Segurança de Sistemas e Informação

(SEGSI)
PL08

*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**)*
{@isep.ipp.pt}

Exercise 1: Deploying the environment

With the advent of new paradigms such as shift-left [1] and GitOps [2] a new attack surface emerges. Jenkins and all the components that comprise a complete CI/CD pipeline. In this exercise, we will deploy several services to enable us to understand what misconceptions and security mishaps might occur.

1. Go to the Github Repository [3] and follow the **Take the challenge** section.
2. Be sure to have at least 10GB of RAM available in your machine since several services will be running.
3. What kind of attacks [4] might be portrayed in such environments?
4. If this opens a new attack surface, why are companies moving to this paradigm? Compare the threats and the benefits and

Exercise 2: Attacking the environment

This environment consists of several challenges for you to learn and experiment tackle each one with the mindset of an attacker to leverage the CI/CD pipeline in your favor.

1. **Follow the White Rabbit** investigate the credential store of the Jenkins installation and retrieve the flag.
2. **Mad Hater**. Investigate what commands are being executed and how can you leverage them to gain access to the flag.
3. **Caterpillar** with ReadOnly access we have access to sensitive information. Investigate what information you have access to and can leverage to compromise the pipeline.
4. What are your considerations in trying to bring security to these types of accesses? What would you do to prevent such mistakes?

References

[1] S. Gunja, “Shift left vs shift right: A devops mystery solved,” Oct 2022. [Online]. Available: https://www.dynatrace.com/news/blog/what-is-shift-left-and-what-is-shift-right/

[2] GitLab, “What is gitops?” Mar 2023. [Online]. Available: https://about.gitlab.com/topics/gitops/

[3] Cider-Security-Research, “Cider-security-research/cicd-goat: A deliberately vulnerable ci/cd environment. learn ci/cd security through multiple challenges.” [Online]. Available: https://github.com/cider-security-research/cicd-goat#Linux--Mac

[4] “Owasp top 10 ci/cd security risks — owasp foundation.” [Online]. Available: https://owasp.org/www-project-top-10-ci-cd-security-risks/