UNIT 1:

Reading 1:

2.1

1. Who was known as the founder of the Internet? What did he develop?

Larry Roberts, known as the founder of the Internet, developed the project which was called ARPANET from its inception .

2. How was access to sensitive military locations controlled during World War IT?

By means of badges , keys, and the facial recognition of authorized personnel by security guards

3. When was a famous study entitled “Protection Analysis: Final Report” published? What did it focus on? Why?

In 1978, It focused on a project undertaken by ARPA to discover the vulnerabilities of operating system security .

4. What is the difference between MULTICS system and UNIX system?

While the MULTICS system implemented multiple security levels and passwords , the UNIX system did not.

5. When has the Internet become an interconnection of millions of networks and why?

In 1990s, Since its inception as a tool for sharing Defense Department information .

6. What led to more complex and more technologically sophisticated Computer security safeguards before?

The growing need to maintain national security eventually

7. When did the technology become pervasive, reaching almost every corner of the globe with an expanding array of uses?

After the Internet was commercialized

8. What has made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure?

The growing threat of cyber attacks

2.2

1. The security of each computer's stored information is now contingent on the level of security of every other computer to which it is connected.

A. True

2. Ken Thompson, Dennis Ritchie, Rudd Canada, and Doug McElroy are the Multiplexed Information and Computing Service's inventers.

B. False

3. Ken Thompson, Dennis Ritchie, Rudd Canada, and Doug McElroy are the Multiplexed Information and Computing Service's inventers.

B. False

4. Initial planning and development for MULTICS started in 1964, in Cambridge, Massachusetts. Originally it was a cooperative project led by MIT.

C. NI

5. A task force was built by the Advanced Research Projects Agency so as to study the process of securing classified information system.

A. True

6. Access to the ARPANET was expanded in 1981, when the National Science Foundation funded the Computer Science Network.

C. NI

2.3

1. ……, networks of computers became more common, as did the need to connect these networks to each other.

A. At the close of the 20" century C. In the mid-1960s.

B. In the late 1970s. D. During the Cold War

2. The primary threats to security were …….

A. sabotage

B. physical theft of equipment

C. espionage against the products of the systems

D. All are correct

3…….. primary function, text processing, did not require the same level of security as that of its predecessor.

A. ARPANET's C. MULTICS'

B. ARPA's *D. UNIX's*

4. Early computing approaches relied on ……..

A. information security theory and cryptography.

B. security that was built into the physical environment of the data center that housed the computers.

C. the growing threat of cyber attacks.

D. the level of security of every computer.

5. Network security was referred to as network insecurity..... the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET.

A. Because of C. Therefore

B. However D. Although

Reading 2

2.1

1. Which areas does information security include?

Information security includes the broad areas of information security management, computer and data security, and network security.

2. Why does the C.LA. triangle model no longer adequately address the constantly changing environment?

The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or non human threats.

3. What is security? What is information security?

Security is "the quality or state of being secure to be free from danger."

Information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

4. How many fundamental characteristics does information have? What are they?

Information has 7 fundamental characteristics: confidentiality, accuracy, authenticity, utility, possession, integrity and availability.

5. Since when has the C.LA triangle been industry standard for computer security? What is it based on?

The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability.

6. What should a successful organization have to protect its operation?

Physical security , personnel security , operations security , communications security , network security and information security .

7. What is attack? What types of attack are mentioned in the passages?

Attack: An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect.

8. What is vulnerability? Give some examples of vulnerabilities.

Vulnerability: A weaknesses or fault in a system or protection mechanism that opens it to attack or damage. Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door.

2.2

1. Network security is to protect the individual or group of individuals who are authorized to access the organization and its operations.

B. False

2. Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, and identity theft.

C. NI

3. The C.I.A. triangle model still has adequately addressed the constantly changing environment up to now.

B. False

4. Operations security is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence.

C. NI

5. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle.

A. True

6. Organizations must minimize risk to match their risk appetite – the quantity and nature of risk the organization is willing to accept.

A. True

7. Organizations must minimize risk to match their risk appetite – the quantity and nature of risk the organization is willing to accept.

B. False

8. Organizations must minimize risk to match their risk appetite – the quantity and nature of risk the organization is willing to accept.

B. False

2.3

1. ……. is a category of objects, persons, or other entities that presents a danger to an asset.

A. Threat C. Risk

B. Security posture D. Vulnerability

2. …….. , 1s a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people.

A. Personnel security C. Network security

B. National security D. Physical security

3. Someone casually reading sensitive information not intended for his or her use is …….

A. intentional attack C. direct attack

B. a passive attack D. active attack

4. …… can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker.

A. A protection profile *C. An exploit*

B. A threat agent D. An asset

5. Authorized users have ..... to a system, whereas hackers have ……. to a system.

A. illegal access/ legal access C. lawful/illicit

B. legal access/ illegal access *D. B&C are correct*

6. …… attacks originate from the threat itself. ..... attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.

A. Direct/Indirect C. B&C are correct

B. Passive/Active D. Indirect/Passive

7. In information security, ... exists when a vulnerability known to an attacker is present.

A. safeguard C. risk

B. exposure D. security posture

8. When an organization's information is stolen, it has suffered a .....

A. casualty C. damage

B. loss D. All are correct

Reading 3:

2.1

1. When is information authentic ?

When it is in the same state in which it was created, placed, stored, or transferred.

2. When is information considered inaccurate ?

If information has been intentionally or unintentionally modified

3. When has information confidentiality ?

When it is protected from disclosure or exposure to unauthorized individuals or systems.

4. How many critical characteristics does information have ? What are they ?

7 critical characteristics . They are availability , accuracy , authenticity, confidentiality, integrity, utility, possession.

5. Why is a key method given in the integrity of information ?

Because the integrity of information is threatened

6. Why is information integrity the cornerstone of information systems?

Because information is of no value or use if users cannot verify its integrity .

7. When is the integrity of information threatened ?

When the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.

8. What can you use to protect the confidentiality of information ?

A number of measures, including Information classification, Secure document storage, Application of general security policies, Education of information custodians and end user.

2.2

1. Once authorized patrons have access to the contents of the stacks, they expect to find the information they need available in a useable format and familiar language.

A. True

2. When unauthorized individuals or systems can view information, confidentiality is breached.

A True

3. The value of authenticity of information is especially high when it is personal information about employees, customers, or patients.

B. False

4. The value of authenticity of information is especially high when it is personal information about employees, customers, or patients.

A. True

5. If a computer system performs the different hashing algorithm on a file and obtains a different number than the recorded hash value for the file, the file has been compromised and the integrity of the information is lost.

B. False

6. Within economics the concept of utility is used to model worth or value, but its usage has evolved significantly over time.

C. NI

2.3

1. Which critical characteristics of information is the quality or state of being genuine or original, rather than a reproduction or fabrication?

A. Authenticity C. Accuracy

B. Confidentiality D. Utility

2. Why is an E-mail spoofing a problem for many people today?

A. Because often the modified field is the address of the originator.

B. Since often the modified field is the address of the originator.

C. A & B are correct

D. Because of often the modified field is the address of the originator.

3. The ……. is the quality or state of having value for some purpose or end.

A. integrity C. availability

B. utility of information D. A&B are correct

4. …….. is the quality or state of ownership or control.

A. The utility of information

B. The availability of information

C. The confidentiality of information

D. The possession of information

5. Incorrect information in your checking account can result from external or Internal ……

A. access C. report

B. errors D. transmission

6. If a bank teller mistakenly adds or subtracts too much from your account,……

A. The value of hash is unchanged.

B. The availability of information is useless.

C. the value of the information is changed.

D. The confidentiality of information is stolen.

7. You can use..... measures to protect the confidentiality of

information.

A. information classification, application of general security policies

B. secure document storage

C. education of information custodians and end user

D. All are correct

Reading 4

2.1

1. Which tools of physical security are often applied to restrict access to and interaction with the hardware components of an information system?

Hardware and networks

2. What happens when an unauthorized user obtains an organization’s procedures?

when an unauthorized user obtain an organization ‘s procedures, this poses a threat to the integrity of the information .

3. When local area networks are connected to other networks such as the Internet, new security challenges rapidly emerge?

When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.

4. What is an information system?

an information system is the entire set of software, hardware, data, people, procedures, and networks

5. Why is data the main target of intentional attacks?

Because data is often the most valuable asset possessed by an organization.

6. Which component of Information system is the most difficult to secure?

Software

7 . What became common in airport before 2002? Give details.

laptop thefts in airports were common.

8. Why do software programs become an easy target of accidental or intentional attacks?

Information security is all too often implemented as an afterthought, rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

9. Why is securing the physical location of computers and the computers themselves important?

Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information.

10. Do only software and hardware enable information to be input, processed, output, and stored." If no, what components enable it to do so?

2.2

1. Information systems hardware is the part of an information system you can touch — the physical components of the technology.

C. NI

2. The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software.

A. True

3. The physical technology that enables network functions is becoming less and less accessible to organizations of every size.

B. False

4. The invaders were so ferocious that the Chinese emperor commanded the construction of a great wall that would defend against the Hun invaders.

A. True

5. Physically securing the information system isn't so important as educating employees about safeguarding procedures.

B. False

2.3

1. Many system development projects do not make full use of the ..... management system's security capabilities, and in some cases the database is …….. in ways that are less secure than traditional file systems.

