Glossary of Security Terms

Become your company's cyber security thesaurus. Find the definition of the most commonly used cyber security terms in our glossary below.

A-B

Access Control
Access Control ensures that resources are only granted to those users who are entitled to them.

Access Control List (ACL)
A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Control Service
A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

Access Management Access
Management is the maintenance of access information which consists of four tasks: account administration, maintenance, monitoring, and revocation.

Access Matrix
An Access Matrix uses rows to represent subjects and columns to represent objects with privileges listed in each cell.

Account Harvesting
Account Harvesting is the process of collecting all the legitimate account names on a system.

ACK Piggybacking
ACK piggybacking is the practice of sending an ACK inside another packet going to the same destination.

Active Content
Program code embedded in the contents of a web page. When the page is accessed by a web browser, the embedded code is automatically downloaded and executed on the user's workstation. Ex. Java, ActiveX (MS)

Activity Monitors
Activity monitors aim to prevent virus infection by monitoring for malicious activity on a system, and blocking that activity when possible.

Address Resolution Protocol (ARP)
Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

Advanced Encryption Standard (AES)
An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.

Algorithm
A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer.

Applet
Java programs; an application program that uses the client's web browser to provide a user interface.

ARPANET
Advanced Research Projects Agency Network, a pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990.

Asymmetric Cryptography
Public-key cryptography; A modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

Asymmetric Warfare
Asymmetric warfare is the fact that a small investment, properly leveraged, can yield incredible results.

Auditing
Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

Authentication
Authentication is the process of confirming the correctness of the claimed identity.

Authenticity
Authenticity is the validity and conformance of the original information.

Authorization
Authorization is the approval, permission, or empowerment for someone or something to do something.

Autonomous System
One network or series of networks that are all under one administrative control. An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

Availability
Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

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 symbolsN"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.

Blue Team
The people who perform defensive cybersecurity tasks, including placing and configuring firewalls, implementing patching programs, enforcing strong authentication, ensuring physical security measures are adequate and a long list of similar undertakings.

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.

C-D

Cache
Pronounced cash, a special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

Cache Cramming
Cache Cramming is the technique of tricking a browser to run cached Java code from the local disk, instead of the internet zone, so it runs with less restrictive permissions.

Cache Poisoning
Malicious or misleading data from a remote name server is saved [cached] by another name server. Typically used with DNS cache poisoning attacks.

Call Admission Control (CAC)
The inspection and control all inbound and outbound voice network activity by a voice firewall based on user-defined policies.

Cell
A cell is a unit of data transmitted over an ATM network.

Certificate-Based Authentication
Certificate-Based Authentication is the use of SSL and certificates to authenticate and encrypt HTTP traffic.

CGI
Common Gateway Interface. This mechanism is used by HTTP servers (web servers) to pass parameters to executable scripts in order to generate responses dynamically.

Chain of Custody
Chain of Custody is the important application of the Federal rules of evidence and its handling.

Challenge-Handshake Authentication Protocol (CHAP)
The Challenge-Handshake Authentication Protocol uses a challenge/response authentication mechanism where the response varies every challenge to prevent replay attacks.

Checksum
A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

Cipher
A cryptographic algorithm for encryption and decryption.

Ciphertext
Ciphertext is the encrypted form of the message being sent.

Circuit Switched Network
A circuit switched network is where a single continuous physical circuit connected two endpoints where the route was immutable once set up.

Client
A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

Cloud Computing
Utilization of remote servers in the data-center of a cloud provider to store, manage, and process your data instead of using local computer systems.

Cold/Warm/Hot Disaster Recovery Site
* Hot site. It contains fully redundant hardware and software, with telecommunications, telephone and utility connectivity to continue all primary site operations. Failover occurs within minutes or hours, following a disaster. Daily data synchronization usually occurs between the primary and hot site, resulting in minimum or no data loss. Offsite data backup

tapes might be obtained and delivered to the hot site to help restore operations. Backup tapes should be regularly tested to detect data corruption, malicious code and environmental damage. A hot site is the most expensive option. * Warm site. It contains partially redundant hardware and software, with telecommunications, telephone and utility connectivity to continue some, but not all primary site operations. Failover occurs within hours or days, following a disaster. Daily or weekly data synchronization usually occurs between the primary and warm site, resulting in minimum data loss. Offsite data backup tapes must be obtained and delivered to the warm site to restore operations. A warm site is the second most expensive option. * Cold site. Hardware is ordered, shipped and installed, and software is loaded. Basic telecommunications, telephone and utility connectivity might need turning on to continue some, but not all primary site operations. Relocation occurs within weeks or longer, depending on hardware arrival time, following a disaster. No data synchronization occurs between the primary and cold site, and could result in significant data loss. Offsite data backup tapes must be obtained and delivered to the cold site to restore operations. A cold site is the least expensive option.

Collision
A collision occurs when multiple systems transmit simultaneously on the same wire.

Competitive Intelligence
Competitive Intelligence is espionage using legal, or at least not obviously illegal, means.

Computer Emergency Response Team (CERT)
An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

Computer Network
A collection of host computers together with the sub-network or inter-network through which they can exchange data.

Confidentiality
Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

Configuration Management
Establish a known baseline condition and manage it.

Cookie
Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent client-side state information for HTTP-based applications, retrieving the state information in later connections.

Corruption
A threat action that undesirably alters system operation by adversely modifying system functions or data.

Cost Benefit Analysis
A cost benefit analysis compares the cost of implementing countermeasures with the value of the reduced risk.

Countermeasure
Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion Prevention Systems (IPS) commonly employ countermeasures to prevent intruders form gaining further access to a computer network. Other counter measures are patches, access control lists and malware filters.

Covert Channels
Covert Channels are the means by which information can be communicated between two parties in a covert fashion using normal system operations. For example by changing the amount of hard drive space that is available on a file server can be used to communicate information.

Crimeware
A type of malware used by cyber criminals. The malware is designed to enable the cyber criminal to make money off of the infected system (such as harvesting key strokes, using the infected systems to launch Denial of Service Attacks, etc.).

Cron
Cron is a Unix application that runs jobs for users and administrators at scheduled times of the day.

