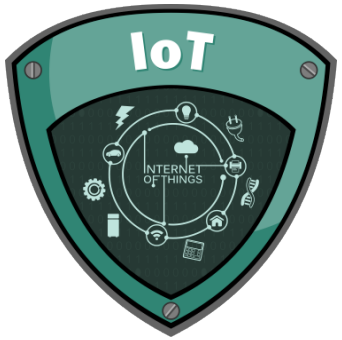
Offensive IoT Exploitation
Setting up the Pentest VM



Aditya Gupta (@adi1391)
Founder, Attify (http://attify.com)
adi@attify.com

Certification : http://securitytube-training.com
Videos : http://pentesteracademy.com

Getting started

- Get a Kali VM image from https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/
- If you use the ISO, some of the SDR and Firmware emulation might have issues
- Let’s now go ahead and install/set-up the tools needed for the course.

Getting started

Kali Linux VMware Images | Kali Linux VirtualBox Images | Kali Linux Hyper-V Images

Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.2G	**2016.2**	fd91182f6abcba7d3efa4de0b58f4db42def49a4
Kali Linux 32 bit VM PAE	Torrent	2.2G	**2016.2**	84d53e456f66d6de4759f759ab8004609cc127ad
Kali Linux Light 64 bit VM	Torrent	0.7G	**2016.2**	2fa5378f4ce25a31c4cbf0511e9137506b1fb5e0
Kali Linux Light 32 bit VM	Torrent	0.7G	**2016.2**	1951c180968c76b557c11d21893419b6bbbc826e

Tools to install

- Firmware analysis toolkit (consists of Firmadyne, qemu, binwalk, firmware mod kit, firmwalker and mitmproxy)
- Kdiff3
- Radare2
- OpenOCD
- Flashrom
- Buildroot
- GDB-multiarch
- GNURadio companion and GQRX
- RTL-SDR tools
- Ubertooth, HackRF tools (optional)
- Zigbee tools – Killerbee

Firmware analysis toolkit

- Navigate to https://github.com/attify/firmware-analysis-toolkit
- Follow the instructions

Flashrom

- Version 0.99
- wget http://download.flashrom.org/releases/flashrom-0.9.9.tar.bz2
- ./configure
- make && make install

Radare2, OpenOCD, GDB, SDR tools

- apt-get install radare2
- apt-get install openocd
- apt-get install gdb-multiarch
- apt-get install gnuradio gqrx rtl-sdr
- apt-get install hackrf ubertooth

Killerbee

- apt-get install python-gtk2 python-cairo python-usb python-crypto python-serial python-dev libgcrypt-dev
- hg clone https://bitbucket.org/secdev/scapy-com
- cd scapy-com
- python setup.py install
- cd ..

Killerbee

- git clone https://github.com/riverloopsec/killerbee.git
- cd killerbee
- python setup.py install
- cd tools/
- chmod +x *

Other additional tools

- Arduino IDE : https://www.arduino.cc/en/Main/Software
- XCTU - https://www.digi.com/products/xbee-rf-solutions/xctu-software/xctu : Used for programming Xbee (optional, to be performed only if you want to do a hands-on on the Xbee/Zigbee section in SDR)