www.sitesassure.com

Adware

Software that displays advertising content on your computer. Like its cousin spyware, some adware runs with your full knowledge and consent, some doesn't. More often an annoyance than a security risk, adware may also monitor browsing activities and relay that information to someone else over the Internet.

Backup

An extra copy of computer files, usually kept physically separate from the originals. Essential for recovery when original files are damaged or lost.

Backdoor

A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.
Blended threat
An attack combining a number of traditional attack methods, like a worm, a Trojan horse, and a keylogger. Most require a combination of security tools and protection layers to defend.

Brute Force

An automated process of trial and error used to guess a person's username, password, credit-card number or cryptographic key. Many systems will allow the use of weak passwords or small cryptographic keys. An attacker can cycle though the dictionary word by word, generating thousands or potentially millions of incorrect guesses searching for the valid password.

There are two types of brute force attacks: normal brute force and reverse brute force. A normal brute force attack uses a single username against many passwords. A reverse brute force attack uses many usernames against one password. In systems with millions of user accounts, the odds of multiple users having the same password dramatically increases.

Cross-Site Request Forgery (CSRF)

An attack that tricks the victim into loading a page that contains a malicious request. The request inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf, like change the victim's e-mail address, home address, or password, or purchase something. CSRF attacks generally target functions that cause a state change on the server, but can also be used to access sensitive data.

For most sites, browsers will automatically include with such requests any credentials associated with the site, such as the user's session cookie, basic auth credentials, IP address, or Windows domain credentials. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish a CSRF attack from a legitimate user request. The attacker can then make the victim perform actions that they didn't intend to, such as logout, purchase item, change account information, retrieve account information, or any other function provided by the vulnerable website.

Cross-site scripting (XSS)
A type of computer security vulnerabilitytypically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.

Directory traversal
A HTTP exploit which allows attackers to access restricted directories and execute commands outside of the web server's root directory. Web servers provide two main levels of security mechanisms. Access Control Lists (ACLs)

Domain spoofing or Domain hijacking
Manipulation of the domain name system to associate a legitimate Web address with an imposter or otherwise malicious website. Used to perpetrate phishing and other types of attack, the user is sent to the imposter website with little or no warning.

DoS
Denial-of-Service. An attack on a computer or network in which bandwidth is flooded or resources are overloaded to the point where the computer or network's services are unavailable to clients. Can also be carried out by malicious code that simply shuts down resources.

Distributed Denial of Service Attack (DDoS)
A denial of service DoS attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet

Firewall (network)
A hardware or software device, or both, that controls network access and communications between a network and the Internet, or between one part of a network and another.

Firewall (personal)
Software that controls access and communications between a computer and the Internet or a local network. Blocks hackers and other unauthorized traffic, while allowing authorized traffic through.

Hacker
Commonly, a person who uses programming skills and technical knowledge to gain unauthorized access to computer systems for malicious or criminal purposes. The programming community, however, prefers to use the term "cracker" for such persons; they reserve "hacker" for any well-respected, highly skilled programmer.

Format String Attack
Format String Attacks alter the flow of a Web application by using string-formatting library features to access other memory space. Vulnerabilities occur when user-supplied data are used directly as formatting string input for certain C/C++ functions (e.g. fprintf, printf, sprintf, setproctitle, syslog, . . .).
If an attacker passes a format string consisting of printf conversion characters (for example: "%f", "%p", "%n", and so on.) as parameter value to the web application, they may:
Execute arbitrary code on the server
Read values off the stack
Cause segmentation faults / software crashes

Keylogger
Software that monitors and captures everything a user types into a computer keyboard. Used for technical support and surveillance purposes. Can also be integrated into malware and used to gather passwords, user names, and other private information.

Layer 1 Intrusion Detection
is a signature-based detection system, where it detects the most common hacking behaviors through a surface scanning in the URL. Once a hacking behavior is found in the targetted URL that matches one of the hacking signature defined in the layer 1 rulesets, the activity and the corresponding IP will be banned immediately.

Layer 2 Intrusion Detection
iA pattern-based Instruction Detection Systems, where it scans all request variables against a set of hacking patterns. If it finds a matching pattern, a counter will start accumulating the risk score until the scanning is completed. The attack will be banned or sanitized if the total risk score exceed the pre-configured risk threshold.

Malware
Derived from “malicious software.” Software designed to do harm by causing damage to systems or data, invading privacy, stealing information, or infiltrating computers without permission. Includes viruses, worms, Trojan horses, some keyloggers, spyware, adware, and bots.

Phishing
An attempt to mislead people into divulging confidential information, such as Social Security numbers and passwords. Phishing typically uses legitimate-looking email or IMs in combination with imposter websites to make fraudulent requests for information (e.g., to go “fishing” for data). See also, social engineering.

Pharming
An attempt to defraud Internet surfers by hijacking a website’s domain name, or URL, and redirecting users to an imposter website where fraudulent requests for information are made. See also, URL spoofing.

Spam
Unsolicited email, usually sent in bulk to a large number of random accounts; often contains ads for products or services. Also used inphishing scams and other online fraud. Can be minimized using email filtering software.

Spyware
Software that collects information about your computer and how you use it and relays that information to someone else over the Internet.Spyware ordinarily runs in the background, and in some cases installs itself on your computer without your knowledge or permission.

SQL Injection
A very severe attack used to exploit websites that construct SQL statements from user-supplied input to steal information from a database and/or to gain access to an organization’s host computers through the computer that is hosting the database.

Structured Query Language (SQL) is a specialized programming language for sending queries to databases. However, many database products supporting SQL do so with proprietary extensions to the

standard language. Web applications may use user-supplied input to create custom SQL statements for dynamic web page requests.

SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.

SQL Injection attacks may be prevented by enforcing the use of parameterized statements.

Trojan horse

A malicious program disguised as legitimate software; often gives someone else the power to take remote control of your computer; may also attack data or systems. Unlike viruses and worms, Trojan horses cannot replicate or propagate themselves and therefore must rely on other methods of distribution.

URL spoofing

Attempting to masquerade or closely mimic the URL displayed in a Web browser's address bar. Used in phishing attacks and other online scams to make an imposter website appear legitimate, the attacker obscures the actual URL by overlaying a legitimate looking address or by using a similarly spelled URL.

Virus

A program that can self-replicate and infect files, programs, and computer systems. Some viruses simply replicate and spread themselves, while others can also damage your computer system and data.

Web Application Firewall (WAF)

A device or software module that applies a set of policy rules to incoming traffic to block potential attacks on a Web application. Also known as a WAF.

Whitelist

When performing input validation, the set of items that, if matched, results in the input being accepted as valid. If there is no match to the whitelist, then the input is considered invalid. That is, a whitelist uses a 'default deny' policy.

Worm

Adapted from The Shockwave Rider, a science fiction novel. An often malicious program that can copy and propagate itself over the Internet using email programs or other transport tools. May also compromise the security of an infected computer or cause system and data damage