Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Wireless Network Audits using Open Source tools

Wireless networks following the 802.11b or "WiFi" standard are becoming extremely popular, due to their ease of installation. At the same time, a well-designed and secure installation of a WiFi network is not a trivial task. Many companies therefore need professional help to audit their WiFi deployments or pilots, and ensure that their use of this new technology is not done at the expense of security and performance. Many tools exist to enable security professionals to do WiFi networks surveys, ranging from "Free" Open...

Copyright SANS Institute

Author Retains Full Rights

AD

Name: Edouard Lafargue
Assignment Version number: 1.4b
Paper version number: 1.0

Wireless Network Audits using Open Source tools

Abstract:

Wireless networks following the 802.11b or "WiFi" standard are becoming extremely popular, due to their ease of installation. At the same time, a well-designed and secure installation of a WiFi network is not a trivial task. Many companies therefore need professional help to audit their WiFi deployments or pilots, and ensure that their use of this new technology is not done at the expense of security and performance.

Many tools exist to enable security professionals to do WiFi networks surveys, ranging from "Free" Open source tools, to sophisticated commercial products. The intention of this paper is to show that Open Source tools are particularly well-suited for doing WiFi surveys, and will detail a practical setup and the capabilities it offers.

© SANS Institute 2003, Author retains full rights.

Introduction to Wireless Network Surveys 3
Wireless Network Surveys 3
Steps of a Wireless Network Survey 3
Wireless Security Survey 4
Wireless Site Audit 5
Software 6
RF Monitoring Software 6
Packet Analyzers 7
Mapping software 8
Vulnerability Assessment 8
Hardware 8
GPS Receivers 9
Spectrum Analyzers 9
Hardware-based WiFi monitors 9
Using Open-source software for WiFi surveys 9
The Wireless analyzers scene 9
Why is Open-source relevant with WiFi? 14
Considerations on Open Source 14
Focus on the open-source offering 14
Example of a Survey setup 16
Kit List 16
Setup capabilities 16
Channel hopping / Multichannel monitoring 16
Advanced AP Detection 16
Passive Monitoring 17
IP Block Detection 17
Cisco product detection via CDP, manufacturer identification, default configuration detection 17
Detection of Netstumbler clients 17
Traffic logging and analysis 17
WEP 17
GPS Support and mapping 18
Real-time performance monitoring for each AP 18
Conclusion 18
Practical Example 19
Installation and configuration of the software 19
Cisco Aironet Drivers 19
Configuration 19
Running the setup 20
Hardware Connections 20
Software 20
Acronyms 24
References 25

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Introduction to Wireless Network Surveys

Wireless Network Surveys

Wireless network surveys, or audits, are essentially similar to their "fixed network" equivalent in their goal: they aim at both identifying security and performance issues in the network, and at establishing a baseline against which future surveys will be measured.

The main difference between a fixed network survey and a wireless survey concerns the physical transport layer -radio in one case, cables in the other-, and layer 2 characteristics. Using the radio spectrum for communications leads to very specific issues that have to be taken into account, such as:

- Network access range, fading, and interferences.
- Unauthorized network access.
- Interference with other neighboring networks.
- 802.11 security issues.

Even though unauthorized network access can be an issue with physical networks (physical security breach), it is much more of a concern with WiFi networks, as it is very easy to eavesdrop for an intruder, and at the same time difficult to detect someone passively listening to traffic, though it is not always impossible [IDS1].

Radio-specific issues are an important factor in the design of a WiFi network. 802.11b networks use the microwave 2.4-2.48 GHz range, which is a frequency that does not propagate well in the atmosphere, and thus enables a more dense cell implementation. It also means that it is very sensitive to fading and propagation oddities.

The goal of this paper is to start with defining a high-level list of the tasks that have to be performed during a wireless survey, and from this list of tasks, create the list of the requirements that the surveying tools have to fulfill in order to perform those tasks.

This approach enables us to create a set of criteria against which the various existing tools can be compared, whether they are Open-source tools or commercial.

Steps of a Wireless Network Survey

We will separate wireless network surveys in two main families: Wireless network security audits and wireless site surveys. Though the focus of this paper is on wireless security, we will nevertheless go over the description of wireless site surveys, as they contain a security component that should not be underestimated: security needs to be considered from the beginning design phase, not as an

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

additional component added at a later stage!

A **wireless network security audit** will generally be conducted on an existing 802.11 network that has already been deployed either as a pilot or for production. This audit will aim at identifying issues, and establish a baseline for the network.

A **wireless site survey**, on the other hand, will usually be conducted before installing a 802.11 network, and will aim at identifying at an early stage issues that may occur during deployment, and gather the relevant information needed to design the structure of the 802.11 network that will be installed on site.

Wireless Security Survey

A wireless security survey can be broken into the following phases. The following list is not meant to be a detailed breakdown of the tasks to accomplish, but just identifies the main steps.

Phase I – Audit Preparation

- Decide assessment strategy:
  - Raise network management awareness for audit or not
  - Passive/Active/Disrupting survey
- Amount of effort: high-gain antennas, casual access, physical intrusion, rogue AP installation
- Legal Issues
- Audit timeframes
- Following the strategy that is decided, constitute Team
- Kit

Phase II – Security Audit

- Run network stumblers outside of building, determine leaking coverage
- Packet logging and analysis
- Identify relevant leaked info
- Identify AP hardware and configuration
- WEP Key decryption depending on network traffic
- Rogue AP installation – get users to connect to rogue AP and hijack traffic
- Exploits of known factory configuration weaknesses
- Exploits of known deficiency of identified network design

Project Milestone:

- Map of leaking coverage around site/campus
- List of WiFi AP identified, along with configuration

Phase III – Security Recommendations

- WiFi architecture recommendations
- Adapting existing architecture to offer better security
- Introduce stronger/smarter encryption
- WiFi configuration recommendations
- AP configuration

