CPCU Greater Detroit Chapter

Presents

HACKED! A Discussion of Cyber Liability

Cyber Security Limited Glossary

Various resources:
www.webopedia.com.
csrc.nist.gov/publications/nistir/ir7298.../nistir-7298-revision1.pdf
http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=%2Frzaj4%2Frzaj4rzaj45bfsecurityterminology.htm
http://www.madirish.net/22#dos
http://www.sans.org/security-resources/glossary-of-terms/

Adware: A form of spyware that collects information about the user in order to display advertisements in the Web browser based on the information it collects from the user's browsing patterns.
ARPANET (Advanced Research Projects Agency Network): A pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990.
Attachment: A document, a picture, a video clip, program or any other kind of file that can be attached and sent with an e-mail or instant message. Malicious programs, viruses or spyware are commonly spread through attachments. Never open or download an IM or e-mail attachment from an unknown source or one that you are not expecting. Be cautious of attachments ending in .exe, .com, .scr, .bat or .pif.
Authentication: To gain access to many secure systems, you have to identify yourself. Authentication is the process of providing information to identify yourself. Many systems utilize an ID and a password for users to authenticate. Other systems require an ID, a password, and a series of other tests (i.e. personal questions, fingerprint scans, etc) for a more robust authentication.
Banker Trojan: In computer and network security terminology, a Banker Trojan-horse (commonly called Banker Trojan) is a malicious program used in an attempt to obtain confidential information about customers and clients using online banking and payment systems.
Botnet: A botnet refers to a type of bot running on an IRC network that has been created with a trojan. When an infected computer is on the Internet the bot can then start up an IRC client and connect to an IRC server. The Trojan will also have been coded to make the bot join a certain chat room once it has connected. Multiple bots can then join in one channels and the person who has made them can now spam IRC chat rooms, launch huge numbers of Denial of Service attacks against the IRC servers causing them to go down.
Browser hijacker: A specific type of spyware that will allow a hacker or malicious perpetrator to spy on the infected computer's Internet browsing activity. Using a browser hijacker the person responsible for the spyware can deliver pop-up ads, reset the browser homepage, or direct the browser to Web sites the victim would not normally visit.
Computer Virus: A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.
Computer Worm: A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. Also see virus.

HACKED! A Discussion of Cyber Liability

Cookie: A small data file that a Web site installs on your computer's hard drive to collect information about your activities on the site or to allow other capabilities on the site. Web sites use cookies to identify returning visitors and profile their preferences on the site. For example, many online shopping sites use cookies to monitor what items a particular shopper is buying to suggest similar items. Cookies are somewhat controversial as they raise questions of privacy and can be used by hackers as spyware.

Cracker: To break into a computer system. The term was coined in the mid-80s by hackers who wanted to differentiate themselves from individuals whose sole purpose is to sneak through security systems. Whereas crackers sole aim is to break into secure systems, hackers are more interested in gaining knowledge about computer systems and possibly using this knowledge for playful pranks. Although hackers still argue that there's a big difference between what they do and what crackers do, the mass media has failed to understand the distinction, so the two terms - hack and crack - are often used interchangeably.

Cyber Attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Crime: Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet.

Denial of Service Attack (DoS): Also sometime misnomered as dDos (Distributed Denial of Service), a denial of service is an attack which causes a targets internet connection to become flooded out. This is usually accomplished by sending an unusually large number or size of packets to a target, causing servers to crash or internet connections to stop responding. Due to advances in techniques to combat DoS attacks, many attackers have turned to a distributed Denial of Service. This type of attack involves a large number of machines to attack a target at once, thereby increasing the chances of service interruption. DoS attacks are commonly combined with packet spoofing to hide the origin of the attack. Some DoS events are caused by completely legitimate traffic. The slashdot effect, for instance, which is caused by a huge number of people requesting a web page and crashing the web server, is a completely legitimate DoS attack.

