COURSE TECHNOLOGY
CENGAGE Learning

EC-Council | Press

Computer Forensics
Investigating Wireless Networks and Devices

Volume 5 of 5 mapping to

C|HFI™
Computer Hacking Forensic INVESTIGATOR
Certification

COURSE TECHNOLOGY
CENGAGE Learning

EC-Council | Press

The Experts: EC-Council

EC-Council's mission is to address the need for well educated and certified information security and e-business practitioners. EC-Council is a global, member based organization comprised of hundreds of industry and subject matter experts all working together to set the standards and raise the bar in Information Security certification and education.

EC-Council certifications are viewed as the essential certifications needed where standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are securing networks around the world and beating the hackers at their own game.

The Solution: EC-Council Press

The EC-Council | Press marks an innovation in academic text books and courses of study in information security, computer forensics, disaster recovery, and end-user security. By repurposing the essential content of EC-Council's world class professional certification programs to fit academic programs, the EC-Council | Press was formed.

With 8 Full Series, comprised of 27 different books, the EC-Council | Press is set to revolutionize global information security programs and ultimately create a new breed of practitioners capable of combating this growing epidemic of cybercrime and the rising threat of cyber war.

This Certification: C|HFI – Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. The C|HFI materials will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute.

Security|5
Security|5 is an entry level certification for anyone interested in learning computer networking and security basics. Security|5 means 5 components of IT security: firewalls, anti-virus, IDS, networking, and web security.

Wireless|5
Wireless|5 introduces learners to the basics of wireless technologies and their practical adaptation. Learners are exposed to various wireless technologies; current and emerging standards; and a variety of devices.

Network|5
Network|5 covers the 'Alphabet Soup of Networking' – the basic core knowledge to know how infrastructure enables a work environment, to help students and employees succeed in an integrated work environment.

Additional Certifications Covered By EC-Council Press:

E|DRP – EC-Council
Disaster Recovery Professional
E|DRP covers disaster recovery topics, including identifying vulnerabilities, establishing policies and roles to prevent and mitigate risks, and developing disaster recovery plans.

C|EH - Certified Ethical Hacker
Information assets have evolved into critical components of survival. The goal of the Ethical Hacker is to help the organization take pre-emptive measures against malicious attacks by attacking the system himself or herself; all the while staying within legal limits.

E|NSA – EC-Council
Network Security Administrator
The E|NSA program is designed to provide fundamental skills needed to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information.

E|CSA - EC-Council Certified Security Analyst
The objective of E|CSA is to add value to experienced security professionals by helping them analyze the outcomes of their tests. It is the only in-depth Advanced Hacking and Penetration Testing certification available that covers testing in all modern infrastructures, operating systems, and application environments.

Investigating Wireless Networks and Devices

EC-Council | Press

Volume 5 of 5 mapping to

C | HFI™

Computer | Hacking Forensic INVESTIGATOR

Certification

COURSE TECHNOLOGY
CENGAGE Learning™

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

COURSE TECHNOLOGY
CENGAGE Learning™

Investigating Wireless Networks and Devices: EC-Council | Press

Course Technology/Cengage Learning Staff:

Vice President, Career and Professional Editorial: Dave Garza

Director of Learning Solutions: Matthew Kane

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Editorial Assistant: Meghan Orvis

Vice President, Career and Professional Marketing: Jennifer Ann Baker

Marketing Director: Deborah Yarnell

Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Content Project Manager: Brooke Greenhouse

Senior Art Director: Jack Pendleton

EC-Council:

President | EC-Council: Sanjay Bavisi

Sr. Director US | EC-Council: Steven Graham

Library of Congress Control Number: 2009933551

ISBN-13: 978-1-4354-8353-8

ISBN-10: 1-4354-8353-7

Cengage Learning
5 Maxwell Drive
Clifton Park, NY 12065-2919
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **international.cengage.com/region**

Cengage Learning products are represented in Canada by
Nelson Education, Ltd.

For more learning solutions, please visit our corporate website at **www.cengage.com**

Printed in the United States of America
1 2 3 4 5 6 7 12 11 10 09

Brief Table of Contents

This page intentionally left blank

Table of Contents

This page intentionally left blank

Preface

Hacking and electronic crimes sophistication has grown at an exponential rate in recent years. In fact, recent reports have indicated that cyber crime already surpasses the illegal drug trade! Unethical hackers, better known as *black hats,* are preying on information systems of government, corporate, public, and private networks and are constantly testing the security mechanisms of these organizations to the limit with the sole aim of exploiting them and profiting from the exercise. High-profile crimes have proven that the traditional approach to computer security is simply not sufficient, even with the strongest perimeter, properly configured defense mechanisms such as firewalls, intrusion detection, and prevention systems, strong end-to-end encryption standards, and anti-virus software. Hackers have proven their dedication and ability to systematically penetrate networks all over the world. In some cases, black hats may be able to execute attacks so flawlessly that they can compromise a system, steal everything of value, and completely erase their tracks in less than 20 minutes!

The EC-Council Press is dedicated to stopping hackers in their tracks.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization comprised of industry and subject matter experts all working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the *Certified Ethical Hacker* (C|EH) program. The goal of this program is to teach the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge from hundreds of subject matter experts, the C|EH program has rapidly gained popularity around the globe and is now delivered in more than 70 countries by more than 450 authorized training centers. more than 60,000 information security practitioners have been trained.

C|EH is the benchmark for many government entities and major corporations around the world. Shortly after C|EH was launched, EC-Council developed the *Certified Security Analyst* (E|CSA). The goal of the E|CSA program is to teach groundbreaking analysis methods that must be applied while conducting advanced penetration testing. The E|CSA program leads to the *Licensed Penetration Tester* (L|PT) status. The *Computer Hacking Forensic Investigator* (C|HFI) was formed with the same design methodologies and has become a global standard in certification for computer forensics. EC-Council, through its impervious network of professionals and huge industry following, has developed various other programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are securing networks around the world and beating the hackers at their own game.

About the EC-Council | Press

The EC-Council | Press was formed in late 2008 as a result of a cutting-edge partnership between global information security certification leader, EC-Council and leading global academic publisher, Cengage Learning. This partnership marks a revolution in academic textbooks and courses of study in information security, computer forensics, disaster recovery, and end-user security. By identifying the essential topics and content of EC-Council professional certification programs, and repurposing this world-class content to fit academic programs, the EC-Council | Press was formed. The academic community is now able to incorporate this powerful cutting-edge content into new and existing Information Security programs. By closing the gap between academic study and professional certification, students and instructors are able to leverage the power of rigorous academic focus and high demand industry certification. The EC-Council | Press is set to revolutionize global information security programs and ultimately create a new breed of practitioners capable of combating the growing epidemic of cybercrime and the rising threat of cyber-war.

Computer Forensics Series

The EC-Council | Press Computer Forensics Series, preparing learners for C|HFI certification, is intended for those studying to become police investigators and other law enforcement personnel, defense and military personnel, e-business security professionals, systems administrators, legal professionals, banking, insurance and other professionals, government agencies, and IT managers. The content of this program is designed to expose the learner to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Advanced techniques in computer investigation and analysis with interest in generating potential legal evidence are included. In full, this series prepares the learner to identify evidence in computer-related crime and abuse cases as well as track the intrusive hacker's path through client system.

Books in Series

- *Computer Forensics: Investigation Procedures and Response*/1435483499
- *Computer Forensics: Investigating Hard Disks, File and Operating Systems*/1435483502
- *Computer Forensics: Investigating Data and Image Files*/1435483510
- *Computer Forensics: Investigating Network Intrusions and Cybercrime*/1435483529
- *Computer Forensics: Investigating Wireless Networks and Devices*/1435483537

Investigating Wireless Networks and Devices

Investigating Wireless Networks and Devices discusses how to investigate wireless attacks, as well as PDA, iPod, iPhone, and BlackBerry forensics.

Chapter Contents

Chapter 1, *Investigating Wireless Attacks*, discusses various types of wireless technologies available, the types of attacks launched against them, and how to investigate these attacks. Chapter 2, *PDA Forensics*, provides an understanding of what is stored on PDAs and the associated security issues. It also includes a discussion on PDA forensic tools and how to implement countermeasures. Chapter 3, *iPod and iPhone Forensics*, focuses on how data stored on these devices and this data can be retrieved. Chapter 4, *BlackBerry Forensics*, discusses how the device works, ways to increase its security, and what to do if it must be taken as evidence.

Chapter Features

Many features are included in each chapter and all are designed to enhance the learner's learning experience. Features include:

- *Objectives* begin each chapter and focus the learner on the most important concepts in the chapter.
- *Key Terms* are designed to familiarize the learner with terms that will be used within the chapter.
- *Case Examples*, found throughout the chapter, present short scenarios followed by questions that challenge the learner to arrive at an answer or solution to the problem presented.
- *Chapter Summary*, at the end of each chapter, serves as a review of the key concepts covered in the chapter.
- *Review Questions* allow learners to test their comprehension of the chapter content.
- *Hands-On Projects* encourage learners to apply the knowledge they have gained after finishing the chapter. Files for the Hands-On Projects can be found on the Student Resource Center. Note: You will need your access code provided in your book to enter the site. Visit *www.cengage.com/community/eccouncil* for a link to the Student Resource Center.

Student Resource Center

The Student Resource Center contains all the files you need to complete the Hands-On Projects found at the end of the chapters. Access the Student Resource Center with the access code provided in your book. Visit *www.cengage.com/community/eccouncil* for a link to the Student Resource Center.

Additional Instructor Resources

Free to all instructors who adopt the *Investigating Wireless Networks and Devices* book for their courses is a complete package of instructor resources. These resources are available from the Course Technology Web site, *www.cengage.com/coursetechnology,* by going to the product page for this book in the online catalog, and choosing "Instructor Downloads."

Resources include:

- *Instructor Manual*: This manual includes course objectives and additional information to help your instruction.
- *ExamView Testbank*: This Windows-based testing software helps instructors design and administer tests and pre-tests. In addition to generating tests that can be printed and administered, this full-featured program has an online testing component that allows students to take tests at the computer and have their exams automatically graded.
- *PowerPoint Presentations*: This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as teaching aids for classroom presentations, to be made available to students for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides.
- *Labs*: These are additional hands-on activities to provide more practice for your students.
- *Assessment Activities*: These are additional assessment opportunities including discussion questions, writing assignments, Internet research activities, and homework assignments along with a final cumulative project.
- *Final Exam*: This exam provides a comprehensive assessment of *Investigating Wireless Networks and Devices* content.

Cengage Learning Information Security Community Site

Cengage Learning Information Security Community Site was created for learners and instructors to find out about the latest in information security news and technology.

Visit *community.cengage.com/infosec* to:

- Learn what's new in information security through live news feeds, videos and podcasts;
- Connect with your peers and security experts through blogs and forums;
- Browse our online catalog.

How to Become C|HFI Certified

Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. The C|HFI certification focuses on the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. The C|HFI certification is primarily targeted at police and other law enforcement personnel, defense and military personnel, e-business security professionals, systems administrators, legal professionals, banking, insurance and other professionals, government agencies, and IT managers. This certification will ensure that you have the knowledge and skills to identify, track, and prosecute the cyber-criminal.

C|HFI certification exams are available through authorized Prometric TESTING CENTERS. To finalize your certification after your training by taking the certification exam through a Prometric testing center, you must:

1. Apply for and purchase an exam voucher by visiting the EC-Council Press community site: *www.cengage.com/community/eccouncil,* if one was not purchased with your book.
2. Once you have your exam voucher, visit *www.prometric.com* and schedule your exam, using the information on your voucher.

C|HFI certification exams are also available through Prometric Prime. To finalize your certification after your training by taking the certification exam through Prometric Prime, you must:

1. Purchase an exam voucher by visiting the EC-Council Press community site: *www.cengage.com/community/eccouncil*, if one was not purchased with your book.
2. Speak with your instructor about scheduling an exam session, or visit the EC-Council community site referenced above for more information.
3. Take and pass the C|HFI certification examination with a score of 70% or better.

Other EC-Council | Press Products

Ethical Hacking and Countermeasures Series

The EC-Council | Press *Ethical Hacking and Countermeasures* series is intended for those studying to become security officers, auditors, security professionals, site administrators, and anyone who is concerned about or responsible for the integrity of the network infrastructure. The series includes a broad base of topics in offensive network security, ethical hacking, as well as network defense and countermeasures. The content of this series is designed to immerse learners into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, ethical hackers are able to set up strong countermeasures and defensive systems to protect their organization's critical infrastructure and information. The series, when used in its entirety, helps prepare readers to take and succeed on the C|EH certification exam from EC-Council.

Books in Series
- *Ethical Hacking and Countermeasures: Attack Phases*/143548360X
- *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms*/1435483618
- *Ethical Hacking and Countermeasures: Web Applications and Data Servers*/1435483626
- *Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems*/1435483642
- *Ethical Hacking and Countermeasures: Secure Network Infrastructures*/1435483650

Network Security Administrator Series

The EC-Council | Press *Network Administrator* series, preparing learners for E|NSA certification, is intended for those studying to become system administrators, network administrators and anyone who is interested in network security technologies. This series is designed to educate learners, from a vendor neutral standpoint, how to defend the networks they manage. This series covers the fundamental skills in evaluating internal and external threats to network security, design, and how to enforce network level security policies, and ultimately protect an organization's information. Covering a broad range of topics from secure network fundamentals, protocols and analysis, standards and policy, hardening infrastructure, to configuring IPS, IDS and firewalls, bastion host and honeypots, among many other topics, learners completing this series will have a full understanding of defensive measures taken to secure their organizations' information. The series, when used in its entirety, helps prepare readers to take and succeed on the E|NSA, Network Security Administrator certification exam from EC-Council.

Books in Series
- *Network Defense: Fundamentals and Protocols*/1435483553
- *Network Defense: Security Policy and Threats*/1435483561
- *Network Defense: Perimeter Defense Mechanisms*/143548357X
- *Network Defense: Securing and Troubleshooting Network Operating Systems*/1435483588
- *Network Defense: Security and Vulnerability Assessment*/1435483596

Security Analyst Series

The EC-Council | Press *Security Analyst/Licensed Penetration Tester* series, preparing learners for E|CSA/LPT certification, is intended for those studying to become network server administrators, firewall administrators, security testers, system administrators and risk assessment professionals. This series covers a broad base of topics in advanced penetration testing and security analysis. The content of this program is designed to expose the learner to groundbreaking methodologies in conducting thorough security analysis, as well as advanced

penetration testing techniques. Armed with the knowledge from the *Security Analyst* series, learners will be able to perform the intensive assessments required to effectively identify and mitigate risks to the security of the organizations infrastructure. The series, when used in its entirety, helps prepare readers to take and succeed on the E|CSA, Certified Security Analyst, and L|PT, License Penetration Tester certification exam from EC-Council.

Books in Series
- *Certified Security Analyst: Security Analysis and Advanced Tools*/1435483669
- *Certified Security Analyst: Customer Agreements and Reporting Procedures in Security Analysis*/1435483677
- *Certified Security Analyst: Penetration Testing Methodologies in Security Analysis*/1435483685
- *Certified Security Analyst: Network and Communication Testing Procedures in Security Analysis*/1435483693
- *Certified Security Analyst: Network Threat Testing Procedures in Security Analysis*/1435483707

Cyber Safety/1435483715

Cyber Safety is designed for anyone who is interested in learning computer networking and security basics. This product provides information cyber crime; security procedures; how to recognize security threats and attacks, incident response, and how to secure Internet access. This book gives individuals the basic security literacy skills to begin high-end IT programs. The book also prepares readers to take and succeed on the Security|5 certification exam from EC-Council.

Wireless Safety/1435483766

Wireless Safety introduces the learner to the basics of wireless technologies and its practical adaptation. *Wireless|5* is tailored to cater to any individual's desire to learn more about wireless technology. It requires no pre-requisite knowledge and aims to educate the learner in simple applications of these technologies. Topics include wireless signal propagation, IEEE and ETSI wireless standards, WLANs and operation, wireless protocols and communication languages, wireless devices, and wireless security networks. The book also prepares readers to take and succeed on the Wireless|5 certification exam from EC-Council.

Network Safety/1435483774

Network Safety provides the basic core knowledge on how infrastructure enables a working environment. It is intended for those in office environments and home users who wants to optimize resource utilization, share infrastructure, and make the best of technology and the convenience it offers. Topics include foundations of networks, networking components, wireless networks, basic hardware components, the networking environment and connectivity as well as troubleshooting. The book also prepares readers to take and succeed on the Network|5 certification exam from EC-Council.

Disaster Recovery Professional

The *Disaster Recovery Professional* series, preparing the reader for E|DRP certification, introduces the learner to the methods employed in identifying vulnerabilities and how to take the appropriate countermeasures to prevent and mitigate failure risks for an organization. It also provides a foundation in disaster recovery principles, including preparation of a disaster recovery plan, assessment of risks in the enterprise, development of policies, and procedures, and understanding of the roles and relationships of various members of an organization, implementation of the plan, and recovering from a disaster. Students will learn how to create a secure network by putting policies and procedures in place, and how to restore a network in the event of a disaster. The series, when used in its entirety, helps prepare readers to take and succeed on the E|DRP, Disaster Recovery Professional certification exam from EC-Council.

Books in Series
- *Disaster Recovery*/1435488709
- *Business Continuity*/1435488695

This page intentionally left blank

Acknowledgements

Michael H. Goldner is the Chair of the School of Information Technology for ITT Technical Institute in Norfolk Virginia, and also teaches bachelor level courses in computer network and information security systems. Michael has served on and chaired ITT Educational Services Inc. National Curriculum Committee on Information Security. He received his Juris Doctorate from Stetson University College of Law, his undergraduate degree from Miami University and has been working for more than 15 years in the area of information technology. He is an active member of the American Bar Association, and has served on that organization's cyber law committee. He is a member of IEEE, ACM, and ISSA, and is the holder of a number of industrially recognized certifications including, CISSP, CEH, CHFI, CEI, MCT, MCSE/Security, Security +, Network +, and A+. Michael recently completed the design and creation of a computer forensic program for ITT Technical Institute, and has worked closely with both EC-Council and Delmar/Cengage Learning in the creation of this EC-Council Press series.

This page intentionally left blank

Chapter 1

Investigating Wireless Attacks

Objectives

After completing this chapter, you should be able to:

- Understand wireless networking technologies
- Describe wireless attacks
- Hijack and modify a wireless network
- Describe the association of a wireless access point (WAP) and a device
- Perform network forensics in a wireless environment
- Enumerate the steps for investigating a wireless attack
- Describe active and passive wireless scanning techniques
- Describe the tools used to investigate wireless attacks
- Describe rogue access points and the tools used to detect them

Key Terms

Active attack a type of attack in which an attacker tries to alter or corrupt the data or services on a network

Passive attack a type of attack where an unauthorized user monitors communications to gather information

Warchalking a technique involving using chalk to place a special symbol on a sidewalk or another surface to indicate a nearby wireless network that offers Internet access

Wardriving a technique hackers use to locate insecure wireless networks while driving around

Warflying a technique hackers use to locate insecure wireless networks while flying around

Introduction to Investigating Wireless Attacks

This chapter focuses on investigating wireless attacks. It discusses the various types of wireless technologies available and the different types of attacks launched against them. It also covers how to investigate a wireless attack.

Wireless Networking Technologies

The growth of wireless networking technology has given rise to many security issues. Wireless technology has become popular because of its convenience and low cost. A wireless local area network (WLAN) allows workers to access digital resources without being tied to their desks. It is often cheaper and easier to set up a wireless network than to run cables throughout an organization's facilities. The following are some of the more prominent wireless networking technologies:

- Bluetooth
- Infrared
- Ultrawideband
- ZigBee
- Wireless USB
- Wi-Fi
- WiMAX
- Satellite

Wireless Attacks

There are various kinds of wireless attacks. The following are some methods hackers use to facilitate wireless attacks:

- *Wardriving*: ***Wardriving*** is a technique hackers use to locate insecure wireless networks while driving around.
- *Warflying*: Similar to wardriving, ***warflying*** involves flying around in an aircraft, looking for open wireless networks.
- *Warchalking*: ***Warchalking*** involves using chalk to place a special symbol on a sidewalk or another surface to indicate a nearby wireless network that offers Internet access.

Passive Attacks

A ***passive attack*** is a type of attack where an unauthorized user monitors communications to gather information. For example, eavesdropping on network traffic is a passive attack. An eavesdropper can easily seize the network traffic using tools such as Network Monitor, Tcpdump, or AirSnort.

Passive attacks are difficult to detect and identify. Passive attacks are often symmetric, meaning that the attacker can monitor the communication in both directions. Some other examples of passive attacks are traffic analysis and traffic monitoring.

Electronic Emanations

Electronic emanations are the electromagnetic waves of radiation that electronic devices emit during their operation. Wireless technology is subject to these emanations. An attacker can intercept the emanations and use them to figure out how to gain the proper credentials to join a wireless network. The major problem is that the administrator of the network cannot identify that the attacker has intercepted the signals.

Active Attacks

Active attacks on wireless networks are similar to those on wired networks, in which an attacker tries to alter or corrupt the data or services on a network. These types of attacks include flooding, spoofing, and unauthorized access. The information that an attacker collects during a successful passive attack can make it easier for him or her to actively attack a network.

Denial-Of-Service Attacks

Wireless systems are vulnerable to the same protocol-based DoS attacks that strike wired networks. They are also vulnerable to other types of DoS attacks, because the signals used to transmit data over the air can be easily disrupted. The main objective of DoS attacks is to deny access to network services and resources. It is difficult to track such attacks on wireless networks.

Modes of Attack DoS attacks have varied modes of attacks that include consumption, alteration, and physical destruction of network components or resources. The following are some common modes of attack:

- *Consumption of resources*: This involves consuming the resources a system needs, including the following:
  - *Bandwidth*: An intruder can redirect packets to the network in order to consume all of the available bandwidth on the network.
  - *Memory*: This is normally accomplished by saving unnecessary e-mails, causing intentional errors, or sharing unimportant files and folders.
- *Alteration of resources or information*: Altering the configuration of a machine can prevent a user from being able to use it.
- *Physical destruction of the computer/network elements*: This type of attack concerns the destruction of the physical elements, such as computers and routers.

Results of DoS Attacks The most significant loss due to these attacks is the time and money that an organization loses while the services are unavailable.

Flooding

The goal of flooding is to degrade the performance of the network by directing unnecessary packets of data toward it. This may result in a loss of connection requests or a complete denial of service. Flooding is a multicasting technique wherein packets from one source are directed toward multiple destinations on the network.

Man-In-The-Middle Attack

A man-in-the middle (MITM) attack is when an intruder accesses information being transmitted between the sender and the receiver. The transmission proves to be insecure because the information is not encrypted. In such cases, there is a possibility of the intruder altering the data.

The following are the two types of MITM attacks:

1. *Eavesdropping*: Eavesdropping is a passive attack technique. The attacker intercepts data being transmitted between one system and another. Security mechanisms such as IPSec, SSH, and SSL help prevent eavesdropping.
2. *Manipulation*: Manipulation is an extended step of eavesdropping. In this type of man-in-the-middle attack, the attacker manipulates the data that he or she intercepts. This manipulation can be done using a technique such as ARP poisoning.

Hijacking and Modifying a Wireless Network

In a wireless network, TCP/IP packets go through switches, routers, and wireless access points. Each device looks at the destination IP address and checks for that address in its table of local IP addresses. This table is dynamically built up from traffic that passes through the device and from Address Resolution Protocol (ARP) notifications from devices joining the network. If the destination IP address is not in the device's table, it passes the address off to its default gateway.

However, there is no authentication or verification of the validity of a packet that a device receives. A malicious user can send messages to routing devices and access points stating that his or her MAC address is associated with a known IP address. All traffic that goes through those devices that is intended for the hijacked IP address will instead go to the malicious user's machine.

Association of a Wireless Access Point and a Device

A wireless access point (WAP) is a node configured to allow wireless devices to access the local area network (LAN). WAPs are just plugged into a switch or into an Ethernet hub. An access point has its own range. When

two or more access points are in an environment, the range overlaps to provide roaming. The following two methods provide some level of security between a device and the WAP with which it is associated:

1. *MAC filtering*: The media access control (MAC) address is the 12-character (48 bits written in hexadecimal notation) unique hardware address of a particular system. The MAC address is used in the data-link layer of the network. MAC filtering is used to restrict unauthorized users. Only those devices with MAC addresses on the WAP's white list are allowed access to the network.
2. *Preshared key (PSK) or use of encryption*: The wireless device and the access point use a shared secret key. A checksum is added to every packet transmitted over the network. If the packet is cracked, then the value of the checksum changes, and it is easy to identify the intrusion. The transmitting device creates a packet-concentrated vector that is combined with the key to encrypt the packet. At the receiving end, the same key is used to decrypt the packet.

Network Forensics in a Wireless Environment

The following are the steps involved in performing forensic investigations in a wireless environment:

1. Obtain a search warrant.
2. Identify wireless devices.
3. Document the scene and maintain the chain of custody.
4. Detect wireless connections.
5. Determine the wireless field's strength.
6. Map wireless zones and hot spots.
7. Connect to the wireless network.
8. Acquire and analyze wireless data.
9. Generate a report.

Obtain a Search Warrant

The investigator should ensure that the search warrant application addresses the on-site examination of all computers and wireless-related equipment. The investigator can perform forensic analysis only on those pieces of equipment specified in the warrant. He or she should be careful not to overlook wireless devices that are in range of a WAP but may not be in the same room.

Identify Wireless Devices

The investigator needs to identify all the different wireless devices connected to the network. He or she needs to check the physical locations of the following wireless hardware:

- Wireless routers
- Wireless access points
- Wireless modems
- Wireless network adapters
- Repeaters
- Hard drives
- Antennas

Searching for Additional Devices

To find additional wireless devices on the network that may not be readily apparent, the investigator can put his or her forensic laptop in promiscuous mode and send deauthentication packets using the Aireplay tool. This may force the active wireless equipment to reconnect to the default wireless access point, which will be redirected to the forensic laptop (since the laptop is running in promiscuous mode). Aireplay is a wireless assessment tool that injects specially crafted data packets into a wireless stream.

Detecting Wireless Access Points (WAPs)

The investigator can use the following techniques to find WAPs:

- *Manual detection*: For manual detection, the investigator has to configure some sort of mobile device such as a handheld PC or laptop. To detect WAPs, the investigator has to physically visit the area where a WAP is likely to be. He or she can then use techniques such as wardriving or warflying to detect the WAPs.
- *Active wireless scanning technique*: The active scanning technique involves broadcasting a probe message and waiting for a response from devices in the range. This technique identifies many WAPs but obviously cannot find those WAPs that do not respond to the probe message.
- *Passive wireless scanning technique*: The passive scanning technique identifies the presence of any wireless communication. Through this technique, an investigator can identify all active WAP connections, but he or she may not find a WAP that is not currently serving any devices.
- *Nessus vulnerability scanner*: The investigator can use Nessus to find WAPs by performing the following steps:
  - Update plug-in #11026 with the nessus-update-plugins command.
  - Choose plug-in #11026 in the General family of scans.
  - Enable a port scan for ports 1–100.
  - Disable the **Safe Checks** option.
  - Enable the **Enable Dependencies at Runtime** option.

Rogue Access Point

A rogue access point is an unauthorized access point in a wireless network. Attackers typically deploy these access points to sniff important data on the network. Attackers can also use rogue access points to hijack user sessions on the wireless network.

An investigator can detect a rogue access point by following two steps:

1. *Access point detection*: The investigator first needs to use one of the techniques for detecting a wireless access point to discover the access point on the network.
2. *Verifying whether or not the access point is a rogue access point*: After identifying the access point in the network, the next step is to verify whether or not the identified access point is a rogue access point. To tell whether an access point is authorized, the investigator has to check the following:
   - MAC
   - SSID
   - Vendor
   - Media type
   - Channel

Tools for Detecting Rogue Access Points

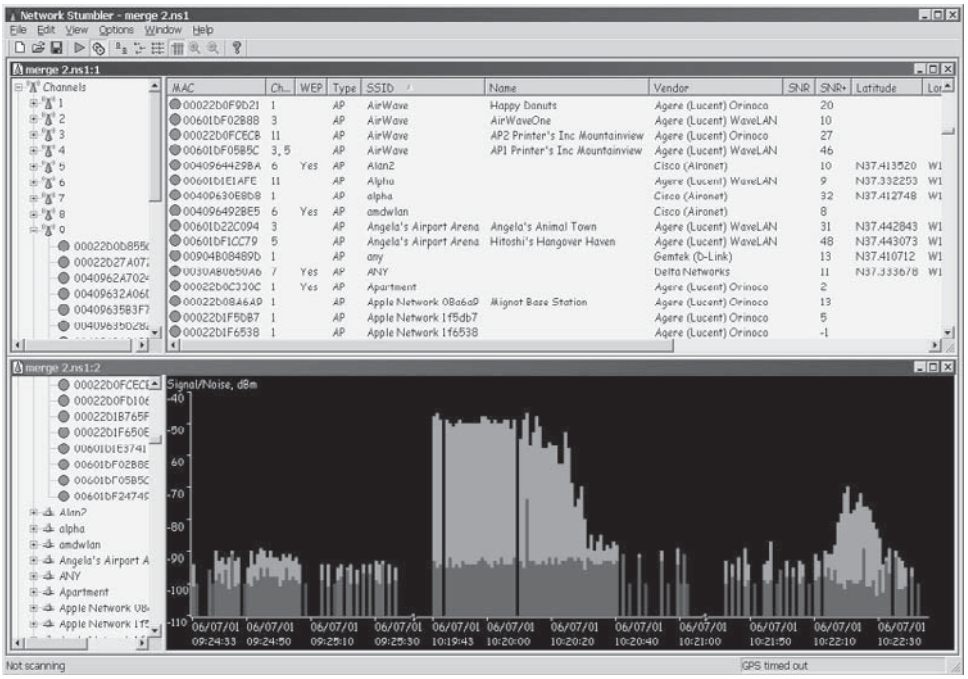
Network Stumbler and MiniStumbler are other tools that help investigators discover rogue access points.

Network Stumbler Network Stumbler (Figure 1-1) is a Windows utility that is often used for wardriving. It is a high-level WLAN scanner that operates by sending a steady stream of broadcast packets on all possible channels. Access points respond to the broadcast packets to verify their existence, even if beacons have been disabled.

Network Stumbler displays information about the access point, including the following:

- Signal-to-noise ratio
- MAC address
- SSID
- Channel details

A user can also connect to a GPS to find location information about any access points discovered.



Source: http://www.netstumbler.com/. Accessed 2/2007.

Figure 1-1 Network Stumbler displays information about the access points it discovers.

MiniStumbler MiniStumbler is the smaller sibling of Network Stumbler. It provides much of the same information as Network Stumbler, but is written for handheld devices running Pocket PC or Windows Mobile operating systems. Figure 1-2 shows a screenshot from MiniStumbler.

Document the Scene and Maintain the Chain of Custody

The investigator should do the following at the scene:

- Document all devices connected to the wireless network
- Take photographs of all evidence
- Document the state of each device during seizure
- Maintain the chain of custody of documents, photographs, and evidence

Detect Wireless Connections

The investigator can detect wireless connection using scanning tools such as the following:

- ClassicStumbler
- MacStumbler
- iStumbler
- Airport Signal
- Airfart
- Kismet

ClassicStumbler

ClassicStumbler scans for WAPs and displays information about each WAP within range. The information it displays includes the following:

- Signal strength
- Noise strength