Hands-On Lab: Footprinting, Scanning, and Enumeration

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 9780357506431; Footprinting, Scanning, and Enumeration

Table of Contents

[Introduction 2](#_Toc76727756)

[Objective 2](#_Toc76727757)

[Estimated Completion Time 2](#_Toc76727758)

[Materials Required 2](#_Toc76727759)

[Minimum System Configuration 2](#_Toc76727760)

[Network Reconnaissance with Command Line Tools 3](#_Toc76727761)

[Opening Command Window (CMD) 3](#_Toc76727762)

[Using nslookup 3](#_Toc76727763)

[Using ping 5](#_Toc76727764)

[Using traceroute 7](#_Toc76727765)

[Web Reconnaissance with Web Browsers 9](#_Toc76727766)

[Opening Web site in Web Browser (CMD) 9](#_Toc76727767)

[Using page source 9](#_Toc76727768)

[Using Inspect 10](#_Toc76727769)

[Using Whois 11](#_Toc76727770)

[Using Other Web Resources 14](#_Toc76727771)

[Scanning with Nmap 14](#_Toc76727772)

[Download and Install Nmap 14](#_Toc76727773)

[Use Nmap 16](#_Toc76727774)

[Self-Reflection and Response 21](#_Toc76727775)

[Instructor’s Response 21](#_Toc76727776)

# Introduction

In this set of labs, students learn how attackers perform reconnaissance on potential targets using a variety of tools to perform what is known as “Footprinting.” This process includes both researching information from printed resources as well as gathering facts that can be collected from online resources and through social engineering efforts.

# Objective

Upon completion of this activity, the student will be able to:

* Identify network addresses associated with an organization.
* Identify the systems associated with the network addresses.

These activities will help you complete future labs in this course.

# Estimated Completion Time

If students are prepared, they should be able to complete this lab in 40 to 60 minutes.

\*\*\*\* Evan, please track your time and suggest better times for this lab \*\*\*\*\*\*

# Materials Required

This lab can be used from any Windows computer system where the user is authenticated with the appropriate rights and privileges to modify the targeted software on the system being used. Lab-based computer systems often have these privileges locked.

Students will need to be able to invoke and run Windows PowerShell.

# Minimum System Configuration

To complete the labs included, it is recommended that you operate them from a computer system (desktop or laptop) that is running Windows 10 and has:

* Intel i5 or better CPU
* 8 GB RAM (minimum) - 16 GB RAM (recommended)
* 1 TB Hard Drive with at least 250 GB free (minimum) - 350 GB free (recommended)
* Microsoft Windows 10 or latest version

## Network Reconnaissance with Command Line Tools

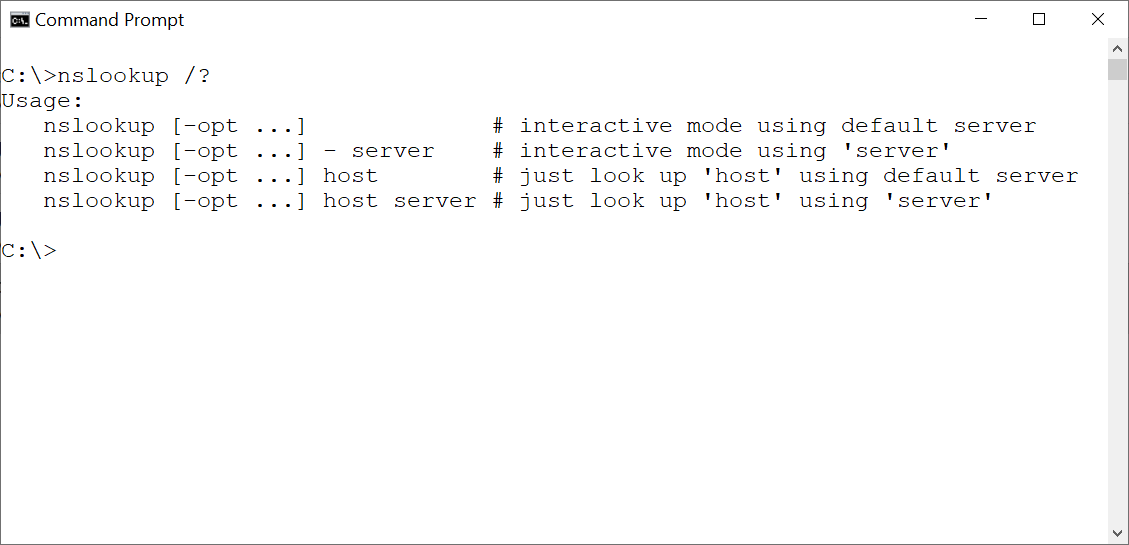
This lab uses utilities available in most operating systems. Many of these tools – like nslookup, ping, traceroute, and whois are command-line tools designed to assist network and systems administrators in debugging connections and systems. In the wrong hands, they provide information on the availability and identity of systems that can be used to exploit them.

### Opening Command Window (CMD)

1. Open a command window by typing **cmd** in the window search bar and press **Enter**. You can also run these command from Windows Powershell.

