

Hacking Webservers

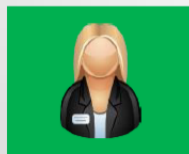
Module 12



Hacking Webservers

Module 12

Engineered by **Hackers**. Presented by Professionals.



Ethical Hacking and Countermeasures v8

Module 12: Hacking Webservers

Exam 312-50

The screenshot shows a web page with a dark header. On the left is a navigation menu with buttons for Home, Products, Gallery, Services, and Contact. The main content area has a red background. The article title is 'GoDaddy Outage Takes Down Millions of Sites, Anonymous Member Claims Responsibility'. The date is 'Monday, September 10th, 2012'. The article text includes a final update stating GoDaddy is up and claims the outage was due to internal errors, not a DDoS attack. It also mentions that GoDaddy's DNS service is down and that a member of Anonymous is claiming responsibility. The article concludes with a tipster's report on the technical cause of the failure and a bio of the Anonymous member.

Security News

GoDaddy Outage Takes Down Millions of Sites, Anonymous Member Claims Responsibility

Monday, September 10th, 2012

Final update: GoDaddy is up, and claims that the outage was due to internal errors and not a DDoS attack.

According to many customers, sites hosted by major web host and domain registrar GoDaddy are down. According to the official GoDaddy Twitter account the company is aware of the issue and is working to resolve it.

Update: customers are complaining that GoDaddy hosted e-mail accounts are down as well, along with GoDaddy phone service and all sites using GoDaddy's DNS service.

Update 2: A member of Anonymous known as AnonymousOwn3r is claiming responsibility, and makes it clear this is not an Anonymous collective action.

A tipster tells us that the technical reason for the failure is being caused by the inaccessibility of GoDaddy's DNS servers — specifically CNS1.SECURESERVER.NET, CNS2.SECURESERVER.NET, and CNS3.SECURESERVER.NET are failing to resolve.

AnonymousOwn3r's bio reads "Security leader of #Anonymous (~Official member~)." The individual claims to be from Brazil, and hasn't issued a statement as to why GoDaddy was targeted.

<http://techcrunch.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Security News

GoDaddy Outage Takes Down Millions of Sites, Anonymous Member Claims Responsibility

Source: <http://techcrunch.com>

Final update: GoDaddy is up, and claims that the outage was due to internal errors and not a DDoS attack.

According to many customers, sites hosted by major web host and domain registrar GoDaddy are down. According to the **official GoDaddy Twitter account, the company is aware of the issue and is working to resolve it.**

Update: Customers are complaining that GoDaddy hosted e-mail accounts are down as well, along with GoDaddy phone service and all sites using GoDaddy's DNS service.

Update 2: A member of Anonymous known as AnonymousOwn3r is claiming responsibility, and makes it clear this is not an Anonymous collective action.

A tipster tells us that the technical reason for the failure is being caused by the inaccessibility of GoDaddy's DNS servers — specifically CNS1.SECURESERVER.NET, CNS2.SECURESERVER.NET, and CNS3.SECURESERVER.NET are failing to resolve.

AnonymousOwn3r's bio reads "**Security leader of #Anonymous (~Official member~).**" The individual claims to be from Brazil, and hasn't issued a statement as to why GoDaddy was targeted.

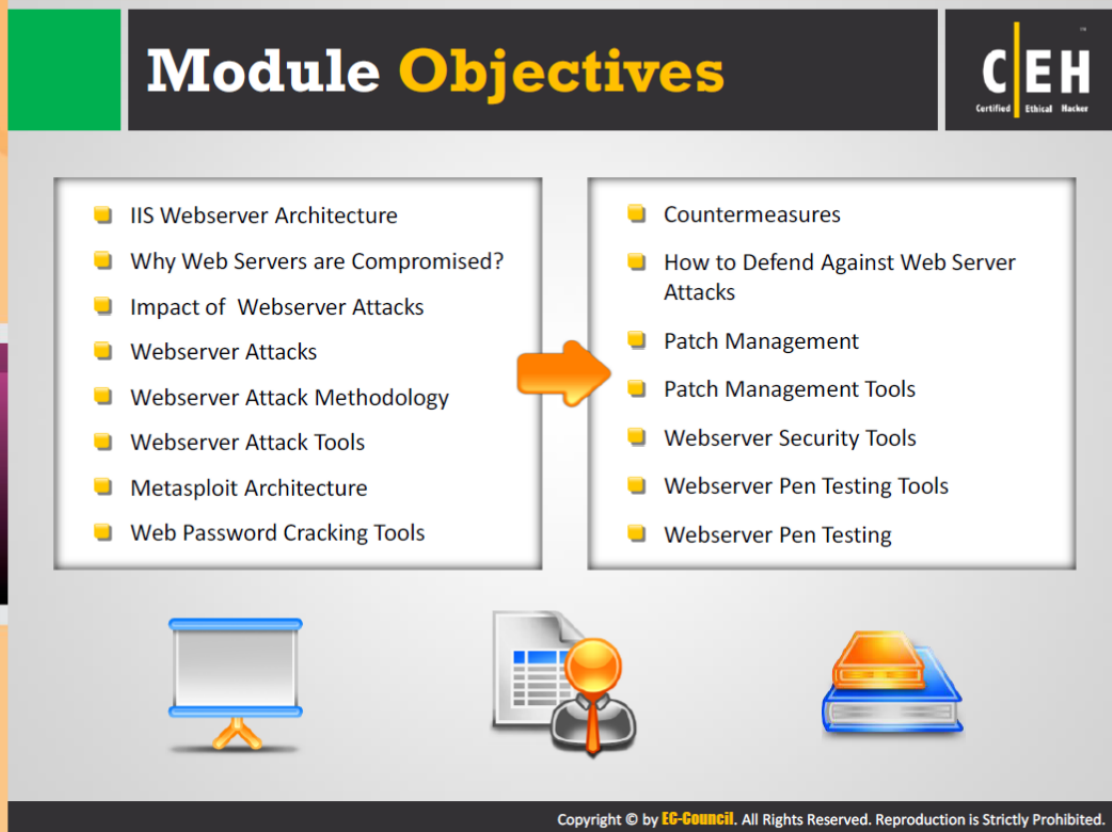
Last year GoDaddy was pressured into opposing SOPA as customers transferred domains off the service, and the company has been the center of a few other controversies. However, AnonymousOwn3r has tweeted "I'm not anti go daddy, you guys will understand because i did this attack."



Copyright © 2012 AOL Inc.

By Klint Finley

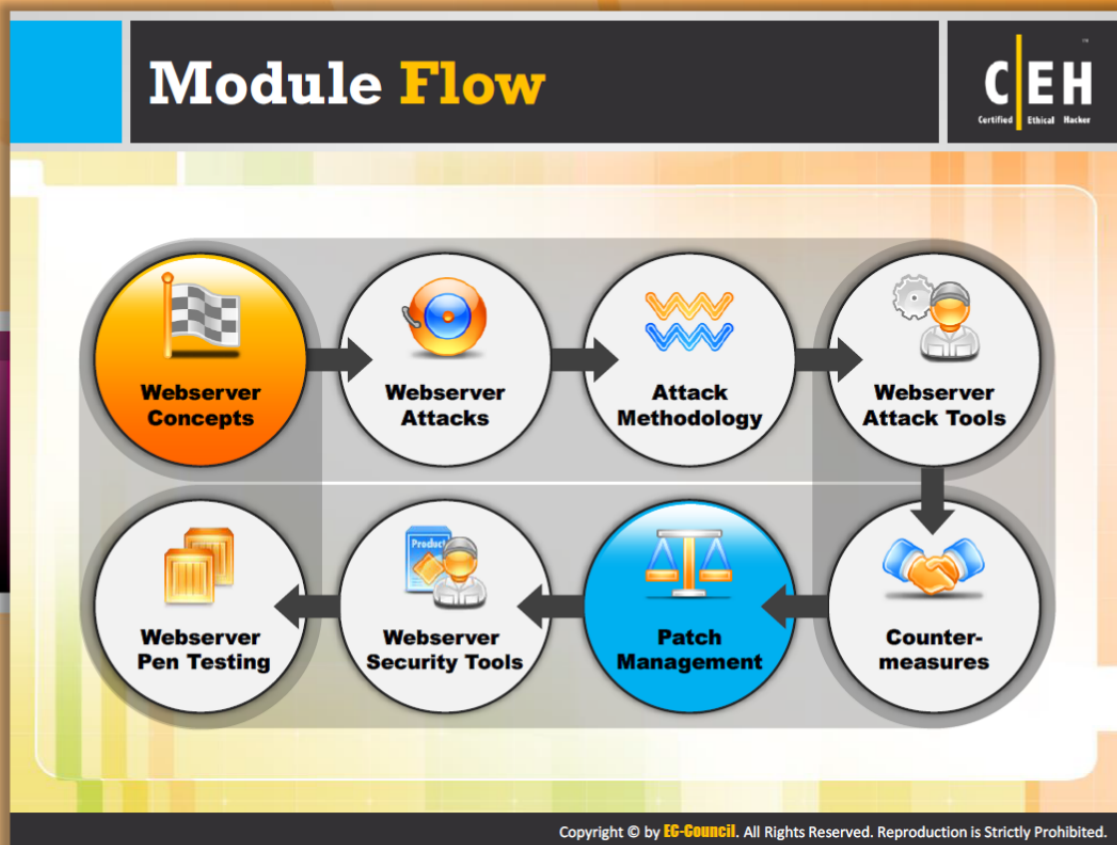
<http://techcrunch.com/2012/09/10/godaddy-outage-takes-down-millions-of-sites/>



Module Objectives

Often, a breach in security causes more damage in terms of goodwill than in actual quantifiable loss. This makes web server security critical to the normal functioning of an organization. **Most organizations consider their web presence to be an extension of themselves.** This module attempts to highlight the various security concerns in the context of webservers. After finishing this module, you will be able to understand a web server and its architecture, how the attacker hacks it, what the different types of attacks that an attacker can carry out on the web servers are, tools used in web server hacking, etc. Exploring web server security is a vast domain and to delve into the finer details of the discussion is beyond the scope of this module. This module makes you familiarize with:

- IIS Web Server Architecture
- Why Web Servers Are Compromised?
- Impact of Webserver Attacks
- Webserver Attacks
- Webserver Attack Methodology
- Webserver Attack Tools
- Metasploit Architecture
- Web Password Cracking Tools
- Countermeasures
- How to Defend Against Web Server Attacks
- Patch Management
- Patch Management Tools
- Webserver Security Tools
- Webserver Pen Testing Tools
- Webserver Pen Testing

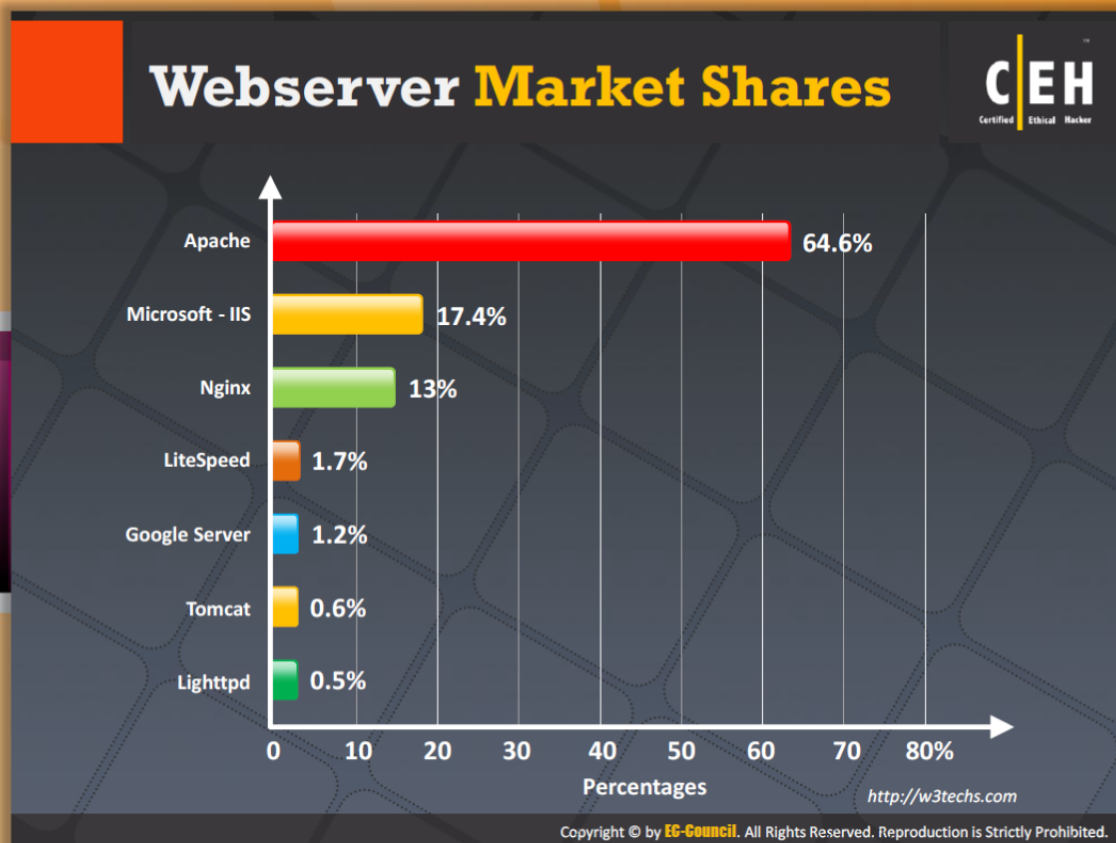


Module Flow

To understand hacking web servers, first you should know what a web server is, how it functions, and what are the other elements associated with it. All these are simply termed web server concepts. So first we will discuss about web server concepts.

 Webserver Concepts	 Webserver Attacks
 Attack Methodology	 Webserver Attack Tools
 Webserver Pen Testing	 Webserver Security Tools
 Patch Management	 Counter-measures

This section gives you brief overview of the web server and its architecture. It will also explain common reasons or mistakes made that encourage attackers to hack a web server and become successful in that. This section also describes the impact of attacks on the web server.



Web Server Market Shares

Source: <http://w3techs.com>

The following statistics shows the percentages of websites using various web servers. From the statistics, it is clear that **Apache is the most commonly used web server**, i.e., 64.6%. Below that **Microsoft - IIS server is used by 17.4 % of users**.

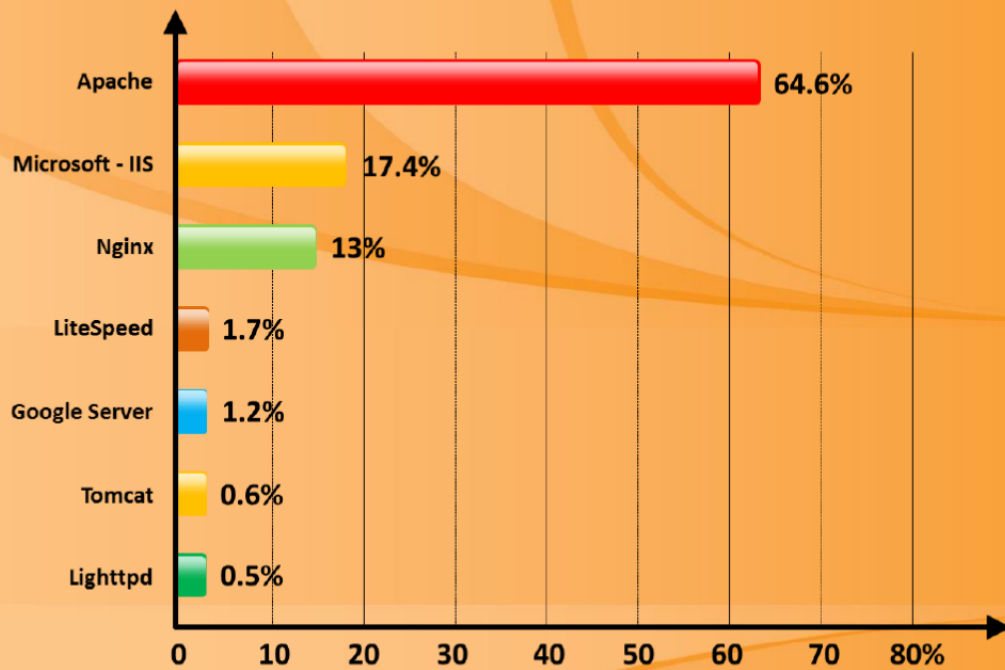
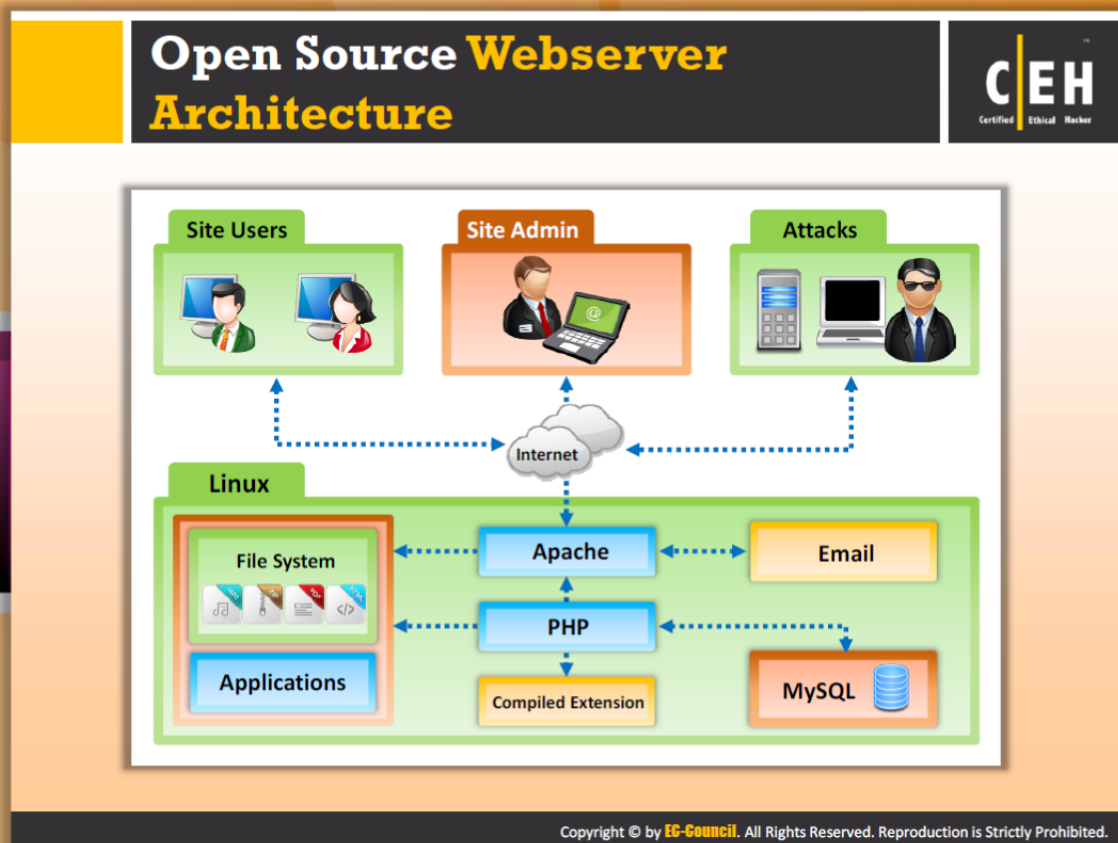


FIGURE 12.1: Web Server Market Shares



Open Source Web Server Architecture

The diagram bellow illustrates the basic components of open source web server architecture.

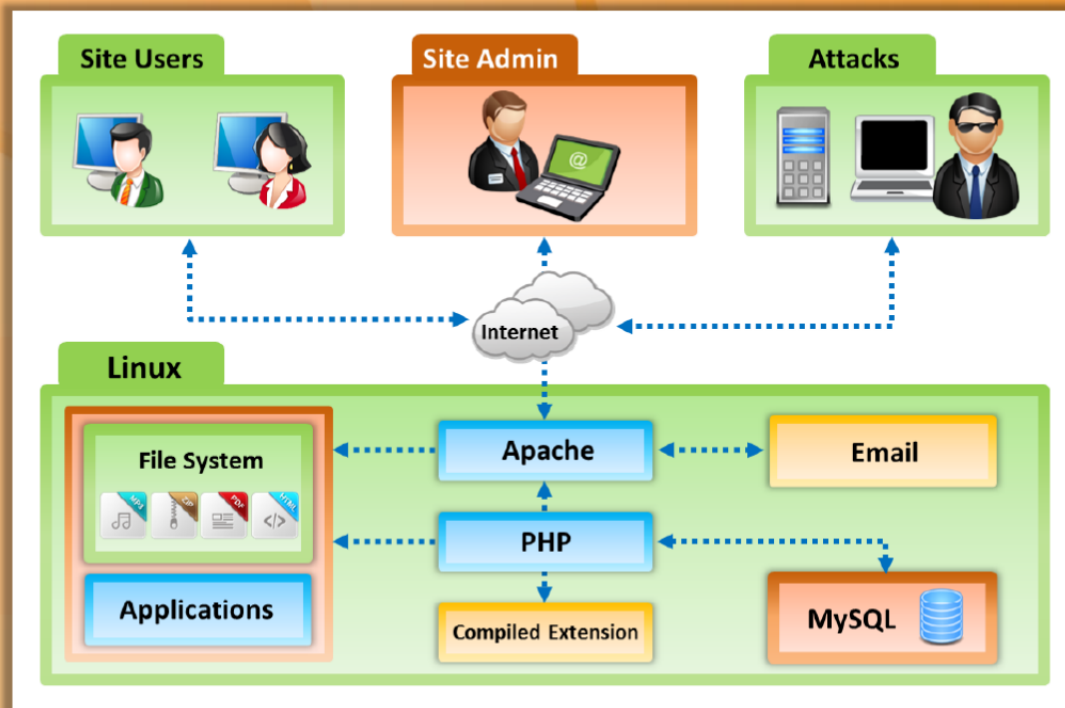
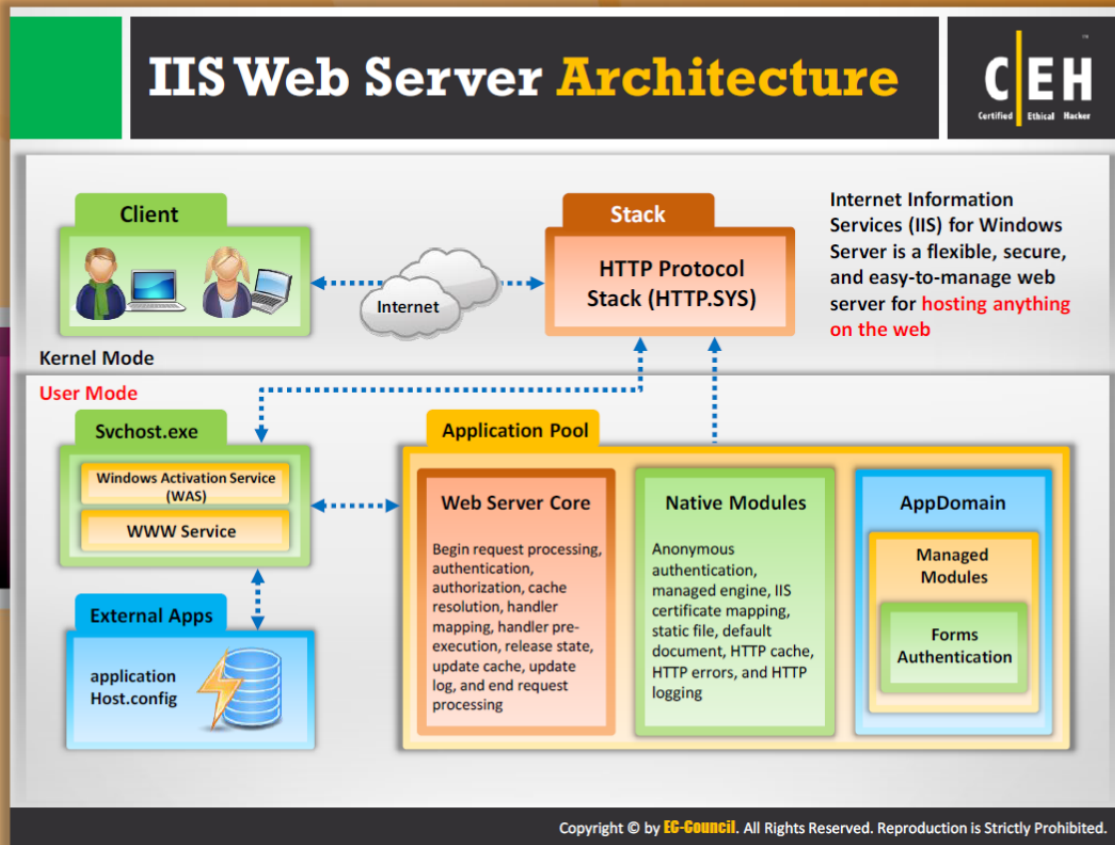


FIGURE 12.2: Open Source Web Server Architecture

Where,

- **Linux** – the server's operating system
- **Apache** – the web server component
- **MySQL** – a relational database
- **PHP** – the application layer



IIS Web Server Architecture

IIS, also known as Internet Information Service, is a web server application developed by Microsoft that can be used with Microsoft Windows. This is the second largest web after Apache HTTP server. It occupies around **17.4% of the total market share**. It supports HTTP, HTTPS, FTP, FTPS, SMTP, and NNTP.

The diagram that follows illustrates the basic components of IIS web server architecture:

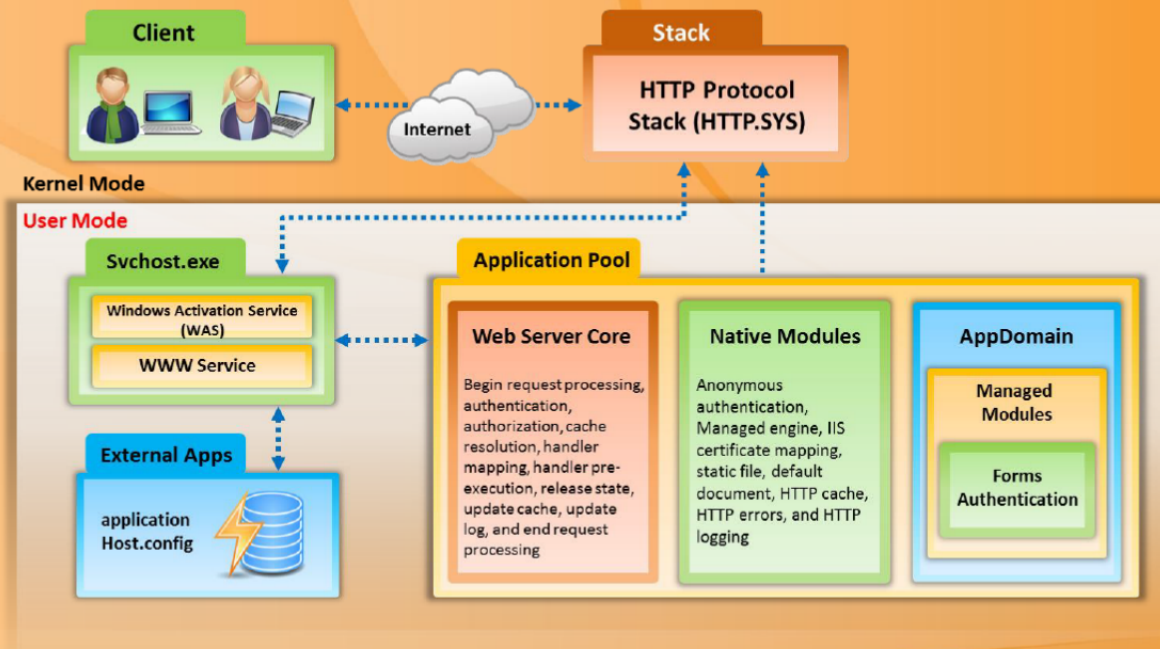


FIGURE 12.3: IIS Web Server Architecture

Website Defacement



- Web defacement occurs when an intruder **maliciously alters visual appearance of a web page** by inserting or substituting provocative and frequently offending data
- Defaced pages exposes visitors to some **propaganda** or misleading information until the unauthorized change is discovered and corrected





Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



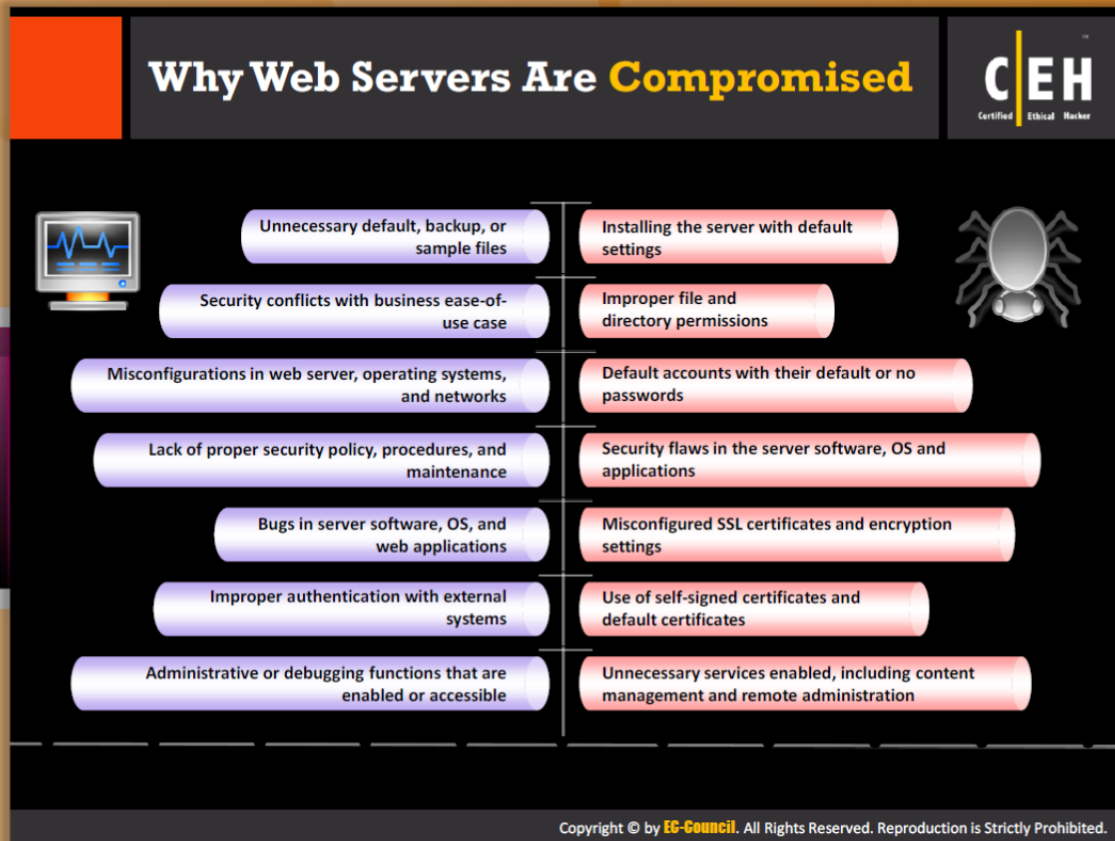
Website Defacement

Website defacement is a process of changing the **content of a website** or web page by **hackers**. Hackers break into the web servers and will alter the hosted website by creating something new.

Web defacement occurs when an intruder maliciously alters the visual appearance of a web page by inserting or substituting provocative and frequently offensive data. Defaced pages expose visitors to propaganda or misleading information until the unauthorized change is discovered and corrected.



FIGURE 12.4: Website Defacement



Why Web Servers Are Compromised

There are inherent security risks associated with web servers, the local area networks that host web sites and users who access these websites using browsers.

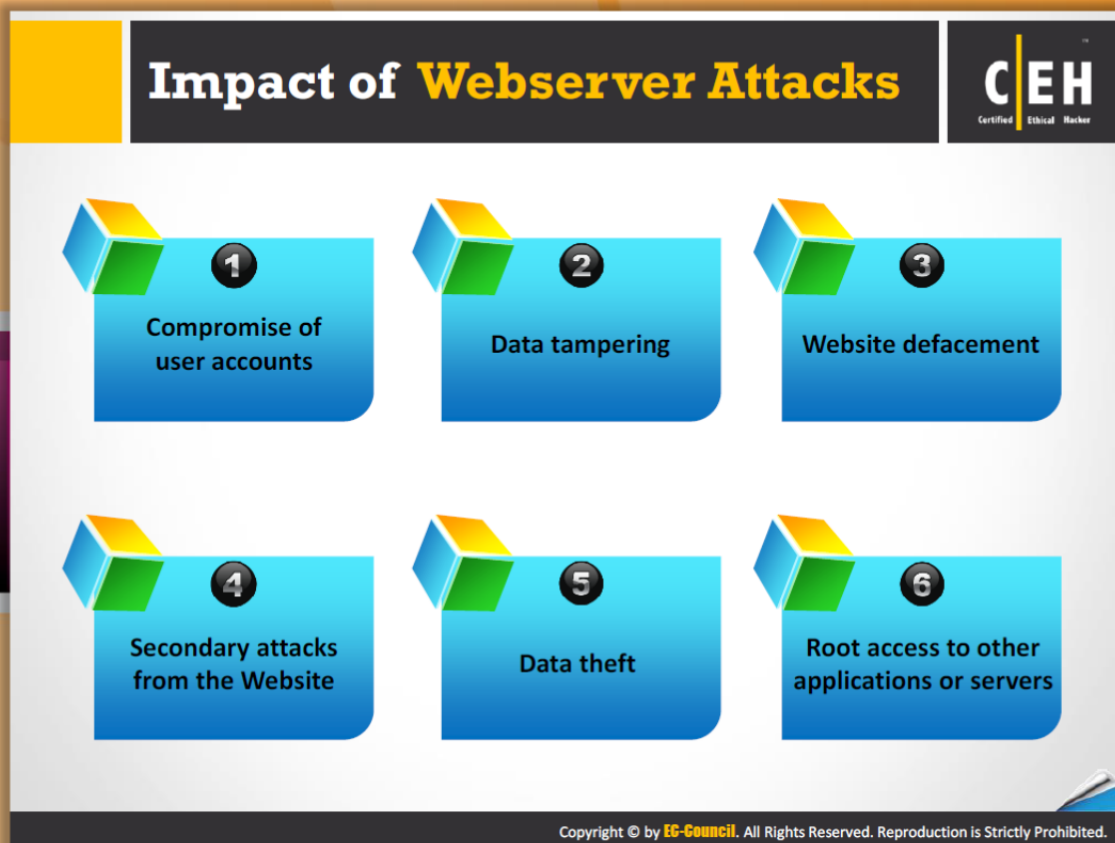
- **Webmaster's Concern:** From a webmaster's perspective, the biggest security concern is that the web server can expose the local area network (LAN) or the corporate intranet to the threats the Internet poses. This may be in the form of viruses, Trojans, attackers, or the compromise of information itself. Software bugs present in large complex programs are often considered the source of imminent security lapses. However, web servers that are large complex devices and also come with these inherent risks. In addition, the open architecture of the web servers allows arbitrary scripts to run on the server side while replying to the remote requests. Any CGI script installed at the site may contain bugs that are potential security holes.
- **Network Administrator's Concern:** From a network administrator's perspective, a poorly configured web server poses another potential hole in the local network's security. While the objective of a web is to provide controlled access to the network, too much of control can make a web almost impossible to use. In an intranet environment, the network administrator has to be careful about configuring the web server, so that the legitimate users are recognized and authenticated, and various groups of users assigned distinct access privileges.