Crossover Cable
A crossover cable reverses the pairs of cables at the other end and can be used to connect devices directly together.

Cryptanalysis
The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the cipher text to plaintext without knowing the key.

Cryptographic Algorithm or Hash
An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.

Cut-Through
Cut-Through is a method of switching where only the header of a packet is read before it is forwarded to its destination.

Cyclic Redundancy Check (CRC)
Sometimes called "cyclic redundancy code." A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

Daemon
A program which is often started at the time the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. The term daemon is a Unix term, though many other operating systems provide support for daemons, though they're sometimes called other names. Windows, for example, refers to daemons and System Agents and services.

Data Aggregation
Data Aggregation is the ability to get a more complete picture of the information by analyzing several different types of records at once.

Data Custodian
A Data Custodian is the entity currently using or manipulating the data, and therefore, temporarily taking responsibility for the data.

Data Encryption Standard (DES)
A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Data Mining
Data Mining is a technique used to analyze existing information, usually with the intention of pursuing new avenues to pursue business.

Data Owner
A Data Owner is the entity having responsibility and authority for the data.

Data Warehousing
Data Warehousing is the consolidation of several previously independent databases into one location.

Datagram
Request for Comment 1594 says, "a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network." The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports. A datagram or packet needs to be self-contained without reliance on earlier

exchanges because there is no connection of fixed duration between the two communicating points as there is, for example, in most voice telephone conversations. (This kind of protocol is referred to as connectionless.)

Day Zero
The "Day Zero" or "Zero Day" is the day a new vulnerability is made known. In some cases, a "zero day" exploit is referred to an exploit for which no patch is available yet. ("day one"-> day at which the patch is made available).

Decapsulation
Decapsulation is the process of stripping off one layer's headers and passing the rest of the packet up to the next higher layer on the protocol stack.

Decryption
Decryption is the process of transforming an encrypted message into its original plaintext.

Defacement
Defacement is the method of modifying the content of a website in such a way that it becomes "vandalized" or embarrassing to the website owner.

Defense In-Depth
Defense In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.

Demilitarized Zone (DMZ)
In computer security, in general a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy. DMZ's provide either a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination. In some cases, a screened subnet which is used for servers accessible from the outside is referred to as a DMZ.

Denial of Service
The prevention of authorized access to a system resource or the delaying of system operations and functions.

Dictionary Attack
An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

Diffie-Hellman
A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

Digest Authentication
Digest Authentication allows a web client to compute MD5 hashes of the password to prove it has the password.

Digital Certificate
A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Digital Envelope
A digital envelope is an encrypted message with the encrypted session key.

Digital Signature
A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

Digital Signature Algorithm (DSA)
An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Digital Signature Standard (DSS)
The US Government standard that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

Disassembly
The process of taking a binary program and deriving the source code from it.

Disaster Recovery Plan (DRP)
A Disaster Recovery Plan is the process of recovery of IT systems in the event of a disruption or disaster.

Discretionary Access Control (DAC)
Discretionary Access Control consists of something the user can manage, such as a document password.

Disruption
A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Distance Vector
Distance vectors measure the cost of routes to determine the best route to all known networks.

Distributed Scans
Distributed Scans are scans that use multiple source addresses to gather information.

Domain
A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

Domain Hijacking
Domain hijacking is an attack by which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

Domain Name
A domain name locates an organization or other entity on the Internet. For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www". The "org" part of the domain name reflects the purpose of the organization or entity (in this example, "organization") and is called the top-level domain name. The "sans" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name.

Domain Name System (DNS)
The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Due Care
Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

Due Diligence
Due diligence is the requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

DumpSec
DumpSec is a security tool that dumps a variety of information about a system's users, file system, registry, permissions, password policy, and services.

Dumpster Diving
Dumpster Diving is obtaining passwords and corporate directories by searching through discarded media.

Dynamic Link Library
A collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file).

Dynamic Routing Protocol
Allows network devices to learn routes. Ex. RIP, EIGRP Dynamic routing occurs when routers talk to adjacent routers, informing each other of what networks each router is currently connected to. The routers must communicate using a routing protocol, of which there are many to choose from. The process on the router that is running the routing protocol, communicating with its neighbor routers, is usually called a routing daemon. The routing daemon updates the kernel's routing table with information it receives from neighbor routers.

E-F

Eavesdropping
Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to a facility or network.

Echo Reply
An echo reply is the response a machine that has received an echo request sends over ICMP.

Echo Request
An echo request is an ICMP message sent to a machine to determine if it is online and how long traffic takes to get to it.

Egress Filtering
Filtering outbound traffic.

Emanations Analysis
Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Encapsulation
The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

Encryption
Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Ephemeral Port
Also called a transient port or a temporary port. Usually is on the client side. It is set up when a client application wants to connect to a server and is destroyed when the client application terminates. It has a number chosen at random that is greater than 1023.

Escrow Passwords
Escrow Passwords are passwords that are written down and stored in a secure location (like a safe) that are used by emergency personnel when privileged personnel are unavailable.

Ethernet
The most widely-installed LAN technology. Specified in a standard, IEEE 802.3, an Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Devices are connected to the cable and compete for access using a CSMA/CD protocol.

Event
An event is an observable occurrence in a system or network.

Exponential Backoff Algorithm
An exponential backoff algorithm is used to adjust TCP timeout values on the fly so that network devices don't continue to timeout sending data over saturated links.

Exposure
A threat action whereby sensitive data is directly released to an unauthorized entity.

Extended ACLs (Cisco)
Extended ACLs are a more powerful form of Standard ACLs on Cisco routers. They can make filtering decisions based on IP addresses (source or destination), Ports (source or destination), protocols, and whether a session is established.

Extensible Authentication Protocol (EAP)
A framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialog sequences.

Exterior Gateway Protocol (EGP)
A protocol which distributes routing information to the routers which connect autonomous systems.

False Rejects
False Rejects are when an authentication system fails to recognize a valid user.

Fast File System
The first major revision to the Unix file system, providing faster read access and faster

(delayed, asynchronous) write access through a disk cache and better file system layout on disk. It uses inodes (pointers) and data blocks.

