EX.NO: 2 **SECURITY PRINCIPLES** ROLL NO : 231901035
DATE : 12.02.2025 NAME: NITHEESH K
K

Aim:

To understand the **CIA triad, security models, Defense-in-Depth, Zero Trust, and threat vs. risk** in cybersecurity.

Procedure:

1. **Learn the CIA Triad**
   Study the core principles of cybersecurity: Confidentiality, Integrity, and Availability.

2. **Understand DAD Threats**
   Explore how Disclosure, Alteration, and Destruction impact security and data protection.

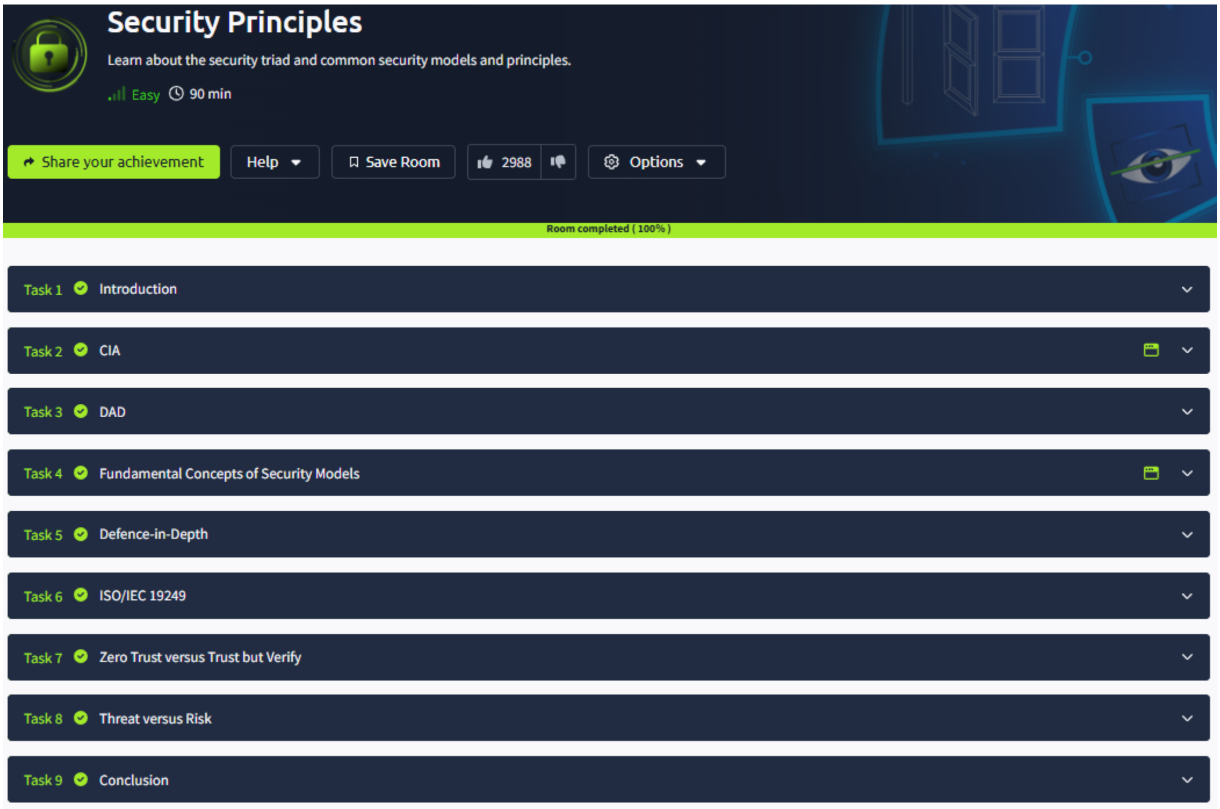
3. **Explore Security Models**
   Understand security models such as Bell-LaPadula, Biba, and Clark-Wilson, and their role in defining access control and integrity.

4. **Apply Defense-in-Depth**
   Learn how to implement multiple layers of security to protect systems and data at various levels.

5. **Study ISO/IEC 19249 Security Framework**
   Review the international standard that defines security design principles for IT systems.

6. **Compare Zero Trust vs. Trust but Verify**
   Analyze the Zero Trust model which assumes no inherent trust, versus the traditional "Trust but Verify" approach.

7. **Differentiate Threats from Risks**
   Understand the difference between threats (potential harm) and risks (likelihood and impact of harm).



