Covers all Exam Objectives for CEHv6

Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

CEH™

Certified Ethical Hacker

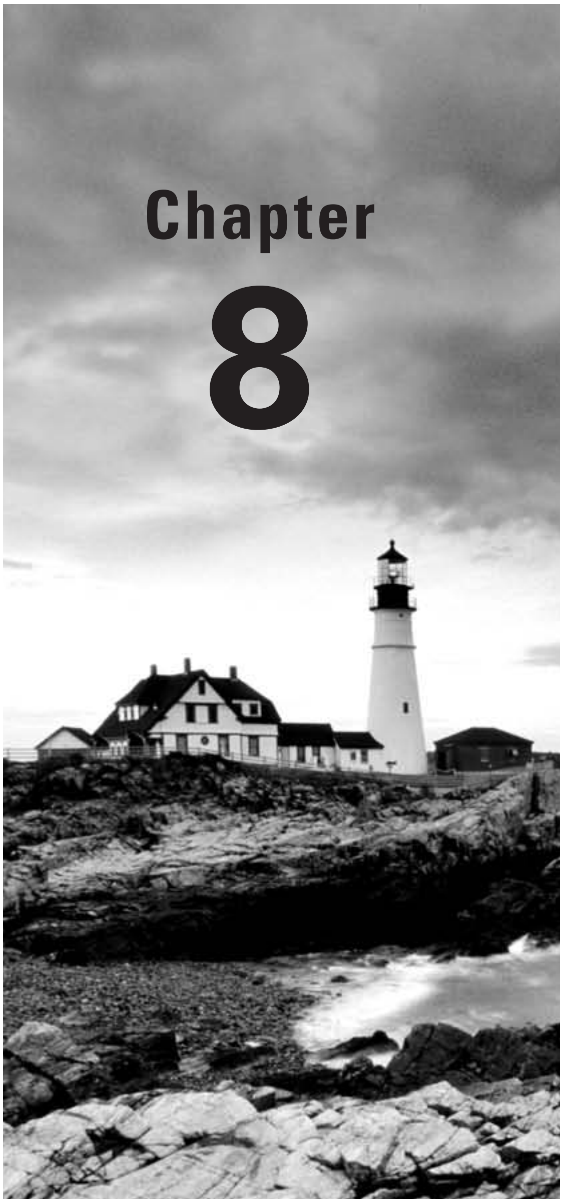
STUDY GUIDE

Exam 312-50
Exam EC0-350

Kimberly Graves

SYBEX | SERIOUS SKILLS.

Table of Contents



Chapter

8

Web Hacking: Google, Web Servers, Web Application Vulnerabilities, and Web-Based Password Cracking Techniques

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ List the types of web server vulnerabilities
- ✓ Understand the attacks against web servers
- ✓ Understand IIS Unicode exploits
- ✓ Understand patch-management techniques
- ✓ Understand Web Application Scanner
- ✓ What is the Metasploit Framework?
- ✓ Describe web server hardening methods
- ✓ Understand how web applications work
- ✓ Objectives of web application hacking
- ✓ Anatomy of an attack
- ✓ Web application threats
- ✓ Understand Google hacking
- ✓ Understand web application countermeasures

- ✓ **List the authentication types**
- ✓ **What is a password cracker?**
- ✓ **How does a password cracker work?**
- ✓ **Understand password attacks—classification**
- ✓ **Understand password-cracking countermeasures**

This chapter introduces the essentials of hacking web servers and exploiting web server and web application vulnerabilities. Web-based password-cracking techniques are also covered.

Web servers and web applications have a very high potential to be compromised. The primary reason for this is that the systems that run web server software must be publicly available on the Internet. The web server cannot be completely isolated and to some degree must be available to legitimate users. Once a web server has been compromised, the system can provide hackers with another door into the network. Not only the web server software but also applications that run on the web server are open to attack and can be exploited. Due to their function, web servers are more accessible than other systems and less protected, so they're easier to exploit.

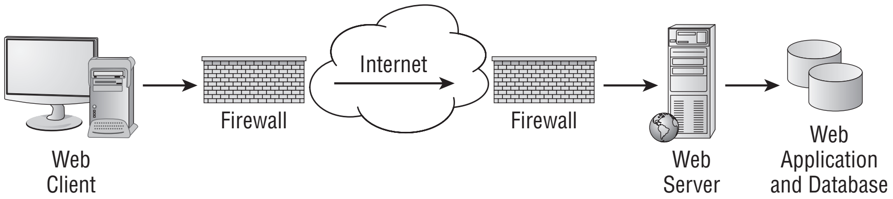
The target information on a web server usually resides in a database on the web server; this database is accessed via a web application. For this reason, web servers and web applications go hand in hand. Compromising the web server is usually done to gain access to the underlying data in the web application.

How Web Servers Work

Web servers use Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) to allow web-based clients to connect to them and view and download files. HTTP is an Application-layer protocol in the TCP/IP stack. HTTP and HTTPS are the primary protocols used by web clients accessing web pages residing on web servers on the Internet. Hypertext Markup Language (HTML) is the language used to create web pages and allows those pages to be rendered in web browser software on web clients.

The HTTP protocol operates as shown in Figure 8.1.

FIGURE 8.1 HTTP protocol components



1. The web client initially opens a connection to the web server IP address using TCP port 80.
2. The web server waits for a GET request from the client requesting the home page for the website.
3. The web server responds with the HTML code for the web server home page.
4. The client processes the HTML code and the web client's browser software renders the page on the client device.

Understanding how web servers work—and consequently how they are hacked—is an important part of your job as a CEH. This includes knowing their vulnerabilities, as well as understanding the types of attacks a hacker may use. In addition, you should know when to use patch-management techniques and understand the methods used to harden web servers.

We'll look at all these topics in the following sections.

Types of Web Server Vulnerabilities

Web servers, like other systems, can be compromised by a hacker. The following vulnerabilities are most commonly exploited in web servers:

Misconfiguration of the Web Server Software A common issue with using Microsoft's Internet Information Server (IIS) as a web server is the use of the default website. The permissions on the default website are open, meaning the default settings leave the site open to attack. For example, all users in the everyone group have full control to all the files in the default website directory. It is critical to edit and restrict permissions once IIS is installed on the server as the default system user, IUSR_COMPUTERNAME, is a member of the everyone group. Consequently, anyone accessing the default website will be able to access all files in the default website folder and will have dangerous permissions such as Execute and Full Control to the files. See Exercise 8.1 to learn how to disable the default website in IIS.

