

# Glossary

This glossary contains the key terms from the book. All the terms from each chapter's "Define Key Terms" tasks are defined here.

**3-leg perimeter** A type of DMZ where a firewall has three legs that connect to the LAN, the Internet, and the DMZ.

**10 tape rotation** A backup rotation scheme in which ten backup tapes are used over the course of two weeks.

**802.1X** An authentication technology used to connect devices to a LAN or WLAN. It is an example of port-based network access control (NAC).

**acceptable use policy (AUP)** Policy that defines the rules that restrict how a computer, network, or other system may be used.

**access control list (ACL)** A list of permissions attached to an object specifying what level of access a user, users, or groups have to that object. When dealing with firewalls, an ACL is a set of rules that applies to a list of network names, IP addresses, and port numbers.

**access control model** Specifies methodologies by which admission to physical areas and, more importantly, computer systems is managed and organized.

**account expiration** The date when a user's account he uses to log on to the network expires.

**accounting** The tracking of data, computer usage, and network resources. Often it means logging, auditing, and monitoring of the data and resources.

**active interception** Normally refers to placing a computer between the sender and the receiver in an effort to capture and possibly modify information.

**active reconnaissance** Gaining information about a target system using active, engaging techniques.

**ad filtering** Ways of blocking and filtering out unwanted advertisements; pop-up blockers and content filters are considered to be ad filtering methods.

**address space layout randomization (ASLR)** A technique used to prevent the exploitation of memory vulnerabilities.

**Advanced Encryption Standard (AES)** A symmetric key encryption standard, used with WPA and WPA2, that is the successor to DES/3DES and is composed of three different block ciphers: AES-128, AES-192, and AES-256.

**advanced persistent threat (APT)** A set of computer-attacking processes that targets private organizations or nation states. Also refers to a group (often a government) that persistently targets a specific entity.

**adware** Type of spyware that pops up advertisements based on what it has learned about the user.

**agile model** A type of SDLC based on being adaptive to change, and cooperation between business people, customers, and developers. *See* software development life cycle (SDLC). *Compare with* waterfall model.

**air gap** A method of securing a control unit, system, or network through isolation and possibly shielding.

**algorithms** Well-defined instructions that describe computations from their initial state to their final state.

**always-on VPN** A method of VPN where the user can always access the connection without the need to periodically disconnect and reconnect. It often uses SSL/TLS for encrypted connections instead of PPTP or L2TP.

**anomaly-based monitoring** Also known as statistical anomaly-based monitoring, establishes a performance baseline based on a set of normal network traffic evaluations.

**AP isolation** Each client connected to the AP will not be able to communicate with each other, but they can each still access the Internet.

**application blacklisting** A method of disallowing one or more applications from use.

**application containerization** A virtualization method that allows an organization to run applications without launching an entire virtual machine. Also known simply as *containerization*.

**application firewall** A firewall that can control the traffic associated with specific applications. Works all the way up to the application layer of the OSI model.

**application-level gateway (ALG)** Applies security mechanisms to specific applications, such as FTP and/or BitTorrent. It supports address and port translation and checks whether the type of application traffic is allowed.

**application whitelisting** A method of restricting users to specific applications.

**ARP poisoning** An attack that exploits Ethernet networks and may enable an attacker to sniff frames of information, modify that information, or stop it from getting to its intended destination.

**asymmetric key algorithm** A type of cipher that uses a pair of different keys to encrypt and decrypt data.

**attack vector** The path or means by which an attacker gains access to a computer.

**attestation** The act of verifying whether a process is secure; for example, the secure boot process of a UEFI-based system.

**attribute-based access control (ABAC)** An access model that is dynamic and context-aware and uses IF-THEN statements and a combination of policies to control access to resources.

**audit trail** Record or log that shows the tracked actions of users, regardless of whether the users successfully completed the actions.

**authentication** When a person's identity is confirmed. Authentication is the *verification* of a person's identity.

**authorization** When a user is granted access to specific resources after authentication is complete.

**availability** Data is obtainable regardless of how information is stored, accessed, or protected.

**backdoors** Used in computer programs to bypass normal authentication and other security mechanisms in place.

**back-to-back perimeter** A type of DMZ that is located between the LAN and the Internet.

**backup generator** Part of an emergency power system used when there is an outage of regular electric grid power.

**baiting** When a malicious individual leaves malware-infected removable media, such as a USB drive or optical disc, lying around in plain view.

**banner grabbing** A technique used to gain information about servers and take inventory of systems and services. It can be used legitimately by network administrators or illegitimately by attackers to grab information such as HTTP headers.

**baseline reporting** Identification of the security posture of an application, system, or network.

**baselining** The process of measuring changes in networking, hardware, software, and so on.

**behavior-based monitoring** A monitoring system that looks at the previous behavior of applications, executables, and/or the operating system and compares that to current activity on the system.

**biometrics** The science of recognizing humans based on one or more physical characteristics.

**birthday attack** An attack on a hashing system that attempts to send two different messages with the same hash function, causing a collision.

**black-box testing** When people test a system but have no specific knowledge of the system code involved with the system.

**black hat** A hacker that breaks into computer systems without permission, with the express purpose of theft, piracy, credit card fraud, or other illegal activities.

**blackout** When a total loss of power for a prolonged period occurs.

**block cipher** A type of algorithm that encrypts a number of bits as individual units known as blocks.

**Blowfish** A 64-bit block cipher designed by Bruce Schneier as an alternative to DES.

**bluejacking** The sending of unsolicited messages to Bluetooth-enabled devices such as mobile phones and tablets.

**bluesnarfing** The unauthorized access of information from a wireless device through a Bluetooth connection.

**botnet** A group of compromised computers used to distribute malware across the Internet; the members are referred to as “bots” and are usually zombies.

**broadcast storm** When there is an accumulation of broadcast and multicast packet traffic on the LAN coming from one or more network interfaces.

