Chapter Summary

- Computer security is more than the hunt for intruders; It also includes creating a protective mindset and abiding by security policies.
- The terms "Hacking" and "Hacker" did not originally have the negative connotation they often do today.
- Intruders to systems can be classified as *directed* and *undirected* hackers, each with different motives but often having similar effects on the systems they target.
- Crackers can find holes in systems put there intentionally or unintentionally by system administrators and programmers.
- Crackers use malicious software such as: Viruses, Worms and Trojan programs, to infiltrate systems.
- One of the greatest risks to a company and its computers is *social engineering* human manipulation.
- There are 4 types of attacks on computers: Access, Modification, Denial of Service and Repudiation.
- Total risk to an organization is made up of: Vulnerability, Treat and existing countermeasures.
- Intruders target the: confidentiality, integrity, availability or accountability of a system's information.
- Counter-measures in managing security include: common-sense behavior, creating and following security procedures, using encryption, anti-virus software, firewalls and system setup and architecture.
- You need to install anti-virus software, perform system updates, physically restrict access to your computer and have a good backup system.
- Users support cracking by: using weak passwords you need to have strong passwords.
- One way to secure communication over a network is to encrypt the information by using one of a number of encryption schemes, such as using private and public keys.
- Firewalls and routers can be set up so that certain ports are available, and certain servers such as the company Website server can sit in a DMZ, a more public and less protected part of the network.
- Prosecuting computer attacks has often been difficult because of vitiations in national and international laws as-well-as the difficulty in proving the case
- Despite the difficulties in persecuting computer crimes, there are laws and ethical reasoning that dictate committing such crimes is un-wise.

Key Terms:

accountability (58) Antacks on a system that can include: snooping, aewestropping and interception; more commonly known as spying accountability (58) Antibulity (58) Antibulity (58) Antibulity (58) Antibulity (58) Aprogram designed to detect and block computer viruses authentication: (58) A technique for veryfring that someone is who they say they are; A password is one type of authentication Accessibility (58) Accessibility of information and services on a normal basis backdoors; (52) Shortcus into programs created by system designed to fedicate system maintenance but used and abused by crackers. Biological identification such as fingerprints, voice dynamics or retiral scans bot; (53) A software program that can roam the internet autonomously; bots can be quite being and useful (i.e.) those used by Google buffer overflow; (52) A program tire to place more information into a memory location than that location can handle. A method that allows users to connect only by having the network initiate a call to a specified number checksum; (65) A method that allows users to connect only by having the network initiate a call to a specified number checksum; (65) A method that allows users to connect only by having the network initiate a call to a specified number checksum; (65) A method that allows users to connect only by having the network initiate a call to a specified number checksum; (65) A method that allows users to connect only by having the network initiate a call to a specified number checksum; (65) A mathematical mans to check the content of a file or value, to ensure that it has not been tampered with conditional content of a file or value, to ensure that has not been tampered with conditional content of a file or value, to ensure that has not been tampered with the content of a file or value, to ensure that has not been tampered with the content of a file or value, to ensure that has not been tampered with the content of a file or value, to ensure that has not been tampered with the content of a file or va	acceptable use policy (AUP): (61)	An organizational policy that defines who can use company computers and networks, when and how
incompatibility (58) Molinis sure a system is an secure as feasible and a record of activities exist for reconstructing a break in authorized software (44) A program designed to detect and block computer visuous computer visuous authorized computer visuous computer visuous (58) A technique for verifying that someone is who they say they are, A password is one type of authoritication visualization; (58) A cossibility of information and services on a normal basis Tackdoors; (53) Shortcust into programs created by system designes to facilitate system maintenance but used and abused by crackers. Biomentics; (53) Shortcust into programs created by system designes to facilitate system maintenance but used and abused by crackers. Biomentics; (53) Biological identification such as fingerprist, voice dynamics or refulal scans. Biometrics; (53) A software program that can cannot the intermet autonomously; bots can be quite being and useful [i.e.] those used by Google before foreofficers; (52) A program this to logice more information into a memory duction than that location can handle checksium; (65) A method that allows users to connect only by having the network initiate a call to a specified number checksium; (65) A mathematical mains to check the content of a file or value, to ensure that his has not been tampered with condition; (65) A mathematical mains to check the content of a file or value to ensure that his has not been tampered with condition; (65) A mathematical mains to check the content of a file or value to ensure that his has not been tampered with condition; (65) A mathematical mains to check the content of a file or value to ensure that his has not been tampered with condition; (65) A mathematical mains to check the content of a file or value to ensure that his has not been tampered with condition; (65) A mathematical mains to check the condition of the		
indivirus software (64) A program designed to detect and block computer visuses symmetric corpyration (88) A technique for verifying that someone is who they say they are; A password is one type of authentication availability; (58) A technique for verifying that someone is who they say they are; A password is one type of authentication availability; (58) A technique for verifying that someone is who they say they are; A password is one type of authentication availability; (58) A technique for verifying that someone is who they say they are; A password is one type of authentication availability; (58) A technique for verifying that someone is who they say they are; A password is one type of authentication availability; (58) A technique for verifying that someone is who they say they are; A password is one type of authentication availability; (53) A technique for verifying that someone is who they say they are built being and useful [i.e.] those used by Google buffer overflow: (52) A program tries to place more information into a memory location than that location can handle. Callback: (63) A mathematical means to check the content of a file or value, to ensure that it has not been tampered with confidentiality; (57) Ensuring that only those authorized to use and store I to not be users' machine copyright: (72) Cookie: (85) A program that can gather information about a user and store I to not be users' machine copyright: (72) Cookie: (86) A unwelcome system include with malicious intent. A contain under the say of the says of the s	` '	
symmetric encryption (68)		
authentication: (S8) A checkingue for verifying that someone is who they say they are; A password is one type of authentication availability; (S8) hackdoors: (S2) Shortcuts into programs created by system designes to facilitate system maintenance but used and abused by crackers. Biological identifications such as fingerprints, voice dynamics or retinal scans. Bott: (S3) A software program that can care the internet autonomously, bots can be put being and useful [Le] those used by Google buffer overflow: (S2) A program tries to place more information into a memory location than that location can handle. Callback: (C6) A method that allows users to connect only by having the network-initiate a call to a specified number checkum; (C6) A mathematical means to check the content of a file or value, to ensure that it has not been trampered with confidentiality; (S7) Enuring that only those authorized to occess information and so so condice; (S6) A program that can gather information about a user and store it on the users' machine copyright: (72) The legal right granted on a muthor for exclusive sale of merchandises or content and a numerican service of the content of a file or value, to ensure that it has not been trampered with condition of service attacks; (56) An unwelcome system intruder with malicious intent. denallarized once: (70) An unwelcome system intruder with malicious intent. denallarized once: (70) An unwelcome system intruder with malicious intent. denallarized once: (70) A colorise outside the firewalt that is more vulnerable to attack from outside digital certificate: (66) digital certificate: (66) file digital certificate: (67) file denal of Service attacks; (56) A written plan for responding to natural or other classiters, intended to minimize downtime and damage to systems and data dumpster diving; (59) File denally a cacked meritary of the classiters, intended to minimize downtime and damage to systems and classificate that productivity and human asset from the call of the particu		
invalibibity: [58] Accessibility of information and services on a normal basis lackdoors: (\$22) Shortcus into programs created by yethen designers to fallitate system maintenance but used and abused by crackers. Nometrics: (\$3) Shortcus into programs created by yethen designers to fallitate system maintenance but used and abused by crackers. Bobit: (\$3) A software program that can noam the intermet autonomously, bots can be quite benign and useful [i.e.] those used by Google buffer overflow. (\$2) A program tries to place more information into a memory location than that location can handle. Cellback: (\$5) A method that allows users to connect conity by always, the network initiate a call to a specified number (hecksum: (\$5) A method that allows users to connect conity by always, the network initiate a call to a specified number (hecksum: (\$5) A method that allows users to connect conity by always, the network initiate a call to a specified number (hecksum: (\$5) A method that allows users to connect conity to vary the construction of a file of the control of a file of the contr		
