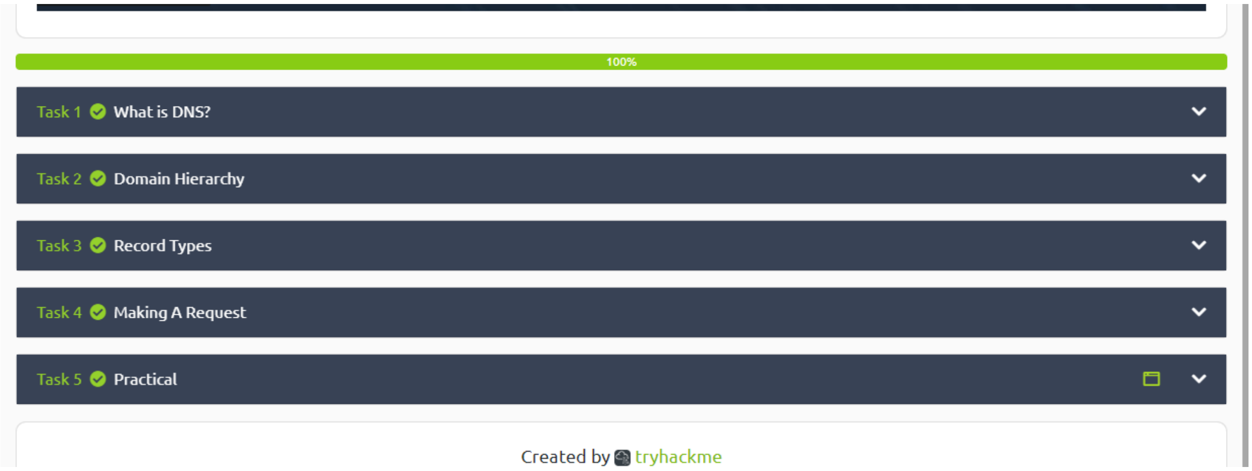
DNS In Detail

Covers the concepts of DNS and how searches work when finding servers and sites. First goes over the domain hierarchy covering TLD, SLD, and Subdomains. Afterwards it goes over DSN Record Types, What happens when we make a DNS request, and a practical where we use nslookup to find information like cname, and TXT.



100%

Task 1 ✓ What is DNS?

Task 2 ✓ Domain Hierarchy

Task 3 ✓ Record Types

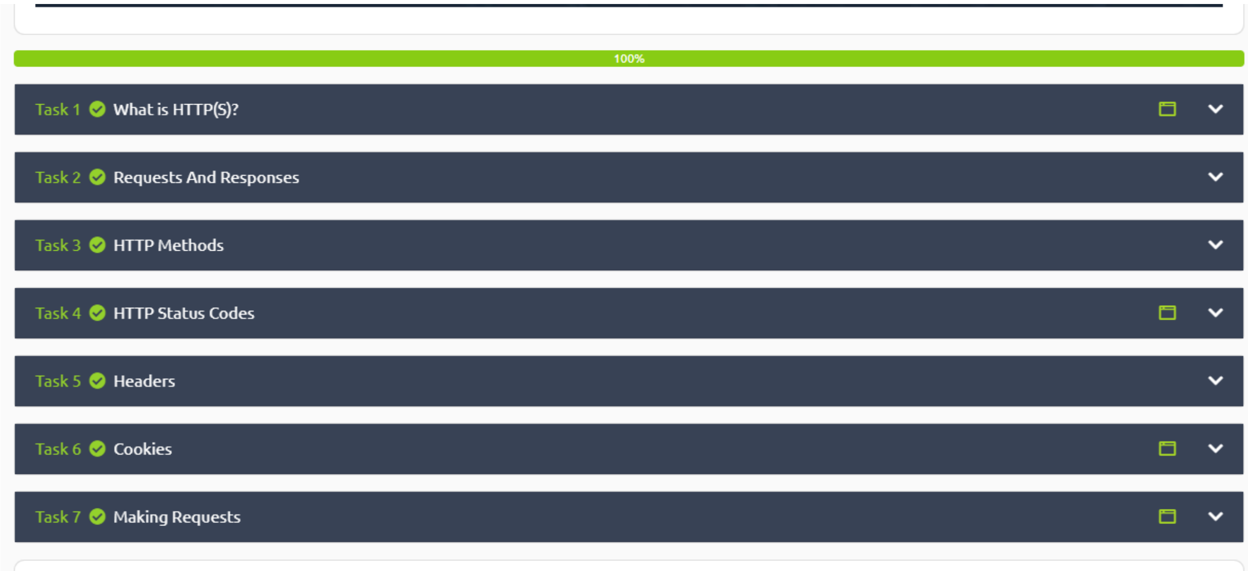
Task 4 ✓ Making A Request

Task 5 ✓ Practical

Created by tryhackme

HTTP In Detail

Covers the basic knowledge in how data is sent from web servers in the form of webpage data. It involves description of heavers, cookies, command line methods, status codes etc.