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Encryption configuration

Wireless Site Audit

A wireless site audit can be broken into the following phases:

Phase I – Planning / Info gathering

- Gather information about the site where survey will be done
- Building Blueprints
- Building Structure
- Gather information about the population that will be or is using WiFi
- Laptops/Desktops
- Mobility / Roaming
- Planned population
- Gather information about planned or existing wanted network capacity and service levels (bandwidth per user)

Phase II – Site Survey 1 : Radio Survey

- Team goes to site and evaluates pre-existing 802.11 networks that can be reached from site
- Team evaluates sources of disruption:
- Rogue sources – microwave ovens, unfiltered electrical appliances
- Spectrum Competition: Bluetooth, proprietary 2.4GHz wireless transmissions, cordless phones
- For existing 802.11 networks owned by the customer, do
- Rogue access points survey

Project Milestone:
- Radio survey report
- Recommendations for alleviating issues encountered during Radio Survey

Phase III – Site Survey 2: Physical Survey
- Physical building security survey: access control, user identification
- AP location strategy:
- Fading zones
- Coverage and out of building radio leaking
- AP Power Level adjustment
- Physical AP enclosure and physical security
- Antenna location

Project Milestone:
- Recommendations for building security – Corporate Badge, Door control
- Map of location of all AP
- Radio configuration of all AP

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Channel allocation strategy
- Power Levels

Software

In the course of the two survey types described above, specific software will be used. More precisely, we need:

- RF Monitoring software ("stumblers")
- Packet analyzers
- Mapping software
- Software kits for exploiting known weaknesses

RF Monitoring Software

RF monitoring software is the WiFi equivalent of network packet sniffers for ethernet. While packet sniffing on switched ethernet networks can sometimes be difficult to run, because of traffic separation on various network segments, Wireless sniffing is comparatively easier: all the stations that use a given WiFi network transmit on the same set of channels, and some WiFi network cards can be configured to listen to all traffic on all channels.

In order to conduct a wireless security survey, in view of the tasks specified above, the monitoring software must be able to provide at least the following features:

- AP and client detection and identification: WEP, SSID, manufacturer, configuration.

The first task of the RF monitor is to identify existing 802.11x traffic and what Access Points and clients can be detected at a specific location.

Most RF monitoring software will also be able to automatically determine the manufacturer and model of detected access points and client workstations.

- Geographical tagging of APs.

This is an essential feature of RF monitors: one of the biggest security threats of WiFi networks is the lack of control on the actual range of the installed Access Points. The RF monitor must be able to map the coverage of all the Access points it detects. This is usually achieved using GPS receivers.

- Packet logging for analysis by third-party software.

The third main feature of a RF monitor is the ability to log all the packets it receives

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

in a file format that is compatible with higher-level analyzers. Those analyzers are the same as those used for fixed network surveys and can decode higher-level protocols and detect security issues that are not specific to the Wireless aspect of the network.

When conducting wireless site surveys, emphasis is put on the radio layer, and network performance. On top of the features previously mentioned, surveyors will need software that can do:

- Power level and signal strength mapping.

Because 802.11x signals are very sensitive to fading, RF monitors must be able to map not only the range of access points, but also the signal strength and quality over the coverage area.

- AP coverage mapping.

- Network interference from neighboring WiFi networks.

One big potential problem that can be discovered during a WiFi site survey is the existence of access points that can be reached on the site and do not belong to the company that is doing the survey. It is important that the RF monitor detects those and maps their coverage. Failure do do this can result in workstations associating with the wrong access points once the WiFi network is installed, which can lead to serious security problems.

Other features

In practice, other features will also help in producing better survey results:

- Multiple probe results consolidation: laptops, handhelds, etc

This enables several people to survey the same site at the same time, and send all their results to the same server. Handheld devices are particularly well-suited for site surveys, and it is important to be able to be able to store the information they collect in one central database to create a synthetic view of the result of the surveys.

- Higher-level detection features

This can for example include Cisco product detection via CDP, SSID decloaking, WEP decryption, default AP configuration detection, detection of stumblers, etc. These are features that are not strictly necessary for doing a survey, but will improve the quality of the end result and make the life of the surveyors easier.

Packet Analyzers

Packet analyzers decode the traffic that has been recorded by the RF monitor. They

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

are usually not specific to WiFi, but need to be able to decode 802.11 payloads.

Packets analyzers let users identify security and performance problems.
For example, using the correct set of filters on a packet analyzer, it is relatively easy to detect the presence of “active stumblers” on a network [IDS1].

Mapping software

Mapping software is used for the production of reports, and to plot access point coverage, power levels, etc. Depending on the way they are used, mapping packages can be either a cosmetic enhancement to the final survey report, or bring real value.

Vulnerability Assessment

This step is not specific to wireless security surveys, and very similar to its fixed network equivalent.

There are a lot of automated vulnerability assessment tools available on the market, which can automatically produce very detailed reports, such as Nessus.

Using automated tools is a trade off: if they are kept up to date and follow security disclosures on reliable security groups (CERT advisories [Cert1]), they do add real value. If not, they bring a false sense of security.

When it comes to wireless-specific vulnerabilities, the same few issues keep popping up [wlansec1] [wlansec2] [wlansec3]:

- Access points kept in factory configuration
- Access points having hard-coded back doors for factory use and repairs
- WEP and more generally encryption not being properly configured

RF monitors all check the presence of WEP on access points, but few are able to detect factory configurations. This sort of checks often has to be done manually.

Concerning WEP, its vulnerability has been discussed in many papers since the initial proof of concept given in “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP” [wlansec3]. In practice between 5 and 10 million packets need to be gathered in order to effectively crack WEP keys [airsnort1], which makes WEP cracking a task destined only to motivated people, who arguably are also precisely the ones who are most dangerous.