lackdoors: (S2) Shortcus into programs created by system designers to facilitate system maintenance but used and abused by crackers. blometrics: (S3) Blological identification such as fingerprints, voice dynamics or retinal scans bot: (S3) A software program that can roam the internet autonomously, bots can be quite benign and useful [i.e.] those used by Gogie buffer overflow: (S2) A program tries to place more information into a memory location than that location can handle. callback: (S1) A method that allows users to connect only by having the network initiates call to a specified number (checking). (S2) Checkium: (S5) A method that allows users to connect only by having the network initiates call to a specified number (checking). (S2) Cookie: (S5) A method that allows users to connect only by having the network initiates call to a specified number (checking). (S2) Cookie: (S5) A program that can gather information about a user and store it on the users' machine (copyright: (22) The legal right greated to an author for exclusive sale of merchandise or content An unwelcome system intruder with malicious intent. A location outside the firewall that is more vulnerable to attack from outside demiliarized zone; (T0) A location outside the firewall that is more vulnerable to attack from outside demiliarized zone; (S6) Idigital certificate; (S6) Gigital certificate; (S6) Five in the company of the certificate o	` '	
bot: (53) Biological identification such as fingerprints, write dynamics or retinal scans but: (52) A software program that can roam the internet autonomously; bots can be quite benign and useful [i.e.] those used by Google buffer overflow: (52) A program time to place more information into a memory location than that location can handle. Callback: (61) A method that allows users to connect only by having the network initiate a call to a specified number checksum; (65) A mathematical means to check the content of a file or value, to ensure it it has not been tampered with conductive contents. (65) A mathematical means to check the content of a file or value, to ensure it it has not been tampered with conductive conductive contents. (65) A program that can gather information about a user and store it on the users' machine conductive contents. (65) A program that can pather information about a user and store it on the users' machine. Copyright: (72) The legal right granted to an author for exclusive sale of merchandise or content caracter: (50) An unwelcome system intruder with macilcous intent. Genital creditation of the content of a file or content caracter. (50) A location outside the firewall that is more valentable to attack from outside direct backer: (50) Generally a cracker notivated by greed and/or politics. direct backer: (50) Generally a cracker motivated by greed and/or politics. direct backer: (50) Generally a cracker motivated by greed and/or politics. direct backer: (50) Generally a cracker motivated by greed and/or youtland to the disaster recovery plant: (61) A written plan for responding to natural or other disasters; intended to minimize downtime and damage to systems and data dumpter diving: (55) Picking through people's trash to find things of value; it has been used by thieves to glean potentially damaging information incryption. (77) Transforming original data [clinical in cooded or encuryled data is on the only by without plant in the content of the productivity and human easiers. (7		
bother overflow: (52) A software program that can coam the internet autonomously, bots can be quite beings and useful [i.e.] those used by Google buffer overflow: (52) A program tries to place more information into a memory location than that location can handle.		
Earlier overflow: (52) A program tries to place more information into a memory location than that location can handle:	, ,	
caliback: (61) A method that allows users to connect only by having the network initiate a call to a specified number checkers. (65) A mothematical means to check the content of a file or value, to ensure that it has not been tampered with confidentially: (57) Ensuring that only those authorized to access information can do so confidentially: (57) Ensuring that only those authorized to access information can do so confidentially: (57) Final page of the page		
Indexisum: (65) A mathematical means to check the content of a file or value, to ensure that it has not been tampered with confidentiality: (57) Ensuring that only those authorized to access information can do so cooke: (85) A program that can gather information about a user and store it on the users' machine copyright: (72) The legal right granted to an author for exclusive sale of merchandise or content cracker: (50) An unwelcome system intruder with malicious intent. denilariared zone: (70) A location outside the frewall that is more vulnerable to attack from outside clearly of the digital equivalent of an ID card used with encryption and issued by a 3rd party certification authority direct flacker: (50) Generally a cracker motivated by greed and/or politics. disaster recovery plan: (61) A written plan for responding to natural or other disasters; intended to minimize downtime and damage to systems and data durater driving: (55) Picking through people's trash to find things of value; it has been used by thieves to glean potentially damaging information encryption: (57) Transforming original data plaintest into coded or encrypted data so that only authorized parties can interpret it encryption key: (65) A string of bits used in an encryption algorithm to encrypt or decrypt data; ergonamics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human east ericliss: (78) Principles for judging right and worning, held by a person or group Principles for judging right and worning, held by a person or group Principles for judging right and worning, held by a penumber system; Allows entry only to authorized users hacker: (50) A technically produced to the political notion is that cracking tisted is useful for society. A principles for judging right and worning, held by a penumber system; Originally denoted good intent. Packets manifestor. (51) A document written anonymously, that justifies cracking into system	. ,	
confice (85) A program that can gather information about a user and store it on the users' machine copyright: (72) The legal right granted to an author for exclusive sale of merchandise or content (racker: (50) An unwelcome system intruder with malicious intent. denillal racker: (50) An unwelcome system intruder with malicious intent. denillal of Service attacks: (56) Attacks that prevent legitimate users from using the system or accessing information digital certificate: (66) The digital equivalent of an ID card used with encryption and issued by a 3rd party certification authority direct backer: (50) Generally a cracker motivated by greed and/or politics. disaster recovery plan: (61) picking through people's trash for individual or other disasters, intended to minimize downtime and damage to systems and data dumpster disking: (55) Picking through people's trash for individual or other disasters, intended to minimize downtime and damage to systems and data dumpster disking: (55) Picking through people's trash for individual or other disasters, intended to minimize downtime and damage to systems and data dumpster disking: (55) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption key: (65) A string of bits used in an encryption algorithm to encrypt or decrypt data; ricevall: (69) A string of bits used in an encryption algorithm to encrypt or decrypt data; ricevall: (69) SW and HM that sits between an external network and an internal computer system; Allows entry only to authorized users hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker: (51) hacker: (53) A document written anonymnously, that justifies oracking into systems as an ethical exercis		
