Training Title: PRACTICAL IoT HACKING

OVERVIEW

General Information

Our lives are becoming digital every day. Our homes, clothes, and workplaces are getting smarter.IoT devices are becoming widespread in every aspect of our lives. When this is the case, security risks begin to emerge.

With the emergence of security risks, the cyber security requirements in this area are also increasing. Especially in this field, the need for individuals who can perform Penetration Test is increasing.

With this training, you will gain penetration testing capabilities related to IoT devices and improve your existing knowledge. You will have not only talent but also a lot of equipment necessary to perform IoT penetration tests.

Course highlights:

- 4 days of hands-on IoT hacking, led by professional trainers experienced in real-world
- A focus on practical IoT Hacking Techniques
- IoT Hacking Kit for all students

Course details:

- In-person learning – 20% theory, 80% practical

First Day (Before Start)

- About the IoT
- Current IoT Vulnerabilities
    - Constant Embedded Sensitive Information
    - Hardware Debug Ports
    - Insecure Firmware
    - Insecure Data Storage
    - Insufficient Authorization
    - Insecure Communication
    - Insecure Configuration
    - Insufficient Input Filtering
    - Insecure Mobile Application Interface
    - Insecure Web Interface
- Basic Electricity and Electronic 27
    - What is Electricity?
    - What is Static Electricity?
    - Electrical Conductivity and Insulation
    - Electrical Current

    - Voltage, Current, and Resistance
    - Electrical Circuit
    - Connection Types in Electrical Circuits
    - Basic Circuit Elements   30
        - Resistance
        - Sensor
        - Capacitor
        - Transistor
        - Diode
        - Bobin
        - Relay
        - Voltage Regulator
        - Microcontroller and Microprocessor
        - Integrated Circuit
    - Exercise: Fundamental - 1
    - Exercise: Fundamental - 2
    - Exercise: Fundamental - 3
- Soldering
    - Tools and Equipment
    - Soldering Techniques
    - Security Precautions
    - Important Tips
    - Preparation
    - Soldering
    - Solder Disassembling
    - CyberPath Soldering Board
        - Exercise: Soldering - Level 1
        - Exercise: Soldering - Level 2
        - Exercise: Soldering - Level 3
        - Exercise: Soldering - Level 4
        - Exercise: Soldering - Level 5
        - Exercise: DeSoldering for all level

Second Day (Protocol Day)

- IoT Protocols
    - MQTT
        - About the MQTT
        - Use Cases
        - Exercise: MQTT - 1
        - Exercise: MQTT - 2
        - Exercise: MQTT - 3
    - CoAP
        - About the CoAP
        - Exercise: CoAP - 1
        - Exercise: CoAP - 2
        - Exercise: CoAP - 3

Third Day ((Hard|Firm)ware Day)

- Attack Surface Mapping
- Circuit Analysis of Hardware
    - Exercise: UART Hacking (Enumeration and Exploitation)
    - Exercise: Attack Surface Mapping
    - Exercise: SPI Hacking (Enumeration and Exploitation)
    - Exercise: JTAG Hacking (Enumeration and Exploitation)
    - Exercise: I2C Hacking (Enumeration and Exploitation)
- About The Firmware
- How can I obtain a firmware?
- Firmware Analysis Tools
    - Exercise: Static Firmware Analysis
    - Exercise: Dynamic Firmware Analysis with GDB
    - Exercise: Firmware Emulation with QEMU
    - Exercise: Automation of Firmware Emulation with QEMU
    - Exercise: Exploiting Buffer Overflow CVE Real Word Example
- About the Side-Channel Attack
    - Exercise: Side-Channel Attack - 1
    - Exercise: Side-Channel Attack - 2

Fourth Day (RF Day)

