Individual SNOWeek15

Date: Jan 2023
Version 1.0

Class: CB01

Student number: 4961854

Student name: Heiko Morales

The Rise of the Supply Chain Attack

What was the presentation about?

The presentation talks about the various attacks that exist when using public repositories on the net. That is to say, how hackers infect these repositories that the user later downloads and in this way manage to execute malicious code remotely (Attack, s.f.).

What did you learn?

There are several things I have learnt but the most important ones are how to validate public repositories, the techniques hackers use for different types of attacks and the need to use official repositories from leading brands.

How could the Case study and/or Multidisciplinary project be improved based on the topic you just learned?

In our case we use many libraries to develop the api, the web page and the application as such. Therefore, the previous knowledge could be applied perfectly well.

would you recommend this topic to be explained/included in the S3 Infra course?

Yes, because in this course we learn to create infrastructure based on code and things we use are from public repositories such as docker containers, kubernetes or even code to implement different functions.

Security where to start and what to measure

What was the presentation about?

Discusses the evolution of security development and operations that occur in a CI/CD pipeline and how to make them secure (alldevops, s.f.).

What did you learn?

There are several things I have learnt but the most important ones are learning the most common vulnerabilities in production, finding the sweet spot in speed, security and stability or the fact that social engineering is more and more responsible for cybersecurity attacks. It has also taught me different methods to make security simpler and more effective with the method of measuring the security of the network.

How could the Case study and/or Multidisciplinary project be improved based on the topic you just learned?

In our case we use to implement a pipeline would be perfect as there are several services which have been developed by us. Therefore a secure CI/CD system would be perfect for developing and deploying new versions of the application.

would you recommend this topic to be explained/included in the S3 Infra course?

Yes, because in this course we learn automated CI/CD processes and therefore we should learn how to create them in a safe way.

Managing the Credentials in a secure way

What was the presentation about?

discusses how to properly manage all company credentials from active directory credentials to database administration passwords (alldevops, s.f.).

What did you learn?

There are several things I have learnt but the most important ones are the types of attacks that can be encountered when trying to steal a credential. Another very important thing would be the solution to this problem that is given in different types such as applying SSL encryption or using access lists. Finally we learned several tools to manage dynamic credentials such as aiven.

How could the Case study and/or Multidisciplinary project be improved based on the topic you just learned?

In our case, we have several services that must have a credential and, in our case, even if we are only 3 people, we already have more than 15 credentials. That is why a correct use of the credentials would be vital. On the other hand, our project deals specifically with the problem that is presented in the presentation.

would you recommend this topic to be explained/included in the S3 Infra course?

Yes, the correct use of credentials is essential in all senses. This topic seems to me very important for anyone who has several passwords and taking into account the number of passwords we handle per day this should be an important topic.

API Security

What was the presentation about?

talks about api security and the different challenges you face when trying to secure this type of services.

What did you learn?

There are several things I have learnt but the most important ones are the different critical points of apis. It also talks about how cybercriminals attack apis. They use authentication methods, service abuse or even malicious requests. Finally, it teaches us how to solve the previous problems with firewalls, automated full lifecycle apis...

How could the Case study and/or Multidisciplinary project be improved based on the topic you just learned?

In our case, it is a very important help because we use an api created by ourselves. This api could be much more secure by applying the new concepts that I have learned in this presentation.

would you recommend this topic to be explained/included in the S3 Infra course?

Yes, but only if the students are encouraged to experiment with creating their own APIs, otherwise it would not be of much use, only as good practice.