**CONFIABILIDADE E SEGURANÇA CIBERNÉTICA**
(DACYS)
PL05
*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**), Nuno Peralta* (**NSP**)
{@isep.ipp.pt}

# Exercise 1: Wireshark Intro

One of the main security concerns while building infrastructure is the concept of secure communications.
This concept defines that communications if being intercepted cannot be easily eavesdropped and will keep its contents secure.
Therefore, it is paramount to analyse all communication protocols to ensure that no leakage is done. Download the files from Moodle and try to answer the following questions.

1. Start a capture from your virtual machine, can you detect vulnerable protocols?
2. Identify the flows from your machine, what conversations do you see?
3. From the capture, what protocols exist?
4. Can you gather sensitive information from the protocols?
5. From a Security Engineer perspective, what would be your suggestions to fix these protocols and apply security communications?
6. How can the concept of zero trust align with this?

# Exercise 2: Decrypt traffic

Often we need to intercept traffic, either during a malware investigation or troubleshooting erroneous connections. Therefore, one should be able to decrypt traffic that is passing on the network. Take the second capture from the Moodle and answer the following questions:

1. What are the intervenients?
2. How do you decrypt the traffic?
3. How could you secure even further the communication, considering Perfect Forwarding Secrecy?

# Exercise 3: Malware investigations

Packet Capturing is essential to understand how the malware is replicating or what it is doing. Next is a capture of malicious activity:

1. What is the exploit being performed?
2. What does the attacker do?
3. Considering an IDS/IPS solution how would you detect packets similar to these on that system?