Fast Flux
Protection method used by botnets consisting of a continuous and fast change of the DNS records for a domain name through different IP addresses.

Fault Line Attacks
Fault Line Attacks use weaknesses between interfaces of systems to exploit gaps in coverage.

File Transfer Protocol (FTP)
A TCP/IP protocol specifying the transfer of text or binary files across the network.

Filter
A filter is used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

Filtering Router
An inter-network router that selectively prevents the passage of data packets according to a security policy. A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forward it on a second network. A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. The policy is implemented by rules (packet filters) loaded into the router.

Finger
A protocol to lookup user information on a given host. A Unix program that takes an e-mail address as input and returns information about the user who owns that e-mail address. On some systems, finger only reports whether the user is currently logged on. Other systems return additional information, such as the user's full name, address, and telephone number. Of course, the user must first enter this information into the system. Many e-mail programs now have a finger utility built into them.

Fingerprinting
Sending strange packets to a system in order to gauge how it responds to determine the operating system.

Firewall
A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

Flooding
An attack that attempts to cause a failure in (especially, in the security of) a computer

system or other data processing entity by providing more input than the entity can process properly.

Forest
A forest is a set of Active Directory domains that replicate their databases with each other.

Fork Bomb
A Fork Bomb works by using the fork() call to create a new process which is a copy of the original. By doing this repeatedly, all available processes on the machine can be taken up.

Form-Based Authentication
Form-Based Authentication uses forms on a webpage to ask a user to input username and password information.

Forward Lookup
Forward lookup uses an Internet domain name to find an IP address

Forward Proxy
Forward Proxies are designed to be the server through which all requests are made.

Fragment Offset
The fragment offset field tells the sender where a particular fragment falls in relation to other fragments in the original larger packet.

Fragment Overlap Attack
A TCP/IP Fragmentation Attack that is possible because IP allows packets to be broken down into fragments for more efficient transport across various media. The TCP packet (and its header) are carried in the IP packet. In this attack the second fragment contains incorrect offset. When packet is reconstructed, the port number will be overwritten.

Fragmentation
The process of storing a data file in several "chunks" or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

Frames
Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that "frame" the data. (Some control frames contain no data.)

Full Duplex
A type of duplex communications channel which carries data in both directions at once. Refers to the transmission of data in two directions simultaneously. Communications in which both sender and receiver can send at the same time.

Fully-Qualified Domain Name
A Fully-Qualified Domain Name is a server name with a hostname followed by the full domain

name.

Fuzzing
The use of special regression testing tools to generate out-of-spec input for an application in order to find security vulnerabilities. Also see "regression testing".

G-H

Gateway
A network point that acts as an entrance to another network.

gethostbyaddr
The gethostbyaddr DNS query is when the address of a machine is known and the name is needed.

gethostbyname
The gethostbyname DNS quest is when the name of a machine is known and the address is needed.

GNU
GNU is a Unix-like operating system that comes with source code that can be copied, modified, and redistributed. The GNU project was started in 1983 by Richard Stallman and others, who formed the Free Software Foundation.

Gnutella
An Internet file sharing utility. Gnutella acts as a server for sharing files while simultaneously acting as a client that searches for and downloads files from other users.

Hardening
Hardening is the process of identifying and fixing vulnerabilities on a system.

Hash Function
An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.

Hash Functions
(cryptographic) hash functions are used to generate a one way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a

larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHA1.

Header
A header is the extra information in a packet that is needed for the protocol stack to process the packet.

Hijack Attack
A form of active wiretapping in which the attacker seizes control of a previously established communication association.

Honey Client
see Honeymonkey.

Honey pot
Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

Honeymonkey
Automated system simulating a user browsing websites. The system is typically configured to detect web sites which exploit vulnerabilities in the browser. Also known as Honey Client.

Hops
A hop is each exchange with a gateway a packet takes on its way to the destination.

Host
Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

Host-Based ID
Host-based intrusion detection systems use information from the operating system audit records to watch all operations occurring on the host that the intrusion detection software has been installed upon. These operations are then compared with a pre-defined security policy. This analysis of the audit trail imposes potentially significant overhead requirements on the system because of the increased amount of processing power which must be utilized by the intrusion detection system. Depending on the size of the audit trail and the processing ability of the system, the review of audit data could result in the loss of a real-time analysis capability.

HTTP Proxy
An HTTP Proxy is a server that acts as a middleman in the communication between HTTP clients and servers.

HTTPS
When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.

Hub
A hub is a network device that operates by repeating data that it receives on one port to all the other ports. As a result, data transmitted by one host is retransmitted to all other hosts on the hub.

Hybrid Attack
A Hybrid Attack builds on the dictionary attack method by adding numerals and symbols to dictionary words.

Hybrid Encryption
An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.

Hyperlink
In hypertext or hypermedia, an information object (such as a word, a phrase, or an image; usually highlighted by color or underscoring) that points (indicates how to connect) to related information that is located elsewhere and can be retrieved by activating the link.

Hypertext Markup Language (HTML)
The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

Hypertext Transfer Protocol (HTTP)
The protocol in the Internet Protocol (IP) family used to transport hypertext documents across an internet.

I-K

Identity
Identity is whom someone or what something is, for example, the name by which something is known.

Incident
An incident as an adverse network event in an information system or network or the threat of the occurrence of such an event.

Incident Handling
Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Incremental Backups
Incremental backups only backup the files that have been modified since the last backup. If dump levels are used, incremental backups only backup files changed since last backup of a lower dump level.

Inetd (xinetd)
Inetd (or Internet Daemon) is an application that controls smaller internet services like telnet, ftp, and POP.

Inference Attack
Inference Attacks rely on the user to make logical connections between seemingly unrelated pieces of information.

Information Warfare
Information Warfare is the competition between offensive and defensive players over information resources.

Ingress Filtering
Ingress Filtering is filtering inbound traffic.

Input Validation Attacks
Input Validations Attacks are where an attacker intentionally sends unusual input in the hopes of confusing an application.

Integrity
Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

Integrity Star Property
In Integrity Star Property a user cannot read data of a lower integrity level then their own.

Internet
A term to describe connecting multiple separate networks together.