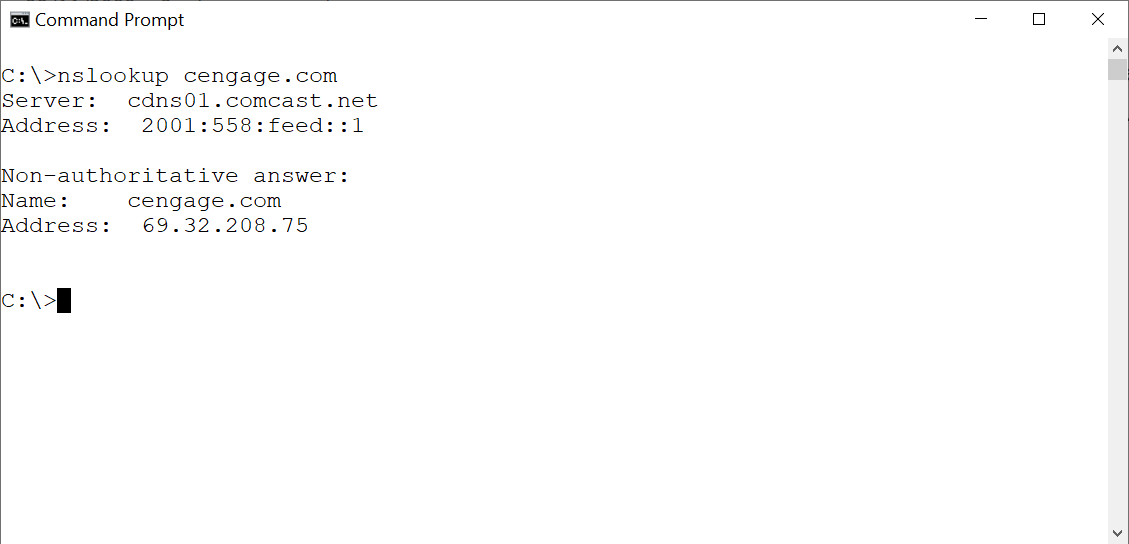
### Using nslookup

1. Type **nslookup /?**. You should see the help menu for nslookup.



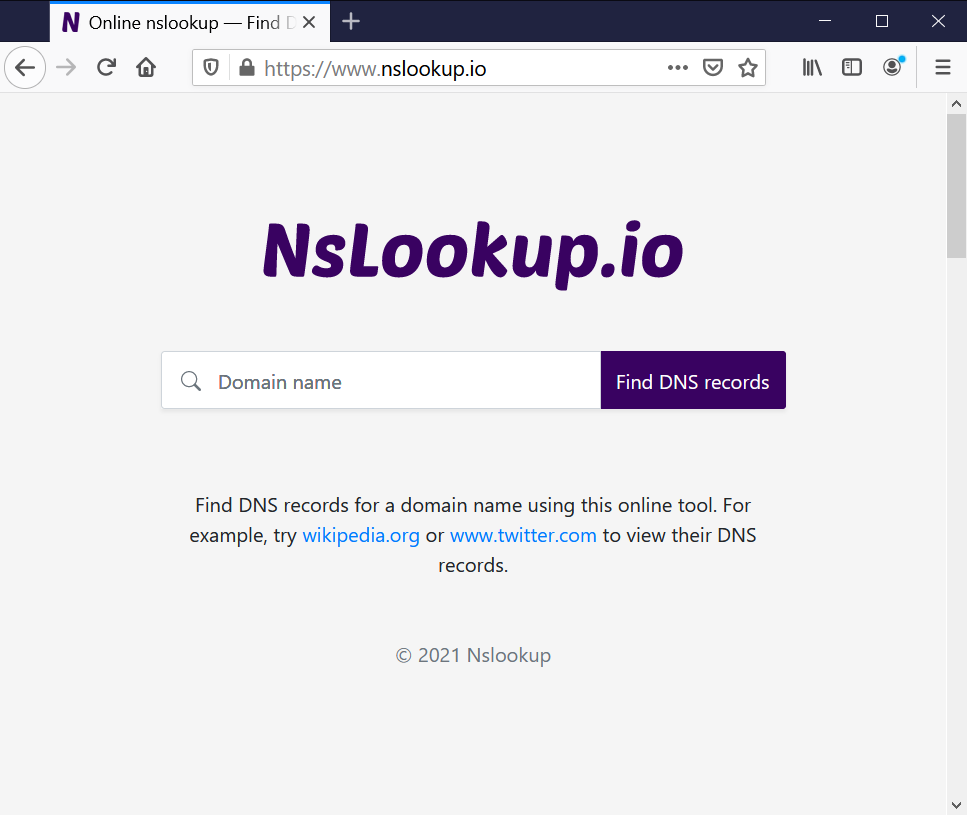
**Figure L08-1** nslookup help menu

1. Interactive mode nslookup puts the user in a session with the DNS system, whereas “just look up” just provides a response. Type **nslookup cengage.com** and press **Enter**. You should see a response like Figure L08-2, which gives you a) your DNS server and b) the IP address for the DNS server for Cengage. Repeat for your university’s domain (e.g. *stateuniv*.edu). For the Microsoft tech document, visit https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb490721(v=technet.10)?redirectedfrom=MSDN.



**Figure L08-2** nslookup for cengage.com

1. The same action can be performed using the web site at nslookup.io (See Figure L08-3. As some systems may be configured to prohibit nslookups, this may be a better alternative. The web site also will provide name server (NS) and mail server (MX) records, among others. Repeat your previous searches using this web site.
2. As nslookup gives you some fundamental information about the IP address range associated with a particular organization, the attacker may verify availability of identified servers using ping or may move to a more detailed, yet equally available service – traceroute and whois.