Hardware

While most WiFi surveys can be done using only software tools and wireless network

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

cards, it is important to note that in some cases, specialized hardware can be used for specific aspects of the surveys.

GPS Receivers

The GPS system is a military system managed by the United States, which enables devices to know their geographical coordinates within a precision of a few meters.

GPSes are often used for wireless surveys, as this enables RF monitors to add geographical information to the information they log, and most if not all RF monitoring software supports GPSes.

It is nevertheless important to note that the GPS system does not work indoor, which makes its use irrelevant for surveys inside offices.

Spectrum Analyzers

Spectrum analyzers are high-end devices that monitor the strength of various frequencies in the RF spectrum. Their use is not trivial, they are expensive and they need to be operated by qualified personnel. [willtek1]

They enable surveyors to create a very precise map of RF coverage for access points, and can also spot sources of interference, such as other devices operating in the 2.4GHz band: bluetooth, cordless phones, defective microwave ovens… [microwave1] [microwave1]

Hardware-based WiFi monitors

There are a few WiFi monitors on the market that use dedicated hardware [WLANHACK1]. They usually combine the features of a software-based RF monitor with the added functionality of a basic spectrum analyzer. These will not be covered in this paper.

Using Open-source software for WiFi surveys

The Wireless analyzers scene

The previous section gave an overview of the steps of a WiFi survey, and what precise features are required to perform a good survey.

Despite the fact WiFi is still a fairly new technology, there is a lot of software on the market. Below is a partial list, that includes both Open Source, freeware and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

commercial software [WLANHACK1], [wtelco1].

© SANS Institute 2003, Author retains full rights

Name / URL	License	Platform	802.11x	Description
Kismet www.kismetwireless.net	GPL	Linux (PC & iPaq	a & b	Kismet is an 802.11 wireless network sniffer - this is different from a normal network sniffer (such as Ethereal or tcpdump) because it separates and identifies different wireless networks in the area. Kismet works with any 802.11b wireless card which is capable of reporting raw packets (rfmon support), which include any prism2 based card (Linksys, D-Link, Rangelan, etc), Cisco Aironet cards, and Orinoco based cards. Kismet also supports the WSP100 802.11b remote sensor by Network Chemistry and is able to monitor 802.11a networks with cards which use the ar5k chipset. [kismet1]
Airsnort http://airsnort.shmoo.com/	GPL	Linux (PC & iPaq)	b	AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. [airsnort1]
Wellenreiter http://www.remote-exploit.org/	GPL	Linux (PC/iPaq)	b	Wellenreiter is a GTK/Perl wireless network discovery and auditing tool.
Airtraf http://www.elixar.com/	GPL	Linux	b	AirTraf 1.0 is a wireless sniffer that can detect and determine exactly what is being transmitted over 802.11 wireless networks. This open-source program tracks and identifies legitimate and rogue access points, keeps performance statistics on a by-user and by-protocol basis, measures the signal strength of network components, and more. [airtraf1]
APTools http://aptools.sourceforge.net/	GPS	Linux, Windows	b	APTools is a utility that queries ARP Tables and Content-Addressable Memory (CAM) for MAC Address ranges associated with 802.11b Access Points. It will also utilize Cisco Discovery Protocol (CDP) if available. If an Access Point that is web managed is identified, the security configuration of the Access Point is audited via HTML parsing. [aptools1]
NetStumbler and Ministumbler http://www.stumbler.net/	Freeware	Win2k, mac, WinCE	b	NetStumbler and Ministumbler were amongst the first to be released and started the whole “wardriving” movement.
AirMagnet Duo, Handheld & Laptop www.airmagnet.com	Commercial	Win CE 3, 98, NT 4, 2000, XP	a & b	Aironet Duo is a 802.11a and 802.11b network scanner. “the AirMagnet Duo provides performance management, expert advice, connection troubleshooting tools, a complete set of network diagnostic tools, and a built-in Site Survey tool.” [airmagnet1]
AiroPeek NX (WildPackets) www.wildpackets.com	Commercial	Windows 2000, XP	a & b	“AiroPeek NX combines expert analysis capabilities with WildPackets' wireless LAN analysis technology. This allows IT professionals to manage every segment of their extended network with powerful problem detection heuristics and 802.11-specific diagnostic capabilities. AiroPeek NX is the only wireless management tool you need to deploy, secure, and troubleshoot your wireless LAN”. [airopeek1]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

LANFielder (Wireless Valley Communications) www.wirelessvalley.com	Commercial	Win CE 3, 98, NT 4, 2000, XP	b	"LANFielder® provides real-time, site-specific network performance measurements for any IP-based data network including 802.11b WLAN. LANFielder lets you instantly measure, visualize, and archive true network performance, on site or remotely". [lanfielder1]
LinkFerret Baseband Technologies www.baseband.com	Commercial	Win 98, NT 4, 2000, XP	a	"The LinkFerret Network Monitor provides a cost effective, easy to use way to monitor your network traffic, display frames in brief, hex and detail windows, create reports, view statistics, filter protocols, create link filters, and more." [baseband1]
Sniffer Wireless Network Associates www.sniffer.com	Commercial	Win CE 3, 98, NT 4, 2000, XP	a & b	Sniffer Wireless is the wireless equivalent of the well-known Sniffer network analyzer, with a few added features (rogue AP detection).
Wireless Scannner Internet Security Systems www.iss.net	Commercial	Win 2000, XP	b	"Internet Security Systems' Wireless Scanner' application provides automated detection and security analyses of mobile networks utilizing 802.11b WLAN (Wi-Fi) access points and clients." [iss1]
WLANBit tricycle and Procycle www.wlanbit.com	Commercial	WinCE, win2000	b	Tricycle and Procycle are 802.11b site survey and measurement tools that work on PDAs and laptops, respectively. [WLANBIT1]
Ethereal www.ethereal.com	GPL	Windows, Linux	a & b	Ethereal is a powerful protocol analyzer for Unix and Windows. It supports the 802.11 protocol.
Gpsdrive http://www.kraftvoll.at/software/index.shtml	GPL	Linux, iPaq	n.a.	GPS Drive is a GPS mapping system that can download maps from the internet and use them to draw the location of Access Points
Wepattack http://wepattack.sourceforge.net/	GPS	Linux, iPaq	B	"WepAttack is a WLAN open source Linux tool for breaking 802.11 WEP keys. This tool is based on an active dictionary attack that tests millions of words to find the right key. Only one packet is required to start an attack."