**brownout** When the voltage drops to such an extent that it typically causes the lights to dim and causes computers to shut off.

**brute-force attack** A password attack where every possible password is attempted.

**buffer overflow** When a process stores data outside the memory that the developer intended to be used for storage. This could cause erratic behavior in the application, especially if the memory already had other data in it.

**business impact analysis (BIA)** The examination of critical versus noncritical functions; part of a business continuity plan (BCP).

**butt set** A device that looks similar to a phone but has alligator clips that can connect to the various terminals used by phone equipment, enabling a person to listen in to a conversation. Also called a lineman’s handset.

**CAM table** The Content Addressable Memory table, a table that is in a switch's memory that contains ports and their corresponding MAC addresses.

**CAPTCHA** A type of challenge-response mechanism used primarily in websites to tell whether or not the user is human. Stands for Completely Automated Public Turing test to tell Computers and Humans Apart.

**certificate** Digitally signed electronic document that binds a public key with a user identity.

**certificate authority (CA)** The entity (usually a server) that issues digital certificates to users.

**certificate revocation list (CRL)** A list of certificates no longer valid or that have been revoked by the issuer.

**chain of custody** Documents who had custody of evidence all the way up to litigation or a court trial (if necessary) and verifies that the evidence has not been modified.

**Challenge Handshake Authentication Protocol (CHAP)** An authentication scheme used by the Point-to-Point Protocol (PPP) that is the standard for dial-up connections.

**change management** A structured way of changing the state of a computer system, network, or IT procedure.

**chromatic dispersion** The refraction of light as in a rainbow. If light is refracted in such a manner on fiber-optic cables, the signal cannot be read by the receiver.

**cipher** An algorithm that can perform encryption or decryption.

**circuit-level gateway** Works at the session layer of the OSI model and applies security mechanisms when a TCP or UDP connection is established; acts as a go-between for the transport and application layers in TCP/IP.

**closed-circuit television (CCTV)** A video system (often used for surveillance) that makes use of traditional coaxial-based video components, but is used privately, within a building or campus.

**cloud computing** A way of offering on-demand services that extend the capabilities of a person's computer or an organization's network.

**cluster** Two or more servers that work with each other.

**cold site** A site that has tables, chairs, bathrooms, and possibly some technical setup (for example, basic phone, data, and electric lines), but will require days if not weeks to set up properly.

**collision** When two different files end up using the same hash, which is possible with less secure hashing algorithms.

**Common Vulnerabilities and Exposures (CVE)** An online list of known vulnerabilities (and patches) to software, especially web servers. It is maintained by the MITRE Corporation.

**computer security audits** Technical assessments made of applications, systems, or networks.

**confidentiality** Preventing the disclosure of information to unauthorized persons.

**content filters** Individual computer programs that block external files that use JavaScript or images from loading into the browser.

**context-aware authentication** An adaptive way of authenticating users based on their usage of resources, and the confidence that the system has in the user.

**Controller Area Network (CAN)** A multimaster serial bus that allows connectivity between the various microcontrollers in an automobile.

**cookies** Text files placed on the client computer that store information about it, which could include your computer's browsing habits and credentials. Tracking cookies are used by spyware to collect information about a web user's activities. Session cookies are used by attackers in an attempt to hijack a session.

**crossover error rate (CER)** The collective analysis and comparison of the false acceptance rate (FAR) and false rejection rate (FRR). It is also known as equal error rate.

**cross-site request forgery (XSRF)** An attack that exploits the trust a website has in a user's browser in an attempt to transmit unauthorized commands to the website.

**cross-site scripting (XSS)** A type of vulnerability found in web applications used with session hijacking. XSS enables an attacker to inject client-side scripts into web pages.

**crosstalk** When a signal transmitted on one copper wire creates an undesired effect on another wire; the signal "bleeds" over, so to speak.

**cryptanalysis attack** A password attack that uses a considerable set of precalculated encrypted passwords located in a lookup table.

**cryptographic hash functions** Hash functions based on block ciphers.

**cryptography** The practice and study of hiding information.

**data emanation** Also known as signal emanation, the electromagnetic field generated by a network cable or network device, which can be manipulated to eavesdrop on conversations or to steal data.

**Data Encryption Standard (DES)** An older type of block cipher selected by the U.S. federal government back in the 1970s as its encryption standard; due to its weak key, it is now considered deprecated.

**data loss prevention (DLP)** Systems that are designed to protect data by way of content inspection. They are meant to stop the leakage of confidential data, often concentrating on communications.

**data at rest** Inactive data that is archived.

**data in transit** Data that crosses the network or data that resides in computer memory.

**data in use** Data that is undergoing constant change.

**default account** An account installed by default on a device or within an operating system with a default set of user credentials that are usually insecure.

**defense in depth** The building up and layering of security measures that protect data from inception, on through storage and network transfer, and lastly to final disposal.

**demilitarized zone (DMZ)** A special area of the network (sometimes referred to as a subnetwork) that houses servers that host information accessed by clients or other networks on the Internet.

**denial-of-service (DoS)** A broad term given to many different types of network attacks that attempt to make computer resources unavailable.

**dictionary attack** A password attack that uses a prearranged list of likely words, trying each of them one at a time.

**differential backup** Type of backup that backs up only the contents of a folder that have changed since the last full backup.

**Diffie-Hellman key exchange** Invented in the 1970s, the first practical method for establishing a shared secret key over an unprotected communications channel.

**digital signature** A signature that authenticates a document through math, letting the recipient know that the document was created and sent by the actual sender and not someone else.

**directory traversal** Also known as the ../ (dot dot slash) attack, a method of accessing unauthorized parent directories.

**disaster recovery plan (DRP)** A plan that details the policies and procedures concerning the recovery and/or continuation of an organization's technology infrastructure.

