ontained in the ______.

gh setting up packet-filtering

'ork security.

supply is a component of ______ security.

signed to ______.

IS servers

olled industrial operations

ion

s

luates data in the payload and compares it with a prede-

alse?

vare is designed to replicate itself? (Choose all that apply.)

what is the starting point for developing a rule base?

cified types

cified types

of a possible attack are called ______.

## Hands-On Projects

The hands-on projects in this book require one or more of the following operating systems: Windows 7 Professional, Windows Server 2008 R2 SP1, and Ubuntu desktop. Students can work in teams of two with one system running Windows Server 2008 as a real or virtual machine, and the other running Windows 7 and Ubuntu as a dual boot or as virtual machines. Recommended initial configurations are detailed in the Introduction of this book.

### Hands-On Project 1-1: Installing a Personal Firewall

**Time Required:** 20 minutes

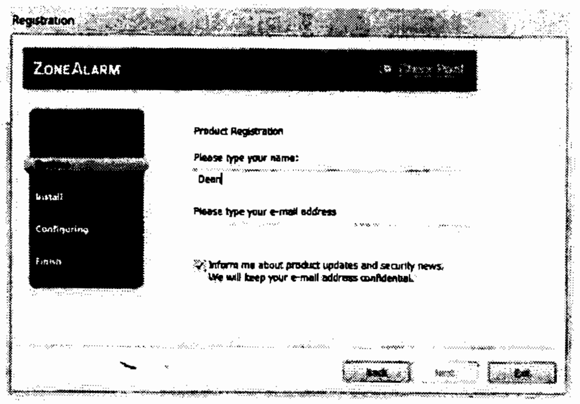
**Objective:** Install ZoneAlarm Free Firewall.

**Description:** Freeware firewall programs are not as full featured as commercial firewalls, but they are useful for testing and learning how the programs work. In this activity, you use a Windows 7 computer to download and use the freeware version of a popular personal firewall, ZoneAlarm by Check Point. Both Windows Server 2008 and Windows 7 are used in this project.

1. Boot the Windows Server 2008 system so that the Windows 7 user can log on to the domain. Log on to Windows 7 with an administrative account.
2. To disable the Windows firewall, click the **Start** button, and click **Control Panel**. If necessary, click **Category** in the upper-right corner and select **Small icons**. Click **Windows Firewall**, and click **Turn Windows Firewall on or off**. In each of the three sections—Domain network location settings, Home or work (private) network location settings, and Public network location settings—click the option button next to **Turn off Windows Firewall (not recommended)**. Click **OK** and close the Windows Firewall window.
3. Start your Web browser, and go to **http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm**.
4. Click the **Download** button to the right of ZoneAlarm Free Firewall to start the download. If the Internet Explorer bar appears and informs you that the file download has been blocked, click the bar and click **Download File**. Click **Save** and download the program to your Downloads folder.
5. When the download is finished, click **Open Folder**, right-click the downloaded program file, and click **Run as administrator**. If necessary, click **Yes** in response to the User Account Control warning.
6. Click the check box to accept the terms of the license agreement, and click **Next**.
7. Click to uncheck the top check box, which improves your Internet protection with the ZoneAlarm Security Toolbar. Click **Next**.

These options can be added any time after the installation is completed.

8. Enter your name, uncheck the **Inform me about product updates and security news.** check box (see Figure 1-5), and click **Next.**



Product Registration

Please type your name:

Dean

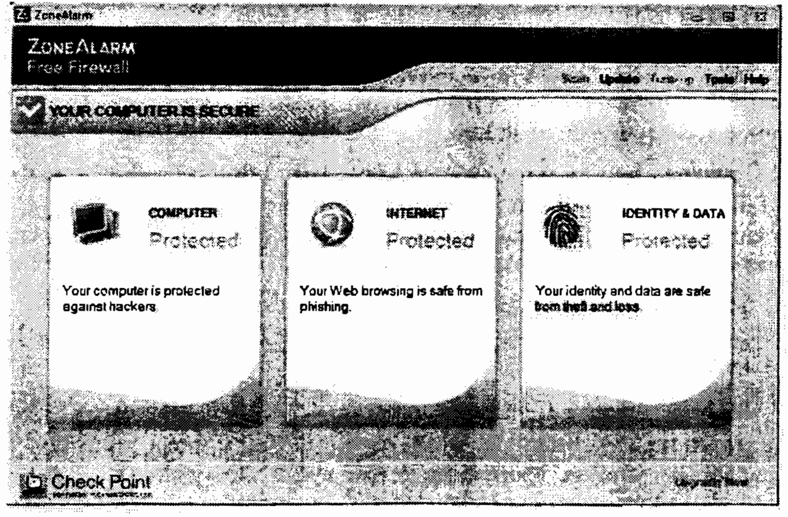
Please type your e-mail address

☑ Inform me about product updates and security news.
We will keep your e-mail address confidental.