Internet Control Message Protocol (ICMP)
An Internet Standard protocol that is used to report error conditions during IP datagram processing and to exchange other information concerning the state of the IP network.

Internet Engineering Task Force (IETF)
The body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership.

Internet Message Access Protocol (IMAP)
A protocol that defines how a client should fetch mail from and return mail to a mail server. IMAP is intended as a replacement for or extension to the Post Office Protocol (POP). It is defined in RFC 1203 (v3) and RFC 2060 (v4).

Internet Protocol (IP)
The method or protocol by which data is sent from one computer to another on the Internet.

Internet Protocol Security (IPsec)
A developing standard for security at the network or packet processing layer of network communication.

Internet Standard
A specification, approved by the IESG and published as an RFC, that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet.

Interrupt
An Interrupt is a signal that informs the OS that something has occurred.

Intranet
A computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.

Intrusion Detection
A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IP Address
A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP Flood
A denial of service attack that sends a host more echo request ("ping") packets than the protocol implementation can handle.

IP Forwarding
IP forwarding is an Operating System option that allows a host to act as a router. A system that has more than 1 network interface card must have IP forwarding turned on in order for the system to be able to act as a router.

IP Spoofing
The technique of supplying a false IP address.

ISO
International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

Issue-Specific Policy
An Issue-Specific Policy is intended to address specific needs within an organization, such as a password policy.

ITU-T
International Telecommunications Union, Telecommunication Standardization Sector (formerly "CCITT"), a United Nations treaty organization that is composed mainly of postal, telephone, and telegraph authorities of the member countries and that publishes standards called "Recommendations."

Jitter
Jitter or Noise is the modification of fields in a database while preserving the aggregate characteristics of that make the database useful in the first place.

Jump Bag
A Jump Bag is a container that has all the items necessary to respond to an incident inside to help mitigate the effects of delayed reactions.

Kerberos
A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment.

Kernel
The essential center of a computer operating system, the core that provides basic services for all other parts of the operating system. A synonym is nucleus. A kernel can be contrasted with a shell, the outermost part of an operating system that interacts with user commands. Kernel and shell are terms used more frequently in Unix and some other operating systems than in IBM mainframe systems.

L-M

Lattice Techniques
Lattice Techniques use security designations to determine access to information.

Layer 2 Forwarding Protocol (L2F)
An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user.

Layer 2 Tunneling Protocol (L2TP)
An extension of the Point-to-Point Tunneling Protocol used by an Internet service provider to enable the operation of a virtual private network over the Internet.

Least Privilege
Least Privilege is the principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

Legion
Software to detect unprotected shares.

Lightweight Directory Access Protocol (LDAP)
A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.

Link State
With link state, routes maintain information about all routers and router-to-router links within a geographic area, and creates a table of best routes with that information.

List Based Access Control
List Based Access Control associates a list of users and their privileges with each object.

Loadable Kernel Modules (LKM)
Loadable Kernel Modules allow for the adding of additional functionality directly into the kernel while the system is running.

Log Clipping
Log clipping is the selective removal of log entries from a system log to hide a compromise.

Logic bombs
Logic bombs are programs or snippets of code that execute when a certain predefined event occurs. Logic bombs may also be set to go off on a certain date or when a specified set of circumstances occurs.

Logic Gate
A logic gate is an elementary building block of a digital circuit. Most logic gates have two inputs and one output. As digital circuits can only understand binary, inputs and outputs can assume only one of two states, 0 or 1.

Loopback Address
The loopback address (127.0.0.1) is a pseudo IP address that always refer back to the local host and are never sent out onto a network.

MAC Address
A physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

Malicious Code
Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

Malware
A generic term for a number of different types of malicious code.

Mandatory Access Control (MAC)
Mandatory Access Control controls is where the system controls access to resources based on classification levels assigned to both the objects and the users. These controls cannot be changed by anyone.

Masquerade Attack
A type of attack in which one system entity illegitimately poses as (assumes the identity of) another entity.

md5
A one way cryptographic hash function. Also see "hash functions" and "sha1"

Measures of Effectiveness (MOE)
Measures of Effectiveness is a probability model based on engineering concepts that allows one to approximate the impact a give action will have on an environment. In Information warfare it is the ability to attack or defend within an Internet environment.

Monoculture
Monoculture is the case where a large number of users run the same software, and are vulnerable to the same attacks.

Morris Worm
A worm program written by Robert T. Morris, Jr. that flooded the ARPANET in November, 1988, causing problems for thousands of hosts.

Multi-Cast
Broadcasting from one host to a given set of hosts.

Multi-Homed
You are "multi-homed" if your network is directly connected to two or more ISP's.

Multiplexing
To combine multiple signals from possibly disparate sources, in order to transmit them over a single path.

N-O

NAT
Network Address Translation. It is used to share one or a small number of publicly routable IP addresses among a larger number of hosts. The hosts are assigned private IP addresses, which are then "translated" into one of the publicly routed IP addresses. Typically home or small business networks use NAT to share a single DLS or Cable modem IP address. However, in some cases NAT is used for servers as an additional layer of protection.

National Institute of Standards and Technology (NIST)
National Institute of Standards and Technology, a unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

Natural Disaster
Any "act of God" (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component.

Netmask
32-bit number indicating the range of IP addresses residing on a single IP network/subnet/supernet. This specification displays network masks as hexadecimal numbers. For example, the network mask for a class C IP network is displayed as 0xffffff00. Such a mask is often displayed elsewhere in the literature as 255.255.255.0.

Network Address Translation
The translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

Network Mapping
To compile an electronic inventory of the systems and the services on your network.

Network Taps
Network taps are hardware devices that hook directly onto the network cable and send a copy of the traffic that passes through it to one or more other networked devices.

Network-Based IDS
A network-based IDS system monitors the traffic on its network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network traffic on other segments, and traffic on other means of communication (like phone lines) can't be monitored. Network-based IDS involves looking at the packets on the network as they pass by some sensor. The sensor can only see the packets that happen to be carried on the network segment it's attached to. Packets are considered to be of interest if they match a signature.Network-based intrusion detection passively monitors network activity for indications of attacks. Network monitoring offers several advantages over traditional host-based intrusion detection systems. Because many intrusions occur over networks at some point, and because networks are increasingly becoming the targets of attack, these techniques are an excellent method of detecting many attacks which may be missed by host-based intrusion detection mechanisms.