Security Principles

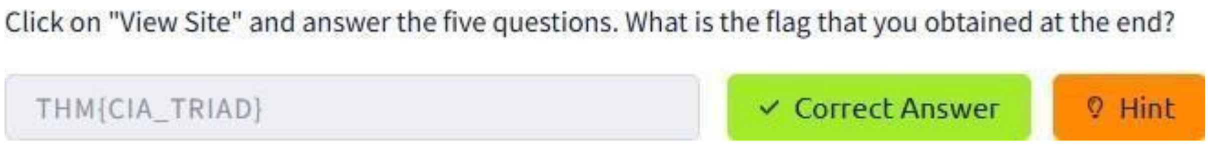
Learn about the security triad and common security models and principles.

Easy 90 min

Room completed (100%)

- Task 1 ✓ Introduction
- Task 2 ✓ CIA
- Task 3 ✓ DAD
- Task 4 ✓ Fundamental Concepts of Security Models
- Task 5 ✓ Defence-in-Depth
- Task 6 ✓ ISO/IEC 19249
- Task 7 ✓ Zero Trust versus Trust but Verify
- Task 8 ✓ Threat versus Risk
- Task 9 ✓ Conclusion

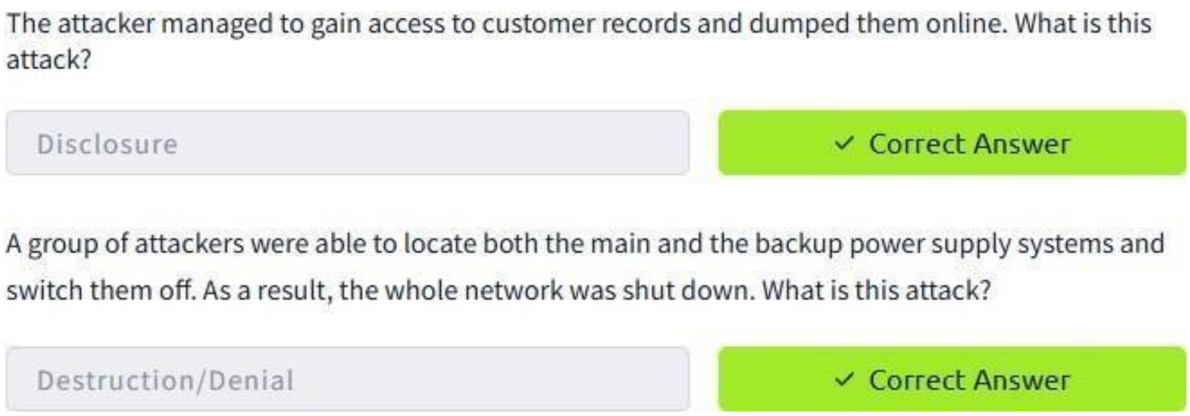
TASK 2 : CIA:



Click on "View Site" and answer the five questions. What is the flag that you obtained at the end?

THM{CIA_TRIAD}

TASK 3 : DAD:



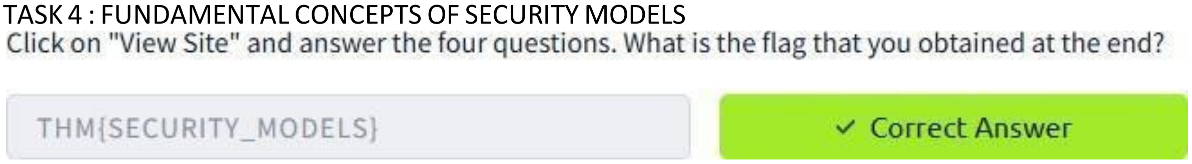
The attacker managed to gain access to customer records and dumped them online. What is this attack?

Disclosure

A group of attackers were able to locate both the main and the backup power supply systems and switch them off. As a result, the whole network was shut down. What is this attack?

Destruction/Denial

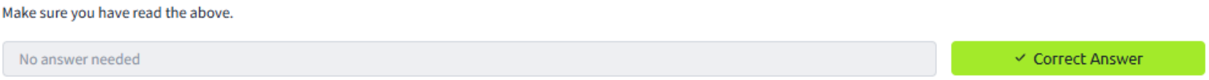
TASK 4 : FUNDAMENTAL CONCEPTS OF SECURITY MODELS



Click on "View Site" and answer the four questions. What is the flag that you obtained at the end?

