EQUILIBRIUM
CYBER SECURITY SERVICES

Network Security Glossary of Terms

0-day
A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack.

AAA
Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.

AES
The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

Asymmetric cryptography
Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Back Door
A back door is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. However, attackers often use back doors that they detect or install themselves, as part of an exploit. In some cases, a worm is designed to take advantage of a back door created by an earlier attack. For example, Nimda gained entrance through a back door left by Code Red.

Bastion Host
On the Internet, a bastion host is the only host computer that a company allows to be addressed directly from the public network and that is designed to screen the rest of its network from security exposure.

Black Hat
Black hat is used to describe a hacker (or, if you prefer, cracker) who breaks into a computer system or network with malicious intent. Unlike a white hat hacker, the black hat hacker takes advantage of the break-in, perhaps destroying files or stealing data for some future purpose. The black hat hacker may also make the exploit known to other hackers and/or the public without notifying the victim. This gives others the opportunity to exploit the vulnerability before the organization is able to secure it.

Botnet
A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet. A report from Symantec came to a similar conclusion.

Bluesnarfing
Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled.

Certificate Authority
A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

Common Vulnerabilities and Exposures CVE
Common Vulnerabilities and Exposures (CVE) is a dictionary of standard terms related to security threats. These threats fall into two categories, known as vulnerabilities and exposures. A vulnerability is a fact about a computer, server or network that presents a definite, identifiable security risk in a certain context. An exposure is a security-related situation, event or fact that may be considered a vulnerability by some people but not by others.

Darknet
A darknet is a routed allocation of IP address space that is not discoverable by any usual means. The term is used to refer to both a single private network and the collective portion of Internet address space that has been configured in that manner.

DDoS Attack
A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

EQUILIBRIUM
CYBER SECURITY SERVICES

DMZ

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the UN "police action" in the early 1950s.) A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

Gray Hat

Gray hat describes a cracker (or, if you prefer, hacker) who exploits a security weakness in a computer system or product in order to bring the weakness to the attention of the owners. Unlike a black hat, a gray hat acts without malicious intent. The goal of a gray hat is to improve system and network security. However, by publicizing a vulnerability, the gray hat may give other crackers the opportunity to exploit it. This differs from the white hat who alerts system owners and vendors of a vulnerability without actually exploiting it in public.

Honey Pot

A honey pot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. (This includes the hacker, cracker, and script kiddy.)

HTTPS

HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks. HTTPS was developed by Netscape.

HTTPS and SSL support the use of X.509 digital certificates from the server so that, if necessary, a user can authenticate the sender.

IDS

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organisation) and misuse (attacks from within the organisation). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

IKE

The Internet Key Exchange (IKE) is an IPsec (Internet Protocol Security) standard protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access. Specified inIETF Request for Comments (RFC) 2409, IKE defines an automatic means of negotiation and authentication for IPsec security associations (SA). Security associations are security policies defined for communication between two or more entities; the relationship between the entities is represented by a key. The IKE protocol ensures security for SA communication without the pre-configuration that would otherwise be required.

IPSec

IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication.

Earlier security approaches have inserted security at the application layer of the communications model. IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks.

Malware

Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission.

Man in the middle attack

A man-in-the-middle (MitM) attack is an exploit in which an intruder intercepts communications between two parties, usually an end user and a website. The attacker can use the information accessed to commit identity theft or other types of fraud.

NBAR

Network Based Application Recognition (NBAR) is a mechanism that classifies and regulates bandwidth for network applications to ensure that available resources are utilised as efficiently as possible. Cisco Systems developed NBAR as part of its Content Networking platform for implementing intelligent network services.

Network Access Control (NAC)

Network access control (NAC), also called network admission control, is a method of bolstering the security of a proprietary network by restricting the availability of network resources to endpoint devices that comply with a defined security policy.

One Time Password (OTP)

A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session.

An OTP is more secure than a static password, especially a user-created password, which is typically weak. OTPs may replace authentication login information or may be used in addition to it, to add another layer of security.

OTP tokens are usually pocket-size fobs with a small screen that displays a number.

OWASP Top 10

The OWASP Top Ten is a list of the 10 most dangerous current Web application security flaws, along with effective methods of dealing with those flaws. OWASP (Open Web Application Security Project) is an organisation that provides unbiased and practical, cost-effective information about computer and Internet applications.

Penetration Testing
Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

PKI
A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

Without PKI, sensitive information can still be encrypted (ensuring confidentiality) and exchanged, but there would be no assurance of the identity (authentication) of the other party.

Port Scan
A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favourite 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.

SAML
SAML (Security Assertion Mark-up Language) is an Extensible Mark-up Language (XML) standard that allows a user to log on once for affiliated but separate Web sites. SAML is designed for business-to-business (B2B) and business-to-consumer (B2C) transactions.

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

Script Kiddy
Script kiddy (sometimes spelled kiddie) is a derogative term, originated by the more sophisticated crackers of computer security systems, for the more immature, but unfortunately often just as dangerous exploiter of security lapses on the Internet. The typical script kiddy uses existing and frequently well-known and easy-to-find techniques and programs or scripts to search for and exploit weaknesses in other computers on the Internet - often randomly and with little regard or perhaps even understanding of the potentially harmful consequences.

Session Key
A session key is an encryption and decryption key that is randomly generated to ensure the security of a communication session between a user and another computer or between two computers.

Smurf Attack
A smurf attack is an exploitation of the Internet Protocol (IP) broadcast addressing to create a denial of service. The attacker uses a program called Smurf to cause the attacked part of a network to become inoperable. The exploit of smurfing, as it has come to be known, takes advantage of certain known characteristics of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP).

Spear Phishing
Spear phishing is an e-mail spoofing fraud attempt that targets a specific organisation, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.

SSL
(Secure Sockets Layer) SSL uses a combination of public-key and symmetric-key encryption to secure a connection between two machines, typically a Web or mail server and a client machine, communicating over the Internet or an internal network.

Steganography
Steganography (pronounced STEHG-uh-NAH-gruhf-ee, from Greek steganos, or "covered," and graphie, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.

Trojan horse
A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

White Hat
White hat describes a hacker (or, if you prefer, cracker) who identifies a security weakness in a computer system or network but, instead of taking malicious advantage of it, exposes the weakness in a way that will allow the system's owners to fix the breach before it can be taken advantage by others (such as black hat hackers.) Methods of telling the owners about it range from a simple phone call through sending an e-mail note to a Webmaster or administrator all the way to leaving an electronic "calling card" in the system that makes it obvious that security has been breached.

Worm
In a computer, a worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user.