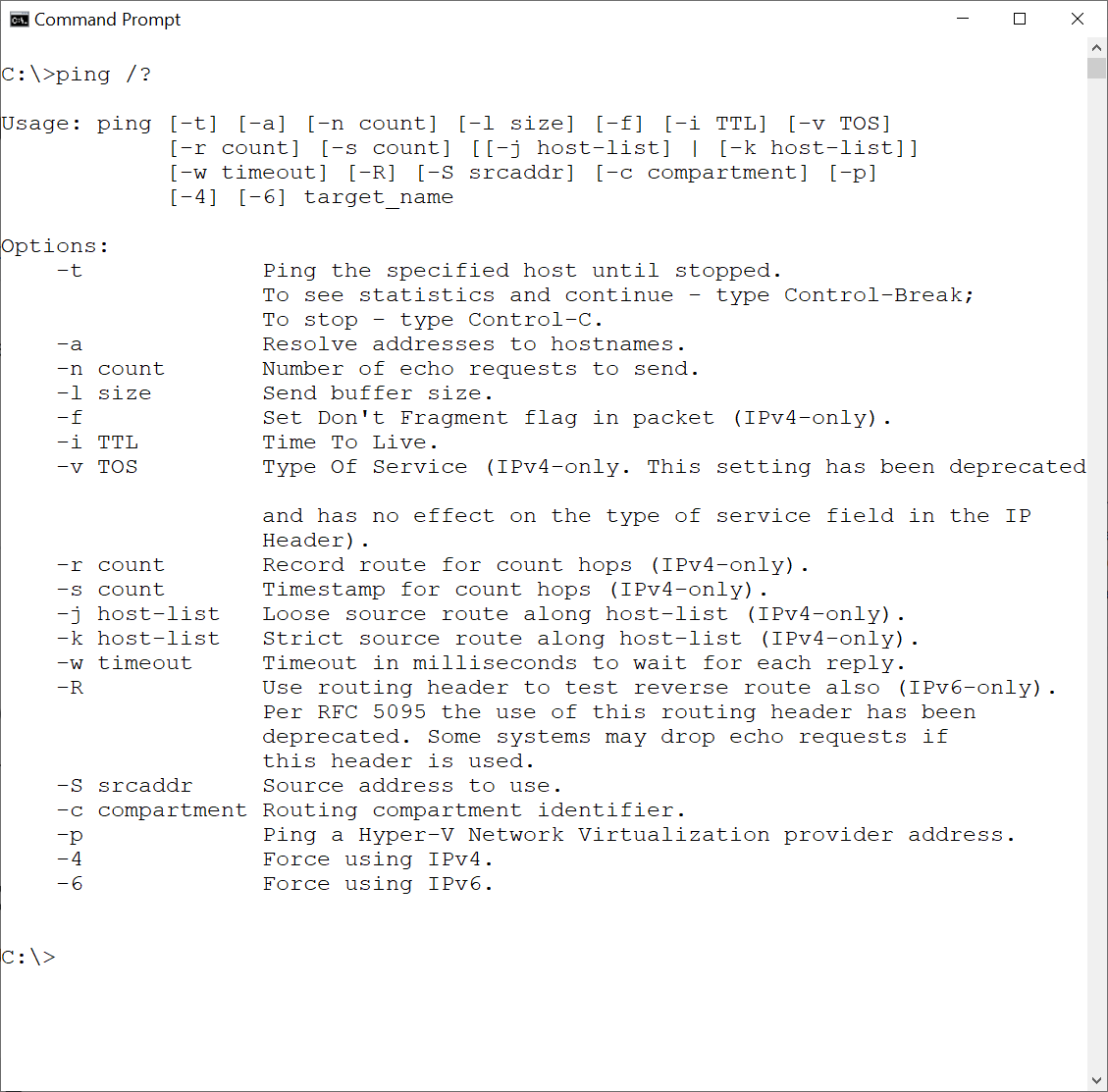


**Figure L08-3** nslookup.io

### Using ping

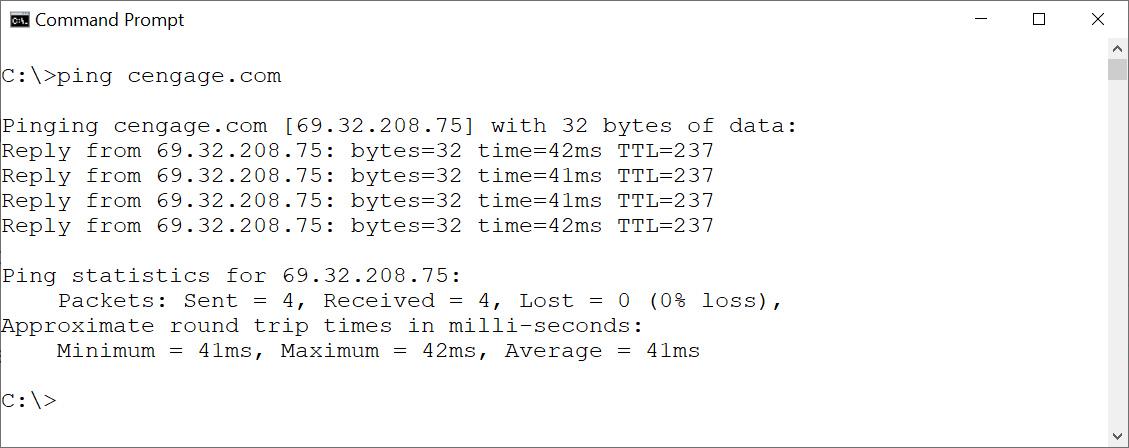
Ping is a systems utility designed to confirm the availability of a server. It was named for the sound made by sonar systems. Note that ping may be disabled on servers – at least on their public interfaces - as it is a tool commonly used as the basis for attacker tools and exploits.

1. In your command window, type **ping /?** and press **Enter**. Your results should be like Figure L08-4, with the basic command structure and available options.



**Figure L08-4** ping /?

1. Ping works with either domain names or IP addresses. In your command window, type **ping cengage.com** and press **Enter**. You should receive a number of successful pings including the time in milliseconds it takes for the ICMP echo request to travel to the Cengage server and return. (Note: for computer gamers, pings are often used to find a gaming server closer to the gamer allowing quicker response and better performance!). If you were a systems administrator trying to figure out why you can not communicate with a particular system, ping is very useful as you can experiment with different troubleshooting techniques.



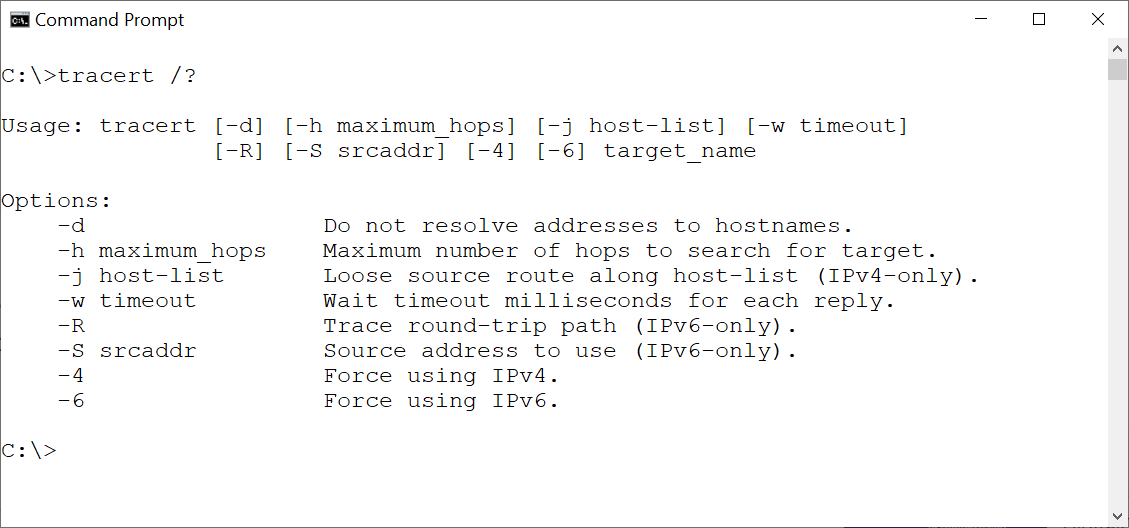
**Figure L08-5** ping cengage.com results

You will notice in the previous example that the ping only used four messages before stopping. If you needed ping to continue non-stop, you would use the *-t* option which would continue until you enter *Ctrl + C* to stop it.  
Attackers use ping to see if the system is up and responding to requests, which would then allow them to move to other tools to begin to collect additional information.

### Using traceroute

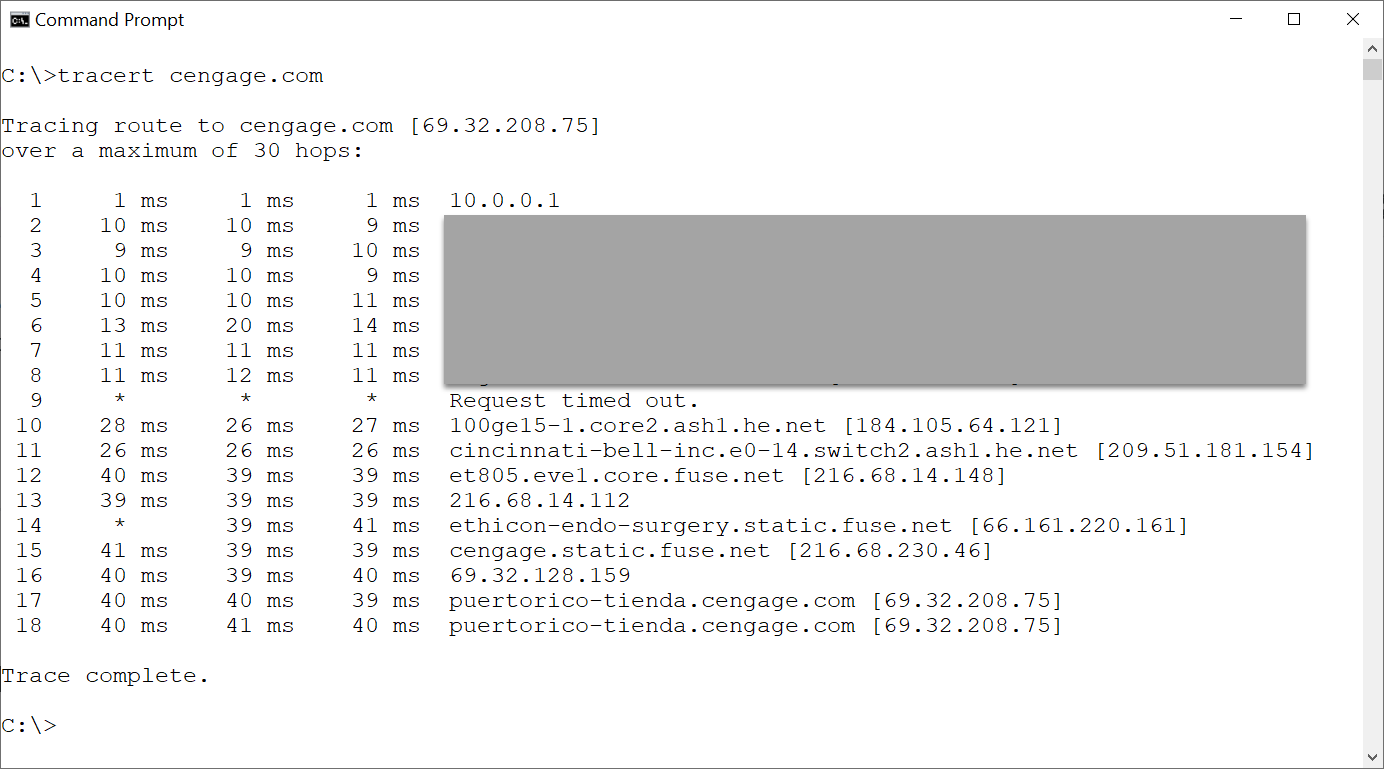
Traceroute provides a listing of all of the intermediate servers and networking devices between the user and the target. Again, either IP addresses or DNS names may be used to perform a traceroute.

