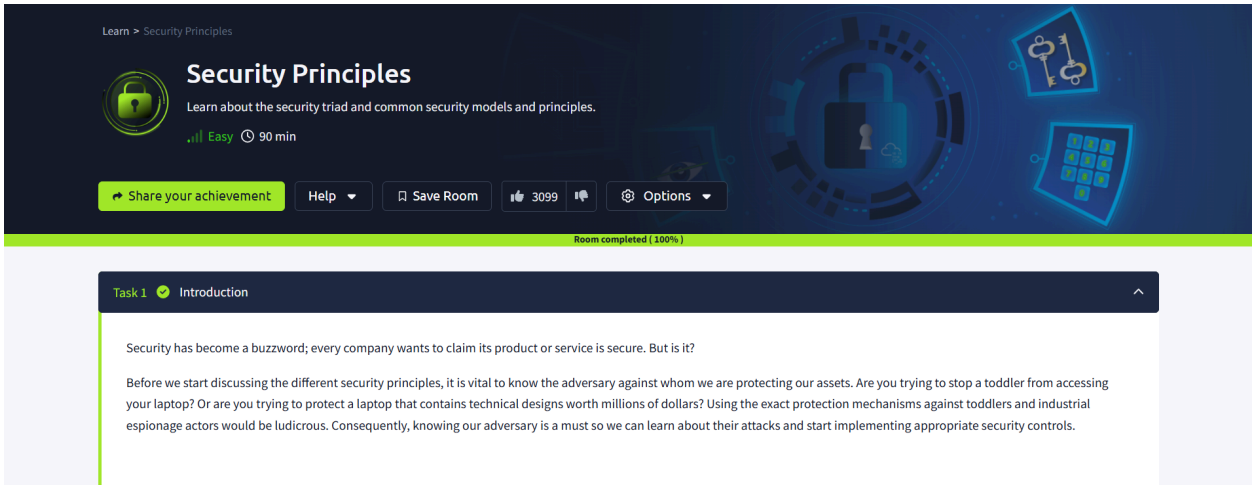
EXERCISE 2
SECURITY PRINCIPLES

AIM:

To understand the Security Triad (Confidentiality, Integrity, Availability) and explore common security models and principles that help in designing and maintaining secure systems



Protecting confidentiality and integrity to an extreme can restrict availability, and increasing availability to an extreme can result in losing confidentiality and integrity. Good security principles implementation requires a balance between the three.

Answer the questions below

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

Disclosure ✓ Correct Answer

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 ✓ Correct Answer

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

Answer the questions below

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

THM{SECURITY_MODELS} ✓ Correct Answer

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

Answer the questions below

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

2 ✓ Correct Answer

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 ✓ Correct Answer

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 ✓ Correct Answer

Task 7 ✓ Zero Trust versus Trust but Verify

Task 8 ✓ Threat versus Risk

RESULT:

Successfully gained knowledge of the Security Triad, various security models (such as Bell-LaPadula, Biba, and Clark-Wilson), and fundamental security principles to enhance system protection and risk management.