HACKERU

IoT Exploitation

CR114

05
Days

IoT Exploitation

Outline

The Internet of Things maps all physical devices, vehicles, weapons, home appliances and other items, embedded with electronics, software and sensors that have an IP address and network connectivity. This highly immersive and advanced training plan will cover the fundamentals of how IoT devices operate and communicate, and disclose what lies in the background of their physical set-up. Students will explore different methodologies of detecting vulnerabilities on these devices and learn how to exploit them on the hardware, software and application layers. Participants will exercise those techniques and will practice further using physical tools designed to help with the penetration process. The course also prepares attendees to master radio and Bluetooth exploitation methods, that are critical assets for IoT researchers. By completing the training, participants will have prominent skills and practical experience in the domain of IoT exploitation, and will be familiar with some of the most advanced tools and techniques on the market.

Target Audience

The course targets participants with a solid foundation knowledge in computer networking and information security, who wish to understand the world of IoT security.

Primarily:

- SoC Analysts & Incident Responders
- Junior penetration testers
- System security personnel who are interested in malware analysis

Prerequisites

- Solid knowledge and experience in infrastructure security and network penetration testing
- Familiarity with Linux
- Basic assembly
- Familiarity with web-app penetration testing – an advantage

Objectives

On completing this course, delegates will be able to:

- Understanding IoT architecture and its different components in depth.
- Learning how to locate vulnerabilities and exploit IoT devices on 3 different layers: hardware, software and application.
- Extracting vendor information from examined IoT devices and injecting data into others.
- Working with advanced tools to accomplish advanced tasks of IoT vulnerability discovery and exploitation.
- Learning to deal with radio and Bluetooth technologies, that are highly popular in the IoT world, to extract transmitted information, intercept and control the traffic.

Hardware Requirements

The course requires the following hardware kit for each user or pair of users:

- USB-TTL/FT232/BusPirate/Attify Badge
- RTL-SDR
- Arduino
- A vulnerable device for hardware hacking
- HackRF/Ubertooth

Content

Day 1

Module 01
Introduction to IoT

The first module will introduce participants to Shodan, the most comprehensive search engine for different types of computers and devices connected to the internet. Shodan allows multiple filtering techniques for locating IPs of various IoT devices, such as: servers, routers, webcams, etc. A decisive use of Shodan allows accessing a huge amount of valuable information on the target. During this module, students will become familiar with GUI and CLI uses of Shodan, learn how to use correct filtering to reach the desired database, and extract useful information for later exploitation.

- Exploring Shodan
  - Graphic user interface
  - Command line interface: Using automation, Collecting data with advance filtering, Extracting data
- Mapping operating-systems, applications and IoT devices to specific vulnerabilities

Day 2

Module 02
Firmware Analysis & Exploitation

This module takes participants further into conducting full-scale analysis on IoT devices, by laying out the components of the system and locating vulnerabilities. At this stage, students will learn how to expose and extract vendor information embedded in the device, and alternatively, inject their own credentials or other types of information into it. By the end of this stage, students will have acquired a substantial amount of information and skills to prepare them for more advanced stages in the following modules.

- Mounting file systems
- Firmware analysis
  - Using Binwalk: Identifying hardcoded vendor “secrets”
- Emulating firmware binary
- Firmware analysis toolkit - using firmware emulation

> Learning how to locate vulnerabilities and exploit IoT devices on 3 different layes: hardware, software and application.

Day 3

Module 03
Exploiting Web Application Vulnerabilities on IoT Devices

After covering the IoT vulnerability landscape on the hardware and software layers, in the following module, students will examine the web-application side of IoT devices and explore for more vulnerabilities lying on this platform, that can also be a potential door to access the device and take over it.

- OWASP IoT Top 10
- Exploitation with Burp Suite
- Exploitation using command injection
- Exploitation using brute force
- Exploitation with CSRF
- Extracting vendor credentials

Day 4

Module 04
Using Physical Tools for IoT Exploitation

During this module, students will practice with various physical tools designed for identifying vulnerabilities and exploiting IoT devices in a variety of manners. Participants will experience the work with these tools hands-on and try to penetrate a vulnerable IoT device.

