

# PROGRAM

---

## 5 – Day International Training Workshop on Internet Security: Enhancing Information Exchange Safeguards December 19 – 23, 2017 Almaty, Republic of Kazakhstan

---

Day 1 – December 19, 2016 (Monday)

---

### TIME

### INAUGURAL CEREMONY

---

08:30 – 09:00	Arrival of Guests and Registration
09:00 – 09:15	Welcome Address by KazNU's Representative
09:15 – 09:30	Speech of INIT's Representative
09:30 – 09:45	Speech of ISESCO's Representative
09:45 – 10:00	Speech of COMSATS' Representative
10:00 – 10:20	Inaugural Address by Chief Guest
<b>10:20 – 11:00</b>	<b>Group Photo and Tea Break</b>

---

### MODULE 1: ORGANIZATIONAL SECURITY

Instructor: Dr. Haider Abbas

---

### TIME

### TECHNICAL SESSION

---

11:00 – 12:30	<b>Session 1:</b> <ul style="list-style-type: none"><li>• Cyber Security: A Challenge for every Nation</li><li>• How to certify your Organization: Practical Approaches to Organizational Information Security Management</li><li>• Cloud Computing Security</li></ul>
<b>12:30– 13:30</b>	<b>Lunch Break</b>
13:30 – 15:00	<b>Session 2:</b> <ul style="list-style-type: none"><li>• ISO 27001, Information Security Management System, An International Standard</li><li>• Risk Assessment –Identification, Risk Calculation Methods and Treatment strategies, Gap Analysis</li></ul>
<b>15:00 – 15:30</b>	<b>Tea Break</b>
15:30 – 17:00	<b>Session 3:</b>

---

Practical exercises on:

- Information Security Policy/Procedures Writing
- Information Assets Identifications & Valuation
- Gap Analysis
- Statement of Applicability
- Risk Assessment & Treatment Auditing and Certification Process

---

**Day 2 – December 20, 2017 (Wednesday)**

---

**MODULE 2: UNDERSTANDING DIGITAL FORENSICS AND HANDS ON MBR/MFT**

**Instructor: Mr. M WASEEM IQBAL**

---

<b>TIME</b>	<b>TECHNICAL SESSION</b>
09:00 – 10:30	<b>Session 1:</b> <ul style="list-style-type: none"><li>• Understanding Computer Forensics</li><li>• Data Acquisition</li></ul>
<b>10:30 – 11:00</b>	<b>Tea Break</b>
11:00 – 12:30	<b>Session 2:</b> <ul style="list-style-type: none"><li>• Working with Master Boot Record- MBR/VBR/Partition Tables</li></ul>
<b>12:30 – 13:30</b>	<b>Lunch Break</b>
13:30 – 15:00	<b>Session 3:</b> <ul style="list-style-type: none"><li>• Working with Master File Tables –MFT</li><li>• (Scenarios/ Experimentation)</li></ul>
<b>15:00 – 15:30</b>	<b>Tea Break</b>
15:30 – 19:00	<b>Session 4:</b> <ul style="list-style-type: none"><li>• Working with Master File Tables –MFT</li><li>• (Scenarios/ Experimentation)</li></ul>

---

---

**Day 3 – December 21, 2017 (Thursday)**

---

**MODULE 3: ETHICAL HACKING**

**Instructor: Mr. Asad Raza**

---

<b>TIME</b>	<b>TECHNICAL SESSION</b>
09:00 – 10:30	<b>Session 1 Wireless Hacking and Countermeasures</b> <ul style="list-style-type: none"><li>• Security Issues in Wireless Networks</li><li>• WEP Cracking</li><li>• WPA Cracking</li><li>• WPA2 Cracking</li><li>• Counter measures t</li></ul>
<b>10:30 – 11:00</b>	<b>Tea Break</b>
11:00 – 12:30	<b>Session 2: Reconnaissance &amp; Scanning</b> <ul style="list-style-type: none"><li>• Scanning using NMAP</li><li>• Enumerating open ports and services</li><li>• Nessus Vulnerability Scanner</li></ul>
<b>12:30 – 13:30</b>	<b>Lunch Break</b>
13:30 – 15:00	<b>Session 3: Gaining Access &amp; Privilege Escalatio</b> <ul style="list-style-type: none"><li>• Introduction to Metasploit Framework</li><li>• Exploiting Windows 7, 8 and 10</li><li>• Antivirus bypass</li><li>• Privilege Escalation</li></ul>

---

---

**15:00 – 15:30**

**Tea Break**

---

15:30 – 17:00

**Session 4: Password Attacks & Social Engineering**

- Intercepting http and https passwords
  - Dictionary Attacks vs Rainbow tables
  - Social Engineering toolkit
- 

**Day 4 – December 22, 2016 (Friday)**

---

**MODULE 4: Digital Forensics and Incident Response**

**Instructor: Mr. Muhammad Faheem Qureshi**

---

**TIME**

**TECHNICAL SESSION**

---

09:00 – 10:30

**Session 1:**

- Role of Incident Handling and Response
  - The Process of IR and its components
- 

**10:30 – 11:00**

**Tea Break**

---

11:00 – 12:30

**Session 2:**

- Introduction to Digital Forensics
  - Phases of Digital Forensics
- 

**12:30 – 14:30**

**Friday Prayer & Lunch Break**

---

14:30 – 15:30

**Session 3:**

- Storage Forensics Lab
  - Memory Forensics Lab
  - OS Forensics Lab
- 

**15:30 – 16:00**

**Tea Break**

---

16:00 – 17:00

**Session 4:**

- Mobile Forensics Lab
  - Incident Response La
- 

**Day 5 – December 23, 2016 (Saturday)**

---

**MODULE 5: 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 – 14:30

**Prayers & Lunch Break**

---

14:30 – 16:00

**Session 3 More Advanced Attack Techniques**

- The Concept of Kill Chain
- Where we stand?
- Layered Security Approach
- Summing it up

---

16:00– 16:30

**Tea Break**

---

**Day 5 – December 23, 2016 (Saturday)**

---

**TIME**

**CLOSING CEREMONY**

16:30 – 16:40

Concluding Remarks

16:40 – 16:50

Vote of Thanks

16:50 – 17:00

Certificate Distribution

---