Operating System or Application Bugs, or Flaws in Programming Code All programs, including the OS and web server applications, should be patched or updated on a regular basis. For Windows systems, this includes security patches, hotfixes, and Windows Updates. All of these patches can be automated or manually applied to the systems once they have been tested.

Vulnerable Default Installation Operating system and web server software settings should not be left at their defaults when installed, and should be updated on a continuous basis.

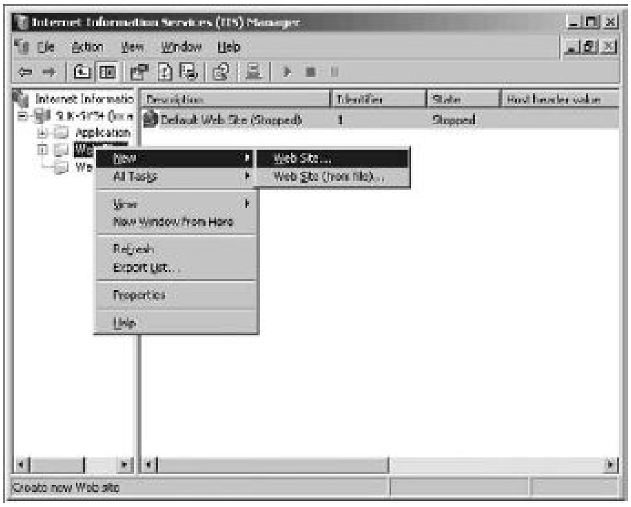
Hackers exploit these vulnerabilities to gain access to the web server. Because web servers are usually located in a demilitarized zone (DMZ)—which is a publicly accessible area between two packet filtering devices and can be easily accessed by the organization's client systems—an exploit of a web server offers a hacker easier access to internal systems or databases.

EXERCISE 8.1

Disabling the Default Website in Internet Information Server

To disable the default website in IIS and add a new site, follow these steps:

1. Open IIS on your Windows Server or virtual machine (VM).
2. Select Web Sites in the left pane.
3. Right-click the default website in the right pane and select Stop from the context menu. The default website is now stopped.
4. To create a new site, right-click Web Sites in the left pane and select New ➢ Web Site.

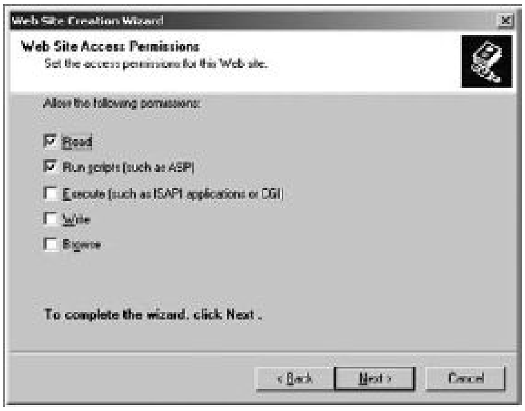


Internet Information Services (IIS) Manager

Description	Identifier	State	Host header value
Default Web Site (Stopped)	1	Stopped	

Create new Web site

5. The Web Site Creation Wizard launches. Within the wizard will be a screen to change permission on the website directory.



Web Site Creation Wizard

Web Site Access Permissions
Set the access permissions for this Web site.

Allow the following permissions:

☑ Read
☑ Run scripts (such as ASP)
☐ Execute (such as ISAPI applications or CGI)
☐ Write
☐ Browse

To complete the wizard, click Next .

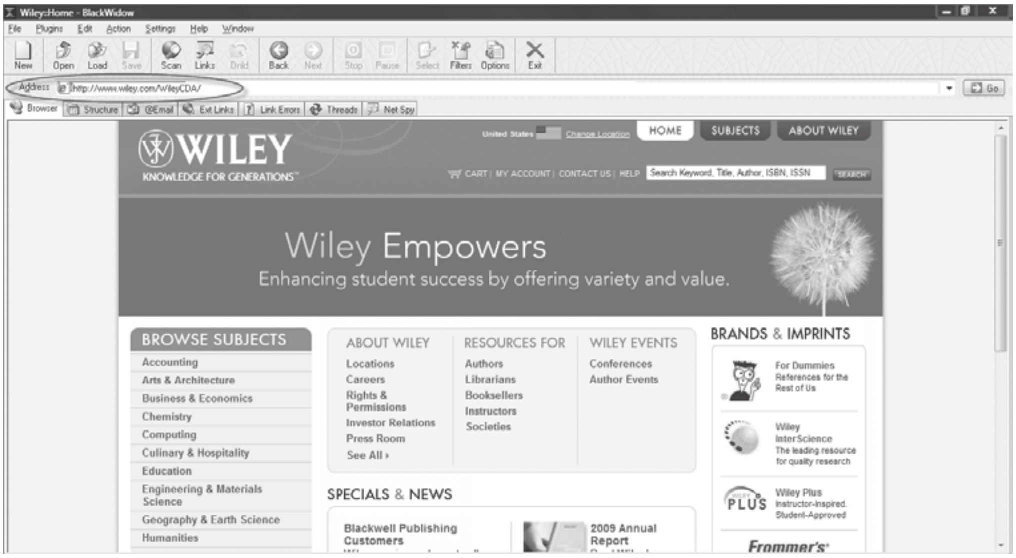
Website cloaking is the ability of a web server to display different types of web pages based on the user's IP address.

In many cases, it is useful to gather all or a portion of the files that make up a website. One option is to right-click any web page and select View Source from the context menu. This command will open up a new window with the source code for the page. You can then save the text file as a document on the local machine. This approach works, but it isn't a practical way of copying all the files for a target website. An easy-to-use program called BlackWidow can make the process of copying website files much easier. Exercise 8.2 shows you how to use the BlackWidow program to copy an entire website or a portion of the site.

EXERCISE 8.2

Using BlackWidow to Copy a Website

1. Download and install the BlackWidow application from `www.softbytelabs.com`.
2. Open the BlackWidow program.
3. Enter a target website address in the BlackWidow address bar:



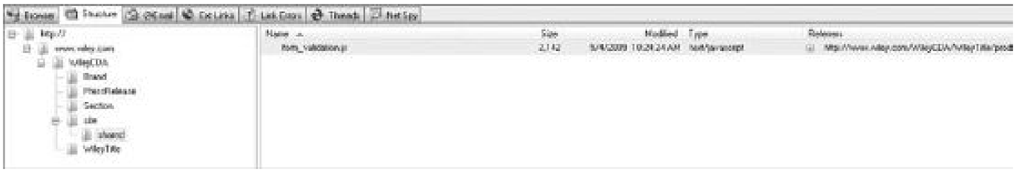
Address http://www.wiley.com/WileyCDA/

Wiley::Home - BlackWidow
File Plugins Edit Action Settings Help Window
New Open Load Save Scan Links Dnld Back Next Stop Pause Select Filters Options Exit
Go
Browser Structure @Email Ext Links Link Errors Threads Net Spy
WILEY
KNOWLEDGE FOR GENERATIONS
HOME SUBJECTS ABOUT WILEY
Wiley Empowers
Enhancing student success by offering variety and value.
BROWSE SUBJECTS
ABOUT WILEY
RESOURCES FOR
WILEY EVENTS
BRANDS & IMPRINTS
SPECIALS & NEWS

4. Click the Scan button on the BlackWidow toolbar.
5. Click the Structure tab.

EXERCISE 8.2 *(continued)*

6. Browse the website folder structure. Right-click a file or folder and choose Copy Selected Files to copy the website files to your computer.



