MUST IUC- Sub-Project 6 Cybersecurity Training
at
Mbarara University of Science and Technology

Facilitators: Gunther Van Landeghem & Liesbeth Kenens
Thomas Moore University of Applied Sciences

11th - 14 April 2023

Introduction

Sub-Project 6 of the “University as a Facilitator to Community Based Sustainable Solutions to Demographic Challenges in South Western Uganda (UCOBS)” project seeks to improve Institutional and Community ICT Capacity to Access and Utilize Information.

This is set to be achieved through investment in the university’s ICT infrastructure and technical capacity.

Coninuous utilization and reliance of communication technologies has opened the world to a new threat to crime/unauthorized attacks that take advantages of vulnerabilities and gaps created by this use of technology to share information and resources.

It’s in this spirit that a one- week Cybersecurity Training workshop was held at Mbarara University of Science and Technology between the 11th and 14th April 2023.

The general objective of the training was to generally improve the university’s readiness to avert cyber-attacks as it seeks to rely more on ICTs for its core functions of teaching, learning, research, community engagement and administration.

Cybersecurity being a continuous effort, the training workshop specifically aimed at;

i. Creating awareness and orientation on existing cyber-attack and security trends
ii. Providing an overview of available tools and technologies to avert cyber attacks
iii. Providing a springboard to the development of Cyber Security Strategy for Mbarara University of Science and Technology

Participants to the training were mainly technical staff from the university’s Computing Services and academic staff from the Faculty of Computing and Informatics.

Participants

#	Name	Faculty/Department/ Unit	Role
1	Dr. Fred Kaggwa	Faculty of Computing & Informatics	Project 6 Team Lead
2	Amos Baryashaba	Computing Services	Head, Computing Services
3	Lasto Mubiru	Computing Services	Systems/Network Admin
4	Owen Muhangi	Computing Services	Web Admin
5	Peter Bambanza	Computing Services	Computer Technician
6	Martin Kijumi	University Library	Computer Technician
7	Kelly Tumwine	Faculty of Applied Sciences & Technology	Sen. Computer Technician
8	Walter Okello	Faculty of Computing & Informatics	Lecturer
9	Richard Ntwari	Faculty of Computing & Informatics	Lecturer
10	Ambrose Atuhaire	Faculty of Computing & Informatics	Assistant Lecturer
11	Aggrey Obbo	Faculty of Computing & Informatics	Lecturer

Training Content

1.0 Threat Actors and Defenders: orientation in cybersecurity, frameworks as a guide.
- 1.1 Anatomy of IoT Attack
- 1.2 Attack Life Cycle
- 1.3 CIANA
- 1.4 Fujitsu
- 1.5 Cybersecurity domains
- 1.6 Cybersecurity certificates
- 1.7 The Cybership SOC
- 1.8 Responsible Disclosure & Bug Bounty

2.0 Operating System Hardening
- 2.1 Linux Hardening
- 2.2 Windows Hardening
- 2.3 Passwords and Password managers
- 2.4 STIGs and SCAP
- 2.5 Host Firewall

3.0 Network Security Fundamentals Part 1
- 3.1 Social Engineering
- 3.2 OSINT
- 3.3 Awareness
- 3.4 The Dark Web

4.0 Network Security Fundamentals Part 2
- 4.1 Active RECON
- 4.2 PCAP and Wireshark
- 4.3 Wireshark & nmap

5.0 Threats and Attacks
- 5.1 Examination of an attack
- 5.2 IoC

6.0 Network Defense
- 6.1 Metasploit
- 6.2 Risk management

7.0 Endpoint Protection
- 7.1 HIDS-EDR-XDR
- 7.2 SIEM
- 7.3 Wazuh

8.0 Threat Intel
- 8.1 Zero trust & policies
- 8.2 NIST framework
- 8.3 Threat Intel document & Platforms

The training sessions were delivered through presentations, scenarios, videos, interactions and practical exercises

Challenges

The following emerged as challenges categorized as the training workshop challenges and MUST Cybersecurity challenges

Training Workshop Challenges

i. The time available for the training workshop was not adequate for the rich content planned and provided
ii. The requisite infrastructure to set up and test technologies and tools has not yet been procured

MUST Cybersecurity Challenges

i. The number of technical staff is inadequate for cybersecurity role(s) to be assigned
ii. The skills technical capacity of the university was found to be wanting
iii. The basic infrastructure to implement cybersecurity technologies and tools is inadequate

Recommendations

i. That MUST kickstarts its Cybersecurity readiness plans with the implementation of WAZUH, a SIEM solution through Lander Wuyts student internship program
ii. Initial procurement of server and firewall infrastructure for MUST
iii. Initialization of Security Policy framework for MUST
iv. That the Cybersecurity trainings and capacity building program with the Flemish partners be continuous