DUCKYPI COURSE

USB Automation & Security Awareness (Concept-Based Training)

Section 1: Introduction

What is this: Overview of USB automation tools and course roadmap.

How it works: Explains objectives, workflow, and ethical boundaries.

Tools Covered: N/A

Section 2: Digispark Setup

What is this: Setup of Digispark device on Windows.

How it works: Installing drivers, configuring environment, and testing device.

Tools Covered: Digispark, Arduino IDE

Section 3: Raspberry Pi Pico Setup

What is this: Setup of Raspberry Pi Pico for automation.

How it works: Installing required tools and verifying functionality.

Tools Covered: Raspberry Pi Pico, Arduino

Section 4: Penetration Testing Concepts

What is this: Understanding USB-based attack simulations.

How it works: Devices emulate keyboard input to automate commands.

Tools Covered: Pico Ducky, Digispark

Section 5: Windows Automation Concepts

What is this: Automating system-level actions.

How it works: Scripts execute predefined sequences on target systems.

Tools Covered: Pico Ducky

Section 6: Android Interaction Concepts

What is this: USB interaction with Android devices.

How it works: Simulated input triggers actions on connected devices.

Tools Covered: Digispark

Section 7: Security Manipulation Awareness

What is this: Understanding system security weaknesses.

How it works: Explains how misconfigurations can be exploited.

Tools Covered: Windows Settings

Section 8: Script-Based Automation

What is this: Creating automation scripts.

How it works: Commands are pre-written and executed via USB device.

Tools Covered: Arduino Scripts

Section 9: NodeMCU Setup

What is this: Configuring NodeMCU board.

How it works: Install, configure and test IoT-based board.

Tools Covered: NodeMCU, Arduino IDE

Section 10: Social Engineering Concepts

What is this: Human-based attack vectors.

How it works: Users are tricked into interacting with malicious setups.

Tools Covered: WiFi Tools

Section 11: WiFi Attack Awareness

What is this: Understanding fake WiFi risks.

How it works: Attackers create rogue access points to capture data.

Tools Covered: NodeMCU

Section 12: Defense & Safety

What is this: How to stay protected.

How it works: Recognizing suspicious USB devices and networks.

Tools Covered: Security Practices