Computer Security Related Terms and Definitions

By Bob (Daddybob) Kober – 26 Oct 2005

TABLE OF CONTENTS

Computer Security Related Terms and Definitions

By Bob (Daddybob) Kober – 26 Oct 2005

Adware - (ADvertisementWARE)
Adware is any software application or program in which advertising banners are displayed or Pop-up windows appear while the program is running. Adware is considered "spyware" and is installed without the user's knowledge. It typically displays targeted ads based on words searched for on the Web or derived from a user's surfing habits that have been periodically sent in the background to a Web server.

Ad Server
An ad server is a Web-based server that delivers banner ads to the requesting Web pages. For websites that sell their own ads, the ad server may be an in-house or co-located machine at an Internet service provider (ISP), or it may be owned by an Internet advertising company.

Backbone
The backbone of the Internet is the collection of major communications pipelines that transfer the data from one end of the world to the other. Larger ISP's make up the backbone. They connect through major switching centers called MAE (Metropolitan Area Exchange) and exchange data from each others customers through peering agreements.

Backdoor
A backdoor is a secret or undocumented means of getting into a computer system. Many programs have backdoors placed by the programmer to allow them to gain access to troubleshoot or change the program. Some backdoors are placed by hackers once they gain access to allow themselves an easier way in next time or in case their original entrance is discovered.

Browser Hijacker
A Browser Hijacker is any program that changes some settings in your browser. Browser hijackers commonly redirect your "search" page to pass all searches to a certain pay-per-search site, change the default home page to the desired company page and often transmit URLs (websites) viewed toward the desired company server.

Cookie
A Cookie is a small data file created by a Web server that is stored on your computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the Web site to identify users and keep track of their preferences. It is also commonly used to "maintain the state" of the session as a user browses around on the site.

Note: The default settings in your Web browser typically allow "first-party" cookies that do not contain any personal information, but "third-party" cookies are created by a Web site other than the one you are currently visiting; for

example, by a third-party advertiser on that site. A lot of personal data resides in the cookie files in your computer. As a result, this storehouse of private information is sometimes the object of attack.

Denial of Service (DoS)
A denial of service attack floods a network with an overwhelming amount of traffic, slowing its response time for legitimate traffic or grinding it to a halt completely. The more common attacks use built-in "features" of the TCP/IP protocol to create exponential amounts of network traffic.

Dialer
A Dialer is a type of software that silently disconnects your modem from your usual Internet service provider and dials another phone number. The new number is usually a long distance or 1-900 billable call.

Dumpster Diving
Dumpster diving is a term used when looking for treasure in someone else's trash. In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. It is also a way to gain the information necessary to carry out Identify Theft

Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network.

E-mail Harvester
An E-Mail Harvester is a person or software that searches the Internet looking for valid e-mail addresses. E-mail addresses are compiled into directories that are purchased and maintained by spammers.

Encryption
Encryption is taking your text, data, or other communications and encoding it so that those who should not see or hear it will not be able to. An encrypted file will appear as gibberish unless you have the password or key necessary to decrypt the information.

Firewall
Any software program or hardware device designed to prevent computers on a network from communicating directly with external computer systems by filtering the information coming through the Internet connection into your private network or computer system. A Firewall keeps hackers out and personal

data in by acting as a barrier through which all information passing between the network or computer and external systems must pass.

Hacker
A slang term for a person who writes programs in an attempt to gain unauthorized access to computer systems Although it may refer to any programmer, it implies very tedious "hacking away" in an attempt to steal, disrupt or corrupt a computer system or network.

Heuristics
Heuristics uses past experience to make educated guesses about the present. Using rules and decisions based on analysis of past network or email traffic, heuristic scanning in antivirus software can self-learn and use artificial intelligence to attempt to block viruses or worms that are not yet known about and for which the antivirus software does not yet have a filter to detect or block.

Hoax
A Hoax is usually an e-mail that gets mailed in chain letter fashion describing some devastating, highly unlikely type of virus. Hoaxes are detectable as having no file attachment, no reference to a third party who can validate the claim.

Note: Some "hoaxes" instruct you to change or delete a specific system file or setting which can damage your system.

Honeypot
A honeypot is a computer system intended to attract or lure attackers to it. A honeypot serves to distract attackers from the real targets as a decoy as well as a means to track and monitor attacks to learn from them in order to develop better protection for the real systems.