Attacking a Web Server

Web servers typically listen on TCP port 80 (HTTP) and TCP port 443 (HTTPS). Because those ports must be open and available to web clients, any firewalls or packet filtering devices between the web client and web server must pass traffic destined for those ports. Web application software sits on top of the web server software and allows access to additional ports.

One of the initial information-gathering steps targeting web servers is *banner grabbing*. Banner grabbing is an attempt to gather information about a web server such as the OS and web server software and version. Exercise 8.3 shows you how to use banner grabbing.

EXERCISE 8.3

Banner Grabbing

1. At the command prompt on your Windows PC, type

```
telnet <IPaddress> 80
```

The IP address is the address of the web server target. Also, the URL can be used instead of the IP address.

2. Next, in the telnet window type

```
HEAD/HTTP/1.0
```

Then press Enter.

The web server banner will then be returned. The banner will look something like the following:

```
Server: Microsoft-IIS/5.0
Date: Fri, 14 Aug 2009 1:14:42 GMT
Content-Length:340
Content-Type: text/html
```

The banner grabbing result will usually identify the web server type and version. This information is important because exploits against this web server type and version can be identified. The next step after banner grabbing would be to attack the web server or attack a web application and gain access to data on the server.

A benign but visible type of attack against web servers is defacement. Hackers deface websites for sheer joy and an opportunity to enhance their reputations rather than gathering any useful data. *Defacing* a website means the hacker exploits a vulnerability in the OS or web server software and then alters the website files to show that the site has been hacked. Often the hacker displays their hacker name on the website's home page.

Common website attacks that enable a hacker to deface a website include the following:

- Capturing administrator credentials through man-in-the-middle attacks
- Revealing an administrator password through a brute-force attack
- Using a DNS attack to redirect users to a different web server
- Compromising an FTP or email server
- Exploiting web application bugs that result in a vulnerability
- Misconfiguring web shares
- Taking advantage of weak permissions
- Rerouting a client after a firewall or router attack
- Using SQL injection attacks (if the SQL server and web server are the same system)
- Using telnet or Secure Shell (SSH) intrusion
- Carrying out URL poisoning, which redirects the user to a different URL
- Using web server extension or remote service intrusion
- Intercepting the communication between the client and the server and changing the cookie to make the server believe that there is a user with higher privileges (applies to cookie-enabled security)

Exercise 8.4 walks you through using the Metasploit Framework to exploit a web server vulnerability.

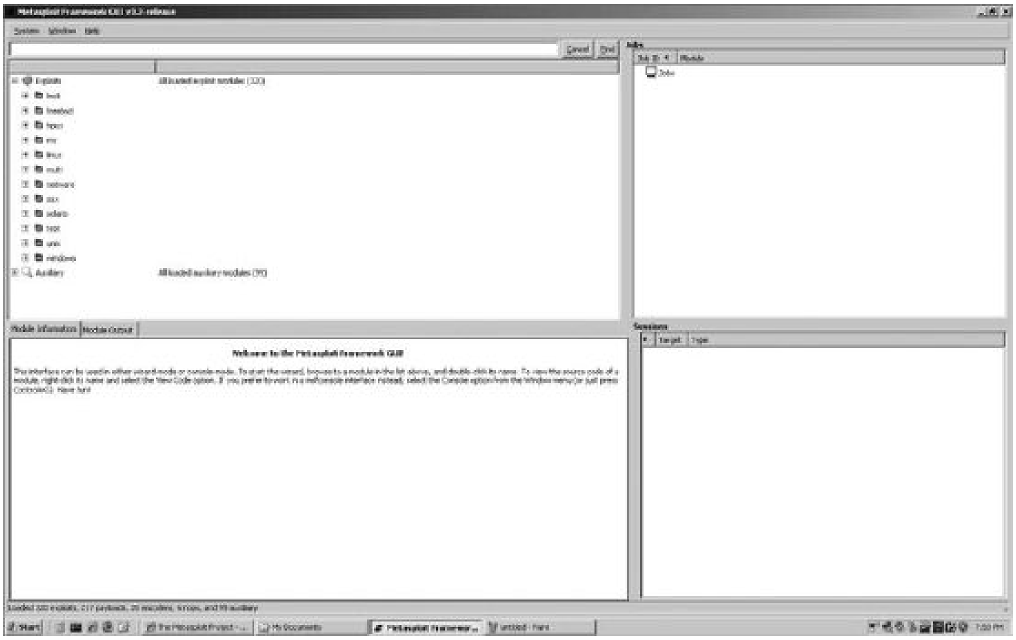
WARNING

It is important that the machine or VM have all antivirus and firewall programs completely shut down prior to installing Metasploit. Otherwise, the antivirus or firewall can block some components of Metasploit, causing it not to function or open properly. As we mentioned in the lab setup guide in the Introduction to this book, you should never install Metasploit on a production machine. Use either a VM or lab test machine to run this software.

EXERCISE 8.4

Using Metasploit to Exploit a Web Server Vulnerability

1. Download and install Metasploit 3.2 on your Windows XP or Vista computer or VM (`www.metasploit.com`).
2. Choose all the default options when installing Metasploit.
3. Select the Online Update option in the Metasploit 3 folder under Programs.
4. After the online update has completed, open the Metasploit GUI file in the Metasploit 3 folder.



