International Telecommunication Union

International Telecommunication Union

ITU Africa Regional Cyberdrill

Hosted By

Uganda Communications Commission

18th – 21st November 2019 in Kampala, Uganda

Day 1 and 2: Training

Training Track I : Developing Cyber Threat Intelligence Capabilities

Description: Many organizations follow a defensive approach to security, revolving around the deployment of protection security controls with a varying degree of monitoring capabilities. This course covers how organizations can use Cyber Threat Intelligence to proactively identify threats and actionable information in order to better prepare against future attacks while at the same time minimizing the impact of ongoing ones. This course addresses the wide range of CTI standards, technologies and services and how they can be chosen and used effectively, based on the organizational context, maturity and specific needs of the organization.

Audience: CSIRT/CERT members, Incident Responders, SOC Analysts, security consultants.

Course level: Intermediate

Pre-requisites: The course is hands-on and a laptop is required to be able to work through all the practical hands-on

workshops. The minimum laptop requirements are:

x86-compatible 1.5 GHz minimum or higher , 4GB RAM minimum or higher, 20GB available hard drive space, capable of installing virtualization software

Monday 18 November 2019

[09:00 – 9:30]	Registration
[09:30– 10:00]	Defending Cyber threat intelligence
[10:00 – 10:30]	Coffee Break
[10:30 – 12:00]	Threat indicators The Kill chain
[12:00 – 13:30]	Lunch Break
[13:30 – 15:00]	The diamond model of intrusion analysis Mapping attacks to the kill chain
[15:00 – 15:30]	Coffee Break
[15:30 – 17:00]	Analyzing campaign and threat actors Using CTI to improve defense, monitoring and response

Tuesday 19 November 2019

[09:00 – 9:30]	Registration
[09:30– 10:00]	Leveraging SIEM and LOG management solutions to develop internal CTI
[10:00 – 10:30]	Coffee Break
[10:30 – 12:00]	Developing CTI capabilities
[12:00 – 13:30]	Lunch Break
[13:30 – 15:00]	Choosing CTI platforms, providers and services
[15:00 – 15:30]	Coffee Break
[15:30 – 17:00]	Sources of CTI and Sharing CTI

Training Track II : Reverse Engineering Introduction course

Description: At the beginning an introduction to the course is made, setting common terminology and describing different analysis methods. Second and the biggest part of the training is an introduction to the assembly language. This course will introduce concepts, tools, and techniques used for binary code execution.. However, it would be beneficial for trainees to have a prior knowledge of the x86 assembly language. The later part of the training introduces a number of tools commonly used for the advanced artefact analysis. Two of them, the IDA Pro Free edition3 for static and OllyDbg4 for dynamic analyses, will be used extensively during the rest of the course Mobile Incident Handling. The students will familiarize themselves with the risks found on Mobile platforms and also ways of identifying and mitigating such risks.

Audience: CERT staff involved in the process of incident handling, especially those responsible for detection of new threats related directly to the CERT customers

Course level: Intermediate

Pre-requisites: The course is hands-on and a laptop is required to be able to work through all the practical hands-on

workshops. The minimum laptop requirements are:

x86-compatible 1.5 GHz minimum or higher , 4GB RAM minimum or higher, 20GB available hard drive space, capable of installing virtualization software

Monday 18 November 2019

[09:00 – 9:30]	Registration
[09:30– 10:00]	Introduction to the training
[10:00 – 10:30]	Coffee Break
[10:30 – 12:00]	Intel x86 family of processors, along with a description of the binary code execution, processor internals and system calls
[12:00 – 13:30]	Lunch Break
[13:30 – 15:00]	The analysis process rather than learning assembly instructions
[15:00 – 15:30]	Coffee Break
[15:30 – 17:00]	Familiarization with Android, AVD, and ADB

Tuesday 19 November 2019

[09:00 – 9:30]	Registration
[09:30– 10:00]	Cloning an Application
[10:00 – 10:30]	Coffee Break
[10:30 – 12:00]	Analyzing Cloned Application
[12:00 – 13:30]	Lunch Break
[13:30 – 15:00]	Analyzing Simple locker
[15:00 – 15:30]	Coffee Break
[15:30 – 17:00]	Analyzing Other traces

Day 3 and 4 : Cyber Exercises

Wednesday 18 November 2019

[09:00 – 09:30]	Team creation, registering team accounts to Cyber Range
[09:30– 11:00]	**Scenario 1** Mr. Marwan Ben Rached, Technical Officer Cybersecurity, **ITU**
[11:00 – 11:30]	Coffee Break
[11:30 – 13:00]	**Scenario 1** Mr. Marwan Ben Rached, Technical Officer Cybersecurity, **ITU**
[13:00 – 14:00]	Lunch Break
[14:30 – 15:30]	**Scenario 2** Dr. Almerindo Graziano, CEO, **Silsensec**
[15:30 – 16:00]	Coffee Break
[16:00 – 17:30]	**Scenario 2** Dr. Almerindo Graziano, CEO, **Silsensec**

Thursday 25 September 2019

[9:00– 10:30]	**Scenario 3** Dr. Emad Eldin Helmy Khalil, **FIRST**
[10:30 – 11:00]	Coffee Break
[11:00 – 12:30]	**Scenario 3** Dr. Emad Eldin Helmy Khalil, **FIRST**
[12:30 – 13:30]	Lunch Break
[13:30 – 15:00]	**Scenario 4** **AfricaCERT**
[15:00 – 15:15]	Coffee Break
[15:15 – 17:00]	**Scenario 4** **AfricaCERT**