- ⓘ **End User's Concern:** Usually, the end user does not perceive any immediate threat, as surfing the web appears both safe and anonymous. However, active content, such as ActiveX controls and Java applets, make it possible for harmful applications, such as viruses, to invade the user's system. Besides, active content from a website browser can be a conduit for malicious software to bypass the firewall system and permeate the local area network.

The table that follows shows the causes and consequences of web server compromises:

Cause	Consequence
Installing the server with default settings	Unnecessary default, backup, or sample files
Improper file and directory permissions	Security conflicts with business ease-of-use case
Default accounts with their default passwords	Misconfigurations in web server, operating systems and networks
Unpatched security flaws in the server software, OS, and applications	Lack of proper security policy, procedures, and maintenance
Misconfigured SSL certificates and encryption settings	Bugs in server software, OS, and web applications
Use of self-signed certificates and default certificates	Improper authentication with external systems
Unnecessary services enabled, including content management and remote administration	Administrative or debugging functions that are enabled or accessible

TABBLE 12.1: causes and consequences of web server compromises

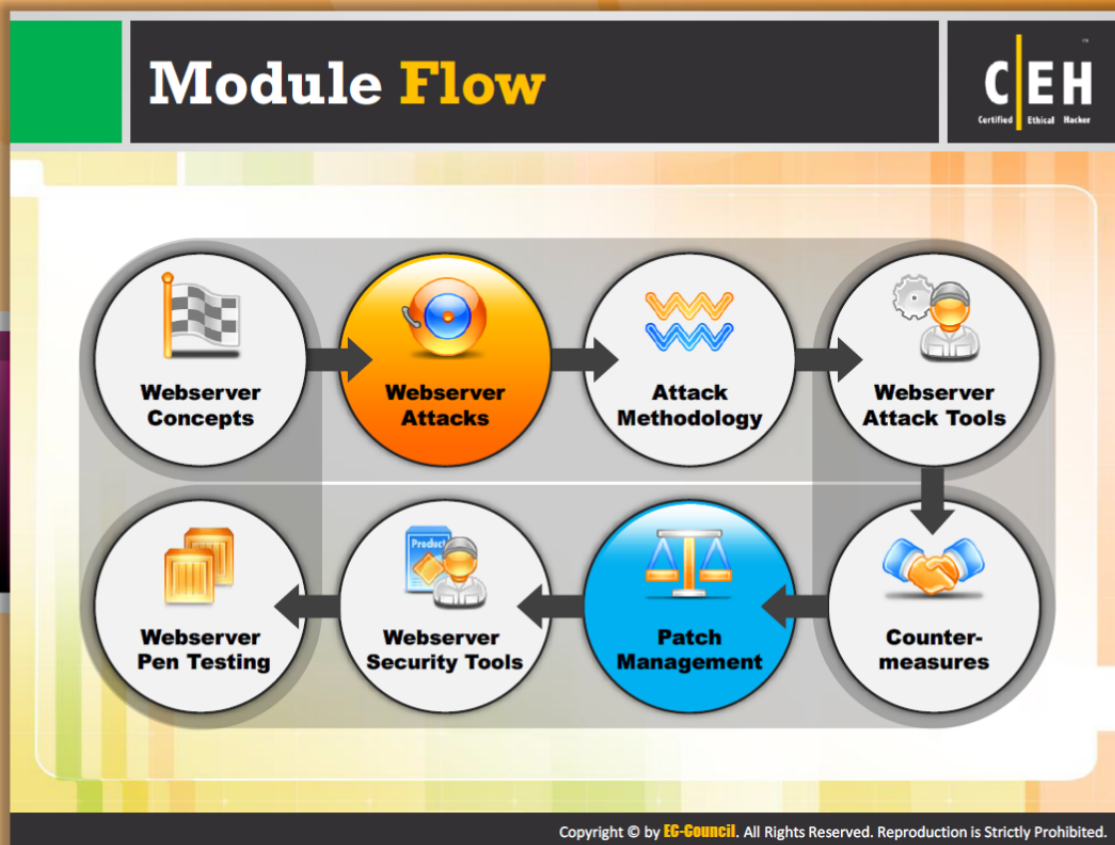


Impact of Web Server Attacks

Attackers can cause various kinds of damage to an organization by attacking a web server. The damage includes:

- **Compromise of user accounts:** Web server attacks are mostly concentrated on user account compromise. If the attacker is able to compromise a user account, then the attacker can gain a lot of useful information. Attacker can use the compromised user account to launch further attacks on the web server.
- **Data tampering:** Attacker can alter or delete the data. He or she can even replace the data with malware so that whoever connects to the web server also becomes compromised.
- **Website defacement:** Hackers completely change the outlook of the website by replacing the original data. They change the website look by changing the visuals and displaying different pages with the messages of their own.
- **Secondary attacks from the website:** Once the attacker compromises a web server, he or she can use the server to launch further attacks on various websites or client systems.
- **Data theft:** Data is one of the main assets of the company. Attackers can get access to sensitive data of the company like source code of a particular program.

- **Root access to other applications or server:** Root access is the highest privilege one gets to log in to a network, be it a dedicated server, semi-dedicated, or virtual private server. Attackers can perform any action once they get root access to the source.

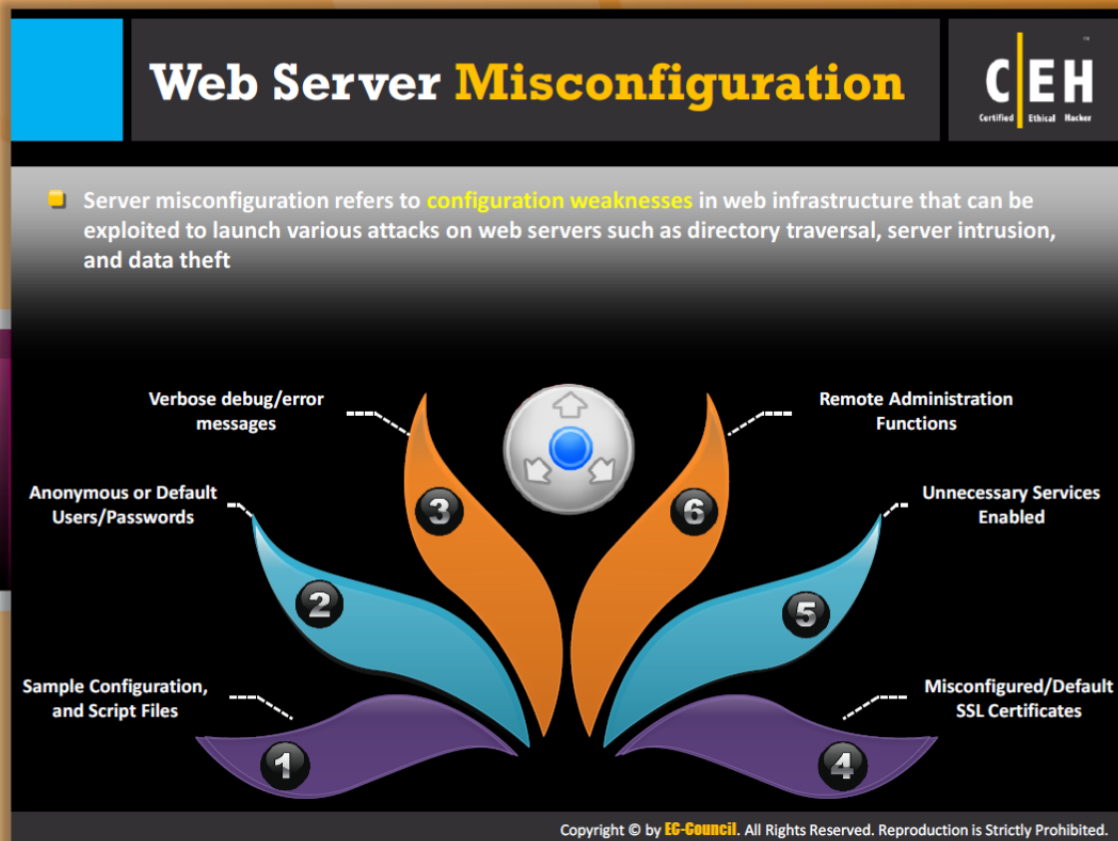


Module Flow

Considering that you became familiar with the web server concepts, we move forward to the possible attacks on web server. Each and every action on online is performed with the help of web server. Hence, it is considered as the critical source of an organization. This is the same reason for which attackers are targeting web server. There are many attack technique used by the attacker to compromise web server. Now we will discuss about those attack techniques.

attack, HTTP response splitting attack, web cache poisoning attack, http response hijacking, web application attacks, etc.

 Webserver Concepts	 Webserver Attacks
 Attack Methodology	 Webserver Attack Tools
 Webserver Pen Testing	 Webserver Security Tools
 Patch Management	 Counter-measures




Web Server Misconfiguration

Web servers have various vulnerabilities related to configuration, applications, files, scripts, or web pages. Once these vulnerabilities are found by the attacker, like remote accessing the application, then these become the doorways for the attacker to enter into the network of a company. These loopholes of the server can help attackers to bypass user authentication. **Server misconfiguration refers to configuration weaknesses in web infrastructure** that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft. Once detected, these problems can be easily exploited and result in the total compromise of a website.


- Remote administration functions can be a source for breaking down the server for the attacker.
- Some unnecessary services enabled are also vulnerable to hacking.
- Misconfigured/default SSL certificates.
- Verbose **debug/error messages**.
- Anonymous or default users/passwords.
- Sample configuration and script files.

Web Server Misconfiguration Example



httpd.conf file on an **Apache** server


```
<Location /server-status>
SetHandler server-status
</Location>
```



This configuration allows anyone to view the **server status** page, which contains detailed information about the current use of the web server, including information about the **current hosts** and requests being processed

php.ini file

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```



This configuration gives **verbose error messages**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Misconfiguration Example

Consider the httpd.conf file on an Apache server.

```
<Location /server-status>
SetHandler server-status
</Location>
```

FIGURE 12.5: httpd.conf file on an Apache server

This configuration allows anyone to view the server status page that contains detailed information about the current use of the web server, including **information about the current hosts** and requests being processed.


Consider another example, the php.ini file.

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```

FIGURE 12.6: php.inifile on an Apache server


This configuration gives verbose error messages.

Directory Traversal Attacks



In directory traversal attacks, attackers use `../` (dot-dot-slash) sequence to access restricted directories outside of the web server root directory

Attackers can use **trial and error method to navigate the outside of root directory and access sensitive information in the system**

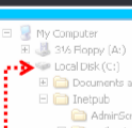


`http://server.com/scripts/../../../../Windows/System32/cmd.exe?/c+dir+c:\`

Volume in drive C has no label.
Volume Serial Number is D45E-9FEE

Directory of C:\

06/02/2010 11:31 AM	1,024 .rnd
09/28/2010 06:43 PM	0 123.text
05/21/2010 03:10 PM	0 AUTOEXEC.BAT
09/27/2010 08:54 PM	<DIR> CATALINA_HOME
05/21/2010 03:10 PM	0 CONFIG.SYS
08/11/2010 09:16 AM	<DIR> Documents and Settings
09/25/2010 05:25 PM	<DIR> Downloads
08/07/2010 03:38 PM	<DIR> Intel
09/27/2010 09:36 PM	<DIR> Program Files
05/26/2010 02:36 AM	<DIR> Snort
09/28/2010 09:50 AM	<DIR> WINDOWS
09/25/2010 02:03 PM	569,344 WinDump.exe
7 File(s) 570,368 bytes	
13 Dir(s) 13,432,115,200 bytes free	



My Computer

- 3 1/2 Floppy (A:)
- Local Disk (C:)
- Documents and Settings
- Inetpub
 - AdminScripts
 - mailroot
 - wwwroot
 - company
 - downloads
 - images
 - news
 - scripts
 - support
- mysql
- PHP
- Program Files
- WINDOWS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Directory Traversal Attacks

Web servers are designed in such a way that the public access is limited to some extent. **Directory traversal is exploitation of HTTP** through which attackers are able to access restricted directories and execute commands outside of the web server root directory by manipulating a URL. Attackers can use the trial-and-error method to navigate outside of the root directory and access sensitive information in the system.

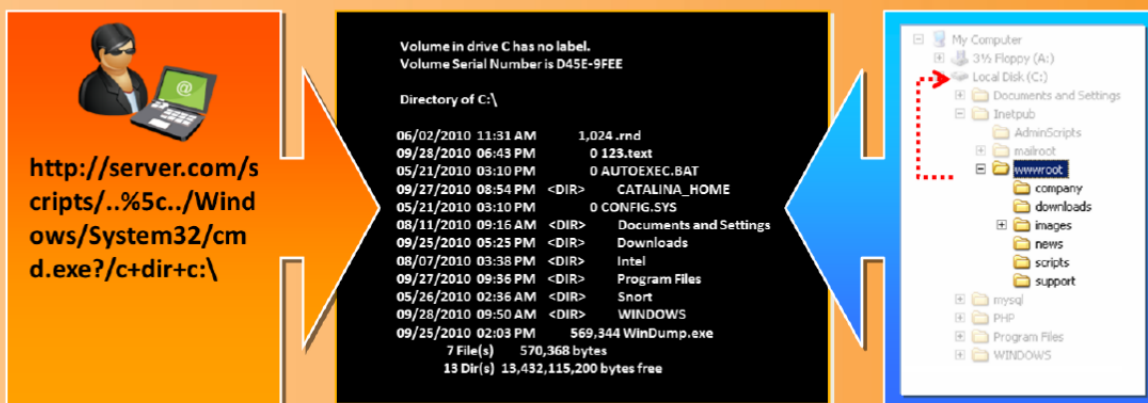
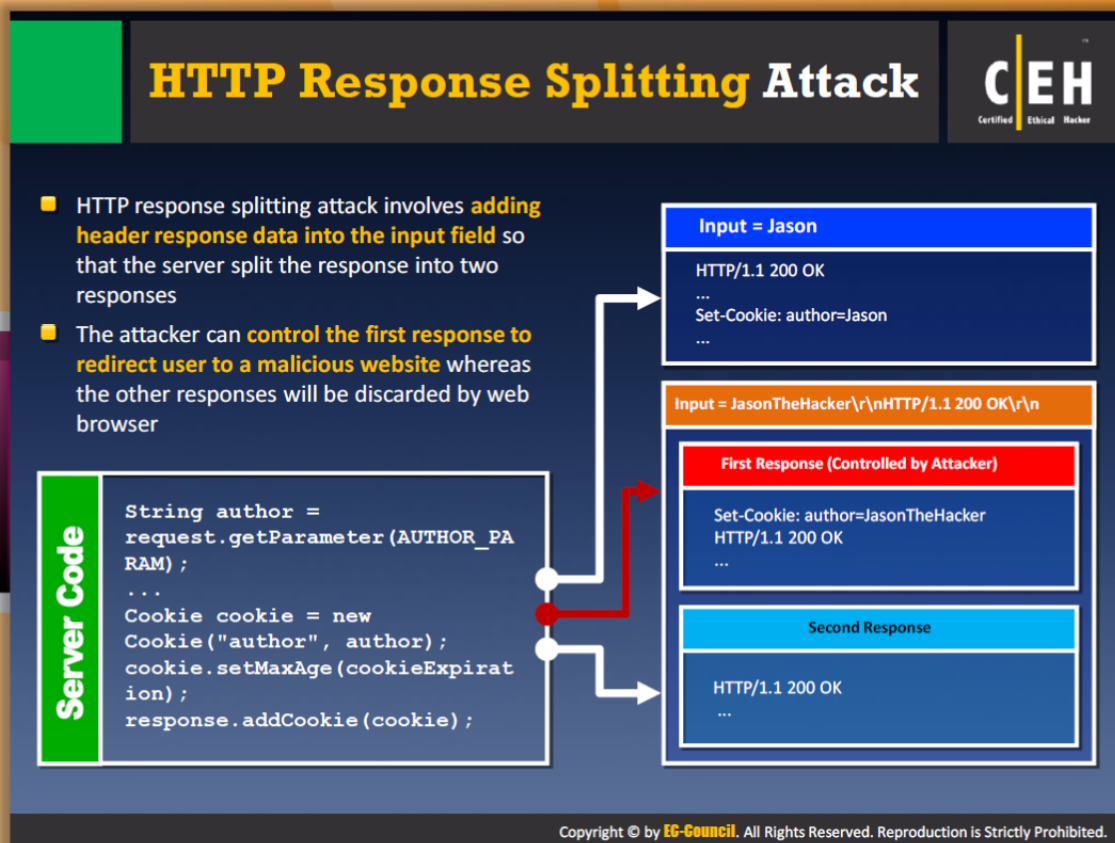


FIGURE 12.7: Directory Traversal Attacks



HTTP Response Splitting Attack

An HTTP response attack is a web-based attack where a server is tricked by injecting new lines into response headers along with arbitrary code. **Cross-Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection** are some of the examples for this type of attacks. The attacker alters a single request to appear and be processed by the web server as two requests. The web server in turn responds to each request. This is accomplished by adding header response data into the input field. An attacker passes malicious data to a vulnerable application, and the application includes the data in an HTTP response header. The attacker can control the first response to redirect the user to a malicious website, whereas the other responses will be **discarded by web browser**.

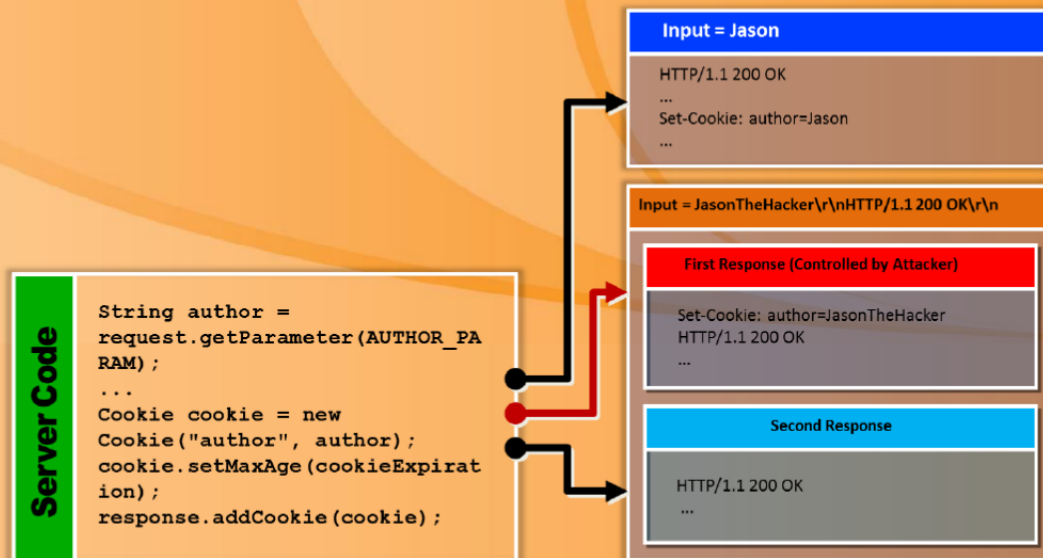
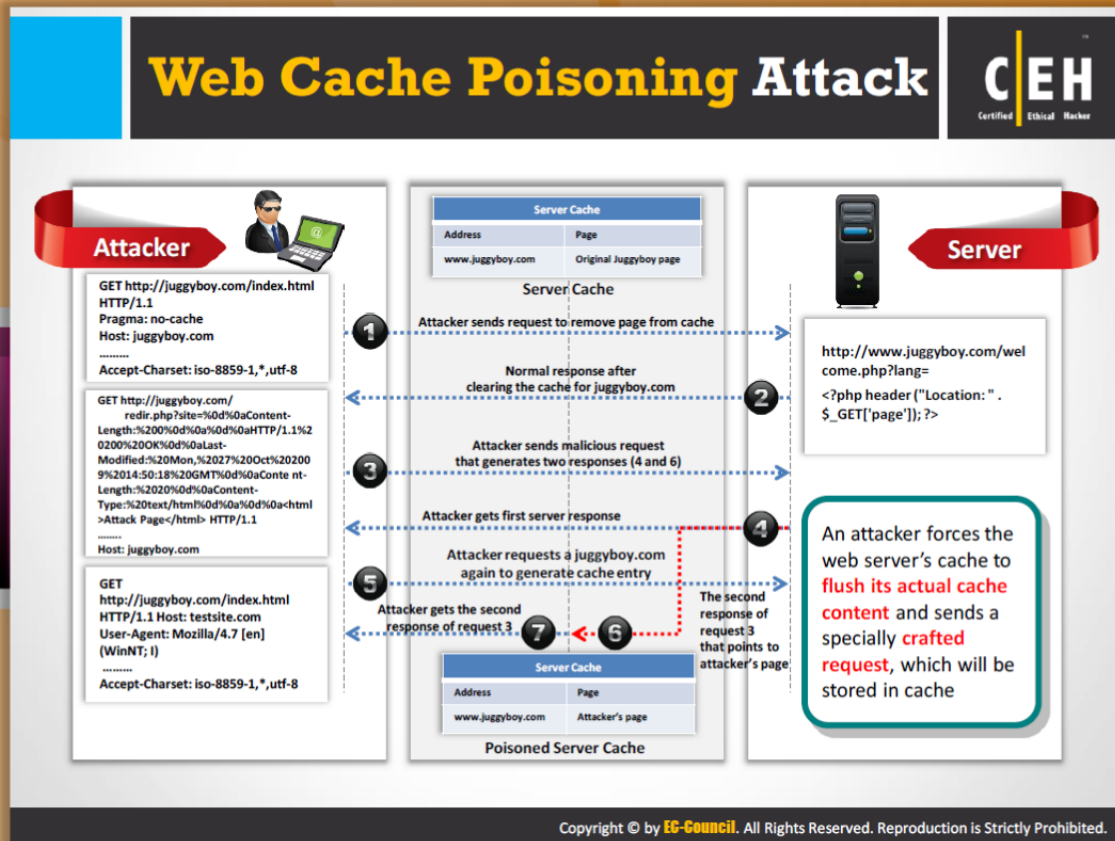


FIGURE 12.8: HTTP Response Splitting Attack



Web Cache Poisoning Attack

Web cache poisoning is an attack that is carried out in contrast to the **reliability of an intermediate web cache source**, in which honest content cached for a random URL is swapped with infected content. Users of the web cache source can unknowingly use the poisoned content instead of true and secured content when demanding the required URL through the web cache.

An attacker forces the web server's cache to flush its actual cache content and sends a specially crafted request to store in cache. In the following diagram, the **whole process of web cache poisoning is explained in detail with a step-by-step procedure**.

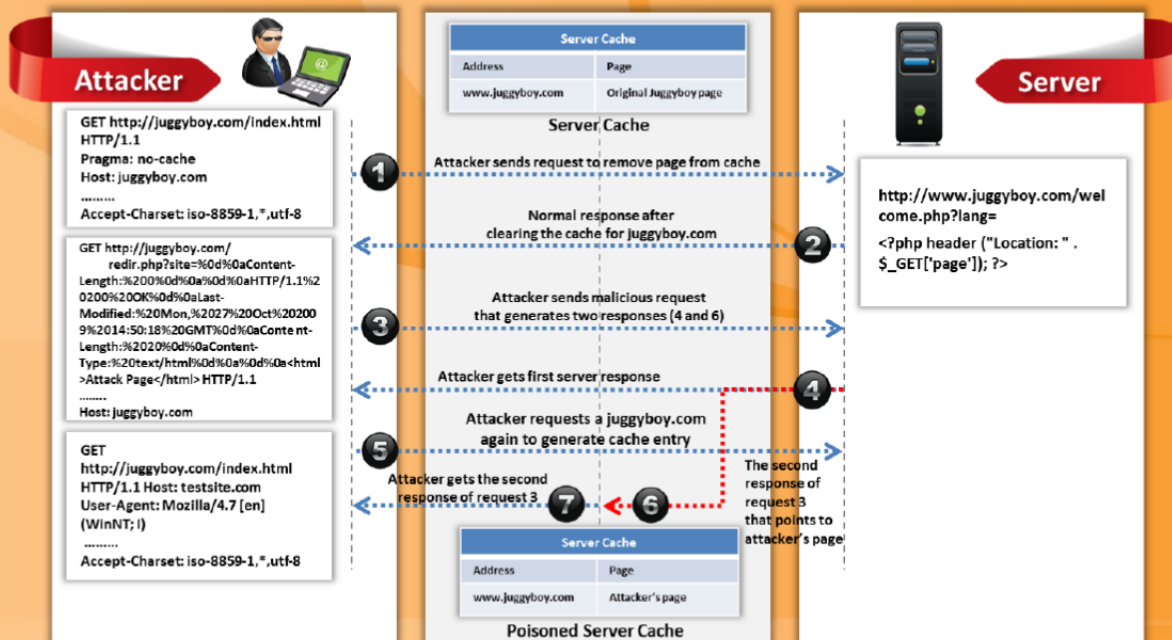
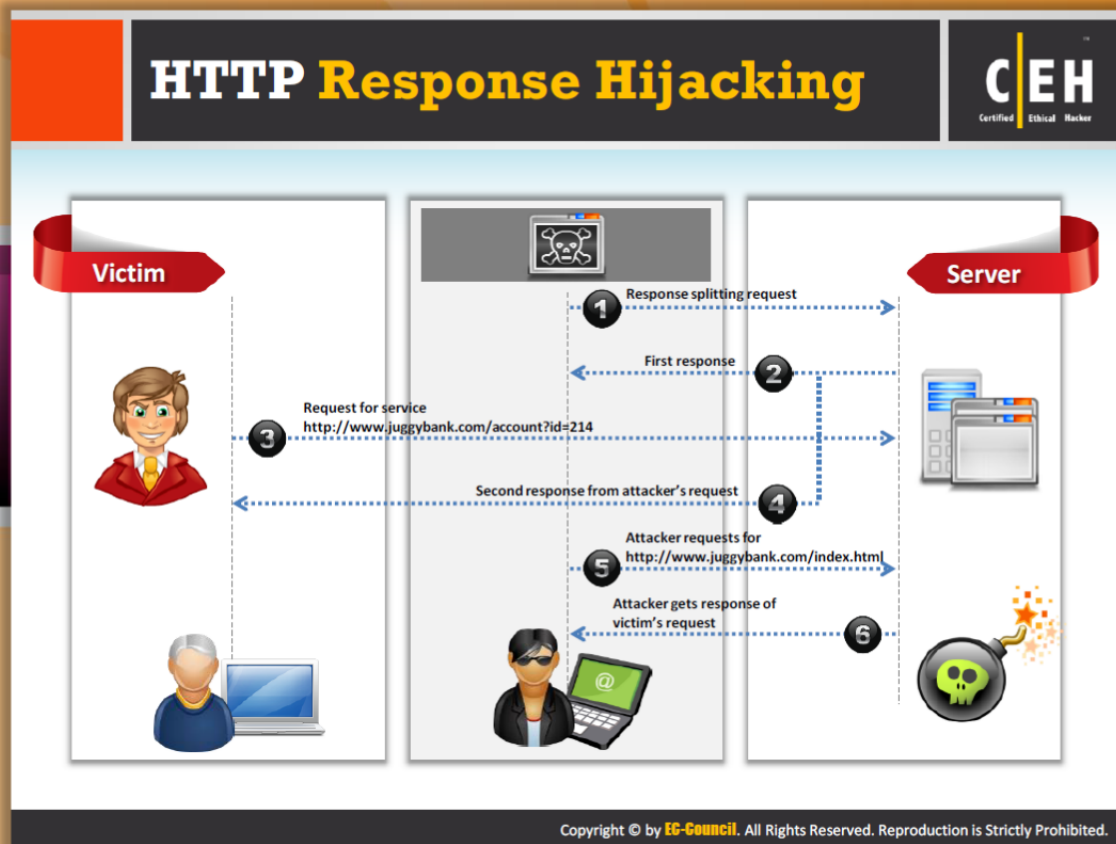


FIGURE 12.9: Web Cache Poisoning Attack



HTTP Response Hijacking

HTTP response hijacking is accomplished with a response splitting request. In this attack, **initially the attacker sends a response splitting request to the web server**. The server splits the response into two and sends the first response to the attacker and the second response to the victim. On receiving the response from web server, the victim requests for service by giving credentials. At the same time, the attacker requests the index page. Then the web server sends the response of the victim's request to the attacker and the victim remains uninformed.

The diagram that follows shows the **step-by-step** procedure of an HTTP response hijacking attack:

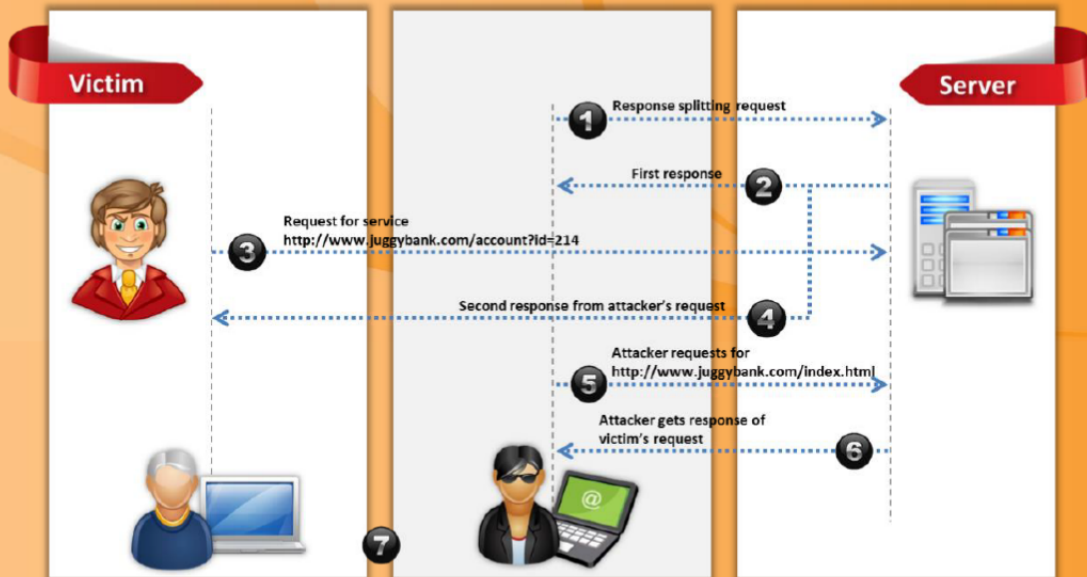
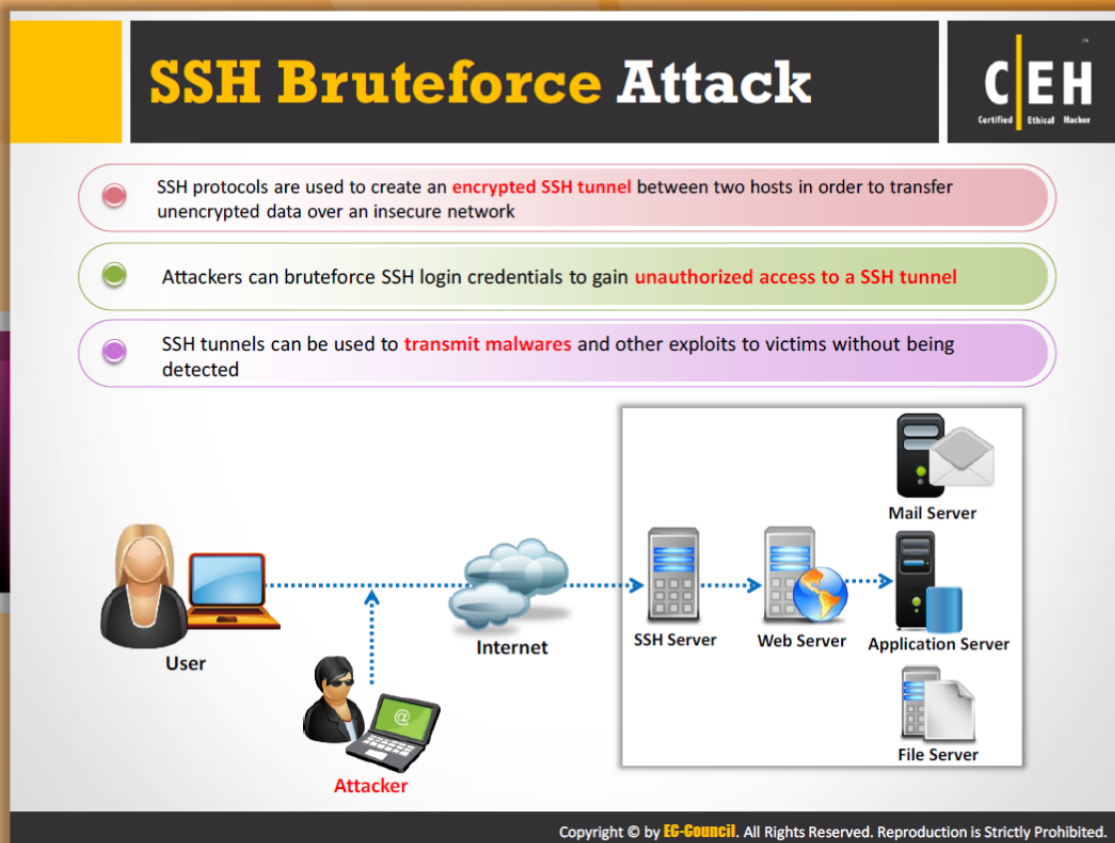


FIGURE 12.10: HTTP Response Hijacking



SSH Brute Force Attack

SSH protocols are used to create an encrypted SSH tunnel between two hosts in order to transfer unencrypted data over an insecure network. In order to conduct an attack on SSH, first the attacker scans the **entire SSH server to identify the possible vulnerabilities**. With the help of a brute force attack, the attacker gains the login credentials. Once the attacker gains the login credentials of SSH, he or she uses the same **SSH tunnels** to transmit malware and other exploits to victims without being detected.