Welcome to the Metasploit Framework GUI

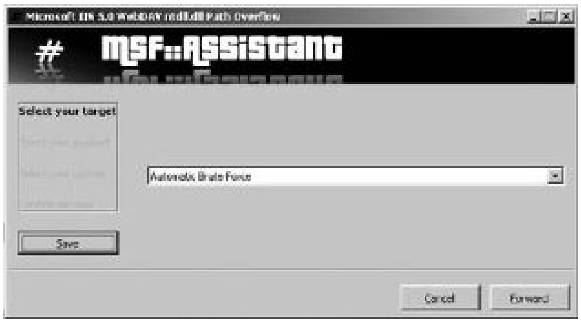
This interface can be used in either wizard-mode or console-mode. To start the wizard, browse to a module in the list above, and double-click its name. To view the source code of a module, right-click its name and select the View Code option. If you prefer to work in a msfconsole interface instead, select the Console option from the Window menu (or just press Control+O). Have fun!

Loaded 320 exploits, 217 payloads, 20 encoders, 6 nops, and 99 auxiliary

5. Expand the Windows folder under Exploits and then expand the IIS folder.

EXERCISE 8.4 ***(continued)***

6. Double-click the `ms03_007_ntdll_webdav` exploit. The MSF Assistant Wizard launches.



Microsoft IIS 5.0 WebDAV ntdll.dll Path Overflow

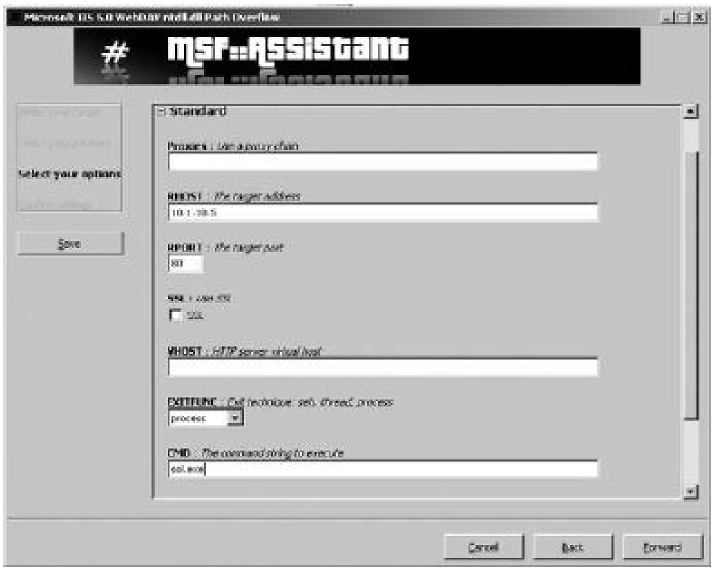
Automatic Brute Force

7. Click the Forward button to move to the next screen of the wizard.

8. Select Windows/Exec from the Payload drop-down list, and then click Forward.

9. Type the IP address of the target IIS web server in the RHOST field. *This server should be an unpatched version of Windows 2000 for this particular payload to work. If that is not the case, choose a different payload to which the server is vulnerable.*

10. Type **`sol.exe`** in the CMD field. This is the executable that will be run on the remote target host. `sol.exe` is the solitaire game, which should be on all Windows operating systems. The payload is what will be delivered to the target system. In this case, it is similar to typing **`sol.exe`** at the command prompt of the IIS server. Obviously this executable is benign, but this exercise illustrates how a more dangerous executable, such as a virus or Trojan, could be run on a target system.



Microsoft IIS 5.0 WebDAV ntdll.dll Path Overflow

Proxies : *Use a proxy chain*

RHOST : *The target address*
10.1.38.5

RPORT : *The target port*
80

SSL : *Use SSL*
□ SSL

VHOST : *HTTP server virtual host*

EXITFUNC : *Exit technique: seh, thread, process*
process

CMD : *The command string to execute*
sol.exe

EXERCISE 8.4 *(continued)*

11. Click the Forward button to move to the next screen of the wizard.
12. Click the Apply button. The exploit will appear under Jobs until it is delivered to the target system.
13. Confirm in the Windows IIS Server VM or on the IIS PC that the Solitaire program is running. If the program is not running, confirm that Solitaire is installed on the IIS server and try the Metasploit exploit again.

Hacking Internet Information Server

Windows IIS is one of the most popular web server software products. Because of the popularity and number of web servers running IIS, many attacks can be launched against IIS servers. The three most common attacks against IIS are as follows:

- Directory traversal
- Source disclosure
- Buffer overflow

A *directory-traversal attack* is based on the premise that web clients are limited to specific directories within the Windows files system. The initial directory access by web clients is known as the *root directory* on a web server. This root directory typically stores the home page usually known as Default or Index, as well as other HTML documents for the web server. Subdirectories of the root directory contain other types of files; for example, scripts may contain dynamic scripting files for the web server. The web server should allow users to access only these specific directories and subdirectories of root. However, a directory-traversal attack permits access to other directories within the file system.

Windows 2000 systems running IIS are susceptible to a directory-traversal attack, also known as the Unicode exploit. The vulnerability in IIS that allows for the directory traversal/Unicode exploit occurs only in unpatched Windows 2000 systems and affects CGI scripts and Internet Server Application Programming Interface (ISAPI) extensions such as `.asp`. The vulnerability exists because the IIS parser was not properly interpreting Unicode, thus giving hackers system-level access.

Essentially, Unicode converts characters of any language to a universal hex code specification. However, the Unicode is interpreted twice, and the parser only scans the resulting request once (following the first interpretation). Hackers could therefore sneak file requests through IIS. For example, utilizing `%c0% af` instead of a slash in a relative pathname exploits the IIS vulnerability. In some cases, the request lets the hacker gain access to files that they otherwise shouldn't be able to see. The Unicode directory traversal vulnerability allows a hacker to add, change, or delete files, or upload and run code on the server. The ability to add or run files on the system enables a hacker to install a Trojan or backdoor on the system.

NOTE The IIS Unicode exploit is an outdated vulnerability and is presented in this text as a proof of concept—that is, proof that the vulnerability exists and can be exploited.

Buffer overflow attacks are not unique to web servers and can also be launched against other types of systems. A buffer overflow involves sending more data, usually in the form of a text string, than the web server is capable of handling. The primary entry point for buffer overflows is a web form on the web server. Buffer overflows and countermeasures will be covered in detail in the next chapter.

Source disclosure attacks occur when the source code of a server application can be gathered. Source disclosure attacks can lead to a hacker identifying the application type, programming language, and other application-specific information. All this information can allow a potential hacker to identify security holes and potential exploits that can be delivered to the web server. Again, most of a hacker's time is spent gathering information about a target in order to identify the best point of entry for an exploit.

