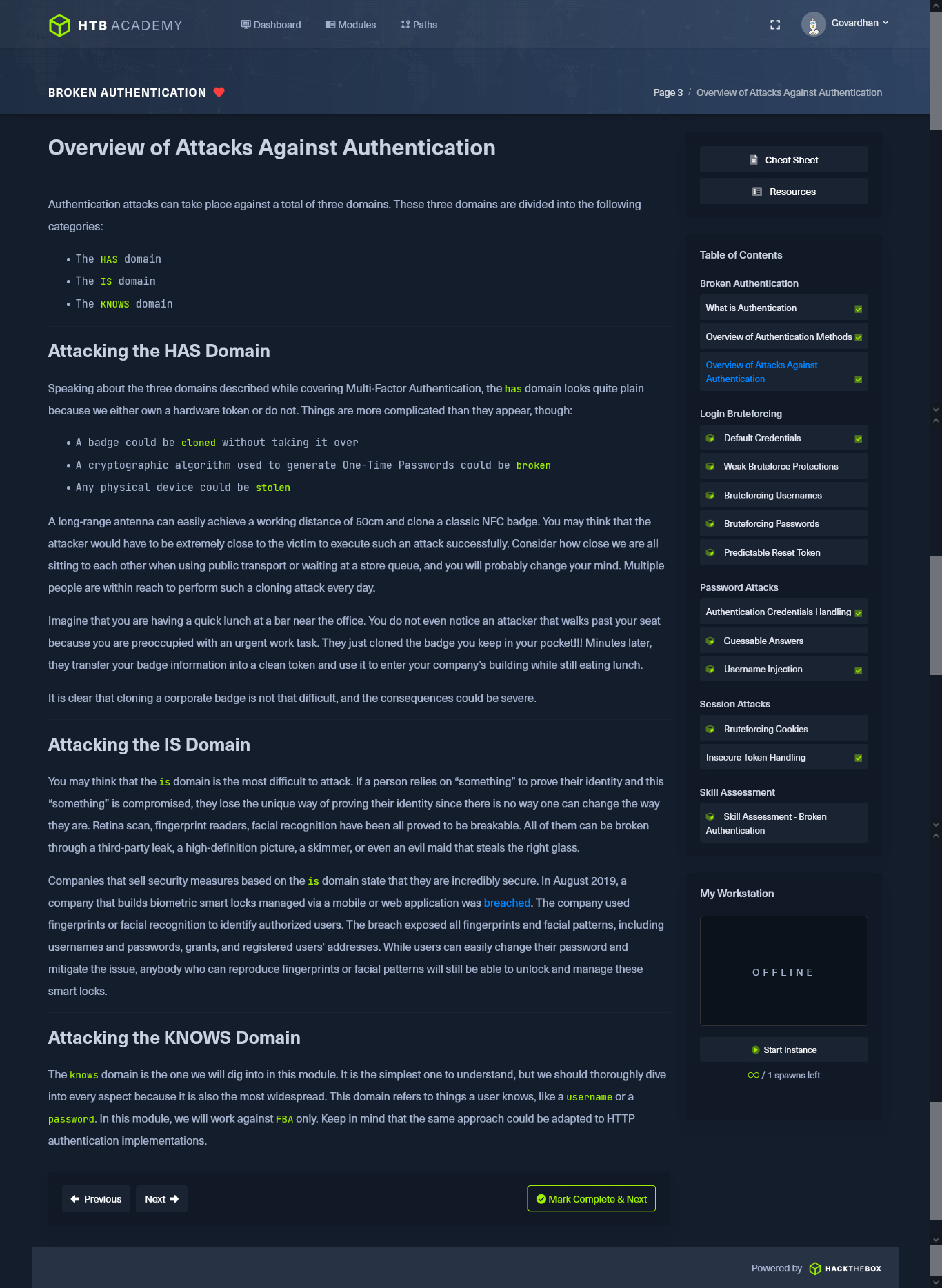

Overview of Attacks Against Authentication

Authentication attacks can take place against a total of three domains. These three domains are divided into the following categories:

- The `HAS` domain
- The `IS` domain
- The `KNOWS` domain

Attacking the HAS Domain

Speaking about the three domains described while covering Multi-Factor Authentication, the `has` domain looks quite plain because we either own a hardware token or do not. Things are more complicated than they appear, though:

- `A badge could be cloned without taking it over`
- `A cryptographic algorithm used to generate One-Time Passwords could be broken`
- `Any physical device could be stolen`

A long-range antenna can easily achieve a working distance of 50cm and clone a classic NFC badge. You may think that the attacker would have to be extremely close to the victim to execute such an attack successfully. Consider how close we are all sitting to each other when using public transport or waiting at a store queue, and you will probably change your mind. Multiple people are within reach to perform such a cloning attack every day.

Imagine that you are having a quick lunch at a bar near the office. You do not even notice an attacker that walks past your seat because you are preoccupied with an urgent work task. They just cloned the badge you keep in your pocket!!! Minutes later, they transfer your badge information into a clean token and use it to enter your company's building while still eating lunch.

It is clear that cloning a corporate badge is not that difficult, and the consequences could be severe.

Attacking the IS Domain

You may think that the `is` domain is the most difficult to attack. If a person relies on "something" to prove their identity and this "something" is compromised, they lose the unique way of proving their identity since there is no way one can change the way they are. Retina scan, fingerprint readers, facial recognition have been all proved to be breakable. All of them can be broken through a third-party leak, a high-definition picture, a skimmer, or even an evil maid that steals the right glass.

Companies that sell security measures based on the `is` domain state that they are incredibly secure. In August 2019, a company that builds biometric smart locks managed via a mobile or web application was breached. The company used fingerprints or facial recognition to identify authorized users. The breach exposed all fingerprints and facial patterns, including usernames and passwords, grants, and registered users' addresses. While users can easily change their password and mitigate the issue, anybody who can reproduce fingerprints or facial patterns will still be able to unlock and manage these smart locks.

Attacking the KNOWS Domain

The `knows` domain is the one we will dig into in this module. It is the simplest one to understand, but we should thoroughly dive into every aspect because it is also the most widespread. This domain refers to things a user knows, like a `username` or a `password`. In this module, we will work against `FBA` only. Keep in mind that the same approach could be adapted to HTTP authentication implementations.

← Previous   Next →   Mark Complete & Next

Cheat Sheet

Resources