CSP004_C_E: Network Protection for Energy Control Systems
CyberSecPro Training Module
Compulsory assignment

Trainers:

- Cristina Alcaraz, University of Malaga, Spain
- Abdelkader Shaaban, AIT, Austrian

Practicalities for the activities

- The proposed activities are individual in nature
- The deadline for the submission is established in the DCM platform
- It is compulsory to provide reports in PDF format with concise, clear, and original contents
- All the reports should include the name and surname of each person
- All the materials used for the reports should properly be referenced, making use of a specific section for this ("References")

Assignments: Cyber Defense with the GNS3 Network Simulator

Objective: This exercise aims to demonstrate your ability to conduct cyber-attacks using multiple penetration testing tools within a virtual and isolated environment. This will help you gain knowledge in building mitigation and prevention strategies to address such actions and build a secure network considering security issues.

Setup:

- **Network Environment:** Create a virtual network using GNS3 consisting of multiple virtuals machines, including at least one attacker machine, gateway, and victim machines.

Tools and Software:

- **Attack Tools:** Wireshark, hping3, Scapy, arpspoof, Bettercap**.**
- **Defense Tools:** SURICATA, SIEM solution, VPN software, Arpwatch, or XArp for ARP spoofing detection**.**

Tasks:

- **Attack Scenario:** Define your network scenario to simulate an attacker targeting the victim machine(s). The knowledge gained within the module will support you in building up this scenario. Use the above tools to simulate cyber-attacks against the target machines (only within the virtual network developed in GNS3) and show how these tools can be utilized for these attacks. You may

extend your previously conducted practical tasks into this task to leverage how different cyber-attack actions and tools can be conducted in your network scenario.

- **Detection and Analysis:** Perform automated detection of ARP spoofing using Arpwatch, XArp, or any similar tools to detect ARP spoofing and alert on unusual ARP traffic. Use SURICATA to detect signs of attacks; you may use any of the existing rules or try to create customized ones. A VPN solution to mitigate MITM risks by encrypting traffic between the victims and the gateway.

Reporting: Describe the attack scenario that you have created for your task. Document each step taken during the attack scenario, including tools used, the idea behind each attack, and the expected outcome. In the defense phase, report on each detection and prevention tool's effectiveness. Conclude with your reflections on the overall security of the network and what the security recommendations are for improving the defenses based on the exercise outcomes.

The purpose of this task is to demonstrate your ability to mitigate and prevent cyber risks due to cyber-attacks. The tools used in this exercise can help you identify various cyber risks through simulated cyber-attack activities (i.e. inside the GNS3 simulator and within the home LAN) and gain the knowledge needed to address existing security weaknesses to avoid or mitigate related cyber risks. Therefore, all these activities are solely intended for educational purposes ONLY and not for any malicious or unauthorized activities.