Bluetooth Security Mastery Guide (Day 1-30)

This guide covers Bluetooth security testing, scanning, sniffing, and exploitation, organized day-by-day for progressive learning.

Day 1: Install Tools

- **Command:** `apt install bluez hciconfig hcitool bluetoothctl`
- **Purpose:** Set up Bluetooth testing tools.

Day 2: Understand Bluetooth Types

- **Task:** Learn differences between Classic Bluetooth and BLE.
- **Purpose:** Choose appropriate testing methods.

Day 3: Learn Protocols

- **Task:** Study L2CAP, RFCOMM, HCI protocols.
- **Purpose:** Identify communication layers and vulnerabilities.

Day 4: Adapter Capabilities

- **Task:** Check if your adapter supports sniffing and BLE.
- **Purpose:** Ensure proper hardware for testing.

Day 5: Lab Testing

- **Task:** Test scanning and connection in lab environment.
- **Purpose:** Avoid illegal activity.

Day 6: Classic Device Discovery

- **Command:** `hcitool scan`
- **Purpose:** Discover nearby Classic Bluetooth devices.

Day 7: BLE Device Discovery

- **Command:** `hcitool lescan`
- **Purpose:** Discover nearby BLE devices.

Day 8: Device Management

- **Command:** `bluetoothctl`

- **Purpose:** Manage Bluetooth connections, pairings, and trust.

Day 9: Record Device Info

- **Task:** Note MAC addresses, device names, signal strength.
- **Purpose:** Identify targets for further testing.

Day 10: Check Connectivity

- **Command:** `l2ping <MAC>`
- **Purpose:** Test reachability and latency of devices.

Day 11: Service Enumeration

- **Command:** `sdptool browse <MAC>`
- **Purpose:** List services offered by the target device.

Day 12: Check Serial Communication

- **Command:** `rfcomm`
- **Purpose:** Identify open RFCOMM channels for testing.

Day 13: Explore Vulnerable Services

- **Task:** Identify unprotected or misconfigured services.
- **Purpose:** Find potential attack vectors.

Day 14: Traffic Sniffing Setup

- **Tool: Ubertooth One**
- **Purpose:** Prepare for Bluetooth traffic capture.

Day 15: Capture BLE Advertising Packets

- **Task:** Record advertising packets.
- **Purpose:** Analyze device info, UUIDs, and communication patterns.

Day 16: Wireshark Integration

- **Task:** Capture Bluetooth traffic in Wireshark.
- **Purpose:** Inspect packets and identify weaknesses.

Day 17: Analyze Captured Traffic

- **Task:** Look for device info, services, and potential vulnerabilities.
- **Purpose:** Identify attack vectors.

Day 18: Lab Pairing Test

- **Task:** Pair with lab devices safely.
- **Purpose:** Test authentication protocols.

Day 19: Test Default PINs

- **Task:** Attempt pairing with common default codes.
- **Purpose:** Identify weak device security.

Day 20: Test Weak Pairing Protocols

- **Task:** Check for insecure Bluetooth pairing methods.
- **Purpose:** Discover potential attack points.

Day 21: BLE MITM Setup

- **Tool: BtleJuice**
- **Purpose:** Set up man-in-the-middle attacks on BLE communication.

Day 22: Eavesdropping Test

- **Task:** Capture BLE communication in lab.
- **Purpose:** Detect sensitive data exposure.

Day 23: Service Exploitation Lab

- **Task:** Test vulnerable services for data leaks.
- **Purpose:** Simulate real-world attacks safely.

Day 24: Device Spoofing

- **Task:** Impersonate trusted devices.
- **Purpose:** Test security against impersonation.

Day 25: Automation Scripts

- **Task:** Automate scanning, pairing, and capture.
- **Purpose:** Increase efficiency.

Day 26: Multi-Device Testing

- **Task:** Simultaneously monitor multiple devices.
- **Purpose:** Assess environment-wide Bluetooth security.

Day 27: Analyze MITM Data

- **Task:** Review captured data from BtleJuice or sniffers.
- **Purpose:** Identify vulnerabilities and sensitive information.

Day 28: Document Findings

- **Task:** Record vulnerable devices, services, and protocols.
- **Purpose:** Prepare professional report.

Day 29: Responsible Disclosure

- **Task:** Plan disclosure of vulnerabilities found in authorized testing.
- **Purpose:** Ensure ethical handling.

Day 30: Review & Ethics

- **Task:** Review entire testing process and safety practices.
- **Purpose:** Maintain legal and ethical Bluetooth security testing.

Note: Only test Bluetooth devices you own or are explicitly authorized to assess. Unauthorized Bluetooth attacks are illegal.