

# CYBER SECURITY & ETHICAL HACKING TRAINER (Model : NL - CSHT)

## Technical

### SALIENT FEATURES

- Kali Linux based nodes: Sender, Receiver and Intruder for hands-on real-time attack and defense practice
- Cybersecurity covered through ethical hacking practice
- Many main topics covered under various experiment
- Topics covered include Network Administration, Cybersecurity Fundamentals, Network/System Security & Threat Prevention Techniques, Network/System Threats & Ethical Hacking, Cryptography, Cryptography Applications to IoT Cloud
- Kali Linux PC is ergonomically designed and aesthetically mounted in sturdy aluminium 30×30 profile rack with built-in USB keyboard, USB mouse, HDMI monitor & SMPS
- Live traffic monitoring using port mirroring to analyze real-time packet flow on WIN LAB PC screen using industry-standard network monitoring software (Wireshark) - Open Source
- User-friendly student workbook & instructor guide provided for step-by-step experimentation

### TECHNICAL SPECIFICATION

#### Node Configuration

3 Linux PCs (Sender, Receiver, Intruder/Hacker) – role selectable at runtime, connected in LAN using smart switch port

#### Node Hardware

- Quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.8 GHz
- 4 GB LPDDR4-3200 SDRAM
- 2.4 GHz & 5.0 GHz IEEE 802.11ac wireless
- Bluetooth 5.0
- BLE Gigabit Ethernet
- 2 USB 3.0 ports, 2 USB 2.0 ports
- Micro-SD card slot for booting operating system & application folder

#### Node Software

- Pre-installed Kali Linux
- GUI executables, Tailored Python & Bash scripts provided in home directory for experiments

#### PC Software

- One Lab PC with WIN10 / WIN11 with USB port required (PC not in scope of supply)

#### PC Hardware

- Wireshark used to capture/display data transactions as security breaches take place during experiments using USB-to-Ethernet dongle



#### Power Supply

- Each node has built-in SMPS (5V / 5A)
- Power adapter provided for smart switch port

#### General

- Operating temperature: 0°C to 50°C
- Power: 100–250 VAC / 50–60 Hz
- Dimensions: 910 mm (L) × 530 mm (W) × 300 mm (D)
- Net Weight: 15 kg, Gross Weight: 20 kg

#### Accessories

- RJ45 cables – 4 Nos
- USB-to-Ethernet dongle – 1 No
- USB keyboard – 3 Nos
- USB mouse – 3 Nos
- Smart Ethernet switch – 1 No
- Power adapter – 1 No
- 3-socket AC power extension – 3 Nos

### List of Experiments

Setting up network connections	Network Identification & discovery	Steganography
Intrusion Detection System (IDS)	Firewall Protection	Intrusion Prevention System (IPS)
Authentication	Password Sniffing	Session Hijacking
Trojan & Spyware	Virus & Worms	Distributed Denial of Service (DDOS)
Spoofing using Wireshark	Packet Sniffing using Wireshark	Website & Email Security
Malware	Viruses	Worms
Trojans	Backdoors	Spyware
Digital Signature	Encryption – Symmetric	Encryption – Asymmetric
Block Cipher	Hashing	Message Authentication