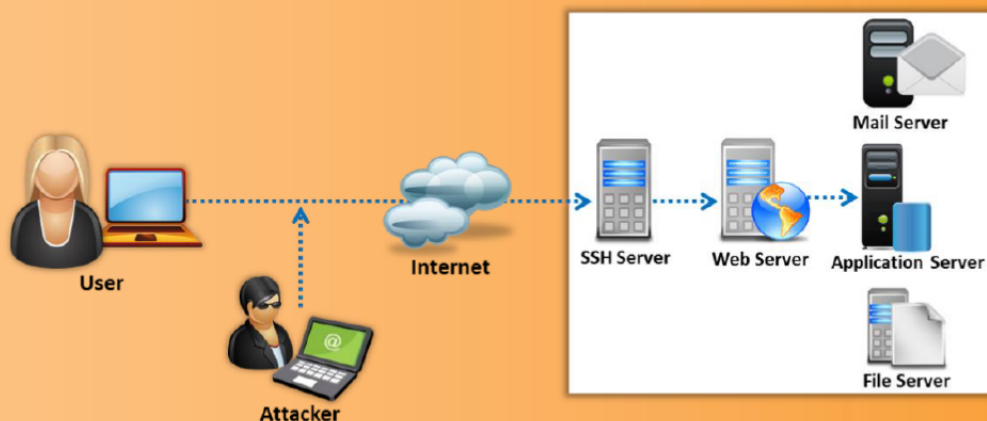
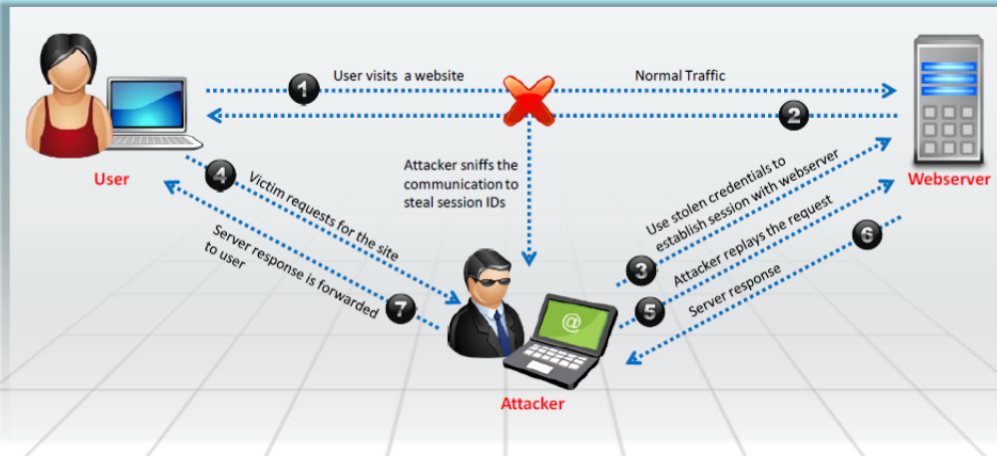


FIGURE 12.11: SSH Brute Force Attack

Man-in-the-Middle Attack



- Man-in-the-Middle (MITM) attacks allow an attacker to access sensitive information by **intercepting and altering communications** between an end-user and webservers
- Attacker **acts as a proxy** such that all the communication between the user and webserver passes through him



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Man-in-the-Middle Attack

A man-in-the-middle attack is a method where an intruder intercepts or modifies the message being exchanged between the user and web server through eavesdropping or intruding into a connection. This allows an **attacker to steal sensitive information** of a user such as online banking details, user names, passwords, etc. transferred over the Internet to the web server. The attacker lures the victim to connect to the web server through by pretending to be a proxy. If the victim believes and agrees to the attacker's request, then all the communication between the user and the web server passes through the attacker. Thus, the **attacker can steal sensitive user information**.

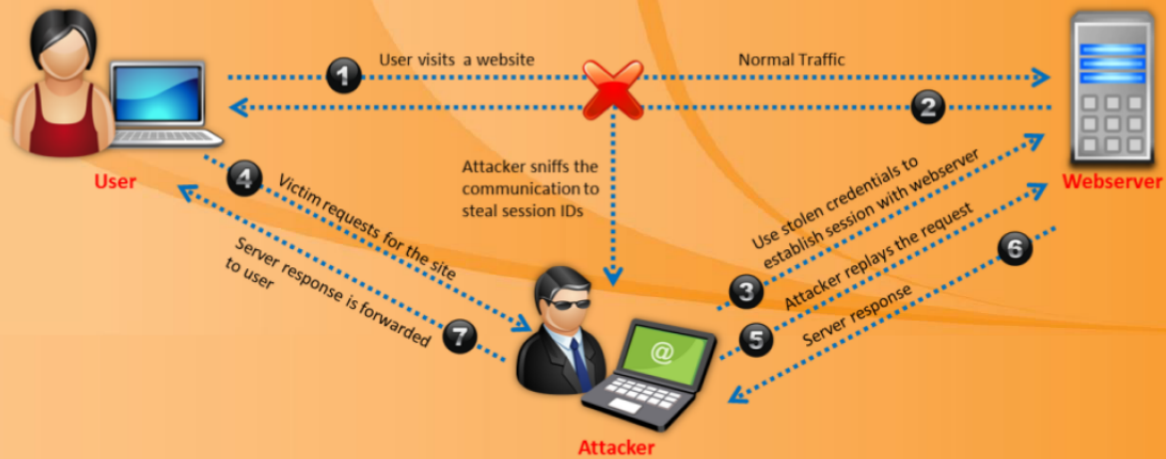
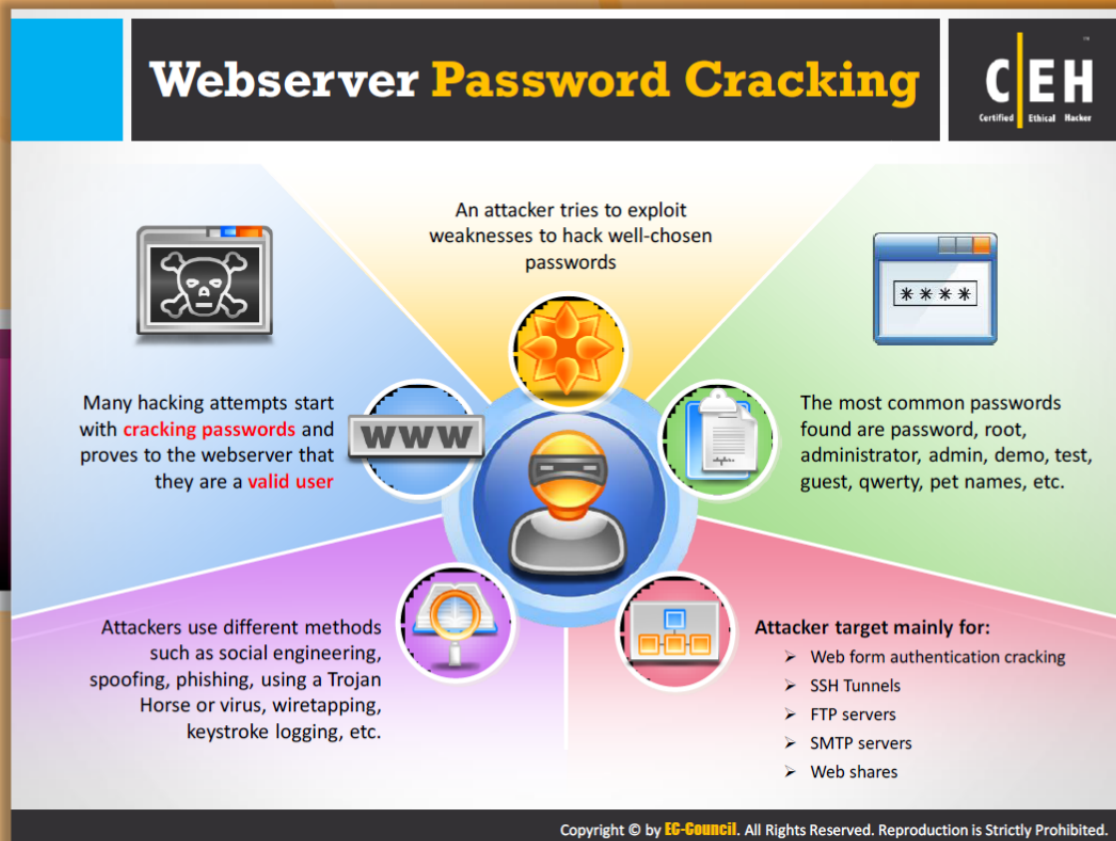


FIGURE 12.12: Man-in-the-Middle Attack



Web Server Password Cracking

Most hacking starts with password cracking only. Once the password is cracked, the hacker can log in to the network as an authorized person. Most of the common passwords found are **password, root, administrator, admin, demo, test, guest, QWERTY, pet names, etc.** Attackers use different methods such as social engineering, spoofing, phishing, using a Trojan horse or virus, wiretapping, keystroke logging, a brute force attack, a dictionary attack, etc. to crack passwords.

Attackers mainly target:

- Web form authentication cracking
- SSH tunnels
- FTP servers
- SMTP servers
- Web shares

Webserver Password Cracking Techniques



- Passwords may be cracked **manually** or with **automated tools** such as Cain and Abel, Brutus, THC Hydra, etc.
- Passwords can be cracked by using following techniques:



1 Guessing

A common cracking method used by attackers to guess passwords either by humans or by automated tools provided with dictionaries

2 Dictionary Attacks

A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly



3 Brute Force Attack

The most time-consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken.



4 Hybrid Attack

A hybrid attack works similar to dictionary attack, but it adds numbers or symbols to the password attempt

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

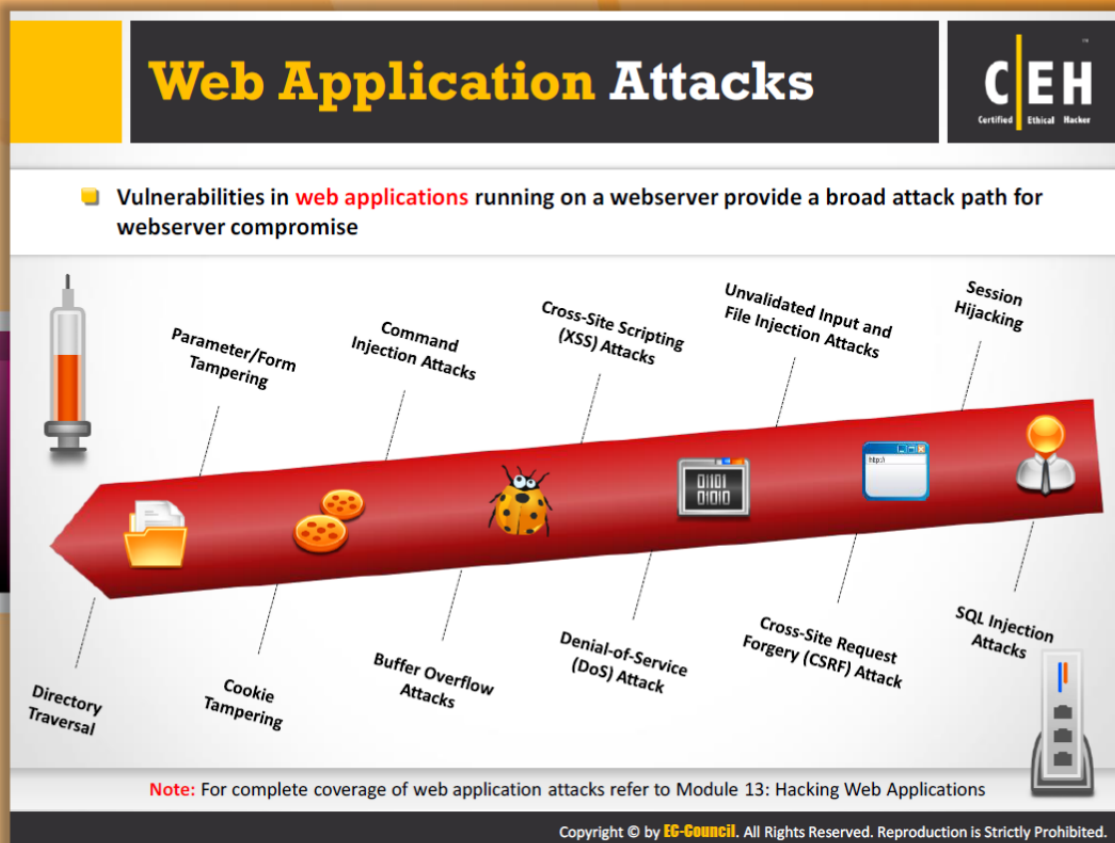


Web Server Password Cracking Techniques

Passwords may be cracked manually or with automated tools such as Cain & Abel, Brutus, THC Hydra, etc. Attackers follow various techniques to crack the password:

- **Guessing:** A common cracking method used by attackers is to guess passwords either by humans or by automated tools provided with dictionaries. Most people tend to use heir pets' names, loved ones' names, license plate numbers, dates of birth, or other weak pass words such as "QWERTY," "password," "admin," etc. so that they can remember them easily. The same thing allows the attacker to crack passwords by guessing.
- **Dictionary Attack:** A dictionary attack is a method that has predefined words of various combinations, but this might also not be possible to be effective if the password consists of special characters and symbols, but compared to a brute force attack this is less time consuming.
- **Brute Force Attack:** In the brute force method, all possible characters are tested, for example, uppercase from "A to Z" or numbers from "0 to 9" or lowercase "a to z." But this type of method is useful to identify one-word or two-word passwords. Whereas if a password consists of uppercase and lowercase letters and special characters, it might take months or years to crack the password, which is practically impossible.

- **Hybrid Attack:** A hybrid attack is more powerful as it uses both a dictionary attack and brute force attack. It also consists of symbols and numbers. Password cracking becomes easier with this method.



Web Application Attacks

Vulnerabilities in web applications running on a web server provide a broad attack path for web server compromise.



Directory Traversal

Directory traversal is **exploitation of HTTP** through which attackers are able to access restricted directories and execute commands outside of the web server root directory by manipulating a URL.



Parameter/Form Tampering

This type of **tampering attack** is intended to manipulate the parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc.



Cookie Tampering

Cookie tampering is the method of **poisoning or tampering with the cookie** of the client. The phases where most of the attacks are done are when sending a cookie from the client side to the server. Persistent and non-persistent cookies can be modified by using different tools.



Command Injection Attacks

Command injection is an attacking method in which a **hacker alters the content of the web page** by using html code and by identifying the form fields that lack valid constraints.



Buffer Overflow Attacks

Most web applications are designed to sustain some **amount of data**. If that amount is exceeded, the application may crash or may exhibit some other vulnerable behavior. The attacker uses this advantage and floods the applications with too much data, which in turn causes a buffer overflow attack.



Cross-Site Scripting (XSS) Attacks

Cross-site scripting is a method where an **attacker injects HTML tags** or scripts into a target website.



Denial-of-Service (DoS) Attack

A denial-of-service attack is a form of attack method **intended to terminate the operations of a website** or a server and make it unavailable to access for intended users.



Unvalidated Input and File Injection Attacks

Unvalidated input and file injection attacks refer to the attacks carried by **supplying an unvalidated input** or by injecting files into a web application.



Cross-Site Request Forgery (CSRF) Attack

The user's web browser is requested by a malicious web page to send requests to a malicious website where various vulnerable actions are performed, which are not intended by the user. This kind of attack is dangerous in the case of **financial websites**.



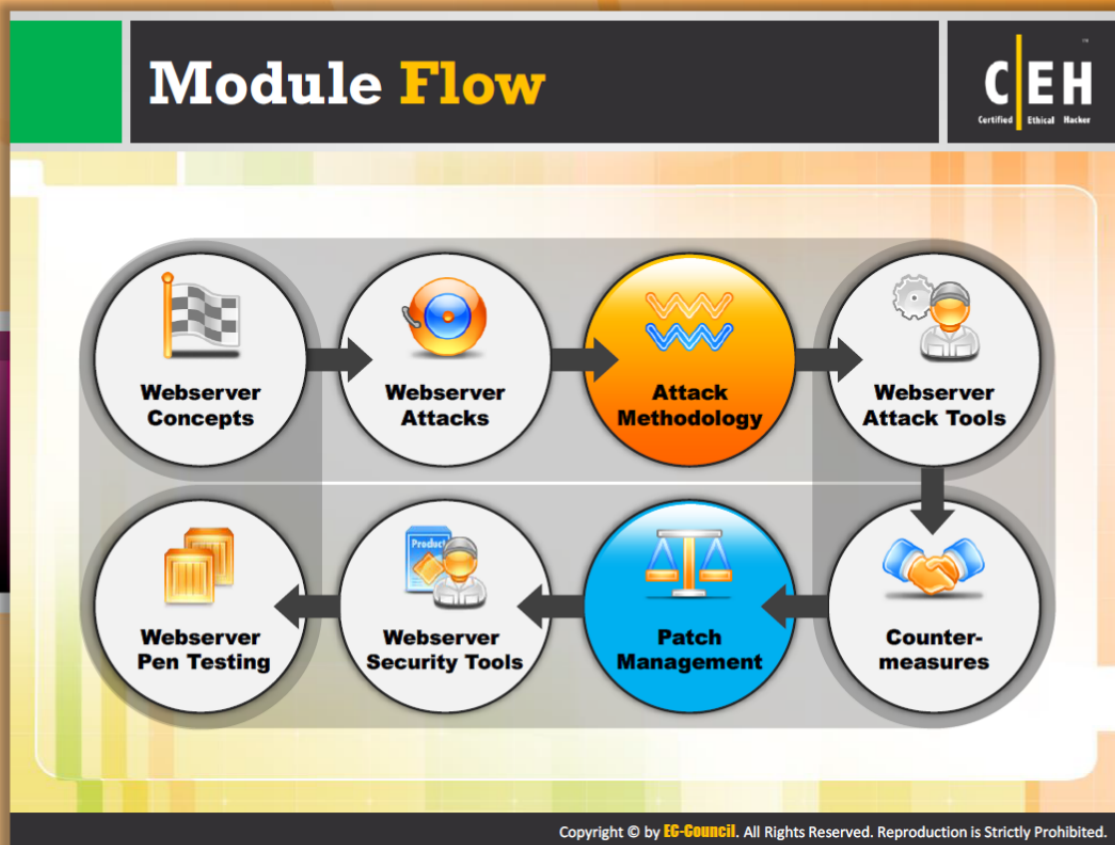
SQL Injection Attacks

SQL injection is a code injection technique that uses the security vulnerability of a database for attacks. The attacker injects malicious code into the strings that are later on passed on to SQL Server for execution.



Session Hijacking

Session hijacking is an attack where the attacker exploits, steals, predicts, and negotiates the real valid **web session** control mechanism to access the authenticated parts of a web application.



Module Flow

So far we have discussed web server concepts and various techniques used by the attacker to hack web server. Attackers usually hack a web server by following a procedural method. Now we will discuss the attack methodology used by attackers to compromise web servers.

 Webserver Concepts	 Webserver Attacks
 Attack Methodology	 Webserver Attack Tools
 Webserver Pen Testing	 Webserver Security Tools
 Patch Management	 Counter-measures

This section provides insight into the attack methodology and tools that help at various stages of hacking.



Web Server Attack Methodology

Hacking a web server is accomplished in various stages. At each stage the attacker tries to gather more information about **loopholes** and tries to gain unauthorized access to the web server. The stages of **web server attack** methodology include:



Information Gathering

Every attacker tries to collect as much information as possible about the target web server. Once the information is gathered, he or she then analyzes the gathered information in order to find the security lapses in the current mechanism of the web server.



Web Server Footprinting

The purpose of footprinting is to gather more information about security aspects of a web server with the help of tools or footprinting techniques. The main purpose is to know about its remote access capabilities, its ports and services, and the aspects of its security.



Mirroring Website

Website mirroring is a method of copying a website and its content onto another server for offline browsing.



Vulnerability Scanning

Vulnerability scanning is a method of finding various **vulnerabilities and misconfigurations of a web server**. Vulnerability scanning is done with the help of various automated tools known as vulnerable scanners.



Session Hijacking


Session hijacking is possible once the current session of the client is identified. Complete control of the user session is taken over by the attacker by means of session hijacking.




Hacking Web Server Passwords

Attackers use various password cracking methods like brute force attacks, hybrid attacks, dictionary attacks, etc. and crack web server passwords.


Webserver Attack Methodology: Information Gathering



- Information gathering involves collecting information about the **targeted company**
- Attackers search the **Internet, newsgroups, bulletin boards**, etc. for information about the company
- Attackers use **Whois, Traceroute, Active Whois**, etc. tools and query the Whois databases to get the details such as a domain name, an IP address, or an autonomous system number



Note: For complete coverage of information gathering techniques refer to Module 02: Footprinting and Reconnaissance



WHOIS information for ebay.com:***
[Querying whois.version-gis.com]
[whois.version-gis.com]
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.
Domain Name: EBAY.COM
Registrar: MARKMONITOR INC.
Whois Server: whois.markmonitor.com
Referral URL: <http://www.markmonitor.com>
Name Server: SJC-DNS1.EBAYDNS.COM
Name Server: SJC-DNS2.EBAYDNS.COM
Name Server: SMF-DNS1.EBAYDNS.COM
Name Server: SMF-DNS2.EBAYDNS.COM
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 15-sep-2010
Creation Date: 04-aug-1995
Expiration Date: 03-aug-2018
<<
<http://www.whois.net>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attack Methodology: Information Gathering

Every attacker before hacking first collects all the required information such as versions and technologies being used by the web server, etc. Attackers search the Internet, newsgroups, bulletin boards, etc. for information about the company. Most of the attackers' time is spent in the **phase of information gathering** only. That's why information gathering is both an art as well as a science. There are many tools that can be used for information gathering or to get details such as a domain name, an IP address, or an autonomous system number. The tools include:

- Whois
- Traceroute
- Active Whois
- Nmap
- Angry IP Scanner
- Netcat



Whois

Source: <http://www.whois.net>

Whois allows you to perform a domain whois search and a whois IP lookup and search the whois database for relevant information on domain registration and availability. This can help provide **insight into a domain's history and additional information**. It can be used for performing a search to see who owns a domain name, how many pages from a site are listed with Google, or even search the Whois address listings for a website's owner.

The image shows two screenshots from the WHOIS.net website. The top screenshot is the homepage with the WHOIS.net logo and a search bar containing 'ebay.com'. The bottom screenshot shows the WHOIS information for 'ebay.com', including details like the domain name, registrar, name servers, and creation/expiration dates.

WHOIS information for ebay.com:***

[Querying whois.verisign-grs.com]
[whois.verisign-grs.com]
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.
Domain Name: EBAY.COM
Registrar: MARKMONITOR INC.
Whois Server: whois.markmonitor.com
Referral URL: <http://www.markmonitor.com>
Name Server: SJC-DNS1.EBAYDNS.COM
Name Server: SJC-DNS2.EBAYDNS.COM
Name Server: SMF-DNS1.EBAYDNS.COM
Name Server: SMF-DNS2.EBAYDNS.COM
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 15-sep-2010
Creation Date: 04-aug-1995
Expiration Date: 03-aug-2018
<<

FIGURE 12.13: WHOIS Information Gathering

Webserver Attack Methodology: Webserver Footprinting



- Gather **valuable system-level information** such as account details, operating system, software versions, server names, and database schema details
- **Telnet** a webserver to footprint a webserver and gather information such as server name, server type, operating systems, applications running, etc.
- Use tool such as **ID Serve**, **httprecon**, and **Netcraft** to perform footprinting





<http://toolbar.netcraft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



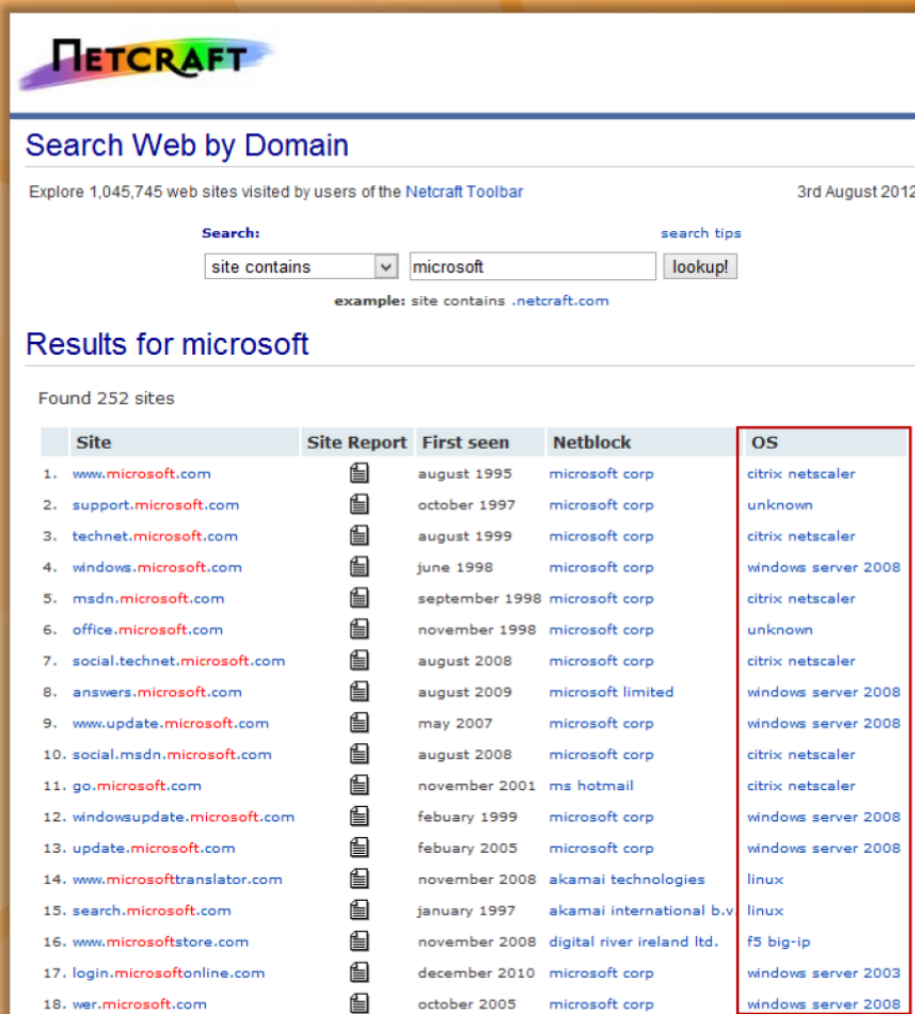
Web Server Attack Methodology: Web server Footprinting

The purpose of footprinting is to gather account details, operating system and other **software versions, server names, and database schema** details and as much information as possible about security aspects of a target web server or network. The main purpose is to know about its remote access capabilities, open ports and services, and the security mechanisms implemented. Telnet a web server to footprint a web server and gather information such as server name, server type, operating systems, applications running, etc. Examples of tools used for performing footprinting include **ID Serve, httprecon, Netcraft**, etc.

Netcraft

Source: <http://toolbar.netcraft.com>

Netcraft is a tool used to determine the OSES in use by the target organization. It has already been discussed in detail in the Footprinting and Reconnaissance module.



NETCRAFT

Search Web by Domain

Explore 1,045,745 web sites visited by users of the Netcraft Toolbar 3rd August 2012

Search: search tips

site contains

example: site contains .netcraft.com

Results for microsoft

Found 252 sites

Site	Site Report	First seen	Netblock	OS
1. www.microsoft.com		august 1995	microsoft corp	citrix netscaler
2. support.microsoft.com		october 1997	microsoft corp	unknown
3. technet.microsoft.com		august 1999	microsoft corp	citrix netscaler
4. windows.microsoft.com		june 1998	microsoft corp	windows server 2008
5. msdn.microsoft.com		september 1998	microsoft corp	citrix netscaler
6. office.microsoft.com		november 1998	microsoft corp	unknown
7. social.technet.microsoft.com		august 2008	microsoft corp	citrix netscaler
8. answers.microsoft.com		august 2009	microsoft limited	windows server 2008
9. www.update.microsoft.com		may 2007	microsoft corp	windows server 2008
10. social.msdn.microsoft.com		august 2008	microsoft corp	citrix netscaler
11. go.microsoft.com		november 2001	ms hotmail	citrix netscaler
12. windowsupdate.microsoft.com		february 1999	microsoft corp	windows server 2008
13. update.microsoft.com		february 2005	microsoft corp	windows server 2008
14. www.microsofttranslator.com		november 2008	akamai technologies	linux
15. search.microsoft.com		january 1997	akamai international b.v	linux
16. www.microsoftstore.com		november 2008	digital river ireland ltd.	f5 big-ip
17. login.microsoftonline.com		december 2010	microsoft corp	windows server 2003
18. wer.microsoft.com		october 2005	microsoft corp	windows server 2008

FIGURE 12.14: Web server Footprinting



Web Server Footprinting Tools

We have already discussed about the Netcraft tool. In addition to the Netcraft tool, there are two more tools that allow you to perform web server footprinting. They are Httprecon and ID Serve.



Httprecon

Source: <http://www.compute.ch>

Httprecon is a tool for advanced web server fingerprinting. The httprecon project is doing some research in the **field of web server fingerprinting**, also known as http fingerprinting. The goal is the highly accurate identification of given httpd implementations. This software shall improve the ease and efficiency of this kind of **enumeration**.

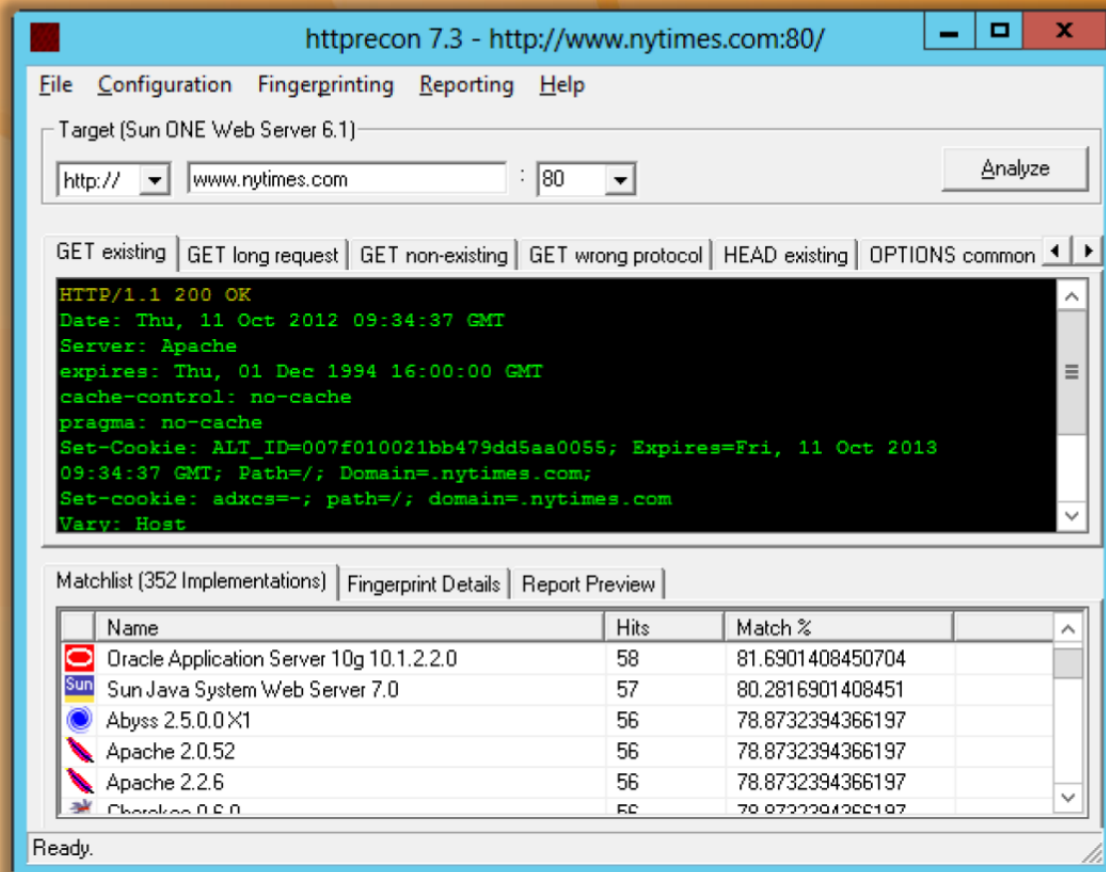


FIGURE 12.15: Httprecon Screenshot



ID Serve

Source: <http://www.grc.com>

ID Serve is a simple Internet server identification utility. ID Serve can almost always identify the make, model, and version of any **website's server software**. This information is usually sent in the preamble of replies to web queries, but it is not shown to the user. ID Serve can also connect with non-web servers to receive and report that server's greeting message. This generally reveals the server's make, model, version, and other potentially useful information. Simply by entering any IP address, ID Serve will attempt to determine the **associated domain name**.

