Glossary of Cybersecurity Terms

advanced
network
systems

advanced network systems

Table of Contents

A

Access control

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

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).

Advanced Encryption Standard (AES)

An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.

Algorithm (encryption)

A set of mathematical rules (logic) for the process of encryption and decryption. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form.

Anti-Virus

A security program that can run on a computer or mobile device and protects you by identifying and stopping the spread of malware on your system. Anti-virus cannot detect all malware, so even if it is active, your system might still get infected. Anti-virus can also be used at the organizational level. For example, email servers may have anti-virus integrated with it to scan incoming or outgoing email. Sometimes anti-virus tools are called 'anti-malware', because these products are designed to defend against various types of malicious software.

APT (Advanced Persistent Threat)

A set of stealthy and continuous computer backing processes, often orchestrated by human(s) targeting a specific entity. APT usually targets nations or organizations for business or political motives.

Attack

An attempt to break into a system.

Auditing

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

Authentication

The process of identifying an individual, usually based on a user name and password. Authentication usually requires something a person has (such as a key, badge, or token), something a person knows (such as a password, ID number, or mother's maiden name), or something a person is (represented by a photo, fingerprint or retina scan, etc). When authentication requires two of those three things, it is considered strong authentication.

Authorization

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

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.

B

Backdoor

A design fault, planned or accidental, that allows an attacker access to the compromised system around any security mechanisms that are in place.

Biometrics

A method of identification that uses physical characteristics of the users to determine access.

Black hat

A person of malicious intent who researches, develops, and uses techniques to defeat security measures and invade computer networks.

Blue screen of death

When a Windows NT-based system encounters a serious error, the entire operating system halts and displays a screen with information regarding the error. The name comes from the blue color of the error screen.

Bot

Also known as a zombie, is an Internet-connected computer that has been infected and compromised by malicious code in order to use the computer for something other than what was intended.

Botnet

A network of compromised computers that are infected with small bits of malicious code (bots). They are frequently used by hackers for disreputable purposes, such as to launch denial of service attacks, or send messages like spam and malicious code without it being traceable. These infected machines allow a remote computer to control by a "botmaster" who has the ability to manipulate them individually, or collectively as bot armies that act in concert.

Breach

An incident that results in the disclosure or potential exposure of data.

Brute force attack

The attempt to gain access to a network using repeated guesses at passwords or data encryption keys.

Business continuity plan

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.

C

Certificate

An electronic document attached to someone's public key by a trusted third party, which attests that the public key belongs to a legitimate owner and has not been compromised. Certificates are intended to help you verify that a file or message actually comes from the entity it claims to come from.

Certificate-based authentication

Certificate-Based Authentication is the use of security protocols and certificates to authenticate and encrypt web traffic.

Cipher text

The result of encrypting either characters or bits using some algorithm. Cipher text is unreadable until it is decrypted.

Click fraud

An online crime that involves automating the act of clicking on a web link to perpetrate a fraud. In a classic click fraud scenario, a legitimate web site decides to advertise on another site, which hosts the ad. The legitimate web site agrees to pay the ad hosting site a few cents each time a potential customer clicks on

the ad, which links back to the legitimate site. Cheaters use automated tools to click the ad over and over, earning money from the legitimate site under false pretenses (since the clicks do not come from actual people interested in the advertised products).

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.

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

Cookie

A text file passed from a web site's server to a web site user's browser. They are used to identify a user and could record personal information such as ID and password, mailing address, credit card number, and more.

A cookie is what enables your favorite web site to "recognize" you each time you revisit it.

Cross-site scripting

An attack performed through Web browsers, taking advantage of poorly-written Web applications. Cross-site scripting attacks can take many forms. One common form is for an attacker to trick a user into clicking on a specially-crafted, malicious hyperlink. The link appears to lead to an innocent site, but the site is actually the attacker's, and includes embedded scripts. What the script does is up to the attacker; commonly, it collects data the victim might enter, such as a credit card number or password.