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This quick sample of the current scene shows that there are many tools that are designed to help with Security surveys.

All products listed in the above table offer the same set of basic features that was covered above. Each also usually has a few differentiation features, such as 3D rendering of coverage maps (such as LanFielder), or “expert systems” that match well-known situations to a database / help system, such as Sniffer Wireless. It is not easy to take those features into account for a comparison between tools, as they have little overlap from one program to another, and their actual usefulness can be a fairly subjective factor.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Why is Open-source relevant with WiFi?

Considerations on Open Source

The open source movement was born in 1984 (http://www.gnu.org/), and has now become an integral part of the software industry. It was born out of the belief that it is the interest of everyone to be able to freely share the source code of their projects, as it will lead to better quality software. This point has been argued countless times, and a good reference on the matter is “The Cathedral and the Bazaar”, by Eric S. Raymond [cathedral1].

It is important to realize that personal motivation is usually the main driver and success factor behind open-source projects: people need to be passionate about their project and motivate the rest of the contributors, in order to get good results.

Keeping this in mind, WiFi has a few characteristics that have made it very popular amongst the Open Source community: it is both a low-cost and a high-tech system. It offers a lot of potential for tweaking and creating community networks ([consume1], [nycwireless1]), and you only need one WiFi card and a cheap antenna to start playing with the technology. In short, its “hype factor” is very high!

For these reasons, and as soon as the cost of 802.11b cards became affordable a few years ago, a lot of high-quality software was written to let people explore the possibilities of 802.11b, leading to the first generation of wireless network survey tools, also called “stumblers”, and to the development of a new hacking activity: “Wardriving”. It is important to note that the characteristics of the tools developed for “wardriving” are exactly those that are needed for doing wireless security surveys! [issa1].

This wardriving movement raised the awareness of the industry about wireless security issues, and pushed professional security software companies to broaden their offering in that area. This new software offer came after most of the open-source scanners and survey tools were developed, as a response to a new threat. For example, the “Sniffer Wireless” product, very similar to kismet in its capabilities, was released in September 2002 [sniffer2], whereas the Kismet project dates back from before December 2001 (from the Changelog in the Kismet source [kismet1]).

Focus on the open-source offering

It is not the intention of this paper to go over the perceived benefits of Open Source software of general, but rather to show that its use is relevant for Wireless security.

As seen in the table above, there is a real open-source offering when it comes to Wireless scanners and survey tools: 802.11a and b protocols are supported by several products, on a lot of varied platforms (Linux, Windows and PocketPC).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

An added benefit of Open Source products is that, as they do not require the purchase of a license, they can easily be used together to complement the features of several different packages and create a more powerful setup.

On the other hand, two issues can sometimes be an issue with corporate use of OpenSource software:

- Lack of support
- Open-source licensing terms

Lack of support is often seen as a big problem, as this forces companies that rely on open source tools to count on community support and there is guarantee that bugs will be fixed.

In our case, this problem is alleviated by the fact that, as mentioned above, wireless tools are being very actively developed and are the same tools used by wardrivers: any bug or shortcoming of those tools will impact both sides of the security field!

The issue of Open-source licenses, especially the Gnu GPL (General Public License) concerns the fact that source code and/or changes to it must be redistributed or made available along with copies of the software (section three of the Gnu GPL). This can be deemed unacceptable in some business situations.

In the case of wireless surveys, this is actually not an issue, as there is no redistribution of any kind of software involved in surveys.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Example of a Survey setup

This section describes a practical example of a survey setup that is suited for wireless security audits. It only relies on Open Source tools.

Kit List

In this setup, the following list of software is being used:

- RF Monitor: Kismet wireless v2.8.0 [kismet1]
- Mapping software: gpdrive v 1.32and kismet mapping module
- Network analyzer: ethereal 0.9.9
- Performance monitoring: airtraf 1.0 [airtraf1]
- Other vulnerability testing and security tools:
    - Airsnort 0.2.1b [airsnort1]
- Operating system: Debian/GNU Linux v2.2 [debian1]
- Linux kernel v2.4.20

The hardware components that were used for the setup were:

- Cisco Aironet LMC352
- External 5db omnidirectional antenna [solwise1]
- Serial GPS (Garmin GPSMap76S)
- Dell Latitude Laptop

Setup capabilities

The software list was chosen to provide at least the features that were described in the first part of the document. More precisely, this set of tools offers the following:

Channel hopping / Multichannel monitoring

All 802.11b channels can be monitored at the same time, thanks to the use of a Cisco 350 series card.

Advanced AP Detection

Kismet detects all APs that send data over the air. It also offers slightly more advanced options that enable more flexible monitoring:

- Hidden SSID decloaking
    - If SSID broadcasting is disabled on an AP, Kismet will detect it from network traffic instead of relying on beacon frames.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Grouping and custom naming of SSIDs
    - This enables to sort access points in various groups for easier management.

Passive Monitoring

RF Monitoring software such as Netstumbler actively probe 802.11b networks, and can disrupt their operation. Kismet does passive monitoring and does not send radio packets. In fact, when a WiFi card is put in RF Monitoring mode, its transmitter is switched off and it cannot send packets.

IP Block Detection

For each detected Access Point, Kismet is able to detect the IP configuration of the network, and identify all clients that are members of it.

