Yet Another Capture the Flag, but There's a Catch

Nicky Janse Dec 8 2021 • 5 min read

Capture the Flag (CTF) is a well-known phenomenon in the cybersecurity world. CTF is gamified exercise in which 'flags' are secretly hidden in purposefully-vulnerable applications, often web based. These CTF's are mostly meant for ethical hackers (so called red teamers) to improve their hacking skills. Only very few to none actually provide CTF's for the increasingly important defensive side of cyber security, the blue teamers. That's where our CTF, the RvB training game stands out.

Are you ready to be a blue teamer?

In the introduction I mentioned blue teaming, but what does this actually mean? That's exactly the question our trainees are asking themselves. The best way to answer this question is to participate in our CTF event, since the RvB training game is all about getting hands on experience as a blue teamer. In order to provide our trainees this experience we've setup our own security operations centre (SOC) along with vulnerable machines and automated attacks for the blue teamers to monitor.

The steps that the trainees have to go through consist of the following.

1. Scanning the security alerts within the Wazuh dashboard.
2. Reporting the incident by creating a ticking in TheHive.
3. Experimenting with- and recreating the attack in DWVA (Damn Vulnerable Web Application).

Let's make some noise!

The Wazuh dashboard will be filled with security alerts generated by (automated) attacks on the DVWA machines. Some of the alerts will be categorized dangerous enough to take action upon. It's up to the trainees to decide for which alerts that's the case. To make it a bit more difficult for the trainees the Wazuh dashboard will also be filled with some noise consisting of ordinary everyday internet traffic.

Incident response for the masses.

In TheHive the students have to read through existing incident reports belonging to the alerts from the Wazuh dashboard. Some of the incident reports will be incomplete and have to be expanded upon by the trainees. Different attack scenarios will guide the trainees through all of the necessary steps to create professional incident reports.

A little read teaming.

The RvB training game is not all about blue teaming. It is equally important for a blue teamer to be familiar with the attacking side. This way he has a better understanding of what he's defending against and with that, the defence itself will be improved. The RvB training game has several DWVA's available to provide our trainees this opportunity. The trainees will be able to mess around and recreate the attack in a secured environment.

Icing on the ~~cake~~train

The RvB training game has a total of six flags hidden in various ways with each flag split into four or five parts. These parts are spread through all of the steps the trainees have to take. Missing a step means missing part of a flag and thus, no progress towards the story. That's right, I said story.

The entire RvB training game revolves around a story where some unknown hacking group is attacking a railway company. By progressing through the story the trainees get to know some details about the hacking group. The more the trainees know, the closer they get to catching them. However, attacks the hacking the hacking group launches get more and more threatening.

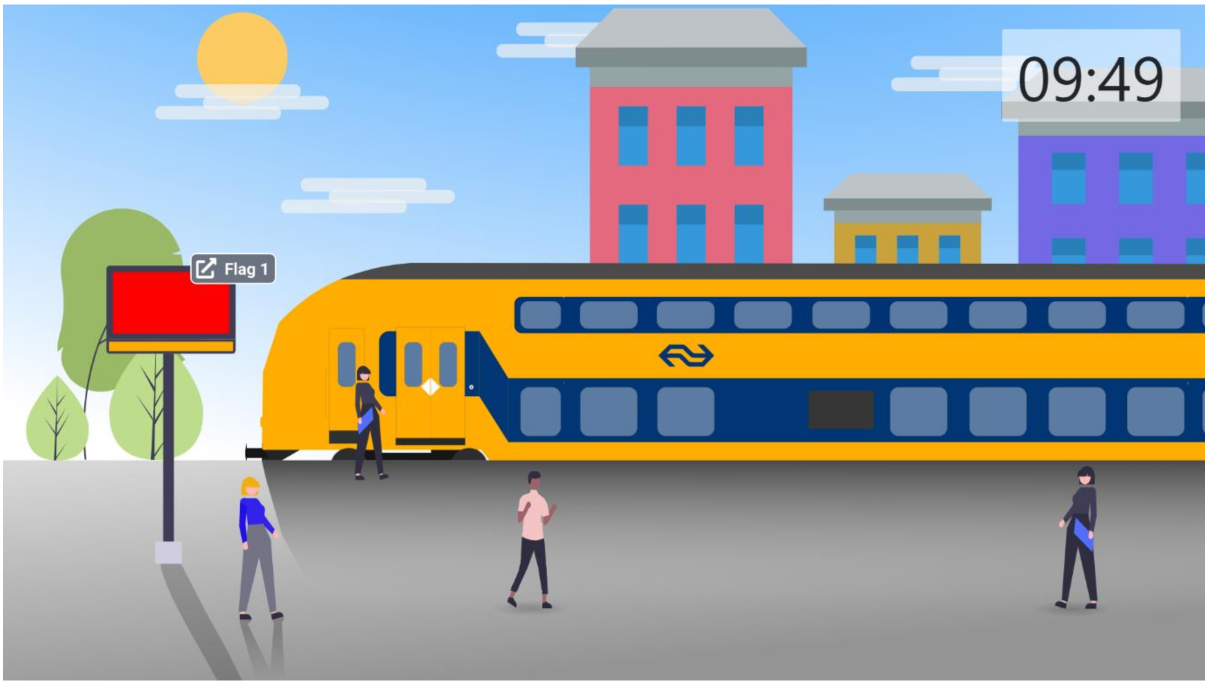

Image 1: First stage of the story

The story is supported by a set of nicely animated images. These images do not only tell the story but they also serve a practical use. Each of the images contain one or two buttons where the trainees can submit their flag belonging to that part of the story. On top of that it will show a timer as the story will be time based to increase the pressure and simulate a real world scenario.

Can the trainees prevent two trains from crashing or will the hacking group prevail and will the trains crash with many hundreds of casualties? Participate in the RvB training game event and be the difference.