A. database/executed *C. A&B are correct*

B. database/implemented D. data/implemented

2. Frequently overlooked component of an IS is ..... They are written instructions for accomplishing a specific task.

A. networks C. software

B. procedures D, database

3. The IS component that created much of the need for increased computer and information security is .....

A. software C. hardware

B. networking D. data

4. ……. of the IS comprises applications, operating systems, and assorted command utilities.

A. The software component C. The network component

B. The hardware component D. A&C are correct

5. Physical security policies deal with ..... as a physical asset and with the protection of physical assets from harm or theft.

A. software C. spyware

B. adware *D. hardware*

6. …….. are often created under the constraints of project management, which limit time, cost, and manpower.

A. software program C. hardware program

B. spyware program D. adware program

7. Unfortunately, most information systems are **built** on hardware platforms that cannot **guarantee** any level of information security if unrestricted access to the hardware is possible.

A. designed/make sure C. A&B are correct

B. designed/ensure D. implemented/certain

8. By taking …… of a security weakness a bank consultant can order millions of dollars to be transferred by wire to his own account.

A. advantage

C. position

B. a flier

D. opportunity

9. In fact, many ..... of daily life are affected by ..... , from smartphones that crash to flawed automotive control computers that lead to recalls.

A. facets/buggy software

C. A&B are correct

B. aspects/buggy software

D. facets/buggy hardware

10. Knowledge of procedures, as with all critical information, should be …….. among members of the organization only on a need-to-know basis.

A. popularized

C. generalized

B. disseminated

D. all are correct

UNIT 2

Reading 1

2.1

1. Why don't any individuals and organizations purchase software as mandated by the owner's license agreements?

Because most software is licensed to a particular purchaser, its use is restricted to a single user or to a designated user in an organization .

2. Which malicious code software programs that hire their true nature and reveal their designed behavior only when activated?

Trojan horses

3. Why are the software components or programs of malicious code designed?

To damage, destroy, or deny service to the target systems.

4. What types of software attacks are mentioned in the text?

Virus, worm, trojan horses, back door or trap door,…

5. What does IP stand for? What is it?

Intellectual property. IP is defined as "the ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person's intellectual property may or may not involve royalty payments or permission, but should always include proper credit to the source."

6. Who is considered an expert hacker?

An expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system.

7. Who are hackers? Which skill levels are divided among hackers?

Hackers are "people who use and create computer software to gain access to information illegally ".

Two skill levels among hackers. The first is the expert hacker, or elite hacker and the novice or unskilled hacker.

8. What is one of the most common methods of virus transmission?

Is via e-mail attachment files.

2.2

1. Trade secrets, copyrights, trademarks, and patents are often considered Intellectual property.

A. True

2. Trade secrets, copyrights, trademarks, and patents are often considered Intellectual property.

B. False

3. Trade secrets, copyrights, trademarks, and patents are often considered Intellectual property.

B. False

4. Before a Trojan horse can infect a machine, the user must download the server side of the malicious application.

C. NI

5. When an organization places its Web servers in the care of a Web hosting provider, that provider assumes responsibility for all Internet services and for the hardware and operating system software used to operate the Web site.

A. True

2.3

1. What is the most common IP breach?

A. the unlawful use or duplication of software-based intellectual property

B. the illegally use of software-based intellectual property

C. A&B are correct

D. the illicit use of software-based intellectual property

2. ……. is a well-known and broad category of electronic and human activities that can breach the confidentiality of information.

A. Trojan Horse

C. Espionage or trespass

B. A polymorphic threat

D. Worm

3. A virus or worm can have a payload that..... a back door or trap door component in a system, which allows the attacker to access the system at will with special privileges.

A. changes

C. installs

B. puts

D. replaces

4. …….. is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures.

A. Trojan Horse C. Virus

B. A polymorphic threat D. Worm

5. Worms also take advantage of open shares found on_ the network in which an infected system is located, placing working copies of the worm code onto the server ..... users of those shares are likely to become infected.

A. so as to C. so that

B. in order that *D. B&C are correct*

6. Which of the followings is a malicious program that replicates itself constantly, without requiring another program environment?

A. Black door C. Virus

B. Worm D. Worm Hoax

Reading 2: Threat (2)

2.1

1. Why do employees's mistakes represent a serious threat to the confidentiality, integrity, and availability of data?

Because employees use data in everyday activities to conduct the organization's business .

2. What threats are mentioned in the text? Which one is the biggest threat to an organization?

Force of nature, human error or failure, information extortion, theft, technical hardware failure or errors, technical software failure or errors, missing, inadequate, or incomplete organizational policy or planning; missing, inadequate, or incomplete controls; sabotage or vandalism ad technological obsolescence

The biggest is human error or failure

3. How can physical theft be controlled?

Quite easily by means of a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems.

4. Why is electronic theft a more complex problem to manage and control?

Because when someone steals a physical object, the loss is easily detected; if it has any importance at all, its absence is noted. When electronic information is stolen, the crime is not always readily apparent. If thieves are clever and cover their tracks carefully, no one may ever know of the crime until it is far too late.

5. Who is Maxus? What did he do? Give details to his act.

Is a Russian hacker. Hacked the online vendor and stole several hundred thousand credit card numbers. When the company refused to pay the $100,000 blackmail, he posted the card numbers to a website, offering them to the criminal community.

6. Can human error or failure be prevented? How can it be protected?

Yes. It can be prevented with training and on going awareness activities, but also with controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of command by a second party .

7. Are natural disasters considered threats in the information security? What effects do they cause?

Yes. They can disrupt not only the lives of individuals but also the storage, transmission, and use of information.

8. Which mistakes do employees often make when they use information systems?

Revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protected information.

2.2

1. Experience, proper training, and the incorrect assumptions are just a few things that can cause these misadventures.

B. False

2. Much human error or failure can be prevented with training and ongoing awareness activities, but also with controls, ranging from simple procedures.

A. True

3. One of the best-known hardware failures is that of the Intel Pentium II chip, which had a defect that resulted in a calculation error under certain circumstances.

A. True

4. Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.

C. NI

5. Technical hardware failures or errors has always been one of the most dangerous threads in the information security.

C. NI

2.3

1. ……. occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it.

A. Information extortion C. Technical failure

B. Human Error D. B&D are correct

2. ……. occur when a manufacturer distributes equipment containing a known or unknown flaw.

A. Technical hardware failures C. Theft

B. inadequate control D. Technological error

3. Which threat is the most dangerous to an organization's information security?

A. Information extortion C. Vandalism

B. An organization's own employees. D. Missing controls

4. The value of information is ..... when it is copied without the owner's knowledge.

A. diminished C. A & B are correct

B. lessened D. minimized

5. Large quantities of ..... are written, debugged, published, and sold

before all their bugs are detected and resolved.

A. software *C. computer code*

B. hardware D. computer language

6……. can present some of the most dangerous threats, because they usually occur with very little warning and are beyond the control of people.

A. Force majeure C. Forces of nature

B. Acts of God *D. All are correct*

Reading 3:

2.1

1. What is a cracking attack? When is it used?

A cracking attack is a component of many dictionary attacks. It is used when a copy of the Security Account Manager (SAM) data file.

2. What is a distributed denial of-service?

Is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

3. Why is sometimes the brute force attack called a password attack?

Since it is often used to obtain passwords to commonly used accounts.

4, Which attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.

Active web scripts with the intent to destroy or steal information .

The malicious code attack

5. Why is a trap door hard to detect?

Because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

6. Why are always the manufacturer's default administrator account names and passwords changed?

Because if attackers can narrow the fields of target accounts, they can devote more time and resources to these accounts.

7. Why are many requests made that the target system becomes overloaded and cannot respond to legitimate requests for service in a DoS attack?

Because the attacker sends a large number of connection or information requests to a target.

8. What is a vulnerability?

Is an identified weakness in a controlled system, where controls are not present or are no longer effective.

2.2

1. A lot of systems and users send information on local networks in clear text so sniffers add risk to the network.

C. NI

2. It is absolutely impossible to defend against DDoS attacks because they are too dangerous.

B. False

3. Similar dictionaries can be used to allow passwords during the reset process and thus guard against easy-to-guess passwords by organizations.

B. False

4. Similar dictionaries can be used to allow passwords during the reset process and thus guard against easy-to-guess passwords by organizations.

A. True

5. Similar dictionaries can be used to allow passwords during the reset process and thus guard against easy-to-guess passwords by organizations.

A. True

2.3

1. Which of the following attacks is a variation of the brute force attack?

A. Dictionary B. Password crack

C. Back door D. Hoax

2. Devers is any technology that aids in gathering information about a person or organization without their knowledge and it is placed on a computer to secretly gather information about the user and report it.

A. Adware B. Denial-of-Service

C. Dictionary *D. Spyware*

3. …….. attacks are the most difficult to defend against, and there are presently no controls that any single organization can apply.

A. Password crack *C. DDoS*

B .Dictionary D. Back door

4. …….. belong to the state-of-the-art malicious code attack.

A.Polymorphic C. multivector

B. Worm *D. All are correct*

5. What attack is considered a weapon of mass destruction on the Internet to

use a popular metaphor?

A. DDoS C. Back Door

B. Brute force D. Password Crack

Reading 4:

2.1

1. What is phishing? What is its variant?

Is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity. A variant is spear phishing.

2. How may pharming also exploit the Domain Name System?

By causing it to transform the legitimate host name into the invalid site's IP address

3. What do sometimes attackers do to sway the target for social engineering?

Threaten, cajole or beg

4. In which attack does an attacker monitor packets from the network, modify them, and insert them back into the network?