Cryptography

The art and science of encoding and decoding messages using mathematical algorithms that utilize a secret key. The concept has broadened to include managing messages that have some combination of: privacy (by being unreadable to anyone but the sender and receiver); integrity (not modified while en route), and non-repudiation (digitally signed in such a way that the originator cannot plausibly claim he or she did not originate it).

D

Darkweb

A hidden neighborhood of the Internet, only accessible using non-standard protocols. The darknet is a marketplace for illegal substances and arms, stolen data, and software used for hacking. It is also a meeting place for, among others, criminals and terrorists. Sites on the darkweb are not indexed and do not appear on search engines. Hidden web real estate can (and is) used for good as well, such as protecting dissidents in repressive regimes.

Data disclosure

A breach for which it was confirmed that data was actually disclosed (not just exposed) to an unauthorized party.

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.

Denial of Service (DoS)

Refers to any outwardly-induced condition that prevents access to a computer resource (rendering it unusable), thus "denying service" to an authorized or legitimate.

Denial of Service attack

A type of attack aimed at making the targeted system or network unusable, often by monopolizing system resources. For example, in February 2000 a hacker directed thousands of requests to eBay's Web site. The network traffic flooded the available Internet connection so that no users could access eBay for a few hours.

Distributed Denial-of-Service (DDoS) attack

Is a type of DOS attack where multiple infected/compromised systems, are used to send traffic to target a single system causing a Denial of Service (DoS) attack. It is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

Dictionary attack

An attempt to guess a password by systematically trying every word in a dictionary as the password. This attack is usually automated, using a dictionary of the hacker's choosing, which may include both ordinary words and jargon, names, and slang.

Digital signature

An electronic identification of a person or thing, intended to verify to a recipient the integrity of data sent to them, and the identity of the sender. Creating a digital signature involves elaborate mathematical techniques that the sender and recipient can both perform on the transmitted data.

DLP (Data Loss Prevention)

A strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

DMZ (Demilitarized Zone)

A partially-protected zone on a network, not fully exposed to the Internet, but at the same time, also not fully behind the firewall. This technique is typically used on parts of the network which must remain open to the public (such as a Web server) but must also access trusted resources (such as a database).

DNS (Domain Name System *or* Service *or* Server*)*

An Internet service that translates domain names *i*nto IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is based primarily on numerical IP addresses. Therefore, every time you use a domain name (e.g., www.example.org), a DNS service has to translate the name into the corresponding numerical IP address (e.g., 198.105.232.4).

Drive-by download

These attacks exploit vulnerabilities in your web browser or its plugins when you simply surf to an attacker-controlled website. Some computer attackers set up their own malicious websites that are designed to automatically attack and exploit anyone that visits it. Other attackers compromise trusted websites such as ecommerce sites and deploy their exploit software there. Often these attacks occur without the victims realizing that they are under attack.

Data mining

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

Day zero

Also known as "Zero Day," this is a term used to mark the day a new vulnerability is made known for which no patch may yet be available (day one = the day at which the patch is made available).

Decryption

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

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.

Dictionary attack

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

Digital certificate

An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

Digital signature

A digital signature is a hash of a message that uniquely identifies the sender.

Disaster Recovery Plan (DRP)

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

Domain

On the Internet, a domain consists of a set of network addresses. In a Windows NT environment, 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".

Dumpster diving

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

E

Elevation of privilege

Almost every computer program has some form of "privilege" built in, meaning, permission to do some set of actions on the system. Permissions are granted to individuals based on their ability to present proper

credentials (for example, a username and password). Privilege has levels -- for example, a guest account typically has fewer privileges than an administrator account. Many network attacks begin with an attacker obtaining limited privileges on a system, then attempting to leverage those privileges into greater privileges that might ultimately lead to controlling the system. Any attempt to gain greater permissions illicitly, is considered an “elevation of privilege."

Encryption

The process of transforming data (called "plaintext") into a form (called "cipher text") that hides its content. As used in a network security context, encryption is usually accomplished by putting the data through any of several established mathematical algorithms developed specifically for this purpose.