**discretionary access control (DAC)** An access control policy generally determined by the owner.

**disk duplexing** When each disk is connected to a separate controller.

**distributed denial-of-service (DDoS)** An attack in which a group of compromised systems attacks a single target, causing a DoS to occur at that host, usually using a botnet.

**diversion theft** When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location.

**DNS amplification attack** An attack that initiates a DNS request with a spoofed source address. Responses (which are larger than the request) are sent to the victim server in an attempt to flood it.

**DNS poisoning** The modification of name resolution information that should be in a DNS server's cache.

**domain name kiting** The process of deleting a domain name during the five-day grace period (known as the add grace period, or AGP) and immediately reregistering it for another five-day period to keep a domain name indefinitely and for free.

**downgrade attack** When a protocol (such as TLS or SSL) is downgraded from the current version to a previous version, exploiting backward compatibility.

**due care** The mitigation action that an organization takes to defend against the risks that have been uncovered during due diligence.

**due diligence** Ensuring that IT infrastructure risks are known and managed.

**due process** The principle that an organization must respect and safeguard personnel's rights.

**dumpster diving** When a person literally scavenges for private information in garbage and recycling containers.

**eavesdropping** When a person uses direct observation to "listen" in to a conversation.

**electromagnetic interference (EMI)** A disturbance that can affect electrical circuits, devices, and cables due to electromagnetic conduction or radiation.

**elliptic curve cryptography (ECC)** A type of public key cryptography based on the structure of an elliptic curve.



**Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)** An asymmetric algorithm created by Diffie and Hellman that is based on elliptic curve cryptography and runs in ephemeral mode.

**encryption** The process of changing information using an algorithm (or cipher) into another form that is unreadable by others—unless they possess the key to that data.

**ethical hacker** An expert at breaking into systems and can attack systems on behalf of the system's owner and with the owner's consent.

**evil twin** A rogue wireless access point that uses the same SSID as a nearby legitimate access point.

**explicit allow** When an administrator sets a rule that allows a specific type of traffic through a firewall, often within an ACL.

**explicit deny** When an administrator sets a rule that denies a specific type of traffic access through a firewall, often within an ACL.

**Extensible Authentication Protocol (EAP)** Not an authentication mechanism in itself but instead defines message formats. 802.1X would be the authentication mechanism and defines how EAP is encapsulated within messages.

**fail-open mode** When a switch broadcasts data on all ports the way a hub does.

**failover clusters** Also known as high-availability clusters, these are designed so that a secondary server can take over in the case that the primary one fails, with limited or no downtime.

**false acceptance** When a biometric system authenticates a user who should *not* be allowed access to the system. It is analyzed with the false acceptance rate (FAR).

**false negative** Speaking in terms of intrusion monitoring, this is when an IDS/IPS fails to block an attack, thinking it is legitimate traffic.

**false positive** Speaking in terms of intrusion monitoring, this is when an IDS/IPS blocks legitimate traffic from passing on to the network.

**false rejection** When a biometric system fails to recognize an authorized person and doesn't allow that person access. It is analyzed with the false rejection rate (FRR).

**Faraday cage** An enclosure formed by conducting material or by a mesh of such material; it blocks out external static electric fields and can stop emanations from cell phones and other devices within the cage from leaking out.

**federated identity management (FIM)** When a user's identity is shared across multiple identity management systems.

**fire suppression** The process of controlling and/or extinguishing fires to protect people and an organization's data and equipment.

**firewall** A part of a computer system or network designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit or deny computer applications based on a set of rules and other criteria.

**first responders** People who perform preliminary analysis of the incident data and determine whether the incident is an incident or just an event, and the criticality of the incident.

**flood guard** Security feature implemented on some firewalls to protect against SYN floods and other flooding attacks. Also known as an attack guard.

**fork bomb** An attack that works by creating a large number of processes quickly to saturate the available processing space in the computer's operating system. It is a type of wabbit.

**Fraggle** A type of DoS similar to the Smurf attack, but the traffic sent is UDP echo traffic as opposed to ICMP echo traffic.

**full backup** Type of backup where all the contents of a folder are backed up.

**fuzz testing** Also called fuzzing, a type of test in which random data is inputted into a computer program in an attempt to find vulnerabilities.

**GNU Privacy Guard (GPG)** A free alternative to PGP that is compliant with OpenPGP.

**grandfather-father-son** A backup rotation scheme in which three sets of backup tapes must be defined—usually they are daily, weekly, and monthly, which correspond to son, father, and grandfather.

**grayware** A general term used to describe applications that are behaving improperly but without serious consequences; often describes types of spyware.

**Group Policy** Used in Microsoft environments to govern user and computer accounts through a set of rules.

**hacktivist** An attacker who has an agenda that may or may not be benign.

**hardening** The act of configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner, and removing unnecessary applications and services.

**hardware security module (HSM)** A physical device that deals with the encryption of authentication processes, digital signings, and payment processes.

**hash** A summary of a file or message. It is generated to verify the integrity of the file or message.

**hash function** A mathematical procedure that converts a variable-sized amount of data into a smaller block of data.

**high availability** When a system or component (such as a RAID array) is continuously operational for an extended period of time. The component should have an average 99.9% uptime or higher.

**hoax** The attempt at deceiving people into believing something that is false.

**honeynet** One or more computers or servers, or an area of a network, used to attract and trap potential attackers to counteract any attempts at unauthorized access of the network.

**honeypot** Generally is a single computer but could also be a file, group of files, or an area of unused IP address space used to attract and trap potential attackers to counteract any attempts at unauthorized access of the network.

**host-based intrusion detection system (HIDS)** A type of system loaded on an individual computer that analyzes and monitors what happens inside that computer—for example, if any changes have been made to file integrity.

**hot and cold aisles** The aisles in a server room or data center that circulate cold air into the systems and hot air out of them. Usually, the systems and cabinets are supported by a raised floor.