In the well-known man-in-the-middle or TCP hijacking attack

5. Why does pharming often use Trojans, worms, or other virus technologies to attack the Internet browser's address bar?

So that the valid URL typed by users is modified to that of the illegitimate

6. What do hackers use to engage in IP spoofing?

Hackers use a variety of techniques to obtain trusted IP addresses, and then modify the packet headers to insert these forged addresses

7. In Which attack can the cookie allow the designer to collect information on how to access password-protected sites?

In the timing attack

2.2

1. Phishing is a technique of fraudulently obtaining private information.

A. True

2. Just a few attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised.

C. NI

3. Sniffers add risk to the network, because many systems and users send information on local networks in clear text.

A. True

4. Pharming and timing attack belong to social engineering attacks.

B. False

5. One of the techniques which spoofing attacker used to gain unauthorized access to computers is forging a source IP address.

A. True

2.3

1. Sending large e-mails with forged header information, ... can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.

A. attackers C. users

B. organizers D. programmers

2. ……. Explores the contents of a Web browsers ‘s cache and …… a malicious cookie on the client’s system.

C. Pharming/uses C. A timing attack/ stores

D. Spam/contains D. None is correct

3. ……. can be used both for legitimate network management functions and for stealing information.

A. Spyware C. Brute force

B. Sniffers D. Dictionary

4. Many organizations attempt **to cope with** the flood of spam by using email filtering technologies.

A. to deal with C. keep up with

B. get on well D. put on with

5. Which attacks can be accomplished by exploiting various technical flaws in the Simple Mail Transport Protocol.

A. Man-the-middle C. Mail Boming

B. Phishing D. Pharming

6 . …… is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity.

A. Dictionary *C. Sniffer*

B. Phishing D. Hoax

UNIT 3

Reading 1:

2.1

1. What is a firewall in computing?

A firewall in an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world, known as the untrusted network (for example, the Internet), and the inside world, known as the trusted network.

2. Where does the term firewall derive from?

The term firewall originally derive from a wall intended to confine a fire within a line of adjacent buildings.

3. Is a firewall in an information security program the same as or different from a building's firewall? What is their similarity or difference?

A firewall in an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world, known as the untrusted network (for example, the Internet), and the inside world, known as the trusted network .

4. What are the functions of stateful filters?

The functions of stateful filters are maintaining knowledge of specific conversations between endpoints by remembering which port number the two IP addresses are using at layer 4 (transport layer) of the OSI model for their conversation, allowing examination of the overall exchange between the nodes.

5. How can firewalls be categorized?

Firewalls can be categorized by processing mode, development era, or structure

6. What are the predecessors to firewalls for network security?

The predecessors to firewalls for network security are Second-generation firewalls perform the work of their first-generation predecessors.

7. What is the most important benefit of application layer filtering?

The most important benefit of application layer filtering is that it can understand certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP))

8. What are the benefits of firewalls in aircraft and automobiles ?

The benefits of firewalls in aircraft and automobiles is an insulated metal barrier that keeps the hot and dangerous moving parts of the motor separate from the inflammable interior where the passengers sit.

2.2

1. Packet filters operates by inspecting packets transferred between computers.

A. True

2. Firewall Toolkit was invented by Marcus Ranum, Wei Xu, and Peter Churchyard.

B. False

3. Circuit-level gateways are the first generation of firewalls

A. True

4. Firewalls are built between or through buildings, structures, or electrical substation transformers, or within an aircraft or vehicle.

C. NI

5. Firewalls can be used to subdivide a building into separate fire areas and are constructed in accordance with the locally applicable building codes.

B. False

2.3

1…….. is typically established between a trusted internal network and untrusted external network in...

A. a panel/computing B. a wall/construction

C. a shield/computing D, A&C are correct

2. When was Firewall was applied and what was it applied for?

A. In 1987/ firewall technology

B. in the late 1980s/ network technology

C. In early 21st century/IP address

D. In October 1993/ Information systems

3. The benefit of firewalls ..... is preventing a fire from spreading from one section of the building to another.

A .In commercial and residential construction

B. in an information security program

C. In computing

C. A&C are correct

4. What is WarGames and when was it made?

A. Third generation firewall/in 2012

B. Packet filters/in early 21“ century

C. A computer-hacking movie/in the 1983

D. stateful filters/ from 1989-1990

5. What became the basis for Gauntlet firewall at Trusted Information Systems?

A. Hypertext Transfer Protocol *B. Firewall Toolkit*

C. User Datagram Protocol D. transport layer

Reading 2:

2.1

1. What does a commercial-grade firewall system consist of?

A commercial-grade firewall system consists of application software that is configured for the firewall application and run on a general-purpose computer

2. What does a commercial-grade firewall system consist of?

Because The firewall rule sets are stored in nonvolatile memory,

3. What are most small office or residential-grade firewalls?

Most small office or residential-grade firewalls are either simplified dedicated appliances running on computing devices or application software installed directly on the user’s computer.

4. What is one of the most effective methods of improving computing security in the SOHO setting?

One of the most effective methods of improving computing security in the SOHO setting is by means of a SOHO or residential-grade firewall.

5. What method is used for protecting the residential user?

Method of protecting the residential user is to install a software firewall directly on the user's system.

6. What are Windows or Linux/Unix?

They are operating systems

7. Why do more and more small businesses and residences become more and more vulnerable to attacks?

Because as more and more small businesses and residences obtain fast Internet connections with digital subscriber lines (DSL) or cable modem connections

2.2

1. Broadband gateways or DSL/cable modem routers are commercial-Grade Firewall Appliances.

B. False

2. If the residental users install a software firewall directly on the their system, their computer completely is protected.

B. False

3. Firewalls can also be categorized by the structures used to implement them. Most commercial-grade firewalls are dedicated appliances.

A. True

4. All firewall devices can be configured in a number of network connection architectures.

C. NI

5. The hardware firewall's use of no routable addresses further extends the protection, making it virtually impossible for the attacker to reach your information.

A. True

2.3

1. …… are stand-alone, self-contained combinations of computing hardware and software.

A. Firewall appliances B. Firewall architectures

C. Firewall systems D. Firewall software

2. Organizations can install ..... on an existing general purpose computer system.

A. firewall hardware *B. firewall architecture*

C. firewall software D. firewall devices

3. Which of the following does the word "they" in the paragraph 4 refer to?

A. digital subscriber lines B. Internet connections

C. cable modem connections D. businesses and residences

4. Which of the following helps your computer still be safe no matter how hard the attackers manage?

A. An anti - virus software program B. A strong password

C. A hardware firewall D. SOHO

5. The SOHO firewall serves first as a stateful firewall to enable ..... access.

A. inside-to-outside B. outside-to-inside

C. A&B are correct D. None is correct

Reading 3

2.1

1. What common architectural implementations are mentioned in the text?

Packet -filtering routers, screened host firewalls, dual-homed firewalls, and screened subnet firewalls.

2. Why do most organizations with an Internet connection have some form of a router at the boundary between the organization's internal networks and the external service provider?

Because many of these routers can be configured to reject packets that the organization does not want to allow into the network .

3. Which approach allows the router to prescreen packets to minimize the network traffic and load on the internal proxy?

Screened host firewalls combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server.

4, What is the protocol for handling TCP traffic via a proxy server?

SOCKS

5. Are there many variants of the screened subnet architecture? What does the first general model consist of?

Yes, there are. It consists of two filtering routers, with one or more dual-homed bastion hosts between them

6. How many NICs does the bastion host contain? What are they?

Two NICs (network interface cards) rather than one, as in the bastion host configuration

One NIC is connected to the external network , and one is connected to the internal network, providing an additional layer of protection.

7. Why is NAT able to prevent external attacks from reaching internal machines with addresses in specified ranges?

Because the internal addresses used by NAT consist of 3 different ranges

8. Why is the bastion host often referred to as the sacrificial host?

Because it stands as a sole defender on the network perimeter

2.2

1. There are three advantages of NAT mentioned in the text.

B. false

2. A method of mapping real, valid, external IP addresses to special ranges of no routable internal IP addresses is NAT.

A. True

3. The application proxy examines an application layer protocol, such as HTTP, and performs the proxy services.

A. True

4. The application proxy examines an application layer protocol, such as HTTP, and performs the proxy services.

B. False

5. Firewall architecture is responsible for the standards and frameworks associated with the architecture of sub-networks

C. NI

2.3

1. …… combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server.

A. Screened host firewalls *B. Firewall systems*

C. Dual-home host firewalls D. Screen subnet firewalls

2. All firewall devices can be configured in ..... network connection architectures.

A. a wide range of B. just a few

C. a variety of *D. A&C are correct*

3. The dominant architecture used today is the ..... firewall.

A. screen host B. dual-home host

C. screened subnet D. C&B are correct

4, The configuration that works best for a particular organization depends on

A. the organization's ability to develop and implement the architectures

B. the objectives of the network

C. the budget available for the function

D. All are correct

5. The benefit of a ..... is its ability to translate between many different protocols at their respective data link layers.

A. dual-homed host B. screen host

C. SOCKS Server D. screen subnet firewall

Reading 4

2.1

1. What type of filtering is common in network routers and gateways?

Static filtering

2. How many subsets of packet-filtering firewalls are mentioned in the text? What are they?

There are 3 subnets of packet-filtering firewalls: static filtering , dynamic filtering, and stateful inspection.

3. How many major processing-mode categories are firewalls categorized? What are they?

5 major processing -mode categories : packet -filtering firewalls, application gateways, circuit gateways, MAC layer firewalls and hybrid

4, What do simple firewall models examine?

