

Assignment 3 (v.1): hardening of the ACME network

In this assignment, your team has to implement security measures to protect the ACME network from possible threats, considering all the services already deployed in the network. The security measures should be defined in a protection plan that includes any configuration hardening of the systems and any operating configuration of the hosts in the network (proxies, IDS/IPS, SIEM, vulnerability scanners, link-local monitors, and alike).

Protection plan

The idea is to develop a protection plan that includes the security measures to be implemented and the justification for each measure. While implementing the protection plan, you should note the steps taken and any challenges encountered, together with any evaluation of the effectiveness of the implemented security measures.

Scheme of your hand-in

Your team has to prepare and upload in Classroom a document that describing the protection plan implemented, following the structure above. The document should be named `ACME_XX_a3_report.pdf`.

You must upload a .zip file named `ACME_XX_a3.zip`, including the PDF file of your report and any configuration files you think are relevant to your solution. The ZIP file is the only file your group has to hand-in in Classroom (only one of the members).

The document should be clear and concise (a few pages, please) and have at least the following pieces of information:

1. Group number with student names and ID numbers (matricola)
2. Brainstorming (options considered for each vulnerability and reasoning behind the choices)
3. Protection plan definition
4. Protection plan implementation
5. Protection plan evaluation
6. Final remarks.