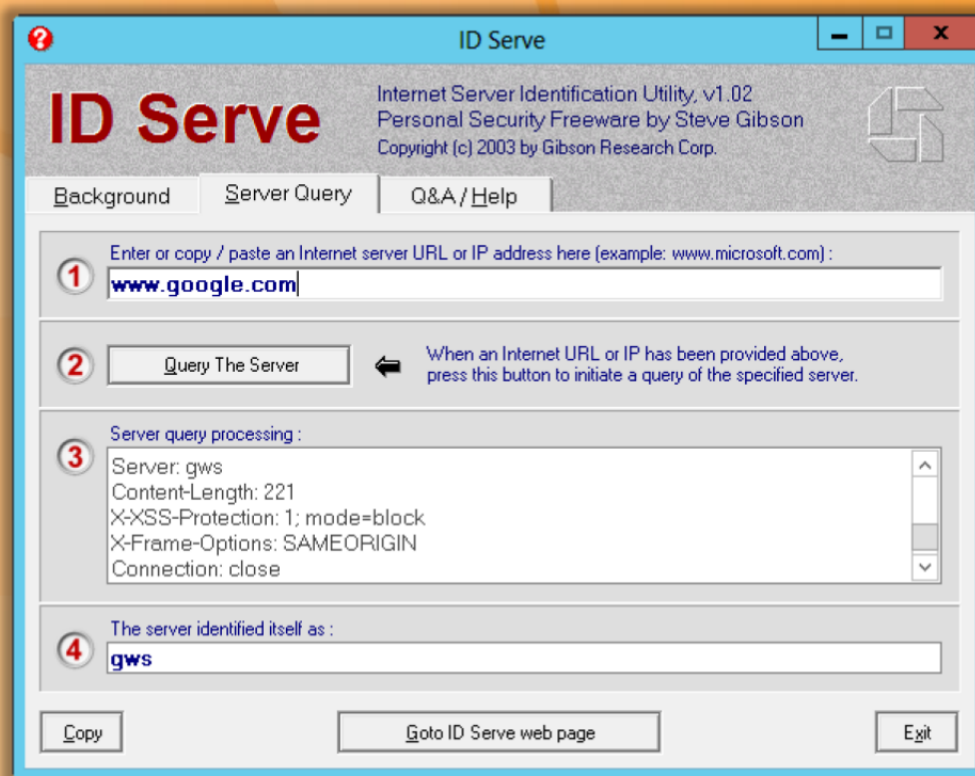

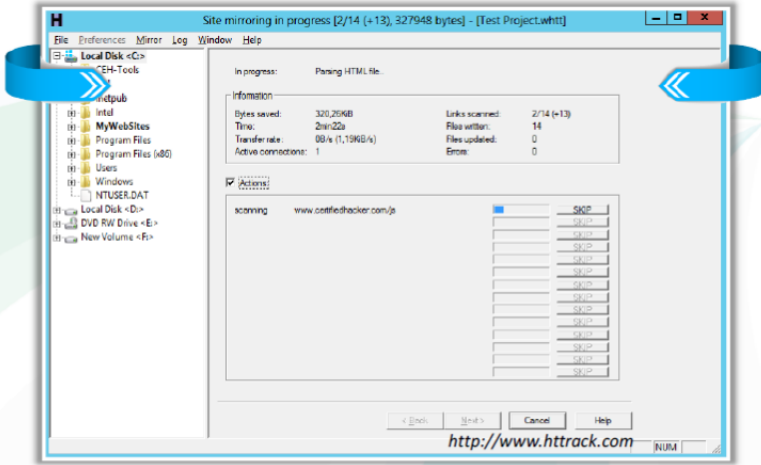


FIGURE 12.16: ID Serve

Webserver Attack Methodology: Mirroring a Website



- Mirror a website to create a complete profile of the site's **directory structure**, **files structure**, **external links**, etc.
- Search for **comments** and other items in the HTML source code to make footprinting activities more efficient
- Use tools **HTTrack**, **WebCopier Pro**, **BlackWidow**, etc. to mirror a website



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attack Methodology: Mirroring a Website

Website mirroring is a method of copying a website and its content onto another server. By mirroring a website, a complete profile of the site's directory structure, file structure, external links, etc. is created. Once the mirror website is created, search for comments and other items in the HTML source code to make footprinting activities more efficient. Various tools used for web server mirroring **include HTTrack, Webripper 2.0, WinWSD, Webcopier, and Blackwidow.**



C

Source: <http://www.httrack.com>

HTTrack is an offline browser utility. It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original **site's relative link-structure**. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online.

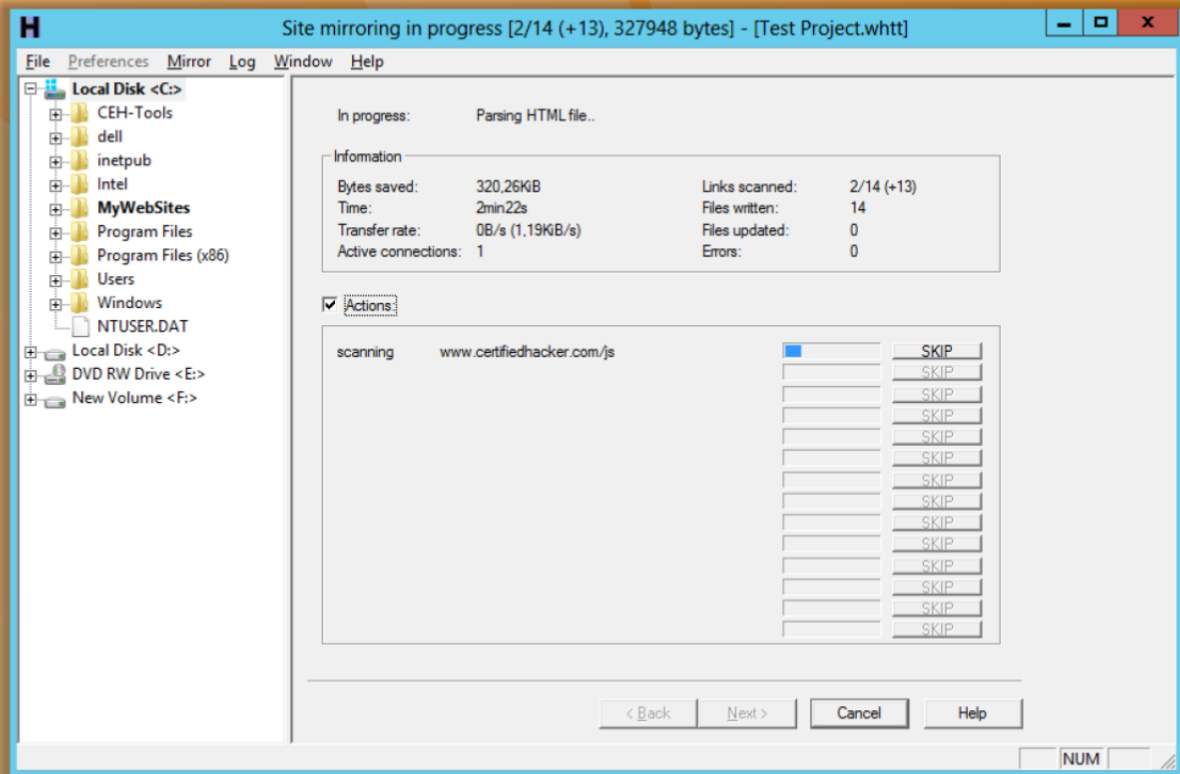


FIGURE 12.17: Mirroring a Website

Webserver Attack Methodology: Vulnerability Scanning

Perform vulnerability scanning to **identify weaknesses** in a network and determine if the system can be exploited

Use a vulnerability scanner such as HP WebInspect, Nessus, Zaproxy, etc. to find **hosts, services, and vulnerabilities**

Sniff the network traffic to find out **active systems, network services, applications, and vulnerabilities** present

Test the **web server infrastructure** for any misconfiguration, outdated content, and known vulnerabilities



<http://www.nessus.org>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attack Methodology: Vulnerability Scanning

Vulnerability scanning is a method of determining various vulnerabilities and misconfigurations of a target web server or network. Vulnerability scanning is done with the help of **various automated tools known as vulnerable scanners**.

Vulnerability scanning allows determining the vulnerabilities that exist in the web server and its configuration. Thus, it helps to determine whether the web server is exploitable or not. Sniffing techniques are adopted in the **network traffic to find out active systems, network services, applications, and vulnerabilities present**.

Also, attackers test the web server infrastructure for any misconfiguration, outdated content, and known vulnerabilities. Various tools are used for vulnerability scanning such as HP WebInspect, Nessus, Paros proxy, etc. to find hosts, services, and vulnerabilities.



Nessus

Source: <http://www.nessus.org>

Nessus is a security scanning tools that scan the system remotely and reports if it detects the **vulnerabilities before the attacker actually attacks** and compromises them. Its five features includes high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis of your security posture with features

that enhance usability, effectiveness, efficiency, and communication with all parts of your organization.

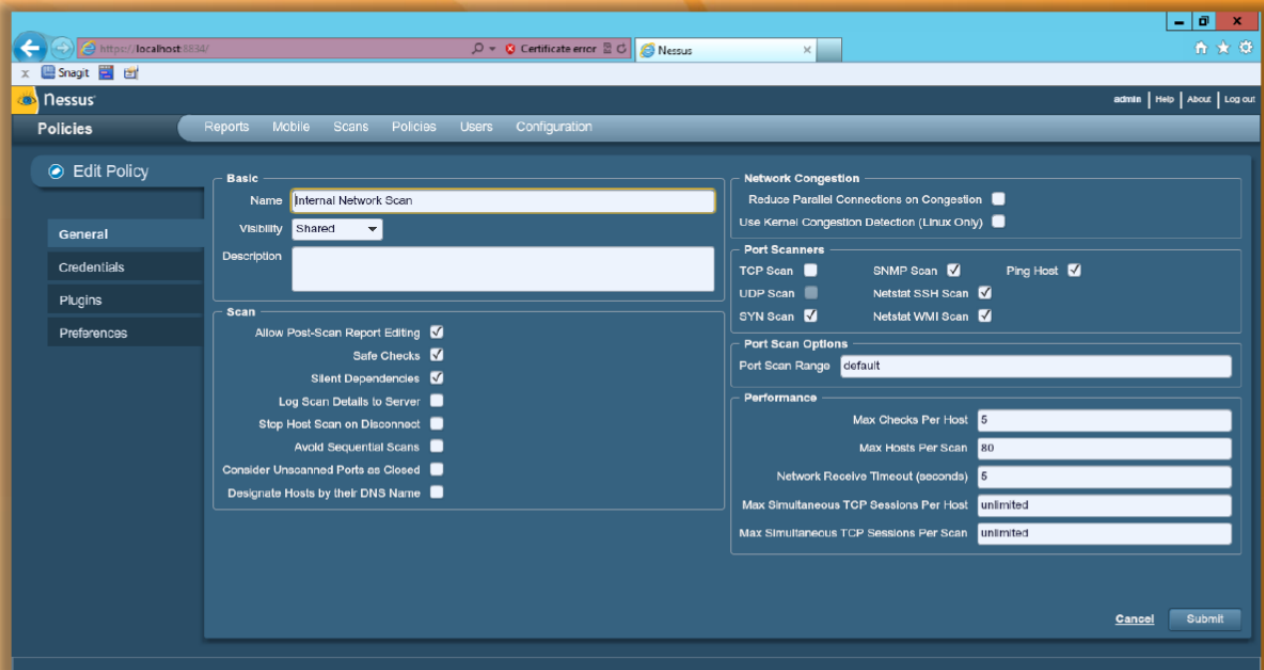


FIGURE 12.18: Nessus Screenshot

Webserver Attack Methodology: Session Hijacking



- Sniff valid session IDs to **gain unauthorized access** to the Web Server and snoop the data
- Use session hijacking techniques such as session fixation, session sidejacking, Cross-site scripting, etc. to **capture valid session cookies and IDs**
- Use tools such as **Burp Suite, Hamster, Firesheep**, etc. to automate session hijacking



<http://portswigger.net>

Note: For complete coverage of Session Hijacking concepts and techniques refer to Module 11: Session Hijacking

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attack Methodology: Session Hijacking

Session hijacking is possible once the current session of the client is identified. Complete control of the user session can be taken over by the attacker once the user establishes authentication with the server. With the help of sequence number prediction tools, attackers perform session hijacking. The attacker, after **identifying the open session, predicts the sequence number of the next packet** and then sends the data packets before the legitimate user sends the response with the correct sequence number. Thus, an attacker performs session hijacking. In addition to this technique, you can also use other session hijacking techniques such as session fixation, session sidejacking, cross-site scripting, etc. to capture valid session cookies and IDs. Various tools used for **session hijacking include Burp Suite, Hamster, Firesheep, etc.**



Burp Suite

Source: <http://portswigger.net>

Burp Suite is an integrated platform for performing **security testing of web applications**. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. The key components of **Burp Suite include proxy, scanner, intruder tool, repeater tool, sequencer tool, etc.**

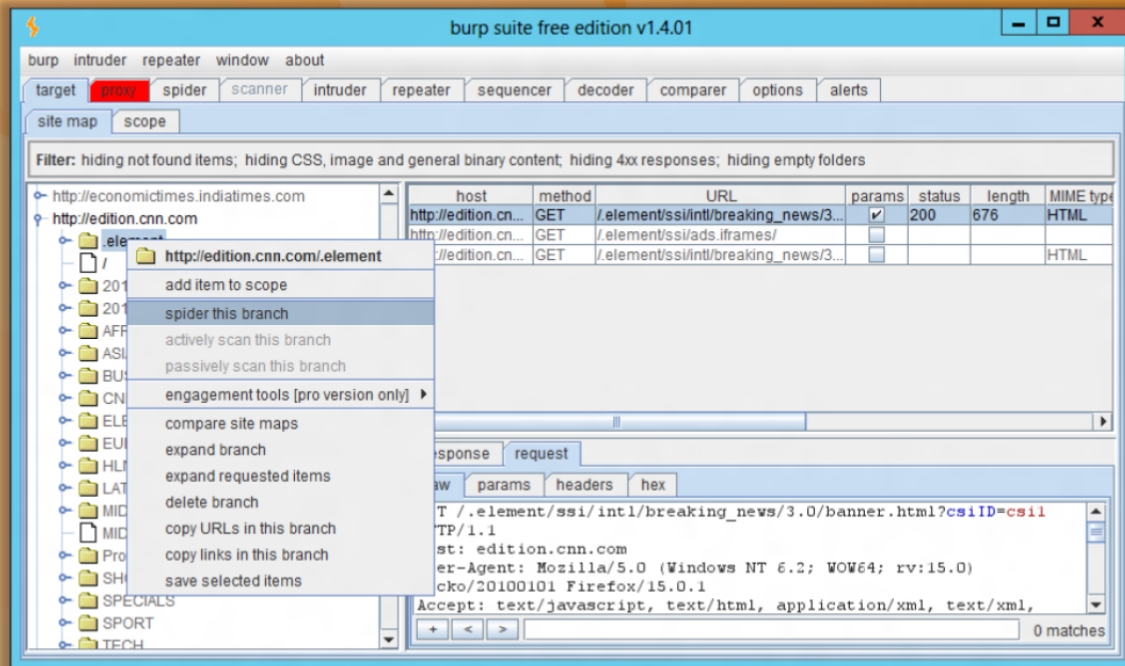




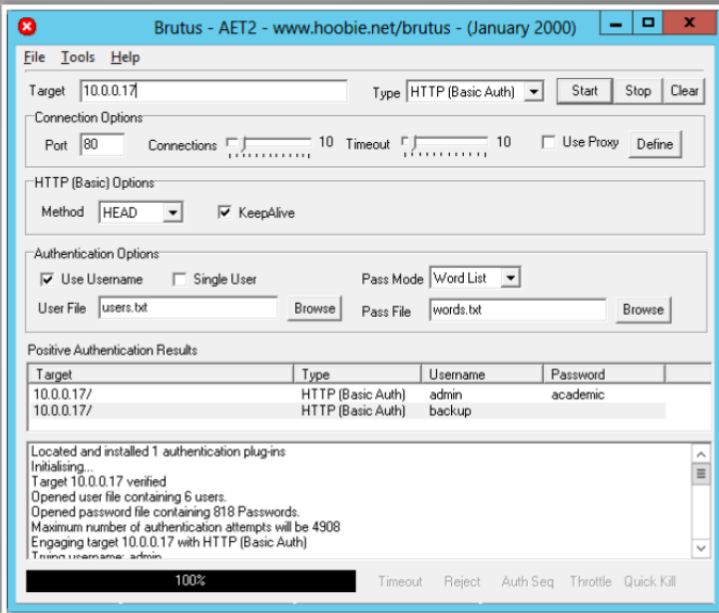
FIGURE 12.19: Burp Suite Screenshot

Webserver Attack Methodology:
Hacking Web Passwords



- Use password cracking techniques such as brute force attack, dictionary attack, password guessing to crack webserver passwords
- Use tools such as **Brutus**, **THC-Hydra**, etc.





http://www.hoobie.net

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attack Methodology: Hacking Web Passwords

One of the main tasks of any attacker is password hacking. By hacking a password, the attacker gains complete control over the web server. Various methods used by attackers for password hacking include **password guessing, dictionary attacks, brute force attacks, hybrid attacks, syllable attacks, precomputed hashes, rule-based attacks, distributed network attacks, rainbow attacks**, etc. Password cracking can also be performed with the help of tools such as Brutus, THC-Hydra, etc.



Brutus

Source: <http://www.hoobie.net>

Brutus is an online or remote password cracking tools. Attackers use this tool for hacking web passwords without the knowledge of the victim. The features of the Brutus tool are been explained briefly on the following slide.

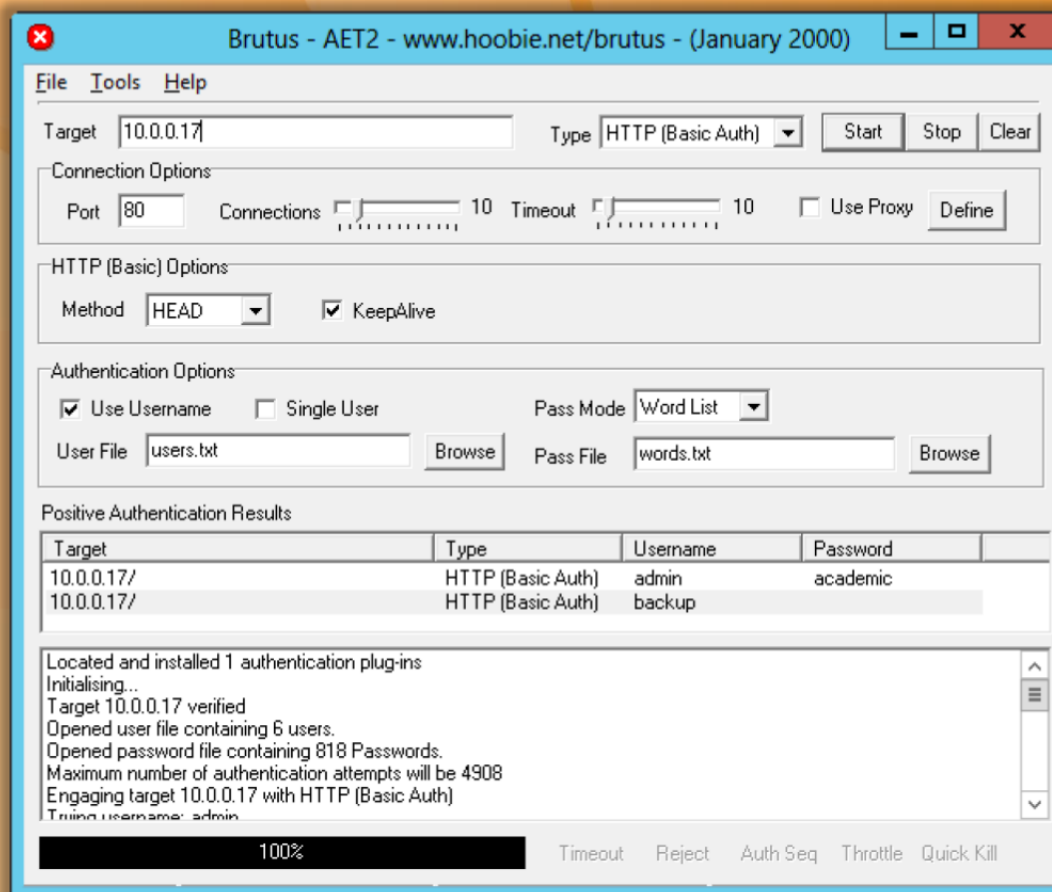
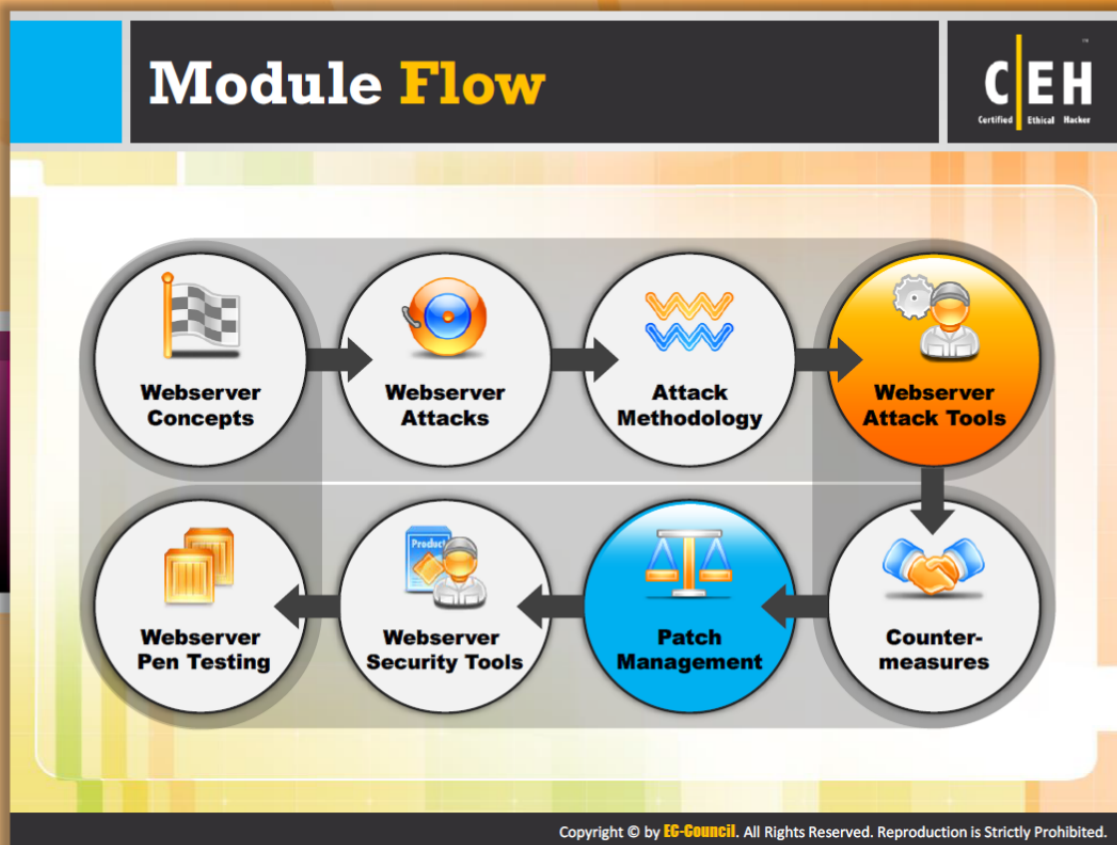


FIGURE 12.20: Brutus Screenshot



Module Flow

The tools intended for monitoring and managing the web server can also be used by attackers for malicious purposes. In this day and age, attackers are implementing various methods to hack web servers. Attackers with minimal knowledge about hacking usually use tools for hacking web servers.

 Webserver Concepts	 Webserver Attacks
 Attack Methodology	 Webserver Attack Tools
 Webserver Pen Testing	 Webserver Security Tools
 Patch Management	 Counter-measures

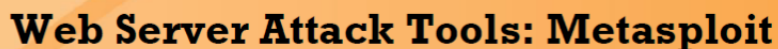
This section lists and describes various web server attack tools.

CEH
Certified Ethical Hacker

- 



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Source: <http://www.metasploit.com>

Metasploit enables teams of penetration testers to coordinate orchestrated attacks against target systems and for team leads to manage project access on a per-user basis. In addition, Metasploit includes customizable reporting.

- Complete penetration test assignments faster by automating repetitive tasks and leveraging multi-level attacks

- Assess the security of web applications, network and endpoint systems, as well as email users
- Emulate realistic network attacks based on the leading Metasploit framework with more than one million unique downloads in the past year
- Test with the world's largest public database of quality assured exploits
- **Tunnel any traffic through compromised targets to pivot deeper into the network**
- Collaborate more effectively with team members in concerted network tests
- Customize the content and template of executive, audit, and technical reports

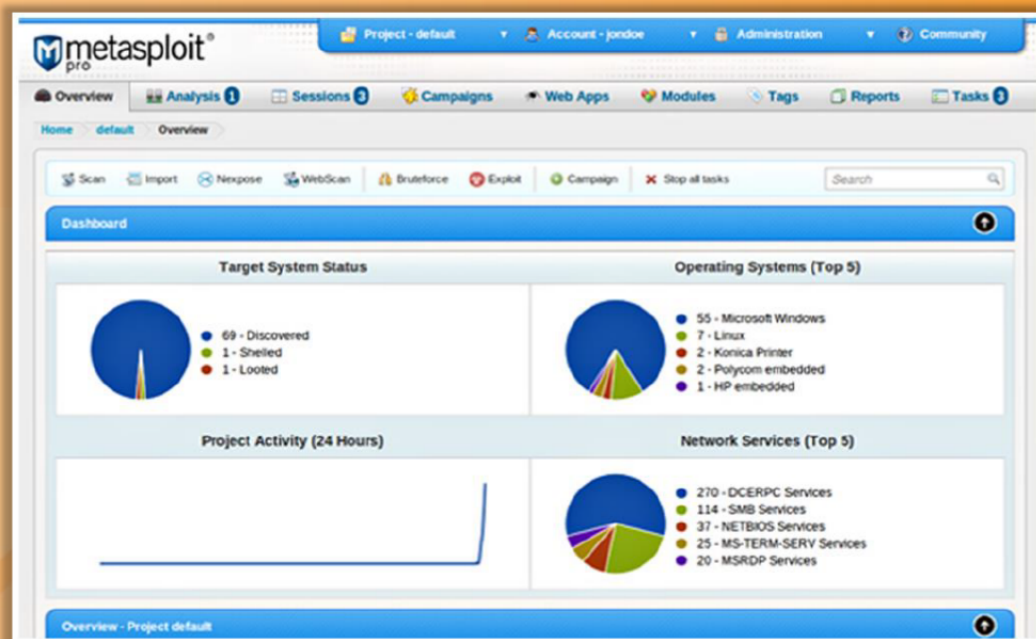
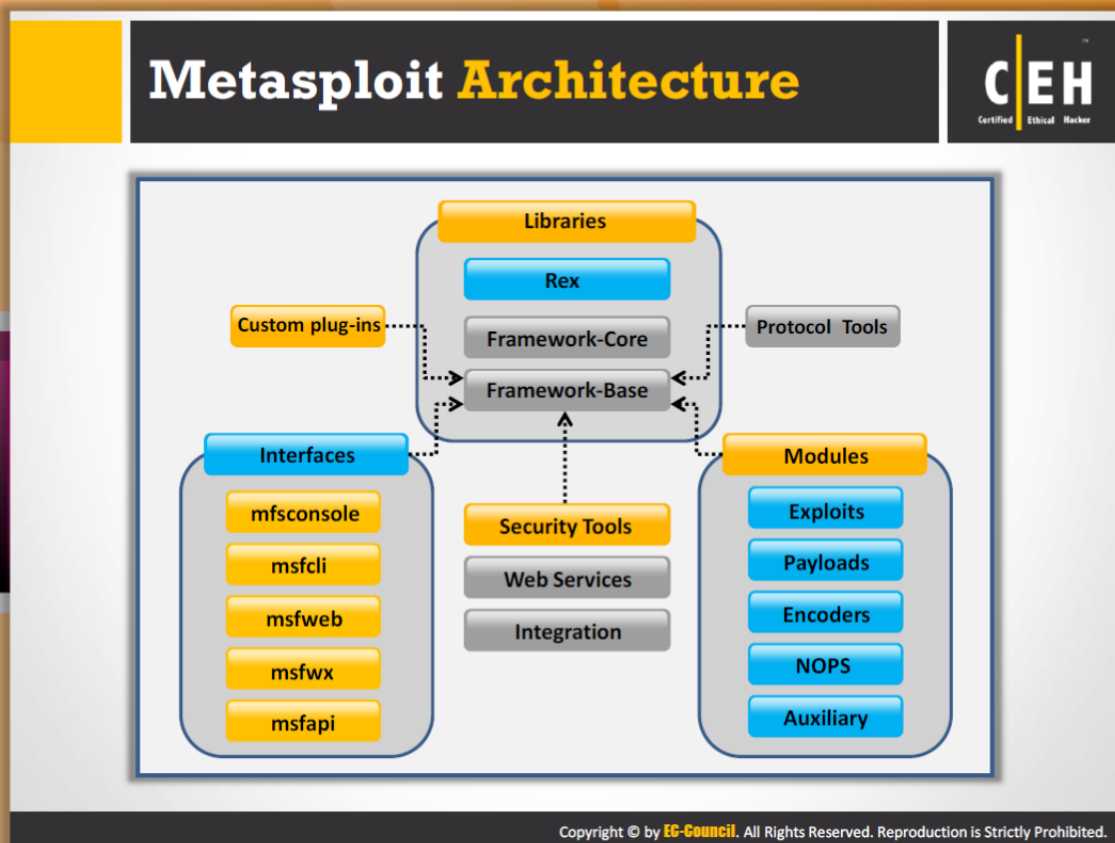


FIGURE 12.21: Metasploit Screenshot



Metasploit Architecture

The Metasploit framework is an open-source exploitation framework that is designed to provide security researchers and pen testers with a uniform model for rapid development of exploits, payloads, encoders, NOP generators, and reconnaissance tools. The framework provides the ability to reuse large chunks of code that would otherwise have to be copied or reimplemented on a per-exploit basis. The **framework was designed to be as modular as possible in order to encourage the reuse of code across various projects**. The framework itself is broken down into a few different pieces, the most low-level being the framework core. The framework core is responsible for implementing all of the required interfaces that allow for interacting with exploit modules, sessions, and plugins. It supports vulnerability research, exploit development, and the creation of custom security tools.

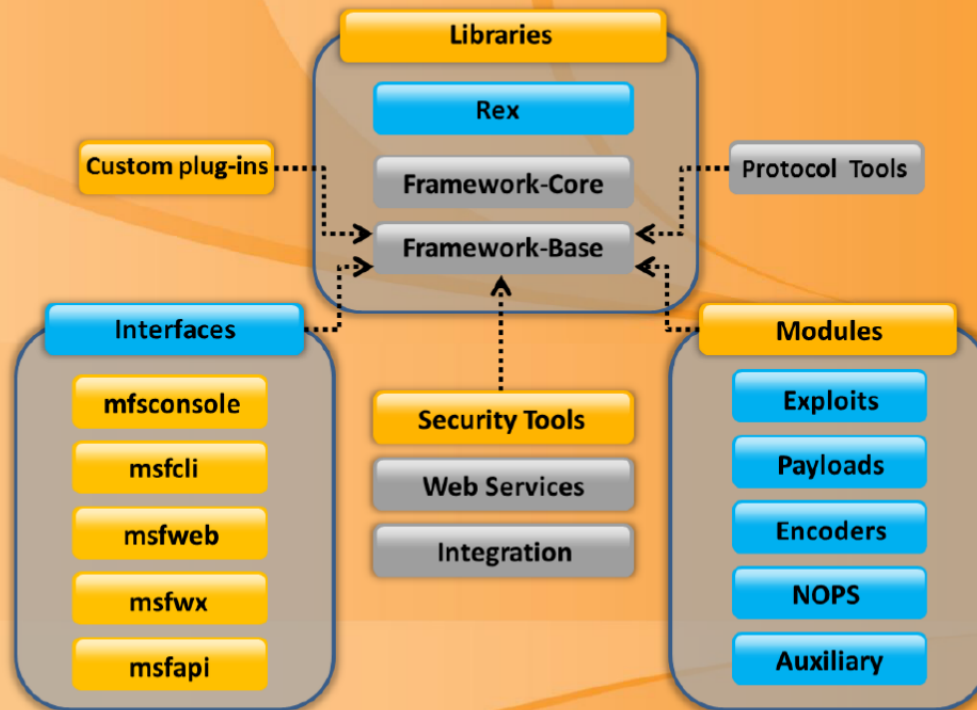


FIGURE 12.22: Metasploit Architecture




Metasploit Exploit Module

The exploit module is the basic module in Metasploit used to encapsulate an exploit using which users target many platforms with a single exploit. This module comes with **simplified meta-information fields**. **Using a Mixins feature**, users can also modify exploit behavior dynamically, perform brute force attacks, and attempt passive exploits.


Following are the steps to exploit a system using the Metasploit framework:

- Configuring Active Exploit
- Verifying the Exploit Options
- Selecting a Target
- Selecting the Payload
- Launching the Exploit


Metasploit Payload Module



- Payload module establishes a **communication channel** between the Metasploit framework and the victim host
- It combines the **arbitrary code** that is executed as the result of an exploit succeeding
- To generate **payloads**, first select a payload using the command:



```
msf > use windows/shell_reverse_tcp
msf payload(shell_reverse_tcp) > generate -h
Usage: generate [options]
Generates a payload.
OPTIONS:
-b <opt> The list of characters to avoid: '\x00\xff'
-e <opt> The name of the encoder module to use.
-h Help banner.
-o <opt> A comma separated list of options in
VAR=VAL format.
-s <opt> NOP sled length.
-t <opt> The output type: ruby, perl, c, or raw.
msf payload(shell_reverse_tcp) >
```



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

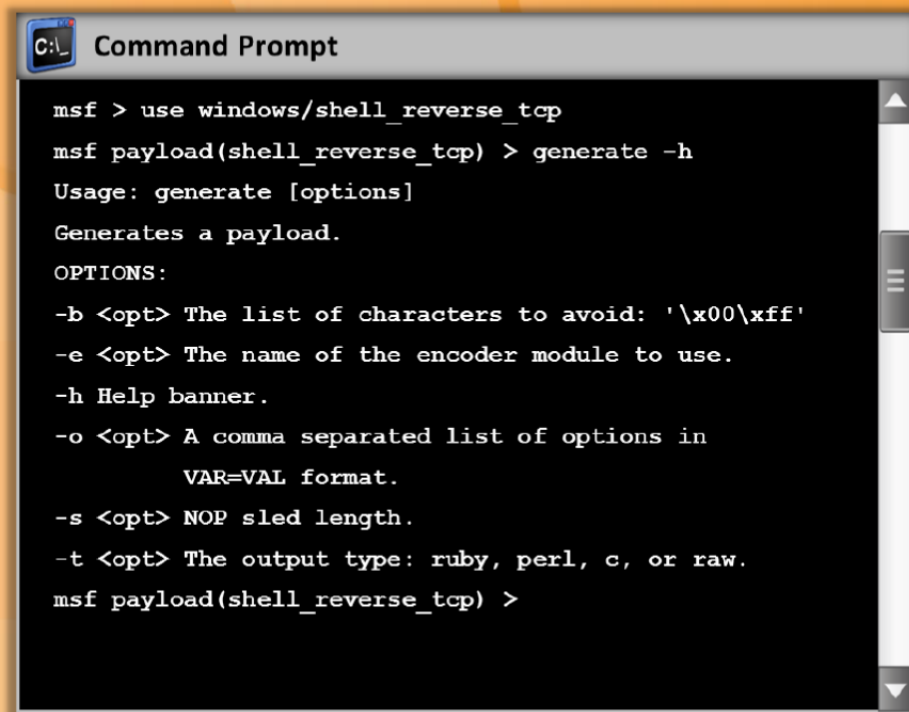


Metasploit Payload Module

The Metasploit payload module offers shellcode that can perform a number of interesting tasks for an attacker. A payload is a piece of software that lets you control a computer system after its been exploited. The **payload is typically attached to and delivered by the exploit**. An exploit carries the payload in its backpack when it break into the system and then leaves the backpack there.