Non-Printable Character
A character that doesn't have a corresponding character letter to its corresponding ASCII code. Examples would be the Linefeed, which is ASCII character code 10 decimal, the Carriage Return, which is 13 decimal, or the bell sound, which is decimal 7. On a PC, you can often add non-printable characters by holding down the Alt key, and typing in the decimal value (i.e., Alt-007 gets you a bell). There are other character encoding schemes, but ASCII is the most prevalent.

Non-Repudiation
Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

Null Session
Known as Anonymous Logon, it is a way of letting an anonymous user retrieve information such as user names and shares over the network or connect without authentication. It is used by applications such as explorer.exe to enumerate shares on remote servers.

Octet
A sequence of eight bits. An octet is an eight-bit byte.

One-Way Encryption
Irreversible transformation of plaintext to cipher text, such that the plaintext cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known.

One-Way Function
A (mathematical) function, f, which is easy to compute the output based on a given input. However given only the output value it is impossible (except for a brute force attack) to figure out what the input value is.

Open Shortest Path First (OSPF)
Open Shortest Path First is a link state routing algorithm used in interior gateway routing. Routers maintain a database of all routers in the autonomous system with links between the routers, link costs, and link states (up and down).

OSI
OSI (Open Systems Interconnection) is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication. Although OSI is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the OSI model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion.

OSI layers
The main idea in OSI is that the process of communication between two end points in a telecommunication network can be divided into layers, with each layer adding its own set of special, related functions. Each communicating user or program is at a computer equipped with these seven layers of function. So, in a given message between users, there will be a flow of data through each layer at one end down through the layers in that computer and, at the other end, when the message arrives, another flow of data up through the layers in the receiving computer and ultimately to the end user or program. The actual programming and hardware that furnishes these seven layers of function is usually a combination of the computer operating system, applications (such as your Web browser), TCP/IP or alternative transport and network protocols, and the software and hardware that enable you to put a signal on one of the lines attached to your computer. OSI divides telecommunication into seven layers. The layers are in two groups. The upper four layers are used whenever a message passes from or to a user. The lower three layers (up to the network layer) are used when any message passes through the host computer or router. Messages intended for this computer pass to the upper layers. Messages destined for some other host are not passed

up to the upper layers but are forwarded to another host. The seven layers are: Layer 7: The application layer...This is the layer at which communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. (This layer is not the application itself, although some applications may perform application layer functions.) Layer 6: The presentation layer...This is a layer, usually part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). Sometimes called the syntax layer. Layer 5: The session layer...This layer sets up, coordinates, and terminates conversations, exchanges, and dialogs between the applications at each end. It deals with session and connection coordination. Layer 4: The transport layer...This layer manages the end-to-end control (for example, determining whether all packets have arrived) and error-checking. It ensures complete data transfer. Layer 3: The network layer...This layer handles the routing of the data (sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level). The network layer does routing and forwarding. Layer 2: The data-link layer...This layer provides synchronization for the physical level and does bit-stuffing for strings of 1's in excess of 5. It furnishes transmission protocol knowledge and management. Layer 1: The physical layer...This layer conveys the bit stream through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier.

Overload
Hindrance of system operation by placing excess burden on the performance capabilities of a system component.

P-Q

Packet
A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Packet Switched Network
A packet switched network is where individual packets each follow their own paths through the network from one endpoint to another.

Partitions
Major divisions of the total physical hard disk space.

Password Authentication Protocol (PAP)
Password Authentication Protocol is a simple, weak authentication mechanism where a user enters the password and it is then sent across the network, usually in the clear.

Password Cracking
Password cracking is the process of attempting to guess passwords, given the password file information.

Password Sniffing
Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Patch
A patch is a small update released by a software manufacturer to fix bugs in existing programs.

Patching
Patching is the process of updating software to a different version.

Payload
Payload is the actual application data a packet contains.

Penetration
Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Penetration Testing
Penetration testing is used to test the external perimeter security of a network or facility.

Permutation
Permutation keeps the same letters but changes the position within a text to scramble the message.

Personal Firewalls
Personal firewalls are those firewalls that are installed and run on individual PCs.

Pharming
This is a more sophisticated form of MITM attack. A user's session is redirected to a masquerading website. This can be achieved by corrupting a DNS server on the Internet and pointing a URL to the masquerading website's IP. Almost all users use a URL like www.worldbank.com instead of the real IP (192.86.99.140) of the website. Changing the pointers on a DNS server, the URL can be redirected to send traffic to the IP of the pseudo website. At the pseudo website, transactions can be mimicked and information like login credentials can be gathered. With this the attacker can access the real www.worldbank.com site and conduct transactions using the credentials of a valid user on that website.

Phishing
The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.

Ping of Death
An attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.

Ping Scan
A ping scan looks for machines that are responding to ICMP Echo Requests.

Ping Sweep
An attack that sends ICMP echo requests ("pings") to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities.

Plaintext
Ordinary readable text before being encrypted into ciphertext or after being decrypted.

Point-to-Point Protocol (PPP)
A protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. It packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

Point-to-Point Tunneling Protocol (PPTP)
A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet.

Poison Reverse
Split horizon with poisoned reverse (more simply, poison reverse) does include such routes in updates, but sets their metrics to infinity. In effect, advertising the fact that there routes are not reachable.

Polyinstantiation
Polyinstantiation is the ability of a database to maintain multiple records with the same key. It is used to prevent inference attacks.

Polymorphism
Polymorphism is the process by which malicious software changes its underlying code to avoid detection.

Port
A port is nothing more than an integer that uniquely identifies an endpoint of a communication stream. Only one process per machine can listen on the same port number.

Port Scan
A port scan is a series of messages sent by someone attempting to break into a computer to

learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

Possession
Possession is the holding, control, and ability to use information.

Post Office Protocol, Version 3 (POP3)
An Internet Standard protocol by which a client workstation can dynamically access a mailbox on a server host to retrieve mail messages that the server has received and is holding for the client.

