Chapter computer

Technology, Computer

Example: Stealing a organization's proprietary information. Such as research and development Information. B. Identity theft- Breaking Into a computer to destroy or alter data records. Examples of data loss: sending a virus that reformats a computer's hard drive. Examples of data manipulation: breaking Into a records system to change Information, such as the price of an item. C. Data loss / manipulation - A form of Information theft where personal Information Is stolen for the purpose of taken over someone's Identity. Using this Information an Individual can obtain legal documents, apply for credit ND make unauthorized online purchases. Identity theft is a growing problem costing billions of dollars per year. Preventing legitimate users from accessing services to which they should be entitled. 2. Activity Identify the type of security threat described by connecting the correct threat with its definition. [pick] 3. Explain what External Threats are. External threats arise from individuals working outside of an organization. They do not have authorized access to the computer systems or network. External attackers work their way into a network mainly from the Internet, wireless links or dialup access servers. . Explain what Internal Threats are. Internal threats occur when someone has authorized access to the network through a user account or have physical access to the network equipment. The internal attacker knows the internal politics and people. They often know what information is both valuable and vulnerable and how to get to it. 5. Explain Social Engineering including how it relates to computer and networking security. Social engineering is a term that refers to the ability of something or someone to influence the behavior of a group of people.

In the context of computer and network security Social Engineering refers to a collection of techniques used to deceive internal users into performing specific actions or revealing confidential information. 6. List and explain the three most commonly used techniques in social engineering. Presenting - Presenting is a form of social engineering where an invented scenario (the pretext) is used on a victim in order to get the victim to release information or perform an effective, the attacker must be able to establish legitimacy with the intended target, or victim.

This often requires some prior knowledge or research on the part of he attacker. For example, if an attacker knows the target's social security number, they may use that information to gain the trust of their target. The target is then more likely to release further information Fishing - Fishing is a form of social engineering where the fisher pretends to represent a legitimate outside organization. They typically contact the target individual (the peevish) via email. The fisher might ask for verification of information, such as passwords or surnames in order prevent some terrible consequence from occurring Fishing / Phone Fishing -

A new form of social engineering that uses Voice over IP (Poi) is known as fishing. With fishing, an unsuspecting user is sent a voice mail instructing them to call a number which appears to be a legitimate telephone-banking service. The call is then intercepted by a thief. Bank account numbers or passwords entered over the phone for verification are then stolen. 8. 2 7. Explain in detail the following terms: Viruses -A virus is a program that runs

and spreads by modifying other programs or files. A virus cannot start by itself; it needs to be activated.

Once activated, a virus ay do nothing more than replicate itself and spread. Though simple, even this type of virus is dangerous as it can quickly use all available memory and bring a system to a halt. A more serious virus may be programmed to delete or corrupt specific files before spreading. Viruses can be transmitted via email attachments, downloaded files, instant messages or via diskette, CD or USB devices. Worms - A worm is similar to a virus, but unlike a virus does not need to attach connected hosts. Worms can run independently and spread quickly.

They do not necessarily require activation or human intervention. Self-spreading network rooms can have a much greater impact than a single virus and can infect large parts of the Internet quickly. Trojan Horses - A Trojan horse is a non-self replicating program that is written to appear like a legitimate program, when in fact it is an attack tool. A Trojan horse relies upon its legitimate appearance to deceive the victim into initiating the program. It may be relatively harmless or can contain code that can damage the contents of the computer's hard drive.

Trojan can also create a back door into a system allowing hackers to gain access. Denial of Service (DOS) - DOS attacks are aggressive attacks on an individual imputer or groups of computers with the intent to deny services to intended users. DOS attacks can target end user systems, servers, routers, and network links. Len general, DOS attacks seek to: Flood a system or network with traffic to prevent legitimate network traffic from flowing Disrupt

connections between a client and server to prevent access to a service SYNC (synchronous) Flooding - a flood of packets are sent to a server requesting a client connection.

The packets contain invalid source IP addresses. The server becomes occupied trying to respond to these fake requests and therefore cannot respond to legitimate ones. Ping of death - a packet that is greater in size than the maximum allowed by IP (65, 535 bytes) is sent to a device. This can cause the receiving system to crash. Distributed Denial of Service (Dodos) - Dodos is a more sophisticated and potentially damaging form of the DOS attack. It is designed to saturate and than DOS attacks. Typically hundreds or thousands of attack points attempt to overwhelm a target simultaneously.

The attack points may be unsuspecting computers that have been previously infected by the Dodos code. The systems that are infected with the Dodos code attack the target site when invoked. Brute Force - Not all attacks that cause network outages are specifically DOS attacks. A Brute force attack is another type of attack that may result in denial of services. With brute force attacks, a fast computer is used to try to guess passwords or to decipher an encryption code. The attacker tries a large number of possibilities in rapid succession to gain access or crack the code.