Endpoint security

In network security, this refers to a methodology of protecting the corporate network when accessed via end users including remote devices such as laptops or other wireless and mobile devices. Each device with a connection to the network creates a potential entry point for security threats.

Event

Any observable occurrence in a system or network that prompts some kind of log entry or other notification.

Exploit

Code that is designed to take advantage of a vulnerability. An exploit is designed to give an attacker the ability to execute additional malicious programs on the compromised system or to provide unauthorized access to affected data or application.

Exposure

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

External network

Any network that can employees would typically be trusted on your network, a primary vendor's network connect to yours, with which you have neither a trusted or semi-trusted relationship. For example, a company's might be semi-trusted, but the public Internet would be untrusted — hence, External.

F

Firewall

Software or hardware that monitors and control the incoming and outgoing traffic on a network based on predetermined security rules. It establishes a barrier between a trusted, secure internal network and untrusted networks (e.g., Internet) to prevent unauthorized access to data or resources.

FTP (File Transfer Protocol)

The most common protocol for specifying the transfer of text or binary files across a network or over the Internet.

G

Gateway

A network point that acts as an entrance to another network. A firewall will often serve as the gateway between the Internet and your network

H

Hardening

The process of identifying and fixing vulnerabilities on a system.

HTTP (Hyper Text Transfer Protocol)

A communications standard designed and used to transfer information and documents between servers or from a server to a client. This standard is what enables your web browser to fetch pages from the Internet.

HTTPS (Secure HTTP)

A variation of HTTP enabling the secure transmission of data. Generally used in conjunction with an enhanced by a security mechanism, (usually SSL) which encrypts the HTTP.

Honeypot

A trap set to detect, deflect or in some manner, counteract attempts at unauthorized use of information systems. Consists of computer data or a network site that appears to be part of a network but is actually isolated and monitored. A honey pot can be used to log access attempts to those ports including a would-be attacker's keystrokes.

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.

I

IDS (Intrusion Detection System)

A security management system that gathers, analyzes and reports on traffic information from various areas within a network. It identifies possible security breaches in progress including both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IPS (Intrusion Prevention System)

A network security appliance that identifies malicious system activity, logs information about this activity, attempts to block/stop it, and reports it.

Incident

An adverse security-related network event that compromises the integrity, confidentiality or availability of an information asset.

Incident management (Incident response)

A term describing the activities of an organization to identify, analyze, and correct a security incident to prevent a future re-occurrence.

IP address

A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols.

IP spoofing

The act of inserting a false (but ordinary-seeming) sender IP address into the "From" field of an Internet transmission's header in order to hide the actual origin of the transmission. There are few, if any, legitimate reasons to perform IP spoofing; the technique is usually one aspect of an attack.

IPSec (Internet Protocol Security)

A methodology of exchanging data over the public Internet while protecting the data from prying eyes as it travels from the originator to the recipient. IPSec provides encryption and authentication options to maximize the confidentiality of data transmissions, employing cryptographic protocols.

J

Java Security Exploit

A term that refers to any number of security flaws in Oracle's Java software, which has a long history of having security vulnerabilities. Java is a high-level programming language that is a commonly used foundation for developing and delivering interactive content on the Web.

K

No entries at this time.

L

Least Privilege

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

M

Malware

Short for “malicious software.” It is a generic description for any type of code or program cyber attackers use to perform malicious actions (capturing information, sabotaging the system, holding it for ransom). Traditionally there have been different types of malware based on their capabilities and means of propagation. However modern malware typically combines the characteristics from several or all of these in a single program.

- Virus: A type of malware that spreads by infecting other files, rather than existing in a standalone manner. Viruses often, though not always, usually spread through human interaction (such as opening an infected file or application).
- Worm: A type of malware that can propagate automatically, typically without requiring any human interaction for it to spread. Worms often spread across networks (infecting millions of computer systems), though can also infect systems through other means, such as USB keys.