copie: (BS) A program that can gather information about a user and store it on the users' machine copyright: (72) The legal right granted to an author for exclusive sale of merchandise or content cracker: (50) An unwelcome system intruder with malicious intent. Allocation outside the firewall that is more vulnerable to attack from outside demilitarized zone: (70) Allocation outside the firewall that is more vulnerable to attack from outside demilitarized zone: (70) The digital equivalent of an ID card used with encryption and issued by a 3rd party certification authority digital certificate: (66) The digital equivalent of an ID card used with encryption and issued by a 3rd party certification authority dissater recovery plan: (61) A written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and data disaster recovery plan: (61) 4 written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and data disaster recovery plan: (61) 4 written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and data disaster recovery plan: (61) 7 Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption (65) A string of bits used in an encryption algorithm to encrypt or decrypt data; ergonomics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hackers' manifestor (51) A technically proficent person who breaks into a computer system; Originally denoted good intent. hacker's manifestor (51) A technically proficent person who breaks into a computer system; Originally entry or human ease hackers' (50) A technically proficent		
topyright: (72) The legal right granted to an author for exclusive sale of merchandise or content Cracker: (50) An unwelcome system intruder with malicious intent. All ocation outside the firewall that is more vulnerable to attack from outside denilaci-of-service attacks: (56) Altacks that prevent legitimate users from using the system or accessing information digital certificate: (56) The digital equivalent of an ID or dur used with encryption and issued by a 3rd party certification authority disaster recovery plan: (51) A written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and data dumpster diving: (55) Picking through people's trash for find things of value; it has been used by thieves to glean potentially damaging information encryption: (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption: (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption: (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption: (58) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise (i.e.) A mind-set. hacktivism: (53) Cracking into a system as a political act. One political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trachism and system and analysism to the can be an about b		
racker: (50) An unwelcome system intruder with malicious intent. demilitarzed zone: (70) A location outside the firewall that is more vulnerable to attack from outside denial of Service attacks: (56) Attacks that prevent legitimate users from using the system or accessing information digital certificate: (66) digital certificate: (66) Attacks that prevent legitimate users from using the system or accessing information direct backer: (50) disaster recovery plan: (61) A written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and data dumpster diving: (55) Picking through people's trash to find things of value; it has been used by thieves to glean potentially damaging information encryption: (57) Transforming original data (plaintext) into code or encrypted data so that only authorized parties can interpret it encryption key: (65) A tring of bits used in an encryption algorithm to encrypt or decrypt data; ergenomics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an entical exercise [i.e.] A mind-set. hackinism: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society, heuristics: (55) In virus detection a set of trule, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypet: (64) A trap laid by a system administrator to catch and track intruders integrity: (58) horizontal control of the production of the production of the production as entire and production as en		
demilitarized zone: (70) A location outside the firewall that is more vulnerable to attack from outside denial of Service attacks: (56) Attacks that prevent legitimate users from using the system or accessing information digital certificate: (66) Girect backer: (50) Generally a cracker motivated by greed and/or politics. disaster recovery plan: (61) A written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and data dumpster diving; (55) Picking through people's trash to find things of value; it has been used by thieves to glean potentially damaging information encryption: (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption key: (65) A string of bits used in an encryption algorithm to encrypt or decrypt data; ergonomics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human east ethics: (78) Principles for judging right and wrong, held by a person or group Firewall: (69) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hackers' manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [16]. A mind-set. hackeri's manifesto: (51) A trap laid by a system and political and track intruders In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypt: (64) A trap laid by a system administrator to catch and track intruders Integrity: (58) A technique for knowing why so somen is; [16], 15, 11N Number. A rived plant property: (72) An idea or product based on an idea that ha		
denial of Service attacks: (56) Attacks that prevent legitimate users from using the system or accessing information digital certificate: (66) The digital equivalent of an ID card used with encryption and issued by a 3rd party certification authority direct backer; (50) Generally a cracker motivated by greed and/or politics. Generally a cracker motivated by greed and/or politics. direct backer; (50) A written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and data dumpster diving; (55) Picking through people's trash to find things of value; it has been used by thieves to glean potentially damaging information encryption; (57) Transforming original data (palainetx) into coded or encrypted data so that only notively admaging information encryption; (57) A string of bits used in an encryption algorithm to encrypt or decrypt data; ergonomics; (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics; (78) Principles for judging right and wrong, held by a person or group firewall; (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker's manifesto; (51) A document written anonymously, that justifies cracking into systems as a related avercise [i.e.] A mind-set. hacktrism: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics; (65) In virus detection as set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system andministrator to catchin and track intruders definition attacks: (56) A technique for knowing who someone is; [i.e.] S.I.N Number. Integrity; (58) integrity; (58) An integrity; (58) An integrity; (58) An integrity (58) A technique for knowing who someone is; [i.e.] S.I.N Number. A firewall that inspects each packet		·
digital certificate: (66) The digital equivalent of an ID card used with encryption and issued by a 3rd party certification authority direct hacker: (50) Generally a cracker motivated by greed and/or politics. A written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and data dumpster diving: (55) Picking through people's trash to find things of value; it has been used by thieves to glean potentially damaging information encryption: (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption key: (55) A string of bits used in an encryption algorithm to encrypt or decrypt data; ergonomics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker's manifesto: (51) A technically proficient person who breaks into a computer system; Originally denoted good intent. Abacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an erbical exercise [i.e.] A mind-set. hacktivism: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. Ineuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is, (i.e.) 5.1.N Number. Integrity: (58) A survance that information is what you think it is and has not been modified a trap laid by a system administrator to catch and track intruders identification attacks: (56) A tracking into systems and an aload that has commercial vau		