Source: ZoneAlarm

**Figure 1-5** ZoneAlarm product registration

9. When the program setup has finished installing, click **Finish.**
10. If necessary, start ZoneAlarm by clicking Start and then clicking ZoneAlarm Security. When ZoneAlarm starts, it displays various windows. Close all of these windows except for the main window shown in Figure 1-6.



Your computer is protected against hackers

Your Web browsing is safe from phishing.

Your identity and data are safe from theft and loss.

Source: ZoneAlarm

**Figure 1-6** ZoneAlarm main window

11. Click **Update** to verify that you have the latest signatures. When the update is

↳ complete, click Close

12. In the main window, click the **Computer Prot**
appears should look similar to Figure 1-7.

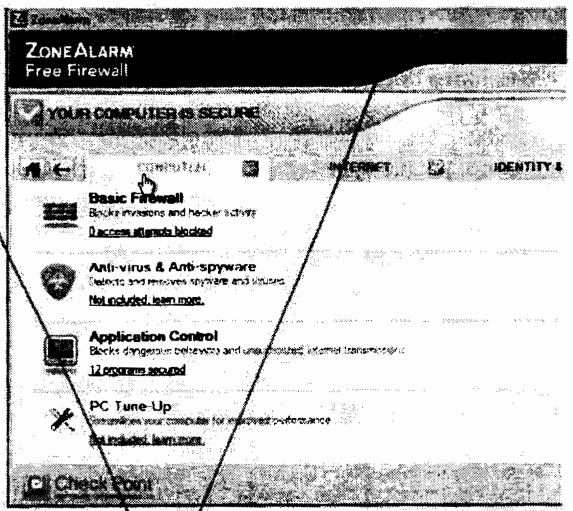

ZoneAlarm
ZoneAlarm
Free Firewall
YOUR COMPUTER IS SECURE
COMPUTER
INTERNET
IDENTITY &
Basic Firewall
Blocks invasions and hacker activity
0 access attempts blocked
Anti-virus & Anti-spyware
Detects and removes spyware and viruses
Not included, learn more.
Application Control
Blocks dangerous behavior and unauthorized internet transmissions
12 programs secured
PC Tune-Up
Optimizes your computer for improved performance
Not included, learn more.
Check Point

**Figure 1-7** ZoneAlarm Computer tab

13. Click the **Basic Firewall** link. How many zon
the zones? What zone settings are associated
14. Click the **Advanced Settings** button. Notice t
protocols are allowed by default.
15. Click **OK** to close the Firewall Settings wind
What functions are not available in this free
link, investigate the settings that you can cor
page, and investigate the Advanced Settings.
16. Click the **Internet** tab. What functions are nc
function is enabled on the Internet tab?
17. Click the **Identity & Data** tab and investigat
available.
18. Leave the system running for the next Hand

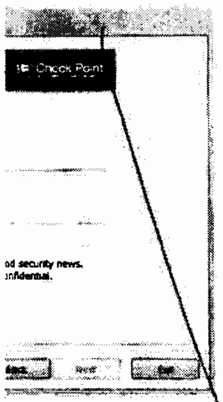
## Hands-On Project 1-2: Installing a P

**Time Required:** 10 minutes

**Objective:** Install Nmap.

**Description:** One of the first steps in attacking a r
who is testing for vulnerabilities or by a hacker lo
the systems on the network. Learning a network

he **Inform me about product updates and security news.**
and click **Next.**



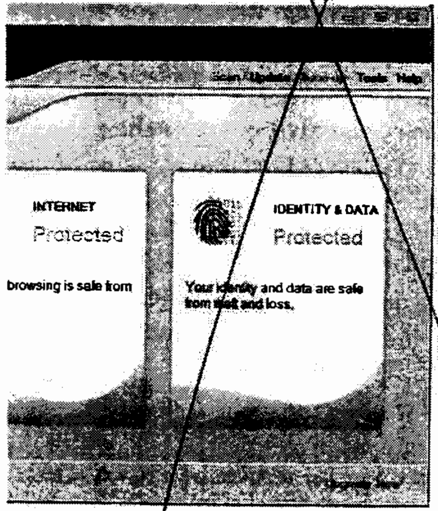
od security news.
onfidential.