- **Trojan:** A shortened form of "Trojan Horse." This type of malware appears to have a legitimate or at least benign use, but masks a hidden sinister function. For example, you may download and install a free screensaver which actually works well as a screensaver. But that software could also be malicious, it will infect your computer once you install it.
- **Spyware:** A type of malware that is designed to spy on the victim's activities, capturing sensitive data such as the person's passwords, online shopping, and screen contents. One popular type of spyware, a keylogger, is optimized for logging the victim's keyboard activity and transmitting the captured information to the remote attacker.

Man-in-the-middle (MitM) attack

A type of cyber-attack in which the actor intercepts, alters, or eavesdrops on data as it travels between the sender and recipient. An example of this is intercepting messages through an unencrypted Wi-Fi connection.

MSSP (Managed Security Service Provider)

An outsourced provider of network security services. Businesses turn to managed security services provider to alleviate the pressures they face daily related to information security. Functions of a managed security service include round-the-clock monitoring and management of intrusion detection systems and firewalls, overseeing patch management and upgrades, performing security assessments and security audits, and responding to security incidents.

N

NIST (National Institute for Standards and Technology)

A division of the U.S. Department of Commerce that publishes open interoperability standards. It is also responsible for distributing complete and accurate information about computer security issues to government and the general public.

NGFW (Next-generation firewall)

An integrated network platform that combines a traditional firewall with other network security functionalities such as deep packet inspection, intrusion prevention, website filtering, bandwidth management, antivirus inspection and third-party integration (i.e. Active Directory). Gartner defines an NGFW as “a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks.”

O

Open source software

A term applied when the source code of a computer program is made available free of charge to the general public. The concept relies on peer review to find and eliminate bugs in the program code. One of the most famous examples of open source software is Linux.

P

Passphrase

An easy-to-remember phrase which offers better security than a single-word password, because it is longer and thus harder to guess or calculate.

Password

A secret sequence of characters or a word that a user submits to a system for purposes of authentication, validation, or verification. WatchGuard recommends the use of passphrases in place of passwords.

Password caching

The temporary storage of a user's username and password by an application.

Patch

A patch is a small update released by a software manufacturer to fix bugs or vulnerabilities in an existing program. Your computer and mobile devices should be updated to install the latest vendor's patches in a timely fashion. Some vendors release patches on a monthly or quarterly basis. Therefore, having a computer that is unpatched for even a few weeks could leave it vulnerable.

Patching

The process of updating software to a more current version.

Phishing

A social engineering technique where the attacker tries to trick the victim into giving up sensitive information by masquerading as a trusted entity. In a common phishing attack, a spoofed email message is sent by the attacker. The attacker tries to steal authentication credentials by providing a link to a fake login form on a malicious website designed to look legitimate (e.g., your bank). Once the victim logs in to a site they think is their bank, their login and password would then be stolen by the attacker. The term has evolved

and often means not just attacks designed to steal your password, but emails designed to send you to websites that hack into your browser, or emails with infected attachments.

Ping

A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply; hence, it was named after the sound echo sonar makes when trying to locate an object.

Protocol

A set of formal rules describing how to transmit data across a network. They exist at several levels in a telecommunications connection.

Proxy server

A server that sits between a client application (such as a web browser) and a "real" server. The proxy server intercepts client requests and forwards them to the other server. Its purpose is two-fold: for outgoing traffic, it allows private, non-routable machines to reach a machine which can reach the Internet for them. Secondly, as it receives responses to the client machine requests (for example, web pages) it can cache them locally so that further client requests can be answered locally and immediately.

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.

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.

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. By changing the pointers on a web server (e.g., www.worldbank.com), the URL can be redirected to send traffic to the IP of the pseudo/fake 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.

Polymorphism

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

Port

On a computer, a port is an interface to which you can connect a device (printer, keyboard, etc.). Within an internet-based environment, a port is a communication endpoint/connection within a network. The port number identifies what type of port it is. For example, port 80 is used for web traffic.

