IE309: IoT Exploitation Intermediate

Course 71580 – 40 Hours

Overview

IoT or the Internet of Things is one of the most upcoming trends. However, within the growth of many new devices coming up every few months not much attention has been paid to its security till now. The course will be based on theoretical and practical use of vulnerabilities in IoT devices, IoT devices architecture, identifying attack surface and exploiting IoT vulnerabilities.

Objectives

- Becoming familiar with the cyber threat of IoT exploitation
- Acquiring the necessary techniques and tools for IoT exploitation
- Mapping IoT devices
- Firmware exploitation and analysis
- Preparing for cyber-attacks
- Becoming familiar with a variety of available tools for performing IoT exploitation tasks

Who Should Attend

- Governmental bodies, army and security officials
- Private organizations that are interested in preparing their teams for IoT offensive exploitation
- Security Professionals and Penetration Testers
- SOC Analysts
- IoT Developers

Prerequisites

- Working experience with virtualization
- Linux basic commands

Course Contents

Module 1: Introduction to IoT Security

During this module, students will be introduced to IoT and smart devices, IoT device architecture analyzation and breaking it down to individual components, techniques and tools. Students will learn to find vulnerabilities all around the internet using smart queries.

- Learning Shodan
- Using Advanced API
- Searching with CLI
- Collecting and Extracting Data
- Mapping the Internet
- Vulnerabilities by Choice: OS, Application, Metasploit

Module 2: Conventional Attack Techniques
In this module we look for more attacks on IoT devices. Students will get familiar with Linux and network-based exploitation and use their skills on IoT device environments.

- Setting your VM for Penetration Testing
- Introduction to Embedded OS
- Mapping Attack Surface of an IoT Device

Module 3: Firmware Analysis
A firmware is running embedded systems and IoT devices, which holds sensitive information and data.
This module will help us analyze firmware's and extract them, also identifying vulnerabilities in the firmware of IoT devices.

- Mounting File Systems
- Firmware Analysis – Identifying Hardcoded Secrets
- Emulating Firmware Binary
- Backdooring a Firmware
- Firmware Emulation using FAT

Module 4: Software-Based Exploitation
In this module we will cover the IoT devices software's aspects, preforming exploitation on ARM and MIPS architectures. We will also identify command injection vulnerabilities in firmware binaries and attack mobile web apps.

- Common Software Exploitation Techniques
- Intro to MIPS
- Binary Debugging
- ARM Buffer Overflow
- Exploitation with GDB on MIPS

Module 5: Digging Deep into Embedded Devices
This module will dive deeper into the world of embedded devices as we know IoT systems have a device-centric architecture. In this module, we look at the circuit board by opening the device, plan exploitation techniques by identifying the on board components.

- Web application Security for IoT
- Exploitation with Burp
- Exploitation with Command Injection
- Exploitation with Blind Command Injection
- Exploitation with Brute-Force
- Exploitation with CSRF