Skills Assessment Report – Information Gathering

Author: Ernesto Ramos ”h4xthan”

June 30, 2025

Introduction

This report presents the solutions for five challenges from the Hack The Box Academy’s Competency Assessment on Web Reconnaissance. The tasks involve the use of tools like `whois`, `nmap`, `ffuf`, `curl`, and `ReconSpider`, with a focus on subdomain enumeration, directory fuzzing, and HTTP analysis.

1 Challenge 1 – WHOIS Information

Question: What is the IANA ID of the registrar for the domain `inlanefreight.com`?

Command Used:

```
whois inlanefreight.com | grep -i registrar
```

Answer: `468`

2 Challenge 2 – HTTP Server Software

Question: What HTTP server software is used by `inlanefreight.htb`?

Tools used:

- `whatweb inlanefreight.htb:51399`
- `nikto -h inlanefreight.htb:51399`
- `nmap -p51399 -sCV <IP>`
- `curl -I inlanefreight.htb:51399`
- `FinalRecon`

Answer: `nginx`

3 Challenge 3 – Hidden Admin API Key

Question: What is the API key found in a hidden admin directory?

- Subdomain enumeration led to `web1337.inlanefreight.htb:51399`
- Then `dev.web1337.inlanefreight.htb:51399` was found
- Directory fuzzing failed, so used FFUF on incrementing index pages

- Filtered by page sizes to find unusual response
- Finally, a `robots.txt` file revealed: `/admin_h1dd3n`
- Inside: `The admin panel is currently under maintenance, but the API is still accessible with the key e963d863ee0e82ba7080fbf558ca0d3f`

Answer: `e963d863ee0e82ba7080fbf558ca0d3f`

4 Challenge 4 – Email Discovery

Question: What is the discovered email address?

- Found within one of the numbered index pages: `Contact us at 1337testing@inlanefreight.htb`

Answer: `1337testing@inlanefreight.htb`

5 Challenge 5 – Commented API Key

Question: What is the API key mentioned in a comment on the site?

- Crawled the dev subdomain using ReconSpider
- Found HTML comment:

  <!-- Remember to change the API key to ba988b835be4aa97d068941dc852ff33 -->

Answer: `ba988b835be4aa97d068941dc852ff33`

Conclusion

This assessment tested a wide range of reconnaissance techniques. Despite moments of frustration, particularly with subdomain and hidden directory discovery, the tasks helped reinforce persistence, methodical analysis, and the value of multiple tools in enumeration workflows. Each step was an opportunity to apply real-world recon logic, as expected in professional penetration testing or bug bounty scenarios.