Two aspects of the packet header : the destination and source address.

5. Where do filtering firewalls inspect packets?

At the network layer, or layer 3, of the Open Systems Interconnect (OSI) model

6. What does the packet-filtering firewall examine?

The header information of data packets that come into a network; every incoming packet

7, What is the primary disadvantage of stateful inspection

Is the additional processing required to manage and verify packets against the state table

2.2

1. There aren't any drawback for stateful firewall according to the text.

B. False

2. The restrictions most commonly implemented in packet-filtering firewalls are based on a combination of IP source and destination address, direction, protocol, and TCP.

A. True

3. Like first generation firewalls, stateful inspection firewalls perform packet filtering, but they take it a step further.

A. True

4. Auditability makes certain that all actions on a system can be attributed to an authenticated identity.

C. NI

5. According to the text, all firewall processing modes are shown.

B. False

2.3

1. ……..lower requires that the filtering rules be developed and installed with the firewall.

A. dynamic packet-filtering

B. Static filtering

C. stateful filtering

D. A&B are correct

2. While static filtering firewalls allow entire sets of one type of packet to enter in response to authorized requests, the ..... allows only a particular packet with a particular source, destination, and port address to enter.

A. dynamic packet-filtering B. static filtering

C. Stateful filtering D. A&C are correct

3. Packet structure varies depending on the nature of the packet. The two

primary service type are ……..

A.UDP B. TCP

C. A&B are correct D. IP

4. Which of the following does the word "they" in paragraph 4 refer to?

A. two aspects *B. Simple firewall model*

C. destination and source address D. rules

5. Packet-filtering firewalls examine every incoming packet header and can …….. filter packets based on header information.

A. automatically B. typically

C. selectively D. computationally

UNIT 4

Reading 1

2.1

1. When were information security intrusion detection systems commercially available?

in the late 1990s

2.What do many IDSs assist administrators to do?

to configure the systems to notify them directly of trouble via e-mail or pagers, to detect the preambles to attacks

3.What is IPS? What can it do?

A current extension of IDS technology. It can detect an intrusion and also prevent that intrusion from successfully attacking the organization by means of an active response.

4.What is an intrusion detection system?

is a device or software application that monitors a network or systems for malicious activity or policy violations

5.How does an IDS work?

like a burglar alarm in that it detects a violation and activates an alarm.

6.How many reasons does an IDPS need installing?

Five

7.What is one of the most important reasons to install an IDPS?

is that they serve as deterrents by increasing the fear of detection among would-be attackers.

8. Give some descriptions of an IDS.

An IDS works like a burglar alarm in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm which can be audible and visual, silent

2.2

1. An IDS works like an alarm clock in that it detects a violation (some system

activity analogous to an opened or broken window) and activates an

alarm.

B. False

2. According to the text four reasons are given to indicate that [IDSs need installing.

B. False

3. When malicious activity or violation appears, an administrator is usually informed in someway.

A. True

4. Writing and implementing good enterprise information security policy are important intrusion prevention activities.

C. NI

5. Delaying or undermining an organization's ability to secure its systems from attack and subsequent loss depends on many factors.

A. True

2.3

1. Which system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms?

A. An IDPS system
B. A SIEM system
C. An IDP
D. A&C are correct

2. To collect attack information in support of an IDPS implementation, you can begin with .....such as Snort.

A. hardware IDPS
B. firmware IDPS
C. a freeware IDPS tool
D. software package

3. What is the term IDPS and IPS generally used for?

A. to describe anti-virus programs
B. to describe current anti-intrusion technologies
C. to describe IDPS modes
D. to describe current anti-intrusion technologies

4. The IDPS can also provide forensic information that may be useful should the attacker be .....

A.arrected B. sued

C. prosecuted D. all are correct

5. A current extension of IDS .....is the intrusion prevention system.

A.system B. technology

C. detection D. intrusion

Reading 2

2.1

1. What is NIDS's function?

It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

2. What is the difference between on-line NIDS and off-line NIDS?

On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not while off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

3. What is a host-based intrusion detection system?

is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces

4, What is a host-based IDS capable of doing?

monitoring all or parts of the dynamic behavior and the state of a computer system, based on how it is configured.

5. What are OPNET and NetSim? What are they used for?

commonly used tools for simulating network intrusion detection systems.

6. What can happen if intruders succeed in modifying any of the objects the HIDS monitors?

nothing can stop such intruders from modifying the HIDS itself – unless security administrators take appropriate precautions.

7. What HIDS might do apart from crypto-techniques?

HIDS might allow administrators to store the databases on a CD-ROM or on other read-only memory devices (another factor militating for infrequent updates...) or storing them in some off-system memory.

8. What types of NIDS are mentioned in the text? What do you rely on to

categorize the design of NIDS?

- *on-line and off-line NIDS*

- *according to the system interactivity property*

2.2

1. According to the text, thanks to Neural networks, IDS can predict attacks when they appear.

A. True

2. Administrator himself is able to identify an attack without intrusion detection systems.

B. False

3. In order to control traffic to and from all devices on the network Network intrusion detection systems are put at a strategic point or points within the network.

A. True

4. Commercially available software solutions often do correlate the findings from NIDS and HIDS in order to find out about whether a network intruder has been successful or not at the targeted host.

C. NI

5. Both NIDS and HIDS have their own capability to do different functions.

B. False

2.3

1. How many types does NIDS have according to the system interactivity property? What are they?

A. It has two types: on-line and off-line NIDS

B. It has one: off-line NIDS

C. It has only one: on-line NIDS

D. B&C are correct

2. Why are Network intrusion detection systems placed at a strategic point or points within the network?

A.To control traffic to and from all devices on the network.

B. To monitor traffic to and from all devices on the network.

C. To supervise traffic from and to all devices on the network.

D. B&C are correct

3. NID Systems .....comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS.

A. are also able to

B. are responsible for

C. are also capable of D. A & C are correct

4. .....can be also combined with other technologies to increase detection and prediction rates.

A. HIDS B.NIDS

C. INN IDS D.ANN

5. Why will a HIDS usually go to great lengths?

A. To prevent the object-database, checksum-database

B. To reports from any form of tampering.

C. A&B are correct

D. To detect the object-database, checksum-database

Reading 3

2.1

1. What are the weaknesses of the signature-based approach?

new attack strategies must continually be added into the IDPS's database of signatures; otherwise, attacks that use new strategies will not be recognized and might succeed. Another weakness of the signature based method is that a slow, methodical attack might escape detection if the relevant IDPS attack signature has a shorter time frame.

2. What are the disadvantages of the statistical anomly-based approach?

these systems require much more overhead and processing capacity than signature-based IDPSs, because they must constantly compare patterns of activity against the baseline. Another drawback is that these systems may not detect minor changes to system variables and may generate many false positives.

3. Why is Statistical Anomaly-Based IDPS less commonly used than the signature-based type?

Because of its complexity and impact on the overhead computing load of the host computer as well as the number of false positives it can generate

4. What is the solution to the weaknesses of the signature-based approach?

is to collect and analyze data over longer periods of time

5. What is the benefit of the statistical anomly-based approach?

is that the IDPS can detect new types of attacks, since it looks for abnormal activity of any type.

6. Why is signature-based IDPS technology widely used?

Because many attacks have clear and distinct signatures,

7. What does SPA stand for? What is it?

It stands for Stateful protocol analysis. It is a process of comparing predetermined profiles of generally accepted definitions of benign activity for each protocol state against observed events to identify deviations.

8. What are the models used for SPA based on?

On industry protocol standards established by such entities as the Internet Engineering Task Force

2.2

1. The signature-based, the statistical-anomaly, and the stateful packet inspection are outstanding approaches used by IDPSs.

A. True

2. Statistical anomaly-based approach is more commonly used than signature-based approach.

A. True

3. Signature-based IDPS never goes wrong so attackers can not do anything with it.

B. False

4. An IDPS can be implemented via one of three basic control strategies.

C. NI

5. One of the advantages of Stateful Protocol Analysis IDPS is that the IDPS may in fact interfere with the normal operations of the protocol it's examining, especially with client- and server-differentiated operations.

B. False

2.3

1. By .....relevant data detected in a session and then using that data to identify intrusions that involve multiple requests and responses, the IDPS can better detect specialized, multisession attacks.

A. storing B. switching

C. transmitting D. processing

2. Which of the following IDPS may not suitable if the actions of the users or systems on a network vary widely, with periods of low activity interspersed with periods of heavy packet traffic?

a. Stateful Protocol Analysis IDPS B. Signature – Based IDPS

C. Statistical Anomaly-Based IDPS D. None is correct

3. Which of the followings is the approach used IDPSs?

a. The signature-based B. the statistical-anomaly

C. the stateful packet inspection D. All are correct (D)

4. Sometimes a knowledge-based IDPS has got another name. It is .....

A. signature-based IDPS B. misuse-detection IDPS

C. A&B D. None is correct

5. Behavior-based IDPS collects statistical summaries by .....traffic that is known to be normal.

A. Keeping track B. controling C. observing D. B & C are correct

Reading 4

2.1

1. What does a honeypot system contain?

pseudo-services that emulate well-known services, but is configured in ways that make it look vulnerable to attacks.

2. What is LaBrea? How does it work?

One tool that provides active intrusion prevention is known as LaBrea. LaBrea is a "sticky" honeypot and IDPS and works by taking up the unused IP address space within a network.

