تجميعات امن الحاسب – midterm1

د. ريم التايب – Oct2021

ملاحظة: أسئلة التشفير الانشائية تطلع بمسافات وحروف كبتل لكن ((بطلب من الدكتورة تكتب بحروف سمول + بدون مسافات عشان طريقة تصحيحها))

هايلايت سماوي = نوع التشفير

هايلايت وردي = المطلوب سواء فك او تشفير

Encrypt the message **Hi Samar with Caesar cipher (k=6)**

The answer is: noygsgx

The message **Khool pb frxqwub** was encrypted using a Caesar cipher. **Decrypt the message.**

The answer is: hellimycountry

Encrypt the message **Good luck** with the keyword **cipher** using **Playfair** cipher .

The answer is: ovtrnsig

Encrypt the message **Hi Samar** with Affine cipher and the key (17,3)

The answer is: sjxdzdg

A coded message is called .....

The answer is: ciphertext

.....: a field of both cryptography and cryptanalysis

The answer is: cryptology

Asymmetric cryptography uses .....

The answer is: 2 key

---------- in a system that may be able to be exploited in order to cause loss or harm.

The answer is: weaknesses

Non-technical means can be used to protect against some classes of attack is called .....

The answer is: policies

.....attempting to reverse calculate a password

The answer is: password crack

.....: unsolicited commercial e-mail; more a nuisance than an attack, though is emerging as a vector for some attacks

The answer is: spam

--------- : study of methods of deciphering ciphertext without knowing key.

The answer is: cryptanalysis

---------- is an object, person, or other entity that represents a constant danger to an asset.

The answer is: threat

----------: Act or action that exploits vulnerability (i.e., an identified weakness) in controlled system

The answer is: attack

DoS is the abreviation of ----------

The answer is: denial-of-service

Things we might want to protect are called .....

The answer is: asset

Quiz1

٩/١١/٢١

Decrypt the following message using **Caesar Cipher.**
plaintext= " khoor zrung"

Hello workd

Encrypt the following message with **Row transposition Cipher . The key is 2143**

plaintext =" hello rim"

Erhol mil

Encrypt the following message with **Playfair Cipher . The key is "Occurence"**

plaintext= "ballon"

DBIZGEBV

Encrypt the following message with **Playfair Cipher . The key is "Occurence"**

plaintext= "tall trees"

pfiz tzeort

٤

Encrypt the following message with **vigenère Cipher . The key is "bannana"**

plaintext= " we love nature"

xe ybvr nbthee

Encrypt the following message with **Autokey Cipher . The key is "bannana"**

plaintext= " we love nature"

Xe ybvr nwxxffz

Encrypt the following message with **Caesar Cipher .**

plaintext= " we are happy"

zh duh kdssb

Midterm2

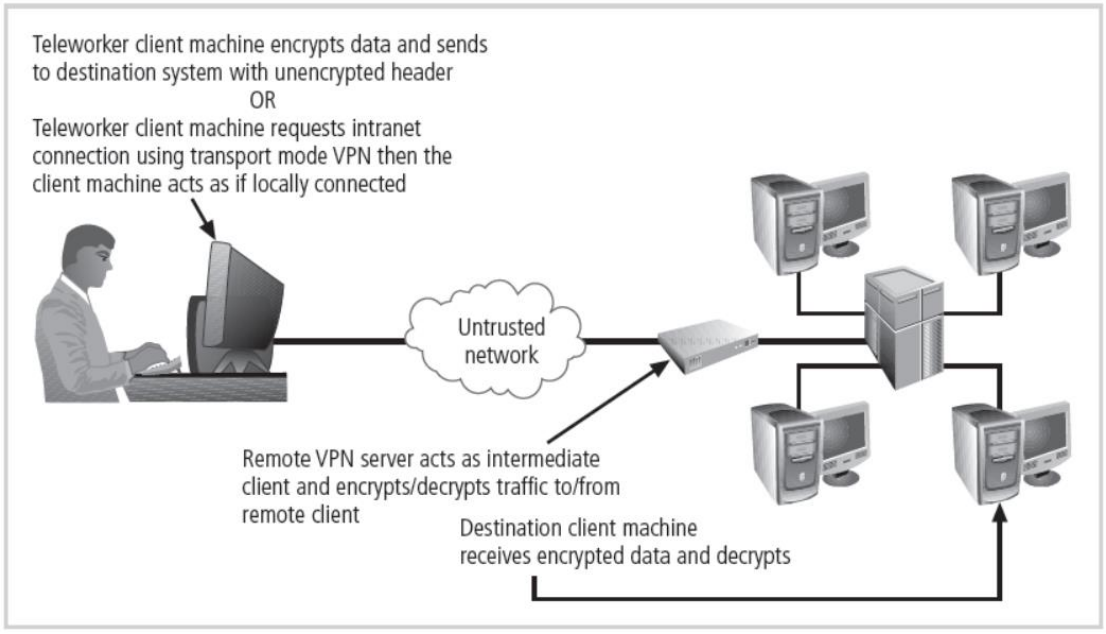
.is not among processing modes of firewal----------

