University	:	Menoufia	**Date**	:	17/1/2019
Faculty	:	Electronic Engineering	**Time**	:	3 Hours (10 AM: 1 PM)
Department	:	Computer Science and Engineering	**No. of Pages**	:	4
Year	:	Third	**Total Mark**	:	70 Marks
Course Name	:	Computer and Information Security	**Exam**	:	Final
Course Code	:	CSE 316	**Examiner**	:	Dr / Ezz Eldin Badawy

Answer All the Following Questions

Question One: Choose the correct answer. **[10 Marks]**

1. A program that an attacker can use to gain superintendent privileges on a target system

   A. Rootgain B. Worm C. Backdoor D. Rootkit

2. It is a security strategy in which numerous protection layers are provided.

   A. Defense in Depth B. Layered Approach C. Both A and B D. Offensive in Depth

3. Which type of hacker represents the highest risk to your organization network?

   A. Black Hat Hackers. B. Disgruntled Employees C. Cracker D. Script Kiddies

4. The act of pretending to be another user

   A. Spoofing B. Phishing C. Hijacking D. Both B and C

5. A technique used by attackers to exploit the human vulnerabilities within a network.

   A. Hyperjaking B. Social Engineering C. Social Hacking D. None of All.

6. Which penetration testing methodology, the tester doesn't know anything about the network topology.

   A. Grey Box Testing B. White Box Testing C. Black Box Hacking D. Blind Box Hacking

7. The collecting and analysis process of disconnected digital evidence related to network or system.

   A. Dead Forensics B. Live Forensics C. Postmortem Forensics D. Both A and C

8. When a computer tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer.

   A. Zero Day Attack B. One Day Attack C. Zero Day Exploit D. Both A and C

9. An attempt to compromise systems on the user's network with the full assistance and knowledge of the IT staff.

   A. Announced Pen Testing B. Unannounced Pen Testing C. Hybrid Pen Testing D. None of All.

10. The attacker tries to abolish all trail of the malicious activity in a hacking phase called

    A. Removing Evidence B. Hiding C.Both A and B D. Maintaining Access

Question Two: Select (T) or (F) for the following sentences. **[10 Marks]**

1. The scrambled text of 'hold' using Atbash Cipher, will be 'slew'. (T/F)
2. Data integrity is the assurance of altering in the information by unauthorized users. (T/F)
3. The single most crucial point of any hacker laboratory is the isolation of the network. (T/F)
4. Confidentiality is the only security service that traditional cryptographic system provides. (T/F)
5. Watermarking is the process of embedding information into a signal such as audio, video or pictures in a way that is easy to remove. (T/F)
6. Cryptanalysis is the art and science of making a cryptosystem that is capable of providing information security. (T/F)
7. Vulnerability scanners can identify weakness and automatically fix and patch the vulnerabilities without user intervention. (T/F)
8. The process of recording what the user accessed, the amount of time the resource is accessed, and any changes made, is called accounting. (T/F)
9. An active attack of cryptosystem is often seen as stealing information. (T/F)
10. Penetration testing is a destructive process. (T/F)

Question Three: Complete the following sentences. **[10 Marks]**

1. .....enables an attacker to install a rogue hypervisor that can take control of the underlying server resources.
2. ..... is the act of convincing a person to reveal private information.
3. The encrypted text of **'DEFCON FOUR'** using simple shift vigenere cipher, will be '.....', where key length (**5 13 2 7**).
4. ..... is a vulnerability that enables an attacker to copy or move a VM in an unauthorized manner.
5. In the cloud computing, cybercrimes can be divided into ..... and .....
6. ..... attack is an attempt to prevent legitimate users from accessing a resource or service.
7. Modern cryptographic systems can be classified into ..... and ..... ciphers.
8. In ....., everything is a file parsed by the host operating system, including the hard disk and the memory.
9. ABCD's of Internet of Things (IoT) refers to .....
10. Identifying and analyzing information security incidents and the related digital evidence is called .....

Question Four: Answer all the following questions. **[20 Marks]**

1. Explain briefly with drawing how dose multi-factor authentication system work with giving an example.
2. Explain the idea of hill cipher through encrypting this plaintext '**ACT**' where key= **GYBNQKURP** and then decrypt the ciphertext to the original text.
3. Explain briefly with diagram the function of carabank malware.
4. Explain with drawing how to establish an ethical hacking sandboxing with describing the basic phases for performing a penetration testing of User X's device in Industrial Network by a Pen Tester as shown in Figure 1.