Putting It All Together Using Source Disclosure Attacks

An example of performing a source disclosure attack would be to run BlackWidow against a web server and copy all the files to a local directory. In reviewing the source files from BlackWidow, you can obtain the name of the server, the IP address, and the version. Additional information-gathering tools such as Netcraft can aid in the discovery of the OS, web server software type, and version. Additional information may be gathered regarding the JavaScript (`.js` files) or Active Server Pages (`.asp` files) that reside on the server. Based on the web server applications and vulnerabilities, Metasploit can be used to deliver a payload to the server. Depending on the patch level and vulnerability, the payload can be fairly benign or serious enough to cause the hacker to gain access to valuable data. The best countermeasure to the source disclosure attack and other types of attacks is to patch the OS, web server, and all server applications to the most current level and maintain an active patch-management program.

A CEH must be aware of all the information-gathering techniques to identify potential vulnerabilities in web servers and web applications. The reason this knowledge is so important for the CEH is so that they can defend against the same attacks and implement countermeasures to prevent attacks.

Patch-Management Techniques

Patch management plays a critical role in preventing and mitigating the risk of attack against web servers and web applications. *Patch management* is the process of updating appropriate patches and hotfixes required by a system vendor. Proper patch management involves choosing how patches are to be installed and verified, and testing those patches on a non-production network prior to installation.

You should maintain a log of all patches applied to each system. To make patch installation easier, you can use automated patch-management systems provided by PatchLink, St. Bernard Software, Microsoft, and other software vendors to assess your systems and decide which patches to deploy.

Real World Scenario

First Week on the Job as a Web Administrator

As a newly hired network administrator for a small company of 40 employees, it was my responsibility to review the configuration and patches for a small network with two servers. The company used IIS 5.0 on a Windows 2000 server that had been serving the corporate website to clients for three years. The servers had been installed and configured by a consulting company three years prior to my joining the staff. The website content was updated regularly by the marketing assistant, but no other update had been made to the server.

So, I embarked upon updating and performing patch management on the web server. The company had no firewall protecting the Internet connection, and the Windows Server OS had not had any patches or hotfixes applied to it since installation. The IIS web server software was also out of date. All of this presented a huge security risk to the organization, and patch management was the highest priority to protect the web server and applications running on it.

As I applied security patches and hotfixes, to first the OS and then IIS, I found that malware, such as the Code Red worm and numerous viruses, had already attacked the system. It took several days of applying patches and hotfixes and updating virus definitions before the web server was brought up-to-date. Luckily for the small company, I was able to bring the OS and web server software up-to-date and implement a system for patch management before the network was damaged or a serious security breach occurred.

Hacking Tools

N-Stalker Web Application Security Scanner allows you to assess a web application for a large number of vulnerabilities, including cross-site scripting, SQL injection, buffer overflow, and parameter-tampering attacks.

The Metasploit Framework is a freeware tool used to test or hack operating systems or web server software. Exploits can be used as plug-ins, and testing can be performed from a Windows or Unix platform. Metasploit was originally a command-line utility, but it now has a web browser interface. Using Metasploit, hackers can write their own exploits as well as utilize standard exploits.

CORE IMPACT and SAINT Vulnerability Scanner are commercial exploit tools used to test and compromise operating systems and web server software.

Web Server Hardening Methods

A web server administrator can do many things to *harden* a server (increase its security). The following are ways to increase the security of the web server:

- Rename the administrator account, and use a strong password. To rename the administrator account in Windows, open the User Manager, right-click the Administrator account, and select Rename.
- Disable default websites and FTP sites. The process to disable default websites was described earlier in this chapter: right-click the default website in IIS Manager and choose Stop. The same process works for the default FTP site.
- Remove unused applications from the server, such as WebDAV. Unnecessary applications can be removed on a server by using Add/Remove Programs in the Windows Control Panel.
- Disable directory browsing in the web server's configuration settings.
- Add a legal notice to the site to make potential attackers aware of the implications of hacking the site.
- Apply the most current patches, hotfixes, and service packs to the operating system and web server software.
- Perform bounds checking on input for web forms and query strings to prevent buffer overflow or malicious input attacks.
- Disable remote administration.
- Use a script to map unused file extensions to a 404 ("File not found") error message.
- Enable auditing and logging.

- Use a firewall between the web server and the Internet and allow only necessary ports (such as 80 and 443) through the firewall.
- Replace the GET method with the POST method when sending data to a web server.

Web Application Vulnerabilities

In addition to understanding how a hacker can exploit a web server, it's important for a CEH to be familiar with web application vulnerabilities. In this section, we'll discuss how web applications work, as well as the objectives of web application hacking. We'll also examine the anatomy of a web application attack and some actual web application threats. Finally, we'll look at Google hacking and countermeasures you should be familiar with.

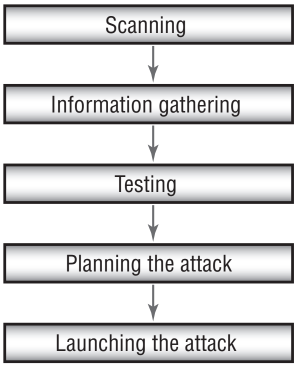
Web applications are programs that reside on a web server to give the user functionality beyond just a website. Database queries, webmail, discussion groups, and blogs are all examples of web applications.

A web application uses a client/server architecture, with a web browser as the client and the web server acting as the application server. JavaScript is a popular way to implement web applications. Because web applications are widely implemented, any user with a web browser can interact with most site utilities.

The purpose of hacking a web application is to gain confidential data. Web applications are critical to the security of a system because they usually connect to a database that contains information such as identities with credit card numbers and passwords. Web application vulnerabilities increase the threat that hackers will exploit the operating system and web server or web application software. Web applications are essentially another door into a system and can be exploited to compromise the system.

Hacking web applications is similar to hacking other systems. Hackers follow a five-step process: they scan a network, gather information, test different attack scenarios, and finally plan and launch an attack. The steps are listed in Figure 8.2.

FIGURE 8.2 The stages of a web application attack



Web Application Threats and Countermeasures

Many web application threats exist on a web server. The following are the most common threats and their countermeasures:

Cross-Site Scripting A parameter entered into a web form is processed by the web application. The correct combination of variables can result in arbitrary command execution. Countermeasure: Validate cookies, query strings, form fields, and hidden fields.

NOTE A countermeasure to cross-site scripting is to replace left and right angle bracket characters (< and >) with `&lt;` and `&gt;` using server scripts. A countermeasure to SSL attacks is to install a proxy server and terminate SSL at the proxy or install a hardware SSL accelerator and terminate SSL at this layer.

SQL Injection Inserting SQL commands into the URL gets the database server to dump, alter, delete, or create information in the database. SQL injection is covered in detail in Chapter 9, "Attacking Applications: SQL Injection and Buffer Overflows." Countermeasure: Validate user variables.