THM{SECURITY_MODELS}

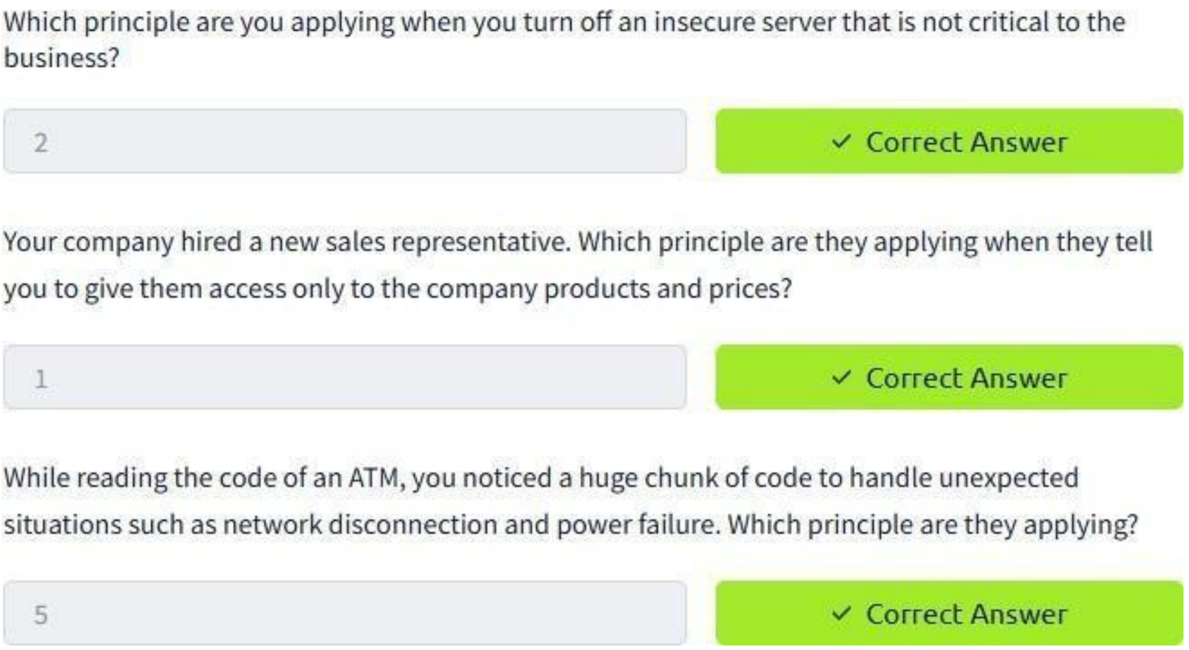
TASK 5 : DEFENCE-IN-DEPTH



Make sure you have read the above.

No answer needed

TASK 6 : ISO/IEC 19249



Which principle are you applying when you turn off an insecure server that is not critical to the business?

2

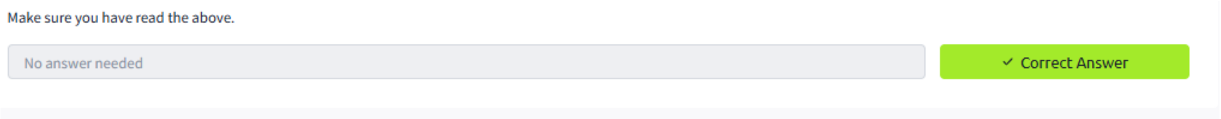
Your company hired a new sales representative. Which principle are they applying when they tell you to give them access only to the company products and prices?

1

While reading the code of an ATM, you noticed a huge chunk of code to handle unexpected situations such as network disconnection and power failure. Which principle are they applying?

5

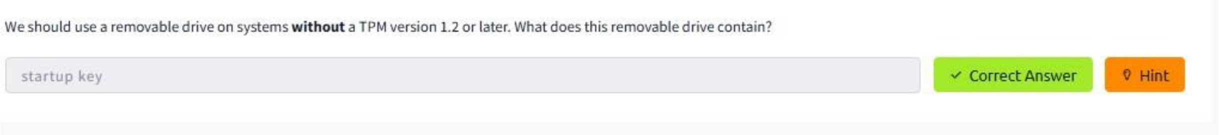
TASK 7 : ZERO TRUST VERSUS TRUST BUT VERIFY



Make sure you have read the above.

No answer needed

TASK 8 : THREAT VERSUS RISK



We should use a removable drive on systems **without** a TPM version 1.2 or later. What does this removable drive contain?

startup key

Result:

TryHackMe platform **Security Principles** tasks have been successfully completed.