IP (Internet Protocol)
The IP is used to deliver data packets to their proper destination. Each packet contains both the originating and destination IP address. Each router or gateway that receives the packet will look at the destination address and determine how to forward the packet on. The packet will be passed from device to device in this way until it reaches its destination.

IP Address
An IP Address is used to uniquely identify devices on the Internet. In the current standard, it is a 32-bit number made up of 4 8-bit blocks. In standard decimal numbers, each block can be any number from 0 to 255. A standard IP Address would look something like "192.168.45.28".

Computer Security Related Terms and Definitions

By Bob (Daddybob) Kober – 26 Oct 2005

Identity Theft
Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

ISP (Internet Service Provider)
An ISP is a company that has the servers, routers, communication lines and other equipment necessary to establish a presence on the Internet. They in turn sell access to their equipment in the form of Internet service as dial-up, cable modem, DSL or other types of connections. i.e.: AOL, MSN, Bellsouth, Earthlink, etc.

Key Logger
A computer program or hardware device specialized to record your keystrokes. It can record anything that you type, including your passwords, e-mails, credit card number. They save the recorded keystrokes into a log file or send them to another machine. Most key-loggers can be detected by spyware removal software.

Malware (Malicious Code)
Malware is a catch-all term used to refer to various types of software that can cause problems or damage your computer. The more common classes of program referred to as malicious code are viruses, worms, Trojan horses, macro viruses, and backdoors.

NAT (Network Address Translation)
NAT is used to mask the true identity of internal computers. Typically, the NAT server or device has a public IP address that can be seen by external Hosts. Computers on the local network use a completely different set of IP addresses which cannot be seen from the outside. When traffic goes out the internal IP address is removed and replaced with the public IP address of the NAT device. When replies come back to the NAT device it determines which internal computer the response belongs to and routes it to its proper destination.

Packet (Datagram)
Data being transmitted is broken up into fragments called packets. Each packet contains a portion of the data being sent as well as header information which includes the destination address.

Packet Sniffing
Packet sniffing is the act of capturing packets of data flowing across a computer network. The software or device used to do this is called a packet sniffer. Packet

sniffing is to computer networks what wire tapping is to a telephone network. It is widely used by hackers to gather information illegally like passwords, IP addresses, protocols being used on the network and other information that will help the attacker do his dirty work.

Packet sniffing also has legitimate uses to monitor network performance or troubleshoot problems with network communications.

Patch
A patch is like a band-aid. As a company finds bugs and defects in their software that needs fixing and they plan to do this in their next release of the application. However, some bugs make the current product inoperable or less functional or may even open security vulnerabilities. For these bugs the users can not wait until the next release to get a fix so the company must create a small interim fix that users can apply to fix the problem. Sometimes called “Hot Fixes”.

Peer-To-Peer Networking (P2P)
Peer-to-Peer Networking is a phrase coined to apply to individual PC's acting as servers to other individual PC's. Made popular by the music file swapping service Napster, and KaZaA, P2P allows users to share files with each other through a network of computers using that same P2P client software. Each computer on the network has the ability to act as a server by hosting files for others to download as well as a client by searching other computers on the network for files they want.

Pharming (Farm-ing)
Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure."

In pharming, larger numbers of computer users can be victimized because it is not necessary to target individuals one by one and no conscious action is required on the part of the victim. A computer with a compromised host file will go to the fake Web site even if a user types in the correct Internet address or clicks on an affected bookmark entry.

Phishing (Fish-ing)
Phishing is committing fraud to get financial information without the user realizing it. Trying to trick somebody into providing bank or credit-card information. This is usually done by sending a fraudulent e-mail purporting to be from a bank, Internet provider, etc. asking for verification of an account number or password.

Computer Security Related Terms and Definitions

By Bob (Daddybob) Kober – 26 Oct 2005

Pop-Up

A Pop-Up is a small window that is displayed on top of the existing windows on screen. A popup window can be used in any application to display new information. It is widely used on Web pages to cause an ad to "pop up;" however, pop-ups can be prevented or made to appear beneath the browser window using various pop-up blockers.

Port

Port has a dual definition in computers. There are various ports on the computer itself: ports to plug in your mouse, keyboard, USB devices, printer, monitor, etc. The kind of ports that are more relevant to information security, however, are virtual ports that are found in TCP/IP. Ports are like channels on your computer. Normal web or HTTP traffic flows on port 80. POP3 email flows on port 110. By blocking or opening these ports into and out of your network you can control what kinds of data can flow through your network.