Command Injection The hacker inserts programming commands into a web form. Countermeasure: Use language-specific libraries for the programming language.

Cookie Poisoning and Snooping The hacker corrupts or steals cookies. Countermeasures: Don't store passwords in a cookie; implement cookie timeouts; and authenticate cookies.

Buffer Overflow Huge amounts of data are sent to a web application through a web form to execute commands. Buffer overflows is covered in detail in Chapter 9. Countermeasures: Validate user input length; perform bounds checking.

Authentication Hijacking The hacker steals a session once a user has authenticated. Countermeasure: Use SSL to encrypt traffic.

Directory Traversal/Unicode The hacker browses through the folders on a system via a web browser or Windows Explorer. Countermeasures: Define access rights to private folders on the web server; apply patches and hotfixes.

Hacking Tools

Instant Source allows a hacker to see and edit HTML source code. It can be used directly from within the web browser.

Wget is a command-line tool that a hacker can use to download an entire website, complete with all the files. The hacker can view the source code offline and test certain attacks prior to launching them against the real web server.

WebSleuth uses spidering technology to index an entire website. For example, WebSleuth can pull all the email addresses from different pages of a website.

BlackWidow can scan and map all the pages of a website to create a profile of the site.

SiteScope maps out the connections within a web application and aids in the deconstruction of the program.

WSDigger is a web services testing tool that contains sample attack plug-ins for SQL injection, cross-site scripting, and other web attacks.

Burp is a Windows-based automated attack tool for web applications. It can also be used to guess passwords on web applications and perform man-in-the-middle attacks.

Google Hacking

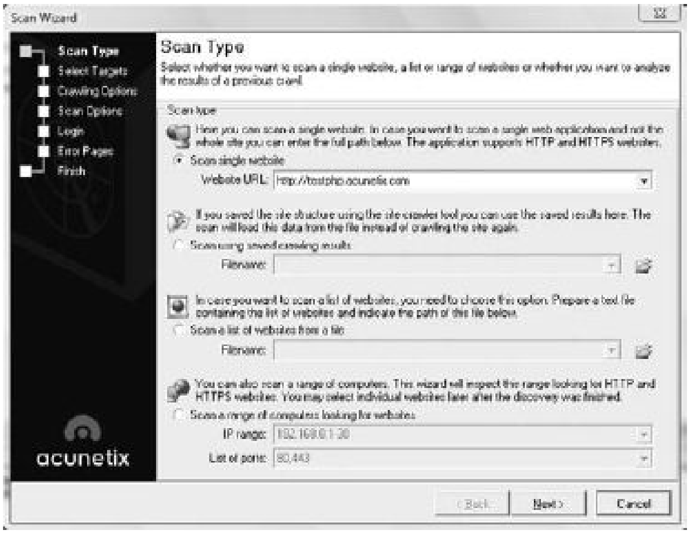
Google hacking refers to using Google's powerful search engine to locate high-value targets or to search for valuable information such as passwords.

Many tools, such as `http://johnny.ihackstuff.com` and Acunetix Web Vulnerability Scanner, contain a list of Google hacking terms organized in a database, to make searching easier (see Exercise 8.5). For example, you can enter the term *password* or *medical records* in the Google search engine and see what information is available. Many times, Google can pull information directly out of private databases or documents.

EXERCISE 8.5

Using Acunetix Web Vulnerability Scanner

1. Download and install Acunetix Web Vulnerability Scanner from `www.acunetix.com`.
2. Open the web scanner and select File ➢ New Scan to open the Scan Wizard:



Scan Type

Select whether you want to scan a single website, a list or range of websites or whether you want to analyze the results of a previous crawl.

Scan type

Here you can scan a single website. In case you want to scan a single web application and not the whole site you can enter the full path below. The application supports HTTP and HTTPS websites.

● Scan single website

Website URL: http://testphp.acunetix.com

If you saved the site structure using the site crawler tool you can use the saved results here. The scan will load this data from the file instead of crawling the site again.

○ Scan using saved crawling results

Filename:

In case you want to scan a list of websites, you need to choose this option. Prepare a text file containing the list of websites and indicate the path of this file below.

○ Scan a list of websites from a file

Filename:

You can also scan a range of computers. This wizard will inspect this range looking for HTTP and HTTPS websites. You may select individual websites later after the discovery was finished.

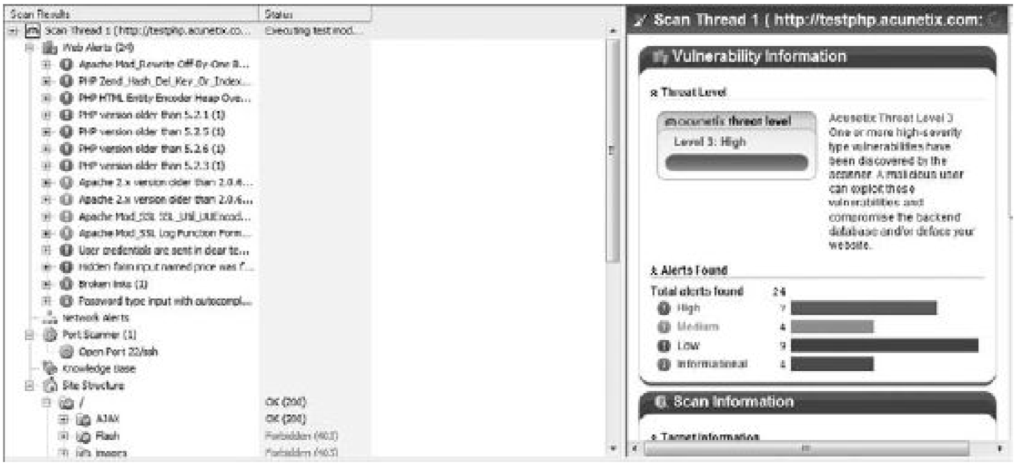
○ Scan a range of computers looking for websites

IP range: 192.168.0.1-30

List of ports: 80,443

EXERCISE 8.5 *(continued)*

3. Follow the wizard prompts; accept the default values for the initial scan.
4. View the scan report once the scan is complete. Notice the web server and application vulnerabilities in the scan report.