With the help of payload, you can upload and download files from the system, take screenshots, and collect password hashes. You can even take over the screen, mouse, and keyboard to fully control the computer.

To generate payloads, first select a payload using the command:





```
C:\_ Command Prompt

msf > use windows/shell_reverse_tcp
msf payload(shell_reverse_tcp) > generate -h
Usage: generate [options]
Generates a payload.
OPTIONS:
-b <opt> The list of characters to avoid: '\x00\xff'
-e <opt> The name of the encoder module to use.
-h Help banner.
-o <opt> A comma separated list of options in
      VAR=VAL format.
-s <opt> NOP sled length.
-t <opt> The output type: ruby, perl, c, or raw.
msf payload(shell_reverse_tcp) >
```


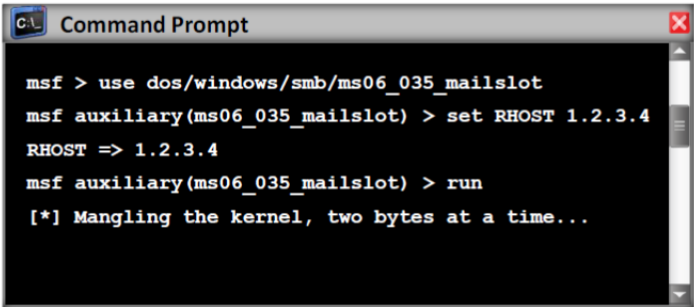
FIGURE 12.23: Metasploit Payload Module

Metasploit Auxiliary Module





- Metasploit's auxiliary modules can be **used to perform arbitrary**, one-off actions such as port scanning, denial of service, and even fuzzing
- To run auxiliary module, either use the **run** command, or use the **exploit** command

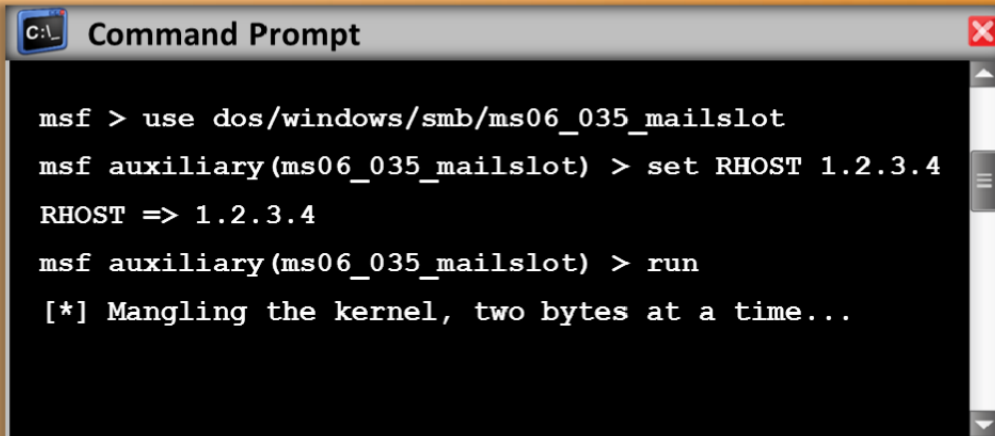


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Metasploit Auxiliary Module


Metasploit's auxiliary modules can be used to perform **arbitrary, one-off actions such as port scanning**, denial of service, and even fuzzing. To run auxiliary module, either use the **run** command or use the **exploit** command.



```
msf > use dos/windows/smb/ms06_035_mailslot
msf auxiliary(ms06_035_mailslot) > set RHOST 1.2.3.4
RHOST => 1.2.3.4
msf auxiliary(ms06_035_mailslot) > run
[*] Mangling the kernel, two bytes at a time...
```

FIGURE 12.24: Metasploit Auxiliary Module

Metasploit NOPS Module




- NOP modules generate a no-operation instructions used for blocking out buffers
- Use **generate** command to generate a NOP sled of an arbitrary size and display it in a given format

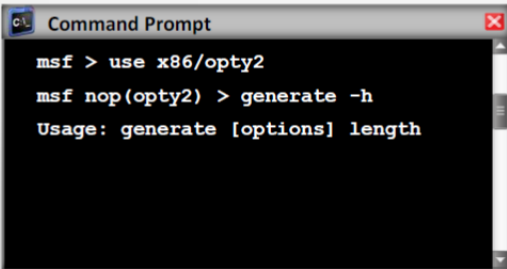
OPTIONS:

- b <opt>: The list of characters to avoid: '\x00\xff'
- h: Help banner.
- s <opt>: The comma separated list of registers to save.
- t <opt>: The output type: ruby, perl, c, or raw

msf nop (opt2) >

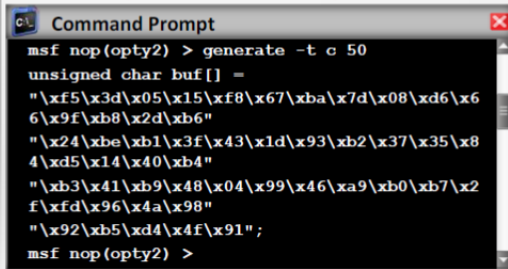


Generates a NOP sled of a given length



```
msf > use x86/opty2
msf nop(opty2) > generate -h
Usage: generate [options] length
```

To generate a 50 byte NOP sled that is displayed as a C-style buffer, run the following command:



```
msf nop(opty2) > generate -t c 50
unsigned char buf[] =
"\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x6
6\x9f\xb8\x2d\xb6"
"\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x8
4\xd5\x14\x40\xb4"
"\xb3\x41\xb9\x48\x04\x99\x46\xa9\xb0\xb7\x2
f\xfd\x96\x4a\x98"
"\x92\xb5\xd4\x4f\x91";
msf nop(opty2) >
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



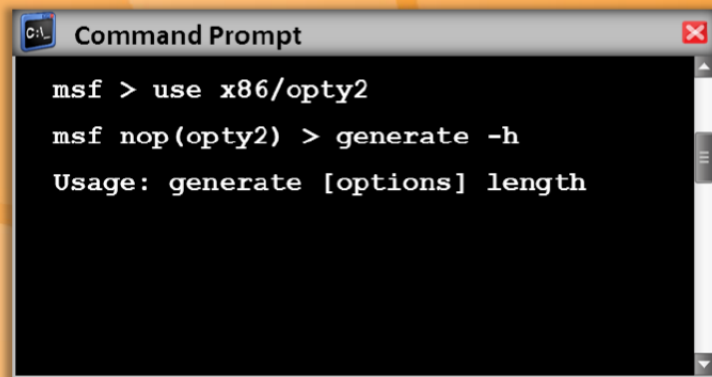
Metasploit NOPS Module

Metasploit NOP modules are used to generate no operation instructions that can be used for **padding out buffers**. The NOP module console interface supports generating a NOP sled of an arbitrary size and displaying it in a given format.

OPTIONS:

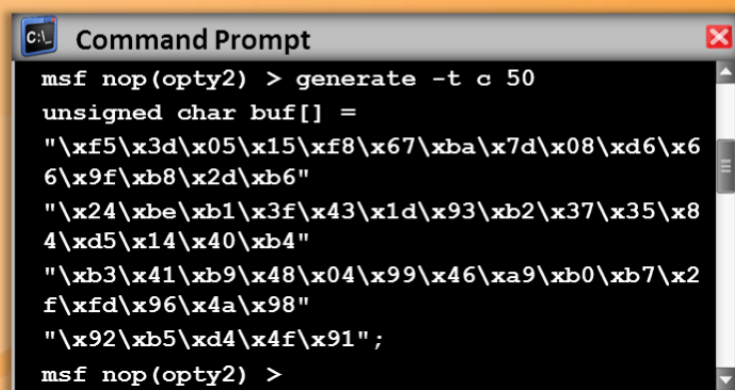
- b <opt> The list of characters to avoid: ?\x00\xff?
- h Help banner.
- s <opt> The comma separated list of registers to save.
- t <opt> The output type: ruby, perl, c, or raw.

Generates a NOP sled of a given length



```
msf > use x86/opty2
msf nop(opty2) > generate -h
Usage: generate [options] length
```

To generate a 50-byte NOP sled that is displayed as a C-style buffer, run the following command:



```
msf nop(opty2) > generate -t c 50
unsigned char buf[] =
"\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x6
6\x9f\xb8\x2d\xb6"
"\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x8
4\xd5\x14\x40\xb4"
"\xb3\x41\xb9\x48\x04\x99\x46\xa9\xb0\xb7\x2
f\xfd\x96\x4a\x98"
"\x92\xb5\xd4\x4f\x91";
msf nop(opty2) >
```

Figure 12.25: Metasploit NOPS Module

Webserver Attack Tools: Wfetch

CEH
Certified Ethical Hacker

- WFetch allows attacker to fully customize an **HTTP request** and send it to a Web server to see the raw HTTP request and response data
- It allows attacker to test the performance of Web sites that contain new elements such as **Active Server Pages (ASP)** or wireless protocols



<http://www.microsoft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Attack Tools: Wfetch

Source: <http://www.microsoft.com>

Wfetch is a **graphical user-interface** aimed at helping customers resolve problems related to the browser interaction with Microsoft's IIS web server. It allows a client to reproduce a problem with a lightweight, very **HTTP-friendly test environment**. It allows for very granular testing down to the authentication, authorization, custom headers, and much more.

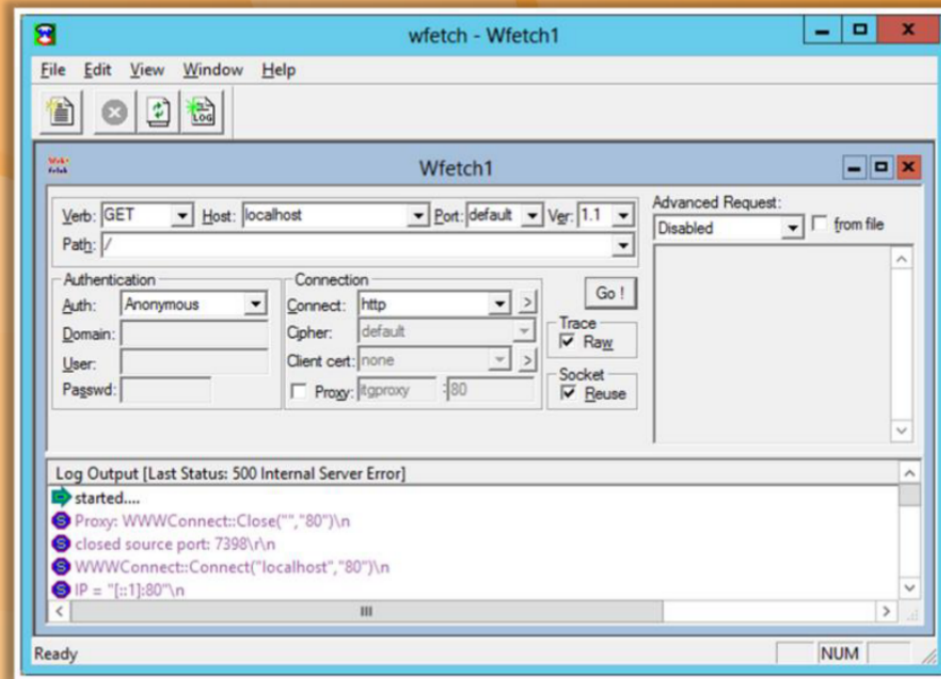




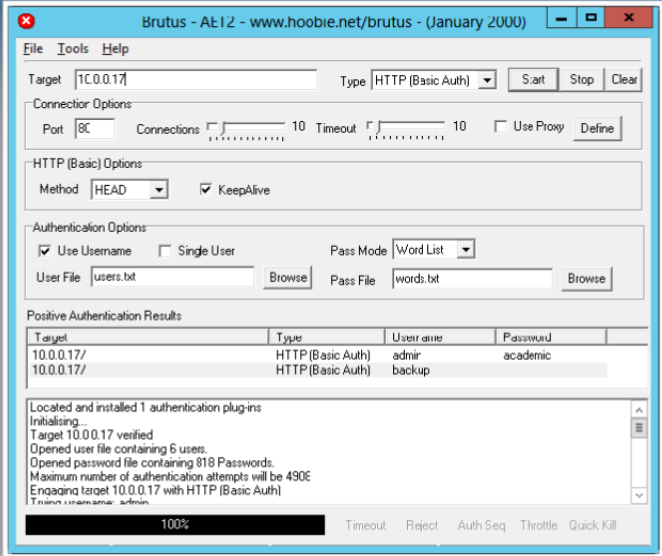
Figure 12.26: Wfetch Screenshot

Web Password Cracking Tool: Brutus



- Brutus supports HTTP, POP3, FTP, SMB, Telnet, IMAP, NNTP and many other authentication types
- It includes a multi-stage authentication engine and can **make 60 simultaneous target connections**
- It supports no user name, single user name, multiple user name, password list, combo (user/password) list and configurable brute force modes
- It includes **SOCKS proxy** support for all authentication types
- It also include user and password list generation and manipulation functionality





Brutus - At 12 - www.hoobie.net/brutus - (January 2000)

File Tools Help

Target: 10.0.0.17 Type: HTTP (Basic Auth) Start Stop Clear

Connector Options

Port: 80 Connections: 10 Timeout: 10 Use Proxy Define

HTTP (Basic) Options

Method: HEAD KeepAlive

Authentication Options

☒ Use Username ☐ Single User Pass Mode: Word List

User File: users.txt Browse Pass File: words.txt Browse

Positive Authentication Results

Target	Type	User name	Password
10.0.0.17/	HTTP (Basic Auth)	admin	academic
10.0.0.17/	HTTP (Basic Auth)	backup	

Located and installed 1 authentication plug-ins
Initialising...
Target 10.0.0.17 verified
Opened user file containing 6 users.
Opened password file containing 818 Passwords.
Maximum number of authentication attempts will be 4906
Engaging target 10.0.0.17 with HTTP (Basic Auth)
100%

Timeout Reject Auth Seq Throttle Quick Kill

<http://www.hoobie.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Password Cracking Tool: Brutus

Source: <http://www.hoobie.net>

Brutus is a **remote password cracker's** tool. It is available for Windows 9x, NT, and 2000, there is no UNIX version available, although it is a possibility at some point in the future. Brutus was written originally to help check routers for default and common passwords.

Features

- HTTP (Basic Authentication)
- HTTP (HTML Form/CGI)
- POP3
- FTP
- SMB
- Telnet
- Multi-stage authentication engine
- No user name, single user name, and multiple user name modes
- Password list, combo (user/password) list and configurable brute force modes

- Highly customizable authentication sequences
- Load and resume position
- Import and Export custom authentication types as BAD files seamlessly
- SOCKS proxy support for all authentication types
- User and password list generation and manipulation functionality
- HTML Form interpretation for HTML Form/CGI authentication types
- Error handling and recovery capability inc. resume after crash/failure

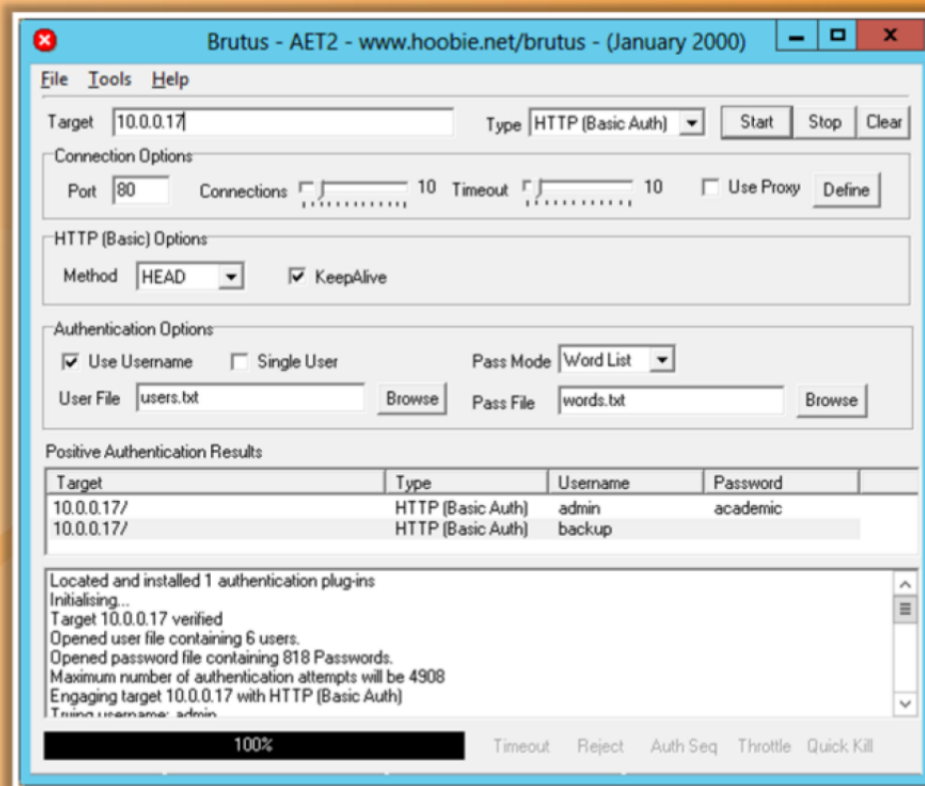




Figure 12.27: Brutus Screenshot

Web Password Cracking Tool: THC-Hydra



Certified Ethical Hacker

 A very fast network logon cracker that support many different services

xHydra

Target:

☒ Single Target

☐ Target List

☐ Prefer IPV6

Port:

Protocol:

Output Options

☒ Use SSL ☒ Be Verbose

☒ Show Attempts ☒ Debug

hydra -S -v -V -d -l Administrator -P /home/.../Desktop/pass -t 16 192.16...

xHydra

Output

Hydra v7.1 (c)2011 by van Hauser/THC & David Maciejak - for legal purposes d

Hydra (http://www.thc.org/thc-hydra) starting at 2012-10-21 17:01:09

[DEBUG] cmdline: /usr/bin/hydra -S -v -V -d -l Administrator -P /home/.../Des

[DATA] 4 tasks, 1 server, 4 login tries (l:1/p:4), ~1 try per task

[DATA] attacking service rdp on port 3389

[VERBOSE] Resolving addresses ...

[DEBUG] resolving 192.168.168.1

done

[DEBUG] Code: attack Time: 1350819069

[DEBUG] Options: mode 1 ssl 1 restore 0 showAttempt 1 tasks 4 max_use <

[DEBUG] Brains: active 0 targets 1 finished 0 todo_all 4 todo 4 sept 0 Found

[DEBUG] Target 0 - target 192.168.168.1 ip 192.168.168.1 login_no <pass_no

[DEBUG] Task 0 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_

[DEBUG] Task 1 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_

[DEBUG] Task 2 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_

[DEBUG] Task 3 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass_

[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to r

[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to

[DEBUG] head_no[0] active 0

[DEBUG] child 0 got target 0 selected

[DEBUG] head_no[1] active 0

[DEBUG] child 1 got target 0 selected

Start Stop Save Output Clear Output

hydra -S -v -V -d -l Administrator -P /home/.../Desktop/pass -t 16 192.16...

<http://www.thc.org>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Password Cracking Tool: THC-Hydra

Source: <http://www.thc.org>

THC-Hydra is used to check for weak passwords. This tool is a brute force tool that is used by attackers as well as administrators. Hydra can **automatically crack email passwords and gain access to routers**, Windows systems, and telnet or SSH protected servers. It is a very fast network logon cracker that supports many different services.

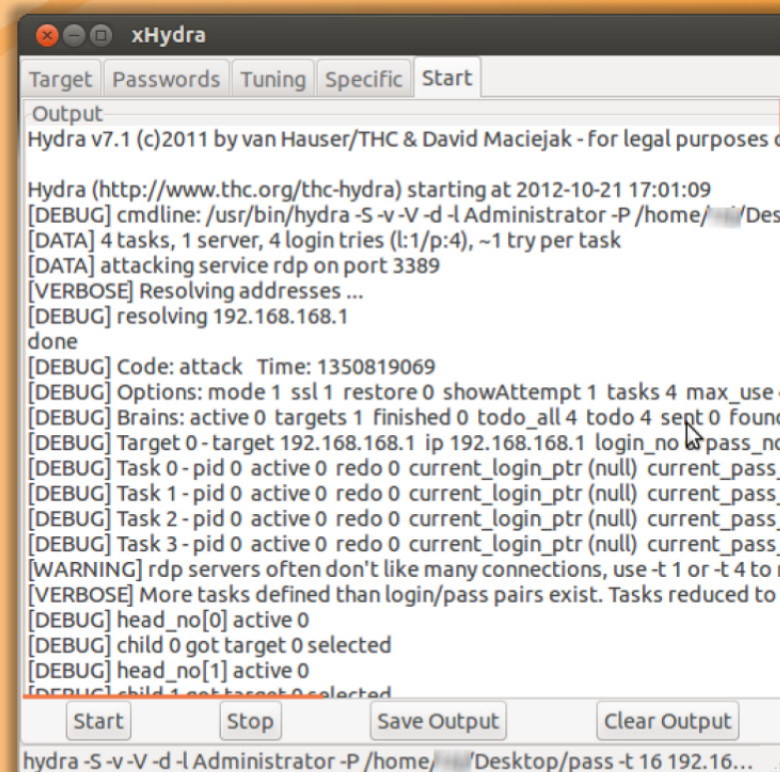
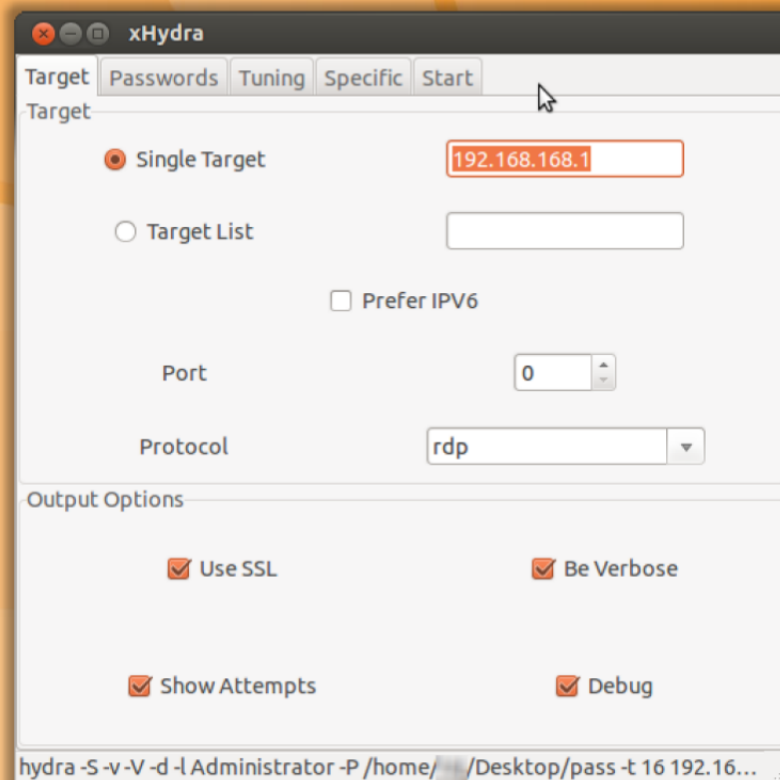


Figure 12.28: THC-Hydra Screenshot



Web Password Cracking Tool: Internet Password Recovery Toolbox

Source: <http://www.rixler.com>

Internet Password Recovery Toolbox is a comprehensive solution for recovering passwords for Internet browsers, email clients, instant messengers, and FTP clients. It can cover **network and dial-up accounts and can be used in the whole area of Internet communication links**. This program offers instantaneous password recovery capabilities for almost every Internet application you expect it to provide: you name it, the program has it.

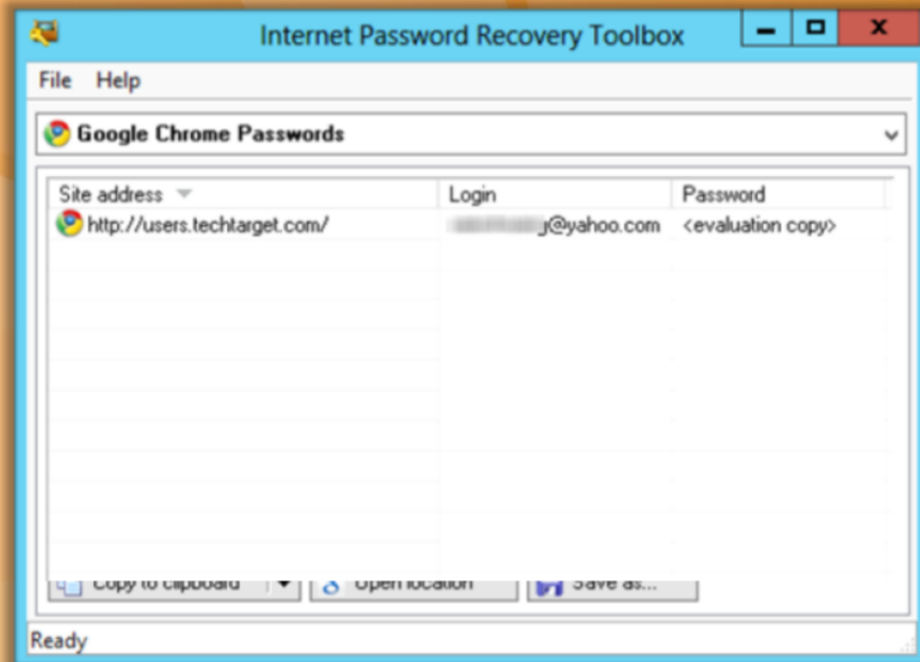
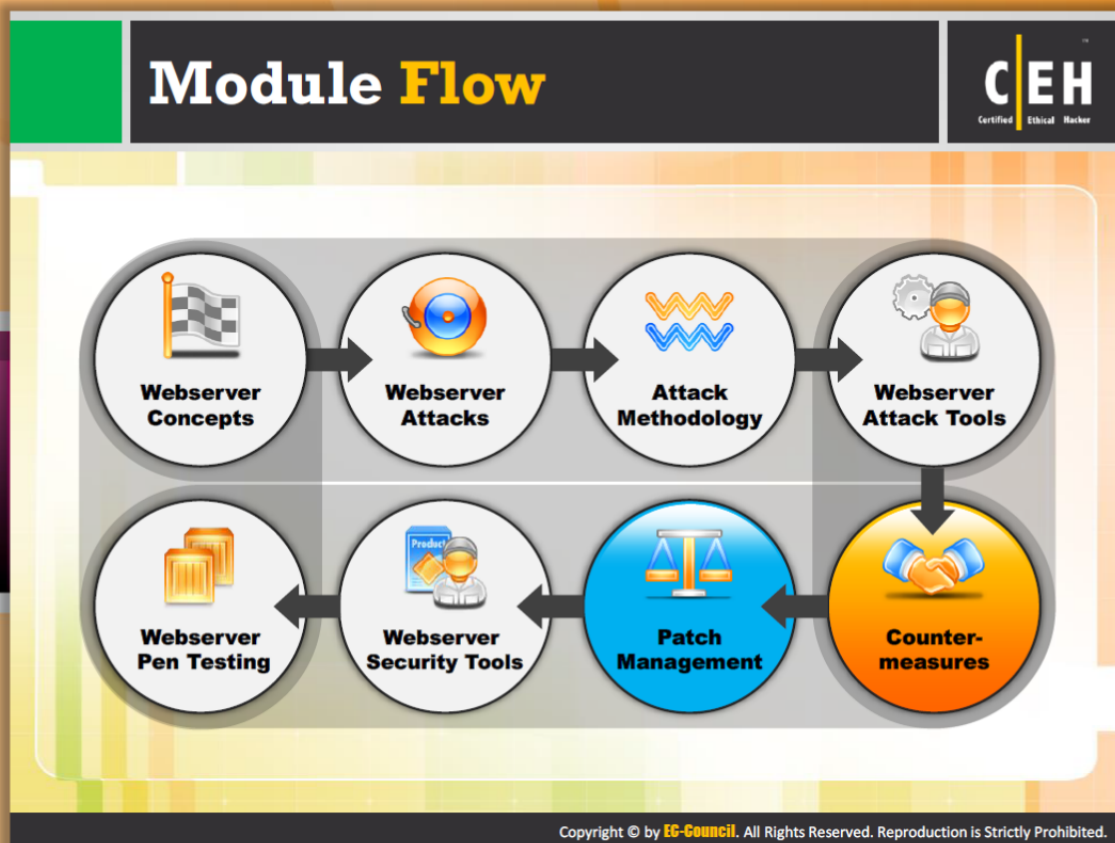


Figure 12.29: Internet Password Recovery Toolbox




Module Flow









So far, we have discussed web server concepts, techniques used by attackers, attack methodology, and tools that help in web server. All these concepts help in breaking into the web server or compromising web server security. Now it's time to discuss the countermeasures that help in enhancing the security of web servers. **Countermeasures are the practice of using multiple security systems or technologies to prevent intrusions.** These are the key components for protecting and safeguarding the web server against web server intrusions.

 Webserver Concepts	 Webserver Attacks
 Attack Methodology	 Webserver Attack Tools
 Webserver Pen Testing	 Webserver Security Tools
 Patch Management	 Counter-measures

This section highlights web server countermeasures that protect web servers against various attacks.

Countermeasures: Patches and Updates



 <p>Scan for existing vulnerabilities, patch, and update the server software regularly</p>	 <p>Before applying any service pack, hotfix, or security patch, read and peer review all relevant documentation</p>
 <p>Apply all updates, regardless of their type on an "as-needed" basis</p>	 <p>Test the service packs and hotfixes on a representative non-production environment prior to being deployed to production</p>
 <p>Ensure that service packs, hotfixes, and security patch levels are consistent on all Domain Controllers (DCs)</p>	 <p>Ensure that server outages are scheduled and a complete set of backup tapes and emergency repair disks are available</p>
 <p>Have a back-out plan that allows the system and enterprise to return to their original state, prior to the failed implementation</p>	 <p>Schedule periodic service pack upgrades as part of operations maintenance and never try to have more than two service packs behind</p>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.









Countermeasures: Patches and Updates

The following are a few countermeasures that can be **adopted to protect web servers against various hacking** techniques:

- Scan for existing vulnerabilities and patch and update the server software regularly.
- Apply all updates, regardless of their type, on an "as-needed" basis.
- Ensure that service packs, hotfixes, and security patch levels are consistent on all Domain Controllers (DCs). Ensure that server outages are scheduled and a complete set of backup tapes and emergency repair disks are available.
- Have a back-out plan that allows the system and enterprise to return to their original state, prior to the failed implementation.
- Before applying any service pack, hotfix, or security patch, read and peer review all relevant documentation.
- Test the service packs and hotfixes on a representative non-production environment prior to being deployed to production.
- Ensure that server outages are scheduled and a complete set of backup tapes and emergency repair disks are available.
- Schedule periodic service pack upgrades as part of operations maintenance and never try to have more than two service packs behind.

Countermeasures: Protocols



-  Block all unnecessary **ports**, **Internet Control Message Protocol (ICMP) traffic**, and unnecessary protocols such as **NetBIOS** and **SMB**
-  Harden the **TCP/IP stack** and consistently apply the **latest software patches and updates** to system software
-  If using **insecure protocols** such as **Telnet**, **POP3**, **SMTP**, **FTP**, take appropriate measures to provide secure authentication and communication, for example, by using **IPSec policies**
-  If remote access is needed, make sure that the remote connection is secured properly, by using **tunneling and encryption protocols**
-  Disable **WebDAV** if not used by the application or keep secure if it is required

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.











Countermeasures: Protocols

The following are the some measures that should be applied to the respective protocols in order to protect web servers from hacking:

- Block all unnecessary ports, Internet Control Message Protocol (ICMP) traffic, and unnecessary protocols such as NetBIOS and SMB.
- Harden the TCP/IP stack and consistently apply the latest software patches and updates to the system software.
- If using insecure protocols such as Telnet, POP3, SMTP, or FTP, take appropriate measures to provide secure authentication and communication, for example, by using IPSec policies.
- If remote access is needed, make sure that the remote connection is secured properly, by using tunneling and encryption protocols.
- Disable WebDAV if not used by the application or keep secure if it is required.

Countermeasures: **Accounts**



	Remove all unused modules and application extensions	✓
	Disable unused default user accounts created during installation of an operating system	✓
	When creating a new web root directory, grant the appropriate (least possible) NTFS permissions to the anonymous user being used from the IIS web server to access the web content	✓
	Eliminate unnecessary database users and stored procedures and follow the principle of least privilege for the database application to defend against SQL query poisoning	✓
	Use secure web permissions, NTFS permissions, and .NET Framework access control mechanisms including URL authorization	✓
	Slow down brute force and dictionary attacks with strong password policies, and then audit and alert for logon failures	✓
	Run processes using least privileged accounts as well as least privileged service and user accounts	✓

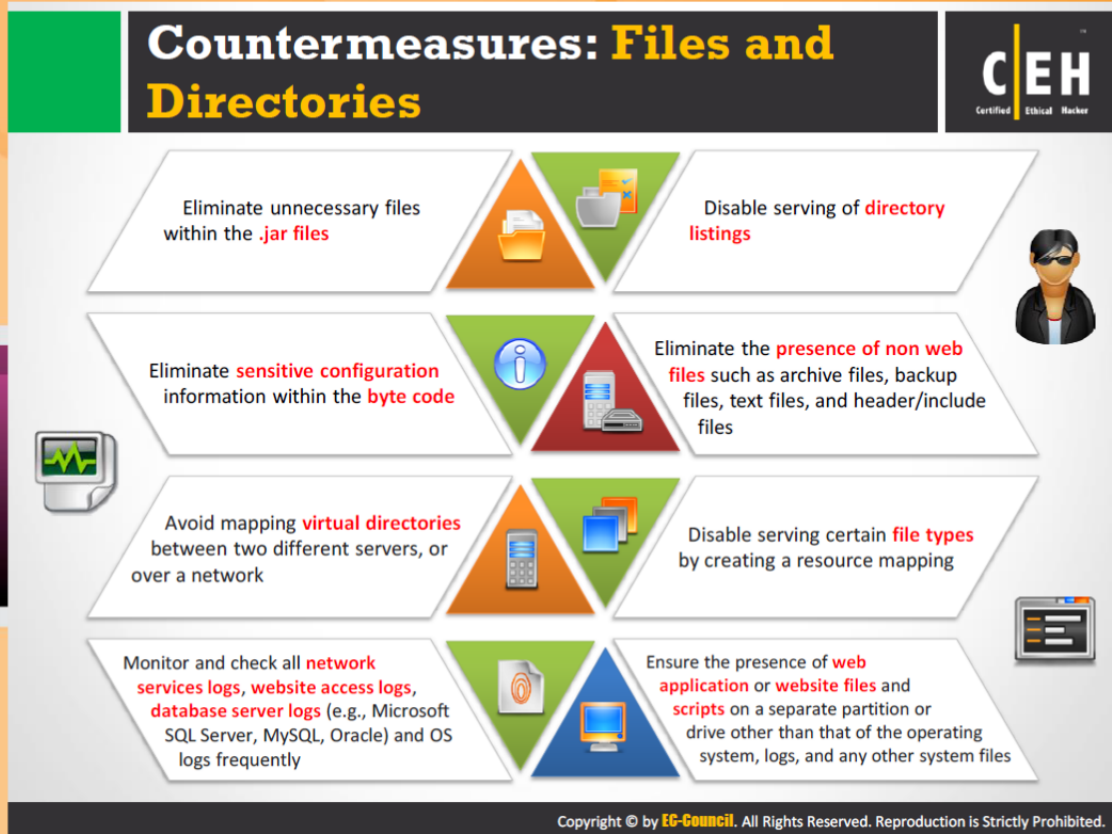
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Countermeasures: Accounts

The following is the list of account countermeasures for hacking web servers:

- Remove all unused modules and application extensions.
- Disable unused default user accounts created during installation of an operating system.
- When creating a new web root directory, grant the appropriate (least possible) NTFS permissions to the anonymous user being used from the IIS web server to access the web content.
- Eliminate unnecessary database users and stored procedures and follow the principle of least privilege for the database application to defend against SQL query poisoning.
- Use secure web permissions, NTFS permissions, and .NET Framework access control mechanisms including URL authorization.
- Slow down brute force and dictionary attacks with strong password policies, and then audit and alert for logon failures.
- Run processes using least privileged accounts as well as least privileged service and user accounts.







Countermeasures: Files and Directories

The following is the list of actions that should be taken against files and directories in order to protect web servers from hacking:

- **Eliminate unnecessary files within .jar files.**
- Eliminate sensitive configuration information within the byte code.
- Avoid mapping virtual directories between two different servers or over a network.
- Monitor and check all network services logs, website access logs, database server logs (e.g., Microsoft SQL Server, MySQL, Oracle), and OS logs frequently.
- Disable serving of directory listings.
- Eliminate the presence of non-web files such as archive files, backup files, text files, and header/include files.
- Disable serving certain file types by creating a resource mapping
- Ensure the presence of web application or website files and scripts on a separate partition or drive other than that of the operating system, logs, and any other system files

How to Defend Against Web Server Attacks



 Ports	<ul style="list-style-type: none">Audit the ports on server regularly to ensure that an insecure or unnecessary service is not active on your web serverLimit inbound traffic to port 80 for HTTP and port 443 for HTTPS (SSL)Encrypt or restrict intranet traffic
 Server Certificates	<ul style="list-style-type: none">Ensure that certificate data ranges are valid and that certificates are used for their intended purposeEnsure that the certificate has not been revoked and certificate's public key is valid all the way to a trusted root authority
 Machine.config	<ul style="list-style-type: none">Ensure that protected resources are mapped to HttpForbiddenHandler and unused HttpModules are removedEnsure that tracing is disabled <code><trace enable="false"/></code> and debug compiles are turned off
 Code Access Security	<ul style="list-style-type: none">Implement secure coding practices to avoid source code disclosure and input validation attackRestrict code access security policy settings to ensure that code downloaded from the Internet or Intranet have no permissions to executeConfigure IIS to reject URLs with <code>"../"</code> to prevent path traversal, lock down system commands and utilities with restrictive access control lists (ACLs), and install new patches and updates

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Web Server Attacks

The following are the various ways to defend against web server attacks:



Ports

- Audit the ports on the server regularly to ensure that an insecure or unnecessary service is not active on your web server.
- Limit inbound traffic to port 80 for HTTP and port 443 for HTTPS (SSL).
- Encrypt or restrict intranet traffic.



Server Certificates

- Ensure that certificate data ranges are valid and that certificates are used for their intended purpose.
- Ensure that the certificate has not been revoked and certificate's public key is valid all the way to a trusted root authority.



Machine.config


- Ensure that protected resources are mapped to HttpForbiddenHandler and unused HttpModules are removed.
- Ensure that tracing is disabled `<trace enable="false"/>` and debug compiles are turned off.



Code Access Security

- Implement secure coding practices to avoid source code disclosure and input validation attack.
- **Restrict code access security policy** settings to ensure that code downloaded from the Internet or intranet has no permissions to execute.
- Configure IIS to reject URLs with "../" to prevent path traversal, lock down system commands and utilities with restrictive access control lists (ACLs), and install new patches and updates.

How to Defend Against Web Server Attacks (Cont'd)




IISLockdown

- Use the IISLockdown tool, which reduces the vulnerability of a **Windows 2000 Web server**. It allows you to pick a specific type of server role, and then use custom templates to improve security for that particular server
- IISLockdown installs the **URLScan ISAPI** filter allowing website administrators to restrict the kind of **HTTP requests** that the server can process, based on a set of rules the administrator controls, preventing potentially **harmful requests** from reaching the server and causing damage

Services

- Disable the services running with **least-privileged** accounts
- Disable **FTP, SMTP, and NNTP** services if not required
- Disable the **Telnet** service
- Switch off** all unnecessary services and disable them, so that next time when the server is rebooted, they are **not started** automatically. This also gives an extra boost to your **server performances**, by freeing some hardware resources



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Web Server Attacks (Cont'd)

IISLockdown

- IISLockdown restricts anonymous access to system utilities, as well as having the ability to write to web content directories. To do this, IISLockdown creates two new local groups called web anonymous users and web applications, and then it adds deny access **control entries (ACEs) for these groups to the access control list (ACL)** on key utilities and directories. Next, IISLockdown adds the default anonymous Internet user account (IUSR_MACHINE) to Web Anonymous Users and the IWAM_MACHINE account to Web Applications. It disables Web Distributed Authoring and Versioning (WebDav) and installs the **URLScan ISAPI filter**.
- Use the IISLockdown tool, which reduces the vulnerability of a Windows 2000 web server. It allows you to pick a specific type of server role, and then use custom templates to improve security for that particular server.
- IISLockdown installs the URLScan ISAPI filter, allowing website administrators to restrict the kind of HTTP requests that the server can process, based on a set of rules the administrator controls, preventing potentially harmful requests from reaching the server and causing damage.

Services

- Disable the services running with least-privileged accounts.
- Disable **FTP, SMTP, and NNTP** services if not required.
- Disable Telnet service.
- Switch off all unnecessary services and disable them, so that the next time the server is rebooted, they are not started automatically. This also gives an extra boost to your server performance, by freeing some hardware resources.



How to Defend Against Web Server Attacks (Cont'd)

- **Registry**
 - Apply **restricted ACLs** and block remote registry administration.
 - Secure the SAM (Stand-alone Servers Only).
- **Share**
 - Remove all unnecessary file shares including the default administration shares if they are not required.
 - Secure the shares with restricted NTFS permissions.
- **IIS Metabase**
 - Ensure that security-related settings are configured appropriately and access to the metabase file is restricted with hardened NTFS permissions.
 - Restrict banner information returned by IIS.
- **Auditing and Logging**
 - Enable a minimum level of auditing on your web server and use **NTFS permissions** to protect the log files.

- **Script Mappings**
 - Remove all unnecessary IIS script mappings for optional file extensions to avoid exploiting any bugs in the ISAPI extensions that handle these types of file.
- **Sites and Virtual Directories**
 - Relocate sites and virtual directories to non-system partitions and use IIS Web permissions to restrict access.
- **ISAPI Filters**
 - Remove unnecessary ISAPI filters from the web server.

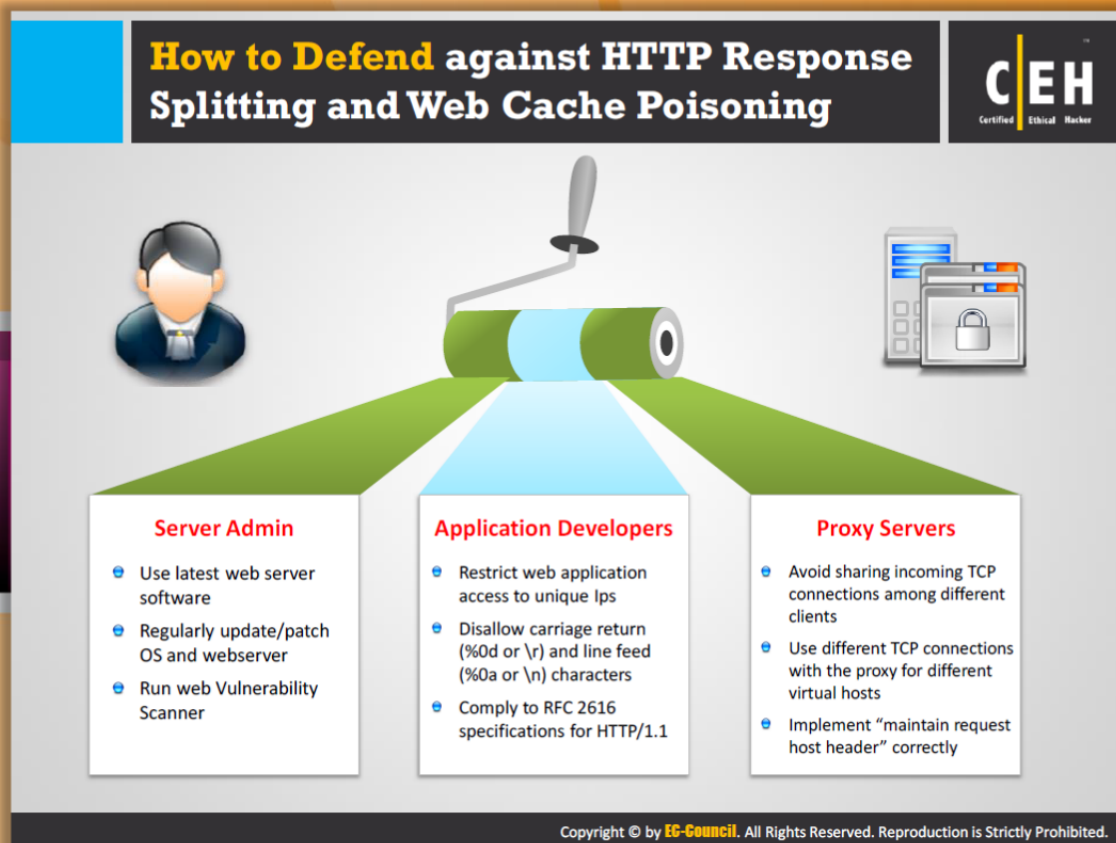


How to Defend Against Web Server Attacks (Cont'd)

The following is a list of actions that can be taken to defend web servers from various kinds of attacks:

- **Create URL mappings** to internal servers cautiously.
- If a database server such as Microsoft SQL Server is to be used as a backend database, install it on a separate server.
- Do use a dedicated machine as a web server.
- Don't install the IIS server on a domain controller.
- Use server-side session ID tracking and match connection with time stamps, IP address, etc.
- Use security tools provided with the **web server and scanners** that automate and make the process of securing a web server easy.
- Screen and filter the incoming traffic request.
- Do physically protect the web server machine in a secure machine room.
- Do configure a separate anonymous user account for each application, if you host multiple web applications.

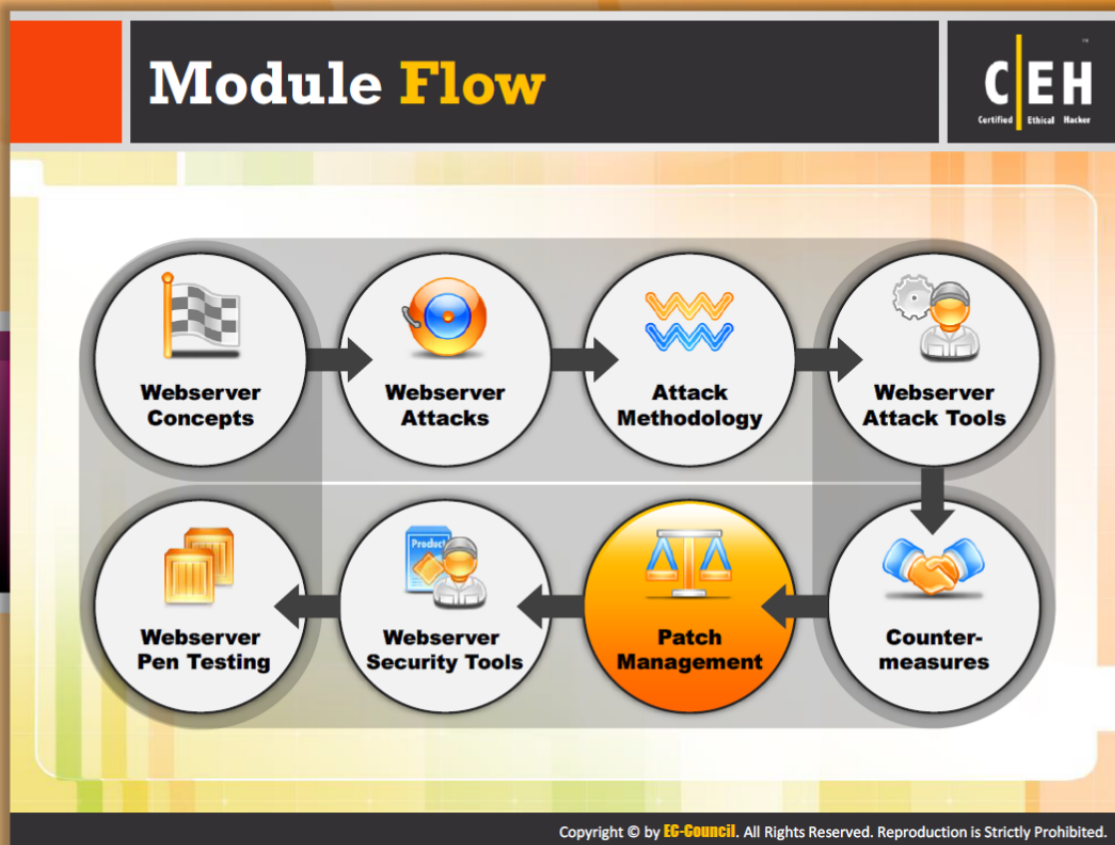
- Do not connect an IIS Server to the Internet until it is fully hardened.
- Do not allow anyone to locally log on to the machine except for the administrator.
- Limit the server functionality in order to support the **web technologies** that are going to be used.



How to Defend against HTTP Response Splitting and Web Cache Poisoning

The following are the measures that should be taken in order to defend against HTTP response splitting and web cache poisoning:

- **Server Admin**
 - Use latest web server software
 - Regularly update/patch OS and web server
 - Run web vulnerability scanner
- **Application Developers**
 - Restrict web application access to unique IPS
 - Disallow carriage return (%0d or \r) and line feed (%0a or \n) characters
 - Comply to RFC 2616 specifications for HTTP/1.1
- **Proxy Servers**
 - Avoid sharing incoming TCP connections among different clients
 - Use different TCP connections with the proxy for different virtual hosts
 - Implement "maintain request host header" correctly

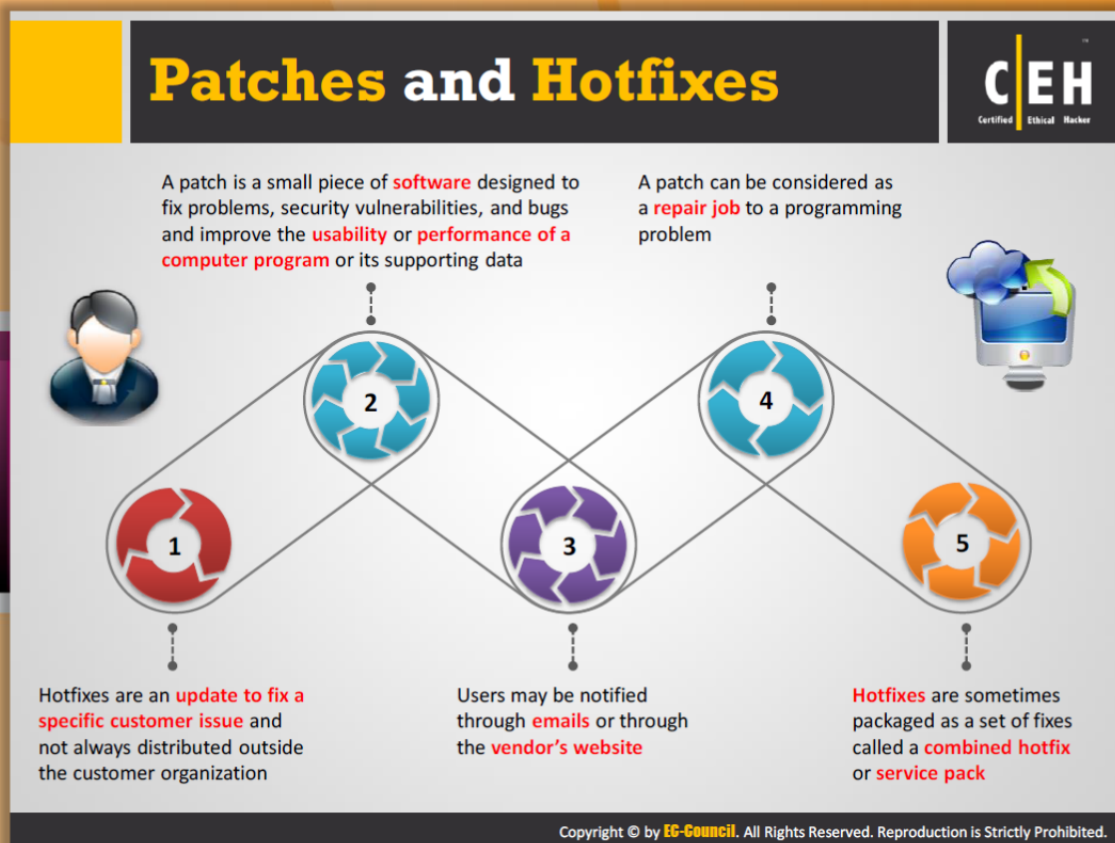


Module Flow

Developers always try to find the bugs in the web server and try to fix them. The bug fixes are released in the form of patches. These patches provide protection against known vulnerabilities. Patch management is a process used to ensure that the appropriate patches are installed on a system and help fix known vulnerabilities.

 Webserver Concepts	 Webserver Attacks
 Attack Methodology	 Webserver Attack Tools
 Webserver Pen Testing	 Webserver Security Tools
 Patch Management	 Counter-measures

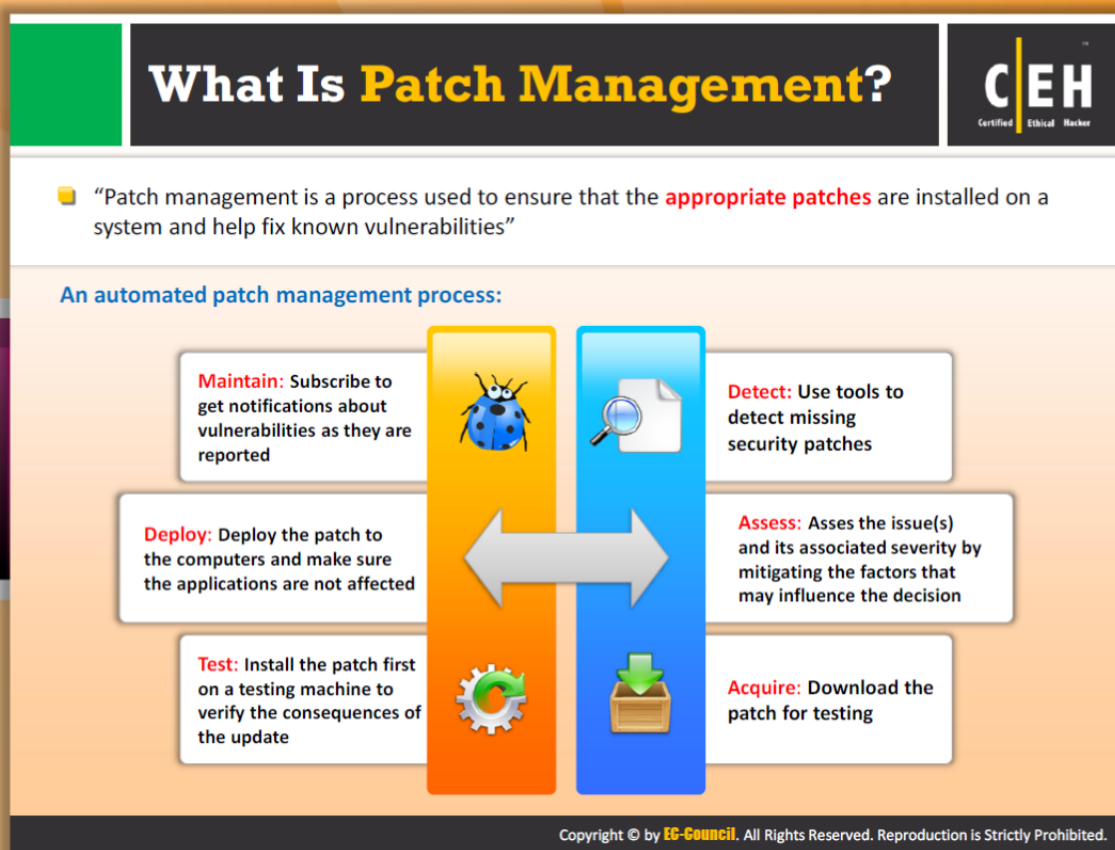
This section describes patch management concepts used to fix vulnerabilities and bugs in the web servers in order to protect them from attacks.



Patches and Hotfixes

A patch is a program used to make changes in the software installed on a computer. Patches are used to fix bugs, to address the security problems, to add functionality, etc. A patch is a **small piece of software designed to fix problems**, security vulnerabilities, and bugs and improve the usability or performance of a computer program or its supporting data. A patch can be considered a repair job to a programming problem.

A hotfix is a package that includes various files used specifically to address various problems of software. Hotfixes are used to fix bugs in a product. Users are updated about the latest hotfixes by vendors through email or they can be downloaded from the official website. **Hotfixes are an update to fix a specific customer issue and not always distributed outside the customer organization.** Users may be notified through emails or through the vendor's website. Hotfixes are sometimes packaged as a set of fixes called a combined hotfix or service pack.

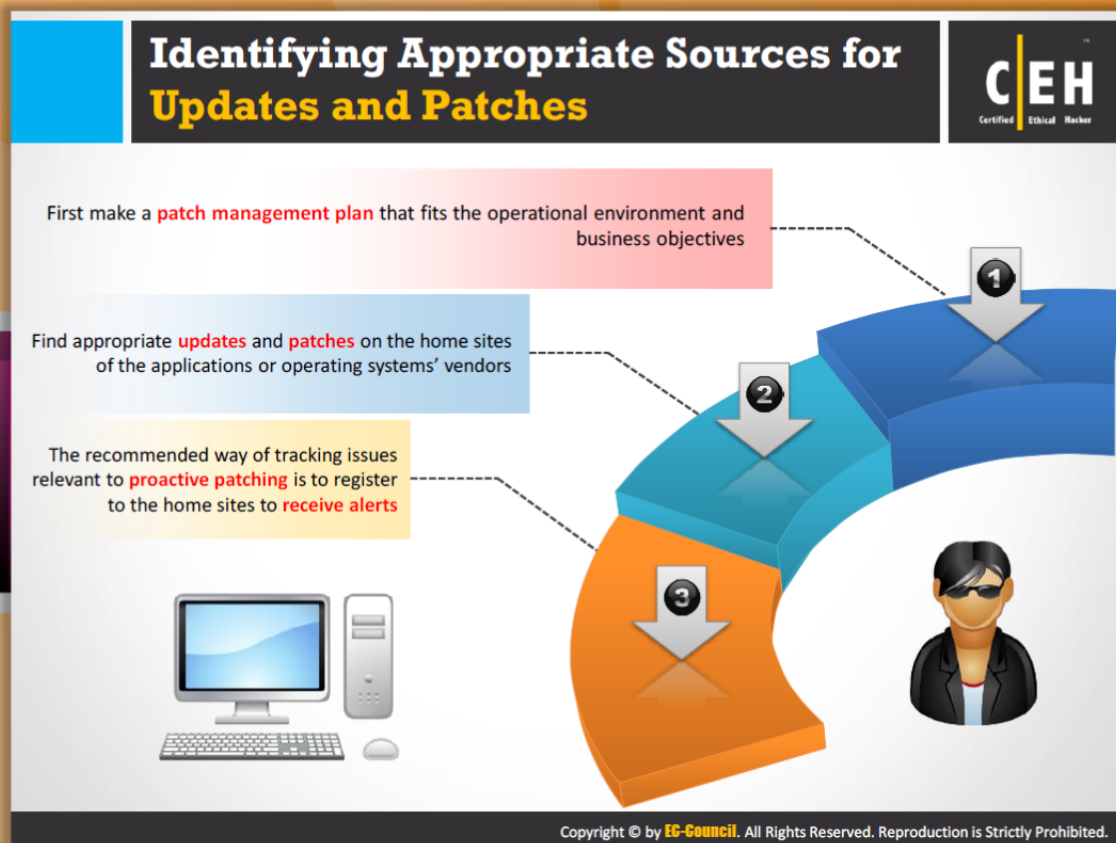


What Is Patch Management?

According to <http://searchenterprisedesktop.techtarget.com>, patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. It involves the following:

- Choosing, verifying, testing, and applying patches
 - Updating previously applied patches with current patches
 - Listing patches applied previously to the current software
 - Recording repositories, or depots, of patches for easy selection
 - Assigning and deploying the applied patches
1. **Detect:** It is very important to always detect **missing security patches** through proper detecting tools. If there is any delay in the detection process, chances of malicious attacks are very high.
 2. **Assess:** Once the detection process is finished it is always better to **assess various issues and the associated factors** related to them and better to implement those strategies where issues can be drastically reduced or eliminated.
 3. **Acquire:** The suitable patch required to fix the issues has to be downloaded.

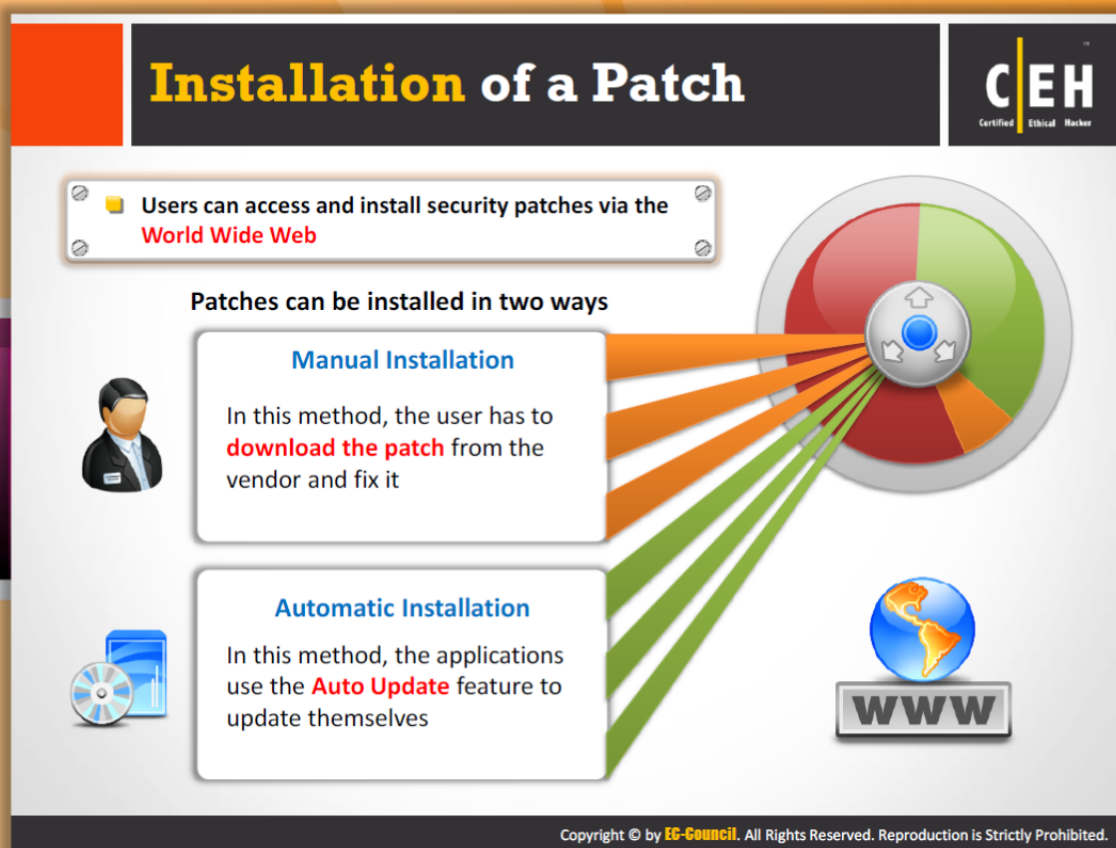
4. **Test:** It is always suggested to first install the required patch on to the testing system rather than the main system as this provides a chance to verify the various consequences of updating.
5. **Deploy:** Patches are to be deployed into the systems with utmost care, so no application of the system is affected.
6. **Maintain:** It is always useful to **subscribe to get notifications** about various possible vulnerabilities as they are reported.



Identifying Appropriate Sources for Updates and Patches

It is very important to identify the appropriate source for updates and patches. You should take care of the following things related to **patch management**.

- Patch management that suits the operational environment and business objectives should be properly planned.
- Find appropriate updates and patches on the home sites of the applications or operating systems' vendors.
- The recommended way of tracking issues relevant to **proactive patching** is to register to the home sites to receive alerts.



Installation of a Patch

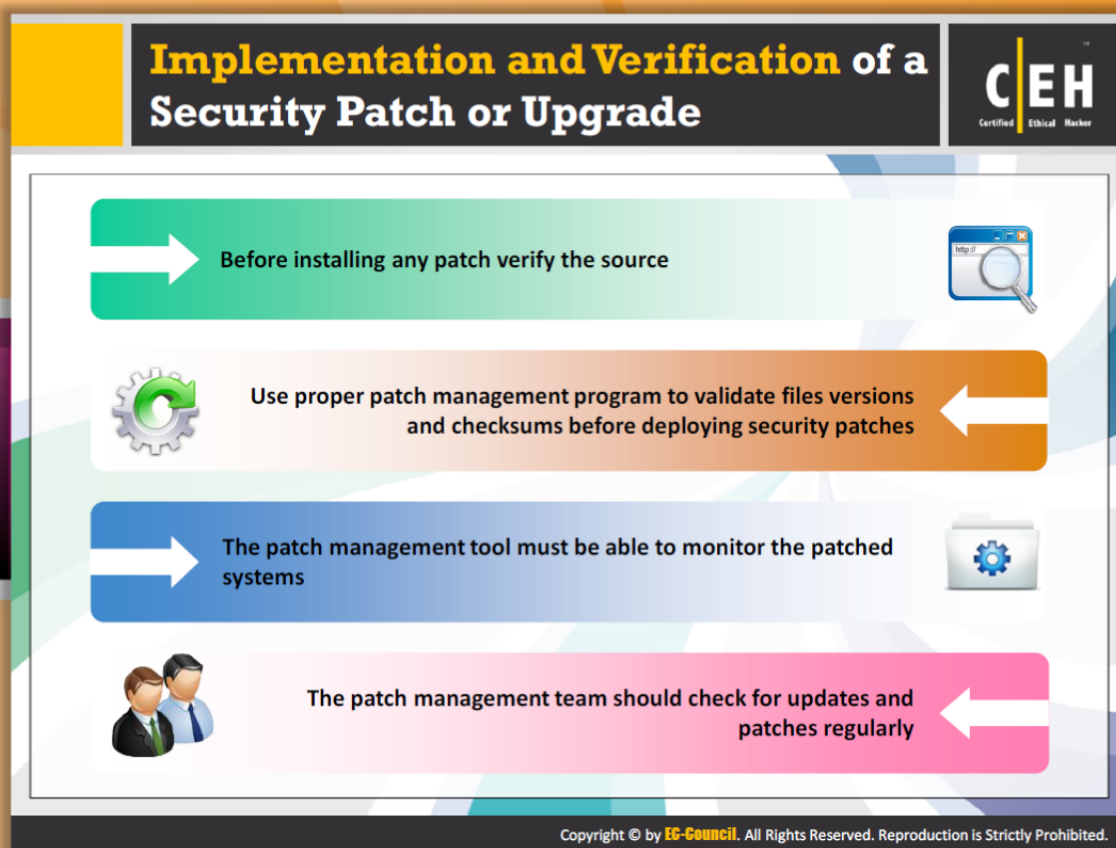
You should search for a suitable patch and install it from Internet. Patches can be installed in two ways:

Manual Installation

In the manual installation process, the user downloads the suitable patch from the vendor and fixes it.

Automatic Installation

In automatic installation, the applications, with the help of the auto update feature, will get updated automatically.



Implementation and Verification of a Security Patch or Upgrade

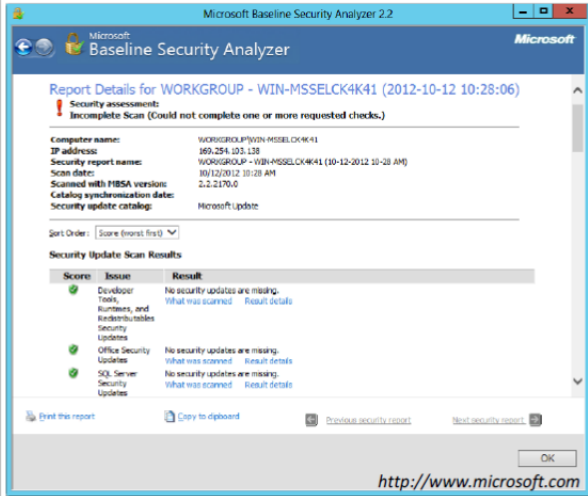

You should be aware of a few things before implementing a patch. The following things should be kept in mind:

- Before installing any patch source, it should be properly verified. Use a **proper patch management program** to validate file versions and checksums before deploying security patches.
- The patch management team should check for updates and patches regularly. A patch management tool must be able to monitor the patched systems.

Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)

Microsoft Baseline Security Analyzer (MBSA) checks for **available updates** to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server

It also scans a computer for insecure **configuration settings**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)

Source: <http://www.microsoft.com>

The Microsoft Baseline Security Analyzer (MBSA) allows you to identify missing security updates and common security misconfigurations. It is a tool designed for **the IT professional that helps small- and medium-sized businesses** determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Improve your security management process by using MBSA to detect common security misconfigurations and missing security updates on your computer systems.

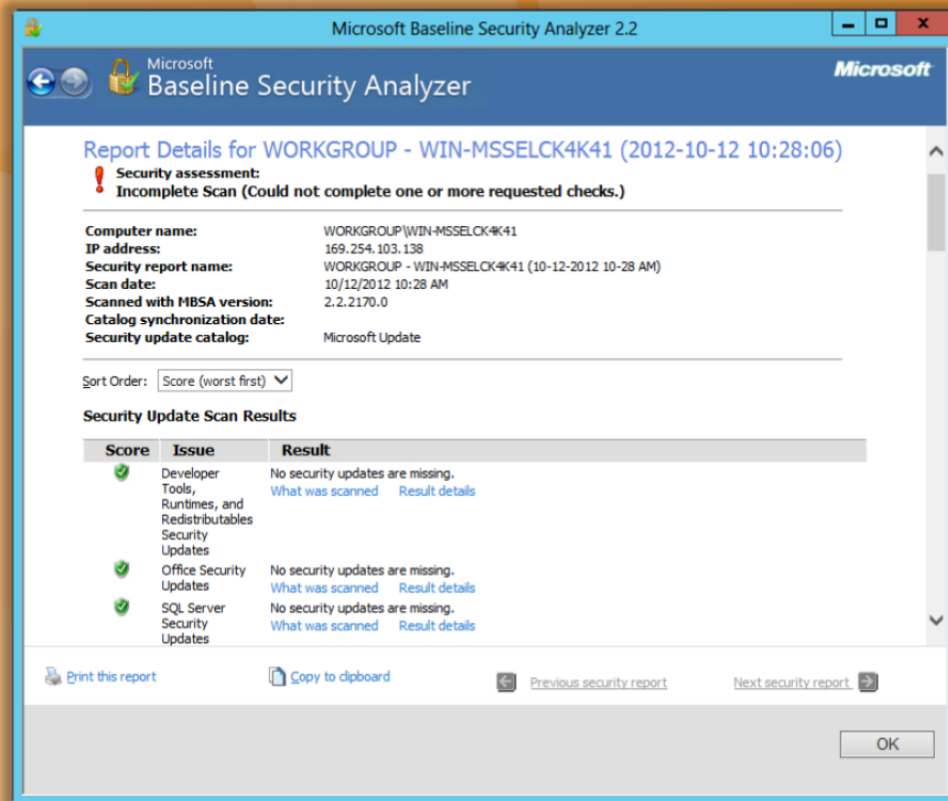


FIGURE 12.30: Microsoft Baseline Security Analyzer (MBSA)

Patch Management Tools



 Altiris Client Management Suite http://www.symantec.com	 Prism Patch Manager http://www.newboundary.com
 GFI LANguard http://www.gfi.com	 MaaS360® Patch Analyzer Tool http://www.maas360.com
 Kaseya Security Patch Management http://www.kaseya.com	 Secunia CSI http://secunia.com
 ZENworks® Patch Management http://www.novell.com	 Lumension® Patch and Remediation http://www.lumension.com
 Security Manager Plus http://www.manageengine.com	 VMware vCenter Protect http://www.vmware.com

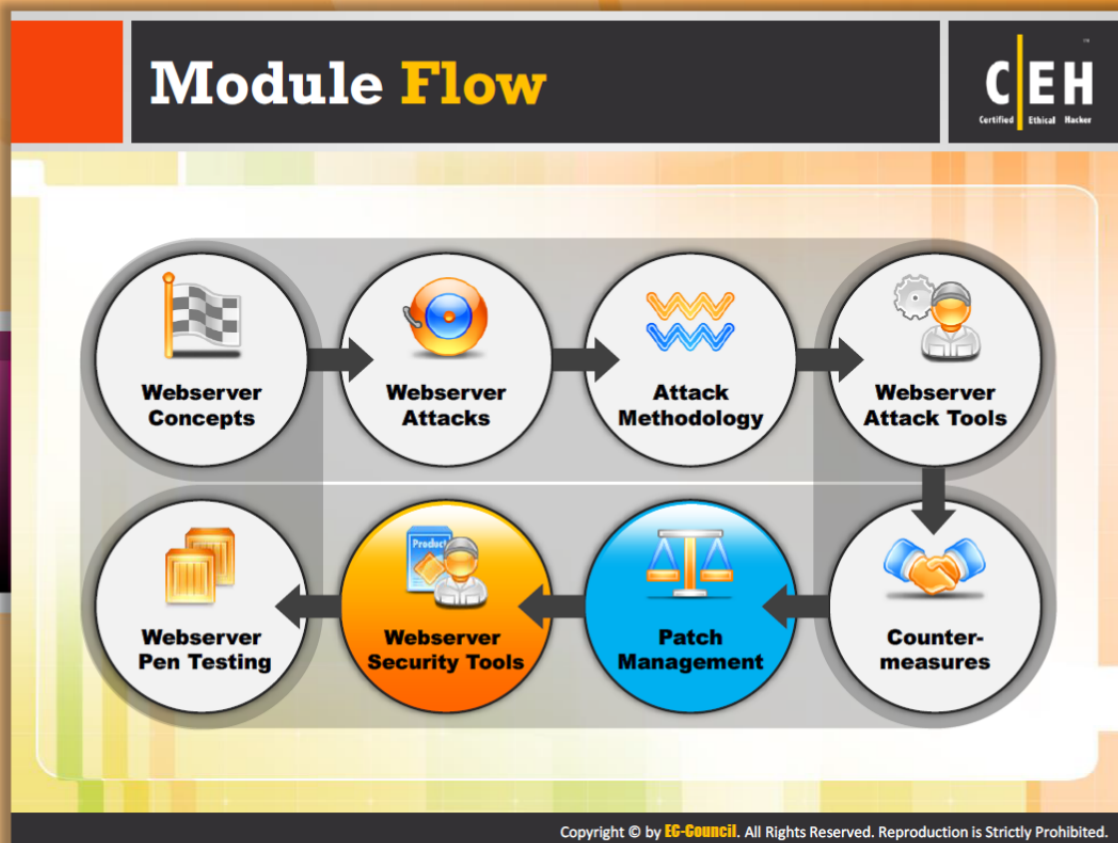
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Patch Management Tools

In addition to MBSA, there are many other tools that can be used for identifying missing patches, security updates, and common security misconfigurations. A **list of patch management tools** follows:

- Altiris Client Management Suite available at <http://www.symantec.com>
- GFI LANguard available at <http://www.gfi.com>
- Kaseya Security Patch Management available at <http://www.kaseya.com>
- ZENworks® Patch Management available at <http://www.novell.com>
- Security Manager Plus available at <http://www.manageengine.com>
- Prism Patch Manager available at <http://www.newboundary.com>
- MaaS360® Patch Analyzer Tool available at <http://www.maas360.com>
- Secunia CSI available at <http://secunia.com>
- Lumension® Patch and Remediation available at <http://www.lumension.com>
- VMware vCenter Protect available at <http://www.vmware.com>



Module Flow

Web servers should always be secured in the networked computing environment to avoid the threat of being attacked. Web server security can be monitored and managed with the help of web server security tools.

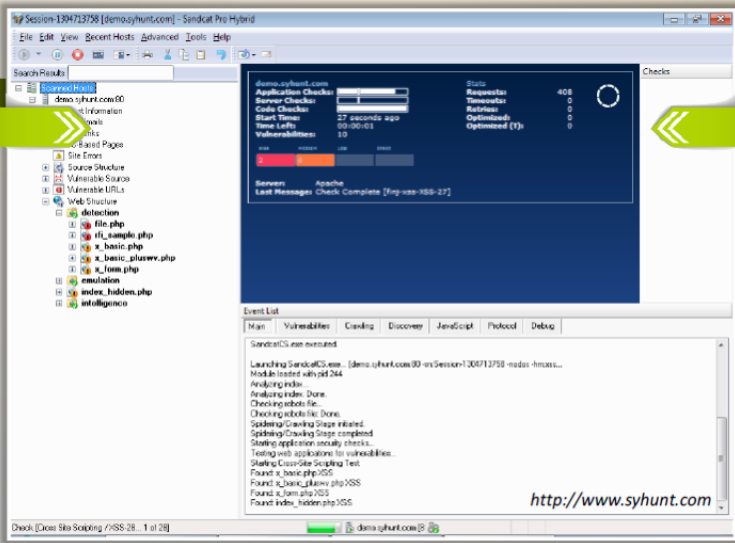
 Webserver Concepts	 Webserver Attacks
 Attack Methodology	 Webserver Attack Tools
 Webserver Pen Testing	 Webserver Security Tools
 Patch Management	 Counter-measures

This section lists and describes various web server security tools.

Web Application Security Scanner: Syhunt Dynamic



Syhunt Dynamic helps to automate **web application security** testing and guard organization's **web infrastructure** against various web application security threats



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Security Scanner: Syhunt Dynamic

Source: <http://www.syhunt.com>

Syhunt Dynamic helps to automate web application security testing and guard organization's web infrastructure against various web application security threats.

Features:

- Black-Box Testing - Assess the web application security through remote scanning. Supports any web server platform.
- White-Box Testing - By automating the process of reviewing the web application's code, Sandcat's code scanning functionality can make the life of QA testers easier, helping them quickly find and eliminate security vulnerabilities from web applications. Supports ASP, ASP.NET, and PHP.
- Concurrency/Scan Queue Support - **Multiple security scans can be queued and the number of threads** can be adjusted.
- Deep Crawling - Runs security tests against web pages discovered by crawling a single URL or a set of URLs provided by the user.
- Advanced Injection - Maps the entire website structure (all links, forms, XHR requests, and other entry points) and tries to find custom, unique vulnerabilities by simulating a

wide range of attacks/sending thousands of requests (mostly GET and POST). Tests for SQL Injection, XSS, File Inclusion, and many other web application vulnerability classes.

- Reporting - **Generates a report containing information about the vulnerabilities.** After examining the application's response to the attacks, if the target URL is found vulnerable, it gets added to the report. Sandcat's reports also contain charts, statistics and compliance information. Syhunt offers a set of report templates tailored for different audiences.