Source: ZoneAlarm

:ration

ıs finished installing, click **Finish.**

m by clicking Start and then clicking ZoneAlarm Security.
displays various windows. Close all of these windows
v shown in Figure 1-6.



INTERNET

Protected

browsing is safe from

IDENTITY & DATA

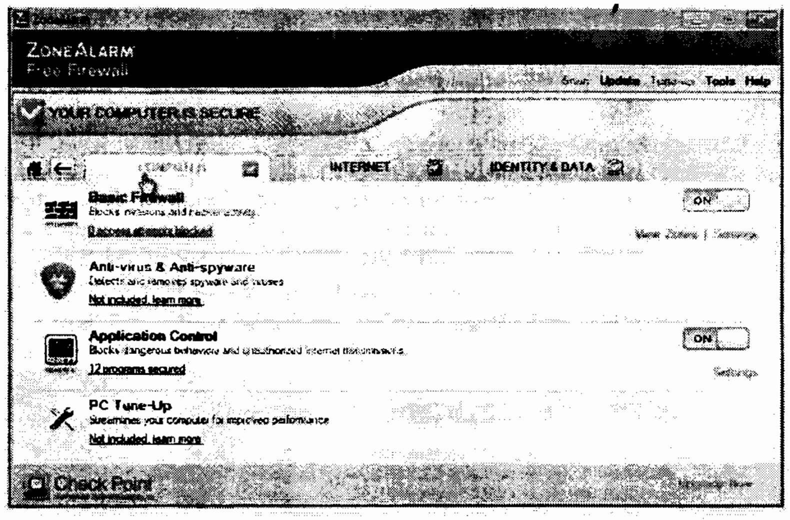
Protected

Your identity and data are safe from theft and loss.

Source: ZoneAlarm

you have the latest signatures. When the update is

12. In the main window, click the **Computer Protected** box. The Computer tab that appears should look similar to Figure 1-7.



Basic Firewall
Blocks intrusions and hacker activity.
0 access attempts blocked

Anti-virus & Anti-spyware
Detects and removes spyware and viruses
Not included, learn more.

Application Control
Blocks dangerous behavior and unauthorized internet transmissions.
12 programs secured

PC Tune-Up
Streamlines your computer for improved performance
Not included, learn more.

Source: ZoneAlarm

**Figure 1-7** ZoneAlarm Computer tab

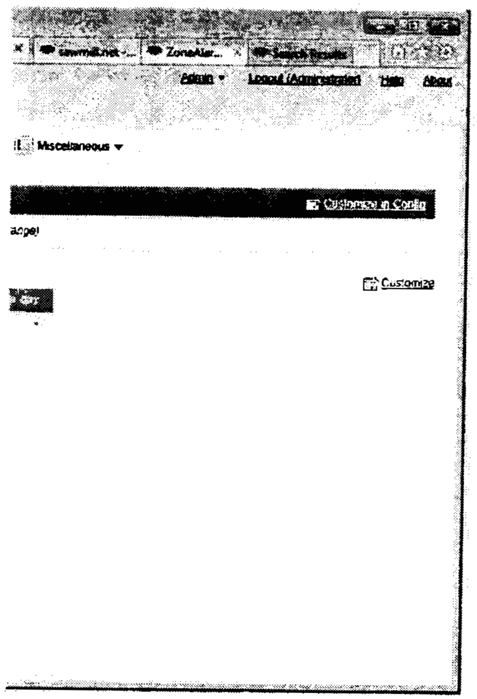
13. Click the **Basic Firewall** link. How many zones are listed? What are the functions of the zones? What zone settings are associated with medium and high security?
14. Click the **Advanced Settings** button. Notice the various settings; for example, VPN protocols are allowed by default.
15. Click **OK** to close the Firewall Settings window and return to the main Computer tab. What functions are not available in this free version? Click the **Application Control** link, investigate the settings that you can configure on the main Application Control page, and investigate the Advanced Settings.
16. Click the **Internet** tab. What functions are not available in this free version? What function is enabled on the Internet tab?
17. Click the **Identity & Data** tab and investigate the functions that are and are not available.
18. Leave the system running for the next Hands-On Project.