Practical Extraction and Reporting Language (Perl)
A script programming language that is similar in syntax to the C language and that includes a number of popular Unix facilities such as sed, awk, and tr.

Preamble
A preamble is a signal used in network communications to synchronize the transmission timing between two or more systems. Proper timing ensures that all systems are interpreting the start of the information transfer correctly. A preamble defines a specific series of transmission pulses that is understood by communicating systems to mean "someone is about to transmit data". This ensures that systems receiving the information correctly interpret when the data transmission starts. The actual pulses used as a preamble vary depending on the network communication technology in use.

Pretty Good Privacy (PGP)TM
Trademark of Network Associates, Inc., referring to a computer program (and related protocols) that uses cryptography to provide data security for electronic mail and other applications on the Internet.

Private Addressing
IANA has set aside three address ranges for use by private or non-Internet connected networks. This is referred to as Private Address Space and is defined in RFC 1918. The reserved address blocks are: 10.0.0.0 to 10.255.255.255 (10/8 prefix) 172.16.0.0 to 172.31.255.255 (172.16/12 prefix) 192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

Program Infector
A program infector is a piece of malware that attaches itself to existing program files.

Program Policy
A program policy is a high-level policy that sets the overall tone of an organization's security approach.

Promiscuous Mode
When a machine reads all packets off the network, regardless of who they are addressed to. This is used by network administrators to diagnose network problems, but also by unsavory characters who are trying to eavesdrop on network traffic (which might contain passwords or other information).

Proprietary Information
Proprietary information is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

Protocol
A formal specification for communicating; an IP address the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection.

Protocol Stacks (OSI)
A set of network protocol layers that work together.

Proxy Server
A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Public Key
The publicly-disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

Public Key Encryption
The popular synonym for "asymmetric cryptography".

Public Key Infrastructure (PKI)
A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

Public-Key Forward Secrecy (PFS)
For a key agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

QAZ
A network worm.

R-S

Race Condition
A race condition exploits the small window of time between a security control being applied and when the service is used.

Radiation Monitoring
Radiation monitoring is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.

Ransomware
A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.

Reconnaissance
Reconnaissance is the phase of an attack where an attackers finds new systems, maps out networks, and probes for specific, exploitable vulnerabilities.

Reflexive ACLs (Cisco)
Reflexive ACLs for Cisco routers are a step towards making the router act like a stateful firewall. The router will make filtering decisions based on whether connections are a part of established traffic or not.

Registry
The Registry in Windows operating systems in the central set of settings and information required to run the Windows computer.

regression analysis
The use of scripted tests which are used to test software for all possible input is should expect. Typically developers will create a set of regression tests that are executed before a new version of a software is released. Also see "fuzzing".

Request for Comment (RFC)
A series of notes about the Internet, started in 1969 (when the Internet was the ARPANET).

An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard.

Resource Exhaustion
Resource exhaustion attacks involve tying up finite resources on a system, making them unavailable to others.

Response
A response is information sent that is responding to some stimulus.

Reverse Address Resolution Protocol (RARP)
RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

Reverse Engineering
Acquiring sensitive data by disassembling and analyzing the design of a system component.

Reverse Lookup
Find out the hostname that corresponds to a particular IP address. Reverse lookup uses an IP (Internet Protocol) address to find a domain name.

Reverse Proxy
Reverse proxies take public HTTP requests and pass them to back-end webservers to send the content to it, so the proxy can then send the content to the end-user.

Risk
Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.

Risk Assessment
A Risk Assessment is the process by which risks are identified and the impact of those risks determined.

Risk Averse
Avoiding risk even if this leads to the loss of opportunity. For example, using a (more expensive) phone call vs. sending an e-mail in order to avoid risks associated with e-mail may be considered "Risk Averse"

Rivest-Shamir-Adleman (RSA)
An algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

Role Based Access Control
Role based access control assigns users to roles based on their organizational functions and determines authorization based on those roles.

Root
Root is the name of the administrator account in Unix systems.

Rootkit
A collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.

Router
Routers interconnect logical networks by forwarding information to other networks based upon IP addresses.

Routing Information Protocol (RIP)
Routing Information Protocol is a distance vector protocol used for interior gateway routing which uses hop count as the sole metric of a path's cost.

Routing Loop
A routing loop is where two or more poorly configured routers repeatedly exchange the same packet over and over.

RPC Scans
RPC scans determine which RPC services are running on a machine.

Rule Set Based Access Control (RSBAC)
Rule Set Based Access Control targets actions based on rules for entities operating on objects.

S/Key
A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. The client generates a one-time password by applying the MD4 cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one.

Safety
Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors, are protected from harm.

Scavenging
Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

Secure Electronic Transactions (SET)
Secure Electronic Transactions is a protocol developed for credit card transactions in which all parties (customers, merchant, and bank) are authenticated using digital signatures, encryption protects the message and provides integrity, and provides end-to-end security for credit card transactions online.

Secure Shell (SSH)
A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

Secure Sockets Layer (SSL)
A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

Segment
Segment is another name for TCP packets.

Sensitive Information
Sensitive information, as defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives.

Separation of Duties
Separation of duties is the principle of splitting privileges among multiple individuals or systems.

Server
A system entity that provides a service in response to requests from other system entities called clients.

Session
A session is a virtual connection between two hosts by which network traffic is passed.

Session Hijacking
Take over a session that someone else has established.

Session Key
In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

SHA1
A one way cryptographic hash function. Also see "MD5"

Shadow Password Files
A system file in which encryption user password are stored so that they aren't available to people who try to break into the system.

Share
A share is a resource made public on a machine, such as a directory (file share) or printer (printer share).

Shell
A Unix term for the interactive user interface with an operating system. The shell is the layer of programming that understands and executes the commands a user enters. In some systems, the shell is called a command interpreter. A shell usually implies an interface with a command syntax (think of the DOS operating system and its "C:>" prompts and user commands such as "dir" and "edit").

Signals Analysis
Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Signature
A Signature is a distinct pattern in network traffic that can be identified to a specific tool or exploit.

Simple Integrity Property
In Simple Integrity Property a user cannot write data to a higher integrity level than their own.