Digital certificate: A digital certificate is a digital document that validates the identity of the certificate's owner, much as a passport does. A trusted party, called a Certificate Authority (CA) issues digital certificates to users and servers. The trust in the CA is the foundation of trust in the certificate as a valid credential. You can use them for the following: Identification - who is the user; Authentication - ensuring that the user is who he says that he is; Integrity - determining whether the contents of a document have been altered by verifying the sender's digital "signature"; Non-repudiation - guaranteeing that a user cannot claim to not have performed some action. For example, the user cannot dispute that he authorized an electronic purchase with a credit card.

Digital signature: A digital signature on an electronic document is equivalent to a personal signature on a written document. A digital signature provides proof of the document's origin. The certificate owner "signs" a document by using the private key that is associated with the certificate. The recipient of the document uses the corresponding public key to decrypt the signature, which verifies the sender as the source.

Disk Scrubbing: When a disk drive will no longer be used, it is important to fully delete all of the information that is on the drive so that no one else can access the information. Scrubbing a disk means writing over each bit on the drive with new (and usually random) information. Because there are now sophisticated tools to recover information from an erased or overwritten drive, best practices recommend scrubbing a disk several times to make sure the drive is truly cleaned.

CPCU Greater Detroit Chapter

P.O. Box 2965
Farmington Hills, MI 48333-2965

HACKED! A Discussion of Cyber Liability

Domain Hijacking: 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 server (DNS): An Internet host that converts Internet names to IP addresses, often by interacting with other DNS servers on the Internet. For example, many DNS servers might recognize vnet.ibm.com. But perhaps only a few know the complete IP address for: system1.vnet.ibm.com. When you attach to the Internet, your Internet client uses a domain name server to determine the IP address for the host system with which you wish to communicate.

Encryption: The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

File Sharing: The process of sending a file from one computer to another computer. Some file sharing systems allow multiple computers to draw files down from one central machine. Other file sharing systems only transfer files from one computer to another. This individual computer to computer type of file sharing is often referred to as peer to peer file sharing.

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Hacker: A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s). Among professional programmers, depending on how it used, the term can be either complimentary or derogatory, although it is developing an increasingly derogatory connotation. The pejorative sense of hacker is becoming more prominent largely because the popular press has coopted the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker.

Hash Functions: (cryptographic) Hash functions are used to generate a one way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHA1.

Honeypot: An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored. Most honeypots are installed inside firewalls so that they can better be controlled, though it is possible to install them outside of firewalls. A firewall in a honeypot works in the opposite way that a normal firewall works: instead of restricting what comes into a system from the Internet, the honeypot firewall allows all traffic to come in from the Internet and restricts what the system sends back out.

Hypertext markup language (HTML): The language that is used to define hypertext documents. Use HTML to indicate how your document should look (such as highlighting and type style) and how it should be linked to other documents or objects.

HTTP (Hypertext Transfer Protocol): This is the predominant language that computers use to communicate with each other on the Internet. Web site addresses tend to start with http://www.

HACKED! A Discussion of Cyber Liability

Password cracking: The process of attempting to guess or crack passwords to gain access to a computer system or network. Crackers will generally use a variety of tools, scripts, or software to crack a system password. The goal of the cracker is to ideally obtain the password for root (UNIX) or system and administrator (Windows, NT). Password cracks work by comparing every encrypted dictionary word against the entries in system password file until a match is found.
P2P: Peer-to-peer (often shortened to P2P) is a specific type of file sharing network. Original file sharing networks used a single centralized server that searches and files would pass through. P2P directly connects one computer to another to make file transfers and to share bandwidth. This often makes the files transfer faster. P2P networks are often more difficult more monitor than a centralized file server.
PGP: Abbreviated as PGP (Pretty Good Privacy), a technique developed by Philip Zimmerman of Network Associates, Inc., for encrypting messages. PGP is one of the most common ways to protect messages on the Internet because it is effective, easy to use, and free. PGP is based on the public-key method, which uses two keys - one is a public key that you disseminate to anyone from whom you want to receive a message. The other is a private key that you use to decrypt messages that you receive.
Pharming: This is a more sophisticated form of MITM attack. A user's session is redirected to a masquerading website. This can be achieved by corrupting a DNS server on the Internet and pointing a URL to the masquerading website's IP. Almost all users use a URL like www.worldbank.com instead of the real IP (192.86.99.140) of the website. Changing the pointers on a DNS server, the URL can be redirected to send traffic to the IP of the pseudo website. At the pseudo website, transactions can be mimicked and information like login credentials can be gathered. With this the attacker can access the real www.worldbank.com site and conduct transactions using the credentials of a valid user on that website.
Phishing: The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the users information.
Port Scanning: Port scanning is the process by which an attacker explores the available services on a remote machine. A port scan usually consists of "stealth" attacks where a scanner sends packets that won't show up in log files. Port scanning reveals the types of remote services (ftp, telnet, etc) that are running on a target machine. Port scans are usually the first step in a cracking attempt and should be taken seriously if discovered.
Proxy Server: A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.
RAT: Short for Remote Access Trojan, a Trojan horse that provides the intruder, or hacker, with a backdoor into the infected system. This backdoor allows the hacker to snoop your system, use your infected system to launch a zombie (attacks on other systems), or even run malicious code.
Security: In the computer industry, refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.
Smart Card: A small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit (IC). Smart cards containing an IC are sometimes called Integrated Circuit Cards (ICCs).
Sniffer: A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal.