## Hands-On Project 1-2: Installing a Port Scanning Tool

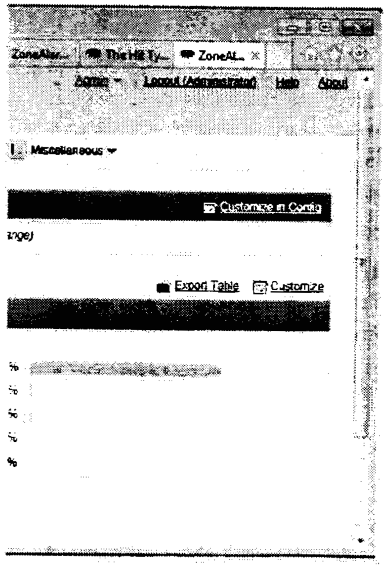
**Time Required:** 10 minutes

**Objective:** Install Nmap.

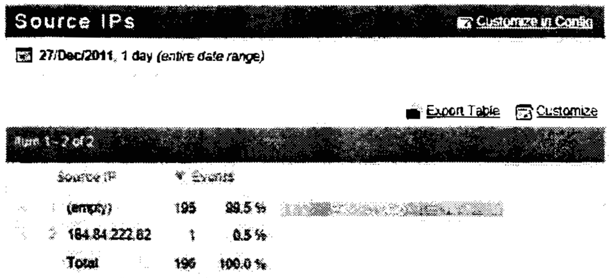
**Description:** One of the first steps in attacking a network, either by a network administrator who is testing for vulnerabilities or by a hacker looking for a system to exploit, is identifying the systems on the network. Learning a network's IP addresses, MAC addresses, operating



Source: Sawmill



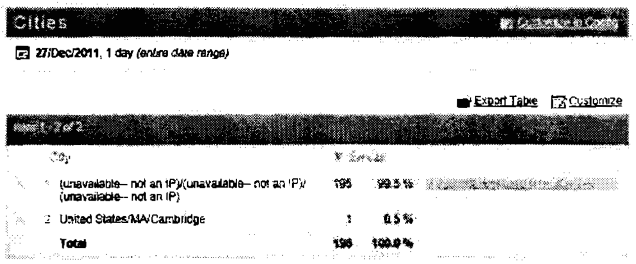
Source: Sawmill



| | Source IP | Events | |
|---|---|---|---|
| 1 | (empty) | 195 | 99.5 % |
| 2 | 184.84.222.82 | 1 | 0.5 % |
| | Total | 196 | 100.0 % |

Source: Sawmill

**Figure 1-12** Source IP addresses of logged events



| | City | Events | |
|---|---|---|---|
| 1 | (unavailable– not an IP)/(unavailable– not an IP)/(unavailable– not an IP) | 195 | 99.5 % |
| 2 | United States/MA/Cambridge | 1 | 0.5 % |
| | Total | 196 | 100.0 % |

Source: Sawmill

**Figure 1-13** Source cities of logged events

11. From the ZoneAlarm window, click the **Computer Protected** link, click **Basic Firewall**, and set Your Trusted Zone security to **Medium**.
12. Log out of Windows 7. If necessary, log out of Server 2008.

# Case Projects

## Case Project 1-1: Determining Legal Requirements for Penetration Testing

Alexander Rocco Corporation, a large real estate management company in Maui, Hawaii, has contracted your computer consulting company to perform a penetration test on its computer network. Penetration testers are hired to attack an organization's network, determine what vulnerabilities are present, and provide recommendations for securing the company's information systems. The management company owns property that houses a five-star hotel, golf courses, tennis courts, and restaurants. Claudia Mae, the vice president, is your only contact at the company. To avoid undermining your tests, you will not be introduced to any IT staff or employees. Claudia wants to determine what you can find out about the company's network infrastructure, network topology, and vulnerabilities without any assistance from her or company personnel.

Based on this information, write a report outlining the steps you should take before beginning the penetration tests. Research applicable state and federal laws, and reference them in your report.