**hot site** A near duplicate of the original site of the organization, complete with phones, computers, networking devices, and full backups.

**hotfix** Originally defined as a patch to an individual OS or application to fix a single problem, installed live while the system was up and running, and without a reboot necessary. However, this term has changed over time and varies from vendor to vendor.

**HTTP proxy (web proxy)** Caches web pages from servers on the Internet for a set amount of time.

**hypervisor** The portion of virtual machine software that allows multiple virtual operating systems (guests) to run at the same time on a single computer.

**identification** When a person is in a state of being identified. It can also be described as something that identifies a person such as an ID card.

**identity proofing** An initial validation of an identity.

**implicit deny** Denies all traffic to a resource unless the users generating that traffic are specifically granted access to the resource. For example, when a device denies all traffic unless a rule is made to open the port associated with the type of traffic desired to be let through.

**incident management** The monitoring and detection of security events on a computer network and the execution of proper responses to those security events.

**incident response** A set of procedures that an investigator follows when examining a computer security incident.

**incremental backup** Type of backup that backs up only the contents of a folder that have changed since the last full backup or the last incremental backup.

**information assurance (IA)** The practice of managing risks that are related to computer hardware and software systems.

**information security** The act of protecting information from unauthorized access. It usually includes an in-depth plan on how to secure data, computers, and networks.

**infrastructure as a service (IaaS)** A cloud computing service that offers computer networking, storage, load balancing, routing, and VM hosting.

**input validation** Also called data validation, a process that ensures the correct usage of data.

**integer overflow** When arithmetic operations attempt to create a numeric value that is too big for the available memory space.

**integrity** Ensuring that data can be modified only by those authorized to do so.

**interconnection security agreement (ISA)** An agreement that is established between two (or more) organizations that own and operate connected IT systems and data; it specifically documents the technical and security requirements of the interconnection between the organizations.

**Internet content filter** A filter that is usually applied as software at the application layer and can filter out various types of Internet activities such as websites accessed, e-mail, instant messaging, and more. It is used most often to disallow access to inappropriate web material.

**Internet Protocol Security (IPsec)** A TCP/IP protocol that authenticates and encrypts IP packets, effectively securing communications between computers and devices using the protocol.

**IP proxy** Secures a network by keeping machines behind it anonymous; it does this through the use of NAT.

**IV attack** A type of related-key attack based on the initialization vector of wireless network communications, where an attacker observes the operation of a cipher using several different keys and finds a mathematical relationship between them, allowing the attacker to ultimately decipher data.

**job rotation** When users are cycled through various assignments.

**Kerberos** An authentication protocol that enables computers to prove their identity to each other in a secure manner.

**key** The essential piece of information that determines the output of a cipher.

**key escrow** When certificate keys are held in case third parties, such as government or other organizations, need access to encrypted communications.

**key recovery agent** Software that can be used to archive and restore keys if necessary.

**key stretching** Takes a weak key, processes it, and outputs an enhanced and more powerful key, usually increasing key size to 128 bits.

**LANMAN hash** The original hash used to store Windows passwords, known as LM hash, based off the DES algorithm.

**Layer 2 Tunneling Protocol (L2TP)** A tunneling protocol used to connect virtual private networks. It does not include confidentiality or encryption on its own. It uses port 1701 and can be more secure than PPTP if used in conjunction with IPsec.

**least functionality** When a computer is configured to only allow required functions, applications, services, ports, and protocols.

**least privilege** When a user is given only the amount of privileges needed to do his or her job.

**Lightweight Directory Access Protocol (LDAP)** An application layer protocol used for accessing and modifying directory services data.

**load-balancing clusters** When multiple computers are connected in an attempt to share resources such as CPU, RAM, and hard disks.

**locally shared objects (LSOs)** Also known as Flash cookies, files stored on users' computers that allow websites to collect information about visitors. Also referred to as "local shared objects."

**logic bomb** Code that has, in some way, been inserted into software; it is meant to initiate some type of malicious function when specific criteria are met.

**MAC filtering** A method used to filter out which computers can access the wireless network; the WAP does this by consulting a list of MAC addresses that have been previously entered.

**MAC flooding** An attack that sends numerous packets to a switch, each of which has a different source MAC address, in an attempt to use up the memory on the switch. If this is successful, the switch will change state to fail-open mode.

**MAC spoofing** An attack where the attacker masks the MAC address of the computer's network adapter. Can be enhanced by a DHCP starvation attack.

**malware** Software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent.

**mandatory access control (MAC)** An access control policy determined by a computer system, not by a user or owner, as it is in DAC.

**mandatory vacations** When an organization requires that employees take a certain number of days of vacation consecutively, helping to detect potential malicious activity such as fraud or embezzlement.

**man-in-the-browser (MITB)** Infects a vulnerable web browser and modifies online transactions. Similar to MITM.

**man-in-the-middle (MITM)** A form of eavesdropping that intercepts all data between a client and a server, relaying that information back and forth.

**mantrap** An area between two doorways, meant to hold people until they are identified and authenticated.

**many-to-one mapping** When multiple certificates are mapped to a single recipient.

**mean time between failures (MTBF)** Defines the average number of failures per million hours for a product in question.

**measured boot** Takes measurements of the secure boot process, signs those results with a TPM, and reports those measurements to a trusted third party such as a remote attestation service.

**memorandum of understanding (MoU)** A letter of intent between two entities (such as government agencies) concerning SLAs and BPAs.

**memory leak** When a program allocates memory but does not free it up properly after the process using it has completed.

**Message-Digest algorithm 5 (MD5)** A 128-bit key hash used to provide integrity of files and messages.

**mobile device management (MDM)** A centralized software solution that allows for the control and configuration of mobile devices.

**multifactor authentication (MFA)** When two or more types of authentication are used when dealing with user access control.

