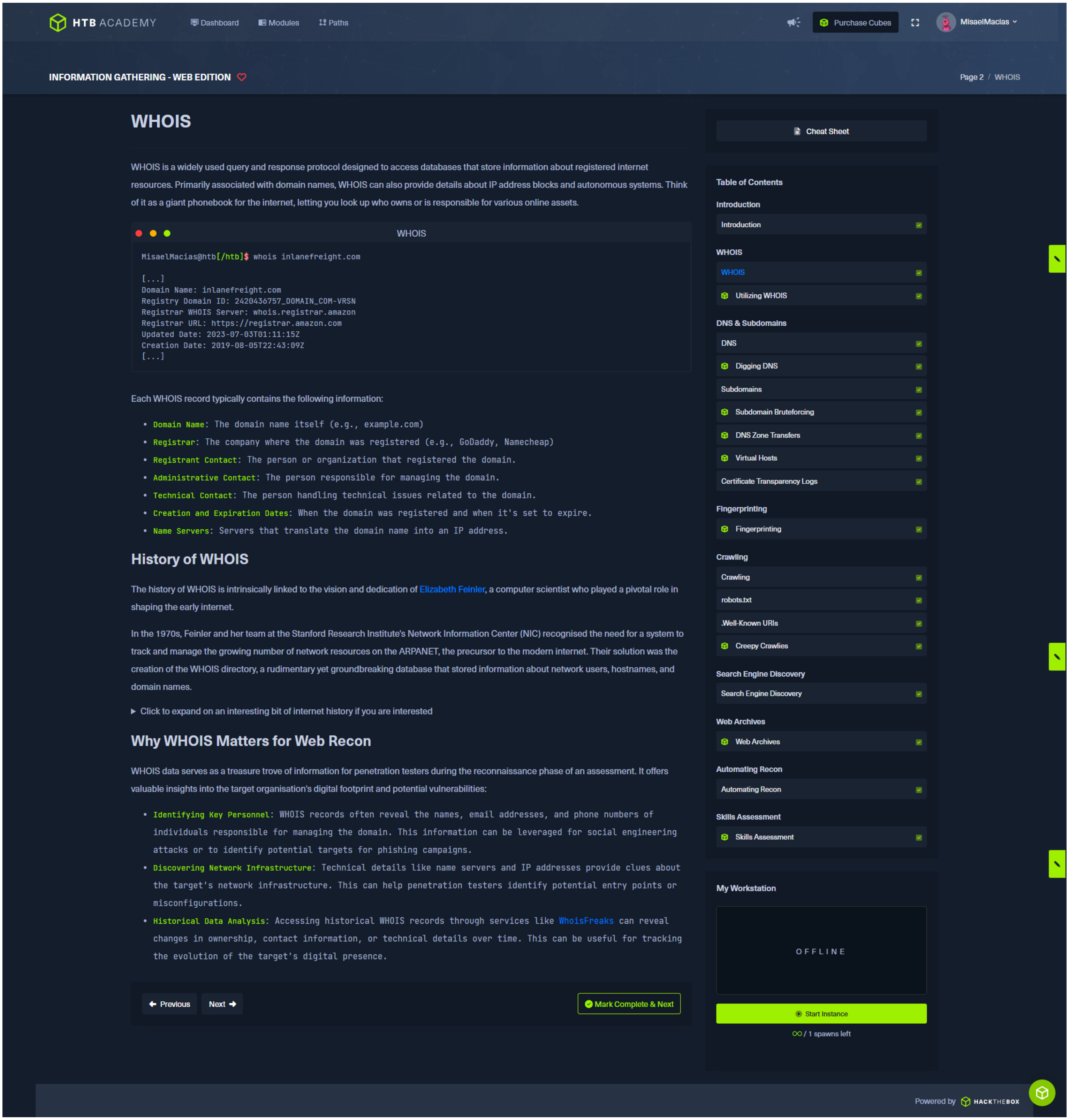

WHOIS

WHOIS is a widely used query and response protocol designed to access databases that store information about registered internet resources. Primarily associated with domain names, WHOIS can also provide details about IP address blocks and autonomous systems. Think of it as a giant phonebook for the internet, letting you look up who owns or is responsible for various online assets.

WHOIS

```
MisaelMacias@htb[/htb]$ whois inlanefreight.com

[...]
Domain Name: inlanefreight.com
Registry Domain ID: 2420436757_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon
Registrar URL: https://registrar.amazon.com
Updated Date: 2023-07-03T01:11:15Z
Creation Date: 2019-08-05T22:43:09Z
[...]
```

Each WHOIS record typically contains the following information:

- `Domain Name`: The domain name itself (e.g., example.com)
- `Registrar`: The company where the domain was registered (e.g., GoDaddy, Namecheap)
- `Registrant Contact`: The person or organization that registered the domain.
- `Administrative Contact`: The person responsible for managing the domain.
- `Technical Contact`: The person handling technical issues related to the domain.
- `Creation and Expiration Dates`: When the domain was registered and when it's set to expire.
- `Name Servers`: Servers that translate the domain name into an IP address.

History of WHOIS

The history of WHOIS is intrinsically linked to the vision and dedication of Elizabeth Feinler, a computer scientist who played a pivotal role in shaping the early internet.

In the 1970s, Feinler and her team at the Stanford Research Institute's Network Information Center (NIC) recognised the need for a system to track and manage the growing number of network resources on the ARPANET, the precursor to the modern internet. Their solution was the creation of the WHOIS directory, a rudimentary yet groundbreaking database that stored information about network users, hostnames, and domain names.

▶ Click to expand on an interesting bit of internet history if you are interested

Why WHOIS Matters for Web Recon

WHOIS data serves as a treasure trove of information for penetration testers during the reconnaissance phase of an assessment. It offers valuable insights into the target organisation's digital footprint and potential vulnerabilities:

- `Identifying Key Personnel`: WHOIS records often reveal the names, email addresses, and phone numbers of individuals responsible for managing the domain. This information can be leveraged for social engineering attacks or to identify potential targets for phishing campaigns.
- `Discovering Network Infrastructure`: Technical details like name servers and IP addresses provide clues about the target's network infrastructure. This can help penetration testers identify potential entry points or misconfigurations.
- `Historical Data Analysis`: Accessing historical WHOIS records through services like WhoisFreaks can reveal changes in ownership, contact information, or technical details over time. This can be useful for tracking the evolution of the target's digital presence.

← Previous Next → Mark Complete & Next

Cheat Sheet

Table of Contents

Introduction
Introduction ✓

WHOIS
WHOIS ✓
Utilizing WHOIS ✓

DNS & Subdomains
DNS ✓
Digging DNS ✓
Subdomains ✓
Subdomain Bruteforcing ✓
DNS Zone Transfers ✓
Virtual Hosts ✓
Certificate Transparency Logs ✓

Fingerprinting
Fingerprinting ✓

Crawling
Crawling ✓
robots.txt ✓
.Well-Known URIs ✓
Creepy Crawlies ✓

Search Engine Discovery
Search Engine Discovery ✓

Web Archives
Web Archives ✓

Automating Recon
Automating Recon ✓

Skills Assessment
Skills Assessment ✓

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left