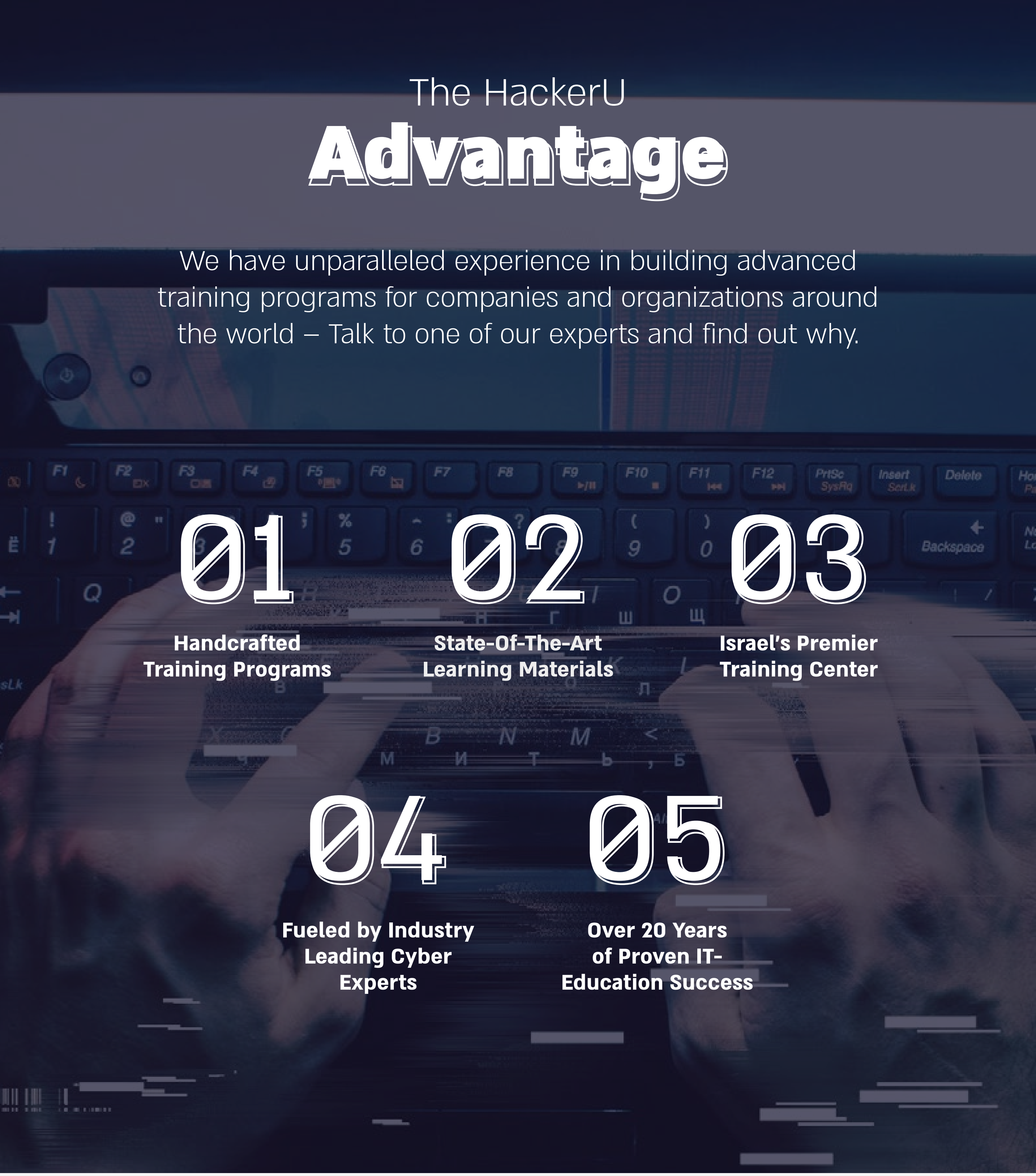
- Reconnaissance basics
- Identifying serial interfaces
- Identifying pinouts with multimeter
- UART
- NAND attack
- JTAG
    - Identifying JTAG pinouts
    - Using JTAGulator
    - Debugging with JTAG
- USB-TTL

Day 5

Module 05
SDR (Software-Defined Radio) Based IoT Exploitation

By using some tools that can analyze radio signals, students will identify and spot signals coming out of different devices and find out their purpose. Participants will analyze different protocols used by the device and decode the signals it broadcasts. This module will give participants an incredible amount of value by familiarizing them with the world of radio hacking.

- Introduction to SDR
- Radio communication analysis
- Attacking protocols
- RTL-SDR
    - Capturing FM signals
    - Analyzing wireless signals
- Extracting text from signals
- Attacking RF (radio frequency)
    - Introduction to RF
    - RF traffic analysis
    - RF replay attack
- HackRF



The HackerU Advantage

We have unparalleled experience in building advanced training programs for companies and organizations around the world – Talk to one of our experts and find out why.

01

Handcrafted Training Programs

02

State-Of-The-Art Learning Materials

03

Israel's Premier Training Center

04

Fueled by Industry Leading Cyber Experts

05

Over 20 Years of Proven IT-Education Success

Info@hackerupro.com

hackerupro.com