**mutual authentication** When two computers (for example, a client and a server) verify each other's identity.

**network access control (NAC)** Sets the rules by which connections to a network are governed.

**network address translation (NAT)** The process of changing an IP address while it is in transit across a router. This is usually implemented so that one larger address space (private) can be remapped to another address space, or single IP address (public).

**network intrusion detection system (NIDS)** A type of IDS that attempts to detect malicious network activities—for example, port scans and DoS attacks—by constantly monitoring network traffic.

**network intrusion prevention system (NIPS)** Designed to inspect traffic and, based on its configuration or security policy, remove, detain, or redirect malicious traffic.

**Network Management System (NMS)** The software run on one or more servers that controls the monitoring of network-attached devices and computers.

**network mapping** The study of physical and logical connectivity of networks.

**network perimeter** The border of a computer network, commonly secured by devices such as firewalls and NIDS/NIPS solutions.

**null pointer dereference** A memory dereference that can result in a memory fault error.

**null session** A connection to the Windows interprocess communications share (IPC\$) that can be exploited by a null session attack, which makes unauthenticated NetBIOS connections to a target computer.

**nonce** A random number issued by an authentication protocol that can only be used once.

**non-promiscuous mode** When a network adapter captures only the packets that are addressed to it.

**non-repudiation** The idea of ensuring that a person or group cannot refute the validity of your proof against them.

**NTLM hash** Successor to the LM hash. A more advanced hash used to store Windows passwords, based off the RC4 algorithm.

**NTLMv2 hash** Successor to the NTLM hash. Based off the MD5 hashing algorithm.

**null session** When used by an attacker, a malicious connection to the Windows interprocess communications share (IPC\$).

**onboarding** When a new employee is added to an organization, and to its identity and access management system.

**one-time pad** A cipher that encrypts plaintext with a secret random key that is the same length as the plaintext.

**one-to-one mapping** When an individual certificate is mapped to a single recipient.

**one-way function** A hash that is easy to compute when generated but difficult (or impossible) to compute in reverse.

**Online Certificate Status Protocol (OCSP)** An alternative to using a certificate revocation list (CRL). It contains less information than a CRL does, and does not require encryption.

**open mail relay** Also known as an SMTP open relay, enables anyone on the Internet to send e-mail through an SMTP server.

**Open Vulnerability and Assessment Language (OVAL)** A standard and a programming language designed to standardize the transfer of secure public information across networks and the Internet utilizing any security tools and services available.

**organized crime** A criminal enterprise run by well-funded and sophisticated people motivated mainly by money, using computer systems and hacking techniques to gain access to company information and secrets.

**packet filtering** In the context of firewalls, inspects each packet passing through the firewall and accepts or rejects it based on rules. Two types of packet filtering include stateless packet filters and stateful packet inspection (SPI).

**pass the hash** An attack where password hashes are obtained from a server and reused in an attempt to trick the server's authentication system.

**passive reconnaissance** Gaining information about a target system without engaging the system.

**password cracker** Software tool used to recover passwords from hosts or to discover weak passwords.



**patch** An update to a system. Patches generally carry the connotation of a small fix in the mind of the user or system administrator, so larger patches often are referred to as software updates, service packs, or something similar.

**patch management** The planning, testing, implementing, and auditing of patches.

**PBKDF2** A type of key stretching software that incorporates salting for additional security, usually in password hashing.

**penetration testing** Also called pen testing, a method of evaluating the security of a system by simulating one or more attacks on that system.

**permanent DoS (PDoS) attack** Generally consists of an attacker's exploiting security flaws in routers and other networking hardware by flashing the firmware of the device and replacing it with a modified image.

**permissions** Control which file system resources a person can access on the network.

**personal firewall** An application that protects an individual computer from unwanted Internet traffic; it does so by way of a set of rules and policies.

**personally identifiable information (PII)** Information used to uniquely identify, contact, or locate a person.

**pharming** When an attacker redirects one website's traffic to another bogus and possibly malicious website by modifying a DNS server or hosts file.

**phishing** The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

**piggybacking** When an unauthorized person tags along with an authorized person to gain entry to a restricted area.

**ping flood** When an attacker attempts to send many ICMP echo request packets (pings) to a host in an attempt to use up all available bandwidth. Also known as an ICMP flood attack.

**Ping of Death (POD)** A type of DoS that sends an oversized and/or malformed packet to another computer.

**pivot** A technique used to gain access to other systems or other parts of the network after an initial system has been exploited.

**platform as a service (PaaS)** A cloud computing service that provides various software solutions to organizations, especially the ability to develop applications without the cost or administration of a physical platform.

**Point-to-Point Tunneling Protocol (PPTP)** A tunneling protocol used to support VPNs. Generally includes security mechanisms, and no additional software or protocols need to be loaded. A VPN device or server must have inbound port 1723 open to enable incoming PPTP connections.

**policy** Rules or guidelines used to guide decisions and achieve outcomes. They can be written or configured on a computer.

**pop-up blocker** An application or add-on to a web browser that blocks pop-up windows that usually contain advertisements.

**port address translation (PAT)** Like NAT, but it translates both IP addresses and port numbers.

**port mirroring** When you configure one or more ports on a switch to forward all packets to another port. Often used when capturing packets.

**port scanner** Software used to decipher which ports are open on a host.

**pre-action sprinkler system** Similar to a dry pipe system, but there are requirements for it to be set off such as heat or smoke.

**pre-shared key** A key based on a generated (or selected) passphrase that is used to enable connectivity between wireless clients and an access point.

**pretexting** When a person invents a scenario, or pretext, in the hope of persuading a victim to divulge information.

**Pretty Good Privacy (PGP)** An encryption program used primarily for signing, encrypting, and decrypting e-mails in an attempt to increase the security of e-mail communications.

**private key** A type of key that is known only to a specific user or users who keep the key a secret.

**privilege escalation** The act of exploiting a bug or design flaw in a software or firmware application to gain access to resources that normally would've been protected from an application or user.