Scan Results	Status
Scan Thread 1 (http://testphp.acunetix.co...	Executing test mod...
Web Alerts (24)	
Apache Mod_Rewrite Off-By-One B...	
PHP Zend_Hash_Del_Key_Or_Index...	
PHP HTML Entity Encoder Heap Ove...	
PHP version older than 5.2.1 (1)	
PHP version older than 5.2.5 (1)	
PHP version older than 5.2.6 (1)	
PHP version older than 5.2.3 (1)	
Apache 2.x version older than 2.0.6...	
Apache 2.x version older than 2.0.6...	
Apache Mod_SSL SSL_Util_UUEncod...	
Apache Mod_SSL Log Function Form...	
User credentials are sent in clear te...	
Hidden form input named price was f...	
Broken links (1)	
Password type input with autocompl...	
Network Alerts	
Port Scanner (1)	
Open Port 22/ssh	
Knowledge Base	
Site Structure	
/	OK (200)
AJAX	OK (200)
Flash	Forbidden (403)
images	Forbidden (403)

Scan Thread 1 (http://testphp.acunetix.com:

Vulnerability Information

Threat Level

acunetix threat level

Level 3: High

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts Found

Total alerts found	24
High	7
Medium	4
Low	9
Informational	4

Scan Information

Target information

5. Create another scan using the wizard and target your lab web server or web server VM. View and analyze the scan report for your lab web server.

Web-Based Password-Cracking Techniques

As a CEH, you need to be familiar with the techniques hackers use to crack web-based passwords. This includes being able to list the various authentication types, knowing what a password cracker is, identifying the classifications of password-cracking techniques, and knowing the available countermeasures. We'll look at each in the following sections.

Authentication Types

Web servers and web applications support multiple authentication types. The most common is HTTP authentication. There are two types of HTTP authentication: basic and digest. Basic

HTTP authentication sends the username and password in cleartext, whereas digest authentication hashes the credentials and uses a challenge-response model for authentication.

In addition, web servers and web applications support the following types of authentication:

NTLM Authentication This type uses Internet Explorer and IIS web servers, making NTLM more suitable for internal authentication on an intranet that uses Microsoft operating systems. Windows 2000 and 2003 servers utilize Kerberos authentication for a more secure option.

Certificate-Based Authentication This type uses an x.509 certificate for public/private key technology.

Token-Based Authentication A token, such as SecurID, is a hardware device that displays an authentication code for 60 seconds; a user uses this code to log into a network.

Biometric Authentication This type uses a physical characteristic such as fingerprint, eye iris, or handprint to authenticate the user.

Password Attacks and Password Cracking

The three types of password attacks are as follows:

Dictionary Uses passwords that can be found in a dictionary

Brute-Force Guesses complex passwords that use letters, numbers, and special characters

Hybrid Uses dictionary words with a number or special character as a substitute for a letter

A *password cracker* is a program designed to decrypt passwords or disable password protection. Password crackers rely on dictionary searches (attacks) or brute-force methods to crack passwords.

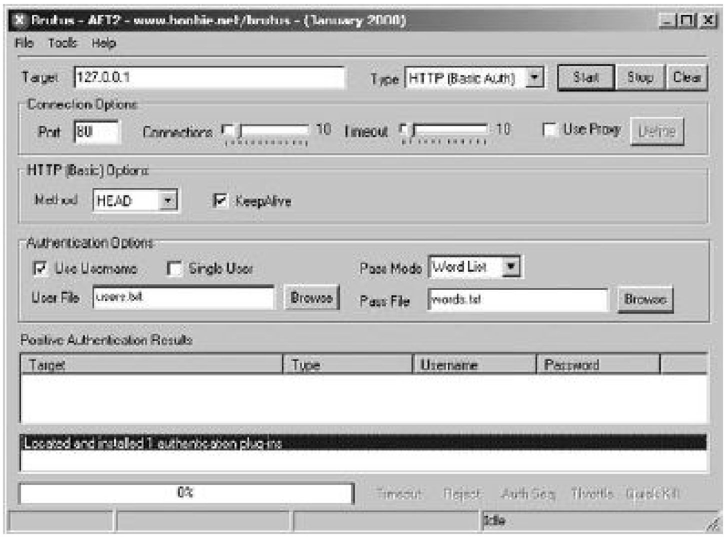
The first step in a dictionary attack is to generate a list of potential passwords that can be found in a dictionary. The hacker usually creates this list with a dictionary generator program or dictionaries that can be downloaded from the Internet. Next, the list of dictionary words is hashed or encrypted. This hash list is compared against the hashed password the hacker is trying to crack. The hacker can get the hashed password by sniffing it from a wired or wireless network or directly from the Security Accounts Manager (SAM) or shadow password files on the hard drive of a system. Finally, the program displays the unencrypted version of the password. Dictionary password crackers can only discover passwords that are dictionary words.

If the user has implemented a strong password, then brute-force password cracking can be implemented. Brute-force password crackers try every possible combination of letters, numbers, and special characters, which takes much longer than a dictionary attack because of the number of permutations. Exercise 8.6 walks you through using a password cracker called Brutus.

EXERCISE 8.6

Using a Password Cracker

1. Download and install Brutus from `www.hoobie.net`.
2. Open Brutus and type the web server address in the target field.



Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

Target: 127.0.0.1

Type: HTTP (Basic Auth)

Connection Options: Port 80; Connections 10; Timeout 10; □ Use Proxy

HTTP (Basic) Options: Method HEAD; ☑ KeepAlive

Authentication Options: ☑ Use Username; □ Single User; Pass Mode Word List; User File users.txt; Pass File words.txt

Positive Authentication Results

Target	Type	Username	Password

Located and installed 1 authentication plug-ins

0%

Idle

3. Click the Start button and view passwords in the positive authentication results field at the bottom of the screen.

Hacking Tool

Webcracker is a tool that uses a word list to attempt to log on to a web server. It looks for the "HTTP 302 object moved" response to make guesses on the password. From this response, the tool can determine the authentication type in use and attempt to log on to the system.

The best password-cracking countermeasure is to implement strong passwords that are at least eight characters long (the old standard was six) and that include alphanumeric characters. Usernames and passwords should be different, because many usernames are transmitted in cleartext. Complex passwords that require uppercase, lowercase, and numbers or special characters are harder to crack. You should also implement a strong authentication mechanism such as Kerberos or tokens to protect passwords in transit.

Summary

Web servers and web application attacks are always of highest concern with the increasing use of the Internet. Web servers and the Internet are used by customers to research companies, make online purchases, access databases at banks and investment firms, and perform numerous other database searches. As this use rises, the potential target information becomes increasingly valuable. Credit card numbers, personal information, and Social Security numbers are the golden target for hackers, and all this information is stored in web application databases.

Web server and web application hacking are the methods hackers use to attempt to breach web server security and deliver exploits that will yield valuable information. A CEH needs to be well versed in identifying potential vulnerabilities and countermeasures to prevent web server attacks.