Privacy

Mode operates at network layer ----------

Packet filtering

This figure shows



Transport mode VPN

---------- VPN is the abreviation of

Virtual private networks

…… best method for preventing an illegal or unethical activity; e.g., laws, policies, technical controls

Deterrence

The step ------ is not one of risk management steps

Risk examination

Among Criteria policy enforcement we found:

reading

,Among causes of unethical and illegal behavior we found

Ignorance

A ..... prevents specific types of information from moving between the untrusted network and known as the trusted network.

Firewalls

define socially acceptable behavior.....

Ethics

requires that filtering rules governing how the firewall decides which packets are allowed and which are------
denied are developed and installed.

Static filtering

rules that mandate or prohibit certain societal behavior.....

Laws

.allows firewall to react to emergent event and update or create rules to deal with event----------

Dynamic filtering

body of expectations that describe acceptable and unacceptable employee behaviors in the workpl.....

Polices

----------is not from subsets of packet filtering firewalls.

Mobile filtering

---------- Operates at transport layer.

Circuit gateway firewall

^

The second step of risk management is……

Know the enemy: identify, examine, and understand threats facing the organization

The first step of risk management is ----------

Know yourself: identify , examine, and understand the information and system currently in place

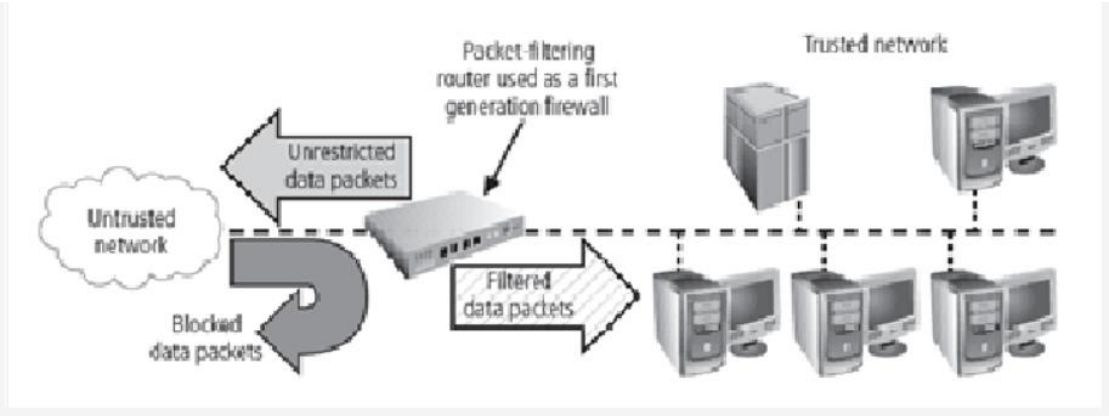
Risk management is composed by ..... main steps

3

..... are fixed moral attitudes.

Cultural more

which firewalls processing mode is presenting in this picture bellow ?