3. How long have IDPS researchers used padded cell and honeypot systems?

Since the late 1980s

4. What should administrators do when using honeypots and honeynets?

be careful not to cross the line between enticement and entrapment.

5. What are honeypots? What are they designed for?

Honeypots are decoy systems designed to lure potential attackers away from critical systems.

6. What systems use a combination of techniques to detect an intrusion and then trace it back to its source?

trap-and-trap systems

7. What does LaBrea do when it notes an ARP request?

it checks to see if the IP address requested is actually valid on the network

2.2

1. A screenshot from a simple IDPS that specializes in honeypot techniques, called Deception Toolkit.

A. True

2, Gathering information about the attacker's activities is one of the Honeypots's aim.

A. True

3. An IDPS is a complex system in that it involves numerous remote monitoring agents that require proper configuration to gain the proper authentication and authorization.

C. NI

4. Both entrapment and enticement are the act of luring an individual into committing a crime to.

B. False

5. When doing their jobs, hackers have never been trapped.

B. False

2.3

1. .....the information in a honeypot appears to be valuable, any unauthorized access to it constitutes suspicious activity.

   A. However B. Although

   C. In order to D. Because

2. Which of the followings is the advantage of honeyport?

   A. Attackers can be diverted to targets that they cannot damage

   B. The legal implications of using such devices are not well understood

C. Administrators and security managers need a high level of expertise to use these systems.

D. None is correct

3. If the intruder is outside the security perimeter of the organization, then numerous legal issues arise.

A.If B. Unless

C. When D. While

4. ..... are instrumented with sensitive monitors and event loggers that detect attempts to access the system and collect information about the potential attacker's activities.

A.Padded cells B. Honeypots

C. Decoys D. B&C are correct

5. A .....is a honeypot that has been protected so that that it cannot be easily compromised.

A. decoy B. honeypot

C. lure D. padded cell

UNIT 5

Reading 1

2.1

1. What is cryptography? What is it used for?

- *Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication to encrypt or decrypt information.*

2. Where does cryptography derive from and what does it mean?

The word "cryptography" is derived from the Greek words kryptos, meaning

hidden, and graphien, meaning to write.

3. What aspects of information security does cryptography relate?
Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

4. What is cryptanalysis?
Cryptanalysis is the study and analysis of existing ciphers or encryption algorithms from an encrypted message (called the ciphertext) without knowing the algorithms and keys used to perform the encryption) in order to assess their quality, to find weaknesses, or to find a way to reverse the encryption process without having the key.

5. What is encryption? What is decryption?
The process of making the information unreadable is called encryption or enciphering. Reversing this process and retrieving the original readable information is called decryption or deciphering.

6. Why does cryptanalysis study and analyze existing ciphers or encryption algorithms?
Because it is in order to assess their quality, to find weaknesses or to find a way to reverse the encryption process without having the key.

7. How many goals does cryptography have? What are they?
There are 4 goals . They are Confidentiality, Data integrity, Authentication and Non-repudiation

8. What major classes of authentication usually subdivided? Why is it subdivided so?

Because two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication.

2.2

1. Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so.

A. True

2. In cryptography, a cryptosystem is a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality.

C. NI

3. Encryption is the process of encoding information which converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.

A. True

4. There is no need to find any ways to solve the situation when the two parties have strong disputes.

B. False

5. The term “code” and “cryptography” are the same and they are changeable.

B. False

2.3

1. Which process needs the key?

A. encryption B. decryption

C. A&B are correct D. recovering the original information

2. What types of attacks are mentioned in the text?

A. Brute force attack B. Ciphertext-only attack

C. Known - plaintext attack *D. All above are correct*

3. …….. is to adequately address confidentiality, data integrity, authentication, and non-repudiation in both theory and practice.

A. fundamental goal of cryptography

B. general object of cryptography

C. basic goal of cryptology

D. general object of cryptanalysis

4. ……. is a service which prevents an entity from denying previous commitments or actions.

A. Non-repudiation B. Authentication

C. Data integrity D. Confidentiality

5. What was considered an early instance of encipherment?

A. Rosetta Stone *B. Egyptian hieroglyphics*

C. Scytale D. A code book

6. A service related to verification. This function is for both parties and

information itself is ……..

A. data integrity B. non-repudiation

C. authentication D. confidentiality

7. Which of the following attacks that can, in theory, be used to attempt to decrypt any encrypted data?

A. A brute-force attack B. dictionary attack

C. A&B are correct D. Man-in the middle attack

8. Which of the followings is the study of analyzing information systems in order to study the hidden aspects of the systems?

A. Cryptography B. Cryptology

C. Cryptanalysis D. A&B are correct

Reading 2

2.1

1. When was cryptography changed from dark art into a science based on mathematics? Who changed it?

By the end of the 19th century Auguste Kerckhoff

2. Who was the father of Information Theory?

Claude Elwood Shannon

3. What device was developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication?

The Enigma machine

4. Who invented Enigma machine and when was it invented?

Dr. Arthur Scherbius/ in the early- to mid-20th century

5. Who introduced the idea of public-key cryptography? What are its algorithms based on? the computational complexity problem.

Whitefield Diffie and Martin Hellman. On the computational complexity problem

6. What device was developed by the Spartans of Greece? When was it developed?

the scytale. In 487 B.C.

7. What did Leon Battista Alberti invented?

a device based on two concentric discs that simplified the use of Caesar ciphers.

8. Which algorithms are the most widely used in the world among crypto algorithms?

RSA algorithms

2.2

1. Giovan Batista Belaso invented a device based on two concentric discs that simplified the use of Caesar ciphers.

B. False

2. The idea of public-key cryptography belongs to Ronald Rivest, Adi Shamir, and Leonard Adleman.

B. False

3. Charles Babbage developed the multiple frequency analysis techniques.

A. True

4. Leon Battista Alberti was an Italian Renaissance humanist author, artist, architect, poet, priest, linguist, philosopher and cryptographer.

C. NI

5. Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process are Belgian.

A. True

2.3

1. Who invented one-time pad encryption for Telex Traffic?

   A. Hugo Alexander Koch B. Gilbert S. Vernam

   C. Dr. Horst Feistel D. Charles Babbage

2. What cipher did Julius Caesar use to secure military and government communications?

   A. Monoalphabetic substitution cipher B.A simple substitution cipher

   C.A & B are incorrect D.Tranposition cipher

3. What is one of the most significant contribution provided by public-key cryptography?

   A. The one-time pad B.The key distribution

   C.The frequency analysis D.The digital signature

4. When was the Enigma cipher broken? Who broke it?

   A. In World War II/The Japanese B. In1939 -1942/The Allies

   C. In World War I/The Americans D.In the 1942/The British

5. Which of the followings is one of the first block ciphers?

   A. Caesar cipher B.Wheel cipher

   C.Lucifer cipher D.Vigenère cipher

6. Who broke Japan's Purple's ciphers?

   A. William Friedman B. Gilbert S. Vernam

   C. Horst Feistel D. Phil Zimmermann

7. What types of cipher were used in radio communications during World War I?

   A. Transposition ciphers Substitution ciphers

   C. Enigma cipher D. A&B are correct

8. Why did the United States decide to take part in World War II?

   A.Because the Zimmerman Telegram was broken.

B. Because the Enigma machine was broken.

C. Because the Purple machine was used.

D. Because Lucifer cipher was used.

Reading 3

2.1

1. What do the letter A,M,C,K denote?

A denotes a finite set called the alphabet of definition. M denotes a set called the message space. C denotes a set called the ciphertext space. K denotes a set called the key space

2. Which letters denote a key pair?

The keys e and d in the preceding definition are referred to as a key pair and sometimes denoted by (e, d).

3. What is D, called?

Dd is called a decryption function or decryption transformation.

4. What does an encryption scheme consist of?

An encryption scheme consists of a set {Ee : e e K} of encryption transformations and a corresponding set {Dd : d e K}.

5. What does one have to do to construct an encryption scheme?

To construct an encryption scheme requires one to select a message space M, a ciphertext space C, a key space K, a set of encryption transformations {Ee : e e K} and a corresponding set of decryption transformations {Dd : d e K}

6. What does one have to do to construct an encryption scheme?

If the owner suspects that the combination has been revealed he can easily reset it without replacing the physical mechanism.

7. How is an encryption scheme used to achieve confidentiality?

An encryption scheme may be used as follows for the purpose of achieving confidentiality. Two parties Alice and Bob first secretly choose or secretly exchange a key pair (e, d). At a subsequent point in time, if Alice wishes to send a message m e M to Bob, she computes c = Ee (m) and transmits this to Bob. Upon receiving c, Bob computes Dd (c) = m and hence recovers the original message m.

2.2

1. A letter of the English alphabet can be assigned unique binary strings of length five.

A. True

2. The structure of the lock is available to anyone who wishes to purchase one but the combination is chosen and set by the owner.

A. True

3. M consists of strings of symbols from the binary alphabet.

B.False

4. There are 23 binary strings of length nine

B. False

5. A decryption scheme consists of a set {E.: e K} of decryption transformations.

B. False

2.3

1. An element of *M* is called …….....

   a a ciphertext space

   b a ciphertext

   c a decryption scheme

   d a plaintext message or simply a plaintext

2. An element of *K* is called …….....

   a an alphabet of definition B. a key

C. a ciphertext D. a plaintext

3. An element of *C* is called …….....

a a ciphertext space B. a decryption scheme

C. a ciphertext D. a key pair

4. One has to …… if some particular encryption or decryption transformation is revealed.

a change the key

b redesign the entire scheme

c change the key

d reset the key

5. The structure of the lock …….but the combination is chosen and set by the owner.

a is available to anyone who wants to purchase one

b is unavailable to anyone who wishes to purchase one

c A & B are correct

d All above

6. The diagram in *Figure 5-3.* Schematic of a simple encryption scheme is good for describing an encryption scheme ……

a when the set is typically of astronomical proportions

b When the set is small

c When is a small set

d B & C are correct

Reading 4

2.1

1. What is the difference among a sender, a receiver, and an adversary?

A sender is an entity in a two-party communication which is the legitimate transmitter of information.

