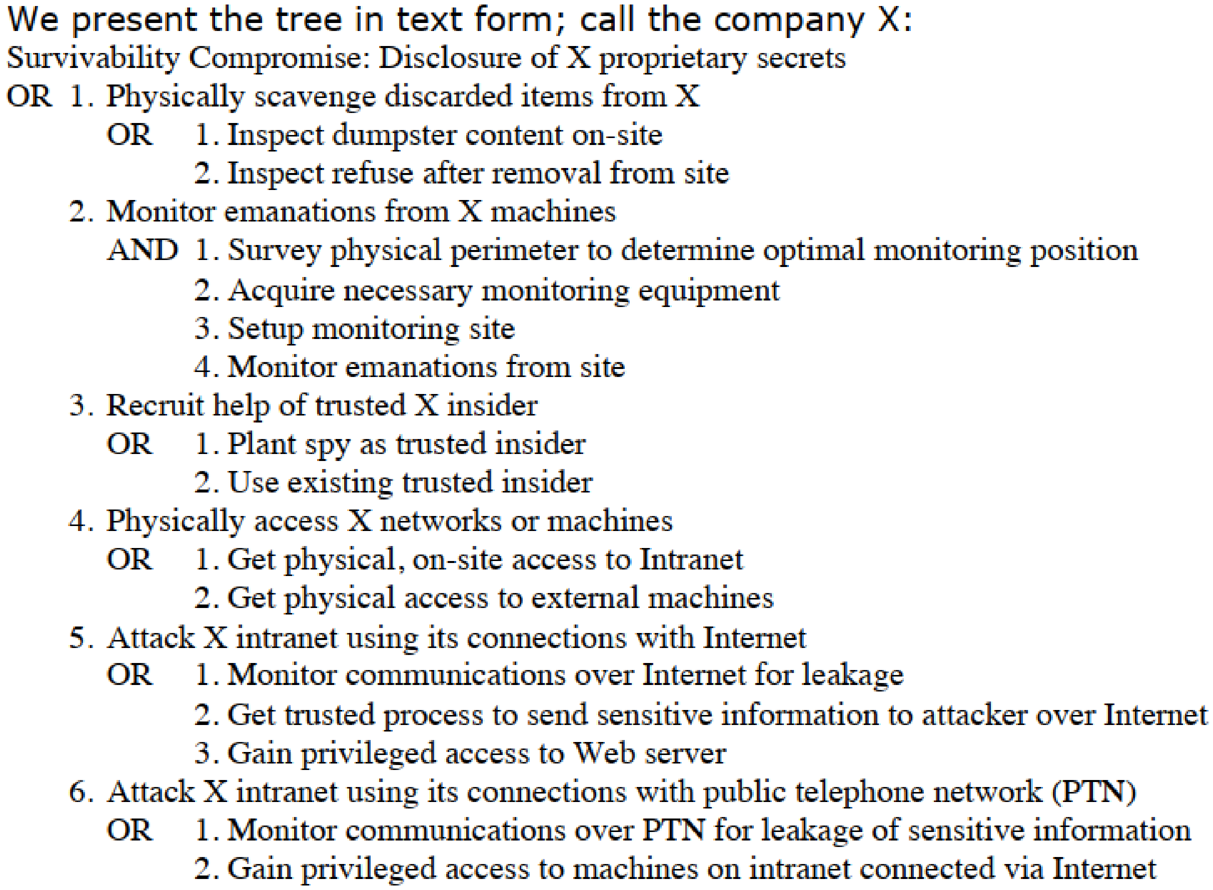
YILDIZ TECHNICAL UNIVERSITY
FACULTY of ELECTRICAL & ELECTRONICS ENG. / DEPT. of COMPUTER ENGINEERING

Student Name Surname:	**Number:**			**Signature:**	
Course: BLM4011 Gr1,2	**Date/Time: 21/11/2022 11:00**			**Duration: 60 min.**	
Exam. Type: Midterm	**MidT 1 ☒**	**MidT 2**	**MakeUp**	**Final**	**MUFinal**
Instructors: Prof. Dr. Hasan Hüseyin BALIK					

Q1 Consider a company whose operations are housed in two buildings on the same property: one building is headquarters, the other building contains network and computer services. The property is physically protected by a fence around the perimeter. The only entrance to the property is through a guarded front gate. The local networks are split between the Headquarters' LAN and the Network Services' LAN. Internet users connect to the Web server through a firewall. Dial-up users get access to a particular server on the Network Services' LAN. Develop an attack tree in which the root node represents disclosure of proprietary secrets. Include physical, social engineering, and technical attacks. The tree may contain both AND and OR nodes. Develop a tree that has at least 15 leaf nodes. **(20p)**

A1)



We present the tree in text form; call the company X:

Survivability Compromise: Disclosure of X proprietary secrets

- OR 1. Physically scavenge discarded items from X
  - OR 1. Inspect dumpster content on-site
  - 2. Inspect refuse after removal from site
- 2. Monitor emanations from X machines
  - AND 1. Survey physical perimeter to determine optimal monitoring position
  - 2. Acquire necessary monitoring equipment
  - 3. Setup monitoring site
  - 4. Monitor emanations from site
- 3. Recruit help of trusted X insider
  - OR 1. Plant spy as trusted insider
  - 2. Use existing trusted insider
- 4. Physically access X networks or machines
  - OR 1. Get physical, on-site access to Intranet
  - 2. Get physical access to external machines
- 5. Attack X intranet using its connections with Internet
  - OR 1. Monitor communications over Internet for leakage
  - 2. Get trusted process to send sensitive information to attacker over Internet
  - 3. Gain privileged access to Web server
- 6. Attack X intranet using its connections with public telephone network (PTN)
  - OR 1. Monitor communications over PTN for leakage of sensitive information
  - 2. Gain privileged access to machines on intranet connected via Internet

Q2) What are the principal ingredients of a public-key cryptosystem? **(20p)**

A2)

Plaintext: This is the readable message or data that is fed into the algorithm as input.

Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.

Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.

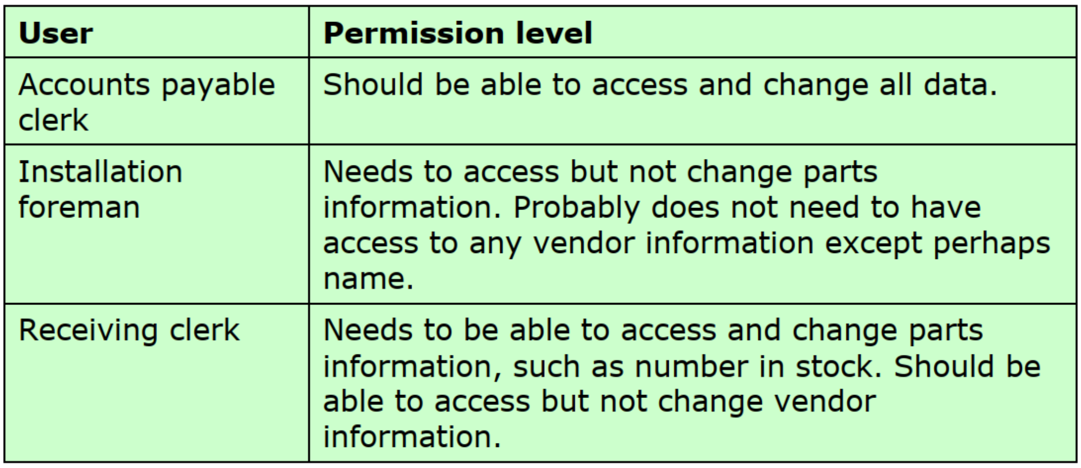
Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Q3) The inclusion of the salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Therefore, those two characters are known to the attacker and need not be guessed. Why is it asserted that the salt increases security? **(20p)**

A3)
Without the salt, the attacker can guess a password and encrypt it. If ANY of the users on a system use that password, then there will be a match. With the salt, the attacker must guess a password and then encrypt it once for each user, using the particular salt for each user.

Q4) Consider the parts department of a plumbing contractor. The department maintains an inventory database that includes parts information (part number, description, color, size, number in stock, etc.) and information on vendors from whom parts are obtained (name, address, pending purchase orders, closed purchase orders, etc.). In an RBAC system, suppose roles are defined for accounts payable clerk, an installation foreman, and a receiving clerk. For each role, indicate which items should be accessible for read-only and read-write access. **(20p)**

A4)



User	**Permission level**
Accounts payable clerk	Should be able to access and change all data.
Installation foreman	Needs to access but not change parts information. Probably does not need to have access to any vendor information except perhaps name.
Receiving clerk	Needs to be able to access and change parts information, such as number in stock. Should be able to access but not change vendor information.

Q5) Suppose you have a new smartphone and are excited about the range of apps available for it. You read about a really interesting new game that is available for your phone. You do a quick Web search for it and see that a version is available from one of the free marketplaces. When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to “Send SMS messages” and to “Access your address-book”. Should you be suspicious that a game wants these types of permissions? What threat might the app pose to your smartphone, should you grant these permissions and proceed to install it? What types of malware might it be? **(20p)**

A5)
If when you download and start to install some game app, you are asked to approve the access permissions “Send SMS messages” and to “Access your address-book”, you should indeed be suspicious that a game wants these types of permissions, as it would not seem needed just for a game. Rather it could be malware that wants to collect details of all your contacts, and either return them to the attacker via SMS, or allow the code to send SMS messages to your contacts, perhaps enticing them to also download and install this malware. Such code is a trojan horse, since it contains covert functions as well as the advertised functionality.