

## WIRELESS SECURITY

---

As wireless devices continue to proliferate, Mandiant has raised the bar of wireless network detection and investigation by introducing our Wireless Investigations class. This two-day intensive hands-on class has been specifically designed for information security professionals and analysts who support wireless environments. It is designed as an operational course using case studies and hands-on lab exercises to ensure attendees are gaining experience in each topic area.

<b>Duration</b>	2 days
<b>Who Should Attend</b>	Information technology staff, information security staff, corporate investigators, or other staff who have a need to perform security audits on their wireless infrastructures.
<b>Prerequisites</b>	Students should have a basic understanding of TCP/IP networks and some familiarity with Windows and UNIX systems. Familiarity with computer security terminology and concepts is helpful.
<b>Students Will Learn</b>	<ul style="list-style-type: none"><li>▪ How to find, identify and access wireless access points using freely available tools in Windows and UNIX operating systems</li><li>▪ Techniques for identifying “cloaked” or non-broadcasting access points will be utilized leading students to breach common security features</li><li>▪ That weaknesses in the WEP algorithm allow skilled attackers to accelerate their attacks against WEP – Students will be provided with the tools and first-hand experience in this process</li><li>▪ Brute force attacks against WPA-PSK can be undertaken using similar tools once the initial handshake is captured</li><li>▪ Methods to “force” an authorized client to disassociate, thus allowing capture of the initial handshake</li><li>▪ That wireless access points typically are not as well protected or managed as other access mechanisms to most environments, and how they can be used as a stepping-stones for attackers</li><li>▪ How to identify a target network, crack the WEP key in use, brute force their way into an administrative role on the access point, and use the network access as an attack vector against “wired” systems on the same network</li></ul>
<b>Exercises</b>	<ul style="list-style-type: none"><li>▪ Wireless Case Studies</li><li>▪ Getting Running</li><li>▪ Hardware &amp; Software</li><li>▪ Wireless Technologies</li><li>▪ Search &amp; Seizure</li><li>▪ Network Exploitation</li></ul>
<b>Course Materials</b>	<ul style="list-style-type: none"><li>▪ Student manual</li><li>▪ Class handouts</li><li>▪ MANDIANT gear</li><li>▪ Free Tools CD with course tools and scripts</li></ul>
<b>Suggested Next Courses</b>	<ul style="list-style-type: none"><li>▪ Network Traffic Analysis</li><li>▪ Linux for Security Professionals</li><li>▪ Incident Response</li></ul>
<b>Contact</b>	1.800.647.7020 <a href="mailto:education@mandiant.com">education@mandiant.com</a> <a href="http://www.mandiant.com/education.htm">www.mandiant.com/education.htm</a>

**Case Study 1**

- Students will be presented with a recent case study demonstrating how a large retailer's wireless network was used by hackers in an attempt to gather credit card transactions

**Getting Started**

- Students will be shown how to bring their systems up on the classroom wireless network in both the Windows and UNIX environments
- Customized shell scripts which automatically create the appropriate environment in UNIX will also be discussed briefly

**Wireless Hardware and Software**

- Students will learn the most common components of a wireless attack kit including the hardware & software utilized
- The deadly combination of PDA devices to covertly scan and identify wireless networks and laptop systems to perform the actual data capture/attack will be discussed including the tools available for both platforms
- Wireless network adaptors and the chipsets present will be discussed in length, with a focus on those chipsets that provide the prerequisite compatibility to be used in a wireless attack environment
- Students will learn how power is determined in a wireless environment, and how differing types of antennas can be used to broaden the radius of wireless access or pinpoint wireless traffic towards a specific access point

**Wireless Technologies**

- Students will learn about the different types of wireless networks they may encounter along with each networks' strengths and weaknesses
- The access mechanisms for open and closed networks will be discussed
- How commonly used security mechanisms on most access points can be easily bypassed or subverted
- Use of Wireshark to capture wireless traffic, including the specific display filters to wireless specific traffic

**Target Recon**

- Students will learn common search methods and using the methods and tools provided, hunt out and discover a number of "rogue" access points
- Both active and passive identification techniques will be employed
- Kismet will be utilized initially by the students to identify the available access points, the MAC addresses of the access point and clients, and the channel which each access point utilizes as a prelude in launching an accelerated attack against WEP

**Case Study 2**

- The details surrounding a recent case involving spoofed emails sent via a wardriving hacker with a vendetta against a particular company
- How the intruder gathered sufficient insider information to forge the emails using a variety of techniques including gaining unauthorized access to the companies network and dumpster diving

**Search and Seizure**

- The default configuration and logging mechanisms for a variety of typical wireless access points will be discussed and later used within class to attempt to gain access to a protected access point
- The importance of gathering the volatile data from wireless devices due to the lack of long term storage in regards to logs and connected device information

**Network Exploitation**

- The WEP encryption process will be discussed along with the inherent shortcomings which allow attacks to "shortcut" their attacks against WEP
- Students will use a variety of first, second and third generation hacking utilities to attempt to crack WEP encrypted network traffic
- Capturing of WEP and clear (non protected) wireless traffic will be accomplished using a variety of tools, and the contents displayed
- Once a WEP key is cracked, students will use this information and apply it to pre-captured wireless traffic to extract all of the content in clear text
- Using the broken WEP key, students will connect to a protected network and launch a brute force attack against the access points in order to take administrative control
- As a connected device, students will also launch attacks against wired devices within the internal network