# ands-On Projects

## Hands-On Project 2-1: Installing the Wireshark Protocol Analyzer

**Time Required:** 10 minutes

**Objective:** Download and install Wireshark.

**Description:** You access the Wireshark Web site, and then download and install Wireshark on both the Windows 7 and Windows Server 2008 computers.

1. Log on to Windows 7 with an administrative account. Log on to Windows Server 2008 with an administrative account. On both systems, complete the following steps.
2. Start your Web browser, and go to **www.wireshark.org/download.html**.
3. Click the appropriate **Windows Installer** link, depending on whether you are using a 32-bit or 64-bit operating system. If the Internet Explorer warning appears about trusted sites, click **Add**, click **Add** again, click **Close**, and then click the **Windows Installer** link again.
4. In the download window, click **Run**. In the next window, click **Run** again. In the Welcome window, click **Next**. In the License Agreement window, click **I Agree**. In the Choose Components window, click **Next**. In the Select Additional Tasks window, click the box next to **Desktop Icon**, and click **Next**. In the Choose Install Location window, click **Next**.
5. Wireshark requires WinPcap. If you completed the Hands-On Projects in Chapter 1, WinPcap is already installed on Windows Server 2008, so you can click **Install** and skip to Step 6. If you did not complete the Chapter 1 Hands-On Projects on Windows Server 2008, or if you are on the Windows 7 system, complete the rest of this step. Verify that the box next to **Install WinPcap** is checked, and click **Install**. In the WinPcap window, click **Next**. In the Welcome to the WinPcap Setup Wizard, click **Next**. Click **I Agree** and click **Install**. Click **Finish**.
6. In the Installation Complete window, click Next. In the Completing the Wireshark Setup Wizard, click **Finish**.
7. Leave the systems logged on for the next Hands-On Project.

## Hands-On Project 2-2: Using Wireshark to Capture IPv4 Pings

**Time Required:** 20 minutes

**Objective:** Capture and begin to analyze network traffic.

**Description:** To get a better idea of what TCP/IP packet headers look like, you can use a network traffic analyzer to capture packets as they enter or leave your network. In this activity, you capture IPv4 ping packets with Wireshark and begin to analyze how ICMP and ARP traffic function.

1. Log on to Windows Server 2008 and Windows 7 with an administrative account.
2. On both systems, access a command prompt and enter **ipconfig** to verify the systems' IP addresses. Verify that you have connectivity by pinging the IPv4 address of Windows

Protocol. Investigate each of these headers in light of the information provided in this chapter. Pay particular attention to the Neighbor Solicitation message. Compare the Type field value to those in Table 2-15 to verify the type of ICMPv6.

5. This chapter had several figures that show header structures, including Figures 2-1, 2-3, 2-5, 2-8, and 2-9. In the following space, create a figure that shows the structure of the Neighbor Solicitation message.

6. Explore the Echo Request and Echo Reply packets in the rest of the capture. Verify the ICMPv6 message types by consulting Table 2-11.
7. Leave your system running for the next project.

## Hands-On Project 2-5: A Challenge

**Time Required:** 20 minutes

**Objective:** Explore a ping option and independently analyze a packet capture.

**Description:** In this project, you experiment with a variation of the ping command and then analyze a packet capture to determine how the result is different from the one you obtained in Hands-On Project 2-4.

1. Access both the Windows 7 and Windows Server 2008 computers with administrative accounts.
2. Set up your system to capture a ping of your partner's system using the IPv6 address, as you have in the previous projects.
3. Enter the command **ping -l 5000 *IPv6_address*,** where -l is the letter *l*, not the number one, and *IPv6_address* is the IPv6 address of your partner's system. Capture the result.
4. Analyze the results. What is the effect of using the -l option with the ping command? How is this result different from that in Hands-On Project 2-4? How does IP handle this difference?
5. Log off your systems.

# Case Projects

## Case Project 2-1: The Differences Between IPv4 and IPv6

You are a network engineer for an IT consulting firm named F1IT. One of your clients, Beautivision, a chain of plastic surgery clinics with 80 locations nationwide, has asked you to prepare a proposal for implementing IPv6 in Beautivision's corporate headquarters, its WAN network, and its clinic locations. In preparation, you need to create a one- to two-page memo that describes the main differences between IPv4 and IPv6. Write the memo to Mary Jane Newman, communications manager for Beautivision. When preparing the memo, keep in mind that Ms. Newman has some knowledge of information technology but is not an expert.