A receiver is an entity in a two-party communication which is the intended recipient of information.

An adversary is an entity in a two-party communication which is neither the sender nor receiver, and which tries to defeat the information security service being provided between the sender and receiver.

2. What are unsecured channel and secured channel?

An unsecured channel is one from which parties other than those for which the information is intended can reorder, delete, insert, or read.

A secured channel is one from which an adversary does not have the ability to reorder, delete, insert, or read.

3.What is the only thing that the two parties keep secret when using an encryption scheme?

When two parties wish to communicate securely using an encryption scheme, the only thing that they keep secret is the particular key pair (e, d) which they are using, and which they must select

4.Can an encryption scheme be broken? When and how?

Yes, it can. By trying all possible keys to see which one the communicating parties are using

5.What does the word This in the last paragraph refer to?

An encryption scheme can be broken by trying all possible keys to see which one the communicating parties are using

6.What is the objective of a designer of an encryption scheme?

to keep information secret (or to protect confidential information)

7.What is information security service? Give some example.

Information security service is a method to provide some specific aspects of security. For example, integrity of transmitted data is a security objective, and a method to ensure this aspect is an information security service.

8.What is the difference between an active adversary and a passive adversary?

A passive adversary is an adversary who is capable only of reading information from an unsecured channel.

An active adversary is an adversary who may also transmit, alter, or delete information on an unsecured channel

2.2

1, The term adversary has five other names including enemy, attacker, opponent, tapper, and eavesdropper.

B.False

2, An appropriate time frame will never be a function of the useful lifespan of the data being protected.

B.False

3, Maintaining the secrecy of the transformations is very difficult indeed.

A.True

4, There are many different terms replacing the word an adversary which tries to play the role of either the legal receiver or the legal sender.

B.False

5, An unsecured channel is one from which an adversary does not have the ability to reorder, delete, insert, or read.

B.False

2.3

1. Which channel is not physically accessible to the adversary?
   A. A physically secure channel or secured channel
   B. An unsecured channel
   C. A secured channel
   D. A. secure channel
2. Which role does an adversary attempt to play in a two-way communication?
   A. the illegitimate sender or the illegitimate receiver
   B. The role of the sender only
   C. the legitimate sender or the legitimate receiver
   D. The role of the receiver only
3. What is a fundamental premise in cryptography?
   A. the set *A, C, K* $\{E_e : e \quad K\}, \{D_d : d \quad K\}$
   B. the sets *M, C, K* $\{E_e : e \quad K\}, \{D_d : d \quad K\}$
   C. Either A or B
   D. Both A and B
4. A/An ……is an entity in a two-party communication which is the legitimate transmitter of information.
   A. sender B. receiver
   C. adversary D. channel
5. A/An …… is an entity in a two-party communication which is the intended recipient of information.
   A. channel B. adversary
   C. sender D. receiver

6…….. an information security service implies defeating the objective of the intended service.

A. Transmitting B. Defeating

C. Breaking D. Conveying

7. A/An ……is an adversary who is capable only of reading information from an unsecured channel.

A. passive adversary B. active adversary

C. entity D. party

8. A/An ….. is a means of conveying information from one entity to another.

A. adversary B. information security service

C. exhaustive search D. channel

9. An ……is an adversary who may also transmit, alter, or delete information on an unsecured channel.

A. passive adversary B. entity

C. active adversary D. party

10.……is a method to provide some specific aspects of security.

A. Channel B. Information security service

C. exhaustive search D. Secure channel

UNIT 6

Reading 1

2.1

1. What are Hash functions?

Hash functions are mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm the identity of a specific message and to confirm that there have not been any changes to the content.

2. Why are hash functions considered one-way operations?

Because in this function the same message always provides the same hash value.

3. What is the message digest?

The message digest is a fingerprint of the author's message that is compared with the recipient's locally calculated hash of the same message.

4. Why are hash functions widely used in e-commerce?

Because hash functions confirm message identity and integrity, both of which are critical functions in e-commerce.

5. What does SHS stand for? What is it?

SHS stands for Secure Hash Standard. It is a standard issued by the National Institute of Standards and Technology (NIST)

6. What are hash algorithms?

Hash algorithms are public functions that create a hash value, also known as a message digest, by converting variable-length messages into a single fixed-length value

7. What is a measurement of the strength of the algorithm against collision attacks?

The number of bits used in the hash algorithm is a measurement of the strength of the algorithm against collision attacks.

8. What attack method has become a concern about the strength of the processes used for password hashing?

A recent attack method called rainbow cracking has generated concern about the strength of the processes used for password hashing

2.2

1. No matter how well passwords constructed, they are broken or cracked even using the fastest computers.

A. True

2. Rainbow cracking is never cracked so it has become a concern about the strength of the processes used for password hashing.

B. False

3. Hash function calculates a hash value based on the user's password input.

A. True

4. Users only have to protect the file of hashed passwords and to implement strict limits to the number of attempts allowed per login session in order to prevent rainbow cracking.

B. False

5. There are not information-theoretically secure schemes

C.NI

2.3

1. Why are hash functions used in password verification systems to confirm the identity of the user?
    A. Because hash functions are mathematical algorithms.
    B. Because hash functions are one-way.
    C. Because hash functions are publish functions.
    D. Because hash functions don't require the use of key.
2. What will attackers do if they gain access to a file of hashed passwords? and.
    A. They can use a combination of brute force
    B. They can use dictionary attacks to reveal user passwords

C. A&B are correct

D. They can generate a message summary or digest.

3. What do users have to do to prevent rainbow cracking?

A. They have to protect the file of hashed passwords

B. They have to implement strict limits to the number of attempts allowed per login session

C. They have to use an password hash salting approach

D. All are correct

4. Which passwords are considered easily to be cracked?

A. Passwords that are dictionary words

B. Passwords that are poorly constructed

C. Passwords that are dictionary words and poorly constructed.

D. Password that are not long enough.

5. By using ..... attacks to reveal user passwords, attackers gain access to a file of hashed passwords.

A. a combination of brute force

B. dictionary

C. a known-plaintext

D. A&B are correct

6. What specifies SHA-1 as a secure algorithm for computing a condensed representation of a message or data file?

A. Standard document FIPS 180-2

B. The National Institute of Standards and Technology

C. A&B are correct

D. Standard document FIPS 180-1

7. Which applications in the information security do cryptographic hash functions bring?

E. digital signatures, message authentication codes

F. and other forms of authentication.

G. A&B are correct

H. message authentication codes

8. Which of the following properties that an ideal cryptographic hash function needs to have?

I. It is easy to compute the hash value for any given message

J. It is infeasible to generate a message that has a given hash and to modify a message without changing the hash

K. It is infeasible to find two different messages with the same hash.

L. All are correct

Reading 2:

2.1

1. What is the primary challenge of symmetric key encryption?

is getting the key to the receiver, a process that must be conducted out of band (meaning through a channel or band other than the one carrying the ciphertext) to avoid interception.

2. What symmetric encryption cryptosystems are the most widely used? Give some information about them.

The Data Encryption Standard (DES)

3. What is called symmetric encryption?

*Encryption methodologies that require the same **secret key** to encipher and decipher the message.*

4. When was a DES key broken and who broke it?

In 1998. By a group called the Electronic Frontier Foundation

5. Why do symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms?

so that the encryption and decryption processes are executed quickly by even small computers.

6. What are the disadvantages of symmetric encryption method?

is that both the sender and the recipient must have the secret key. Also, if either copy of the key falls into the wrong hands, messages can be decrypted by others and the sender and intended receiver may not know the message was intercepted. The primary challenge of symmetric key encryption is getting the key to the receiver.

7. Why was Advanced Encryption Standard born?

to replace both DES and 3DES

8. What is the difference between DES and AES?

DES uses a key length of 128 bits, uses a 64-bit block size and a 56-bit key while AES implements a block cipher called the Rijndael Block Cipher with a variable block length and a key length of 128, 192, or 256 bits.

2.2

1. 3DES has higher level of security than DES.

A.True

2, The Secretary of Commerce approved AES as the official federal governmental standard at the end of May, 2002.

A.True

3, Symmetric encryption method has no drawbacks and it has been sued for a long time.

B.False

4, It is only the U.S. government itself selected AES as federal government standard.

B.False

5, AES is based on the Rijndael cipher developed by two Russian cryptographers.

C. NI

2.3

1. What is Data Encryption Standard based on?

   A. Rijndeal cipher B. Lucifer algorithm

   A. computational hardness D. None is correct

2. The requirements for AES stipulate that the algorithm should .....

   A. be unclassified B. be publicly disclosed.

   A. available royalty-free worldwide D. All are correct

3. When was Data Encryption Standard found unsafe? A. In 1976

   B. In 1998

   C. In 1997 D. In 2002

4. Which of the following agencies in the U.S are allowed to use AES to protect information?

   A. Agencies that are considered a part of national defense.

   B. Agencies that are not a part of the national defense infrastructure.

   C. A & B are correct

   D. Agencies that are considered a part of national policemen.

5. Which of the followings has the highest level of security?

A. DES B. Triple DES

C. AES D. RSA

Reading 3

2.1

1. What is asymmetric encryption?

It uses two different but related keys, and either key can be used to encrypt or decrypt the message.