**promiscuous mode** When the network adapter captures all frames/packets that it has access to regardless of the destination for those packets.

**protected distribution system** Security system implemented to protect unencrypted data transfer over wired networks.

**Protected Extensible Authentication Protocol (PEAP)** Protocol used to encapsulate EAP packets within encrypted and authenticated tunnels.

**protocol analyzer** Software tool used to capture and analyze packets.

**proxy auto-configuration (PAC)** A file in web browsers that automatically chooses an appropriate proxy server.

**proxy server** Acts as an intermediary between clients, usually located on a LAN, and the servers that they want to access, usually located on the Internet.

**pseudorandom number generator (PRNG)** Used by cryptographic applications that require unpredictable output. Example: SHA2PRNG. Threat: random number generator attack. Prevention: additional randomness, AES, SHA256 or higher, and physical control of the system.

**public key** A type of key that is known to all parties involved in encrypted transactions within a given group.

**public key cryptography** Uses asymmetric keys alone or in addition to symmetric keys. The asymmetric key algorithm creates a secret private key and a published public key.

**public key infrastructure (PKI)** An entire system of hardware and software, policies and procedures, and people, used to create, distribute, manage, store, and revoke digital certificates.

**qualitative risk assessment** An assessment that assigns numeric values to the probability of a risk and the impact it can have on the system or network.

**quantitative risk assessment** An assessment that measures risk by using exact monetary values.

**race condition** An exploitable situation that happens when a system or application is performing two tasks and the time between them can be exploited to gain access to the program, change a file, or gain access to a resource.

**radio frequency interference (RFI)** Interference that can come from AM/FM transmissions and cell towers.

**RAID 1** Mirroring. Data is copied to two identical drives. If one drive fails, the other continues to operate.

**RAID 10** Combining the advantages of RAID 1 and 0, normally two sets of RAID 1 mirrors (minimum) that are then striped.

**RAID 5** Striping with parity. Data is striped across multiple drives; fault-tolerant parity data is also written to each drive.

**RAID 6** Striping with double parity. Four drives minimum.

**rainbow table** In password cracking, a set of precalculated encrypted passwords located in a lookup table.

**ransomware** A type of malware that restricts access to a computer system and demands a ransom be paid to restore access.

**recovery point objective (RPO)** In business impact analysis, the acceptable latency of data.

**recovery time objective (RTO)** In business impact analysis, the acceptable amount of time to restore a function.

**redundant ISP** Secondary connections to another ISP; for example, a backup T-1 line.

**redundant power supply** An enclosure that contains two complete power supplies, the second of which turns on when the first fails.

**registration authority (RA)** Used to verify requests for certificates.

**Remote Access Service (RAS)** A networking service that allows incoming connections from remote dial-in clients. It is also used with VPNs.

**remote access Trojan (RAT)** A type of Trojan used to gain back-end access to a server, taking control of it, often for malicious purposes.

**Remote Authentication Dial-In User Service (RADIUS)** Used to provide centralized administration of dial-up, VPN, and wireless authentication.

**remote code execution (RCE)** When an attacker acquires control of a remote computer through a code vulnerability. Also known as arbitrary code execution. Attackers often use a web browser's URL field or a tool such as Netcat to accomplish this.

**removable media controls** Security controls put in place to protect the data residing on USB flash drives and other removable media, and to protect the systems that they connect to.

**replay attack** An attack in which valid data transmission is maliciously or fraudulently repeated or delayed.

**residual risk** The risk that is left over after a security plan and a disaster recovery plan have been implemented.

**risk** The possibility of a malicious attack or other threat causing damage or downtime to a computer system.

**risk acceptance** The amount of risk an organization is willing to accept. Also known as risk retention.

**risk assessment** The attempt to determine the number of threats or hazards that could possibly occur in a given amount of time to your computers and networks.

**risk avoidance** When an organization avoids risk because the risk factor is too great.

**risk management** The identification, assessment, and prioritization of risks, and the mitigation and monitoring of those risks.

**risk mitigation** When a risk is reduced or eliminated altogether.

**risk reduction** When an organization mitigates risk to an acceptable level.

**risk register** Helps to track issues and address problems as they occur. Also known as a risk log.

**risk transference** The transfer or outsourcing of risk to a third party. Also known as risk sharing.

**rogue access point** An unauthorized wireless access point/router that allows access to secure networks. Also, rogue AP.

**role-based access control (RBAC)** An access model that works with sets of permissions, instead of individual permissions that are label-based, so roles are created for various job functions in an organization.

**root of trust (RoT)** A set of code and functions, usually embedded into a trusted platform module, that allows or denies tasks such as booting and drive encryption.

**rootkit** A type of software designed to gain administrator-level control over a computer system without being detected.

**RSA** A public key cryptography algorithm created by Rivest, Shamir, Adleman. It is commonly used in e-commerce.

**sag** An unexpected decrease in the amount of voltage provided.

**salting** The randomization of the hashing process to defend against cryptanalysis password attacks and rainbow tables.

**sandbox** When a web script runs in its own environment for the express purpose of not interfering with other processes, possibly for testing.

**script kiddie** An individual with little technical skill that reuses code and scripts that are freely available on the Internet.

**secure code review** An in-depth code inspection procedure.

**secure coding concepts** The best practices used during the life cycle of software development.

**Secure Hash Algorithm (SHA)** A group of hash functions designed by the NSA and published by the NIST, widely used in government. The most common currently is SHA-1.

**Secure/Multipurpose Internet Mail Extensions (S/MIME)** An IETF standard that provides cryptographic security for electronic messaging such as e-mail.

**Secure Shell (SSH)** A protocol that can create a secure channel between two computers or network devices.

**Secure Sockets Layer (SSL)** A cryptographic protocol that provides secure Internet communications such as web browsing, instant messaging, e-mail, and VoIP.