HACKED! A Discussion of Cyber Liability

Social Engineering: This refers to a direct communication, either in person, by phone, by fax or over the Internet, designed to trick you into providing your personal information. These messages usually ask you to "update" or "confirm" information by typing in a reply or clicking on a link. Legitimate institutions, such as banks, do not send e-mail or IM of this nature due to security concerns on the Internet. "Phishing" is a prime example of social engineering.
SPAM: Electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail. However, if a long-lost brother finds your e-mail address and sends you a message, this could hardly be called spam, even though it's unsolicited. Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup.
Spoof: To fool. In networking, the term is used to describe a variety of ways in which hardware and software can be fooled. IP spoofing, for example, involves trickery that makes a message appear as if it came from an authorized IP address. Also see e-mail spoofing. Spoofing is also used as a network management technique to reduce traffic. For example, most LAN protocols send out packets periodically to monitor the status of the network. LANs generally have enough bandwidth to easily absorb these network management packets. When computers are connected to the LAN over wide-area network (WAN) connections, however, this added traffic can become a problem. Not only can it strain the bandwidth limits of the WAN connection, but it can also be expensive because many WAN connections incur fees only when they are transmitting data. To reduce this problem, routers and other network devices can be programmed to spoof replies from the remote nodes. Rather than sending the packets to the remote nodes and waiting for a reply, the devices generate their own spoofed replies.
Spyware: Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.
SSH: Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.
SSL: Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data - a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http.
Turing number: Abbreviated as TN, turning number is a randomly generated security code, usually a series of digits, displayed as an image that users may need to read and copy into a form field in order to submit or validate a form submission online via a Web browser. Turing numbers are used to ensure there is a human user instead of automated (bot) submissions. Turing numbers are commonly used on e-commerce Web sites or promotional or contest Web sites -anywhere there is a need to avoid automated submissions by bots.
Trojan Horse: A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. The term comes from the Greek

HACKED! A Discussion of Cyber Liability

Virus: A computer virus refers to a program that enters your computer—often through e-mail or Internet downloads—and makes copies of itself, spreading throughout your computer and files. There is a wide range of computer viruses out there. They can be anything from merely annoying to horribly damaging—deleting files or making your computer inoperable. Keep in mind that viruses attach themselves to an application on a computer and aren't actually executed until that application is accessed or run.

Vishing: The telephone equivalent of phishing. Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

VoIP: Voice Over IP (or VoIP) is a way to route conversations, such as telephone conversations, over the internet or other networks.

VPN: Short for virtual private network, a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Worm: Just as a worm burrows through an apple making it inedible, a computer worm is a program built to reproduce itself and spread across a network, rendering it ineffective. A worm may be designed to complete several different malicious activities. However, one common denominator is that a worm can harm a network by consuming large amounts of bandwidth, potentially shutting the network down. Viruses, on the other hand, are more limited to targeting computers one-at-a-time. A virus also requires other programs to execute and replicate, whereas a worm can act independently of other programs.

Zombie: A computer overtaken by a hacker and used to perform malicious tasks. Commonly, zombie computers are used to send large amounts of spam or host fraudulent Web sites.