Meeting Report.

AfricaCERT 12: Nairobi, Kenya

21 au 27 Mai 2017

BACKGROUND

AfricaCERT organizes two annual meetings per year. The meetings provide the opportunity for stakeholders mainly response team and security practioners to meet, attend training events and to discuss challenges related to the cyber readiness of the African Continent. On May 21-27, AfricaCERT 12 was held in Nairobi, Kenya during the *Africa Internet Summit* (*AIS*) (1). The theme of the AfricaCERT 12 meeting was: "Internet Security and vulnerability disclosure". AfricaCERT 12 proivded the opportunity to test new meeting format with more engagement of members. AfricaCERT thanks the « Organisation Internationale de la Francophonie (OIF) », The African Network Operator Group (AfNOG), the Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC), the Agence Nationale de la Sécurité des Systèmes d 'Information (ANSSI), the International Telecommunication Union (ITU), The Forum of Incident Response and Security Teams for their continuous support. AfricaCERT also recognizes and thanks it executive committee and members in particular the Tunisian Computer Emergency Response Team (TunCERT) and the Egyptian National Computer Emergency Response Team EG-CERT for making AfricaCERT 12 a great event.

I. Schedule.

AfricaCERT 12 held the following events:

- One day of boot camp
- Four days of training
- Two days of meetings on Challenge and strategic planning for AfricaCERT.

May 21, 2017	Bootcamp. (AFRICACERT)	
May 22, 2017	CSIRT Creation and MGT (FIRST/AFRICACERT)	
May 23, 2017	CSIRT Creation and MGT (FIRST/AFRICACERT)	
May 24, 2017	CSIRT Exercices (ANSSI)	Pratical Incident Handling (JPCERT/AFRICACERT)

May 25, 2017	CSIRT Security Architecture, Intelligence Feed with Open Source • CSRIT Security Architecture with Open Source, hands-on (AfricaCERT/TunCERT) • Understanding and effectively processing threat reports (Shadow Server)	Log Analysis (JPCERT/AFRICACERT)
May 26, 2017	CSIRT Day. Meeting with CSIRTs	
May 27, 2017	AfricaCERT Strategic meeting: 5 years review and strategic plan	

1. **Bootcamp (May 21, 2017).**

The bootcamp was aimed to prepare the participants for the week:

- for those who already know the topics of the training, it will be a session of refreshing their knowledge, while they are given an opportunity to assist other learners. For those who are discovering, they will enter a new world of another way of doing things they may have already being doing otherwise.
- new recruits: all participants come with some experience and hence some knowledge of the topics of the AfricaCERT workshop. For the sake of the success of the workshop, it is compulsory to make sure there is a common ground understanding and that both participants and facilitators share some common languages.
- Setting up virtual machines

2. FIRST CSIRT Basic Course (2 Days)

The goal of the basic course is to give an introduction into the operation of a CSIRT. It consists of the following six modules:

- CSIRT Fundamentals
- Starting with a CSIRT
- CSIRT Operation

- Working with Information Sources
- Incident Coordination
- CSIRT Performance Measurement

3. JPCERT Course

The Course delivered by JPCERT comprises of several modules organized around Pratical Incident Handling and Log analysis:

- Basic tools for Incident handling
- APT Incident Response
- APT incidents and Stix
- APT Log analysis hands-on

4. CSIRT Exercices (Marcus please complete).

5. CSIRT Security Architecture with Open Source.

Delivered by TunCERT, the course was organized around the potentialities offered by open source security tools in establishing a strong security architecture for their infrastructure, for managing their activities, and for deploying their forensics activities using some open-source security tools.

6. Understanding and effectively processing threat reports.

The training was aimed to give participants an understanding of the types of network security threat feed information that is freely available to CERTs, Network Providers and LEA, and how they can be used for victim remediation. It was based on Shadowserver malicious activity reports and scan data. The full victim remediation chain - end-to-end processing of information from data producers like Shadowserver to CERTs, ISPs and end-users – was demonstrated along with typical barriers that can be encountered for successful remediation.

6. CSIRT Day. Meeting with CSIRTs

The meeting was organized with the support of The *National Kenya* Computer *Incident Response* Team Coordination Center (*National* KE-*CIRT*/CC)

II. Improvements

AfricaCERT 12 brought several improvements.

- The organization of a bootcamp to prepare participants. Over the years, a skills gap has been noticed; affecting the delivery of the courses.
- Members training members. One of the success of AfricaCERT 12 was having TunCERT training other participants, enhancing the sense of community building around AfricaCERT.
- Organization of a CSIRT Day. The CISRT day gave the opportunity to the CISRTS participating at the meeting to network with the others and exchange experience on operations challenges.
- Post-event meeting

A post event meeting has been organized between ANSSSI, JPCERT and AfricaCERT to discuss the lessons learned from the event and for a better preparation for future events. It has been outlined that:

- AfricaCERT should start events preparation in advance in order to meet the challenges related to the preparation of the events ;
- AfricaCERT has made progress compared to previous events

III. Participants and Countries

AfricaCERT 12 has attracted 56 participants from 19 countries.

IV. Finances

AfricaCERT 12 was possible with the financial contribution of the organizations below.

Year	2017
AfNOG	$32500
OIF	$26300
Iservices Systems	$1700

V. Survey

1. AfNOG / AfricaCERT survey

	Excellent	Very good	Good	Fair	Poor
Quality of teaching materials	78%	13%	9%		
Quality of the presentations	76%	14%	10%		
Quality of the lab exercises	63%	20%	17%		
Quality of the working environment	75%	25%			
Meals and coffee breaks	70%	18%	12%		

Other Comments

- Majority requested for more practical rather than theory as done currently.
- Some also suggested Instructors should be better versed in the language of Instruction.

2. Outline of FIRST's Survey (Attached).