100%

Task 1 ✓ What is HTTP(S)?

Task 2 ✓ Requests And Responses

Task 3 ✓ HTTP Methods

Task 4 ✓ HTTP Status Codes

Task 5 ✓ Headers

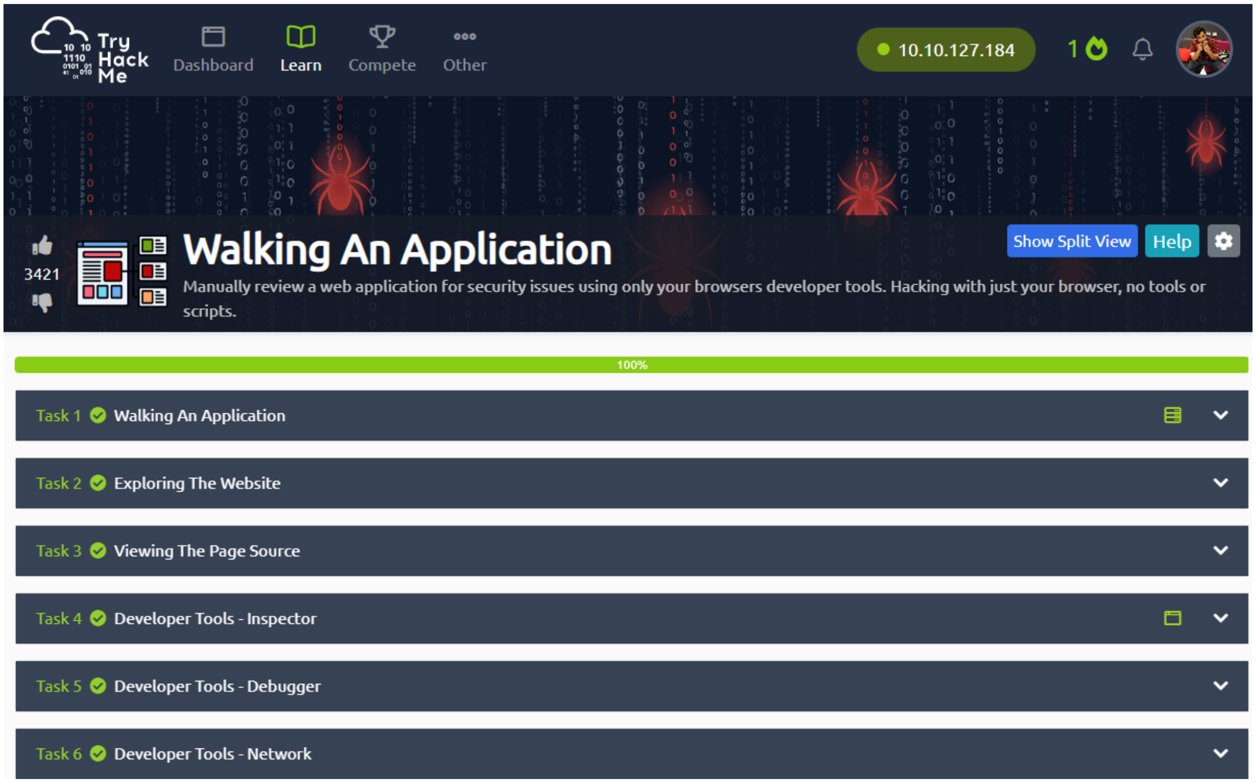
Task 6 ✓ Cookies

Task 7 ✓ Making Requests

Walking an Application

This room covers using your browsers in built tools to manually review web applications for security issues. It covers

- Viewing the page source for things like
  - Links in anchor tags
  - Frameworks being used (bootstrap, etc)
  - Secrets being hidden under page stylings
- Using the Inspector
  - Review how changes in code impact the final page, and can modify the page to reveal information
- Debugger
  - Look for vulns or turn off features in the JS code
- Network,
  - Track files being sent to your browser,



Walking An Application

Manually review a web application for security issues using only your browsers developer tools. Hacking with just your browser, no tools or scripts.

