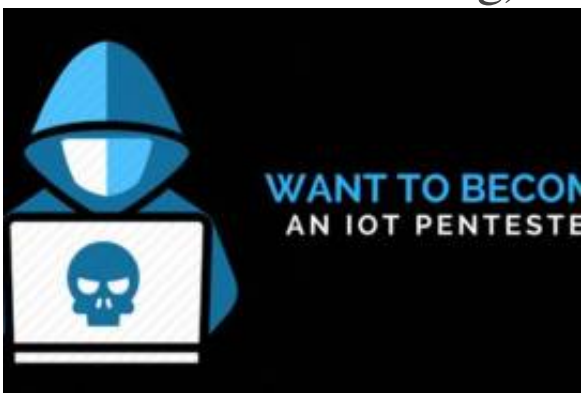
Offensive IoT Exploitation (Learn IoT Pentesting and Smart Device Hacking)



Listing details

Reference Number: RF142565

Common

Description:

After tons of research and conducting 100+ IoT device pentests so far, we have put a training together which will teach you **how to pentest IoT devices**.

"**Offensive IoT Exploitation**" or "**Practical IoT Exploitation**" is an IoT hacking class where we take an offensive approach to break the security of so-called "smart devices". It's a 3-day action packed class covering a number of topics including **Embedded Device Hacking**, Firmware Reverse Engineering, Binary Exploitation, Radio - BLE and ZigBee exploitation and more.

The training puts special emphasis on learning-by-doing, which means that in the three days, you will get a chance to attack and pwn various real-world devices through the skillsets taught by the instructor. There will be no hand-holding, and this class is not for the ones who don't want to perform the exercises in class.

The **Day 1** of the training starts with you getting familiar with the various internal concepts of IoT security architecture, previous vulnerabilities and case studies in IoT devices and takes you all the way through getting firmware for a given target device, reverse engineering it, finding security issues and exploiting them. You will learn concepts such as ARM and MIPS exploitation, Firmware extraction and debugging, Firmware emulation and more.

Day 2 is where things start getting hardcore. The day starts with you taking apart a real world IoT device to understand the underlying circuit boards, its various components and using that knowledge to get a root shell on the device. The exploitation does not end there! You will also learn about topics such as UART exploitation, JTAG debugging and dumping flash chip contents from a device. All of this will be taught with actual labs and handouts so that you are able to grasp 100% of what is taught in the class, and apply it to any IoT device you encounter.

Finally, the Day 3 contains everything that you need to attack devices remotely! Be it Bluetooth Low Energy Exploitation or sniffing and attacking ZigBee devices or even creating your custom radio - we've got it covered! With a combination of labs and exercises, you will learn what it takes for a real-world highly targeted attacker to break into an IoT device.

Date: Wed, May 16, 2018, – Fri, May 18, 2018

Time: 7:00 PM - 10:00 PM

Venue: Boston, MA, United States Map

Cost: $2,599.67

Event Type: Masterclass

More Details

Posted: 7 years ago

Location

Country: United States