Port scan

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.

Program policy

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

Q

QoS – Quality of Service (QoS)

The overall performance of a telephone or computer network, particularly the performance (speed and quality of connection) seen by the users of the network.

R

Remote access tool

A piece of software used to remotely access or control a computer. This tool can be used legitimately by system administrators for accessing the client computers. They can also be used by a malicious actor to control the system without the knowledge of the victim.

Reverse engineering

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

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.

Role based access control

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

Rootkit

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

S

Social engineering

A psychological attack used by cyber attackers to deceive their victims into taking an action that will place the victim at risk. For example, cyber attackers may trick you into revealing your password or fool you into installing malicious software on your computer. They often do this by pretending to be someone you know or trust, such as a bank, company or even a friend.

Spam

An electronic version of junk mail. Unwanted or unsolicited emails, typically sent to numerous recipients with the hope of enticing people to read the embedded advertisements, click on a link or open an attachment. Spam is often used to convince recipients to purchase illegal or questionable products and services, such as pharmaceuticals from fake companies. Spam is also often used to distribute malware to potential victims.

Spear phishing

Spear phishing describes a type of phishing attack that targets specific victims. The attacker uses details gathered about the targeted individuals to increase the credibility of the attack message. Specially crafted emails are sent to very specific individuals, usually all at the same organization. Because of the targeted nature of this attack, spear phishing attacks are often harder to detect and usually more effective at fooling their victims.

Spoofing

Sending an email disguised to look like it is coming from someplace besides its actual origin. The IP address may be changed, the email address may mimic a known domain, and the email formatting may imitate the design attached to a well-known company or site. It is generally used when a hacker wants to make it difficult to trace where an attack is coming from.

Spyware

A type of malware that is designed to spy on the victim's activities, capturing sensitive data such as the person's passwords, online shopping, and screen contents. One popular type of spyware, a keylogger, is optimized for logging the victim's keyboard activity and transmitting the captured information to the remote attacker.

Session hijacking

An intrusion technique whereby a hacker sends a command to an already existing connection between two machines, in order to wrest control of the connection away from the machine that initiated it. The hacker's goal is to gain access to a server while bypassing normal authentication measures.

Sandbox

In computer security, a sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third parties, suppliers, untrusted users and untrusted websites.

SIEM (Security Information and Event Management)

An approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security. The acronym is pronounced "sim" with a silent e.

SOC (Security Operations Center)

A centralized unit that deals with security issues on an organizational and technical level. A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology.

SSL (Secure Sockets Layer)

A computer networking protocol for transmitting private communication over the Internet between servers and clients. It manages security and encrypted communications.

Single sign-on

A computer log-in routine in which one logon provides access to all resources on the network.

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.

Session

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

Session hijacking

The take over of a session that someone else has established.

Signature

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

Smurf

An attack that 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 tool that monitors network traffic as it received in a network interface.

Sniffing

A synonym for "passive wiretapping."

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.

Stateful inspection

A firewall architecture that works at the network layer which 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 (malicious vs. non-malicious behavior).

Stealthing

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

T

Tactical Threat Intelligence

Information about how threat actors are conducting attacks.

Token

Also called a security token or an authentication token. Something a person has that evidences validity, or identity. It is usually a hardware device that resembles a hand-held calculator, since it often has some sort of display and perhaps a keypad for entering numbers. Tokens achieve the goal of "two-factor authentication," considered a strong standard of security when validating who a user is, because accessing a network that uses tokens requires two factors: something the person knows (a password) and something the person has (the token)

Tor

Is free software for enabling anonymous communication. The name is an acronym derived from the original software project name *The Onion Router*. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user and is a popular communication protocol utilized on the "darkweb."

Transmission Control Protocol (TCP)

Is a core protocol of the Internet. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP.

Trust

A methodology that determines which permissions and what actions other systems or users can perform on remote machines.