Task 1 Walking An Application

Task 2 Exploring The Website

Task 3 Viewing The Page Source

Task 4 Developer Tools - Inspector

Task 5 Developer Tools - Debugger

Task 6 Developer Tools - Network

Content Discovery

This was about using some well known and less known tools the cleverly enumerate information out of website. It first goes over some manual techniques such as

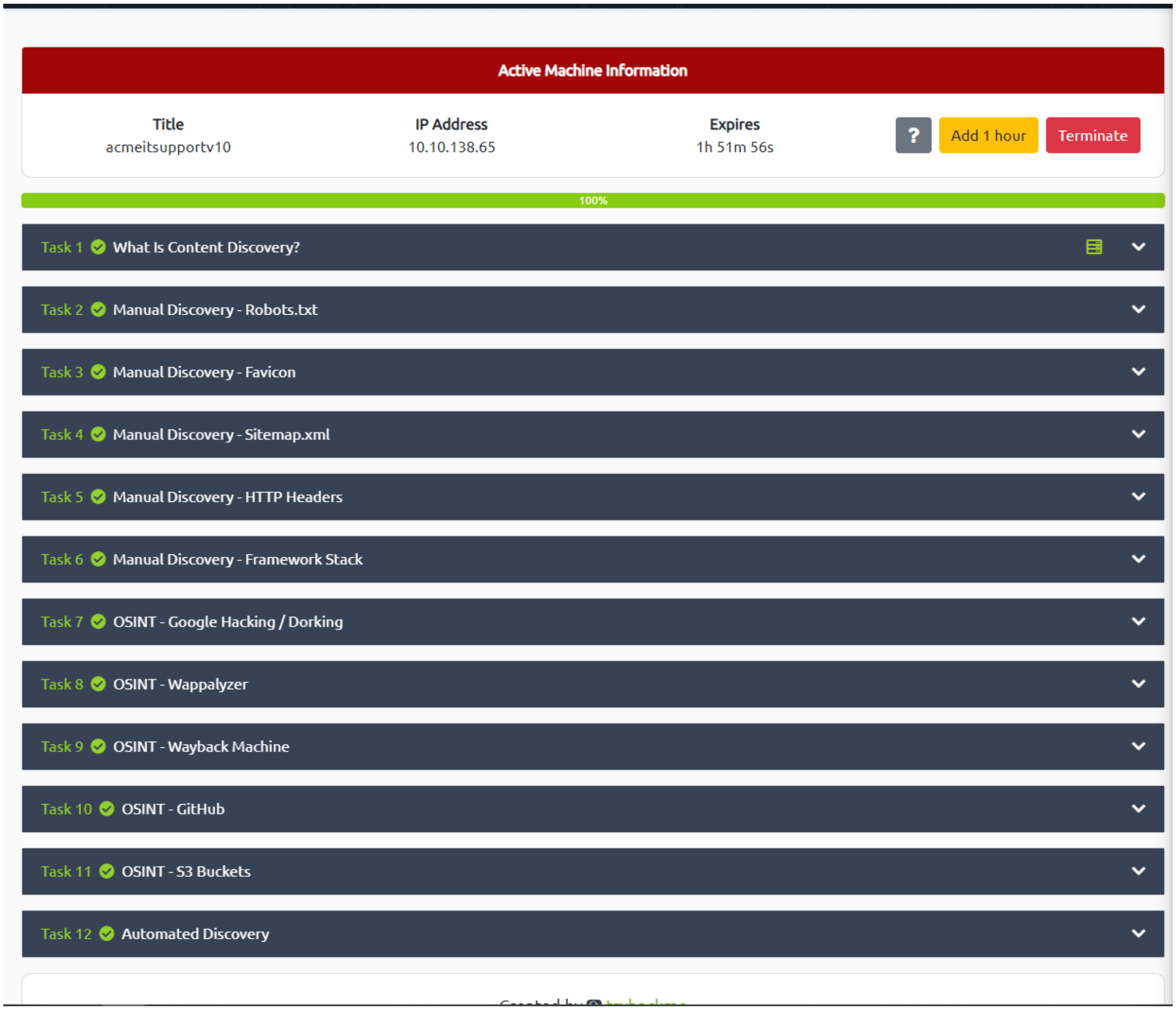
- Robots.txt, which is used to restrict what search engines reveal in their results
- Favicon - which can identify frameworks when web-devs aren't being careful
- Sitemap.xml is the opposite of robots.txt in the sense that it specifies what content site owners want shown

Some Open source techniques covered are

- Dorking - which is using googles advanced search tools to aid in specifying content of interest
- S3 Buckets, which relies on human error, but can hold files that the site owners may not want accessible

And Automated tools

- Like using a word list and launching it against form fields of the website
- Tools like ffuf, dirb, and gobuster



Active Machine Information

Title	IP Address	Expires
acmeitsupportv10	10.10.138.65	1h 51m 56s

100%

Task 1 ✓ What Is Content Discovery?

Task 2 ✓ Manual Discovery - Robots.txt

Task 3 ✓ Manual Discovery - Favicon

Task 4 ✓ Manual Discovery - Sitemap.xml

Task 5 ✓ Manual Discovery - HTTP Headers

Task 6 ✓ Manual Discovery - Framework Stack

Task 7 ✓ OSINT - Google Hacking / Dorking

Task 8 ✓ OSINT - Wappalyzer

Task 9 ✓ OSINT - Wayback Machine

Task 10 ✓ OSINT - GitHub

Task 11 ✓ OSINT - S3 Buckets

Task 12 ✓ Automated Discovery