

# Chapter 3 network security



**Zero Day Attacks** Attacks that exploit previously unknown vulnerabilities, so victims have no time (zero days) to prepare or defend against the attacks.

**XML Attacks** Injects scripts into web application server that will then direct attacks at clients

**Directory Traversal Attack** Takes advantage of vulnerability in the Web application program or the Web server software so that a user can move from the root directory to other restricted directories

**Command Injection Attack** The ability to move to another directory could allow an unauthorized user to view confidential files or even enter commands to execute on a server

**Client-side attacks** Targets vulnerabilities in client applications that interact with a compromised server or process malicious data

**Cookies** Created from the Web site that a user is currently viewing

**Access Rights** Privileges that are granted to users to access hardware and software resources are called

**Privilege Escalation** Exploiting a vulnerability in software to gain access to resources that the user would normally be restricted from obtaining is called

**Transitive Access** An attack involving using a third party to gain access rights is called a/an

**SQL** is a language used to view and manipulate data that is stored in a relational database

TagsHTML is a markup language that uses specific \_\_\_\_ embedded in brackets

HTMLis designed to display data, with the primary focus on how the data looks

XMLis for the transport and storage of data, with the focus on what the data is

rootUsers who access a Web server are usually restricted to the \_\_\_\_ directory

inetpubwwwrootThe default root directory of the Microsoft Internet Information Services (IIS) Web server is

/var/wwwFor a Web server using a Linux operating system, the default root directory is typically

../traversesThe expression \_\_\_\_ up one directory level.

server-sideWeb application attacks are considered \_\_\_\_ attacks.

drive-by-downloadA client-side attack that results in a user's computer becoming compromised just by viewing a Web page and not even clicking any content is known as a

HTTP headerThe \_\_\_\_ is part of an HTTP packet that is composed of fields that contain the different characteristics of the data being transmitted

session hijackingA/an \_\_\_\_ is an attack in which an attacker attempts to impersonate the user by using his session token.

replayA/an \_\_\_\_ attack is similar to a passive man-in-the-middle attack.

DNSWhen TCP/IP was developed, the host table concept was expanded to a hierarchical name system for matching computer names and numbers known as the

DNS poisoning substitutes DNS addresses so that the computer is automatically redirected to another device.

zone transferWhen DNS servers exchange information among themselves it is known as a

DNS poisoningThe Chinese government uses \_\_\_\_ to prevent Internet content that it considers unfavorable from reaching its citizenry.

HTTPAll Web traffic is based on the \_\_\_\_\_ protocol.

markup languageA(n) \_\_\_\_\_ is a method for adding annotations to the text so that the additions can be distinguished from the text itself.

SessionA(n) \_\_\_\_\_ cookie is stored in Random Access Memory (RAM), instead of on the hard drive, and only lasts for the duration of visiting the Web site.

ARPRANETThe predecessor to today's Internet was a network known as

ONCHAPTER 3 NETWORK SECURITY SPECIFICALLY FOR YOUFOR ONLY\$13.

90/PAGEOrder Now