2. What symmetric encryption cryptosystems is one of the most popular public key cryptosystems?

RSA

3. What is the foundation of public-key encryption?

Asymmetric algorithms are one-way functions .A one-way function is simple to compute in one direction, but complex to compute in the opposite direction.

4, What is the highest value of the asymmetric encryption when one key is used as a private key?

It can be used to provide elegant solutions to problems of secrecy and verification.

5. What is a mathematical trapdoor?

is a "secret mechanism that enables you to easily accomplish the reverse function in a one-way function"

6. What is public-key encryption based?

on a hash value

7. What can users do and what can't they do with a trapdoor?

They can use a key to encrypt or decrypt the ciphertext, but not both (they can't use a key to encrypt and decrypt.)

2.2

1, The great advantage of private key cryptography is that any two parties anywhere who have the private key software can securely exchange messages without having to make any prior arrangements.

A.True

2, With a trapdoor, encryption and decryption are performed by using the same key.

B.False

3, Asymmetric encryption is also called public-key encryption because tin a key pair, one key is stored in a public location where anyone can use it.

A.True

4, People who were using public key cryptography had to switch to 150-digit or 200-digit primes if they wanted security.

C.NI

5, Symmetric encryption method is not as good as asymmetric encryption one, so no methods can replace it.

B.False

2.3

6. Who developed RSA algorithm?

A. Ron Rivest
B. Adi Shamir
C. Leonard Adleman
D. All arec correct

7. What is the disadvantage of RSA?

A. Holding a single conversation between two parties requires four keys.

B. Key distribution

C. Holding a single conversation between two parties requires two pairs of keys.

D. A&C are correct

8. What must four organizations do if they want to communicate?

A. Each party must control its public key and four private keys.

B. Each party must manage its public key and four private keys.

C. A&B are correct

D. Each party must manage its private key and four public keys.

9. In which of the following uses is RSA useful?

A. Trading use

B. Commercial use

B. mathematical use

D. computer use

10. Where is RSA embedded?

A. In Netscape Websites

B. In Microsoft

C. In Microsoft and Netscape Web browsers

D. A&C are correct

Reading 4:

2.1

1. What does PKI stand for? What is it?

PKI stands for Public-key Infrastructure. PKI is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely.

2. What components are integrated for a typical solution PKI to protect the transmission and reception of secure information?

They are A certificate authority (CA), A registration authority (RA) , Certificate directories, Management protocols and Policies and procedures.

3. What do common implementations of PKI include?

Common implementations of PKI include systems that issue digital certificates to users and servers; directory enrollment; key issuing systems; tools for managing the key issuance; and verification and return of certificates.

4. What does the strength of a cryptosystem rely?

The strength of a cryptosystem relies on both the raw strength of its key's complexity and the overall quality of its key management security processes.

5. What are digital certificates?

Digital certificates are public-key container files that allow computer programs to validate the key and identify to whom it belongs.

6. What is critical to the successful use of encryption and nonrepudiation services within the PKI's area of trust.10?

Managing the security and integrity of the private keys used for nonrepudiation or the encryption of data files

7. What are Public-key Infrastructure systems based on?

PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs).

8. What mechanisms can PKI solutions provide for limiting access and possible exposure of the private keys?

These mechanisms include password protection, smart cards, hardware tokens, and other hardware-based key storage devices that are memory-capable

2.2

1. The purpose of a digital certificate is to establish the identity of users within the ecosystem.

A. True

2. An entity must be uniquely identifiable within each CA domain on the basis of information about that entity. A third-party validation authority can provide this entity information on behalf of the CA.

A. True

3. The strength of key's complexity and the overall quality of key management are the fundamental factors that are not important for information security protection.

B. False

4. The CA provides a certificate revocation list to its users, but it doesn't take their keys when a private key is agreed, or when their privilege of using keys in the area of authority are lost.

B. False

5. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

C.NI

2.3

11. What can the CA do when the user loses the privilege of using keys in the area of authority?

A. The CA can withdraw the user's keys.

B. The CA can revoke the user's keys.

C. A&B are correct

D. A The CA can destroy the user's keys.

12. What is the function of a central system operated by a CA?

A. It generates cryptographically strong keys that are considered by all users to be independently trustworthy.

B. It provides private key backup, key recovery, and key revocation.

C. A&B are correct

D. It verifies any user against the current certification revocation list.

13.Which mechanisms should PKI users select in digital certification?

A. The key security mechanisms that provide a level of key protection appropriate to their needs.

B. The convenient mechanisms that help them exchange communication quickly.

C. The good transaction mechanisms that enable them do what they need

D. A&C are correct

14.The .....by the CA enables secure, encrypted, nonrepudiable e-business transactions. nen soan lai cau nay

A. policy of certificate

B. issuance of certificates

C. mechanisms of certificate

D. procedure of certificate

15.How often does the CA distribute a certificate revocation list to all users?

A. Yearly

B. Regulary

C. Twice a year

D. Monthly

Reading 5

2.1

1. What are correlation attacks?

are a collection of brute-force methods that attempt to deduce statistical relationships between the structure of the unknown key and the ciphertext generated by the cryptosystem.

2.What method can prevent correlation attacks?

The only defense against this attack is the selection of strong cryptosystems that have stood the test of time, thorough key management, and strict adherence to the best practices of cryptography in the frequency of key changes.

3. What is a man-in-the-middle attack?

attempts to intercept a public key or even to insert a known key structure in place of the requested public key. Thus, attackers attempt to place themselves between the sender and receiver, and once they've intercepted the request for key exchanges, they send each participant a valid public key

4. What method can prevent the traditional man in-the-middle attack?

Establishing public keys with digital signatures can prevent the traditional man in-the-middle attack, as the attacker cannot duplicate the signatures.

5. When can dictionary attacks be successful?

when the ciphertext consists of relatively few characters

6. When may the attacker launch a replay attack in timing attack?

When he finishes breaking an encryption

7. What method was used to get unauthorized access to secure communications?

brute force attacks

8. What type of attacks are mentioned according to the text?

man-in-the-middle, correlation, dictionary, and timing.

2.2

1, An attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other is called a man - in - the - middle attack.

A.True

2, Although frequency analysis is the able to permit an inexperienced attacker to crack most any code quickly, modern algorithms can break it.

A.True

3, A well-known one-way hash function is used to store passwords, so the attacker is not able to crack it and the information is never stolen.

B.False

4, More sophisticated means of hiding information from those who should not see it have been developed increasingly so the information security is always sate.

B.False

5, A dictionary attack is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary.

C.NI

2.3

1. What attacks were used to gain unauthorized access to secure communications?

A. Brute force attacks B. known-plaintext attacks

C. selected –plaintex attacks D. All are correct

2. Attackers may conduct a .....by sending potential victims a specific text that they are sure the victims will forward on to others.

A. known-plaintext attack B. selected-plaintext attack

C. Brute force attack D. A &C are correct

3. .....have been used to mount successful attacks on block cipher encryptions such as DES.

A. Differential and linear cryptanalysis B. Differential cryptanalysis

C. Frequency analysis D. Linear cryptanalysis

4. In which attack does the attacker eavesdrop on the victim's session? A. In a dictionary attack B. In a correlation attack

C. In a man-in-the middle attack D. In a timing attack

5. Which of the following does the word "**these**" in the paragraph 6 refer to?

A. Correlation attacks

B. Brute-force methods

C. Differential and linear cryptanalysis

D. Advanced methods

UNIT 7

Reading 1

2.1

1. How can you define a secure facility?

A secure facility is a physical location that has in place controls to minimize the risk of attacks from physical threats.

2. Why are guards considered the most effective form of control for situations that require decisive action in the face of unfamiliar stimuli?

*Guards can evaluate each situation as it arises and make reasoned responses. Most guards have clear standard operating procedures **(SOPs)** that help them to act decisively in unfamiliar situations*

3, When should dogs be used for physical security?

When an organization is protecting valuable resources.

4. What are the weaknesses of ID cards and name badges?

ID cards and name badges are not foolproof and even the cards designed to communicate with locks can be easily duplicated, stolen, or modified.

5. What is tailgating?

Tailgating occurs when an authorized person presents a key to open a door, and other people, who may or may not be authorized, also enter.

6. What are the measures to prevent tailgating?

Launching a campaign to make employees aware of tailgating is one way to combat this problem. There are also technological means of discouraging tailgating, such as mantraps (which are discussed in a following section) or turnstiles.

