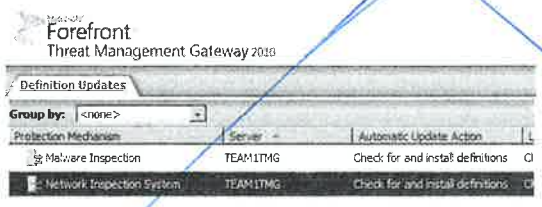
Click Yes in the Security Warning window. Examine the report. Close the report after determining what data the report provides.

16. Click **Update Center**. Assuming that you have not had Internet access during these projects, you should see red alerts for Malware Inspection and Network Inspection System. Connect your system to the Internet. This may involve modifying the external interface IP address, default gateway, DNS server, and proxy settings. Check with your instructor for details.
17. In the right frame, click **Check for Definitions**. If the check is successful, the Definition Updates tab will look similar to Figure 11-25.



Used with permission of Microsoft Corporation

Figure 11-25 Definition updates completed

18. Log off all systems.

Case Projects

Case Project 11-1: VPN Filtering Rules

You work for a network consulting firm. Your client wants to implement a VPN system that supports PPTP-, SSTP-, and L2TP-based VPNs. The system will be used primarily for remote client access. You need to prepare a report for the client that explains the implications of providing this functionality in terms of firewall configuration. Your report must address the protocols and ports that need to be considered as the firewall policy is created. Prepare a one- to two-page report that addresses these issues.

Case Project 11-2: Threat Management Gateway Features

After receiving the report that you prepared in Case Project 11-1, your client has decided that an "all-in-one" product may be better than patching together a VPN infrastructure. You need to prepare a report that explains the features in the Microsoft Forefront TMG 2010 product. Your client has some technical understanding, but she needs to have the TMG features explained in a practical way so that she can consider how the product could assist in lowering costs and improving business processes. Prepare a two- to three-page report that meets the stated requirements.

10. Which of the following factors enables attackers to program ActiveX controls to run malicious code on a user's Web browser? (Choose all that apply.)
    a. ActiveX controls run in a sandbox that allows interaction with the OS.
    b. ActiveX controls do not require user action to be activated.
    c. ActiveX controls run automatically when the browser loads the Web page that contains them.
    d. ActiveX controls have almost full access to the Windows OS.
11. A Web server can be hardened just by configuring the Web application correctly. True or False?
12. For optimum efficiency, configure a domain controller to function also as an IIS Web server. True or False?
13. When securing an Apache Web server, which of the following tasks is not necessary?
    a. installing the latest Apache patches
    b. disabling processing of server-side includes (SSIs)
    c. deleting unneeded or default Apache files and sample code
    d. creating a privileged user ID for the Apache Web User account with root access
14. In a DNS zone transfer, what is actually transferred?
    a. fully qualified domain names and IP addresses
    b. usernames and passwords
    c. server MAC addresses
    d. UDP and ICMP messages
15. To keep log files organized, store them on the server you are monitoring. True or False?

Hands-On Projects

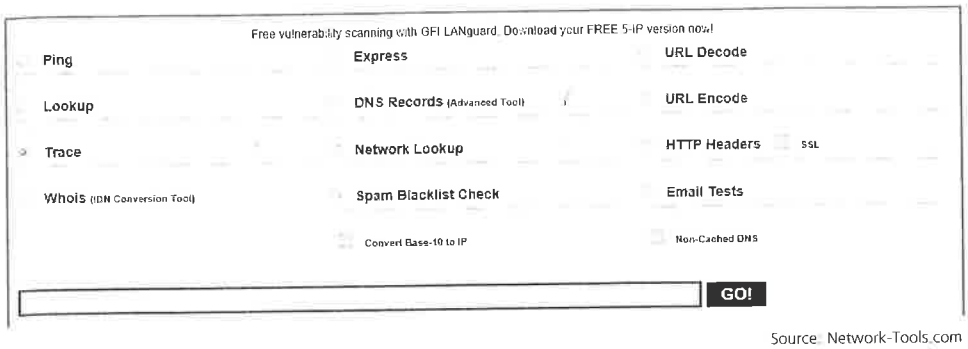
Hands-On Project 12-1: Finding Domain Information

Time Required: 10 minutes

Objective: Find your network's DNS and ISP information.

Description: In this activity, you use network tools from *Network-Tools.com* to discover domain information about your network.

1. Log on either to the Windows Server 2008 or Windows 7 system.
2. If necessary, configure your network interface for Internet access.
3. Start your Web browser and go to *http://network-tools.com*. Figure 12-8 shows the interface for this tool.



Source: Network-Tools.com

Figure 12-8 Network-Tools

4. Click the **Lookup** option button, enter your school's domain name (such as schoolname.edu) in the text box below the option buttons, and then click **GO**. What is the IP address that corresponds to your school's domain name? What country and region are shown for this domain name?
5. Click the **Whois** option button, and then click **GO**. Who is the contact for your school's domain name? What name servers are listed for your school's domain?
6. Click the **DNS Records** option button, and then click **GO**. What are the mail servers for your school's domain (MX records)?
7. Click the **Trace** option button, and then click **GO**. Which ISPs handle the school's Internet traffic?
8. Exit your browser, and leave your system running for the next project.

Hands-On Project 12-2: Examining Internet Explorer Security Settings

Time Required: 20 minutes

Objective: Become familiar with the security settings in Internet Explorer version 9.

Description: In this activity, you examine Internet Explorer's settings for handling security functions, such as browsing history, cookie management, security zones, and pop-ups.

1. If necessary, log on to Windows 7.
2. Start Internet Explorer. Verify the version number by clicking the **Tools** icon and then clicking **About Internet Explorer**. These controls are indicated by an "A" and "B" in Figure 12-9. If necessary, use Windows Update to upgrade Internet Explorer to version 9.

Case Projects

Case Project 12-1: Web Server Security Analysis

A challenge that faces the information security community is to make sure their organizations' top decision makers understand the importance of effective security policies. Understandably, managers who are responsible for an organization's financial stability want to ensure that investments in "nonrevenue" activities are necessary and effective. In many ways, the field of information security is in its infancy; practitioners do not have a long history of research that indicates the most effective security countermeasures against specific threats. Also, the threats are constantly changing. As new generations of information security workers secure digital assets, they will also need to create a solid body of research-based evidence to support the practices they recommend. In this project, you read and summarize a research project that addresses Web server security.

Go to *www.sans.org/reading_room/whitepapers/webservers/comparative-study-attacks-corporate-iis-apache-web-servers_33734*. Read the entire article, including the appendices. Answer the following questions:

1. What was the purpose of the research project?
2. What did the research demonstrate about the relative security of the IIS and Apache software?
3. What do you think detracted from the credibility of the report?
4. What were the main findings of the study?
5. What did the results of the study imply about the frequency of automated attacks versus the frequency of manually controlled attacks against Web servers?
6. Based on the results of the study, what policies and procedures would you recommend for Web server security?
7. Based on this study, which operating system is easier to attack: Windows or Linux?

Case Project 12-2: A Recently Discovered Web-based Attack

Use available resources to find a Web-based attack that has been discovered in the last two years. Prepare a one- to two-page report that summarizes the attack and includes the following information:

- The name of the attack
- Its technical mechanism and features
- The presumed goal of the attack
- Severity in terms of risk and damage
- Likely targets
- Known security controls