1. In your command window, type **tracert /?** and press **Enter**. You should see results like Figure L08-6.



**Figure L08-6** tracert /?

1. Next, type tracert **cengage.com** and press **Enter**. This may take a minute as each “hop” between your system and Cengage’s server responds. As you can see from Figure L08-7, when a specific node doesn’t respond in time (times out), you get an asterix (\*) rather than a value. The traceroute continues, however, until you get to the destination. (Note the gray box is to conceal the author’s home networks).



**Figure L08-7** tracert cengage.com results

1. You can see how the series of tools provides more and more information on the target and its networks and systems. If the target system was inside the organization’s network, and the network wasn’t properly configured, the traceroute would include network addresses of internal systems. From here we go to web-based resources.

## Web Reconnaissance with Web Browsers

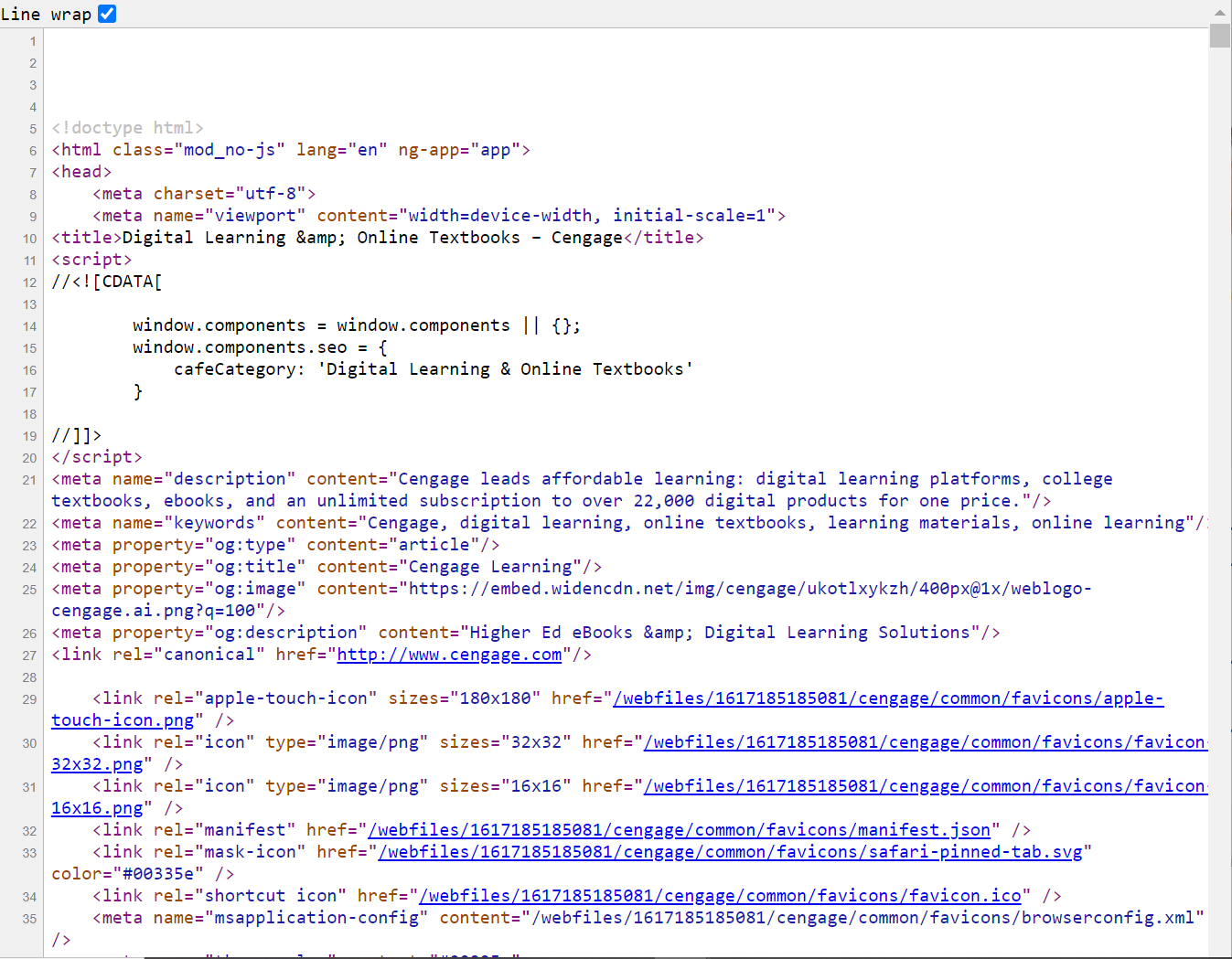
This lab uses a function built into certain web browsers and web sites to support the development of web pages and the assignment of web addresses.

### Opening Web site in Web Browser (CMD)

1. In your browser search bar, go to **www.cengage.com** and press **Enter**.

### Using page source

1. Right click on the web page and select **View Page Source** (note: this is the same command in Chrome, Firefox, and Edge).
2. If you are using Google Chrome, check the **Line wrap** box at the top. You should see results similar to Figure L08-8.

