CYBER SECURITY AND DIGITAL FORENSICS - LAB PRACTICAL

PROGRAM OVERVIEW

This program is designed as a hybrid industrial training, integrating online digital academy modules and intensive hands-on physical sessions. It targets students and professionals in Cyber Security, Digital Forensics, IT, and Computer Science. Both proprietary and open-source tools will be used, equipping the participants with practical skills for job-readiness.

Program Purpose and Objectives:

1. Provide participants with practical cybersecurity and digital forensic capabilities.
2. Use locally available and open-source tools widely used in cybersecurity and digital forensic investigations.
3. Prepare participants for industry certifications such as; Security+, CEH, CHFI and Certified Fraud Examiner.
4. Offer hybrid learning: LMS, virtual labs, physical workshops, mentorship, and industry exposure.
5. Build a talent pipeline for African companies struggling to recruit cybersecurity and digital forensic professionals.
6. Enhance threat detection skills and automate threat responses - Participants should be able to identify, manage and respond to security events and incidents

1.0 CYBER SECURITY

Outline:

Topics covered include; Network Discovery, Vulnerability Assessment and Penetration Testing, Intrusion Detection, Log Analysis, Password Security and Cracking, Social Engineering, Firewalls, Security Incident and Events Management, Network Traffic Analysis, and Malware Analysis.

Lab Practical

Syllabus Topics and Tools

The syllabus focuses on practical, hands-on learning using industry-standard commercial and open-source tools:

- **Network Discovery and Vulnerability Scanning**: Participants shall use NetDiscover, Nessus, Nmap, OpenVAS and OWASP ZAP to map devices and identify system and application vulnerabilities.
- **Intrusion Detection**: Utilizing Suricata, Zeek or Snort to monitor and alert on potential security breaches.
- **Log Analysis:** Analyzing network data and visualize logs with Splunk/Wazuh, ELK stack (Elasticsearch, Logstash, Kibana).
- **Security Testing**: Using open-source password cracking tools to test password strength, Password Security and Auditing (John the Ripper, Hashcat, and Hydra).
- **Wireless Security and Hacking**: Participants shall use tool like; Aircrack-ng, Kismet, Wifite, Airgeddon, Wireshark, Hashcat, Metasploit, and Fern.
- **Social Engineering**: Conduct simulated social engineering attacks using open-source tools like the SET (Social Engineering Toolkit – SEToolkit), ZPhisher, and GoPhish. The participants will learn how to defend against social engineering attacks.
- **Network Traffic Analysis:** The participants will learn how to detect and identify anomalies, security incidents and trends in network traffic and identify potential security threats using open-source tools like Wireshark, Network Miner and TCPdump to capture and analyze network traffic. Using log files as evidence; participants should be able to Analyze Firewall Logs, IDS Logs, Honeypot Logs, Router Logs, DHCP Logs, VPN Logs, SSH Logs, DNS Server Logs, and other Network Log Analysis Tools). Wireshark or tcpdump, tshark and network miner,
- **Malware Analysis:** Participants shall learn how to analyze and identify malware behavior to prevent emerging threats and attacks, malware analysis types and tools (Static and Dynamic). Analyze malware samples using static and dynamic analysis open-source tools including sandboxes like FlareVM, Cuckoo Sandbox, Viru Total, any.run, and REMnux.

- **Configuring Firewalls and policy rules** (PfSense/OpnSense, FortiGate, Checkpoint)
- **Cyber Threat Intelligence:** Participants will understand the importance of CTI, The Diamond Model, Cyber Kill Chain and MITRE ATT&CK Methodologies, Advanced Persistent Threats (APTs) and Indicators of Compromise and Indicators of Attacks. OSINT tools shall be introduced.

2.0 ETHICAL HACKING AND PENETRATION TESTING

Lab Practical

Syllabus Topics and Tools

- **System Hacking:** Using tools like Kali Linux, Metasploit Framework**,** Nmap, Burp Suite, OpenVAS, Nessus, SQLMap, OWASPZap, DirBurster, Gobuster and DVWA etc. Participants should be able to learn the following stages of an attack;
    - Reconnaissance
    - Weaponization
    - Delivery and gaining access (social engineering, brute-force, dictionary attacks, keyloggers).
    - Exploitation
    - Installation
    - Post Exploitation
        - Privilege escalation
        - Persistence - Maintaining access (backdoors, rootkits)
        - Lateral Movement
        - Clearing logs and covering tracks

3.0 DIGITAL FORENSICS

Lab Practical

Syllabus Topics and Tools

- **Mobile Device Security and Forensics**
  - **Mobile Device Acquisition:** Participants shall learn how to acquire mobile forensic images using tools like Magnet Axiom, Belkasoft Evidence Center and Cellebrite UFED Touch/PC (Physical, Logical, File System) and the use of Android Emulators such as Genymotion.
  - **Analysis of Mobile Device Data:** Participants shall learn how to Analyze mobile forensic images using tools like; Autopsy, Magnet Axiom, Belkasoft Evidence Center and Cellebrite Physical Analyzer.

- **Computer Forensics:**
  - **Computer Device Acquisition:** Participants shall learn how to acquire computer forensic images using tools like FTK Imager, Paladin, TX1 Imager, dcfldd, dd and dc3dd.
  - **Analysis of Computer Device Data:** Participants shall learn how to Analyze computer forensic images using tools like; Autopsy, Magnet Axiom, Belkasoft Evidence Center, Encase and FTK.
  - **Network Forensics**: Traffic Analysis: Techniques for capturing and analysing network traffic. Intrusion Detection and Analysis: Identifying and analysing network intrusions. Log Analysis: Investigating and interpreting logs from various network devices.
  - **Memory Forensics**: Live acquisition and analysis of computer memory using FTK Imager, DumpIT, Magnet RAM Capturer, Belkasoft RAM Capturer, and Volatility.

- **Malware Analysis and Reverse Engineering**

  Participants should be able to;
  - Understand Malware Types and their Behaviors
  - Perform Static and Dynamic Analysis using open-source tools

- Use Reverse Engineering Tools – Ghidra, Immunity Debugger, IDA Pro.
- Malware Detection and Defense Strategies

4.0 Data Recovery

Lab Practical

Syllabus Topics and Tools

- The participants shall be introduced to top data recovery tools such as; Disk Drill, EaseUS Data Recovery Wizard, Recuva, TestDisk and Stellar Data Recovery. These tools recover deleted files, photos, and partitions from hard drives, SSDs, and USB drives.

5.0 Lab Set-Up Requirements

- Laptop with minimum of 16GB RAM, 1TB SSD.
- Windows OS 11 Pro (Preferably for the Host Machine)
- Kali Linux or Parrot
- Ubuntu Server
- VirtualBox or VMware installed.
- Reliable stable internet

6.0 Recommended Tools and Infrastructure

Cyber Ranges and CTFs (Capture the Flags) – TryHackMe, HackTheBox, Cyber Tallents and VulnHubs.

END