|  |  |  |
| --- | --- | --- |
|  |  | **mict_logo** |

**Annex 1**

**TRAINING OUTLINE**

|  |
| --- |
| **ITU CENTRES OF EXCELLENCE NETWORK FOR ASIA PACIFIC REGION**  **Internet and IPv6 Infrastructure Security Program**  **23 – 27 May 2016, Nonthaburi, Thailand**  **Supported by**  **AcademyJPG** |

**COURSE DESCRIPTION**

|  |  |
| --- | --- |
| Title | **Internet and IPv6 Infrastructure Security Programme** |
| Method of delivery | Face-to-face |
| Objectives | * To build knowledge of policy makers, regulators, telecom operators, and enterprise network administrators on deployment and management of Internet and IPv6 network infrastructure. * To provide information on Internet infrastructure security, particularly focusing on similarities and differences between IPv4 and IPv6 when it comes to network infrastructure security. * To build skills on how to mitigate IPv6 Internet infrastructure security threat with demonstration of network configurations, and some hands-on exercises. |
| Dates | 23 – 27 May 2016 |
| Duration | Five days |
| Registration deadline | 16 May 2016 |
| Training fees | Free with support from Ministry of ICT (Thailand) and APNIC |
| Course code | **16WS17077ASP-E** |

**LEARNING OUTCOMES**

Upon completion of this training, participants will be able to

* Understand Internet Infrastructure, IPv6 protocol and the required conditions for deployment of IPv6. They will also comprehend the issues related to Internet infrastructure security, threats, vulnerability and mitigation methods. The course will also focus on the similarities and differences in terms of issues related to IPv4 and IPv6 infrastructure security.
* Acquire skills for managing IPv6 Internet infrastructure security threat, methods for network monitoring and configurations.

**TARGET POPULATION**

Network engineers and technical staff from policy makers, regulators, telecom operators, and enterprise network administrators responsible for deployment and management of Internet and IPv6 infrastructure networks.

**FACILITATOR/EXPERTS**

The experts for the training include Dr. Philip Smith, Mr. Dean Pemberton, Ms. Miwa Fujii (APNIC) and Mr. Ashish Narayan (ITU).

**EVALUATION**

The assessment of the participants shall be based on the - time spent on the training and the following parameters:

|  |  |
| --- | --- |
| Evaluation Parameter | Weightage ( in %) |
| Quizzes and presentations | 60 % |
| Attendance | 10 % |
| Participation | 30 % |

The minimum passing requirement for certificate is 60%.

**DRAFT TRAINING SCHEDULE AND CONTENTS / AGENDA**

**(Updated information will be available at** [**http://www.itu.int/itu-d/asp**](http://www.itu.int/itu-d/asp)**)**

|  |
| --- |
| DRAFT AGENDA |
|  |
| **23 May 2016 (Day-1)** |

|  |  |
| --- | --- |
| 0800-0900 | **REGISTRATION** |
| 0900-0930 | **Opening Session:**  Welcome Address   * ITU * APNIC   Opening Address   * MICT (Thailand) |
| 0930 - 1000 | **Session 1: Where are we now: IPv6 deployment update**  Objective: To provide an overview of IPv6, the need for migration and the current IPv6 deployment status in the world, and technical trend. |
| 1000 - 1030 | **Session 2:  Recap – Internet fundamentals**  Objective: To recap fundamental technical information on the Internet Infrastructure |
| 1030-11:00 | **COFFEE BREAK** |
| 1100-1230 | **Session 3: Recap – IPv6 Protocol**  Objective: To recap fundamental technical information about IPv6, introduction to the protocol and the relevant standards. |
| 1230-1400 | **LUNCH BREAK** |
| 1400-1530 | **Session 4: Recap - About IPv6 Addresses**  Objective: To explain IPv6 addressing, how it works, the differences from IPv4, and introduce how a well designed address plan can assist with network security and integrity planning. |
| 1530-1600 | **COFFEE BREAK** |
| 1600-1700 | **Session 5: Roles of ICT Policy maker and regulator in Internet and IPv6 Security** Objective: To develop an understanding of what role the ICT policy maker and regulator should play to promote Internet security in general and IPv6 infrastructure security in particular. |
| 1700-1730 | Quiz 1 |

|  |
| --- |
| 24 May 2016 (Day-2) |

|  |  |
| --- | --- |
| 0900-1030 | **Session 6: Internet Infrastructure Security Introduction**  Objective: Introduction to the main network security issues that infrastructure operators need to be aware of. This includes discussion on packet flooding, Internet worms, DDOS attacks and Botnets |
| 1030-1100 | COFEE BREAK |
| 1100-1230 | **Session 7: IPv6 Security Introduction**  Objective: Introduction to the similarities and differences between IPv4 and IPv6 when it comes to network infrastructure security. This includes discussion about ICMPv6, multicast, extension headers, fragmentation headers, and reconnaissance on IPv6 networks. |
| 1230-1400 | LUNCH BREAK |
| 1400-1530 | **Session 8: Demonstration: Deploying IPv4 and IPv6 Dual Stack network**  Objective: Constructing IPv4 and IPv6 dual stack router based network infrastructure, which will be used for other hands-on workshops to practice implementation of the Internet infrastructure security measures. |
| 1530-1600 | COFEE BREAK |
| 1600-1730 | **Session 9: IPv6 Internet Security: Theory and Practice**  Objective: Introduction to protecting IPv6 networks. This includes explanation on Ingress and Egress filtering, demonstration on filtering IPv6 traffic, and filtering on allocated addressing and bogon addresses. |
|  |  |

