SANDBOX

Definition

The sandbox environment is a separate virtual machine. In this environment, you can execute commands, run suspected unsafe applications that can affect system resources or local applications.

Intention

Sandboxes are designed to prevent threats from entering the network and are often used to test untested or untrusted code. Sandboxing keeps the code down to the test environment, so it doesn't infect or cause damage to the server or operating system.

How it works

Sandboxes work by keeping potentially malicious programs or unsafe code isolated from the rest of the organization's environment. This way it can be safely analyzed without affecting your operating system or host device. If a threat is detected, it can be removed proactively.

Advantage

Using a sandbox has a few benefits such as:

- No risk to your host devices or operating system.
- Evaluate potential malware for threats.
- Test software changes before they go online.
- Additional security strategies.
- Isolate threats in zero-day.

Disadvantage

Besides the great benefits, it also has the following disadvantages:

- Sandboxing is quite time and resource consuming. Running all your digital traffic through a sandbox system is impractical and expensive.
- Sandboxing can be bypassed. Today, more and more malicious threats are designed to bypass sandboxing

Implement

We can implement sandboxing in many ways like:

- Cloud-based deployment
- A special device on the spot
- By a software package
- A web browser extension

What type of Sandboxing

There are 4 types of Sandboxes:

- Developer Sandbox: is the simplest and smallest type used for development and testing in isolated environments.
- Developer Pro Sandbox: This category is larger than the Developer Sandbox used for development and quality assurance tasks as well as integration testing.
- Partial Copy Sandbox: Used mainly for testing. It will copy part of the log from the original environment.
- Full Sandbox: True to its name Full Sandbox includes everything. It is a complete copy of the application such as logs, metadata, etc. Only full sandboxes support performance testing, load testing and staging.

Why does sandboxing reduce SSTI?

As mentioned above, sandboxing is a test environment separate from the general system. So, when we embed the template engine in the sandbox, even if an attacker can take over the template-side, it can only work in the sandbox environment, it can hardly affect the external server-side directly.

References

- https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/
- https://cloudmybiz.com/tip-of-the-week-understanding-sandbox-types/
- https://en.wikipedia.org/wiki/Sandbox_(computer_security)