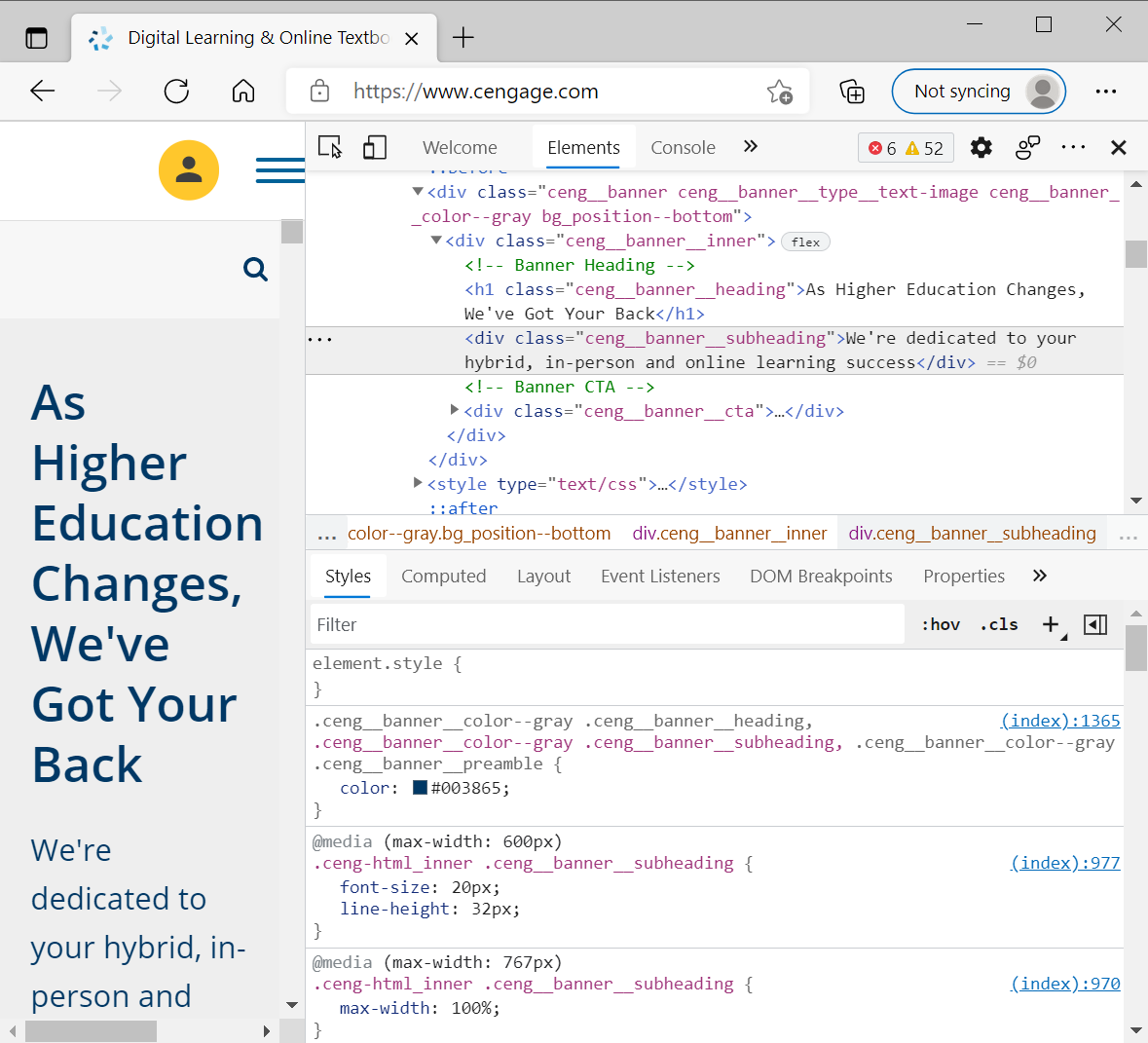


**Figure L08-8** cengage.com view page source results

1. It may be startling to realize you can view the HTML code on most web pages. In the early days of web site design, the web developer would put a good deal of background information in the comments section of the HTML code, including their name, title, phone number, and address, so that if someone found an issue they would know who to contact. Even today, organizations may put information in that they really don’t mean for the average user to be able to view. Attackers will look at this code for clues as to the type of web service, software, operating system, etc. Modern web design emphasizes removing any unnecessary information in the html code to minimize the chance that it can be used to assist an attacker.
2. Scroll down through the code and look for any information that you think an attacker might find useful. Repeat this exercise for your school’s home page.

### Using Inspect

1. Most web browsers have additional tools to assist in web-site development for web developers and unfortunately for attackers will allow them to experiment with the web site code. Using your browser, on the cengage.com home page *right click* and select **inspect**. You should see results like Figure L08-9.



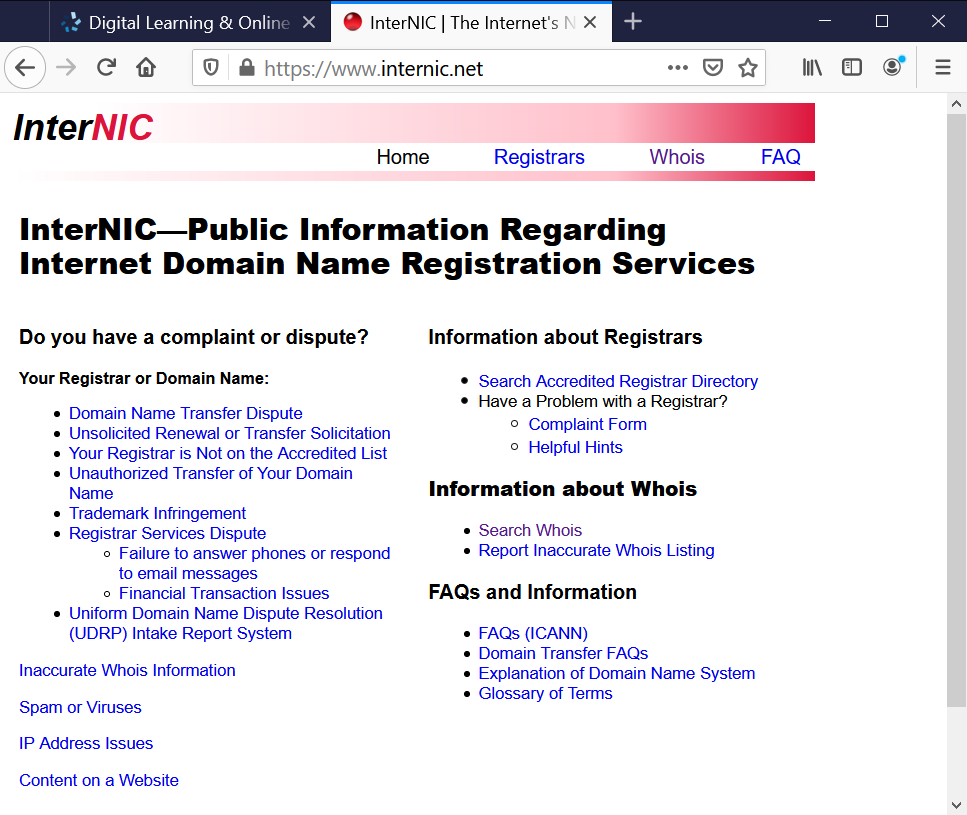
**Figure L08-9** Google Chrome inspect cengage.com results

1. Using this tool, you can change the HTML code and observe the results. Since the editing only takes place on your system, it doesn’t constitute hacking. A talented attacker could, however, experiment to see what they can learn from manipulating the code.

### Using Whois

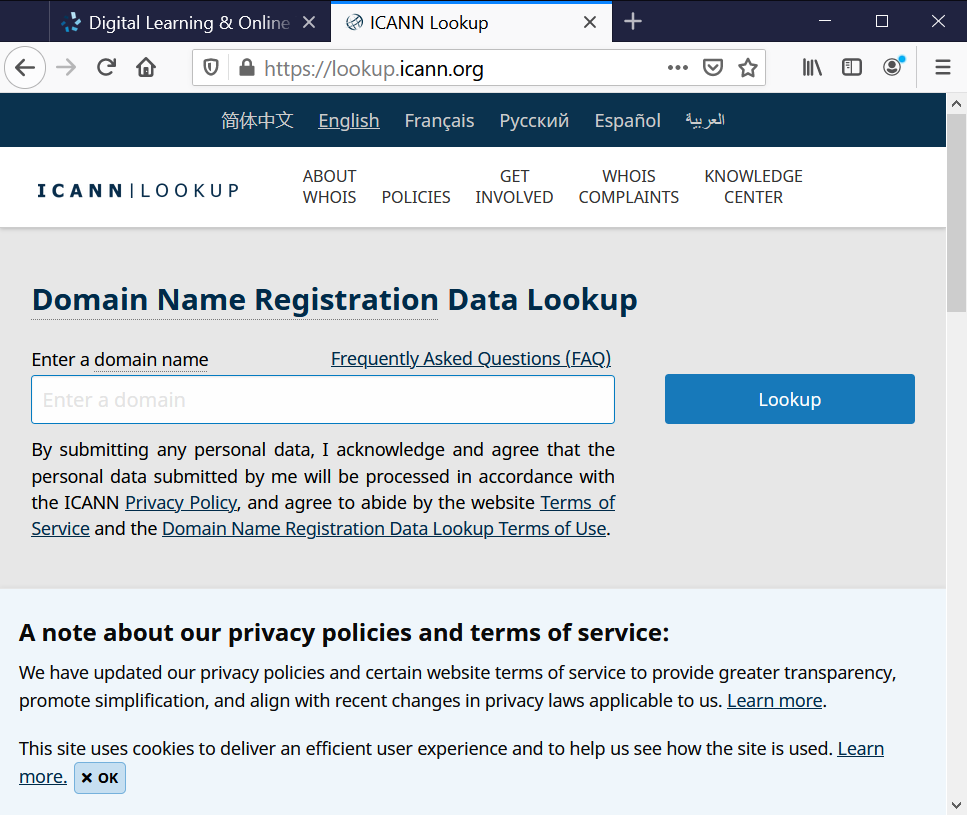
Whois is another network service designed to provide information contained in the Internet’s online databases, like the DNS database and IP registries. Like the other tools, it’s useful to help system and network administrators to troubleshoot problems. Also, like other tools, it can be used by attackers to learn more about an organization’s systems before attempting to directly access them.

