**1) Module Name: DDOS network attack**

Learning Objective: Define how to make the unattackable IoT device under DDOS network attack

Topic Outline: TCP/IP is traditionally implemented in software and run on a processor. This has become a significant bottleneck in data transport when higher bandwidth networks were introduced since the CPU now spends more time handling incoming frames than it does running user algorithms. This performance deterioration interferes with real-time applications and has a detrimental influence on network effectiveness. More functions are now being offloaded into specialized hardware to alleviate this bottleneck. The TCP/IP stack can be partially offloaded to hardware, allowing for significant increases in transmission bandwidth and the security of IoT devices.

*Hardware required:*

Hardware TCPIP ethernet module - WIZ550io -$25

Software TCPIP ethernet module - ENC28J60 -$3

3Com Gigabit Switch -$30

Arduino Uno Kit- $60

Raspberry Pi 4 Model B 2 GB - $200

**2) Module Name: Hardware hacking**

Learning Objective: Setting up a simple hardware hacking experiment and capture I2C traffic directly from the wire.

Topic Outline: Hardware hacking can assist in understanding the gadgets and enhancing device security as the use of IoT devices rises in popularity. As the I2C master, BeagleBone manages the clock and sends data requests to addresses 0x30 and 0x34. The purpose of this experiment is to understand hardware hacking using I2C sniffing.

*Hardware required:*

Adafruit Trinket - Mini Microcontroller - 5V Logic - $6

BeagleBone Black Rev C - 4GB - Pre-installed Debian - $ 80

Saleae Logic 8 - 8 Channels Logic + Analog – Black- $500

Adafruit ItsyBitsy 32u4 - 3V 8MHz - $10

Arduino Leonardo - $25

3) **Module Name: Wireshark Activity**

Learning Objective: To sniff an unsecure network communication

Topic Outline: This activity demonstrates how encrypting communication channels may prevent sniffing attacks. This leads into learning the importance of securing network traffic, and encryption.

*Hardware required:*

Raspberry Pi 4 Model B 2 GB - $200

Micro SD- $10

Power Supply- $10

Ethernet Cable- $10

HDMI cable- $10

4) **Module Name:** USB sanitizer

Learning Objective: To clean documents from untrusted (obtained) USB keys / USB sticks

Topic Outline: Untrusted documents can be automatically converted by the device into a readable but unarmed format, and these clean files can then be stored on a trusted (user-owned) USB key or stick. The goal is to establish document exchange even if the USB stick being used as the transport layer cannot be trusted or if there is doubt about whether the documents it contains are malware-free.

*Hardware required:*

Raspberry Pi 4 Model B 2 GB - $200

HDMI cable- $10