Port Scan (Port Sniffing)

A port scan is a method used by hackers to determine what ports are open or in use on a system or network. By using various tools a hacker can send data to TCP or UDP ports one at a time. Based on the response received the port scan utility can determine if that port is in use. Using this information the hacker can then focus their attack on the ports that are open and try to exploit any weaknesses to gain access

Protocol

A protocol is a set of rules or agreed upon guidelines for communication. When communicating, it is important to agree on how to do it. If one party speaks French and one German the communications will most likely fail. If they both agree on a single language communications will work.

On the Internet the set of communications protocols used is called TCP/IP. TCP/IP is actually a collection of various protocols, each having their own special function or purpose. These protocols have been established by international bodies and are used on almost all platforms around the globe to ensure that all devices on the Internet can communicate successfully.

Proxy Server

A proxy server acts as a middleman between your internal and external networks. It serves the dual roles of speeding up access to the Internet as well as providing a layer of protection for the internal network. By caching pages that have been previously requested, the proxy server speeds up performance by responding to future requests for the same page using the cached information rather than going to the web site again.

When using a proxy server, external systems only see the IP address of the proxy server so the true identity of internal computers is hidden. The proxy server can also be configured with basic rules of what ports or IP addresses are or are not allowed to pass through which makes it a type of firewall.

SMTP (Simple Mail Transfer Protocol)
SMTP, used to send email, provides a common language for different servers to send and receive email messages. The default TCP/IP port for the SMTP is port 25.

Social Engineering
Social Engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. They might call the authorized employee with some kind of urgent problem; social engineers often rely on the natural helpfulness of people as well as on their weaknesses. Appealing to ones vanity or authority, flattery and old-fashioned eavesdropping are typical social engineering techniques

Spam
Spam is E-mail that is not requested. Also known as "unsolicited commercial e-mail" (UCE), "unsolicited bulk e-mail" (UBE), "gray mail" and just plain "junk mail." Spam is used to advertise products or to broadcast some political or social commentary.

Spamware
Spamware is software used by spammers to send large amounts of spam to e-mail address lists. Spamware is also a variety of trojan that can turn your computer into a sender of spam or even viruses.

Spoofing (E-mail)
Email spoofing is the act of forging the header information on an email so that it appears to have originated from somewhere other than its true source. By changing the header information someone can make the email appear to come from whoever they choose. It is used by virus writes. By propagating a virus with a spoofed email source it is more difficult to track its source to stop the virus. Email spoofing is also used by distributors of spam to hide their identity.

Spyware
Spyware is software that sends information about your Web surfing habits to its Web site. Spyware is often installed without the user's knowledge or explicit permission in combination with a free download.

TCP/IP (Transmission Control Protocol / Internet Protocol)
TCP/IP is a suite of protocols which make up the basic framework for communication on the Internet. The first part, TCP, helps to control how the larger data is broken down into smaller

pieces or packets for transmission. It also handles reassembling the packets at the destination end and performing error-checking to ensure all of the packets arrived properly and were reassembled in the correct sequence.

IP is used to route the packets to the appropriate destination. It is the IP protocol which manages the addressing of the packets and it is the IP protocol which tells each router or gateway on the path how and where to forward the packet to direct it to its proper destination.

Trojan Horse
A Trojan Horse is a program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information or make the system more vulnerable to future entry or simply destroy programs or data on the hard disk.

VBScript (Visual Basic Script)
VBScript is an active scripting language created by Microsoft to compete with Netscape's JavaScript. VBScript is based on Microsoft's popular programming language Visual Basic. VBScript is an active scripting language used within HTML to execute small programs to generate a dynamic web page. Using VBScript a developer can cause text or graphics to change when the mouse points at them, update the current date and time on the web page or add personal information like how long it's been since that user last visited the site.

Virus
Viruses are software used to infect a computer. After the virus code is written, it is buried within an existing program. Once that program is executed, the virus code is activated and attaches copies of itself to other programs in the system. Infected programs copy the virus to other programs.

Vulnerability
In computer and network security, vulnerability refers to any flaw or weakness in the computer's or network's defense that could be exploited to gain unauthorized access to, damage or otherwise affect the computer or network.

Worm
A Worm is a destructive program that replicates itself throughout disk and memory, using up computer resources until the computer becomes unusable.