Simple Network Management Protocol (SNMP)
The protocol governing network management and the monitoring of network devices and their functions. A set of protocols for managing complex networks.

Simple Security Property
In Simple Security Property a user cannot read data of a higher classification than their own.

Smartcard
A smartcard is an electronic badge that includes a magnetic strip or chip that can record and replay a set key.

Smurf
The Smurf attack works by spoofing the target address and sending a ping to the broadcast address for a remote network, which results in a large amount of ping replies being sent to the target.

Sniffer
A sniffer is a tool that monitors network traffic as it received in a network interface.

Sniffing
A synonym for "passive wiretapping."

Social Engineering
A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems.

Socket
The socket tells a host's IP stack where to plug in a data stream so that it connects to the right application.

Socket Pair
A way to uniquely specify a connection, i.e., source IP address, source port, destination IP address, destination port.

SOCKS
A protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet. SOCKS uses sockets to represent and keep track of individual connections. The client side of SOCKS is built into certain Web browsers and the server side can be added to a proxy server.

Software
Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

Source Port
The port that a host uses to connect to a server. It is usually a number greater than or equal to 1024. It is randomly generated and is different each time a connection is made.

Spam
Electronic junk mail or junk newsgroup postings.

Spanning Port
Configures the switch to behave like a hub for a specific port.

Split Horizon
Split horizon is a algorithm for avoiding problems caused by including routes in updates sent to the gateway from which they were learned.

Split Key
A cryptographic key that is divided into two or more separate data items that individually convey no knowledge of the whole key that results from combining the items.

Spoof
Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.

SQL Injection
SQL injection is a type of input validation attack specific to database-driven applications where SQL code is inserted into application queries to manipulate the database.

Stack Mashing
Stack mashing is the technique of using a buffer overflow to trick a computer into executing arbitrary code.

Standard ACLs (Cisco)
Standard ACLs on Cisco routers make packet filtering decisions based on Source IP address only.

Star Property
In Star Property, a user cannot write data to a lower classification level without logging in at that lower classification level.

State Machine
A system that moves through a series of progressive conditions.

Stateful Inspection
Also referred to as dynamic packet filtering. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

Static Host Tables
Static host tables are text files that contain hostname and address mapping.

Static Routing
Static routing means that routing table entries contain information that does not change.

Stealthing
Stealthing is a term that refers to approaches used by malicious code to conceal its presence on the infected system.

Steganalysis
Steganalysis is the process of detecting and defeating the use of steganography.

Steganography
Methods of hiding the existence of a message or other data. This is different than cryptography, which hides the meaning of a message but does not hide the message itself. An example of a steganographic method is "invisible" ink.

Stimulus
Stimulus is network traffic that initiates a connection or solicits a response.

Store-and-Forward
Store-and-Forward is a method of switching where the entire packet is read by a switch to determine if it is intact before forwarding it.

Straight-Through Cable
A straight-through cable is where the pins on one side of the connector are wired to the same pins on the other end. It is used for interconnecting nodes on the network.

Stream Cipher
A stream cipher works by encryption a message a single bit, byte, or computer word at a time.

Strong Star Property
In Strong Star Property, a user cannot write data to higher or lower classifications levels than their own.

Sub Network
A separately identifiable part of a larger network that typically represents a certain limited number of host computers, the hosts in a building or geographic area, or the hosts on an individual local area network.

Subnet Mask
A subnet mask (or number) is used to determine the number of bits used for the subnet and host portions of the address. The mask is a 32-bit value that uses one-bits for the network and subnet portions and zero-bits for the host portion.

Switch
A switch is a networking device that keeps track of MAC addresses attached to each of its ports so that data is only transmitted on the ports that are the intended recipient of the data.

Switched Network
A communications network, such as the public switched telephone network, in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices. Any network providing switched communications service.

Symbolic Links
Special files which point at another file.

Symmetric Cryptography
A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification). Symmetric cryptography is sometimes called "secret-key cryptography" (versus public-key cryptography) because the entities that share the key.

Symmetric Key
A cryptographic key that is used in a symmetric cryptographic algorithm.

SYN Flood
A denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.

Synchronization
Synchronization is the signal made up of a distinctive pattern of bits that network hardware looks for to signal that start of a frame.

Syslog
Syslog is the system logging facility for Unix systems.

System Security Officer (SSO)
A person responsible for enforcement or administration of the security policy that applies to the system.

System-Specific Policy
A System-specific policy is a policy written for a specific system or device.

T-U

T1, T3
A digital circuit using TDM (Time-Division Multiplexing).

Tamper
To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

TCP Fingerprinting
TCP fingerprinting is the user of odd packet header combinations to determine a remote operating system.

TCP Full Open Scan
TCP Full Open scans check each port by performing a full three-way handshake on each port to determine if it was open.

TCP Half Open Scan
TCP Half Open scans work by performing the first half of a three-way handshake to determine if a port is open.

TCP Wrapper
A software package which can be used to restrict access to certain network services based on the source of the connection; a simple tool to monitor and control incoming network traffic.

TCP/IP
A synonym for "Internet Protocol Suite;" in which the Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).

TCPDump
TCPDump is a freeware protocol analyzer for Unix that can monitor network traffic on a wire.

TELNET
A TCP-based, application-layer, Internet Standard protocol for remote login from one host to another.

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Threat Assessment
A threat assessment is the identification of types of threats that an organization might be exposed to.

Threat Model
A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability.

Threat Vector
The method a threat uses to get to the target.

Time to Live
A value in an Internet Protocol packet that tells a network router whether or not the packet has been in the network too long and should be discarded.

Tiny Fragment Attack
With many IP implementations it is possible to impose an unusually small fragment size on outgoing packets. If the fragment size is made small enough to force some of a TCP packet's TCP header fields into the second fragment, filter rules that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum

fragment size, a disallowed packet might be passed because it didn't hit a match in the filter. STD 5, RFC 791 states: Every Internet module must be able to forward a datagram of 68 octets without further fragmentation. This is because an Internet header may be up to 60 octets, and the minimum fragment is 8 octets.

Token Ring
A token ring network is a local area network in which all computers are connected in a ring or star topology and a binary digit or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time.

