:15 – 09:30	Speech of INIT's Representative
09:30 – 09:45	Speech of ISESCO's Representative
09:45 – 10:00	Message of Executive Director COMSATS
10:00 – 10:20	Inaugural Address by Chief Guest
10:20 – 11:00	**Group Photo and Tea Break**
MODULE 1: ORGANIZATIONAL SECURITY **Instructor: Dr. Haider Abbas**	
TIME	**TECHNICAL SESSION**
11:00 – 12:30	**Session 1:** • Cyber Security: A Challenge for every Nation • How to certify your Organization: Practical Approaches to Organizational Information Security Management • ISO 27001, Information Security Management System, An International Standard
12:30– 13:30	**Lunch Break**

13:30 – 15:00	**Session 2:** • Risk Assessment – Identification, Risk Calculation Methods and Treatment Strategies, and Gap Analysis • Information Security Policy/Procedures Writing • Information Assets Identifications & Valuation
15:00 – 15:30	**Tea Break**
15:30 – 17:00	**Session 3:** Practical exercises on: • Gap Analysis • Risk Assessment & Treatment • Statement of Applicability • Internal/external Auditing • Organization's Certification Process

Day 2 – December 20, 2016 (Tuesday)	
MODULE 2 : UNDERSTANDING CYBER THREATS **Instructor: Mr. Zafar Mir**	
TIME	**TECHNICAL SESSION**
09:00 – 10:30	**Session 1: Dissecting a Cyber Attack** • Reconnaissance (Recon) • Scanning • Gaining access • Maintaining Access • Covering Tracks and Hiding
10:30 – 11:00	**Tea Break**
11:00 – 12:30	**Session 2: Distributed DoS Attacks** • Anatomy of a Sample DDoS Attack • Evolution of Botnet Configurations and DDoS Attacks • Mitigation Techniques

12:30 – 13:30	**Lunch Break**
13:30 – 15:00	**Session 3: More Advanced Attack Techniques** • The Concept of Kill Chain • Where we stand? • Layered Security Approach • Summing it up
15:00 – 15:30	**Tea Break**
15:30 – 19:00	**City Tour**

Day 3 – December 21, 2016 (Wednesday)	
MODULE 3: VULNERABILITIES ASSESSMENT (RAPID7) **Instructor: Mr. Syed Mustafa Raza**	
TIME	**TECHNICAL SESSION**
09:00 – 10:30	**Session 1: Introduction/Foundation** • Defining vulnerability, exploit, threat and risk • Creating a vulnerability report • Conducting an initial scan • Common Vulnerabilities and Exposure (CVE) list
10:30 – 11:00	**Tea Break**
11:00 – 12:30	**Session 2: Scanning and Exploits** • Vulnerability detection methods • Types of scanners • Port scanning and OS fingerprinting • Enumerating targets to test information leakage • Types of exploits: worm, spyware, backdoor, rootkits, and Denial of Service (DoS) • Deploying exploit frameworks

12:30 – 13:30	**Lunch Break**
13:30 – 15:00	**Session 3: Configuring Scanners & Generating Reports** • Implementing scanner operations and configuration • Choosing credentials, ports and dangerous tests • Creating custom vulnerability tests • Customizing Nessus scans
15:00 – 15:30	**Tea Break**
15:30 – 17:00	**Session 4: Creating and interpreting reports** • Filtering and customizing reports • Interpreting complex reports • Contrasting the results of different scanners

Day 4 – December 22, 2016 (Thursday)	
MODULE 4: ETHICAL HACKING AND MALWARE ANALYSIS **Instructor: Mr. Asad Raza**	
TIME	**TECHNICAL SESSION**
09:00 – 10:30	**Session 1:** • Security Issues in Wireless Networks • WEP Cracking • WPA Cracking • WPA2 Cracking
10:30 – 11:00	**Tea Break**
11:00 – 12:30	**Session 2:** • Enumerating open ports and services • Metasploit Framework Basics • Exploiting Windows Operating System • Privilege Escalation

12:30 – 13:30	**Lunch Break**
13:30 – 15:00	**Session 3:** • Bypassing Antivirus • Hacking Android Mobile Phone • Capturing insure passwords (http) • Capturing security passwords (https)
15:00 – 15:30	**Tea Break**
15:30 – 17:00	**Session 4:** • SQL Injection & Cross-site Scripting • Malware Analysis Tools and Techniques • Viper Malware Analysis Frame Work • Automating Malware Analysis

Day 5 – December 23, 2016 (Friday)	
MODULE 5: DIGITAL FORENSICS **Instructor: Mr. Muhammad Faheem Qureshi**	
TIME	**TECHNICAL SESSION**
09:00 – 10:30	**Session 1** • Introduction to Forensic Science • Evidence Handling • Roles and Responsibilities
10:30 – 11:00	**Tea Break**
11:00 – 12:30	**Session 2** • Phases of a Digital Forensic Process
12:30 – 14:30	**Prayers & Lunch Break**

14:30 – 16:00	**Session 3** • Memory Forensics • Storage Forensics • Microsoft Windows Forensics
16:00– 16:30	**Tea Break**

Day 5 – December 23, 2016 (Friday)	
TIME	**CLOSING CEREMONY**
16:30 – 16:40	Concluding Remarks
16:40 – 16:50	Vote of Thanks
16:50 – 17:00	Certificate Distribution