Practical IoT Hacking:
Basic Edition Training

2 DAY CLASS

Payatu is a NotSoSecure training partner

NOT SO SECURE
A Claranet Group Company

“The great power of Internet Of Things comes with the great responsibility of security”. Being the hottest technology, the developments and innovations are happening at a stellar speed, but the security of IoT is yet to catch up. Since the safety and security repercussions are serious and at times life threatening, there is no way you can afford to neglect the security of IoT products.

“Practical IoT Hacking: Basic Edition“ is a research backed and unique course which offers security professionals, a good understanding of the core of IoT Technology i.e. IoT protocols, sensor tech and their underlying weaknesses. The extensive hands-on labs enable attendees to master the art, tools and techniques to find-n-exploit or find-n-fix the vulnerabilities in IoT, not just on emulators but on real smart devices as well.

The course is aimed at security professionals who want to enhance their skills and move to/specialize in IoT security. The course is structured for beginner level attendees who do not have any experience in IoT, reversing or hardware.

The course specifically focuses on the security issues and attacks on evolving IoT technologies including widely used IoT protocols and platforms in various domains such as home, enterprise etc. It covers grounds-up on various IoT protocols including internals, specific attack scenarios for individual protocols and open source software/hardware tools one needs to have in their IoT penetration testing arsenal. We also discuss in detail how to attack the underlying hardware of the sensors using various practical techniques.

WHO SHOULD TAKE THIS CLASS?

- Penetration testers tasked with auditing IoT
- Bug hunters who want to find new bugs in IoT products
- Governmentofficialsfromdefensiveoroffensiveunits
- 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

PRE-REQUISITES

- Basic knowledge of web and mobile security
- Knowledge of Linux OS
- Basic knowledge of programming (C, python) would be a plus

TRAINERS

Aseem Jakhar is the Director, research at Payatu payatu.com a boutique security testing company specializing in IoT, embedded, mobile and cloud security assessments. He is well known in the hacking and security community as the founder of null - The open security community, registered not-for-profit organization http://null.co.in and also the founder of nullcon security conference nullcon.net and hardwear.io security conference http://hardwear.io He has worked on various security software including UTM appliances, messaging/security appliances, anti-spam engine, anti- virus software, Transparent HTTPS proxy with captive portal, bayesian spam filter to name a few. He currently spends his time researching on IoT security and hacking things. He is an active speaker and trainer at security conferences like AusCERT, Black Hat, Brucon, Defcon, Hack In The Box, Hack.lu, Hack in Paris, PHDays and many more.

* Introduction to IOT
* IOT Architecture
* IoT attack surface
* IoT Security Testing Process
* Expliot – IoT exploitation framework
  - Intorduction
  - Architecture
  - Test Cases
* IoT Protocols Overview
* MQTT
  - Introduction
  - Protocol Internals
  - Reconnaisance
  - Information leakage
  - DOS attack
  - Hands-on with open source tools
* CoAP
  - Introduction
  - Protocol Internals
  - Reconnaissance
  - Cross-protocol attacks
  - Hands-on with open source tools
* Radio IoT Protocols Overview
* Zigbee
  - Introduction and protocol Overview
  - Reconnaissance (Active and Passive)
  - Sniffing and Eavesdropping
  - Replay attacks
  - Hands-on with RZUSBstick and open source tools
* BLE
  - Introduction and protocol Overview
  - Reconnaissance (Active and Passive) with HCI tools
  - GA TT service Enumeration
  - Sniffing GATT protocol communication
  - Reversing GATT protocol communication
  - Read and writing on GATT protocol
  - Cracking encryption
  - Hands-on with open source tools
* Device Reconnaissance * Firmware
  - Types
  - Firmware updates
  - Firmware analysis and reversing
  - Firmware modification
  - Firmware encryption
  - Simulating device environment
* Conventional Attacks
* External Storage Attacks
  - Symlink files
  - Compressed files
* IoT hardware Overview * Introduction to hardware
  - Components
  - Memory
  - Packages
* Hardware Tools
  - Bus Pirate
  - EEPROM readers
  - Jtagulator/Jtagenum
  - Logic Analyzer
* Attacking Hardware Interfaces
  - Hardware Reconnaissance
  - Analyzing the board
  - Datasheets
  - UART
    - What is UART
    - Identifying UART interface
      - Method 1
      - Method 2
  - Accessing sensor via UART
  - JTAG
    - Introduction
    - Identifying JTAG interface
      - Method 1
      - Method 2
    - Extracting firmware from the microcontroller
    - Run-time patching the firmware code
    - Live Debugging of the system
  - I2C
    - Introduction
    - I2C Protocol
    - Interfacing with I2C
    - Manipulating Data via I2C
    - Sniffing run-time I2C communication
  - SPI
    - Introduction
    - SPI Protocol