**security as a service (SECaaS)** A cloud computing service where a large service provider integrates its security services into the customer's infrastructure.

**security log files** Files that log activity of users. They show who did what and when, plus whether they succeeded or failed in their attempt.

**security posture** The risk level to which a system, or other technology element, is exposed.

**security posture assessment (SPA)** An assessment that uses baseline reporting and other analyses to discover vulnerabilities and weaknesses in systems and networks.

**security template** Groups of policies that can be loaded in one procedure.

**security tokens** Physical devices given to authorized users to help with authentication. These devices might be attached to a keychain or might be part of a card system.

**self-encrypting drive (SED)** Hard drives that encrypt all of the contents held within using encryption keys that are maintained independently from the CPU of the housing computer.

**separation of duties (SoD)** This is when more than one person is required to complete a particular task or operation.

**service-level agreement (SLA)** Part of a service contract where the level of service is formally defined.

**service pack (SP)** A group of updates, bug fixes, updated drivers, and security fixes that is installed from one downloadable package or from one disc.

**service set identifier (SSID)** The name of a wireless access point (or network) to which network clients will connect; it is broadcast through the air.

**shoulder surfing** When a person uses direct observation to find out a target's password, PIN, or other such authentication information.

**sideloading** The loading of third-party apps from a location outside of the official application store for that device. Can occur either by direct Internet connection (usually disabled by default), by connecting to a second mobile device via USB OTG or Bluetooth, or by copying apps directly from a microSD card.

**signature-based monitoring** Frames and packets of network traffic are analyzed for predetermined attack patterns. These attack patterns are known as signatures.

**Simple Network Management Protocol (SNMP)** A TCP/IP protocol that monitors network-attached devices and computers. It's usually incorporated as part of a network management system.

**single point of failure** An element, object, or part of a system that, if it fails, will cause the whole system to fail.

**single sign-on (SSO)** When a user can log in once but gain access to multiple systems without being asked to log in again.

**Smurf attack** A type of DoS that sends large amounts of ICMP echoes, broadcasting the ICMP echo requests to every computer on its network or subnetwork. The header of the ICMP echo requests will have a spoofed IP address. That IP address is the target of the Smurf attack. Every computer that replies to the ICMP echo requests will do so to the spoofed IP.

**snapshot backup** A type of backup primarily associated with operating system imaging, but could also be used for applications or individual drives.

**SNMP agent** Software deployed by the network management system that is loaded on managed devices. The software redirects the information that the NMS needs to monitor the remote managed devices.

**software as a service (SaaS)** A cloud computing service where users access applications over the Internet that are provided by a third party.

**software development life cycle (SDLC)** The process of creating systems and applications, and the methodologies used to do so. Also known as *systems development life cycle*.

**spam** The abuse of electronic messaging systems such as e-mail, broadcast media, and instant messaging.

**Spanning Tree Protocol (STP)** A networking protocol that automatically creates a loop-free topology of Ethernet switches. Prevents looping that can occur when connecting both ends of a patch cable to ports on one switch.

**spear phishing** A type of phishing attack that targets particular individuals.

**special hazard protection system** A clean agent sprinkler system such as FM-200 used in server rooms.

**spike** A short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike.

**spim** The abuse of instant messaging systems, a derivative of spam.

**spoofing** When an attacker masquerades as another person by falsifying information.

**spyware** A type of malicious software either downloaded unwittingly from a website or installed along with some other third-party software.

**standby generator** Systems that turn on automatically within seconds of a power outage.

**stateful packet inspection (SPI)** Type of packet inspection that keeps track of network connections by examining the header in each packet.

**static NAT** When a single private IP address translates to a single public IP address. This is also called one-to-one mapping.

**steganography** The science (and art) of writing hidden messages; it is a form of security through obscurity.

**storage segmentation** A clear separation of organizational and personal information, applications, and other content.

**stream cipher** A type of algorithm that encrypts each byte in a message one at a time.

**structured exception handling (SEH)** A way of handling exceptions generated by errors, such as ones that can be initiated by dividing by zero.

**subject alternative name(SAN)** A field (or fields) in PKI certificates that allows an organization to specify additional hostnames, domain names, and so on.

**supervisory control and data acquisition (SCADA)** System of hardware and software that controls and monitors industrial systems such as HVAC.

**surge** An unexpected increase in the amount of voltage provided.

**symmetric key algorithm** A class of cipher that uses identical or closely related keys for encryption and decryption.

**SYN flood** A type of DoS where an attacker sends a large amount of SYN request packets to a server in an attempt to deny service.

**tailgating** A type of piggybacking where an unauthorized person follows an authorized person into a secure area, without the authorized person's consent.

**TCP reset attack** Sets the reset flag in a TCP header to 1, telling the respective computer to kill the TCP session immediately.

**TCP/IP hijacking** When a hacker takes over a TCP session between two computers without the need of a cookie or any other type of host access.



**teardrop attack** A type of DoS that sends mangled IP fragments with overlapping and oversized payloads to the target machine.

**TEMPEST** Refers to the investigations of conducted emissions from electrical and mechanical devices, which could be compromising to an organization.

**Temporal Key Integrity Protocol (TKIP)** An algorithm used to secure wireless computer networks; meant as a replacement for WEP.

**Terminal Access Controller Access-Control System Plus (TACACS+)** A remote authentication protocol similar to RADIUS used in Cisco networks.

**threat modeling** A way of prioritizing threats to an application.

**threat vector** The method a threat uses to gain access to a target computer.

**tickets** Part of the authentication process used by Kerberos.

**time bomb** A Trojan programmed to set off on a certain date.

**time of day restriction** When a user's logon hours are configured to restrict access to the network during certain times of the day and week.

**Towers of Hanoi** A backup rotation scheme based on the mathematics of the Towers of Hanoi puzzle. Uses three backup sets. For example, the first tape is used every second day, the second tape is used every fourth day, and the third tape is used every eighth day.