- About the BLE
- BLE Structure
- BLE Pairing Methods
    - Exercise: BLE Hacking - 1 (Enumeration and Hacking)
    - Exercise: BLE Hacking - 2 (Encrypted Traffic Analysis)
    - Exercise: BLE Hacking - 3 (Pcap Analysis)
- About the RF
    - Exercise: RF Hacking (Radio Signal Capture, Decode And Analysis)
- About the Zigbee
- Zigbee Structure and Communication
    - Exercise: Zigbee Hacking - 1 (Detection, Analysis and Exploitation)
    - Exercise: Zigbee Hacking - 2 (Pcap Analysis)

KEY TAKEAWAYS

- Attendees will be able to explain the steps and methodology used in performing penetration tests on Internet of Things (IoT).
- Attendees will be able to use the free and open source tools in CyberPath IoT VM with our IoT Hacking Kit to discover and identify vulnerabilities in IoT devices.
- Attendees will be able to exploit several hardware, network, web, serial, user interface, RF, and server-side vulnerabilities.

WHO SHOULD TAKE THIS COURSE

- Penetration testers who want to get into IoT security

- Bug hunters who want to find new bugs in IoT products
- Government officials from defensive or offensive units
- Red team members tasked with compromising the IoT infrastructure
- Security professionals who want to build IoT security skills
- Embedded security enthusiasts
- IoT Developers and testers
- Anyone interested in IoT security

AUDIENCE SKILL LEVEL

Beginner/Intermediate

STUDENT REQUIREMENTS

- Basic knowledge of Linux.
- Basic penetration testing experience is desirable, but not required.

WHAT STUDENTS SHOULD BRING

Each attendee must bring a computer that meets the following requirements:

- 64-bit processor with 64-bit operating system
- VT or other 64-bit virtualization settings enabled in your BIOS to run 64-bit VMs
- At least eight (8) GB of RAM, recommended sixteen (16) GB if possible
- At least fifty (50) GB of free hard drive space
- Intel VT or AMD-V virtualization hardware extensions ENABLED in BIOS
- Windows 10.x installed on your host laptop or inside a VM
- Virtualization software, which must be installed and tested with ControlThings Platform VM BEFORE CLASS!
- Windows Users: Recent version of VirtualBox is the ONLY option, a version released within the last year. VMware Workstation (Pro or Player) is NOT compatible with one of our hardware components needed on the last day.
- Mac Users: Recent version of VirtualBox or VMware Fusion (released within the last year)
- Linux Users: Recent version of Gnome Boxes, Libvirt, VirtualBox, or VMware Workstation (released within the last year)
- Access to a local account with administrative permissions that can install software and disable any security services that interferes with course exercises
- Access to and ability to change BIOS settings if needed in class

WHAT STUDENTS WILL BE PROVIDED WITH

The following items (or rough equivalents depending on availability) are provided to each student to use in class and to keep after course completion:

- CyberPath IoT Hacking Box
    - CyberPath HardKnife (Multi Purpose Hardware Attacking Tool)
    - CyberPath Vulnerable Board for Exercises
    - CyberPath Soldering Board (Five Level)
    - CyberPath HardKnife Slot
- Other Components
    - Arduino Nano
    - Soldering Iron Kit
    - Multimeter
    - Screwdriver
    - Electronics Kit(Breadboards, Jumpers, etc.)
    - Latest version of the CyberPath IoT Hacking VM
    - BLE
- Online Materials
    - Exercises Files (Embedded Firmware, BLE, Wifi, Zigbee)
    - Cloud-based IoT Hacking Lab Access (In Training)
    - IoT Hacking Handbook

ABOUT THE TRAINERS

Besim ALTINOK

Besim Altınok
has been doing research on Wi-Fi security and IoT Security for a long time.
He created the WiPi-Hunter project against Wi-Fi hackers. He is the author of a book on Wi-Fi security.
Besim's studies on wireless security have been published in Arkakapı Magazine and other magazines.
Besim also provided IoT Hacking and other advanced special trainings to the leading companies in the field of telecom
He has also spoken and lectured at top conferences including BlackHat Europe, Blackhat ASIA, Defcon and others.