direct hacker: (50) disaster recovery plan: (61) disaster recovery plan: (61) A written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and dat dumpster diving: (55) Picking through people's trash to find things of value; it has been used by thieves to glean potentially damaging information encryption: (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption key: (65) A string of bits used in an encryption algorithm to encrypt or decrypt data; ergonomics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker: (50) A technically proficient person who breask into a computer system; Originally denoted good intent. hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set. hackinsm: (51) Cracking into a system as a political act; One political notion is that cracking istelf is useful for society. heuristics: (55) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I. Number. honeypot: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) A flackson as system that alter information illicity packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its d	, ,	
disaster recovery plan: (61) A written plan for responding to natural or other disasters, intended to minimize downtime and damage to systems and data dumpster diving: (55) Picking through people's trash to find things of value; It has been used by thieves to glean potentially damaging information encryption: (57) Transforming original data (plainets) into coded or encrypted data so that only authorized parties can interpret it encryption key: (65) A string of bits used in an encryption algorithm to encrypt or decrypt data; ergonomics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker's manifesto: (51) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set. hacker's manifesto: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeyot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; (i.e.] S.I.N Number. integrity: (58) A surance that information is what you think it is and has not been modified intellectual property: (72) An idea or product based on an idea that has commercial value, such as ilteracy or artistic work malicious code: (53) A government grant that gives the sole of the product of time. Phreaking: (50) A firewall that inspects each packet and moves it along an established link to its destination; usually fas		
dumpster diving: (55) Picking through people's trash to find things of value; It has been used by thieves to glean potentially damaging information encryption; (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption; (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption; (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption; (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics; (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and thy that sits between an external network and an internal computer system; Allows entry only to authorized users hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set. hacker's manifesto: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (59) Assurance that information is what you think it is and has not been modified intellectual property: (72) Anice or product based on an idea that has commercial value, such as literacy or artistic work modification attacks: (56) Attacks on a system that alter information illicity packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but		, , , , , , , , , , , , , , , , , , , ,
encryption: (57) Transforming original data (plaintext) into coded or encrypted data so that only authorized parties can interpret it encryption key: (65) A string of bits used in an encryption algorithm to encrypt or decrypt data; ergonomics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacktivism: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set. hacktivism: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (58) Assurance that information is what you think it is and has not been modified intellectual property: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) A tracks on a system that alter information illicitity and threaten digital information; often called a virus. A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information and its designatio		
encryption key: (65) A string of bits used in an encryption algorithm to encrypt or decrypt data; ergonomics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human ease ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethicial exercise [i.e.] A mind-set. hacktrys manifesto: (51) Cracking into a system as a political act; one political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number A string of bits useful for society. An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) Attacks on a system that alter information illicity packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure Phreaking: (50) Subverting the phone system to get free service. Prevacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Reverse Engineer: (73) To figure out the design of a program or dev		
ergonomics: (83) Science of the relationship between people and machines, designing work areas to facilitate both productivity and human eas ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set. hacktivism: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics: (55) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (58) Assurance that information is what you think it is and has not been modified intellectual property: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (69) A Attacks on a system that alter information illicitly packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Phreaking: (50) Subverting the phone system to get free service. Phreaking: (50) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56)		
ethics: (78) Principles for judging right and wrong, held by a person or group firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set. hacktivism: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (58) Assurance that information is what you think it is and has not been modified intellectual property: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) Attacks on a system that alter information illicitly packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) Agovernment grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the		
firewall: (69) SW and HW that sits between an external network and an internal computer system; Allows entry only to authorized users hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set. hacker's manifesto: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (58) A surrance that information is what you think it is and has not been modified intellectual property: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) Attacks on a system that alter information illicity packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking		
hacker: (50) A technically proficient person who breaks into a computer system; Originally denoted good intent. hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set. hackivism: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) packet-filtering firewall: (69) packet-filtering firewall: (69) patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) Repudation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Scripts (54) Social Engineering: (54) Social Interaction that preys on human guillibility, sympathy or fear to take		
hacker's manifesto: (51) A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set. hacktivism: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (58) Assurance that information is what you think it is and has not been modified intellectual property: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) Attacks on a system that alter information illicity packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Solida Engineering		
hacktivism: (51) Cracking into a system as a political act; One political notion is that cracking itself is useful for society. heuristics: (65) In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems honeypot: (64) A trap laid by a system administrator to catch and track intruders identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (58) Assurance that information is what you think it is and has not been modified intellectual property: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) Attacks on a system that alter information illicitly packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Script Kiddie: (51) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantag		A technically proficient person who breaks into a computer system; Originally denoted good intent.