Packet – filtering router

Firewalls can be categorized by ..... processing modes

5

There are ……..architectural implementations of firewalls

4

COMPUTER SECURITY

1. Privacy means:
   Confidentiality

2. Malicious software (malware) designed to damage, destroy, or deny service to target systems is
   Software Attacks

3. The three Dimensions of infosecurity cube are:
   confidentiality, integrity, and availability

4. DoS attack means:
   Denial-of-service

5. …….. define socially acceptable behaviors; based on

   cultural mores (fixed moral attitudes or customs of a

   particular group).
   Ethics

6. Illegal taking of another's physical, electronic, or intellectual property is considered as

   Acts of Theft

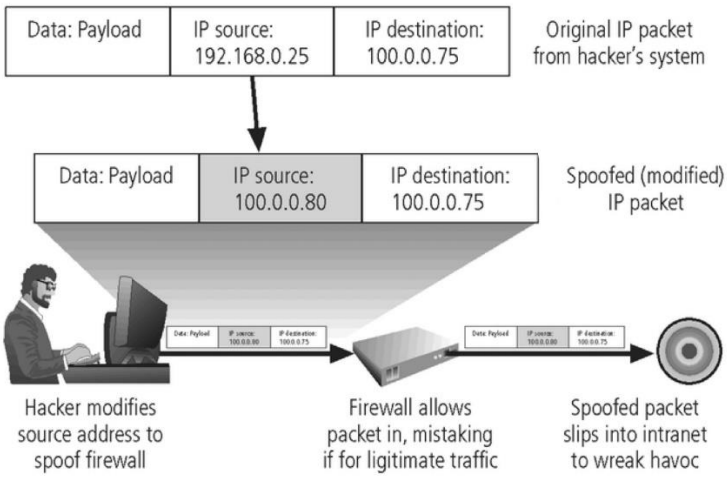
7. ……:Act or action that exploits vulnerability (i.e., an identified weakness) in controlled system

   Attacks

8. From the options below, which of them is not a threat to information security?

   Spoofing

9. The figure below shows a …….



IP spoofing

10. ……. Is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction.

Information security

11. ……. Is an object, person, or other entity that represents a constant danger to an asset.

Threat

12. Deliberate Acts of Espionage or Trespass means …….

Access of protected information by unauthorized individuals

13. …….. is a fixed moral attitudes or customs of a particular group; ethics based on these

Cultural mores

14. …….. rules that mandate or prohibit certain societal behavior

Laws

15. Fire and flood are example of …….. threat

Force of nature

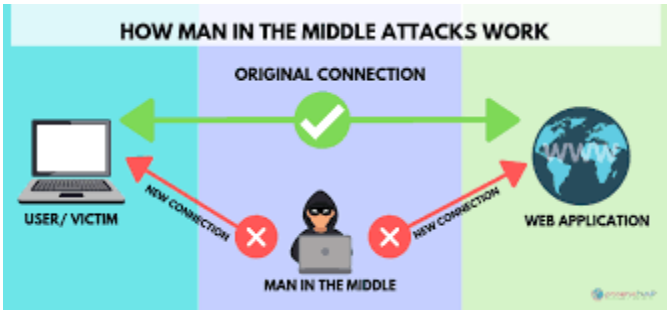
16. Malicious code **can not include** …….

