ITERATION 3

Security monitoring

Operation Mode

- Individual work
- 1,5 days on-site

Objectives

In this module, we are going to see how we can use monitoring tools in the security context.

Competencies

- Understand the supervision principles.

1.1 — Back to Zabbix

3h — On-site

In this module we are going to use Zabbix again. This time we will benefit from a special edition of the software for demo purposes: Zabbix appliance.

We will use the Zabbix appliance in a virtual machine and a Zabbix agent on your development machine. Install the Zabbix appliance in a virtual machine (for example QCOW2 in KVM) and the agent on your development machine. Make sure they communicate correctly.

RESOURCES

- Your notes from the module “Monitoring”, iteration 2
- https://www.zabbix.com/download_appliance

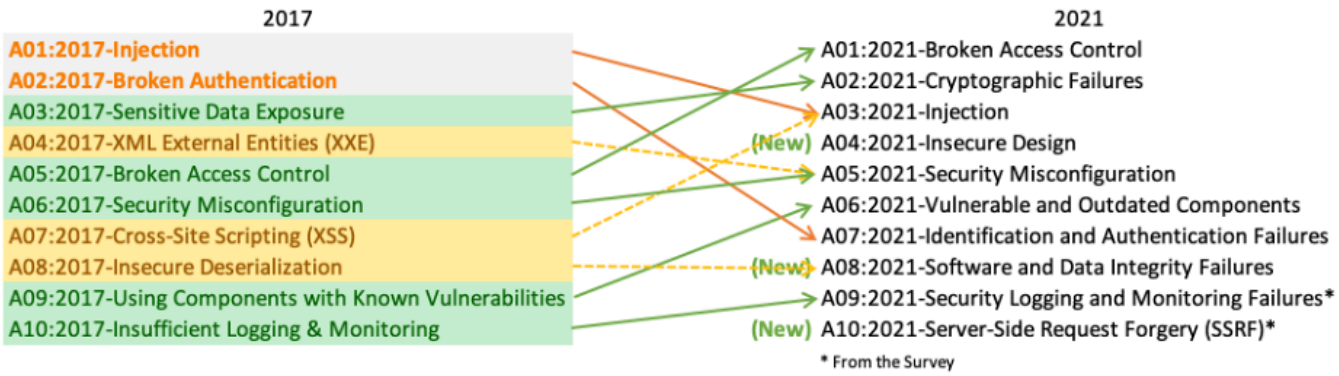
ASSOCIATED COMPETENCIES

- Understand the supervision principles.

1.2 — Zabbix as a security tool

7h — On-site

When we examine the OWASP list (https://owasp.org/Top10/), we can notice that it might be possible to detect some types of issues with monitoring tools. Can you find out which ones?



A05 should be easy... But we can detect most of them.

Configure your Zabbix to notify (by a mean of your choice) on conditions that might mean a security problem:

- A new user added to the system
- A change in /etc/passwd or /etc/shadow
- A change in an important configuration file of your choice (in /etc/ or elsewhere)
- New open ports
- Failed connection attempts
- No more disk space
- ... your own idea ...

In the results form, show a proof of at least five of those (with a screenshot, a message received and so on).

RESOURCES

- https://blog.zabbix.com/security-related-monitoring-with-zabbix/8659/

ASSOCIATED COMPETENCES

- Connaissance des principes de la supervision

Deliveries

In this module, we obtain a functional Zabbix configuration that alerts on possible security issues.