Discuss different types of System Attacks - 2 Pages, 2 References.

*The course textbook[[1]](#footnote-1) has definitions of terms describing different types of attacks, such as:*

**ARP poisoning** – An attack that corrupts the ARP cache. Address Resolution Protocol (ARP) is part of the TCP/IP protocol for determining the MAC address based on the IP address.

**buffer overflow** – An attack that occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer.

**client-side attack** – An attack that targets vulnerabilities in client applications that interact with a compromised server or processes malicious data.

**command injection** – Injecting and executing commands to execute on a server.

**cross-site scripting (XSS)** – Application server to direct attacks at clients.

**denial of service (DoS)[[2]](#footnote-2)** – An attack that attempts to prevent a system from performing its normal functions. There is a website that shows a pictorial representation (map) of the top daily DDOS attacks, worldwide.

**directory traversal** – An attack that takes advantage of a 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.

**distributed denial of service (DDoS)** – An attack that uses multiple zombie computers (even hundreds or thousands) in a botnet to flood a device with requests.

**DNS poisoning** – An attack that substitutes DNS addresses so that the computer is automatically redirected to another device. It corrupts the host table that maps the names to computer numbers.

**HTTP header manipulation** – Modifying HTTP headers to create an attack. It is part of HTTP that is composed of fields that contain the characteristics of the data that is being transmitted.

**man-in-the-middle** – An attack that intercepts legitimate communication and forges a fictitious response to the sender.

**ping flood** – An attack uses Internet Control Message Protocol (ICMP) to flood with packets that echo a request message to a host.

**privilege escalation** – An attack that exploits a vulnerability in software to gain access to resources that the user would normally be restricted from obtaining.

**replay** – An attack that makes a copy of the transmission before sending it to the recipient.

**session hijacking** – An attacker attempts to impersonate the user by using his session token.

**smurf attack** – An attack that broadcasts a ping request to all computers on the network yet changes the address from which the request came to that of the target.

**spoofing** – Impersonating another computer or device.

**SQL injection** – An attack targets SQL servers by injecting commands trusted by the database.

**SYN flood attack** – An attack that takes advantage of procedures for initiating a TCP session.

**transitive access** – An attack involving using a third party to gain access rights.

**XML injection** – An attack that injects XLM tags and data into a database. XML (Extensible Markup Language)is a markup language that is designed to carry data instead of indicating how to display it.

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

**computer virus (virus)** – A malicious computer code that, like its biological counterpart, reproduces itself on the same computer.

**logic bomb** – Computer code that lies dormant until it is triggered by a specific logical event.

**pharming** – A phishing attack that automatically redirects the user to a fake site.

**phishing** – Sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information.

**rootkit** – A set of software tools used by an attacker to hide the actions or presence of other types of malicious software.

*And some of the actions that afford the opportunities to attack, such as:*

**add-ons** – Programs that provide additional functionality to Web browsers.

**attachments** – Files that are coupled to e-mail messages.

**cookie** – A file on a local computer in which a server stores user-specific information. A first-party cookie that is created from the Web site that currently is being viewed. A third-party cookie that was created by a third party that is different from the primary Web site. A secure cookie is only used when using a secure connection. A session cookie is stored in Random Access Memory (RAM), instead of on the hard drive, and only lasts for the duration of visit. A persistent cookie (tracking cookie) is recorded on the hard drive of the computer and does not expire when the browser closes.

**Flash cookie** – A cookie named after the Adobe Flash player. Also known as local shared objects **adware** – (LSOs). Flash cookies cannot be deleted through the browser's normal configuration settings as regular cookies can. Typically, they are saved in multiple locations on the hard drive and can be take up as much as 100,000 bytes of storage per cookie (about 25 times the size of a normal cookie). Flash cookies can also be used to reinstate regular cookies that a user has deleted or blocked.

**session token** – A form of verification used when accessing a secure Web application.

1. SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, 4TH Edition, Mark Ciampa, Ph.D, © 2012 Course Technology, Cengage Learning. [↑](#footnote-ref-1)
2. Digital Attack Map, Top daily DDOS attacks worldwide. Website url: <http://www.digitalattackmap.com> [↑](#footnote-ref-2)