As you can see, the scan feature allows testing areas of the site that might have problems. Any vulnerabilities in the Web site are indicated in the Risk Level column as either High, Medium, Low, or Informational. In this example, the risk level is flagged as Medium. Gathering competitive intelligence through scans of this type is time consuming, and the more you find out, the deeper you want to dig. Setting a reasonable time frame for this phase of your investigation is important, or you might spend too much time on this activity. On the other hand, you don't want to rush your information gathering, because much of what you learn can be used for further testing and investigation. The following section covers additional tools you can use for gathering information.

Using Other Footprinting Tools

The Whois utility is a commonly used Web tool for gathering IP address and domain information. With just a company's Web address, you can discover a tremendous amount of information. Unfortunately, attackers can also make use of this information. Often companies don't realize they're publishing information on the Web that computer criminals can use. The Whois utility gives you information on a company's IP addresses and any other domains the company might be part of. In Activity 4-1, you practice using the Domain Dossier Whois function.

Activity 4-1: Using Footprinting Tools

Time Required: 30 minutes

Objective: Learn how to use footprinting tools, such as the Domain Dossier Whois function.

Description: Security testers need to know how to use tools for gathering information about networks. With the Whois function, you can discover which network configuration factors might be used in attacking a network.

1. Start your Web browser, and go to **http://centralops.net/co/domaindossier.aspx**.
2. Type **mit.edu** in the domain or IP address text box, check the "**domain whois record**" check box, then click the **go** button. Scroll down to view the information displayed (see Figure 4-5).

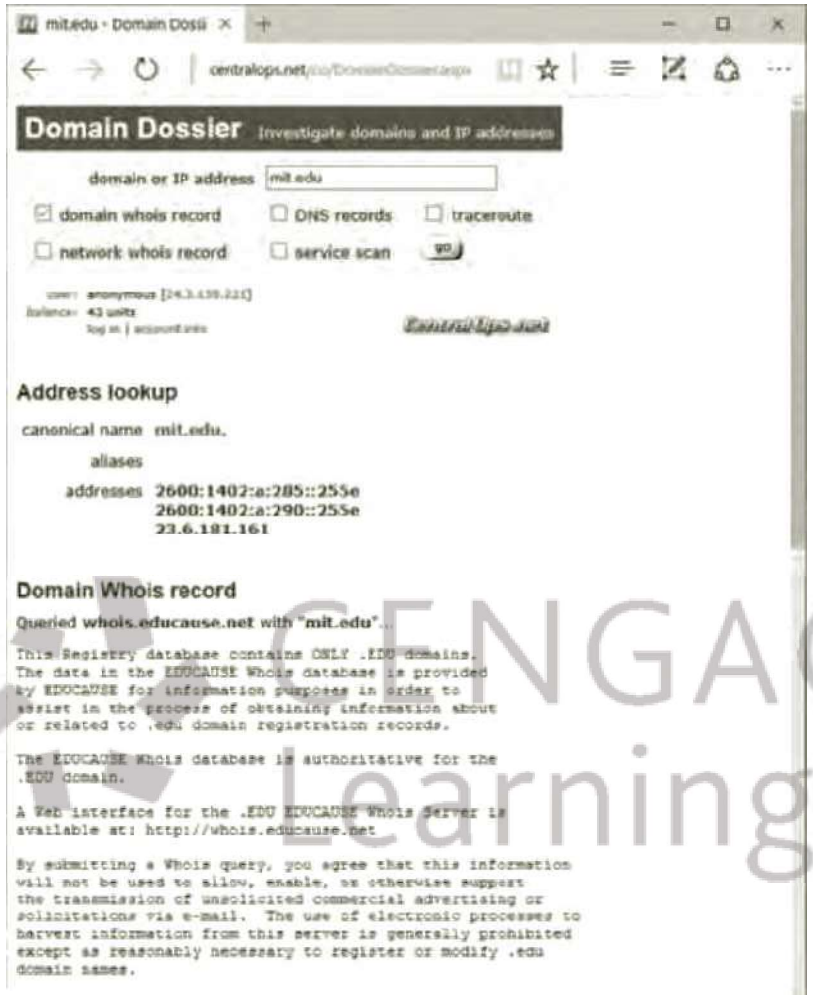

Figure 4-5 Viewing information with the Domain Dossier Whois function

3. Note the IP addresses and name servers listed. Chapter 5 covers port scanning and explains how these IP addresses can be used to gather more information about name servers.
4. Try entering several other organizations' domain names in the domain or IP address text box and repeat Steps 2 and 3. Note that some organizations are more discreet about what is listed in their output screens. For example, when describing an administrative contact, giving just a job title is better than listing an actual name, as you'll soon discover.
5. Leave your Web browser open for the next activity.