**transitive trust** When two or more networks have a relationship where users from one network can gain access to resources on the other.

**Transport Layer Security (TLS)** The successor to SSL, provides secure Internet communications. This is shown in a browser as HTTPS.

**Triple DES (3DES)** Similar to DES but applies the cipher algorithm three times to each cipher block.

**Trojan horse** An application that appears to perform desired functions but is actually performing malicious functions behind the scenes.

**Trusted Computer System Evaluation Criteria (TCSEC)** A DoD standard that sets basic requirements for assessing the effectiveness of computer security access policies. Also known as The Orange Book.

**Trusted Operating System (TOS)** A system that adheres to criteria for multilevel security and meets government regulations.

**Twofish** A 128-bit block cipher designed by Bruce Schneier and based on Feistel.

**typosquatting** Also called URL hijacking, a method used by attackers that takes advantage of user typos when accessing websites. Instead of the expected website, the user ends up at a website with a similar name but often malicious content.

**UDP flood attack** A similar attack to the Fraggle. It uses the connectionless User Datagram Protocol. It is enticing to attackers because it does not require a synchronization process.

**unified threat management (UTM)** A security product that evolved from the firewall and also includes IDS/IPS, antivirus, VPN, content filtering, DLP, and load balancing, among other technologies.

**uninterruptible power supply (UPS)** Takes the functionality of a surge suppressor and combines that with a battery backup, protecting computers not only from surges and spikes, but also from sags, brownouts, and blackouts.

**User Account Control (UAC)** A security component of Windows that keeps every user (besides the actual Administrator account) in standard user mode instead of as an administrator with full administrative rights—even if they are a member of the administrators group.

**vampire tap** A device used to add computers to a 10BASE5 network. It pierces the copper conductor of a coaxial cable and can also be used for malicious purposes.

**virtual machine (VM)** An operating system (or application) created by virtual machine software that runs within a hosting operating system.

**virtual machine escape (VM)** When a user (or malware) is able to break out of a VM's isolation (or lack thereof) and gain access to the hosting computer.

**virtual private network (VPN)** A connection between two or more computers or devices that are not on the same private network.

**virtualization** The creation of a virtual entity, as opposed to a true or actual entity.

**virtualization sprawl** Also known as VM sprawl, when there are too many VMs for an administrator to manage effectively.

**virus** Code that runs on a computer without the user's knowledge; it infects the computer when the code is accessed and executed.

**vishing** A type of phishing attack that makes use of telephones and VoIP.

**VLAN hopping** The act of gaining access to traffic on other VLANs that would not normally be accessible by jumping from one VLAN to another.

**VPN concentrator** A hardware appliance that allows hundreds of users to connect to the network from remote locations via a VPN.

**vulnerability** Weaknesses in your computer network design and individual host configuration.

**vulnerability assessment** Baselineing of the network to assess the current security state of computers, servers, network devices, and the entire network in general.

**vulnerability management** The practice of finding and mitigating software vulnerabilities in computers and networks.

**vulnerability scanning** The act of scanning for weaknesses and susceptibilities in the network and on individual systems.

**war-chalking** The act of physically drawing symbols in public places that denote open, closed, or protected wireless networks.

**war-dialing** The act of scanning telephone numbers by dialing them one at a time and adding them to a list, in an attempt to gain access to computer networks.

**war-driving** The act of searching for wireless networks by a person in a vehicle through the use of a device with a wireless antenna, often a particularly strong antenna.

**warm site** A site that has computers, phones, and servers, but they might require some configuration before users can start using them.

**waterfall model** An SDLC model divided into sequential phases such as planning, design, implementation, testing, integration, deployment, and maintenance. *See* software development life cycle (SDLC).

**watering hole attack** An attack where the attacker profiles which websites a user accesses and installs malware to those sites that either infects the user's computer or redirects the user to other websites.

**web application firewall (WAF)** An application firewall used to protect servers (and their client sessions) from XSS and SQL injection, among other attacks, during HTTP sessions.

**web of trust** A decentralized model used for sharing certificates without the need for a centralized CA.

**web security gateway** An intermediary that can scan for viruses and filter Internet content.

**wet pipe sprinkler system** Consists of a pressurized water supply system that can deliver a high quantity of water to an entire building via a piping distribution system.

**whaling** A phishing attack that targets senior executives.

**white-box testing** A method of testing applications or systems where the tester is given access to the internal workings of the system.

**white hat** A type of hacker that is contracted to break into a company's system.

**Wi-Fi disassociation attack** Also known as Wi-Fi deauthentication attack, when an attacker targets a user's Wi-Fi-connected system, deauthenticates it using special software, and then reauthenticates it to find out SSID and WPA handshake information.

**Wi-Fi Protected Access (WPA)** A security protocol created by the Wi-Fi Alliance to secure wireless computer networks; more secure than WEP.

**Wi-Fi Protected Setup (WPS)** A simplified way of connecting to wireless networks using an eight-digit code. It is now deprecated due to its insecure nature and should be disabled if currently used.

**wildcard certificate** A single public key certificate that can be used by multiple subdomains (or all subdomains) of a single domain; for example, \*.davidlprowse.com.

**Wired Equivalent Privacy (WEP)** A deprecated wireless network security standard, less secure than WPA.

**Wireless Transport Layer Security (WTLS)** A protocol that is part of the Wireless Application Protocol (WAP) stack used by mobile devices. It enables secure user sessions.

**wiretapping** Tapping into a network cable in an attempt to eavesdrop on a conversation or steal data.

**worm** Code that runs on a computer without the user's knowledge; a worm self-replicates, whereas a virus does not.

**X.509** A common PKI standard developed by the ITU-T that incorporates the single sign-on authentication method.

**zero day attack** An attack that is executed on a vulnerability in software before that vulnerability is known to the creator of the software.

**zombie** An individual compromised computer in a botnet.