heuristics: (65)	hacker's manifesto: (51)	A document written anonymously, that justifies cracking into systems as an ethical exercise [i.e.] A mind-set.
honeypot: (64)	hacktivism: (51)	Cracking into a system as a political act; One political notion is that cracking itself is useful for society.
identification: (58) A technique for knowing who someone is; [i.e.] S.I.N Number. integrity: (58) Assurance that information is what you think it is and has not been modified intellectual property: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) Attacks on a system that alter information illicitly packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mai	heuristics: (65)	In virus detection a set of rules, predicting how a virus might act. Anticipating that the virus will affect certain files or systems
integrity: (58) Assurance that information is what you think it is and has not been modified intellectual property: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) Attacks on a system that alter information illicitly packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party	honeypot: (64)	A trap laid by a system administrator to catch and track intruders
intellectual property: (72) An idea or product based on an idea that has commercial value, such as literacy or artistic work malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) Attacks on a system that alter information illicitly packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social Engineering: (54) Social Engineering: (54) Social Interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryp	identification: (58)	A technique for knowing who someone is; [i.e.] S.I.N Number.
malicious code: (53) Code designed to breach system security and threaten digital information; often called a virus. modification attacks: (56) Attacks on a system that alter information illicitly packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt	integrity: (58)	Assurance that information is what you think it is and has not been modified
modification attacks: (56) Attacks on a system that alter information illicitly packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt		An idea or product based on an idea that has commercial value, such as literacy or artistic work
packet-filtering firewall: (69) A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	malicious code: (53)	Code designed to breach system security and threaten digital information; often called a virus.
patent: (73) A government grant that gives the sole right to make use and sell an invention for a specified period of time. Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	modification attacks: (56)	Attacks on a system that alter information illicitly
Phreaking: (50) Subverting the phone system to get free service. Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) Repudiation Attacks: (56) Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) Social Engineering: (54) Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unwanted email, usually wanting to sell users something Spam: (84) Unwanted email, usually wanting to sell users something Solial unit acceptable or intrusion into a persons private life or information Intrusion into a persons private life or information Freedom from unwanted access to or intrusion into a persons private life or information A fire wall that establishes a new link between each packet of information and its designation; slower but more secure A fire wall that establishes a new link between each packet of information and its designation; slower but more secure A fire wall that establishes a new link between each packet of information and its designation; slower but more secure A fire wall that establishes a new link between each packet of information; slower but more secure A fire wall that establishes a new link between each packet of information and its designation; slower but more secure A fire wall that establishes a new link between each packet of information and its designation; slower but more secure A fire wall that establishes a new link between each packet of information and its designation; slower but more secure A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Bequity and its designation; slower but more secure A fire wall that establishes a new link between each packet of information and its	packet-filtering firewall: (69)	A firewall that inspects each packet and moves it along an established link to its destination; usually faster but less secure
Privacy: (83) Freedom from unwanted access to or intrusion into a persons private life or information Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or information software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	1 1	
Proxy firewall: (69) A fire wall that establishes a new link between each packet of information and its designation; slower but more secure Repudiation Attacks: (56) Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Phreaking: (50)	Subverting the phone system to get free service.
Repudiation Attacks: (56) Attacks on a system that injure the information's reliability; Fraud. Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Privacy: (83)	Freedom from unwanted access to or intrusion into a persons private life or information
Reverse Engineer: (73) To figure out the design of a program or devise by taking it apart and analyzing its contents The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something		· · · · · · · · · · · · · · · · · · ·
Risk: (56) The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Repudiation Attacks: (56)	Attacks on a system that injure the information's reliability; Fraud.
Script Kiddie: (51) A novice hacker who simply uses the hacking tools developed by others Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or information and the properties of the world software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Reverse Engineer: (73)	To figure out the design of a program or devise by taking it apart and analyzing its contents
Sniffer: (56) A software program such as wire-shark, that allows the user to listen in on network traffic Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Risk: (56)	The relationship between vulnerability and threat; total risk also includes the potential effect of existing countermeasures
Social Engineering: (54) Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Script Kiddie: (51)	A novice hacker who simply uses the hacking tools developed by others
Software Piracy: (80) Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Sniffer: (56)	A software program such as wire-shark, that allows the user to listen in on network traffic
Spam: (84) Unsolicited e-mails usually wanting to sell you something Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Social Engineering: (54)	Social interaction that preys on human gullibility, sympathy or fear to take advantage of the target [i.e.] to steal money or info.
Spyware: (85) Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Software Piracy: (80)	Illegal copying of software; a problem in the U.S.A and Europe, but rampant in the rest of the world
Symmetric Encryption: (68) Encryption using a private key to both encrypt and decrypt Spam: (84) Unwanted email, usually wanting to sell users something	Spam: (84)	Unsolicited e-mails usually wanting to sell you something
Spam: (84) Unwanted email, usually wanting to sell users something	Spyware: (85)	Software that can: track, collect and transmit to a 3rd party or website certain information about a user's computer habits
	Symmetric Encryption: (68)	Encryption using a private key to both encrypt and decrypt
Trade Secret: (73) A method, device, or piece of information that a company keeps secret and that gives a company a competitive advantage	Spam: (84)	Unwanted email, usually wanting to sell users something
	Trade Secret: (73)	A method, device, or piece of information that a company keeps secret and that gives a company a competitive advantage
Treat: (57) The likely agent of a possible attack, the event that would occur as a result of an attack, and the target of the attack		