|  |
| --- |
| 25 May 2016 (Day-3) |

|  |  |
| --- | --- |
| 0900-1030 | **Session 10: IPv6 Transition Technologies**  Objective: To recap the currently deployed IPv6 transition technologies, analyzing their advantages and disadvantages. |
| 1030-1100 | COFEE BREAK |
| 1100-1230 | **Session 11: Securing the transition mechanisms**  Objective: To look at each transition technology presented during the previous session and discuss techniques around securing them, their advantages and disadvantages as far as security is concerned, and the security implications while transiting to IPv6. |
| 1230-1400 | LUNCH BREAK |
| 1400-1530 | **Session 12: Demonstration:** **Hardening IPv6 network devices**  Objective: To review issues concerning network devices and the threats that target the network infrastructure, and to learn services that should be disabled on a router to avoid vulnerabilities. Topics such as disabling unnecessary services, IPv6 device management, threats against interior routing protocol, Access Control Lists (ACLs) Best Current Practice (BCP) and Quality of Service (QoS) threats will be included. |
| 1530-1600 | COFEE BREAK |
| 1600-1730 | **Session 13: Securing BGP Sessions**  Objective: Introduction to BGP threats including BGP Route Manipulation, BGP Route Hijacking, BGP Denial of Service (DoS), and demonstration on router configuration on IPv4 and IPv6 networks. |
|  |  |

|  |
| --- |
| 26 May 2016 (Day-4) |

|  |  |
| --- | --- |
| 0900-1030 | **Session 14: IPSec and SSL Virtual Private Networks**  Objective: To review encryption technologies such as IPsec and Secure Socket Layer (SSL) that can be used to protect Virtual Private Networks (VPN). Host to Host IPsec communication and Site to Site IPsec VPN will be reviewed along with multipoint IPsec VPN examples. |
| 1030-1100 | COFEE BREAK |
| 1100-1230 | **Session 15: IPv6 Firewalls**  Objective: To review mechanism of IPv6 Firewall, how to filter IPv6 unallocated address spaces, firewalls and Ipv6 headers, firewall and NAT etc. |
| 1230-1400 | LUNCH BREAK |
| 1400-1530 | **Session 16: Demo/Lab**  IPsec, SSL Virtual Private networks configuration examples. |
| 1530-1600 | COFEE BREAK |
| 1600-1730 | **Session 17: Demo/Lab**  IPv6 firewall configuration examples |
| 1700-1730 | Quiz 2 |

|  |
| --- |
| 27 May 2016 (Day-5) |

|  |  |
| --- | --- |
| 0900-1030 | **Session 18: Security monitoring**  Objective: To review tools and techniques to monitor IPv6 networks. To learn monitoring of tunnels and performing forensics of possible IPv6 security events through reviewing configuration and testing of IPv6 intrusion prevention systems. |
| 1030-1100 | COFEE BREAK |
| 1100-1230 | **Session 19: Working Group exercise**  Objective: To summarize learning of the workshop capturing important element of learning that can be used to inform your colleagues who could not participate in this workshop.  Participants will present their choices of router configurations that they applied to mitigate security vulnerabilities and logic behind of such implementation. Each team will be asked to present it in a 10 minute presentation. |
| 1230-1400 | LUNCH BREAK |
| 1400-1530 | **Session 20: Presentation by participants + evaluation**  Objective: To present the learning in front of other participants and instructors. There will be a short QA session at the end of presentation. |
| 1530-1600 | Summary and closing |

**METHODOLOGY**

The face-to-face programs will include

* + Instructor-led presentations,
  + Case studies,
  + Group exercises

**TRAINING COORDINATION**

|  |
| --- |
| **ITU coordinator:**  Mr. Ashish Narayan,  Program Co-ordinator, ITU Regional Office for Asia & the Pacific, 5th Floor, Thailand Post Training Centre,111Moo3 Chaengwattana Road, Laksi Bankok 10210,Thailand  Tel: +66 257 500 55, FAX: +66 257 535 07  Email: [ashish.narayan@itu.int](mailto:ashish.narayan@itu.int)  Ministry of ICT (Thailand) coordinator:  Mrs. Sudaporn Vimolseth, Vice President, TOT Academy  Tel: +66 2580 1076, Fax: +66 2591 8087  Email: [sudaporv@tot.co.th](mailto:sudaporv@tot.co.th) |

**REGISTRATION**

**Registration on ITU Academy Portal**

Application to participate in this course should be made at "https://academy.itu.int” by following the steps:

**Skip STEP 1,** *if you already have a username and password*

**Step 1:** Create a new account in the ITU Academy portal at <https://academy.itu.int/index.php?option=com_hikashop&view=user&layout=form&Itemid=559&lang=en>. After completing the registration form, a message will be sent to your e-mail address inviting you to log in to the platform.

**Step 2:** Once you are logged in, you can search for the course in the training catalogue or directly proceed to the course link: <https://academy.itu.int/index.php?option=com_joomdle&view=coursecategoryextended&cat_id=:&course_id=991:internet-and-ipv6-infrastructure-security&Itemid=478&lang=en>

**Step 3: Click on “Enroll me into this course” and type in the following enrolment key: 16WS17077ASP-E. You will then be able to access the course page.**

*Please note that online registration should be done* ***before 16 May 2016****.*