Connecting with Computer Science Chapter 2 Review:

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.

Connecting with Computer Science Chapter 2 Review:

Key Terms:

acceptable use policy (AUP): (61)	An organizational policy that defines who can use company computers and networks, when and how
access attacks (56)	Attacks on a system that can include: snooping, eavesdropping and interception; more commonly known as spying
accountability (58)	Making sure a system is as secure as feasible and a record of activities exist for reconstructing a break-in
antivirus software (64)	A program designed to detect and block computer viruses
asymmetric encryption (68)	Encryption using both a public key and private key
authentication: (58)	A technique for verifying that someone is who they say they are; A password is one type of authentication
availability: (58)	Accessibility of information and services on a normal basis
backdoors: (52)	Shortcuts into programs created by system designers to facilitate system maintenance but used and abused by crackers.
biometrics: (63)	Biological identification such as fingerprints, voice dynamics or retinal scans
bot: (53)	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 tries 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 that it has not been tampered with
confidentiality: (57)	Ensuring that only those authorized to access information can do so
cookie: (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.
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)	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.
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 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 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)	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
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

Connecting with Computer Science Chapter 2 Review:

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

- **D**enial **o**f **S**ervice

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

Connecting with Computer Science Chapter 2 Review:

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

16.) The best passwords are 8-10 letters

- False

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:

- S-HTTP, SEC, SSL

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

- False

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

- Internal DNS server

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