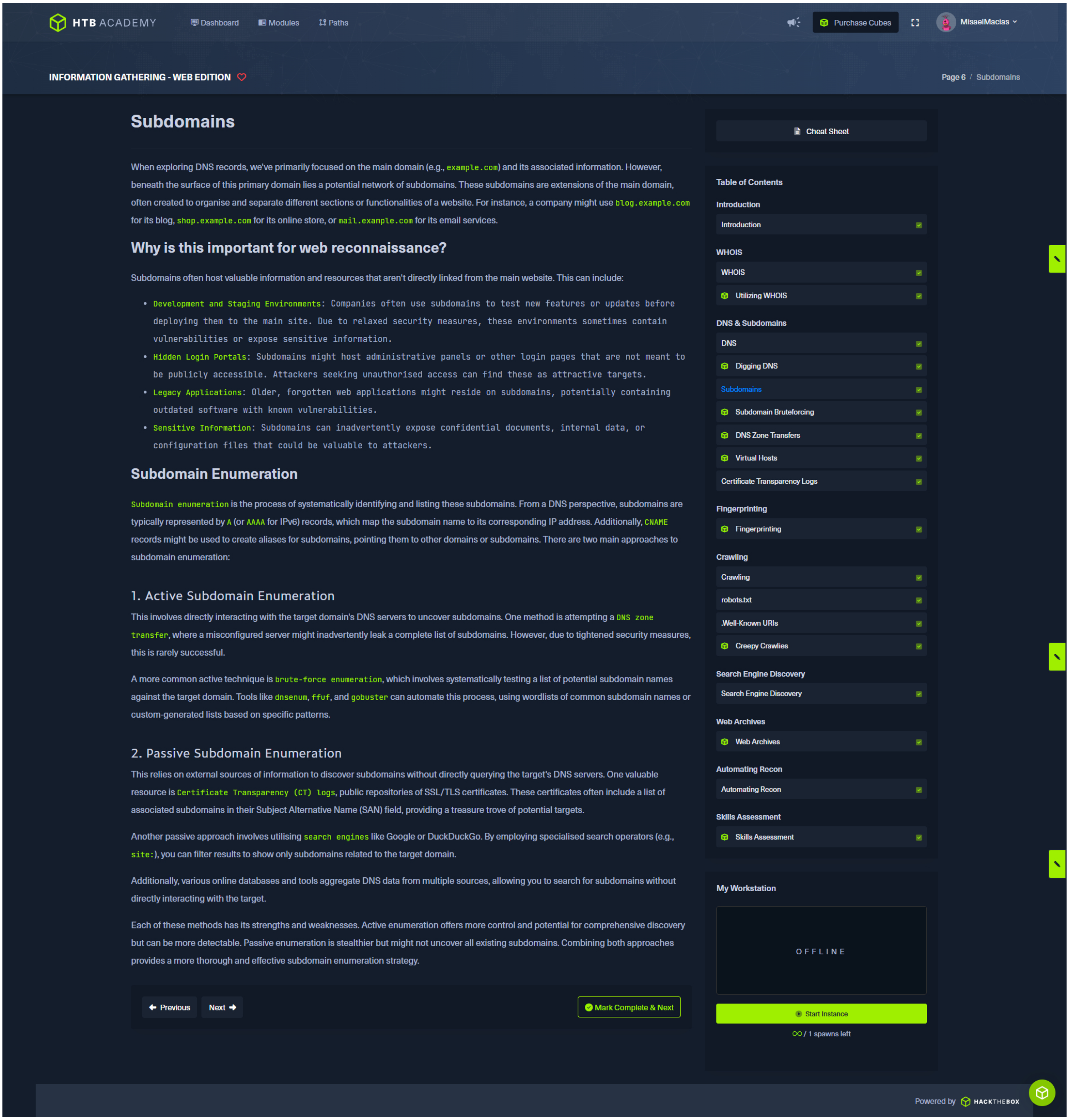

Subdomains

When exploring DNS records, we've primarily focused on the main domain (e.g., `example.com`) and its associated information. However, beneath the surface of this primary domain lies a potential network of subdomains. These subdomains are extensions of the main domain, often created to organise and separate different sections or functionalities of a website. For instance, a company might use `blog.example.com` for its blog, `shop.example.com` for its online store, or `mail.example.com` for its email services.

Why is this important for web reconnaissance?

Subdomains often host valuable information and resources that aren't directly linked from the main website. This can include:

- `Development and Staging Environments`: Companies often use subdomains to test new features or updates before deploying them to the main site. Due to relaxed security measures, these environments sometimes contain vulnerabilities or expose sensitive information.
- `Hidden Login Portals`: Subdomains might host administrative panels or other login pages that are not meant to be publicly accessible. Attackers seeking unauthorised access can find these as attractive targets.
- `Legacy Applications`: Older, forgotten web applications might reside on subdomains, potentially containing outdated software with known vulnerabilities.
- `Sensitive Information`: Subdomains can inadvertently expose confidential documents, internal data, or configuration files that could be valuable to attackers.

Subdomain Enumeration

`Subdomain enumeration` is the process of systematically identifying and listing these subdomains. From a DNS perspective, subdomains are typically represented by `A` (or `AAAA` for IPv6) records, which map the subdomain name to its corresponding IP address. Additionally, `CNAME` records might be used to create aliases for subdomains, pointing them to other domains or subdomains. There are two main approaches to subdomain enumeration:

1. Active Subdomain Enumeration

This involves directly interacting with the target domain's DNS servers to uncover subdomains. One method is attempting a `DNS zone transfer`, where a misconfigured server might inadvertently leak a complete list of subdomains. However, due to tightened security measures, this is rarely successful.

A more common active technique is `brute-force enumeration`, which involves systematically testing a list of potential subdomain names against the target domain. Tools like `dnsenum`, `ffuf`, and `gobuster` can automate this process, using wordlists of common subdomain names or custom-generated lists based on specific patterns.

2. Passive Subdomain Enumeration

This relies on external sources of information to discover subdomains without directly querying the target's DNS servers. One valuable resource is `Certificate Transparency (CT) logs`, public repositories of SSL/TLS certificates. These certificates often include a list of associated subdomains in their Subject Alternative Name (SAN) field, providing a treasure trove of potential targets.

Another passive approach involves utilising `search engines` like Google or DuckDuckGo. By employing specialised search operators (e.g., `site:`), you can filter results to show only subdomains related to the target domain.

Additionally, various online databases and tools aggregate DNS data from multiple sources, allowing you to search for subdomains without directly interacting with the target.

Each of these methods has its strengths and weaknesses. Active enumeration offers more control and potential for comprehensive discovery but can be more detectable. Passive enumeration is stealthier but might not uncover all existing subdomains. Combining both approaches provides a more thorough and effective subdomain enumeration strategy.

← Previous   Next →   Mark Complete & Next

Cheat Sheet

Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left