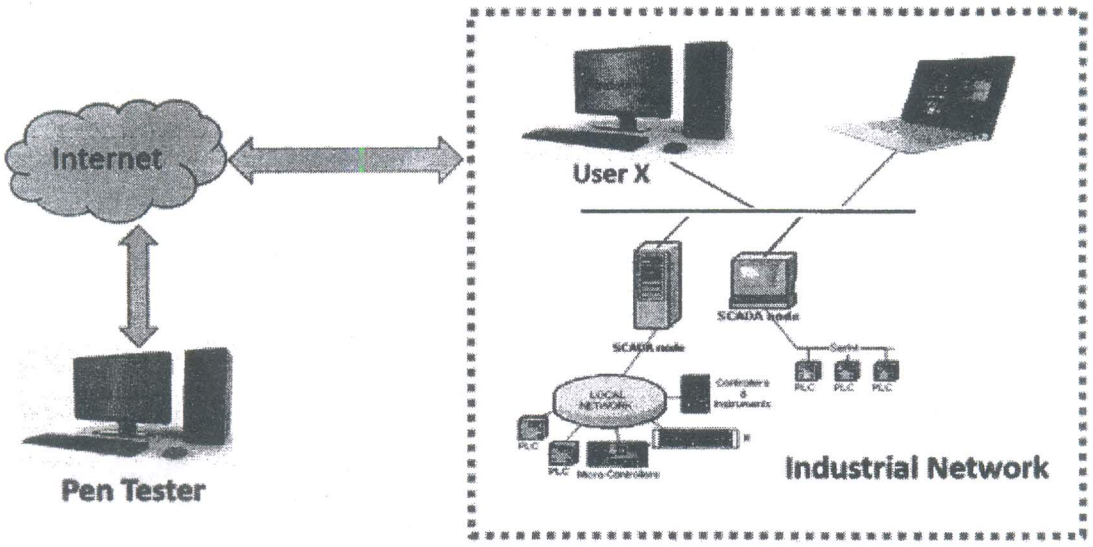

Figure 1. Pen Testing of Industrial Network.

5. What is a virtual machine monitor and clarify its categories.
6. Define credit card skimming and explain briefly with diagrams how does ATM card skimming work then clarify your recommended comprehensive solution for ATM card skimming problem?
7. Suppose you a cloud investigator and a cloud hacking scenario happed as follows: "User_1 is a cloud user who runs a Virtual Machine (VM) in a cloud. User_2 is a malicious user and rented also another VM in the cloud to access cloud infrastructure. The User_2 decided to use User_1's VM to launch several types of attacks to against existing VMs which running in the cloud to steal their data. One of the attacked VMs stores significant data which are stolen by the attacker (i.e. User_2)". Draw this cloud hacking scenario, and explain the investigation process of this cloud hacking to know who is responsible for the hacking.

Question Five: Answer all the following questions. **[20 Marks]**

1. Define cloud forensics and describe its three dimensions and lastly explain the dissimilarity between traditional computer forensic and cloud forensics.

2. Explain briefly a cryptosystem block diagram and clarify with diagrams the difference between symmetric and asymmetric cryptography.
3. Describe with drawing an IoT hacking scenario of Doctor Alex who has a mobile application to manage medical devices connecting with patients in a hospital besides his smart home devices. Then, suggest a particular security solution for protecting the IoT system from such kind of hacking.
4. Explain with drawing how does digital watermarking system work for hiding an image called Flower into another image called Secrets, along with describing the classifications of digital watermarking and finally outline the requirements to develop an efficient digital watermarking scheme.
5. Show step by step how to encrypt this message '**WAR LOST**' using Affine Cipher, where key=13 and m=7.
6. Explain with sketch the process of attacking industrial control systems via stuxnet worm.
7. Define: Postmortem Analysis, Digital Evidence, Static Analysis, Sleuth Kit and Write Blocker. Explain with drawing a digital forensics laboratory structure and mention the factors to consider while building any digital forensics laboratory.

With My Best Wishes