7. List two types of lock mechanism. What is the difference between them?

There are two types of lock mechanisms: mechanical and electromechanical. The mechanical lock may rely on a key that is a carefully shaped piece of metal which is rotated to turn tumblers that release secured loops of steel, aluminum, or brass (as in, for example, brass padlocks). Alternatively, a mechanical lock may have a dial that rotates slotted discs until the slots on multiple disks are aligned, and then retracts a securing bolt (as in combination and safe locks). Electromechanical ***locks*** *can accept a variety of inputs as keys, including magnetic strips on ID cards, radio signals from name badges, personal identification numbers (PINs) typed into a keypad, or some combination of these to activate an electrically powered locking mechanism.*

8. List and describe the four categories of locks. In which situation is each type of lock preferred?

> *Locks can also be divided into four categories based on the triggering process: manual, programmable, electronic, and biometric.*

Manual locks *such as padlocks and combination locks can be opened if you have the key (or combination). When they are installed into doors, they can only be changed by highly trained locksmiths.*
Programmable locks *can be changed after they are put in service, allowing for combination or key changes without a locksmith and even allowing the owner to change to another access method (key or combination) to upgrade security.*
Electronic locks *can be integrated into alarm systems and combined with other building management systems.*
The most sophisticated locks are ***biometric locks****. Finger, palm, and hand readers, iris and retina scanners, and voice and signature readers fall into this category.*

9.What are the two possible modes that locks use when they fail? What implications do these modes have for human safety? In which situation is each mode preferred?

Locks fail in one of two ways: the door lock fails and the door becomes unlocked—a fail-safe lock; or the door lock fails and the door remains locked—a fail-secure lock. A fail-safe lock is usually used to secure an exit, where it is essential that in the event of, for instance, a fire, the door is unlocked. A fail-secure lock is used when human safety in the area being controlled is not the dominant factor. One example of this is a situation in which the security of nuclear or biological weapons needs to be controlled; here, preventing a loss of control of these weapons is more critical to security (meaning it is a security issue of greater magnitude) than protecting the lives of the personnel guarding the weapons.

10. What is a mantrap? When should it be used?

A mantrap is a small enclosure that has separate entry and exit points. To gain access to the facility, area, or room, a person enters the mantrap, requests access via some form of electronic or biometric lock and key, and if confirmed, exits the mantrap into the facility.

11. What are the disadvantages of video monitoring systems?

The first disadvantage is that for the most part they are passive and do not prevent access or prohibited activity. Another drawback to these systems is that people

must view the video output, because there are no intelligent systems capable of reliably evaluating a video feed. To determine if unauthorized activities have occurred, a security staff member must constantly review the information in real time or review the information collected in video recordings.

2.2

1, Anti-tailgating controls are common and affordable measures to deploy.

B.False

2, Only a key that is a carefully shaped piece of metal can be used to open a mechanical lock.

B.False

3, Manual locks are very popular.

A.True

4, Electricity is necessary to operate a mechanical push button locks.

B.False

5, A fail-safe lock could cause more dangers for people than a fail-secure lock.

B.False

6, CCT is the most often used electronic monitoring equipment.

C.NI

Reading 2

2.1

1. What is considered the most serious threat within the realm of physical security? Why is it valid to consider this threat the most serious?

The most serious threat is fire. Fires account for more property damage, personal injury, and death than any other threat to physical security.

2.How do fire suppression systems manipulate the three elements for a fire to burn?

These systems typically work by denying an environment one of the three requirements for a fire to burn: temperature (ignition source), fuel, and oxygen.

3.What is flame point? In which situation can paper reach its flame point?

Flame point is the temperature of ignition. Paper can reach that temperature when it is exposed to a carelessly dropped cigarette, malfunctioning electrical equipment, or other accidental or purposeful misadventures.

4. What is the role of a floor monitor?

During the chaos of a fire evacuation, an attacker can easily slip into offices and obtain sensitive information. To help prevent such intrusions, fire safety programs often designate an individual from each office area to serve as a floor monitor.

5.List and describe the three fire detection technologies covered in the chapter. Which is currently the most commonly used?

There are three basic types of fire detection systems: thermal detection, smoke detection, and flame detection. Smoke detection is the most common.

6. List three ways in which smoke detectors operate. Which type is the most expensive?

Smoke detectors operate in one of three ways: ***photoelectric sensors, Ionization sensors, Air-aspirating detectors.*** *The last one is the most expensive.*

7. List and describe the four classes of fire described in the text. Does the class of a fire dictate how to control the fire?

- *Class A fires: Those fires that involve ordinary combustible fuels such as wood, paper, textiles, rubber, cloth, and trash.* ***Class A fires*** *are extinguished by agents that interrupt the ability of the fuel to be ignited. Water and multipurpose dry chemical fire extinguishers are ideal for these types of fires.*
- *Class B fires: Those fires fueled by combustible liquids or gases, such as solvents, gasoline, paint, lacquer, and oil.* ***Class B fires*** *are extinguished by agents that remove oxygen from the fire. Carbon dioxide, multipurpose dry chemical, and Halon fire extinguishers are ideal for these types of fires.*
- *Class C fires: Those fires with energized electrical equipment or appliances.* ***Class C fires*** *are extinguished with non-conducting agents only. Carbon dioxide, multipurpose dry chemical, and Halon fire extinguishers are ideal for these types of fires. Never use a water fire extinguisher on a Class C fire.*

- *Class D fires: Those fires fueled by combustible metals, such as magnesium, lithium, and sodium.* ***Class D fires*** *require special extinguishing agents and techniques*

2.2

1, Fire is the most popular danger to human safety in an organization's physical space.

C.NI

2, Ionization sensors are most usually found in places where highly valuable materials are stored.

C.NI

3, Flame detector is commonly installed in highly populated areas.

B.False

4, The suitable fire suppression system for small fires is portable extinguisher.

A.True

5, Fire suppression systems in every building need to be inspected and tested every year.

C.NI

Reading 3

2.1

1. What four physical characteristics of the indoor environment are controlled by a properly designed HVAC system?

The temperature, filtration, humidity, and static electricity controls.

2. What are the optimal temperature and humidity ranges for computing systems?

The optimal temperature for a computing environment (and for people) is between 70 and 74 degrees Fahrenheit. The optimal level of humidity in the computing environment is between 40 percent and 60 percent.

3.Why is air filtration NOT as important as it was in the past?

In the past it was thought necessary to fully filter all particles from the air flow from the HVAC system. Modern computing equipment is designed to work better in typical office environments, and thus the need to provide extensive filtration for air-conditioning is now limited to particularly sensitive environments such as chip fabrication and component assembly areas.

4.What is the cause of condensation problems? Which consequences may result from them?

High humidity levels create condensation problems. With condensation comes the short-circuiting of electrical equipment and the potential for mold and rot in paper-based information storage.

5.What do people use to adjust the humidity level?

Humidification or dehumidification systems.

6.Why is it critical that the grounding elements of the electrical system are installed properly?

If the grounding elements of the electrical system are not properly installed, anyone touching a computer or other electrical device could become a ground source, which would cause damage to equipment and injury or death to the person.

7.What are the consequences of overloading a circuit?

Overloading a circuit not only trips circuit breakers, but can also create a load on an electrical cable that is in excess of what the cable is rated to handle, and thus increase the risk of its overheating and starting a fire.

8.What is the role of UPS?

Assuring the delivery of electric power without interruption.

9.Why is an emergency power shutoff necessary, especially in computer rooms and wiring closets?

It is the last line of defense against personal injury and machine damage in the event of flooding or sprinkler activation. It is used to stop the flow of electricity to the room, preventing the water that might be used to extinguish the fire from short-circuiting the computers. While it is never advisable to allow water to come into contact with a computer, there is a much higher probability of recovering the systems if they were not powered up when they got wet.

10.What two critical functions are impaired when water is not available in a facility?

Fire suppression and air-conditioning systems.

2.2

1. Nowadays, temperature control is an important factor to protect most commercial data processing facilities.

C.NI

2, Nowadays, extensive filtration for air-conditioning is a must if you want to maintain an optimal environment for most commercial data processing facilities,

B.false

3, Ten volts of electricity may bring harm to the microchip.

A.True

4, Ventilation shafts are usually utilized by attackers to break into commercial building nowadays.

B.False

5, Both lack of water and a surplus of water could damage the computer systems.

A.True

UNIT 8:

Reading 1:

2.1

1. List and describe the three major steps in executing the project plan.

- *Planning the project*
- *Supervising tasks and action steps*
- *Wrapping up*

2, What is a work breakdown structure (WBS)? Is it the only way to organize a project plan?

It is a planning tool. No.

3.List and define the common attributes of the tasks of a WBS.

- To use the WBS approach, you first break down the project plan into its major tasks. The major project tasks are placed into the WBS, along with the following attributes for each:

- *Work to be accomplished (activities and deliverables)*
- *Individuals (or skill set) assigned to perform the task*
- *Start and end dates for the task (when known)*
- *Amount of effort required for completion in hours or work days*
- *Estimated capital expenses for the task*
- *Estimated noncapital expenses for the task*
- *Identification of dependencies between and among tasks*

4.How does a planner know when a task has been subdivided to an adequate degree and can be classified as an action step?

Given the variety of possible projects, there are few formal guidelines for deciding what level of detail—that is, at which level a task or subtask should become an action step—is appropriate.

5.What is a deliverable? Name two uses for deliverables.

A deliverable is a completed document or program module that can either serve as the beginning point for a later task or become an element in the finished project.

6.How could you determine whether a task or subtask can become an action step?

A task or subtask becomes an action step when it can be completed by one individual or skill set and has a single deliverable.

7.What is a resource? What are the two types?

A resource is the skill set or person needed to accomplish the task.

8.What is a milestone? and why is it significant to project planning?

A milestone is a specific point in the project plan when a task that has a noticeable impact on the progress of the project plan is complete.

9.Who is the best judge of effort estimates for project tasks and action steps? Why?

Planners need to estimate the effort required to complete each task, subtask, or action step. Estimating effort hours for technical work is a complex process. Even when an organization has formal governance, technical review processes, and change control procedures, it is always good practice to ask the people who are most familiar with the tasks or with similar tasks to make these estimates.