Application error

17. Inexperience of an employee can causes ……

Threat

18. This figure represent a …….. attack



A men in the middle

19. Attempting to reverse calculate a password ……

Password crack

20. Security should be considered a balance between ……

protection and availability

21. Cryptology:

science of encryption; combines cryptography and cryptanalysis

22. Secure Multipurpose Internet Mail Extensions (S/MIME) is an extensions MIME by adding

encryption and authentication

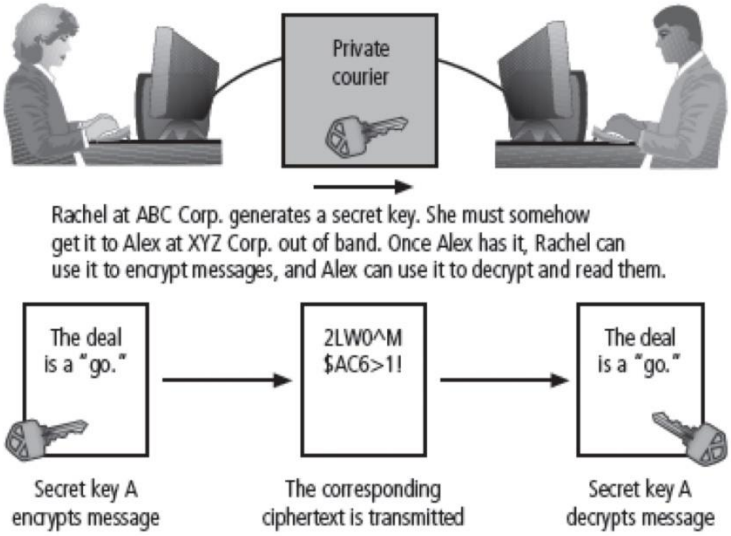
23. Intrusion prevention consists of ……

activities that seek to deter an intrusion from occurring

24. Cryptography means

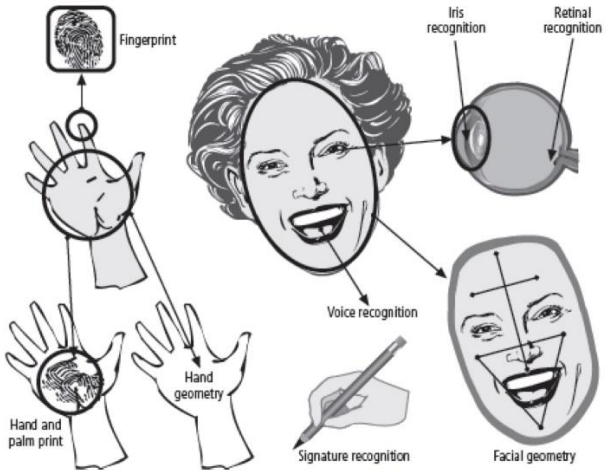
process of making and using codes to secure transmission of information

25. The figure below show an example of ……



Symmetric Encryption

26. The figure below shows



Biometric Access Control

27. Symmetric and asymmetric algorithms distinguished by…….. used for encryption and decryption operations

types of keys

28. Dictionary Attacks are based on

encryption every word in a dictionary using same cryptosystem

29. Correlation Attacks use ……

Differential and linear cryptanalysis

30. The goal of Secure Hypertext Transfer Protocol (S-HTTP) is

provides for encryption of individual messages between client and server across Internet

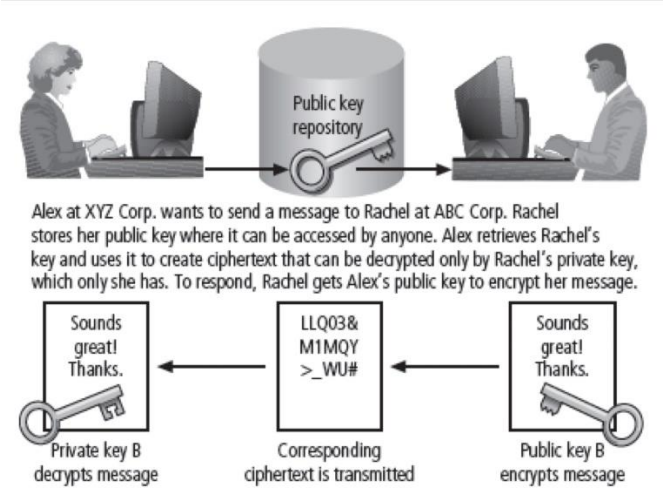
31. Decryption means

the process of converting the ciphertext message back into plaintext(original message)

32. IDPS is the abbreviation of ….

Intrusion Detection and Prevention Systems

33. The figure bellow show …..



Example of Asymmetric Encryption

34. Steganography is

Process of hiding information

35. ……. is the application of SSL over HTTP

S-HTTP

36. Digital Signatures uses …..

Asymmetric encryption

37. Cryptanalysis means

process of obtaining original message from encrypted message without knowing algorithms

38. Privacy Enhanced Mail (PEM): uses 3DES …….. encryption

symmetric key

39. Public-Key Infrastructure means

Integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely

40. SSL protocol uses public key encryption in order to

secure channel over public Internet

41. PKI is the abbreviation of ……

Public-Key Infrastructure

42. Intrusion means

occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system

43. Intrusion reaction means

actions an organization undertakes when intrusion event is detected

44. SSL protocol is the abbreviation of …..

Secure Socket Layer

45. Often grouped into two broad categories

symmetric and asymmetric

46. Attacks means

Attempts to gain unauthorized access to secure communications

47. Encryption means

Encryption: converting original message into a form unreadable by unauthorized individuals

48. Choose the wrong statement about encryption key size

When using ciphers, size of cryptovariable or key is not important

49. The purpose of a firewall on computer networks is to

Prevent unwanted network connections from being made

50. Hybrid firewalls consists to

Combine elements of other types of firewalls

51. There are ….. types of VPN

3

52. On of these subset **is not** a subset of packet filtering network

Hybrid filtering

53. Circuit gateway firewall operates a …..

transport layer

54. Which of the following can be considered to be a hardware firewall?

Router

55. A …… is a private and secure network connection between asystems

VPN

56. A ….. is not architectural implementations of firewalls

Circuit gateway firewall

57. Which one of the following is a key function of a firewall?

Monitoring

58. Packet filtering consists to …..

examine header information of data packets that come into a network

59. Dynamic filtering means …..

allows firewall to react to emergent event and update or create rules to deal with event

60. A …… is a set of security objectives for a company that includes rules of behavior for users and administrators and specifies system requirements.

security policy