Token-Based Access Control
Token based access control associates a list of objects and their privileges with each user. (The opposite of list based.)

Token-Based Devices
A token-based device is triggered by the time of day, so every minute the password changes, requiring the user to have the token with them when they log in.

Topology
The geometric arrangement of a computer system. Common topologies include a bus, star, and ring. The specific physical, i.e., real, or logical, i.e., virtual, arrangement of the elements of a network. Note 1: Two networks have the same topology if the connection configuration is the same, although the networks may differ in physical interconnections, distances between nodes, transmission rates, and/or signal types. Note 2: The common types of network topology are illustrated

Traceroute (tracert.exe)
Traceroute is a tool the maps the route a packet takes from the local machine to a remote destination.

Transmission Control Protocol (TCP)
A set of rules (protocol) used along with the Internet Protocol to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Transport Layer Security (TLS)
A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.

Triple DES
A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the

Data Encryption Algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.

Triple-Wrapped
S/MIME usage: data that has been signed with a digital signature, and then encrypted, and then signed again.

Trojan Horse
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Trunking
Trunking is connecting switched together so that they can share VLAN information between them.

Trust
Trust determine which permissions and what actions other systems or users can perform on remote machines.

Trusted Ports
Trusted ports are ports below number 1024 usually allowed to be opened by the root user.

Tunnel
A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. Most often, a tunnel is a logical point-to-point link - i.e., an OSI layer 2 connection - created by encapsulating the layer 2 protocol in a transport protocol (such as TCP), in a network or inter-network layer protocol (such as IP), or in another link layer protocol. Tunneling can move data between computers that use a protocol not supported by the network connecting them.

UDP Scan
UDP scans perform scans to determine which UDP ports are open.

Unicast
Broadcasting from host to host.

Uniform Resource Identifier (URI)
The generic term for all types of names and addresses that refer to objects on the World Wide Web.

Uniform Resource Locator (URL)
The global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address

or the domain name where the resource is located. For example, http://www.pcwebopedia.com/ind... .

Unix
A popular multi-user, multitasking operating system developed at Bell Labs in the early 1970s. Created by just a handful of programmers, Unix was designed to be a small, flexible system used exclusively by programmers.

Unprotected Share
In Windows terminology, a "share" is a mechanism that allows a user to connect to file systems and printers on other systems. An "unprotected share" is one that allows anyone to connect to it.

User
A person, organization entity, or automated process that accesses a system, whether authorized to do so or not.

User Contingency Plan
User contingency plan is the alternative methods of continuing business operations if IT systems are unavailable.

User Datagram Protocol (UDP)
A communications protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network. UDP uses the Internet Protocol to get a datagram from one computer to another but does not divide a message into packets (datagrams) and reassemble it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in.

V-Z

Virtual Private Network (VPN)
A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall, the corporation could

create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

Virus
A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Voice Firewall
A physical discontinuity in a voice network that monitors, alerts and controls inbound and outbound voice network activity based on user-defined call admission control (CAC) policies, voice application layer security threats or unauthorized service use violations.

Voice Intrusion Prevention System (IPS)
Voice IPS is a security management system for voice networks which monitors voice traffic for multiple calling patterns or attack/abuse signatures to proactively detect and prevent toll fraud, Denial of Service, telecom attacks, service abuse, and other anomalous activity.

War Chalking
War chalking is marking areas, usually on sidewalks with chalk, that receive wireless signals that can be accessed.

War Dialer
A computer program that automatically dials a series of telephone numbers to find lines connected to computer systems, and catalogs those numbers so that a cracker can try to break into the systems.

War Dialing
War dialing is a simple means of trying to identify modems in a telephone exchange that may be susceptible to compromise in an attempt to circumvent perimeter security.

War Driving
War driving is the process of traveling around looking for wireless access point signals that can be used to get network access.

Web of Trust
A web of trust is the trust that naturally evolves as a user starts to trust other's signatures, and the signatures that they trust.

Web Server
A software process that runs on a host computer connected to the Internet to respond to HTTP requests for documents from client web browsers.

WHOIS
An IP for finding information about resources on networks.

Windowing
A windowing system is a system for sharing a computer's graphical display presentation resources among multiple applications at the same time. In a computer that has a graphical user interface (GUI), you may want to use a number of applications at the same time (this is called task). Using a separate window for each application, you can interact with each application and go from one application to another without having to reinitiate it. Having different information or activities in multiple windows may also make it easier for you to do your work. A windowing system uses a window manager to keep track of where each window is located on the display screen and its size and status. A windowing system doesn't just manage the windows but also other forms of graphical user interface entities.

Windump
Windump is a freeware tool for Windows that is a protocol analyzer that can monitor network traffic on a wire.

Wired Equivalent Privacy (WEP)
A security protocol for wireless local area networks defined in the standard IEEE 802.11b.

Wireless Application Protocol
A specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat.

Wiretapping
Monitoring and recording data that is flowing between two points in a communication system.

World Wide Web ("the Web", WWW, W3)
The global, hypermedia-based collection of information and services that is available on Internet servers and is accessed by browsers using Hypertext Transfer Protocol and other information retrieval mechanisms.

Worm
A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Zero Day
The "Day Zero" or "Zero Day" is the day a new vulnerability is made known. In some cases, a "zero day" exploit is referred to an exploit for which no patch is available yet. ("day one" - day at which the patch is made available).

Zero-day attack
A zero-day (or zero-hour or day zero) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the

software developer. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software developer knows about the vulnerability.

Zombies
A zombie computer (often shortened as zombie) is a computer connected to the Internet that has been compromised by a hacker, a computer virus, or a trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.

#

3-way handshake
Machine A sends a packet with a SYN flag set to Machine B. B acknowledges A's SYN with a SYN/ACK. A acknowledges B's SYN/ACK with an ACK.

Subscribe

Courses

Certifications

Degree Programs

Cyber Ranges

Job Tools

Security Policy Project

Posters & Cheat Sheets

White Papers

Focus Areas

Cyber Defense

Cloud Security

Cybersecurity Leadership

Digital Forensics

Industrial Control Systems

Offensive Operations