**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.

**Bandwidth**

Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.

**Banner**

A banner is the information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorized use.

**Basic Authentication**

Basic Authentication is the simplest web-based authentication scheme that works by sending the username and password with each request.

**Bastion Host**

A bastion host has been hardened in anticipation of vulnerabilities that have not been discovered yet.

**BIND**

BIND stands for Berkeley Internet Name Domain and is an implementation of DNS. DNS is used for domain name to IP address resolution.

**Biometrics**

Biometrics use physical characteristics of the users to determine access.

**Bit**

The smallest unit of information storage; a contraction of the term "binary digit;" one of two symbolsÑ"0" (zero) and "1" (one) - that are used to represent binary numbers.

**Block Cipher**

A block cipher encrypts one block of data at a time.

**Boot Record Infector**

A boot record infector is a piece of malware that inserts malicious code into the boot sector of a disk.

**Border Gateway Protocol (BGP)**

An inter-autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).

**Botnet**

A botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack.

**Bridge**

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).

**British Standard 7799**

A standard code of practice and provides guidance on how to secure an information system. It includes the management framework, objectives, and control requirements for information security management systems.

**Broadcast**

To simultaneously send the same message to multiple recipients. One host to all hosts on network.

**Broadcast Address**

An address used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

**Browser**

A client computer program that can retrieve and display information from servers on the World Wide Web.

**Brute Force**

A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

**Buffer Overflow**

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

**Business Continuity Plan (BCP)**

A Business Continuity Plan is the plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

**Business Impact Analysis (BIA)**

A Business Impact Analysis determines what levels of impact to a system are tolerable.

**Byte**

A fundamental unit of computer storage; the smallest addressable unit in a computer's architecture. Usually holds one character of information and usually means eight bits.