It can detect IP addresses and ranges from DHCP requests, IP/UDP traffic, and (R)ARP requests.

Cisco product detection via CDP, manufacturer identification, default configuration detection

Through a built-in database, and decoding of the Cisco CDP protocol, Kismet is able to passively gather a lot of information on each detected device, including in some cases the detection of Access Points left completely or partially in default factory configuration.

Detection of Netstumbler clients

Kismet can detect active wardriving attempts using clients such as Netstumbler.

Traffic logging and analysis

All data gathering is done through the RF Monitor, Kismet. This data is saved in files compatible with most network traffic analyzers, and most notably in our case, Ethereal. This also means that the whole monitoring session can be “replayed” at a later stage, for off-site analysis.

Analysis can be done on the fly, during capture, or at a later date using the saved file.

WEP

The use of airsnort enables the detection of cryptographically weak WEP configurations. Airsnort runs in the background while RF monitoring is ongoing and gathers WEP-specific information.

Kismet can also decode WEP packets in realtime when provided with the relevant WEP keys.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

GPS Support and mapping

When used exclusively indoors, this feature is not relevant. Nevertheless, a full WiFi security survey includes the survey of outside-leakage of the access points.

Using gpsdrive and Kismet simultaneously enables real-time plotting of outdoors AP coverage, and offline creation of more detailed coverage maps.

Real-time performance monitoring for each AP

The “airtraf” client, which can be run at the same time as the rest of the tools, enables users to do real-time monitoring of each access point, and all traffic on the network.

This makes it possible to spot performance issues, potential denial of service attacks, and other issues related to the network.

Conclusion

Comparing the above feature list to the list described in the “Software” section, we can see that this setup offers all the features that are necessary to accomplish all the steps of a wireless survey.

© SANS Institute 2003, Author retains full rights

Practical Example

This section provides more information on how to set the tools up in order to run a survey. It is by no means extensive, but provides high-level information adequate with the scope of this paper.

Installation and configuration of the software

All software was fetched on the official distribution web site of each program:

Kismet: http://www.kismetwireless.net/
Ethereal: http://www.ethereal.com/
Airsnort: http://airsnort.shmoo.com/
Airtraf: http://www.elixar.com/
Gpsdrive: http://www.kraftvoll.at/software/

Alternatively, it was also possible to install all the above software but "airtraf" using the built-in Debian package manager:

```
#apt-get install airsnort kismet ethereal gpsdrive
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
  Kismet airsnort ethereal gpsdrive
0 packages upgraded, 4 newly installed, 0 to remove and 0  not upgraded.
```

This makes installation quicker and easier than compiling everything from source.

Cisco Aironet Drivers
The Cisco drivers used for this project were the "standard" Linux kernel 2.4.20 drivers that are compatible with the aironet 350. Those drivers were compiled as part of the kernel PCMCIA subsystem and did not cause any specific difficulty.

Configuration

Using Kernel drivers 2.4.20, the interface that is used for RF monitoring capture is "wifi0".

The GPS is connected to /dev/ttyS0 on Dell laptops. Create a symbolic link of "/dev/ttyS0" to "/dev/gps" for ease of use:

```
#ln -s /dev/ttyS0 /dev/gps
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Kismet

Specify the right source in kismet.conf:

```
# Cisco DL352
source=cisco_cvs,wifi0,Kismet
```

For the current version of kismet (2.8.0) and kernel drivers 2.4.20, it is necessary to modify the “kismet_monitor” command slightly in order to enable monitoring mode: Monitoring is done on “wifi0”, but the commands to enable monitoring are done on “eth1”: change the “DEVICE2” entry to read “eth1” instead of detecting the name automatically:

```
          "cisco_cvs")
                  echo "Enabling monitor mode for a cisco card on $DEVICE"
                  #DEVICE2=`echo $DEVICE | sed -e 's/wifi/eth/'`
                  DEVICE2="eth1"
```

Other settings

Make sure that the “/etc/network/interfaces” file does not contain an “eth1” entry, otherwise the WiFi card will try to acquire a DHCP address when it is inserted, which is not what we want in this setup.

Running the setup

Hardware Connections

First, power up the GPS and connect it to a free serial port on the laptop. The GPS needs to be configured to output its position using the NMEA protocol, which is supported by virtually every model.

Then, insert the Cisco Aironet card into a free PCMCIA slot in the laptop, and connect the antenna. The LEDS on the side of the card should start to flash.

Software

First of all, the GPS mapping system and daemon must be launched: launch “gpsdrive” and click on the “Start gpsd” button, which will connect to the GPS.

Once gpsdrive is running and connected to the GPS, open a terminal with root privileges and launch “kismet_monitor”:

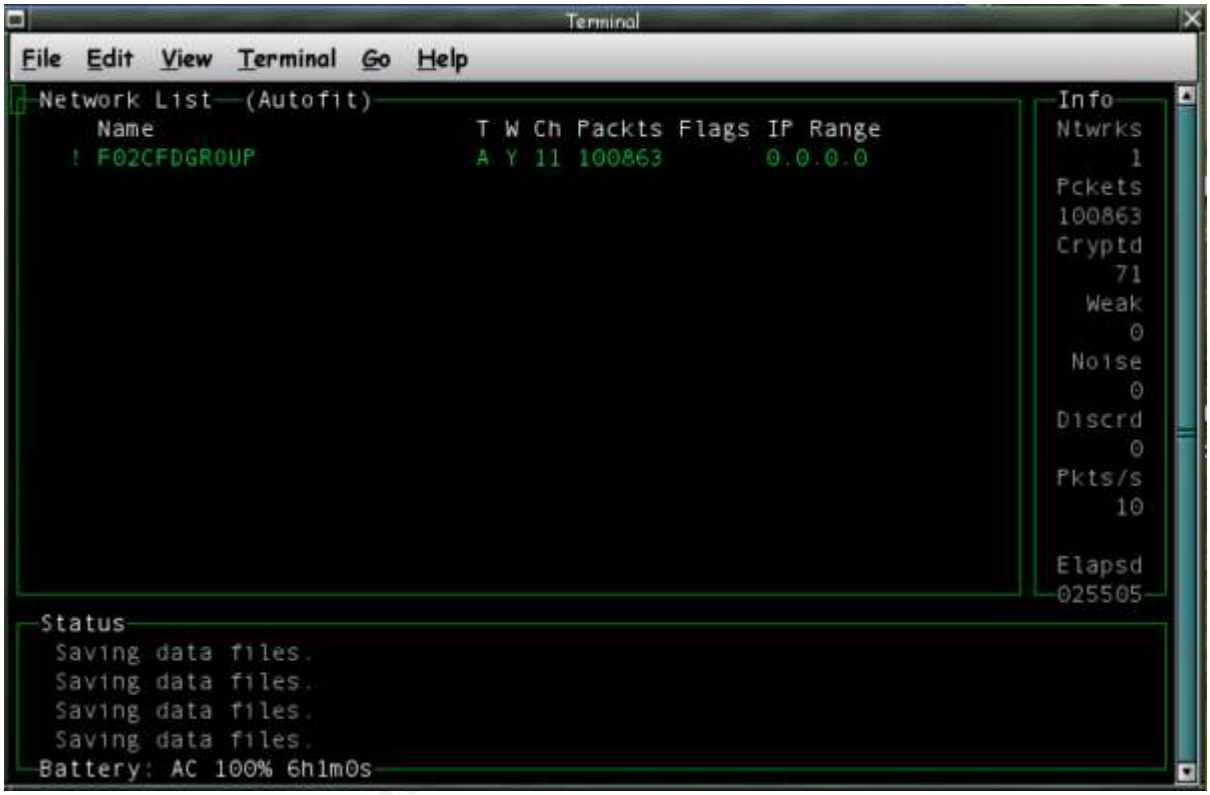
```
lafargue 85>su
Password:
~# kismet_monitor_cisco
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
Using /usr/local/etc/kismet.conf sources...
Enabling monitor mode for a cisco card on wifi0
Modifying device eth1
~#
```

This will put the Cisco LMC-350 in RF monitoring mode.

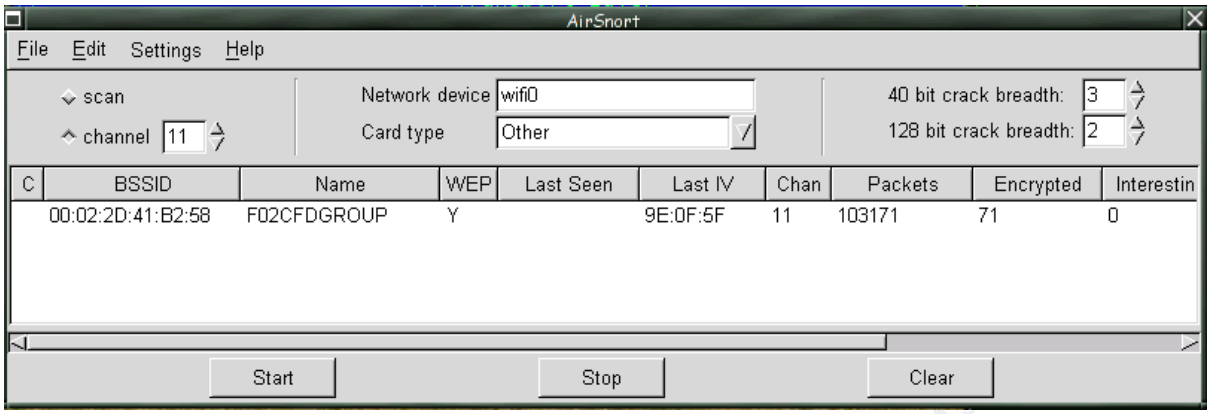
The next step is to launch “Kismet”. For security reasons, kismet will only accept to be run using non-root privileges. From a terminal with non-root privileges, type “kismet”:



Kismet will immediately start to detect the presence of Access Points.

Next, launch “airsnort”, which will work at detecting WEP keys. Airsnort needs root privileges. Launch it from a terminal, and choose “wifi0” and “other” as the card type, as RF monitoring is already enabled at this stage. Once airsnort is launched, it should start to detect the same APs as kismet, and will work at decoding the WEP keys.

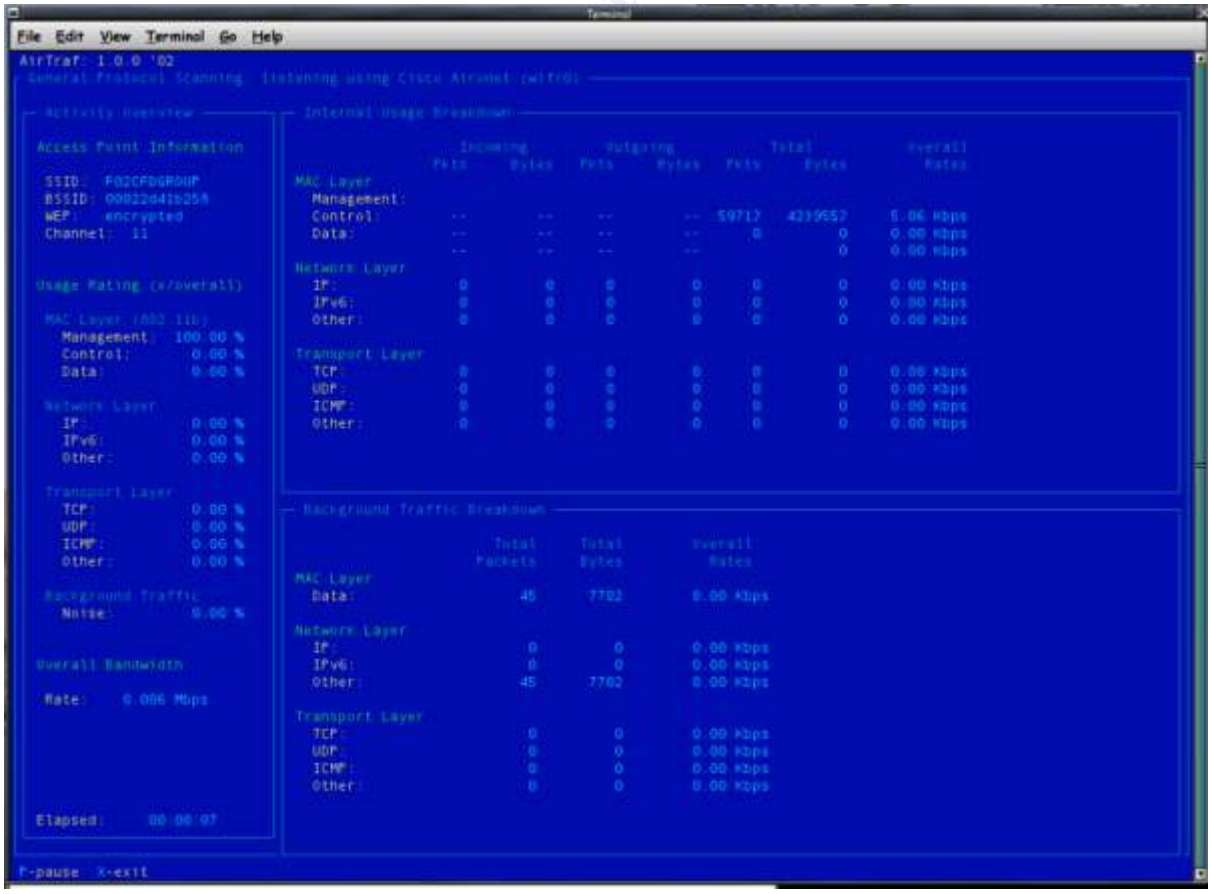
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



The last program to launch is “airtraf”. With the current Linux aironet drivers, Airtraf needs to be manually told what interface to use for traffic capture. From a terminal with root privileges, type:

```
#airtraf -C aironet -I wifi0
```

This will launch airtraf. From the main menu, choose “Scan Channels for AP Activity”, which will enable you to select the AP that needs to be monitored. Once the AP is selected, various screens will enable performance monitoring:



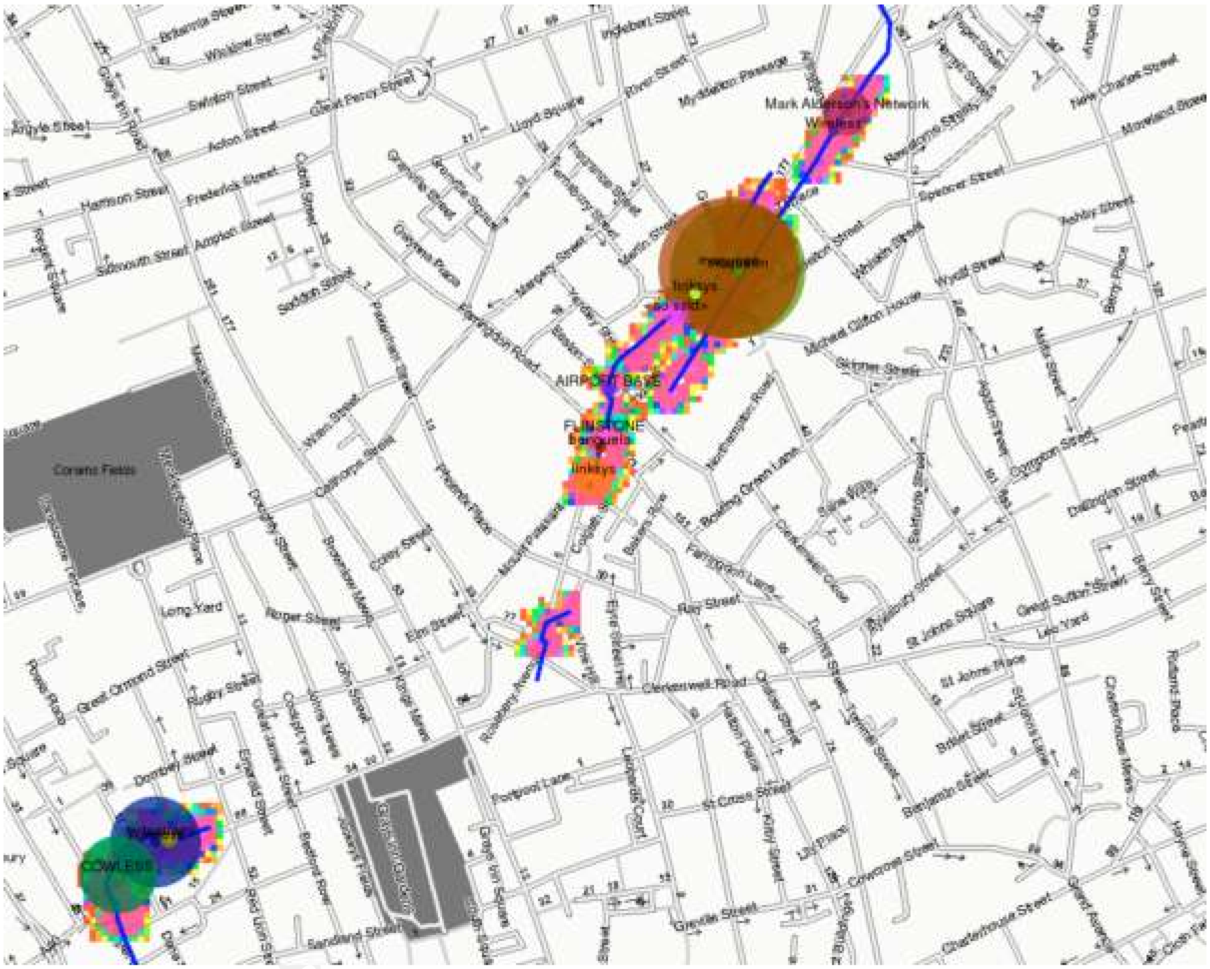
The above airtraf screen shows general network statistics for the currently selected

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

AP.

Mapping

Below is an example of a map that was generated from actual wardriving results in London in mid 2002.



This map shows the theoretical coverage area of access points (in brown, blue and green), and also the interpolated real power levels as received on the WiFi monitor during the drive. This map was generated from Kismet results using the “gpsmap” program included with Kismet.

The basemap was automatically downloaded by gpsmap from online map servers. This shows a concrete example of the kind of mapping that can be realized using the tools described in this setup.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Acronyms

AP: Access Point

WiFi: “Wireless Fidelity”, marketing name of the 802.11b standard

WEP: Wire-Equivalent privacy

SSID: Service Set Identifier.

GPS: Global Positioning System

CDP: Cisco Discovery Protocol

© SANS Institute 2003, Author retains full rights

References

[IDS1]
Wright, Joshua, "**Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection**" http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf (March 2003)

[KISMET1]
Kershaw, Mike **, "KISMET 2.8.0"** http://www.kismetwireless.net/documentation.shtml (march 2003)

[ITWORLD1]
ITWorld, "Test tools ease wireless LAN implementations", 1/27/01" http://www.itworld.com/Comp/1608/ITW-Geier_20010127/index.html (March 2003)

[ETHEREAL1]
"The Ethereal Network Analyzer", www.ethereal.com (March 2003)

[cathedral1]
Raymond, Eric S, "The Cathedral and the Bazaar", O'Reilly, 2001, ISBN 0596001088

[consume1]
"Consume.net" http://www.consume.net/ (March 2003)

[nycwireless1]
"NYC Wireless" http://www.nycwireless.net/ (March 2003)

[wlansec1]
Geir, Jim, "802.11 WEP: Concepts and Vulnerability" http://www.80211-planet.com/tutorials/article.php/1368661 (March 2003)

[wlansec2]
Janszen, Eric, "Understanding Basic WLAN Security Issues" http://www.80211-planet.com/tutorials/article.php/953561 (March 2003)

[wlansec3]
Adam Stubblefield , John Ioannidis, Aviel D. Rubin
"Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", August 2001, http://www.cs.rice.edu/~astubble/wep/ (March 2003)

[sniffer2]
Press Release, "Network Associates Secures High-Speed Wireless Networks With Sniffer(R) Wireless" http://www.sniffer.com/aboutus/press/pr_template.asp?PR=/PressMedia/12092002.asp&Sel=1426 (March 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[issa1]
Doten, Rick, "The Rogue Access Point: A Threat to Wired and Wireless Networks" http://www.issa-ne.org/documents/ISSARogueAPpresentationBoston.ppt (March 2003)

[cert1]
Cert Advisories, http://www.cert.org/advisories/ (March 2003)

[wardriving1]
"Wardriving.com", http://www.wardriving.com/ (March 2003)

[wlanhack1]
Dornan, Andy, "Wireless network analyzers, the Ultimate Hacking tool?", 05 March 2003,
http://www.networkmagazine.com/article/NMG20030305S0001/1 (March 2003)

[wardriving2]
"wireless web portal - security, PDA and mobile, wardriving, themes, networking and HOWTO." http://www.wardriving.info/ (March 2003)

[80211planet]
"801.11 Planet" http://www.80211-planet.com/ (March 2003)

[willtek1]
"9101 Handheld Spectrum Analyzer",
http://www.willtek.com/2_products_services/21_products/product_pages/General_purpose_productsw/9100_HSA (March 2003)

[wtelco1]
"Wireless Sniffer" http://www.personaltelco.net/index.cgi/WirelessSniffer (March 2003)

[simply1]
"Site Survey, Network Design and Project Management"
http://www.simplywireless.com.au/sitesurvey.htm (March 2003)

[WLANBIT1]
"WLANBIT, Products"
http://www.wlanbit.com/products.html (March 2003)

[microwave1]
Intersil Corporation, "Effects of Microwave Interference On IEEE 802.11 WLAN Reliability", May 1998, http://www.wlana.org/learn/microreliab.pdf (March 2003)

[microwave2]
Ad Kamerman, Nedim Erkocevic , "Microwave Oven Interference on Wireless LANs Operating in the 2.4 GHz ISM Band",
http://infotooth.tripod.com/documents/Microwave_Oven_Interference_on_Wireless_L

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ANs_Operating_in_the_2.4_GHz_ISM_Band.pdf (March 2003)

[debian1]
"Debian/GNU Linux --- The Universal Operating System", http://www.debian.org/ (March 2003)

[airsnort1]
"AirSnort Homepage", http://airsnort.shmoo.com/ (March 2003)

[airtraf1]
"Network Security Management Solutions for Wired and Wireless Networks" http://www.elixar.com/ (March 2003)

[aptools1]
"AP Tools" http://aptools.sourceforge.net/ (March 2003)

[airmagnet1]
"AirMagnet Company Site" http://www.airmagnet.com/ (March 2003)

[airopeek1]
"Wildpacket Company Site" http://www.wildpackets.cm/ (March 2003)

[lanfielder1]
"Wireless Valley Communications" http://www.wirelessvalley.com/ (March 2003)

[baseband1]
"Baseband Technologies" http://www.baseband.com/ (March 2003)

[solwise1]
"Solwise Ltd" http://www.solwise.co.uk/ (March 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced