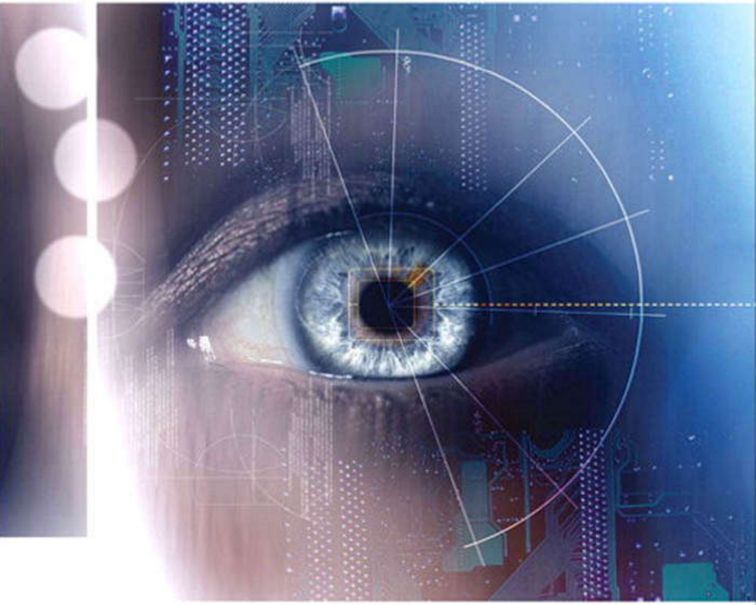


NETWORK DEFENSE AND COUNTERMEASURES:

PRINCIPLES AND PRACTICES

CHUCK EASTTOM

Network Defense and Countermeasures: Principles and Practices

Second Edition

Chuck Easttom

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Network Defense and Countermeasures: Practices and Principles, Second Edition

ISBN-13: 978-0-7897-5094-5
ISBN-10: 0-7897-5094-5

Library of Congress Control Number: 2013948636

Printed in the United States of America

First printing October 2013

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Bulk Sales

Pearson IT Certification offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearson.com

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Managing Editor
Sandra Schroeder

Project Editor
Seth Kerney

Copy Editor
Paula Lowell

Indexer
Heather McNeil

Proofreader
Jess DeGabriele

Technical Editor
Ronald Gonzales

Publishing Coordinator
Vanessa Evans

Interior Designer
Gary Adair

Cover Designer
Mark Shirar

Compositor
Studio Galou, LLC

Contents at a Glance

Table of Contents

About the Author

Chuck Easttom is a security consultant, author, and trainer. He has authored fourteen other books on programming, Web development, security, and Linux. Chuck holds more than 28 different industry certifications including CISSP, CEH, CHFI, ECSA, CIW Security Analyst, MCSE, MCSA, MCDBA, MCAD, Server+, and more. He has served as a subject matter expert for the Computer Technology Industry Association (CompTIA) in the development or revision of four of their certification tests, including the initial creation of their Security+ certification. He also developed the ECES cryptography certification for the EC Council.

Chuck is a frequent guest speaker for computer groups, discussing computer security. You can reach Chuck at his website (**www.chuckeasttom.com**) or by email at chuck@chuckeasttom.com

Dedication

This book is dedicated to all the people working in the computer security field, dillegently working to make computer networks safer.

Acknowledgments

While only one name goes on the cover of this book, it is hardly the work of just one person. I would like to take this opportunity to thank a few of the people involved. First of all, the editing staff at Pearson Certification worked extremely hard on this book. Without them this project would simply not be possible. I would also like to thank my wife, Teresa for all her support while working on this book. She is always very supportive in all my endeavors, a one woman support team!

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write us directly to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification/register for convenient access to any updates, downloads, or errata that might be available for this book.

Preface

The hottest topic in the IT industry today is computer security. The news is replete with stories of hacking, viruses, and identity theft. The cornerstone of security is defending the organizational network. *Network Defense and Countermeasures: Principles and Practices* offers a comprehensive overview of network defense. It introduces students to network security threats and methods for defending the network. Three entire chapters are devoted to firewalls and intrusion-detection systems. There is also a chapter providing a basic introduction to encryption. Combining information on the threats to networks, the devices and technologies used to ensure security, as well as concepts such as encryption provides students with a solid, broad-based approach to network defense.

This book provides a blend of theoretical foundations and practical applications. Each chapter ends with multiple choice questions, exercises, projects, and a case study. Students who successfully complete this textbook, including the end of chapter material, should have a solid understanding of network security. Throughout the book the student is directed to additional resources that can augment the material presented in the chapter.

Audience

This book is designed primarily as a textbook for students who have a basic understanding of how networks operate, including basic terminology, protocols, and devices. Students do not need to have an extensive math background or more than introductory computer courses.

Overview of the Book

This book will walk you through the intricacies of defending your network against attacks. It begins with a brief introduction to the field of network security in Chapter 1, "Introduction to Network Security." Chapter 2, "Types of Attacks" explains the threats to a network—including denial of service attacks, buffer overflow attacks, and viruses.

Chapter 3, "Fundamentals of Firewalls," Chapter 4, "Firewall Practical Applications," Chapter 5, "Intrusion-Detection Systems," and Chapter 7, "Virtual Private Networks," give details on various security technologies including firewalls, intrusion-detection systems, and VPNs. These items are the core of any network's security, so a significant portion of this book is devoted to ensuring the reader fully understands both the concepts behind them and the practical applications. In every case, practical direction for selecting appropriate technology for a given network is included.

Chapter 6, "Encryption Fundamentals," provides a solid introduction to encryption. This topic is critical because ultimately computer systems are simply devices for storing, transmitting, and manipulating data. No matter how secure the network is, if the data it transmits is not secure then there is a significant danger.

Chapter 8, “Operating System Hardening,” teaches operating system hardening. Chapter 9, “Defending Against Virus Attacks,” and Chapter 10, “Defending Against Trojan Horses, Spyware, and Adware,” give the reader specific defense strategies and techniques to guard against the most common network dangers. Chapter 11, “Security Policies,” gives readers an introduction to security policies.

Chapter 12, “Assessing System Security,” teaches the reader how to do an assessment of a network’s security. This includes guidelines for examining policies as well as an overview of network assessment tools. Chapter 13, “Security Standards,” gives an overview of common security standards such as the *Orange Book* and the Common Criteria. This chapter also discusses various security models such as Bell-Lapadula. Chapter 14, “Physical Security and Disaster Recovery,” examines the often-overlooked topic of physical security as well as disaster recovery, which is a key part of network security.

Chapter 15, “Techniques Used by Attackers,” provides the tools necessary to “know your enemy,” by examining basic hacking techniques and tools as well as strategies for mitigating hacker attacks. Chapter 16, “Introduction to Forensics,” helps you understand basic forensics principles in order to properly prepare for investigation if you or your company become the victim of a computer crime. Chapter 17, “Cyber Terrorism,” discusses computer-based espionage and terrorism, two topics of growing concern for the computer security community but often overlooked in textbooks.

Chapter 1

Introduction to Network Security

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Identify the most common dangers to networks.
- Understand basic networking.
- Employ basic security terminology.
- Find the best approach to network security for your organization.
- Evaluate the legal issues that will affect your work as a network administrator.
- Use resources available for network security.

Introduction

Finding a week without some major security breach in the news is difficult.[1, 2] University web servers hacked, government computers hacked, banks' data compromised, health information exposed—the list goes on. It also seems as if each year brings more focus to this issue. Finding anyone in any industrialized nation who had not heard of things such as websites being hacked and identities stolen would be difficult.

More venues for training also exist now. Many universities offer Information Assurance degrees from the bachelor's level up through the doctoral level. A plethora of industry certification training programs are availalbe, including the CISSP, EC Council's CEH, and CompTIA's Security+.

[1] Barnes & Nobles pin breach http://news.yahoo.com/b-n-pin-pad-tampering-sophisticated-crime-121531151--finance.html

[2] University Servers Hacked http://ca.news.yahoo.com/four-mcmaster-university-computer-servers-hacked-195747820.html

Despite this attention from the media and the opportunities to acquire security training, far too many computer professionals—including a surprising number of network administrators—do not have a clear understanding of the type of threats to which network systems are exposed, or which ones are most likely to actually occur. Mainstream media focuses attention on the most dramatic computer security breaches rather than giving an accurate picture of the most plausible threat scenarios.

This chapter looks at the threats posed to networks, defines basic security terminology, and lays the foundation for concepts covered in the chapters that follow. The steps required to ensure the integrity and security of your network are methodical and, for the most part, already outlined. By the time you complete this book, you will be able to identify the most common attacks, explain how they are perpetrated in order to prevent them, and understand how to secure your data transmissions.

The Basics of a Network

Before diving into how to protect your network, exploring what networks are would probably be a good idea. For many readers this section will be a review, but for some it might be new material. Whether this is a review for you, or new information, having a thorough understanding of basic networking before attempting to study network security is critical. Also be aware this is just a brief introduction to basic networking concepts. Many more details are not explored in this section.

A network is simply a way for computers to communicate. At the physical level, it consists of all the machines you want to connect and the devices you use to connect them. Individual machines are connected either with a physical connection (a category 5 cable going into a network interface card) or wirelessly. To connect multiple machines together, each machine must connect to a hub or switch, and then those hubs/switches must connect together. In larger networks, each subnetwork is connected to the others by a router. We look at many attacks in this book (including several in Chapter 2, "Types of Attacks") that focus on the devices that connect machines together on a network (that is, routers, hubs, and switches). If you find this chapter is not enough, this resource might assist you: http://compnetworking.about.com/od/basicnetworkingconcepts/Networking_Basics_Key_Concepts_in_Computer_Networking.htm

Basic Network Structure

Some connection point must exist between your network and the outside world. A barrier is set up between that network and the Internet, usually in the form of a firewall. Many attacks discussed in this book work to overcome the firewall and get into the network.

The real essence of networks is communication—allowing one machine to communicate with another. However, every avenue of communication is also an avenue of attack. The first step in understanding how to defend a network is having a detailed understanding of how computers communicate over a network.

The previously mentioned network interface cards, switches, routers, hubs, and firewalls are the fundamental physical pieces of a network. The way they are connected and the format they use for communication is the network architecture.

Data Packets

After you have established a connection (whether it is physical or wireless), you need to send data. The first part is to identify where you want to send it. All computers (as well as routers) have an IP address that is a series of four numbers between 0 and 255 and separated by periods, such as 192.0.0.5 (note that this is an IPV4 address). The second part is to format the data for transmission. All data is ultimately in binary form (1s and 0s). This binary data is put into packets, all less than about 65,000 bytes. The first few bytes are the header. That header tells where the packet is going, where it came from, and how many more packets are coming as part of this transmission. Some attacks that we will study (IP spoofing, for example) try to change the header of packets to give false information. Other methods of attack simply try to intercept packets and read the content (thus compromising the data).

IP Addresses

The first major issue to understand is how to get packets to their proper destination. Even a small network has many computers that could potentially be the final destination of any packet sent. The Internet has millions of computers spread out across the globe. How do you ensure that a packet gets to its proper destination? The problem is not unlike addressing a letter and ensuring it gets to the correct destination. Let’s begin by looking at IP version 4 addressing because it is the most common in use today, but this section also briefly discusses IP version 6.0.

An IP version 4.0 address is a series of four three-digit numbers separated by periods. (An example is 107.22.98.198.) Each of the three-digit numbers must be between 0 and 255. You can see that an address of 107.22.98.466 would not be a valid one. The reason for this rule is that these addresses are actually four binary numbers: The computer simply displays them to you in decimal format. Recall that a byte is 8 bits (1s and 0s), and an 8-bit binary number converted to decimal format will be between 0 and 255. The total of 32 bits means that approximately 4.2 billion possible IP version 4 addresses exist.

You should not be concerned that new IP addresses are likely to run out soon. Methods are in place already to extend the use of addresses. The IP addresses come in two groups: public and private. The *public* IP addresses are for computers connected to the Internet. No two public IP address can be the same. However, a *private* IP address, such as one on a private company network, has to be unique only in that network. It does not matter if other computers in the world have the same IP address, because this computer is never connected to those other worldwide computers. Network administrators often use private IP addresses that begin with a 10, such as 10.102.230.17. The other private IP addresses are 172.16.0.0–172.31.255.255 and 192.168.0.0–192.168.255.255.

Also note that an ISP often will buy a pool of public IP addresses and assign them to you when you log on. So, an ISP might own 1,000 public IP addresses and have 10,000 customers. Because all 10,000 customers will not be online at the same time, the ISP simply assigns an IP address to a customer when he or she logs on, and the ISP un-assigns the IP address when the customer logs off.

IPV6 utilizes a 128-bit address (instead of 32) and utilizes a hex numbering method in order to avoid long addresses such as 132.64.34.26.64.156.143.57.1.3.7.44.122.111.201.5. The hex address format appears in the form of 3FFE:B00:800:2::C, for example. This gives you 2^{128} possible address (many trillions of addresses) so no chance exists of running out of IP addresses in the foreseeable future.

Uniform Resource Locators

For most people, the main purpose for getting on the Internet is web pages (but there are other things such as e-mail and file downloading). If you had to remember IP addresses and type those in, then surfing the Net would be cumbersome at best. Fortunately, you don't have to. You type in domain names that make sense to humans and those get translated into IP addresses. For example, you might type in www.chuckeasttom.com to go to my website. Your computer, or your ISP, must translate the name you typed in (called a *Uniform Resource Locator*, or URL), into an IP address. The DNS (Domain Name Service) protocol, which is mentioned in Table 1.1, handles this translation process. So you are typing in a name that makes sense to humans, but your computer is using a corresponding IP address to connect. If that address is found, your browser sends a packet (using the HTTP protocol) to port 80. If that target computer has software that listens and responds to such requests (like web-server software such as Apache or Microsoft Internet Information Server), then the target computer will respond to your browser's request and communication will be established. This method is how web pages are viewed. If you have ever received an Error 404: File Not Found, what you're seeing is that your browser received back a packet (from the web server) with error code 404, denoting that the web page you requested could not be found. The web server can send back a series of error messages to your web browser, indicating different situations.

E-mail works the same way as visiting websites. Your e-mail client will seek out the address of your e-mail server. Then your e-mail client will use either POP3 to retrieve your incoming e-mail, or SMTP to send your outgoing e-mail. Your e-mail server (probably at your ISP or your company) will then try to resolve the address you are sending to. If you send something to chuckeasttom@yahoo.com, your e-mail server will translate that e-mail address into an IP address for the e-mail server at yahoo.com, and then your server will send your e-mail there. Note that newer e-mail protocols are out there; however, POP3 is still the most commonly used.

IMAP is now widely used as well. Internet Message Access Protocol operates on port 143. The main advantage of IMAP over POP3 is it allows the client to download only the headers to the machine, and then the user can choose which messages to fully download. This is particularly useful for smart phones.

Mac Addresses

MAC addresses are an interesting topic. (You might notice that MAC is also a sublayer of the data link layer of the OSI model.) A MAC address is a unique address for an NIC. Every NIC in the world has a unique address that is represented by a six-byte hexadecimal number. The Address Resolution Protocol (ARP) is used to convert IP addresses to MAC addresses. So when you type in a web address, the DNS protocol is used to translate that into an IP address. The ARP protocol then translates that IP address into a specific MAC address of an individual NIC.

Protocols

Different types of communications exist for different purposes. The different types of network communications are called *protocols*. A protocol is, essentially, an agreed-upon method of communications. In fact, this definition is exactly how the word *protocol* is used in standard, non-computer usage. Each protocol has a specific purpose and normally operates on a certain port (more on ports in a bit). Table 1.1 lists some of the most important protocols.

TABLE 1.1 Logical Ports and Protocols

Protocol	Purpose	Port
FTP (File Transfer Protocol)	For transferring files between computers.	20 & 21
SSH	Secure shell. A secure/encrypted way to transfer files.	22
Telnet	Used to remotely log on to a system. You can then use a command prompt or shell to execute commands on that system. Popular with network administrators.	23
SMTP (Simple Mail Transfer Protocol)	Sends e-mail.	25
WhoIS	A command that queries a target IP address for information.	43
DNS (Domain Name Service)	Translates URLs into web addresses.	53
tFTP (Trivial File Transfer Protocol)	A quicker, but less reliable form of FTP.	69
HTTP (Hypertext Transfer Protocol)	Displays web pages.	80
POP3 (Post Office Protocol Version 3)	Retrieves e-mail.	110
NNTP (Network News Transfer Protocol)	Used for network news groups (usenet newsgroups). You can access these groups over the web via www.google.com by selecting the Groups tab.	119
NetBIOS	An older Microsoft protocol for naming systems on a local network.	137, 138, 139
IRC (Internet Relay Chat)	Chat rooms.	194

Protocol	Purpose	Port
HTTPS (Hyper Text Transfer Protocol Secure)	HTTP encrypted with SSL or TLS.	443
SMB (Server Message Block	Used by Microsoft Active Directory.	445
ICMP (Internet Control Message Protocol)	These are simply packets that contain error messages, informational messages, and control messages.	No specific port

You should note that this list is not complete. Dozens of other protocols exist, but for now discussing these will suffice. All of these protocols are part of a suite of protocols referred to as TCP/IP (Transmission Control Protocol/Internet Protocol). The most important thing for you to realize is that the communication on networks takes place via packets, and those packets are transmitted according to certain protocols, depending on the type of communication that is occurring. You might be wondering what a port is. Don't confuse this type of port with the connections on the back of your computer, such as a serial port or parallel port. A port in networking terms is a handle, a connection point. It is a numeric designation for a particular pathway of communications. All network communication, regardless of the port used, comes into your computer via the connection on your Network Interface Card (NIC). You might think of a port as a channel on your TV. You probably have one cable coming into your TV but you can view many channels. You have one cable coming into your computer, but you can communicate on many different ports.

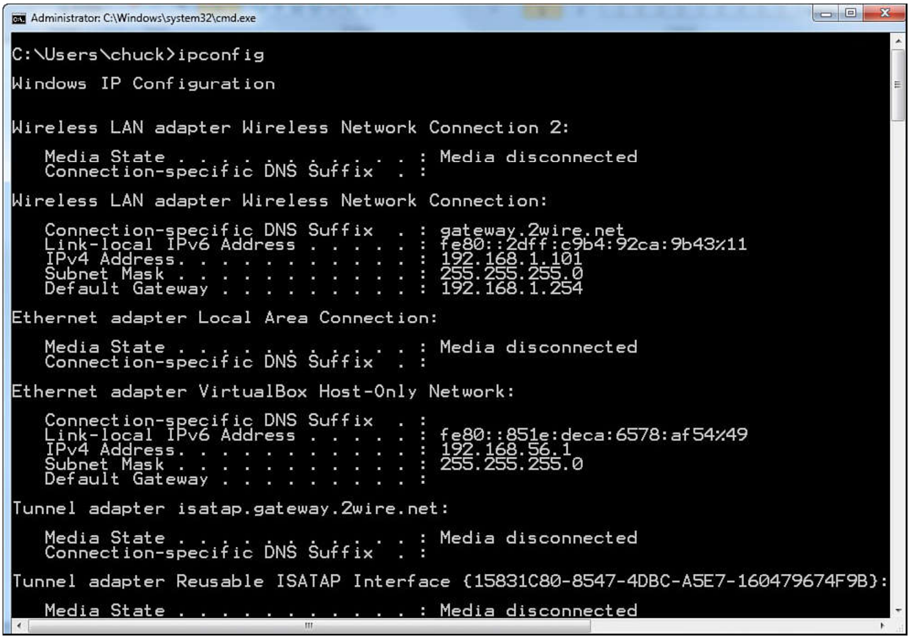
So the picture we've drawn so far of networks is one of machines connected to each other via cables, and perhaps to hubs/switches/or routers. Networks transmit binary information in packets using certain protocols and ports. This is an accurate picture of network communications, albeit a simple one.

Basic Network Utilities

Now that you know what IP addresses and URLs are, you need to be familiar with some basic network utilities. You can execute some network utilities from a command prompt (Windows) or from a shell (Unix/Linux). Many readers are already familiar with Windows, so the text's discussion will focus on how to execute the commands and discuss them from the Windows command-prompt perspective. However, it must be stressed that these utilities are available in all operating systems. This section covers the IPConfig, ping, and tracert utilities.

IPConfig

The first thing you want to do is get information about your own system. To accomplish this fact-finding mission, you must get a command prompt. In Windows 7, you do this by going to the Start menu, selecting All Programs, and then choosing Accessories. You can also go to Start, Run, and type **`cmd`** to get a command prompt. Now you can type in **`ipconfig`**. (You could input the same command in Unix or Linux by typing in **`ifconfig`** from the shell.) After typing in `ipconfig` (ifconfig in Linux), you should see something much like Figure 1.1.

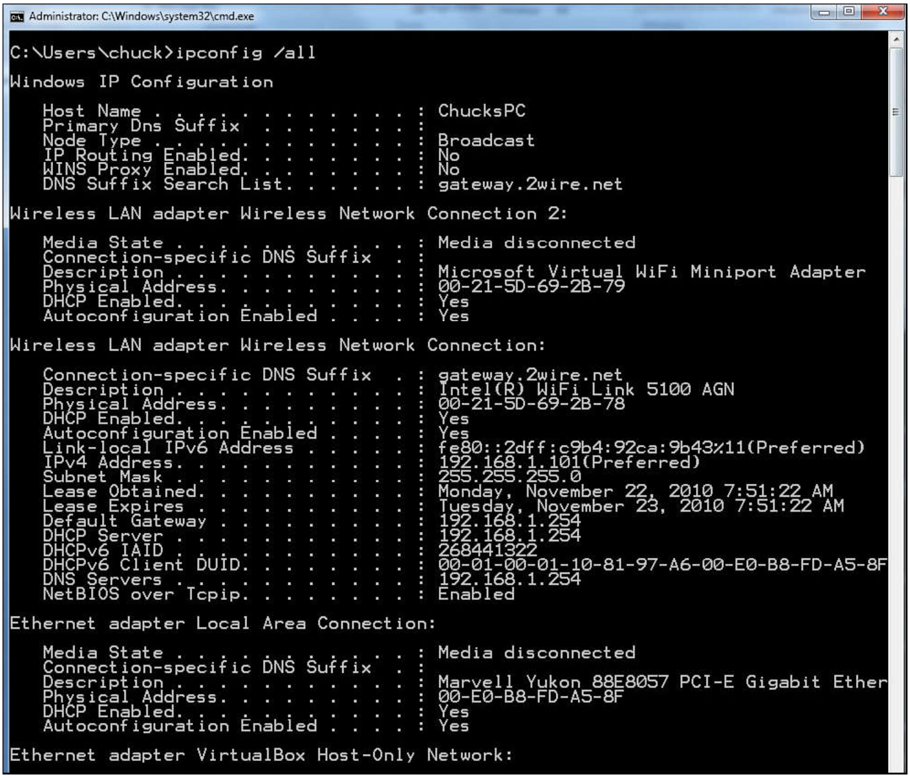


```
C:\Users\chuck>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : gateway.2wire.net
   Link-local IPv6 Address . . . . . : fe80::2dff:c9b4:92ca:9b43%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254

Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::851e:deca:6578:af54%49
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.gateway.2wire.net:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Reusable ISATAP Interface {15831C80-8547-4DBC-A5E7-160479674F9B}:

   Media State . . . . . . . . . . . : Media disconnected
```

FIGURE 1.1 IPConfig.

This command gives you some information about your connection to a network (or to the Internet). Most importantly you find out your own IP address. The command also has the IP address for your default gateway, which is your connection to the outside world. Running the `IPConfig` command is a first step in determining your system's network configuration. Most commands this text mentions, including `IPConfig`, have a number of parameters, or flags, that can be passed to the commands to make the computer behave in a certain way. You can find out what these commands are by typing in the command, followed by a space, and then typing in hyphen question mark: `-?`.

As you can see, you might use a number of options to find out different details about your computer's configuration. The most commonly used method would probably be `IPConfig/all`, shown in Figure 1.2:



```
C:\Users\chuck>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : ChucksPC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Broadcast
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : gateway.2wire.net

Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Virtual WiFi Miniport Adapter
   Physical Address. . . . . . . . . : 00-21-5D-69-2B-79
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : gateway.2wire.net
   Description . . . . . . . . . . . : Intel(R) WiFi Link 5100 AGN
   Physical Address. . . . . . . . . : 00-21-5D-69-2B-78
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2dff:c9b4:92ca:9b43%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, November 22, 2010 7:51:22 AM
   Lease Expires . . . . . . . . . . : Tuesday, November 23, 2010 7:51:22 AM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 268441322
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-10-81-97-A6-00-E0-B8-FD-A5-8F
   DNS Servers . . . . . . . . . . . : 192.168.1.254
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Marvell Yukon 88E8057 PCI-E Gigabit Ether
   Physical Address. . . . . . . . . : 00-E0-B8-FD-A5-8F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:
```

FIGURE 1.2 IPConfig/all.

You can see that this option gives you much more information. For example, `IPConfig/all` gives the name of your computer, when your computer obtained its IP address, and more.

Ping

Another commonly used command is ping. Ping is used to send a test packet, or echo packet, to a machine to find out whether the machine is reachable and how long the packet takes to reach the machine. This useful diagnostic tool can be employed in elementary hacking techniques. Figure 1.3 shows the command.