Cyber Security & Malware Analytics

(For participants from Tanzania)

Duration: 3 weeks (31.1.2024 – 20.2.2024)

Course Content

1) Introduction to Computer Networks & Linux

- Introduction to Networking with Lab
- OSI Model, TCP/IP Headers, IP Protocol and Addressing
- Basic Network Devices & Their functionality
- Routing process and Routing tables with Lab, Access Control lists
- System Administration tools
- Linux Fundamentals and Commands, iptables
- Network Designing, Configuring and Administration

2) Cyber Security Attacks

- Cyber Security Overview
- Introduction to Cyber Attacks
- Impact of Cyber Attacks
- Types of Cyber Attacks
  - Layer-2 Threats: MITM, ARP Poising, Spoofing etc.
  - Malwares
  - Password Attacks
  - DDoS Attacks (Distributed Denial of Service Attacks)
  - Pop-Ups
  - Software Updates
  - Public Unsecured Wi-Fi Network Attacks
  - Phishing Scams
  - Man-in-Middle Attacks
  - Eavesdropping
  - Social Engineering
- Application Security Attacks
  - Injection (SQL Injection)
  - Broken Authentication and session management
  - Cross Site Scripting
  - Broken Access Control
  - Security Misconfigurations
  - Cross Site Request Forgery (CSRF)
- Cyber Security Methods
  - Perimeter Security Fundamentals
  - Network Monitoring
  - PCAP (Packet) Capturing
  - Antivirus and Firewalls
  - Intrusion Detection/Prevention System (IDS/IPS)
  - Honeypots/Honeynets
  - Vulnerability Assessment
  - Attacks (Test Cases)

3) Malware Analytics

- Introduction to malware analysis
- Malware Analysis a practical approach
- Malware analysis techniques- Dynamic and static analysis
- Basic analysis
  - Basic static analysis
  - Malware analysis in virtual machines
  - Setup a safe virtual environment to analyse malware
  - Basic Dynamic analysis
- Advanced static analysis
  - Buffer overflow analysis using immunity debugger
  - IDA Pro