جامعة العلوم والتقانة
كلية علوم الحاسوب وتقانة المعلومات
بكلاريوس نظم المعلومات
بكلاريوس تقنية المعلومات

إمتحانات نهاية الفصل للعام 2017-2018
السنة **الرابعة** الفصل **الثامن** الدفعة IS+ITB2014/2015
المقرر : أمن المعلومات

التاريخ : 2018/5/13م **الزمن :3 ساعات**

الإسم ..... الرقم .....

أجب عن جميع الأسئلة
ورقة الإمتحان تشتمل على 8 صفحات

Question (1):(20 Marks 10,10)

A) Define the following concepts and terms:

1. Information Security

---

2. Risk identification

---

3. policy

---

4. firewall

---

5. Cryptovariable

B) Complete the Following Sentences with suitable word (or words)

1. **Security** is protection against adversaries—from those who would do harm, …… or …….
2. Authorized users have legal access to a system, whereas hackers have illegal access to a system,……regulate this ability.
3. An…….can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object.

4. Control, safeguard**,** or …….**:** Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwiseimprove the security within an organization.
5. Unauthorized …….can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.
6. …….is the process ofidentifyingrisk, as represented by vulnerabilities, to an organization's information assets and infrastructure, and taking steps to reduce this risk to an acceptable level.
7. Once the organizational assets have been identified, a …….assessment process identifies and quantifies therisks facing each asset.
8. For a policy to be effective and thus legally enforceable, it must meet the five criteriaDissemination, Review, Comprehension, Compliance, and …….
9. …….is the matching of an authenticated entity to a list of information assets and corresponding access levels
10. Originally, firewalls focused primarily on service control, but they have since evolved to provide all four: Service control, Direction control, User control, and …….
11. AES implements a block cipher called the …….Cipher with a variable block lengthand a key length of 128, 192, or 256 bits.

Question (2)(20 Marks 10,10)

A) State weather the statements below is True (T)or False (F):

1- often *threat&attack* mean same ( )
2- Data Encryption Standard (DES) encrypts 64-bit data using 56-bit key ( )
3- Network security protect communications media, technology, and content. ( )
4- Risk Factorthe quantity and nature of risk the organization is willing to accept ( )
5- Information has **accuracy** when it is free from mistakes or errors and it has the value that the end user expects ( )
6- When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass ( )
7- A risk controls strategy requires that information security professionals know their organizations' information assets—that is, identify, classify, and prioritize them. ( )
8- Identificationis the process of validating a supplicant's purported identity. ( )
9- Access control list tracks the state and context of each packet in the conversation by recording which station sent what packet and when ( )
10- XOR encryption is a very simple A symmetric cipher that is used in many applications where security is not a defined requirement. ( )
11- **Cipher is** an encryption method or process encompassing the algorithm, key(s) and procedures used to perform encryption and decryption. ( )

B) Match A with B (Use the last Column (p4ut the letter))

A		B		A → B
1	a flaw in a software	A	Asymmetric encryption	1 →
2	secret key	B	Compromises to Intellectual Property	2 →
3	RSA	C	Spoofing	3 →
4	Vigenère cipher	D	Commercial e-mail.	4 →
5	data classification schemes	E	polyalphabetic substitutions	5 →
6	security posture	F	Risk identification	6 →
7	Spam	G	Mandatory access controls	7 →
8	Mail Bombing	H	Vulnerability	8 →
9	forged IP address	I	DOS	9 →
10	software piracy	J	symmetric encryption	10 →

Question (3)(18 Marks 2,4,4,4,4)

1- The same phases used in the traditional SDLC can be adapted to support the implementationof an information security project, While the two processes may differ in intent and specific activities

---

2- Information security performs four important functions for an organization list and brieflydiscusses each of them?

3- Why is data the most important asset an organization possesses? What other assets in the organization require protection?

4- Consider the statement: an individual threat agent, like a hacker, can be a factor in more than one threat category. If a hacker hacks into a network, copies a few files, defaces the Web page, and steals credit card numbers, how many different threat categories does this attack fall into?

5- Describe the "mitigate" strategy,What three planning approaches to mitigate risk by explain?

Question (4) (22Marks 3,3,6,10)

1- According to the NIST documentation on industry best practices, there are several compelling reasons to acquire and use an IDPS what's are (Why Use an IDPS)?

2- What are the firewall characteristics or (goals)?

3- What are the three types of security policies? Where would each be used? What type of policywould be needed to guide use of the Web? E-mail? Office equipment for personal use?

4- **What is the difference between the following**

1- Denial-of-Service (DoS) and (DDoS)

2- Standards and Practices

3- Nondiscretionary controls and Discretionary access controls (DACs).

4- application layer firewall and a packet-filtering firewall

---

5- bit stream method or the block cipher method

Question (5)(20 Marks 6,8,6)

1- If an organization has two information assets to evaluate for risk management, as shown in the accompanying data, which vulnerability should be evaluated for additional controls first? Which one should be evaluated last?

Data:

- Switch L47 connects a network to the Internet. It has two vulnerabilities: it is susceptible to hardware failure at a likelihood of 0.2, and it is subject to an SNMP buffer over flow attack at a likelihood of 0.1. This switch has an impact rating of 90 and has no current controls in place. You are 75 percent certain of the assumptions and data.

- Server WebSrv6 hosts a company Web site and performs e-commerce transactions. It has a Web server version that can be attacked by sending it invalid Unicode values. The likelihood of that attack is estimated at 0.1. The server has been assigned an impact value of 100, and a control has been implanted that reduces the impact of the vulnerability by 75 percent. You are 80 percent certain of the assumptions and data.

2- Use **Vernam cipher** to **encrypt** and **decrypt** the message “INFORMATION ", using the one time pad text“ FPQRYNSZBILACJ" .

3- Using the RSA Algorithm to **encrypt** and **decrypt** the message "TEXT", given the public key (33, 3) and private key (33, 7), using theposition of the letter in the alphabet?

Good luck