1. In the web browser, go to [www.internic.net](http://www.internic.net/). As shown in Figure L08-10, InterNIC is a public database to provide information on domain and IP registrations.



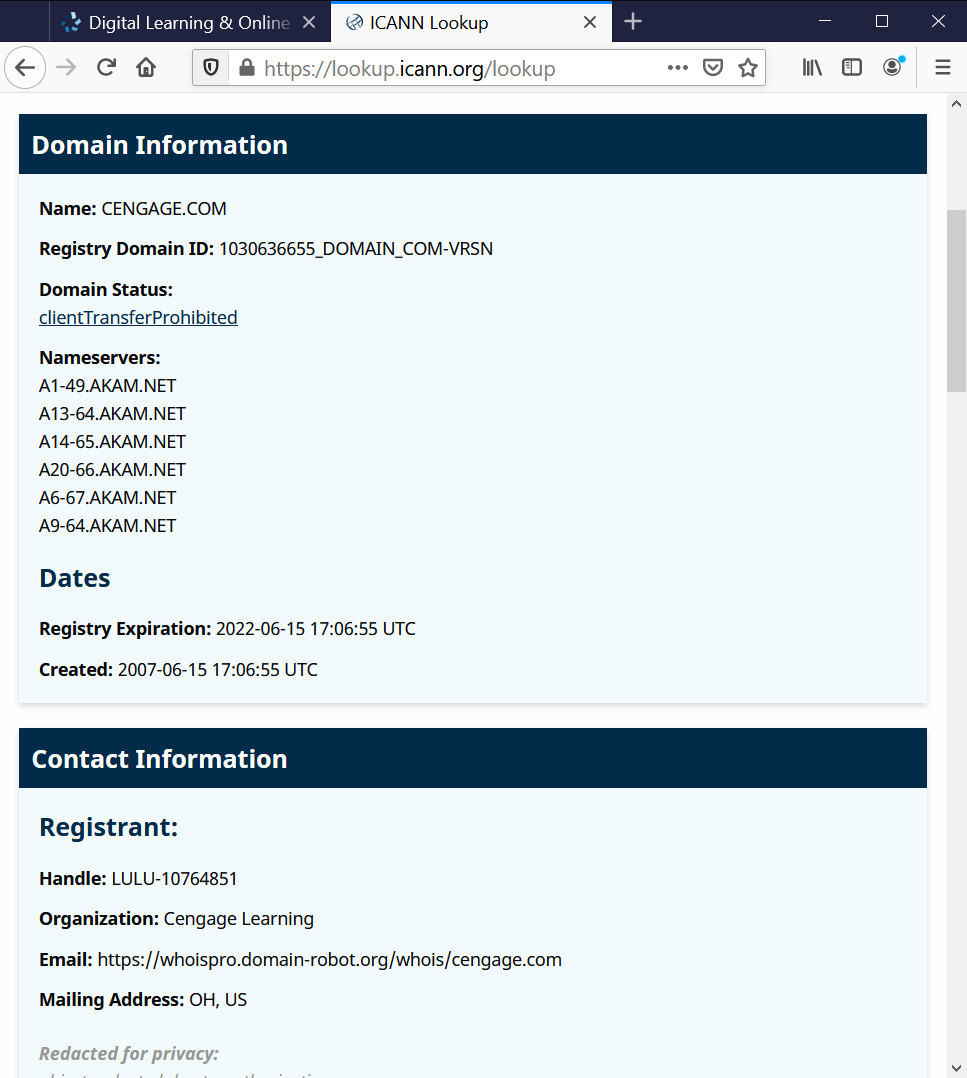
**Figure L08-10** interNIC.net

1. Select the Whois menu option at the top. This will redirect you <https://lookup.icann.org/> as shown in Figure L08-11. ICANN is the non-profit Internet Corporation for Assigned Names and Numbers, responsible for coordinating the databases that manage internet IP addresses and URL names.



**Figure L08-11** ICANN.org

1. Type **cengage.com** in the space provided for Domain Names and press the **Lookup** button. You may have to click to accept the terms of the site in a popup to continue. Scrolling down you should see the information shown in Figure L08-12. Here you will find some of the information previously viewed on the name servers, and domain registration information, among others.



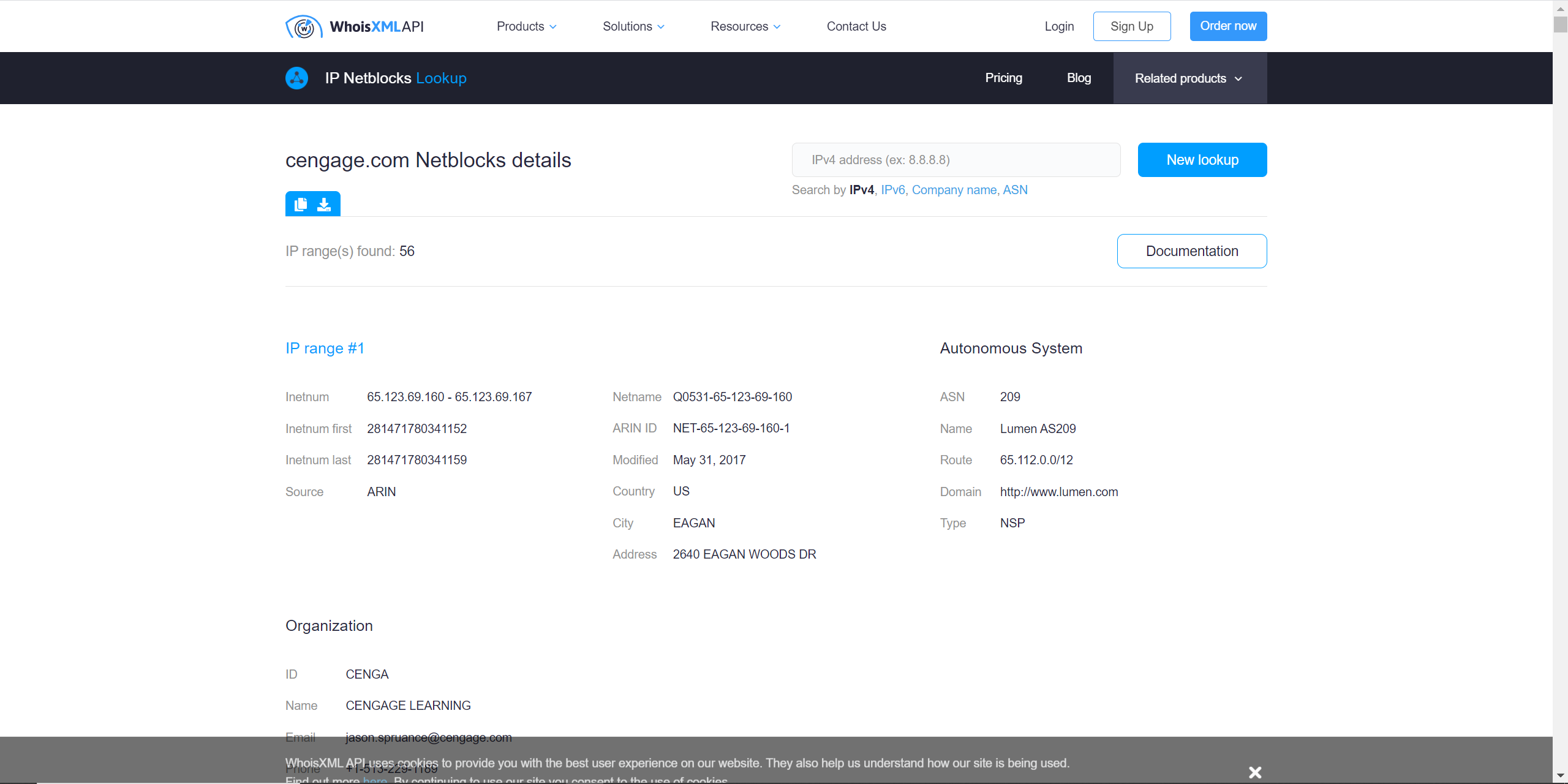
**Figure L08-12** icann.org cengage.com lookup results

1. At the bottom, you can expand the Raw Registry RDAP Response and the Raw Registrar RDAP Response to see the raw data of the various responses. You may notice that several fields have the term “REDACTED FOR PRIVACY: Object redacted due to authorization.” This means the system has been set up to hide some information that could assist attackers. This is a relatively new update to the lookup function. Previously the system would provide a list of all of the IP address ranges and other data associated with the lookup target. If you can’t get what you want here, you may be able to get it from another site.