Trojan Program: (54)	A program that poses as an innocent program; some action or passage of time triggers the program to do its dirty work.
Undirected Hacker: (50)	A cracker motivated by the challenge of breaking into a system.
Virtual Private Network: (61)	A private network connection that tunnels through a larger, public network and is restricted to authorized users
Virus: (53)	An uninvited guest program with the potential to damage files and the operating system(s)
Virus Hoax: (81)	Email that contains a phony virus warning; Started as a prank to upset people or to get them to delete legitimate system files
Virus Signature: (64)	Bits of code that uniquely identify a particular virus.
Vulnerability: (57)	The sensitivity of information combined with the skill level the attacker needs to threaten that information
Worm: (53)	a type of bot that can roam a network looking for vulnerable systems and replicate itself on those systems

Test Your-self:

1.) Who is Cliff Stoll?

• Clifford Stoll is a systems manager at Lawrence Berkely National Laboratory in California who was tracking a \$0.75 accounting error. His search lead him to a programmer in West Germany who turned out to be part of a spy ring

2.) What is the term used for people who thwarted the AT&T phone system

• The term for people who thwart the AT&T phone system are phreaking

3.) What did the term "hacker" originally describe

 The term "hacker" originally described an insider who was able to manipulate the system for the good of the system

4.) What is the difference between a direct and un-directed hacker

- Direct Hacker: Someone who is motivated by the challenge of the act (i.e.) breaking into the system
- Un-Directed Hacker: Someone who has a political agenda and/or is motivated by greed

5.) What other potential intruders to system managers need to guard against, other than crackers.

- Other potential intruders system managers need to guard against are:
 - Script Kiddies
 - Individuals who support Hacktivism

6.) What document justifies hacker activity?