Trusted network

The private network which you intend your firewall to primarily protect. The Trusted network is usually where your most sensitive corporate resources reside or where home office employees do their work.

TCP/IP

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).

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.

Trojan

A shortened form of the term "Trojan Horse." Is a type of malware that appears to have a legitimate or at least benign use, but masks a hidden sinister function to evade security mechanisms. For example, you may download and install a free screensaver which actually works well as a screensaver. But that software could also contain malicious code that infects your computer once you install it.

U

UTM (Unified Threat Management)

A network security solution that is the evolution of the traditional firewall into an all-inclusive security product. UTMs are able to perform multiple security functions within one single system: network firewalling, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data loss prevention and on-appliance reporting.

V

Virus/worm/trojan

A virus is a self-replicating computer program, designed to be slipped into a computer in order to copy, delete, change, damage, or lock data. A virus frequently uses the infected computer to spread itself to other targets. Similarly, a worm does not alter files, but rather, it stays in active memory and replicates itself. A Trojan or Trojan horse is a virus that appears to have a useful function and uses that shell of legitimacy to avoid security measures.

Validation

The act of examining information provided by a person (or a system) to ascertain what rights, privileges, or permissions they may (or may not) have to perform some action. For example, when you attempt to charge a purchase at a retail store to a credit card, the cashier validates your identity by examining your identification and comparing your signature on the receipt with the signature on the credit card.

Verification

In cryptography, the act of testing the authenticity of a digital signature. Verification proves that the information was actually sent by the signer and that the message has not been subsequently altered by anyone else.

VPN (Virtual Private Network)

A means of having the security benefits of a private, dedicated, leased-line network, without the cost of actually owning one. VPN uses cryptography to scramble data so it's unreadable while traveling over the Internet, thus providing privacy over public lines. Companies with branch offices commonly use VPNs to connect multiple locations.

Vulnerability assessment

A process that defines, identifies, and prioritizes the severity of security holes (vulnerabilities) in a computer, network, or communications infrastructure which hackers can exploit.

Virus

A hidden, self-replicating section of computer software, usually malicious code, 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.

W

WPA (Wi-Fi Protected Access)

A data encryption specification for 802.11 wireless networks. Wireless networks rely on radio waves, which broadcast in all directions. Any device within range of a wireless access point could eavesdrop upon its transmissions. WPA encrypts wireless data so that an eavesdropper intercepts gibberish, while authorized endpoints receive clear, decrypted data. WPA replaces *WEP*, a weaker wireless encryption standard that attackers can readily break.

Worm

A self-replicating program that seeks access into other computers by exploiting security flaws. After a worm penetrates another computer, it continues seeking access to other areas. Worms often steal or vandalize computer data. Many viruses are more accurately termed worms, and use e-mail or database systems to propagate themselves to their victims.

Whaling

A type of spear-phishing attack specifically targeted at high-ranking executives in an organization.

White hat

A person who investigates flaws in network security measures in order to strengthen them and to prevent computer networks from being invaded. When such a researcher discovers new security flaws, he or she reports them to the appropriate vendor to be fixed, rather than using the knowledge illicitly.

WEP (Wired Equivalent Privacy)

The security aspects of 802.11b, a standard that enables wireless devices and laptops to access a network via radio frequencies instead of physical wiring. WEP has three tasks: 1) to authenticate clients to access points; 2) to encrypt the data exchanged between the clients and access points; and 3) to include an integrity check with every packet exchanged. The initial implementation of WEP provides weak security. While it is not completely useless, it is best used as another layer of security in conjunction with stronger measures.

Watering Hole

A computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected. Relying on websites that the group trusts makes this strategy efficient, even with groups that are resistant to spear phishing and other forms of phishing.

War Driving

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

Wiretapping

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

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.

X

No entries at this time.

Y

No entries at this time.

Z

Zero day

Also known as "Day Zero," this is a term used to mark the day a new vulnerability is made known for which no patch may yet be available (day one = the day at which the patch is made available).

Zero-day attack

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.