Brute force attacks can cause a denial of service due to excessive traffic to a specific resource or by locking out user accounts. Spy; are - Spy; are is any program that gathers personal information from your imputer without your permission or knowledge. This information is sent to advertisers or others on the Internet and can include passwords and account numbers. Spy; are is

usually installed unknowingly when downloading a file, installing another program or clicking a popup. It can slow down a computer and make changes to internal settings creating more vulnerabilities for other threats.

In addition, spare can be very difficult to remove. Tracking Cookies - Cookies are a form of spare but are not always bad. They are used to record information about an Internet user when they visit websites. Cookies may be useful or desirable by allowing personalization and other time saving techniques. Many web sites require that cookies be enabled in order to allow the user to connect. Edward - Edward is a form of spare used to collect information about a user based on websites the user visits. That information is then used for targeted advertising.

Edward is commonly installed by a user in exchange for a " free" product. When a user opens a browser window, Edward can start new browser instances which attempt to advertise products or services based on a user's surfing practices. The unwanted browser windows can open repeatedly, and can make surfing the Internet very difficult, especially with slow Internet connections. Edward can be very difficult to install. Pop-ups and pop-enders - Pop-ups and pop-enders are additional advertising windows that display when visiting a web site.

Unlike Edward, pop-ups and pop- enders are not intended to collect information about the user and are typically associated only with the web-site being visited. Pop-ups: open in front of the current 8. How does the Cisco curriculum explain what Spam is? Another annoying by-product of our increasing reliance on electronic ammunitions is unwanted bulk email.

Sometimes merchants do not want to bother with targeted marketing. They want to send their email advertising to as many end users as possible hoping that someone is interested in their product or service.

This widely distributed approach to marketing on the Internet is called spam. 8. 3 9. Explain what an acceptable use policy is. A security policy is a formal statement of the rules that users must adhere to when accessing technology and information assets. It can be as simple as an acceptable use policy, or can be several hundred pages in length, and detail every aspect of user connectivity and network usage procedures. 10. List possible security tools and applications used in securing networks. A. Software patches and updates b. Virus protection c. Spy; are protection d.

Spam blockers e. Pop-up blockers f. Firewalls 11. What is a patch? A patch is a small piece of code that fixes a specific problem. 12. What is an update? Package as well as patches for specific issues. 13. List common signs that a virus, worm or Trojan horse may be present on a computer. A. Computer starts acting abnormally b. Program does not respond to mouse and keystrokes. C. Programs starting or shutting down on their own. D. Email program begins sending out large quantities of email e. CPU usage is very high f. There are unidentifiable, or a large number of, processes running.

Computer slows down significantly or crashes g. 14. Ann-virus software relies on what information to remove viruses? Ann-virus software relies on knowledge of the virus to remove it. 15. What is Anti-Spam software? Ann-spam software protects hosts by identifying spam and performing an action, such as placing it into a Junk folder or deleting it. 16. What is the draw back

to Anti-Spam software? Ann-spam software does not recognize all spam, so it is important to open email carefully. It may also accidentally identify wanted email as spam and treat it as such. 8. 4 use to prevent the spread of spam? . Apply SO and application updates when available. B. Run an Antivirus program regularly and keep it up to date. C. Do not forward suspect emails. D. Do not open email attachments, especially from people you do not know. E. Set up rules in your email to delete spam that by-pass the anti-spam software. F. Identify sources of spam and report it to a network administrator so it can be blocked. G. Report incidents to the governmental agency that deals with abuse by spam. 18. Activity Identify the type of security tool described by connecting it to the correct definition. 19.

Explain how firewalls use NAT to help with network security? Firewalls often perform Network Address Translation (NAT). NAT translates an internal address or group of addresses into an outside, public address that is sent across the network. This allows internal IP addresses to be concealed from outside users. 20. Firewall products come packaged in various forms. List and explain each. A dedicated hardware device known as a security appliance. Server-based firewalls - A server-based firewall consists of a firewall application that runs on a network operating system (NOSE) such as UNIX, Windows or Novel.

Integrated Firewalls - An integrated firewall is implemented by adding firewall functionality to an existing device, such as a router. Personal firewalls - Personal firewalls reside on host computers and are not designed for LANA implementations. They may be available by default from the SO or

may be installed from an outside vendor. 21 . What is a demoralized zone or DMZ? In computer networking, a DMZ refers to an area of the network that is accessible o both internal and external users. It is more secure than the external network but not as secure as the internal network. 22.

Using an SIR a more restrictive DMZ can be set up using the port forwarding capability. Explain how this operates. With port forwarding, ports that should be accessible on the server are specified. In this case, only traffic destined for those port(s) is allowed, all other traffic is excluded. 23. The wireless access point within the integrated router is considered part of the internal network. Why can this be a problem? It is important to realize that if the wireless access point is unsecured, anyone who oneness to it is within the protected part of the internal network and is behind the firewall.