

# Practical IoT Hacking

## The Definitive Guide to Attacking the Internet of Things

by Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, & Beau Woods

Errata updated to print 6

Page	Error	Correction	Print corrected
75	<pre>allow_anonymous false password_file /etc/mosquitto/password</pre>	<pre>allow_anonymous false password_file /etc/mosquitto/password <b>listener 1883</b></pre>	Print 3
78	Because MQTT uses TCP port 1833, we add the following line (anywhere in the file is fine):	Because MQTT uses TCP port 1883, we add the following line (anywhere in the file is fine):	Print 3
181	<pre>\$ sudo openocd -f /usr/local/share/openocd/scripts/interface/stlink.cfg -f /usr/local/share/openocd/scripts/<b>targets</b>/stm32f1x.cfg</pre>	<pre>\$ sudo openocd -f /usr/local/share/openocd/scripts/interface/stlink.cfg -f /usr/local/share/openocd/scripts/<b>target</b>/stm32f1x.cfg</pre>	Print 6
182	You can find examples of these handlers if you inspect the <i>openocd/scripts/targets/</i> directory's <i>.cfg</i> files.	You can find examples of these handlers if you inspect the <i>openocd/scripts/target/</i> directory's <i>.cfg</i> files.	Print 6
404	<i>Addition</i>	<b>CatSniffer</b>  CatSniffer is an original multiprotocol and multiband board for sniffing, communicating, and attacking IoT devices using the latest radio IoT protocols. It is a highly portable USB stick that integrates TI CC1352, Semtech SX1262, and an RP2040 for V3 or a Microchip SAMD21E17 for V2. You can find more about it at <a href="https://github.com/ElectronicCats/CatSniffer">https://github.com/ElectronicCats/CatSniffer</a> .	Print 6