Exam Essentials

Know the types of web server vulnerabilities. Misconfiguration, operating system or application bugs and flaws, default installation of operating system and web server software, lack of patch management, and lack of proper security policies and procedures are all web server vulnerabilities.

Know common web application threats. Cross-site scripting, SQL and command injection, cookie poisoning and snooping, buffer overflow, authentication hijacking, and directory traversal are all common web application threats.

Understand Google hacking. Google hacking involves using the Google search engine to locate passwords, credit card numbers, medical records, or other confidential information.

Understand patch-management techniques. Patch management is important for ensuring a system is up-to-date on the latest security fixes. A process for testing, applying, and logging patches to a system should be defined and followed.

Know the various authentication mechanisms for web servers. HTTP basic and digest authentication, NTLM, tokens, biometrics, and certificates are all methods of authenticating to a web server.

Understand how password crackers work. Password crackers use a hashed dictionary file to crack a password.

Know the types of password attacks. Dictionary, hybrid, and brute force are the three types of password attacks.

Review Questions

1. Which of the following are types of HTTP web authentication? (Choose all that apply.)
   - **A.** Digest
   - **B.** Basic
   - **C.** Windows
   - **D.** Kerberos

2. Which of the following is a countermeasure for a buffer overflow attack?
   - **A.** Input field length validation
   - **B.** Encryption
   - **C.** Firewall
   - **D.** Use of web forms

3. A hardware device that displays a login that changes every 60 seconds is known as a/an ______________.
   - **A.** Login finder
   - **B.** Authentication server
   - **C.** Biometric authentication
   - **D.** Token

4. Which is a common web server vulnerability?
   - **A.** Limited user accounts
   - **B.** Default installation
   - **C.** Open shares
   - **D.** No directory access

5. A password of *P@SSWORD* can be cracked using which type of attack?
   - **A.** Brute force
   - **B.** Hybrid
   - **C.** Dictionary
   - **D.** Zero day exploit

6. Which of the following is a countermeasure for authentication hijacking?
   - **A.** Authentication logging
   - **B.** Kerberos
   - **C.** SSL
   - **D.** Active Directory

7. Why is a web server more commonly attacked than other systems?
   - A. A web server is always accessible.
   - B. Attacking a web server does not require much hacking ability.
   - C. Web servers are usually placed in a secure DMZ.
   - D. Web servers are simple to exploit.

8. A client/server program that resides on a web server is called a/an ______________.
   - A. Internet program
   - B. Web application
   - C. Patch
   - D. Configuration file

9. Which is a countermeasure to a directory-traversal attack?
   - A. Enforce permissions to folders.
   - B. Allow everyone access to the default page only.
   - C. Allow only registered users to access the home page of a website.
   - D. Make all users log in to access folders.

10. What is it called when a hacker inserts programming commands into a web form?
    - A. Form tampering
    - B. Command injection
    - C. Buffer overflow
    - D. Web form attack

11. Which of the following commands would start to execute a banner grab against a web server?
    - A. `telnet www.yahoo.com 80`
    - B. `telnet HTTP www.yahoo.com`
    - C. `http://www.yahoo.com:80`
    - D. `HEAD www.yahoo.com`

12. Which of the following exploits can be used against Microsoft Internet Information (IIS) Server? (Choose all that apply.)
    - A. IPP printer overflow attack
    - B. ISAPI DLL buffer overflow attack
    - C. Long URL attack
    - D. Proxy buffer overflow attack

13. Where does the most valuable target information reside on a web server?
    - A. Web server home directory
    - B. Web application system files
    - C. Web application database
    - D. NTHOME directory

14. Which of the following hacking tools performs directory-traversal attacks on IIS?

A. RPC DCOM

B. `IIScrack.dll`

C. WebInspect

15. Which program can be used to download entire websites?

A. WebSleuth

B. WSDigger

C. Wget

D. BlackWidow

16. Web servers support which of the following authentication credentials? (Choose all that apply.)

A. Certificates

B. Tokens

C. Biometrics

D. Kerberos

17. Which tool can be used to pull all email addresses from a website?

A. WebSleuth

B. WSDigger

C. Wget

D. BlackWidow

18. What does SiteScope do?

A. Maps out connections in web applications

B. Views the HTML source for all web pages in a site

C. Gathers email address from websites

D. Tests exploits against web applications

19. What are the three primary types of attacks against IIS servers?

A. Directory traversal

B. Buffer overflows

C. Authentication attacks

D. Source disclosure attacks

20. Which of the following is a common website attack that allows a hacker to deface a website? (Choose all that apply)

A. Using a DNS attack to redirect users to a different web server

B. Revealing an administrator password through a brute-force attack

C. Using a directory-traversal attack

D. Using a buffer overflow attack via a web form

Answers to Review Questions

1. A, B. Digest and basic are the types of HTTP web authentication.

2. A. Validating the field length and performing bounds checking are countermeasures for a buffer overflow attack.

3. D. A token is a hardware device containing a screen that displays a discrete set of numbers used for login and authentication.

4. B. Default installation is a common web server vulnerability.

5. B. A hybrid attack substitutes numbers and special characters for letters.

6. C. SSL is a countermeasure for authentication hijacking.

7. A. A web server is always accessible, so a hacker can hack it more easily than less-available systems.

8. B. Web applications are client/server programs that reside on a web server.

9. A. A countermeasure to a directory-traversal attack is to enforce permissions to folders.

10. B. Command injection involves a hacker entering programming commands into a web form in order to get the web server to execute the commands.

11. A. To make an initial connection to the web server, use telnet to port 80.

12. A, B. IPP printer overflow and ISAPI DLL buffer overflow attacks are types of buffer overflow attacks that can be used to exploit IIS Server.

13. C. The most valuable target data, such as passwords, credit card numbers, and personal information, reside in the database of a web application.

14. D. `IISExploit.exe` is a tool used to perform automated directory-traversal attacks on IIS.

15. C. Wget is a command-line tool that can be used to download an entire website with all the source files.

16. A, B, C. Certificates, tokens. and biometrics are all credentials that can authenticate users to web servers and web applications. Kerberos is a type of security system used to protect user authentication credentials.

17. A. WebSleuth can be used to index a website and specifically pull email addresses from all the pages of a website.

18. A. SiteScope maps out the connections within a web application and aids in the deconstruction of the program.

19. A, B, D. The three most common attacks against IIS are directory traversal, buffer overflows, and source disclosure.

20. A, B. Using a DNS attack to redirect users to a different web server and revealing an administrator password through a brute-force attack are two methods of defacing a website.