Air University

Mid-term Examination, (Fall 22)

Subject and code: IT170	**Total Points: 100**
Class: BSIT II (A, B)	**Time Allowed: 2 hours**
Instructor(s): Sibgha Tahir	**Date: 03-04- 2023**
Weightage of the Paper: 25%	**Time: 11:30 to 01: 30**

Special Instructions: The exam is closed book. Mobile/electronic devices are not permitted or should be given to the invigilator before starting paper. Attempt all questions.

Incharge Signature:

Question 1	**CLO1**	**C1: Remember**	**Marks: 20**

Q.1

1a. List the Four types of user characteristics that an authentication system can use to established the identity of a user, illustration each of them with an example. **[10]**

1b. How can organization ensure the integrity of its data in the face of cyber threats or other security risks? **[10]**

Question 2	**CLO4**	**C4: Analyzing**	**Marks: 25**

2a. **Analyze** the possible Assets, Vulnerability, attacks and threats in the following scenario.

1. The most popular of the tax reporting software platforms China requires foreign companies to download to operate in the country was discovered to contain a backdoor that could allow malicious actors to conduct network reconnaissance or attempt to take remote control of company systems.
2. Nine human rights activists in India were targeted as part of a coordinated spyware campaign that attempted to use malware to log their keystrokes, record audio, and steal credentials.
3. In the midst of escalating tensions between China and India over a border dispute in the Galwan Valley, Indian government agencies and banks reported being targeted by DDoS attacks reportedly originating in China.
4. Suspected Iranian hackers compromised the IT systems of at least three telecom companies in Pakistan, and used their access to monitor targets in the country.

Question 3	**CLO2**	**C2: Understanding**	**Marks: 30**

3a. How can VPNs be used to secure remote access to corporate networks, and what are the challenges involved in deploying and managing them? **[10]**
3b. Summarize the ITU-T X.805 security architecture, and how are they applied to end-to-end network secure communications systems through diagram**?** **[10]**
3c. We know that IPS is dependent on IDS to understand the attack. How does IDS identify malicious traffic? Explain the detection mechanism. **[10]**

Question 4	**CLO3**	**C3: Apply**	**Marks: 25**

4. Explain the Performed IOT attack in given scenario and how it could have been prevented given their arguments.

1. A smart home security system is compromised by an attacker, who gains access to the system's cameras and microphones. Describe the potential risks and consequences of this type of attack, and explain how it could have been prevented.
2. An industrial control system for a factory is connected to the internet, and an attacker gains access to it through a vulnerable device on the network. Describe the types of damage that could be caused by an attacker who gains control of the system, and explain how the system's security could have been improved.
3. A fleet of delivery drones is hacked by a group of cybercriminals, who use them to steal packages and cause chaos. Describe the potential risks and consequences of this type of attack, and explain how the drones could have been secured against hacking attempts.
4. A smart city infrastructure, including traffic lights and emergency services, is targeted by a attack. Describe the potential risks and consequences of this type of attack, and explain how the city's infrastructure could have been secured against this attack.
5. A healthcare provider's IoT devices are compromised by an attacker, who gains access to sensitive patient information. Describe the potential risks and consequences of this type of attack, and explain how the provider's IoT devices could have been secured to protect patient privacy.

Question 5 [CLO 1] [PLO 8] [Marks: 10]

Provide an argument why Biometric authentication system is one of the best way for authentication. Also provide key properties for biometric authentication and prove that, why **iris scan** is better authentication then fingerprint.

Question 6 [CLO 1] [PLO 8] [Marks: 15]

Explain the following IOT Threats:

1. Rolling Code Attack
2. BlueBorne Attack
3. Sybil Attack
4. Replay Attack
5. Forged Malicious Device

Question 7 [CLO 1] [PLO 8] [Marks: 15]

We know that IPS is dependent on IDS to understand the attack. How does IDS identify malicious traffic? Explain the detection mechanism.

***** Good Luck *****