AfricaCERT

United Teams promoting Cybersecurity in Africa

AFTER EVENT REPORT: INCIDENT RESPONSE WORKSHOP AND CSIRT INTRODUCTION

- AFRINIC 13 -

LUANDA - ANGOLA

2nd DECEMBER 2019

Submitted by Choolwe Nalubamba.

TABLE OF CONTENTS

1. BACKGROUND

AfricaCERT conducts every year during the AfriNIC Policy Meeting training activities to engage the AfriNIC community, policy makers and security professionals, including members of incident response teams. This is a report following the introductory workshop on Computer Security Incident Response Teams and the associated functions delivered at the AFRINIC-31 meeting that was held in Luanda-Angola from the 2nd to the 6th of December 2019.

2. AfricaCERT RESOURCE PERSON(s)

MR. CHOOLWE NALUBAMBA **ZAMBIA**

3. SUMMARY OF THE PRESENTATION

The workshop/training was comprised of a participatory presentation complemented with exercises (section 4) given to the class. The workshop basically looked at the challenges that the Internet Service Providers and their infrastructure confront when dealing with Cybersecurity incidents; and also examined strategies that can be employed to build Incident Response Capabilities even with limited financial resources.

The presentation was broken up into eight parts:

i. **Cybersecurity:** This section gave a comprehensive definition of what Cybersecurity is, and the associated tenets.

ii. **Threat Intelligence:** This section looked at the factors that determine what a threat is, and what the threat landscape looks like.

iii. **Improving your Security Posture:** Several actionable steps that can be taken now to improve individual and organisational cybersecurity posture were shared in this section.

iv. **Log Analysis:** This part was a quick tutorial on the typical and common log formats, and their subsequent analysis using open source tools readily available.

v. **Incident Response:** This section started by defining what an Incident is, and moved on to explain what Incident Response is and the processes that constitute it. Example incidents were also shared.

vi. **Introduction to CSIRT:** Following the previous section; this part introduced the genesis of CERTs and went forward to list some of the basic requirements of setting up a CSIRT in a cost-effective and efficient manner. The principles from the ITU and FIRST Service framework formed the basis of this section. SIM3 (Security Incident Management Maturity Model) used in the CSIRT community to indicate how well a team governs, documents, performs and measures their function was also introduced.

vii. **A Brief on Risk Assessment:** This part basically highlighted the purpose of risk assessment, and the need to undertake it on an ongoing basis.

viii. **Network Forensics 101 – For First Responders:** Finally, this section brought together the pieces and delved into Network forensics a little, culminating into a very exciting forensic exercise.

4. EXERCISES – SILENSEC's CYBERRANGE

In order to reinforce some of the concepts that were delivered; exercises were delivered to the participants using Silensec's Cyberrange – a platform currently being used a lot by the ITU in conducting Cyber drills around the world.

4.1 LOG ANALYSIS

This exercise allowed the participants to role-play as a dedicated team of analysts looking at logs from a webserver after a compromise. The participants were expected to rely heavily on Linux command line tools during this exercise.

4.2 NETWORK FORENSICS

The second exercise also allowed the participants to play the role of forensic experts responding to an Incident where a suspect is alleged to have fled the country. The Participants were expected to use Wireshark in answering eight simple questions.

5. RECOMMENDATIONS

These are the few recommendations for AfricaCERT following a successful training event at the AFRINIC-31 meeting held in Luanda:

i. More of such workshops should be held at AFRINIC events. The time should however be increased in order to deliver better quality content.

ii. AfricaCERT should begin to host such continent-wide events.

iii. Conduct outreach programmes through established Regional/International organizations such as SADC, COMESA, ECOWAS, ISOC, and the AU.

iv. Build training programs that can be offered online if possible.

v. Establish a cybergym; to be by AfricaCERT members for red-team/blue-team training simulations.

vi. Build Cyber-threat-intelligence capabilities and offer this service to members.

6. CONCLUSION

This training workshop was such a wonderful and enlightening experience. AFRINIC was appreciative of the support received from AfricaCERT by agreeing to conduct this workshop.