The document justifies hacker activity is the "Hackers Manifesto."

7.) How could most computer intrusions be avoided?

 Most computer intrusions be avoided by: Good system configuration, proper programming techniques and adherence to security policies

8.) What login technique on a UNIX system could crackers take advantage of?

• The UNIX rlogin (remote login) command allows an administrator to log into one system and then log in to other machines remotely without having a password

9.) Explain one careless programming problem connected to URLs

Many online shopping sites have kept information about the purchase a customer is making right in the URL string displayed in the address bar. If the site does not verify the item's price in the cart at purchase and a cracker modifies the price, the cracker potentially walks away with some cheap merchandise.

10.) Explain a buffer overflow and how it can be used by a cracker

• A buffer overflow happens when a program tries to place more information into a location in memory than that location can handle. A cracker aims for an overflow that overloads memory all the wayto a section of memory critical to a machine's operation.

11.) What is the difference between identification and authentication

- **Identification:** A technique for knowing who someone is; [i.e.] S.I.N Number.
- Authentication: A technique for verifying that someone is who they say they are; A password is one type of Authentication

12.) What is the main difference between a virus and a worm

- Worm: a type of bot that can roam a network looking for vulnerable systems and replicate itself on those Systems
- Virus: An uninvited guest program with the potential to damage files and the operating system(s)

13.) A system attack that prevents users from accessing their accounts is called what

• Denial of Service

14.) Give an example of a repudiation attack

• To say an event occurred when it did not. [i.e.] A financial transaction. "Basically Fraud."

15.) What four types of targets are there for an information security specialist

- Access
- Modification
- Denial of Service
- Repudiation

16.) Name four ways you can "get paranoid" and safeguard your system from losing data

- Have a security policy
- Have physical safeguards
- Use passwords to protect everything
- Destroy old copies of sensitive material

17.) What is the term for the most common and accurate antivirus software search technique

Heuristics

18.) Name three laws you could use to prosecute a cracker

- Copyright
- Pattens
- Trade-Secrets

19.) How expensive should the damage caused by a cracker be to be prosecuted by the U.S. Computer Fraud and Abuse Act? Explain.

 The damage caused by a cracker be to be prosecuted by the U.S. Computer Frau and Abuse Act must be shown to exceed \$5000. With credit card fraud, the attacker has to be shown to be in possessio of 15 or more counterfeit or illegally acquired credit card numbers

20.) Name four ways you could protect your privacy

- Avoid leaving a record of your purchases when possible
- Guard against telephone and mail intrusion
- Review privacy rules
- Be responsible and accountable

Practice Exercises

1.) Computer security affects:

	• Everyone
2.)	John Draper created:
	Software for MS
3.)	The term "hacker" originally had a negative connotation
	• False
4.)	The term "script kiddie" refers to what?
	Youthful hacker
5.)	What is the likely motivation of an undirected hacker?
	Technical challenge
6.)	What is the likely motivation of a directed hacker?
	• Anger, greed, politics
7.)	The term hacktivists refers to:
	Hackers motivated by politics
8.)	The Hacker's Manifesto does what?
	 Uses Communist theory to justify hacking for its inherent justice
9.)	What was the backdoor on a basic e-mail program in early versions of UNIX?
	• rlogin
10.)	Trojan programs are different from viruses because they need to be transported by an e-mail program and viruses do not
	• False
11.)	One of the most notorious social engineers of the 1990s was:
	Kevin Mitnick
12.)	In a social engineering attack, a company phone book can be the target.
	• True

13.) What does a modification attack do?

• Modifies evidence of system entry

14.) One way to ensure that you have a backup of information is to use a UPS

- False
- 15.) Which of the following does not stop virus and worm attacks?
 - Opening e-mail attachments

21.)	The legal protection usually sought for software source code is:
	• Copyright
22.)	Utilitarianism is a set of ethical principles the focuses on individual consequences of action
	• False
23.)	The set of ethical principles that puts principles in terms of natural rights is:
	Rule-deontology
24.)	According to an argument in this chapter concerning privacy, an egoist would consider piracy unethical b/c:
	It is illegal
25.)	You should always reply to SPAM email with "Unsubscribe" in the subject line
	False

16.) The best passwords are 8-10 letters

17.) A virus-checking program that uses heuristics uses:

• A set of rules to anticipate a virus's behavior

18.) Encryption algorithm standards used in computers today are:

19.) SSN is a more secure way of transferring files than Telnet

20.) What kind of service is best placed in a DMZ?

• False

• False

• S-HTTP, SEC, SSL

• Internal DNS server