### Using Other Web Resources

There are many other internet resources that can be used to find out an organization’s IP address range. A quick web search finds ip-netblocks.whiosxmlapi.com/lookup. There are many others.

1. Using your web browser, go to ip-netblocks.whiosxmlapi.com/lookup (or other similar web site), enter cengage.com into the lookup. You should see results like Figure L08-12, which found 56 separate IP address ranges for Cengage.



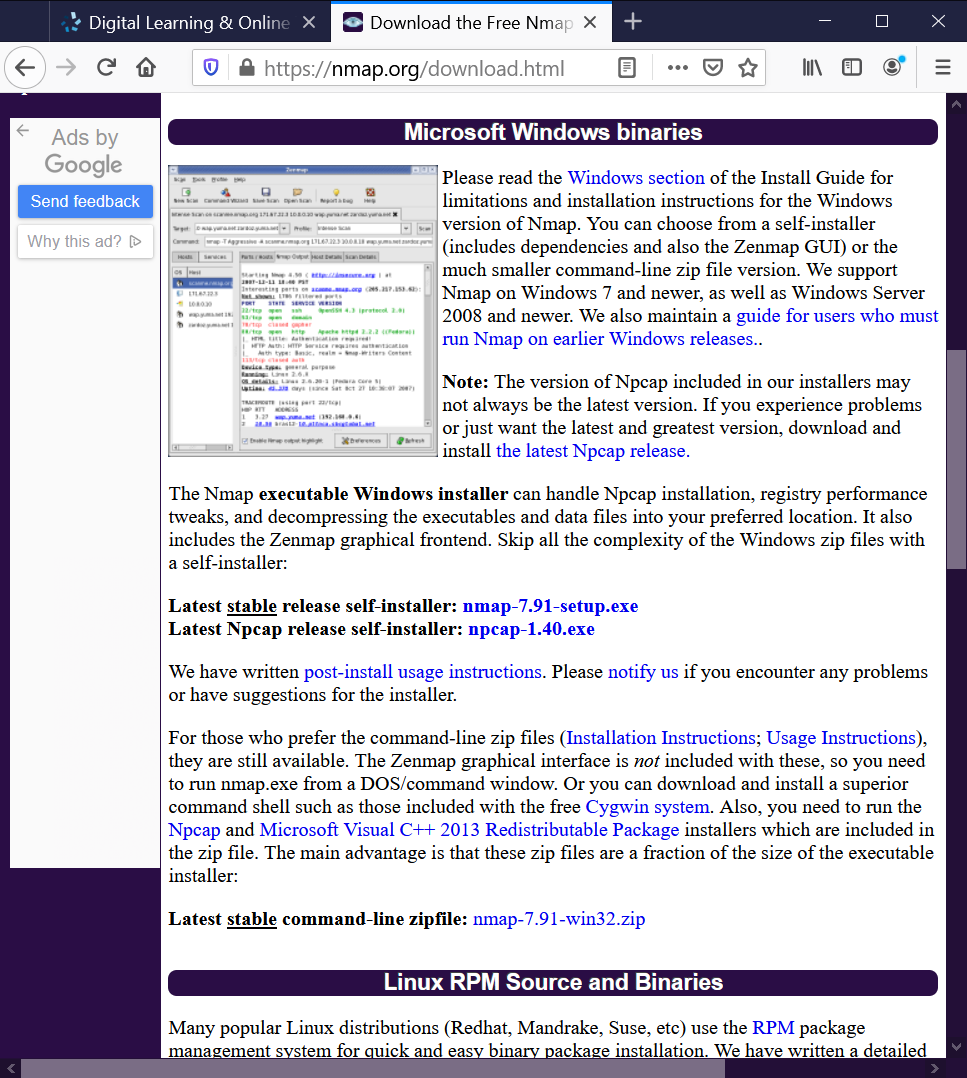
**Figure L08-13** WhoisXMLAPI cengage.com results

1. An attacker could then use these address ranges in other, more sophisticated tools to begin probing the target’s systems to determine more about them. However, a) do not do this, and b) this concludes the “footprinting” section of the lab. Having started with just a domain name, you now know about the target’s DNS server, Name Servers, Mail Servers, and all of the IP address ranges that are assigned to the organization.

## Scanning with Nmap

In this lab, students will scan a network to discovery all systems and then inventory their operating systems and services. Systems administrators use Nmap regularly, however so do attackers. Due to its free and open-source nature, it is a tool of choice for those who don’t wish to expend the funds for an expensive commercial competitor.

### Download and Install Nmap

1. Begin by checking to see if Nmap has already been installed. If not, use a web browser and go to **https://nmap.org/**. There are many resources here beyond what this lab will entail, including a complete installation guide, documents, and references.
2. Click on the Download link on the left. For this lab, you will be downloading both Nmap and Zenmap – the graphical front end for Nmap. Nmap itself is a command line utility. For our purposes, the Zenmap GUI will make our tasks easier. Scroll down to the **Microsoft Windows binaries** section shown in Figure L08-14 and click the link next to **Latest stable release self-installer:** in our case ***nmap-7.91-setup.exe***. You may see a newer edition as Nmap is regularly updated and supported. Save the file to a directory you can easily access later.
3. 

**Figure L08-14** Nmap download information

1. Once the download has finished, double click the .exe to install, and agree to the License Agreement.
2. Accept the default settings in **Choose Components** and click **Next >**.
3. Specify the directory Nmap will install to and click **Install**.
4. You will be required to accept another License Agreement for Npcap (packet capture utility) at this point, then specify installation options. We recommend accepting the defaults, unless you plan to scan a wireless network, in which case you can add that option. Click **Install** again.
5. Click **Next** once completed, then **Finish**.
6. Nmap will finalize overall installation, select **Next >**, accept the Shortcuts by clicking **Next >** again, then click **Finish** one more time.