- Local or Remote Storage - Scan results are saved locally (on the disk) or remotely (in the Sandcat web server). Results can be converted at any time to HTML or multiple other available formats.
- In addition to its GUI (Graphical User Interface) functionalities, Syhunt offers an easy to use command-line interface.

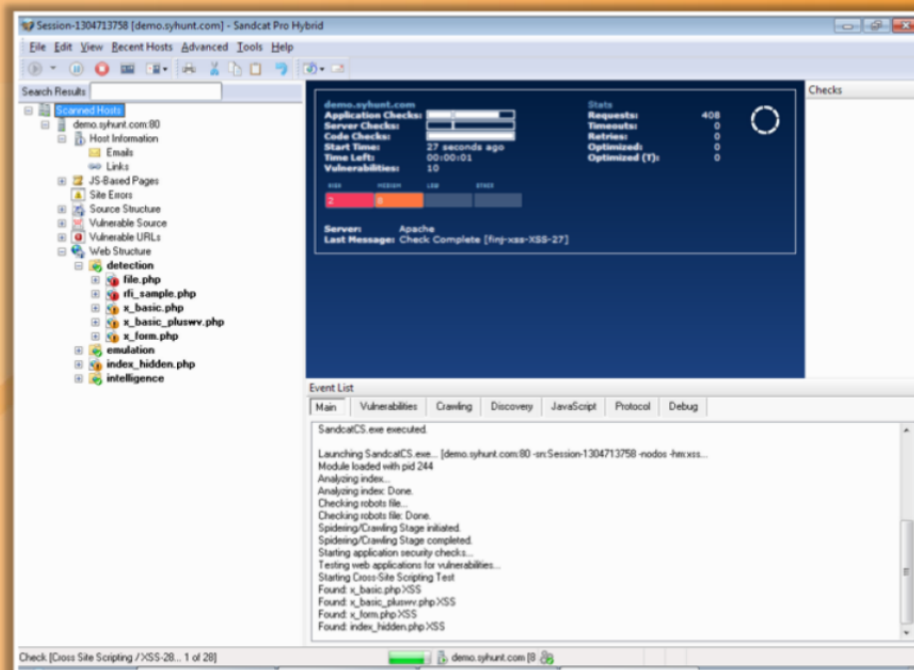


FIGURE 12.31: Syhunt Dynamic Screenshot

Web Application Security Scanner: N-Stalker Web Application Security Scanner



■ N-Stalker is a **WebApp Security Scanner** to search for vulnerabilities such as SQL injection, XSS, and known attacks



<http://www.nstalker.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Security Scanner: N-Stalker Web Application Security Scanner

Source: <http://www.nstalker.com>

N-Stalker Web Application Security Scanner is a web security assessment solution for your web applications. It is a security assessment tool that incorporates **N-stealth HTTP security scanner**. It searches for vulnerabilities such as SQL injection, XSS, and known attacks. It helps in managing the web server and web application security. This security tool is used by developers, system/security administrators, IT auditors, and staff.

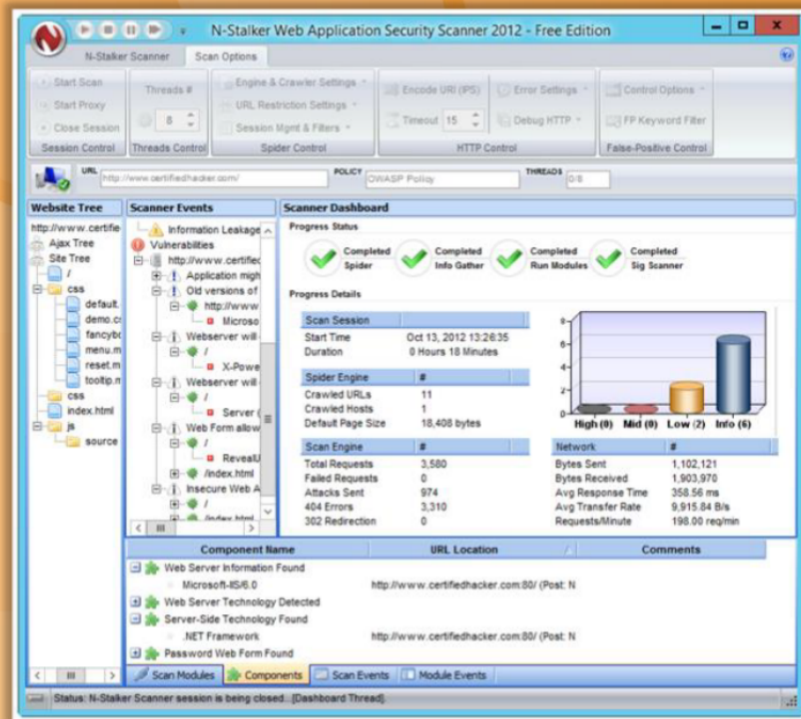


FIGURE 12.32: -Stalker Web Application Security Scanner



Web Server Security Scanner: Wikto

Source: <http://www.sensepost.com>

Wikto is for Windows, with a couple of extra features including fuzzy logic error code checking, a backend miner, Google-assisted directory mining, and **real-time HTTP request/response monitoring**. Wikto is coded in C# and requires the .NET framework.

Wikto may not test for SQL injections, but it is still an essential tool for penetration testers who are looking for vulnerabilities in their Internet-facing web servers.

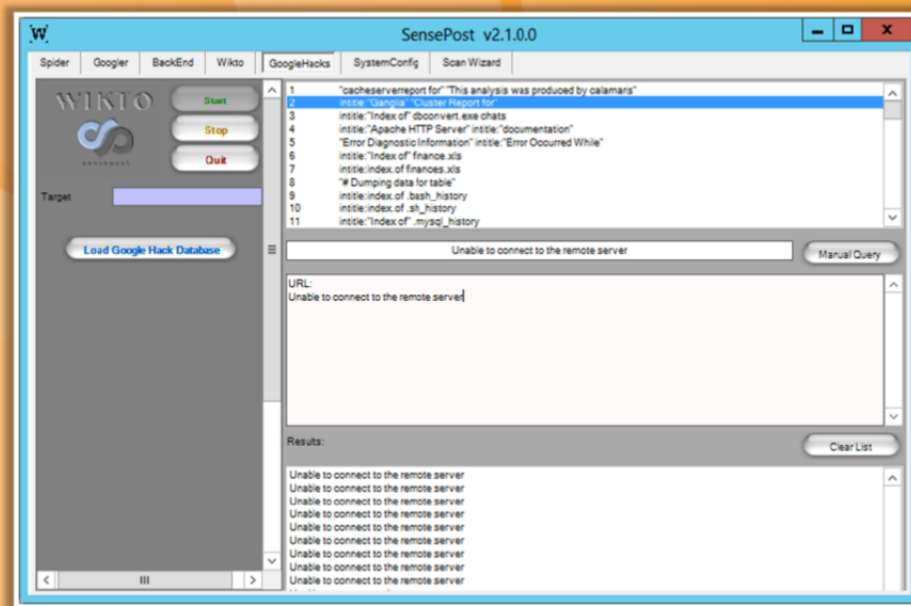


FIGURE 12.33: Wikto Screenshot

Web Server Security Scanner: Acunetix Web Vulnerability Scanner



- Acunetix WVS **checks web applications** for SQL injections, cross-site scripting, etc.
- It includes advanced penetration testing tools to ease **manual security audit processes**, and also creates professional security audit and regulatory compliance reports





Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Security Scanner: Acunetix Web Vulnerability Scanner

Source: <http://www.acunetix.com>

Acunetix Web Vulnerability Scanner checks web applications for SQL injections, cross-site scripting, etc. It includes **advanced penetration testing tools** to ease the manual security audit processes, and also creates professional security audit and regulatory compliance reports.

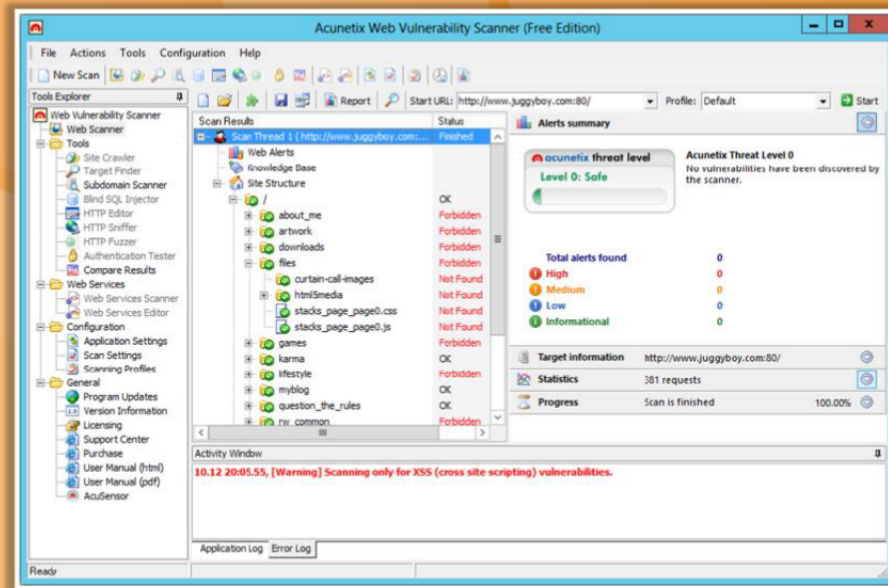



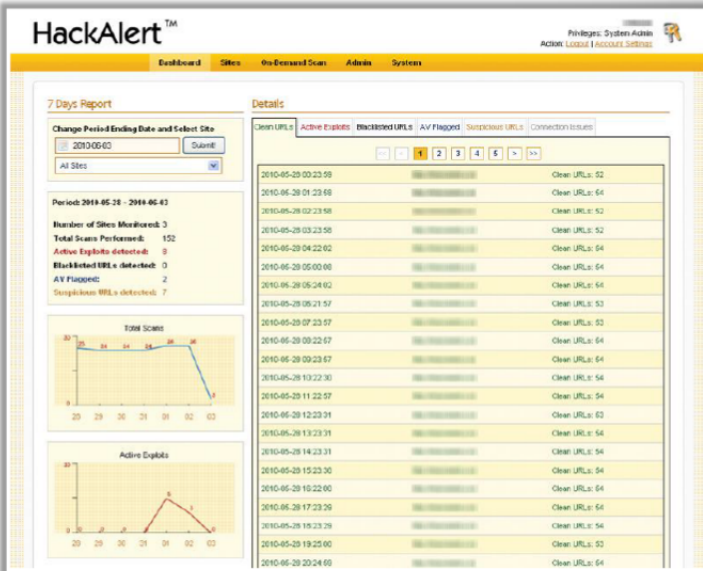
FIGURE 12.34: Acunetix Web Vulnerability Scanner

Web Server Malware Infection Monitoring Tool: HackAlert



HackAlert™ is a **cloud-based service** that identifies hidden zero-day malware and drive-by downloads in websites and online advertisements

- Protects clients and customers from **malware injected** websites, drive by downloads, and malicious advertising
- Identifies malware before the website is flagged as malicious
- Displays injected code snippets to facilitate remediation
- Deploys as cloud-based SaaS or as a flexible API for enterprise integration
- Integrates with WAF or web server modules for instant mitigation



<http://www.armorize.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Malware Infection Monitoring Tool: HackAlert

Source <http://www.armorize.com>

HackAlert is a cloud-based service that identifies **hidden zero-day malware and drive-by downloads in websites** and online advertisements. Optimizing multiple analysis techniques, this service identifies injected malware and generates alarms before search engines blacklist the website. This enables immediate remediation to protect customers, business reputation, and revenues. It is accessed via either a **web-based SaaS interface or a flexible API** that facilitates integration with enterprise security tools.

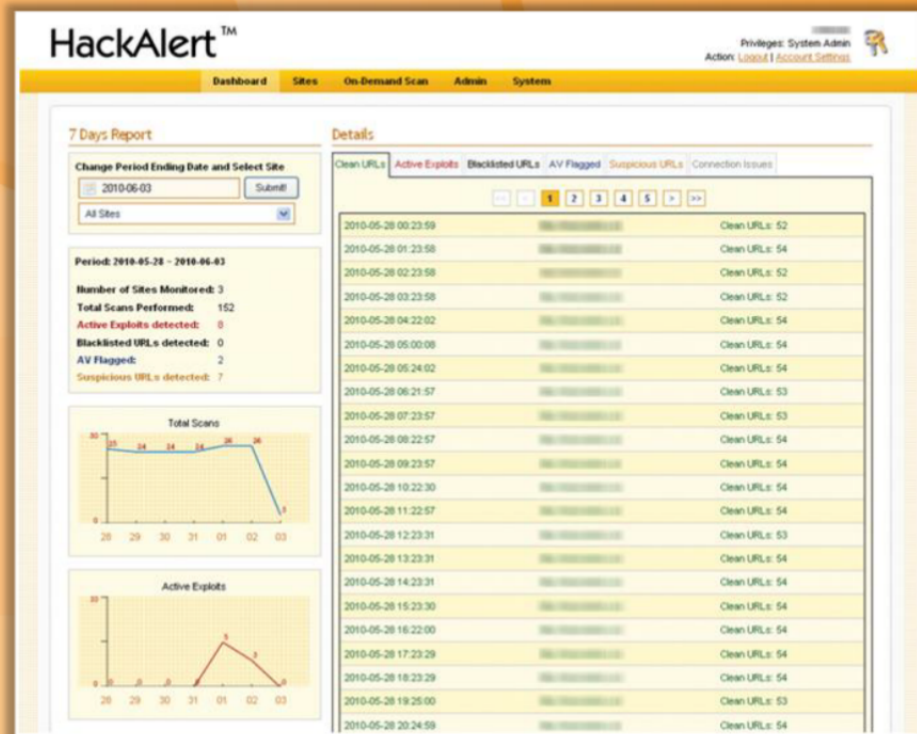


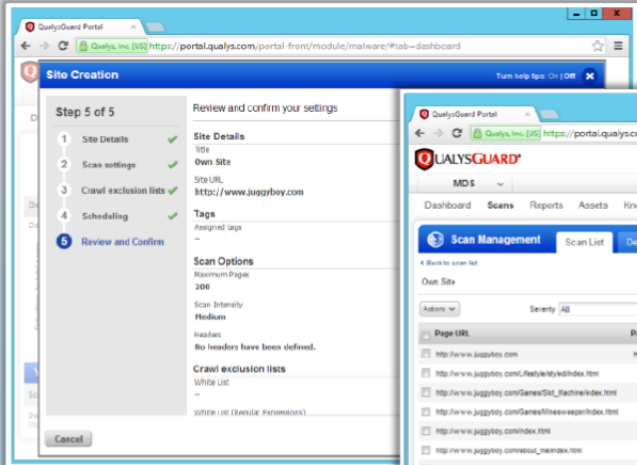
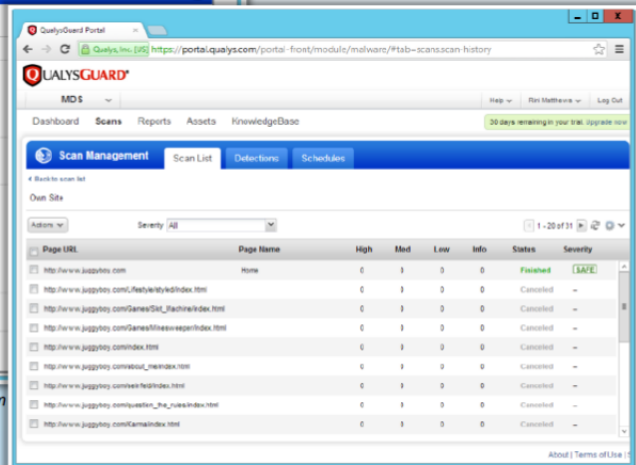


FIGURE 12.35: HackAlert Screenshot

Web Server Malware Infection Monitoring Tool: **QualysGuard Malware Detection**



 QualysGuard® Malware Detection Service scans websites for **malware infections** and **threats**

<http://www.qualys.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Malware Infection Monitoring Tool: QualysGuard Malware Detection

Source: <http://www.qualys.com>

QualysGuard Malware Detection Service scans websites thoroughly for malware infections and for a variety of threats. It provides automated alerts and reports that enable you to identify and resolve the threat. It can also be used to protect the customers of an organization from malware infections and safeguard their brand reputations, preventing website black listing. It regularly schedules scanning to monitor websites on an ongoing basis, with email alerts to quickly notify organizations when infections are discovered. **Malware infection** details are provided so that organizations can take quick action to isolate and remove malware.

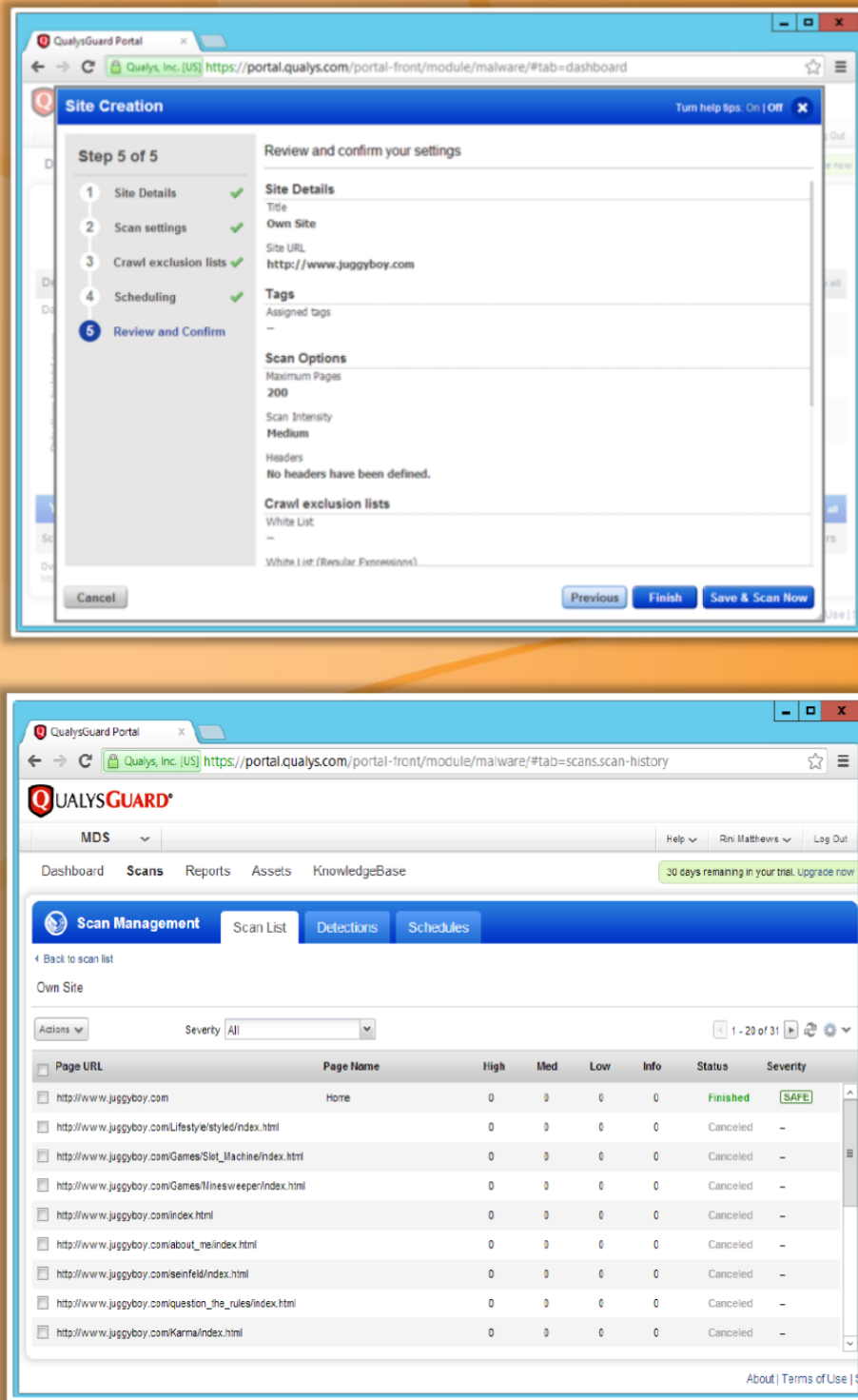













FIGURE 12.36: QualysGuard Malware Detection Screenshot

Webserver Security Tools



 Retina CS http://www.beyondtrust.com	 Arirang http://monkey.org
 Nscan http://nscan.hypermart.net	 N-Stealth Security Scanner http://www.nstalker.com
 NetIQ Secure Configuration Manager http://www.netiq.com	 Infiltrator http://www.infiltration-systems.com
 SAINTscanner http://www.saintcorporation.com	 WebCruiser http://sec4app.com
 HP WebInspect https://download.hpsmartupdate.com	 dotDefender http://www.applicure.com

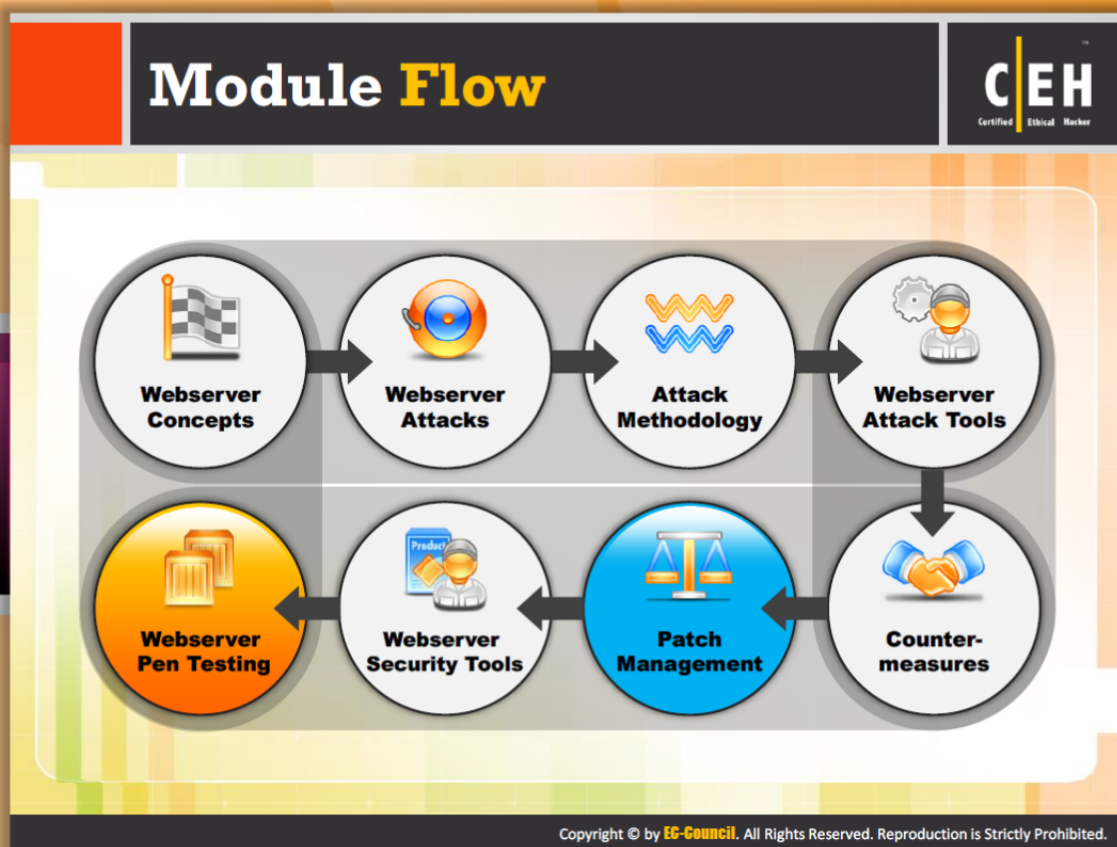
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Webserver Security Tools

Web server Security tools scan large, complex websites and web applications to tackle web-based vulnerabilities. These tools identify application vulnerabilities as well as site exposure risk, rank threat priority, produce highly graphical, intuitive HTML reports, and indicate **site security posture by vulnerabilities and threat level**. Some of web server security tools include:

- Retina CS available at <http://www.beyondtrust.com>
- Nscan available at <http://nscan.hypermart.net>
- NetIQ Secure Configuration Manager available at <http://www.netiq.com>
- SAINTScanner available at <http://www.saintcorporation.com>
- HP WebInspect available at <https://download.hpsmartupdate.com>
- Arirang available at <http://monkey.org>
- N-Stealth Security Scanner available at <http://www.nstalker.com>
- Infiltrator available at <http://www.infiltration-systems.com>
- WebCruiser available at <http://sec4app.com>
- dotDefender available at <http://www.applicure.com>




Module Flow

The whole idea behind ethical hacking is to hack your own network or system in an attempt to find the vulnerabilities and fix them before a real attacker exploits them system. As a penetration tester, you should conduct a penetration test on web servers in order to determine the vulnerabilities on the web server. You should apply all the hacking techniques for hacking web servers. This section describes web server pen testing tools and the steps involved in web server pen testing.

 Webserver Concepts	 Webserver Attacks
 Attack Methodology	 Webserver Attack Tools
 Webserver Pen Testing	 Webserver Security Tools
 Patch Management	 Counter-measures

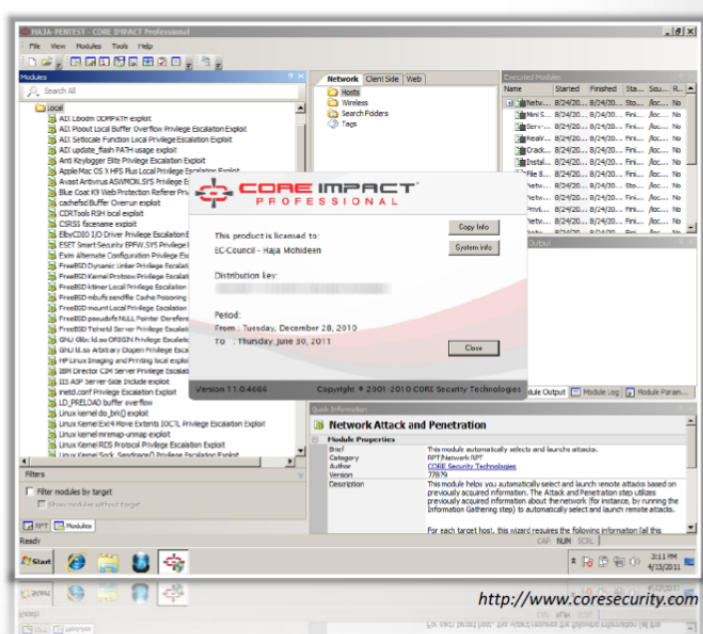
Web Server Pen Testing Tool:

CORE Impact® Pro



CORE Impact® Pro is the software solution for assessing and testing **security vulnerabilities** in the organization:

- Web Applications
- Network Systems
- Endpoint systems
- Wireless Networks
- Network Devices
- Mobile Devices
- IPS/IDS and other defenses



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Pen Testing Tool: CORE Impact® Pro

Source: <http://www.coresecurity.com>

CORE Impact® Pro helps you in penetrating web servers to find vulnerabilities/weaknesses in the web server. By safely exploiting vulnerabilities in your network infrastructure, this tool identifies real, tangible risks to information assets while testing the effectiveness of your existing security investments. This tool is able to perform the following:

- Identify weaknesses in web applications, web servers, and associated databases
- Dynamically generate exploits that can compromise security weaknesses
- Demonstrate the potential consequences of a breach
- Gather information necessary for addressing security issues and preventing data incidents

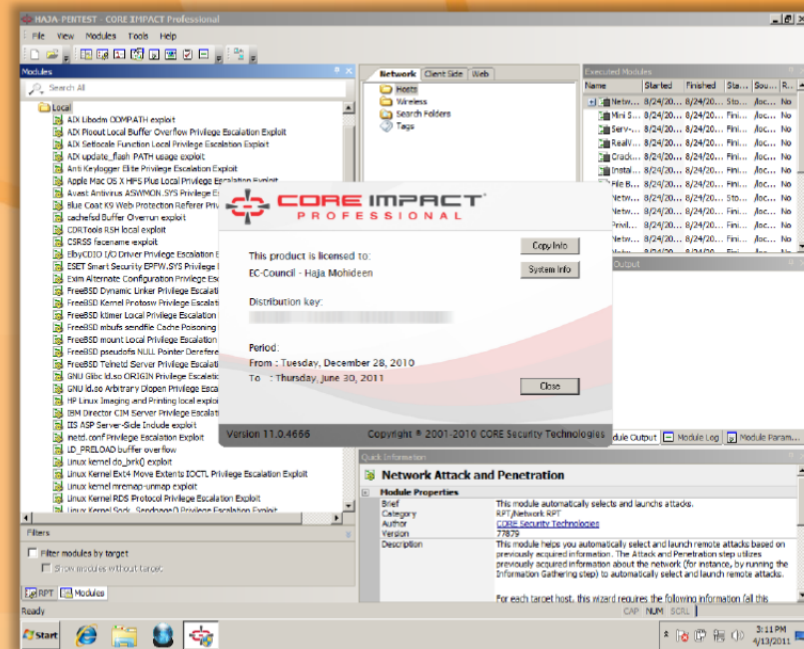
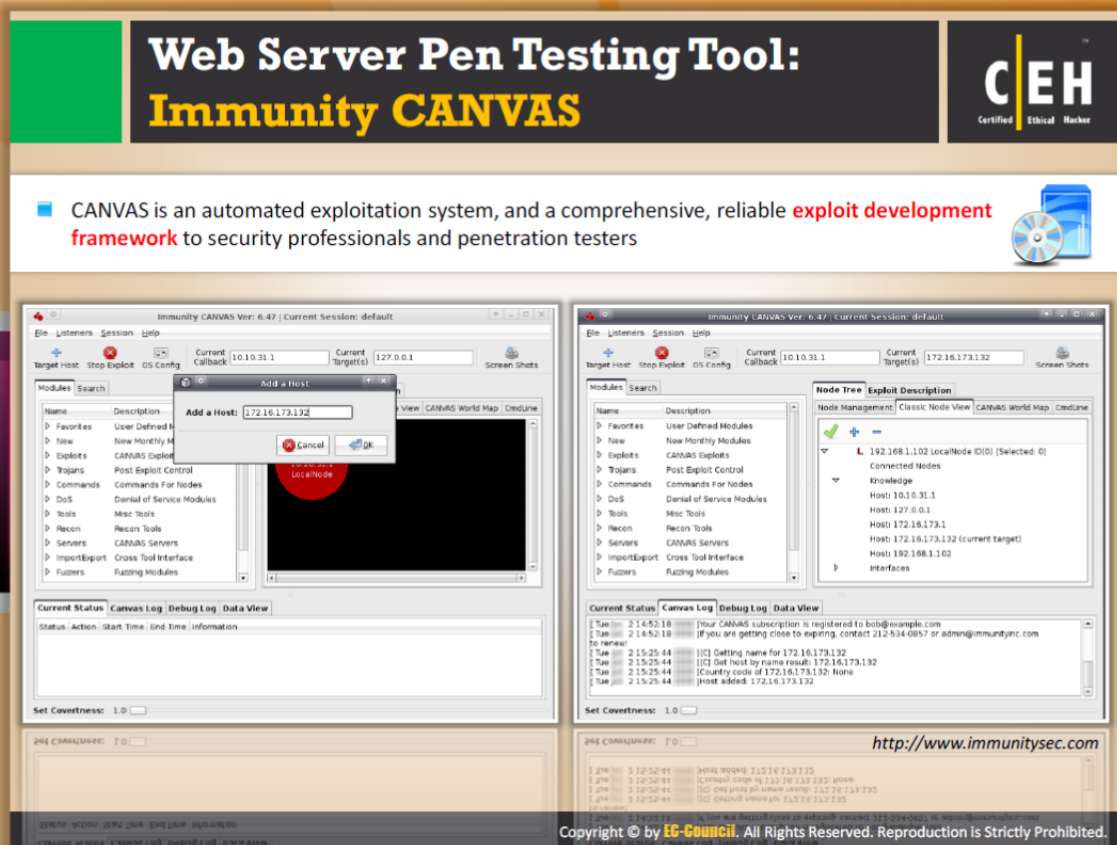


FIGURE 12.37: CORE Impact® Pro Screenshot



Web Server Pen Testing Tool: Immunity CANVAS

Source: <http://www.immunitysec.com>

CANVAS is an automated exploitation system, and a comprehensive, reliable exploit development framework for security professionals and penetration testers. It allows a pen tester to discover all possible security vulnerabilities on the web server.

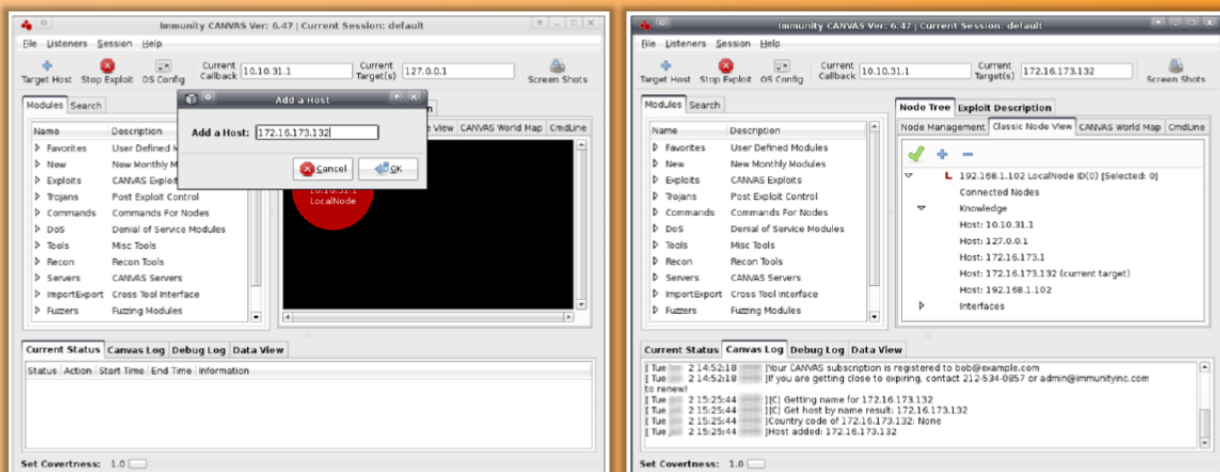
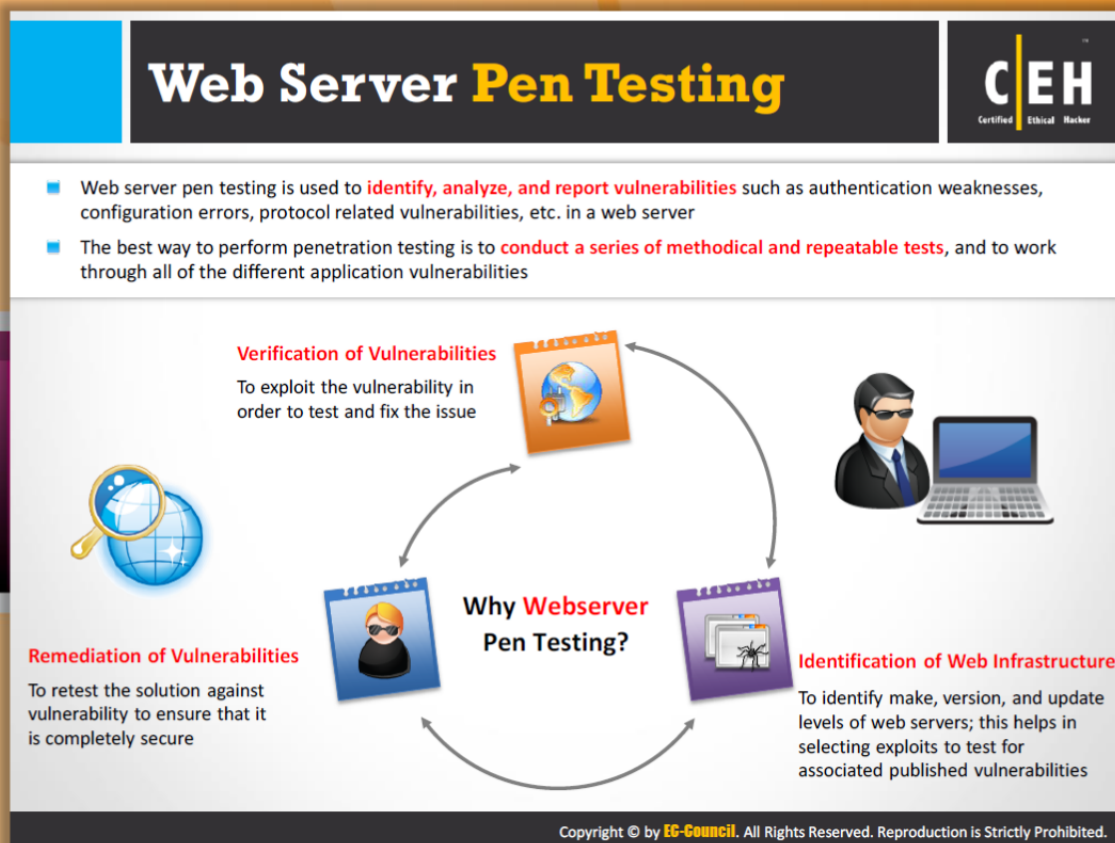


FIGURE 12.38: Immunity CANVAS Screenshot



Web Server Pen Testing

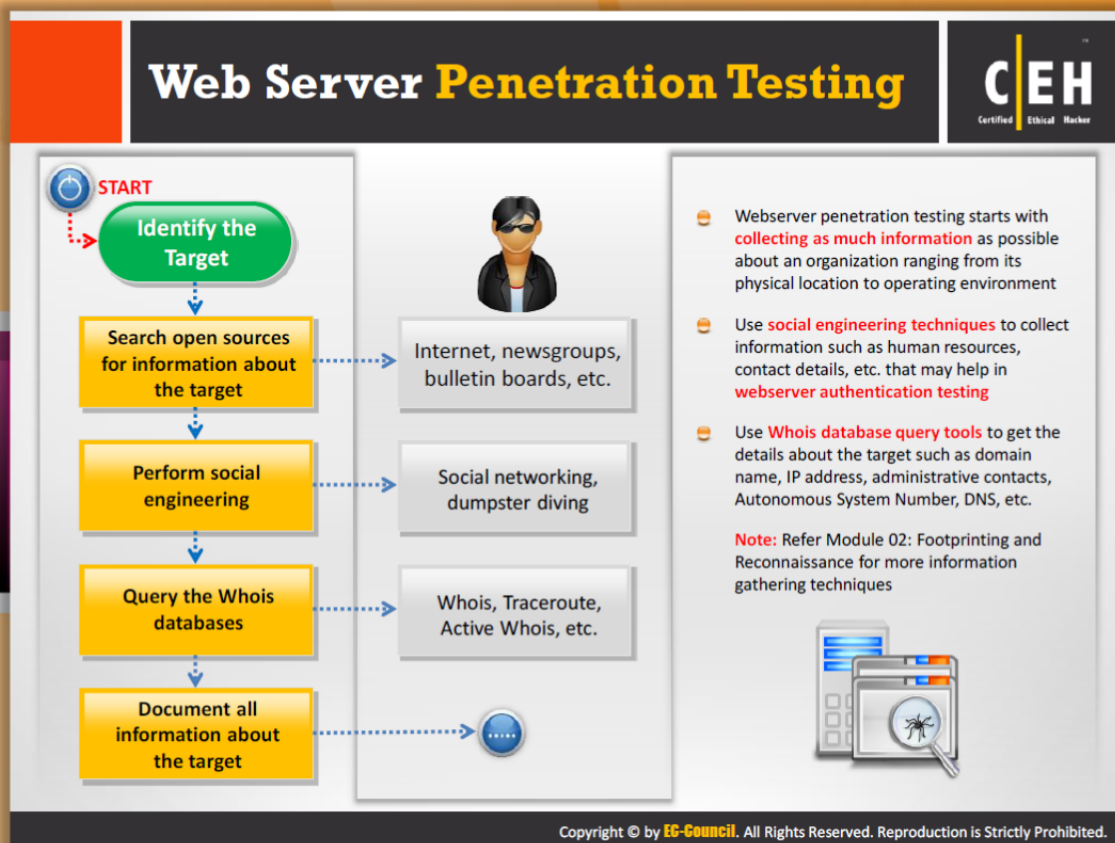
Web server pen testing will help you to identify, analyze, and **report vulnerabilities** such as **authentication weaknesses, configuration errors, protocol-related vulnerabilities**, etc. in a web server. To perform penetration testing, you need to conduct a series of methodical and repeatable tests, and to work through all of the different application vulnerabilities.



Why Web Server Pen Testing?

Web server pen testing is useful for:

- **Identification of Web Infrastructure:** To identify make, version, and update levels of web servers; this helps in selecting exploits to test for associated published vulnerabilities.
- **Verification of Vulnerabilities:** To exploit the vulnerability in order to test and fix the issue.
- **Remediation of Vulnerabilities:** To retest the solution against vulnerability to ensure that it is completely secure.



Web Server Penetration Testing

Web server penetration testing starts with collecting as much information as possible about an organization, ranging from its **physical location to operating environment**. The following are the series of steps conducted by the pen tester to penetrate web server:

Step 1: Search open sources for information about the target

Try to collect as much information as possible about target organization web server ranging from its physical location to operating environment. You can obtain such information from the Internet, newsgroups, bulletin boards, etc.

Step 2: Perform Social engineering

Perform social engineering techniques to collect information such as human resources, contact details, etc. that may help in web server authentication testing. You can also perform social engineering through social networking sites or dumpster driving.

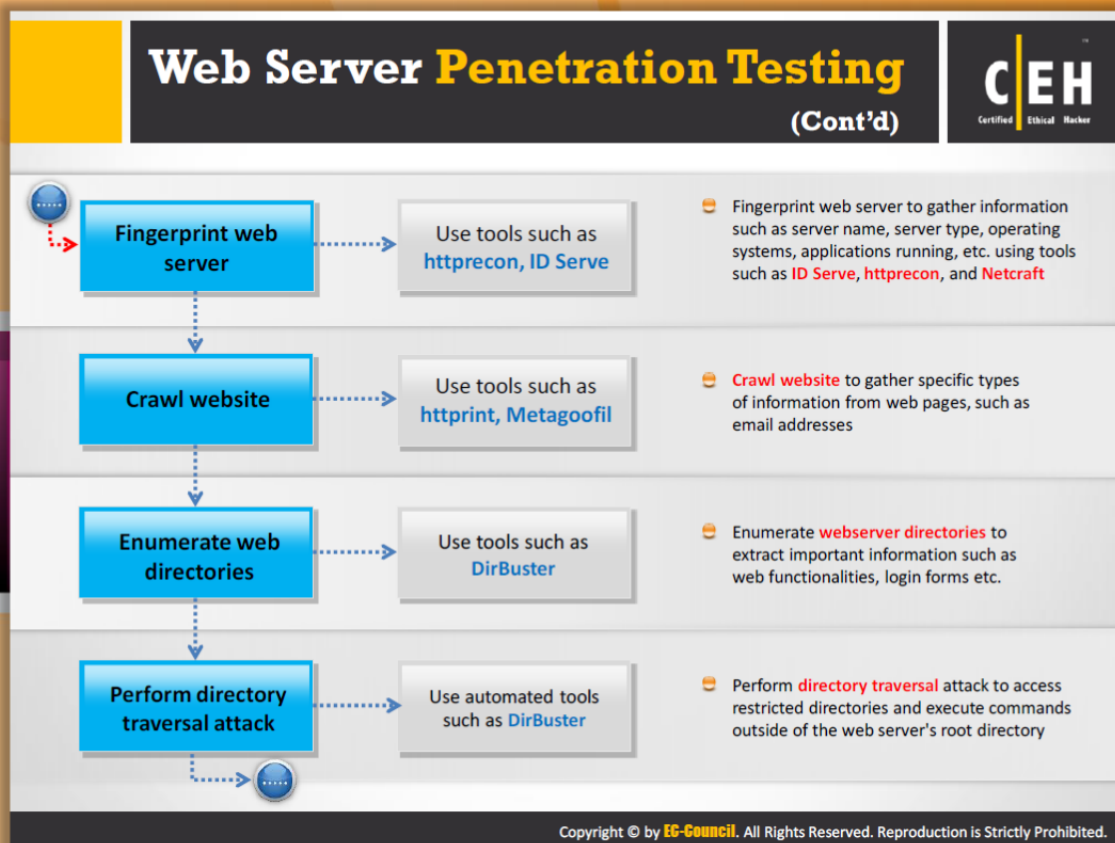
Step 3: Query the Whois databases

You can use Whois database query tools such as **Whois, Traceroute, Active Whois**, etc. to get details about the target such as domain name, IP address, administrative contacts, Autonomous System Number, DNS, etc.

Step 4: Document all information about the target

You should document all the information obtained from the various sources.

Note: Refer Module 02 – Footprinting and Reconnaissance for more information about information-gathering techniques.



Web Server Penetration Testing (Cont'd)

Step 5: Fingerprint the web server

Perform fingerprinting on the web server to gather information such as server name, server type, operating systems, applications running, etc. using tools such as ID Serve, httprecon, and Netcraft.

Step 6: Perform website crawling

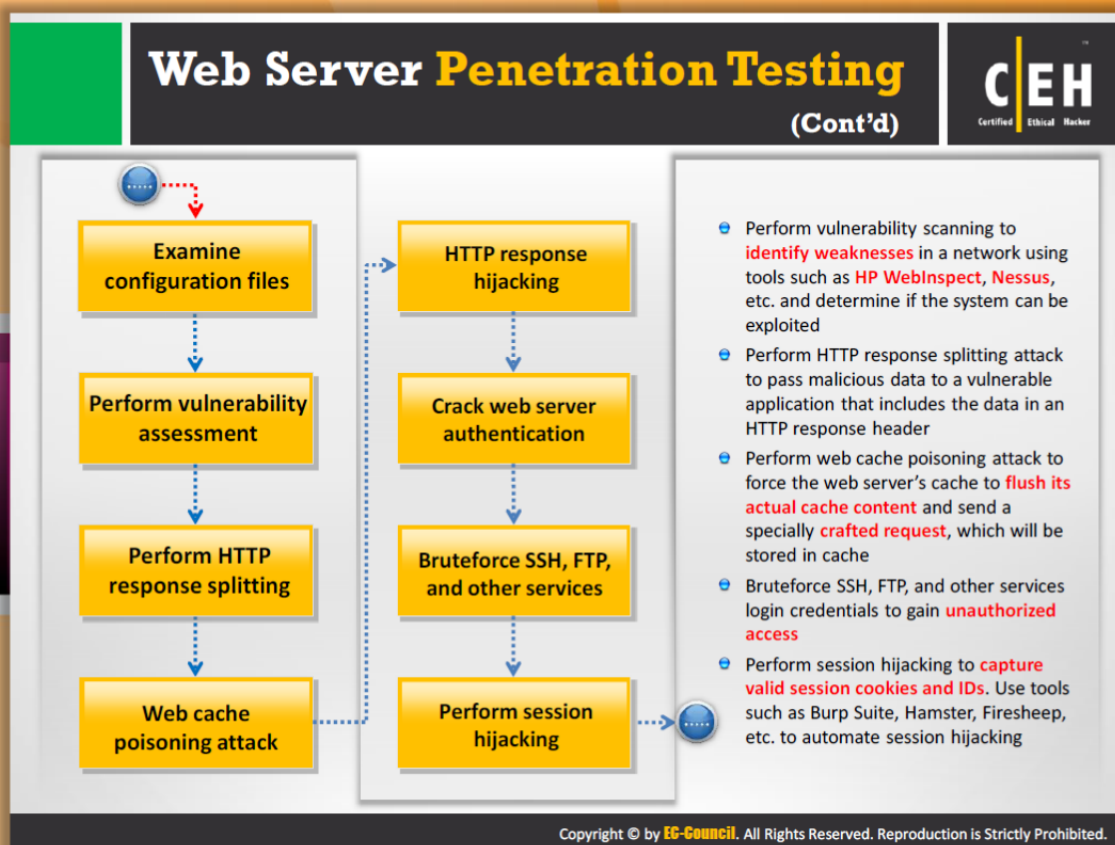
Perform website crawling to gather specific information from web pages, such as email addresses. You can use tools such as httpprint and Metagoofil to crawl the website.

Step 7: Enumerate web directories

Enumerate web server directories to extract important information such as **web functionalities**, **login forms**, etc. You can do this by using tool such as DirBuster.

Step 8: Perform a directory traversal attack

Perform a **directory traversal attack** to access restricted directories and execute commands outside of the web server's root directory. You can do this by using automated tools such as DirBuster.



Web Server Penetration Testing (Cont'd)

Step 9: Perform vulnerability scanning

Perform vulnerability scanning to identify weaknesses in a network using tools such as HP WebInspect, Nessus, etc. and determine if the system can be exploited.

Step 10: Perform an HTTP response splitting attack

Perform an HTTP response splitting attack to pass **malicious data to a vulnerable application** that includes the data in an HTTP response header.

Step 11: Perform a web cache poisoning attack

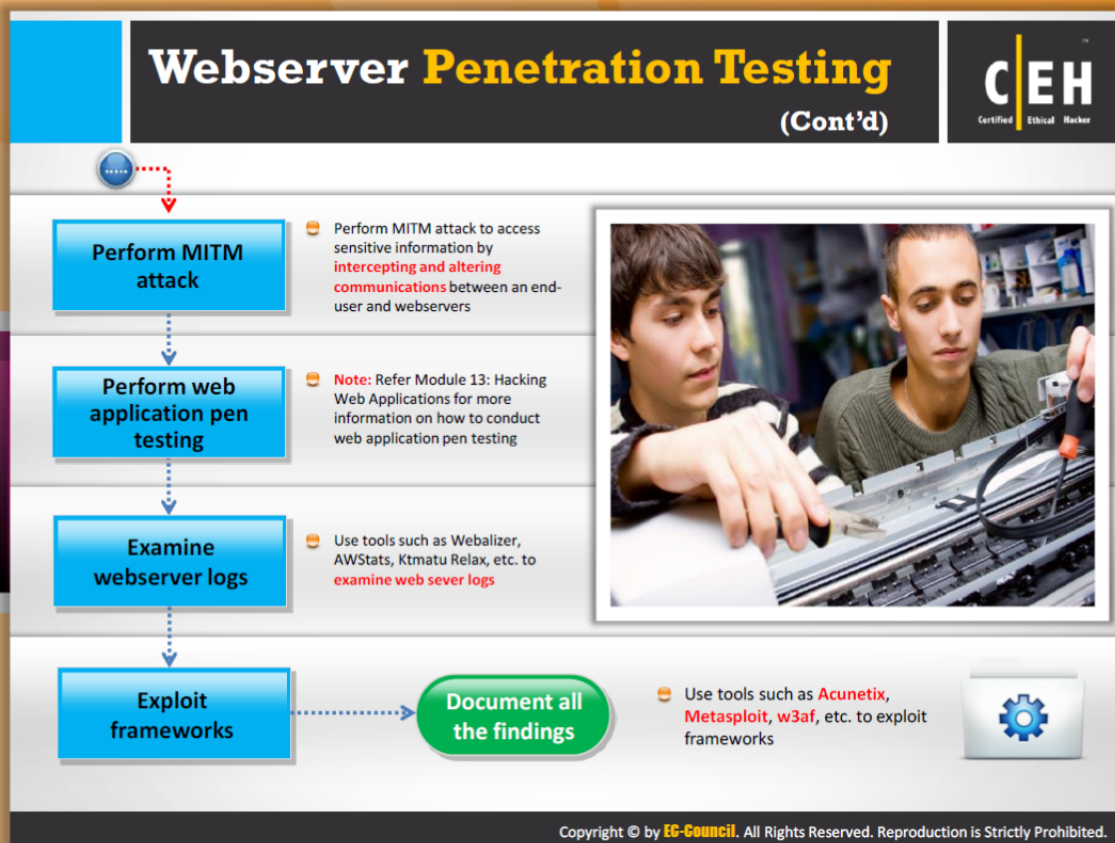
Perform a web cache poisoning attack to force the web server's cache to flush its actual cache content and send a specially crafted request, which will be stored in the cache.

Step 12: Brute force login credentials

Brute force SSH, FTP, and other services **login credentials** to gain unauthorized access.

Step 13: Perform session hijacking

Perform session hijacking to capture valid session cookies and IDs. You can use tools such as Burp Suite, Hamster, Firesheep, etc. to automate session hijacking.



Web Server Penetration Testing (Cont'd)

Step 14: Perform a MITM attack

Perform a MITM attack to access sensitive information by intercepting and altering communications between an end user and web servers.

Step 15: Perform web application pen testing

Perform web application pen testing to determine whether applications are prone to vulnerabilities. **Attackers** can compromise a web server even with the help of a vulnerable web application.

Step 16: Examine web server logs

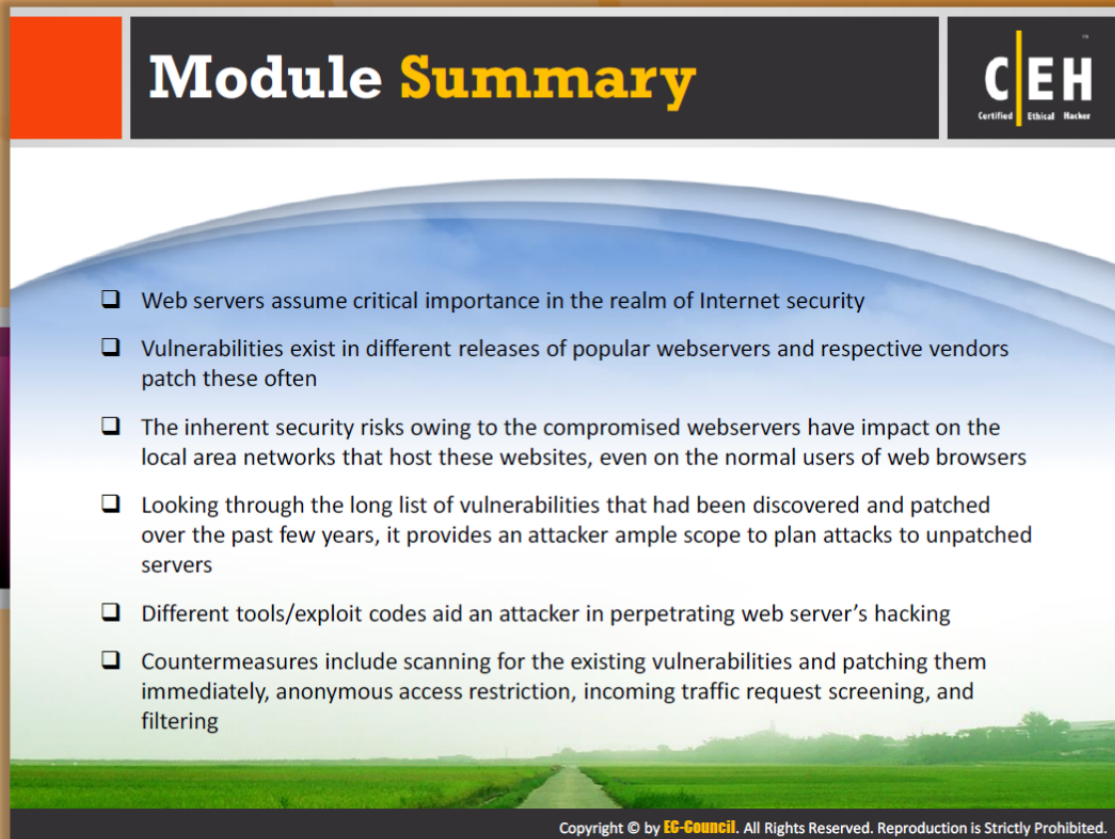
Examine the server logs for suspicious activities. You can do this by using tools such as Webalizer, AWStats, Ktmatu Relax, etc.

Step 17: Exploit frameworks


Exploit the **frameworks** used by the web server using tools such as Acunetix, Metasploit, w3af, etc.

Step 18: Document all the findings

Summarize all the tests conducted so far along with the findings for further analysis. Submit a copy of the penetration test report to the **authorized person**.



Module Summary



- ❑ Web servers assume critical importance in the realm of Internet security
- ❑ Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often
- ❑ The inherent security risks owing to the compromised web servers have impact on the local area networks that host these websites, even on the normal users of web browsers
- ❑ Looking through the long list of vulnerabilities that had been discovered and patched over the past few years, it provides an attacker ample scope to plan attacks to unpatched servers
- ❑ Different tools/exploit codes aid an attacker in perpetrating web server's hacking
- ❑ Countermeasures include scanning for the existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening, and filtering

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

- Web servers assume critical importance in the realm of Internet security.
- Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often.
- The inherent security risks owing to the compromised web servers impact the local area networks that host these websites, even on the normal users of web browsers.
- Looking through the long list of vulnerabilities that had been discovered and patched over the past few years, it provides an attacker ample scope to plan attacks to unpatched servers.
- Different tools/exploit codes aid an attacker in perpetrating web server's hacking.
- Countermeasures include scanning for the existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening, and filtering.