### Use Nmap

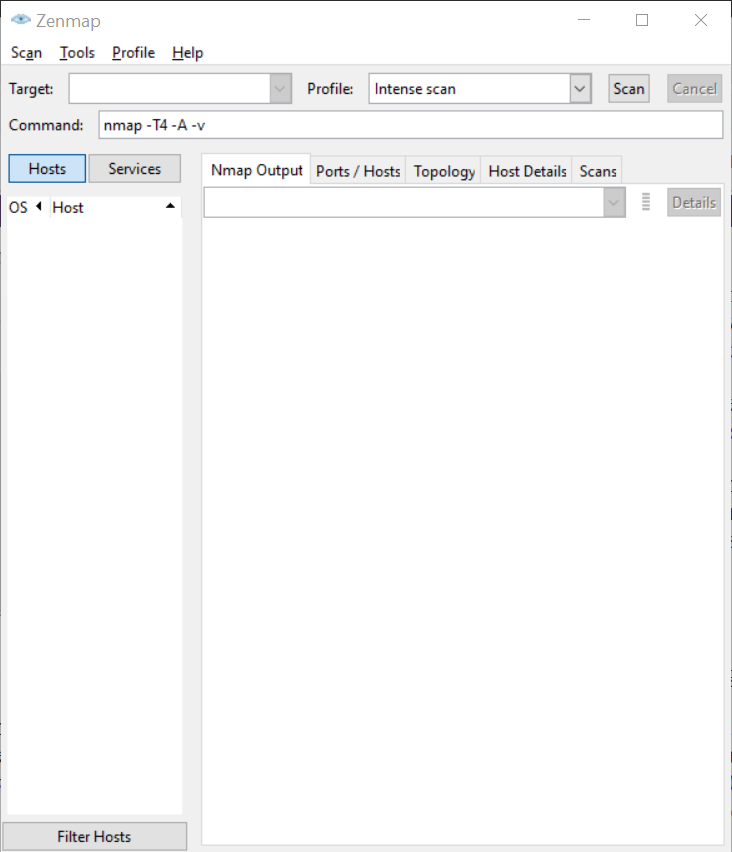
**Do NOT use Nmap on a network that you do not have explicit permission to scan.** Legally you may only scan a network that a) you own, b) you have permission from the systems owner to scan, and c) all users on that system know they may be scanned and have consented to such a scan. Normally the organization owns the network, the CEO or their designated representative (e.g. the CIO) gives permission, and all users acknowledge the need to scan the system in their annual security briefing – and sign a document acknowledge this (along with a list of other necessary activities).

Failure to follow these instructions can result in a loss of Internet Services by your ISP, and/or legal ramification.

**Again, do NOT simply enter a target address and begin scanning.** All examples are provided on a privately owned network by the system owner, with full knowledge by all users.

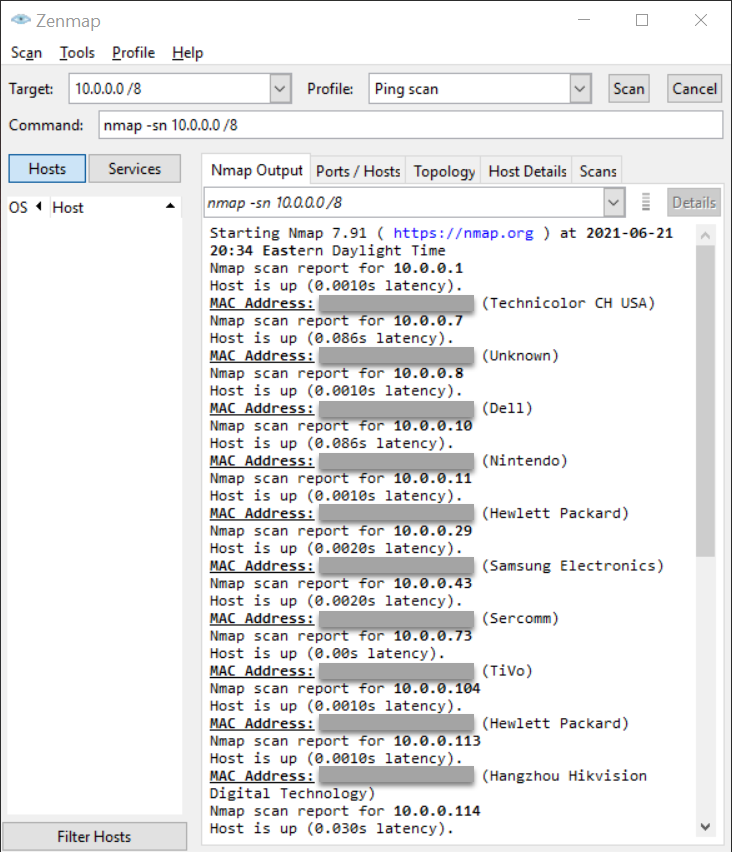
* The Nmap user’s guide is located at <https://nmap.org/book/man.html>.
* Portions of the book “The Official Nmap Project Guide to Network Discovery and Security Scanning” by Gordon “Fyodor” Lyon, are available at <https://nmap.org/book/toc.html>.
* The portion of the book pertaining to Zenmap are located at <https://nmap.org/book/zenmap.html>.

1. Start Nmap by double clicking the **Nmap-Zenmap** desktop icon or selecting it from the Windows menu. The Zenmap GUI will begin as shown in Figure L08-15 below.



**Figure L08-15** Nmap Zenmap Interface

1. The first thing you should note is the Command window which shows the command line for nmap with the default options. You can look up these options at: <https://nmap.org/book/man-briefoptions.html>.
2. Begin with a ping scan, which will simply ping all addresses in the assigned range. Select Ping scan in the pull-down menu next to **Profile**.
3. Next, specify the system(s) or network(s) by entering the IP address in the **Target:** field. The example network is a Class C address in the 10.X.X.X private networking class. The entry in the example is **10.0.0.0 /8** which tells the system that a) it’s an IPv4 address, b) it’s multiple systems on a network segment and c) the right-most 8 bits are the host address, and the rest are the network address. Since all the systems on this network are in this range (10.0.0.1 to 10.0.0.253) this simplifies the scan. Enter your assigned address range in this format:
   1. IP address if one system
   2. IP address and the CIDR extension e.g. /8 for multiple systems on a network   
      Note: you can also use hyphenated ranges (e.g. 10.0.0.1-253)  
      See <https://nmap.org/book/man-target-specification.html> for additional specifications.
4. Click Scan. Since this is a relatively simple scan, the response should be quick. As shown in Figure L08-16, you will see the MAC and IP addresses for any hosts the system detects. (Note: Since MAC addresses are hard coded to specific and identifiable devices, they’ve been redacted in the example.)



**Figure L08-16** Sample Nmap Ping Scan results

1. As is *obvious* from this example, the scanned network is a home network, with several networked technologies. The “Internet of Things” has resulted in an explosion of networked technologies, which must be protected as well. These networked devices may be exploited by an attacker resulting in unwanted breaches of privacy and loss of personal information.
2. Set the value in the Profile: field with **Quick scan plus** and click **Scan**. This will take longer than the previous scan (several minutes) but will provide more detailed information. It is generally recommended NOT to use the Intense scan as there is a chance the scan can cause the scanned system to crash.
3. As you can see from Figure L08-17, you now get detailed information on the OS (as far as Nmap can determine) and open and available ports (color coded no less). The two systems shown are in fact a managed Cisco network switch, and a Dell Windows 7 PC.
4. When finished with the lab, close the Zenmap window. Uninstall if promoted by your instructor.



**Figure L08-17** Nmap Quick scan plus results

# Self-Reflection and Response

Some of the activties in this lab were flagged as being considered potentially hostile unless you have permission to do them. Why would a company want to keep network users from using thse tpye of tools?

|  |
| --- |
| Critical information about the network can be gained by using nmap and similar tools. Nmap will make guesses as to what OS is running on a system and will also point out known vulnerabilities that can exploit unpatched systems. |

Can you think of reasons why you would need to be able to determine who controls a web address or web site?

|  |
| --- |
| A simple reason that you may need to determine who controls a web site or address is to verify that it is a valid website. Another reason to know who controlled a web site, would be to contact the owner of the site. |

What are some reasons you may want to use nmap on your own network?

|  |
| --- |
| I check the network often to see if there are additional devices connected to my network, also nmap can show what ports are open on devices so that you can close unnecessary ports. |

## Instructor’s Response

|  |
| --- |
|  |