SECURITY ASSESSMENT

Submitted to: Application Development Team
Security Analyst: George Ghira

Date of Testing: February 2025
Date of Report Delivery: February 2025

Table of Contents

Security Engagement Summary

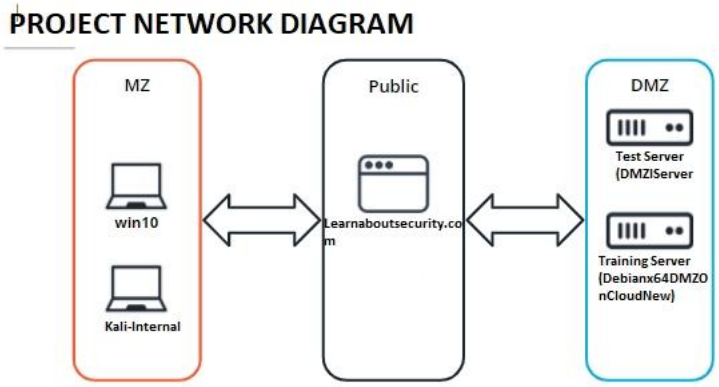
Engagement Overview

The engagement has been conducted in order to determine the security posture of PJ Bank's virtual environment and to highlight any security risks associated with the infrastructure in scope.

Scope

The following devices are in scope of the assessment:

S. No.	Asset Information	Hostname	IP Address
1	Public web server	Learnaboutsecurity.com	
2	Employee Workstation	Win10	10.1.2.4
3	Debian Server in DMZ	DMZiServer	10.1.0.7
4	Web App Server in DMZ	Debianx64DMZOnCloudNew	10.1.0.11



Risk Analysis

<Considering the significant vulnerabilities identified, the overall security risk of the virtual machine tested during the engagement is **<DEFINE SEVERITY HERE as Low Moderate or High>.**

- **High** – severe or catastrophic impact
- **Moderate** – Serious impact
- **Low** – limited impact

>

Recommendations

<Complete this section with recommendations based on major vulnerabilities discovered and/or exploited. The vulnerabilities highlighted in this report should be remediated as soon as possible>

- <Make non-technical and high level recommendations for an executive team to review. The recommendations should include things that executive-level directors, board members, and if provided to the public, someone non-technical can understand.

For example: The company should implement a policy that enforces multi-factor authentication. The security analysts determined that account passwords could be guessed and access to the network was gained remotely. Implementing multi-factor authentication would have prevented the analyst from gaining access to the network in this manner.>

Significant Vulnerabilities Summary

Significant vulnerabilities identified during the vulnerability assessment and validation are summarized below. While additional vulnerabilities may be present, these are considered significant and warrant resolution.

High-Risk Vulnerabilities

<Add the vulnerabilities here, if there are no vulnerabilities in this category, remove the category>

Medium-Risk Vulnerabilities

<Add the vulnerabilities here, if there are no vulnerabilities in this category, remove the category>

Low-Risk Vulnerabilities

<Add the vulnerabilities here, if there are no vulnerabilities in this category, remove the category>

Significant Vulnerability Details

Details about the significant vulnerabilities you listed above are provided below.

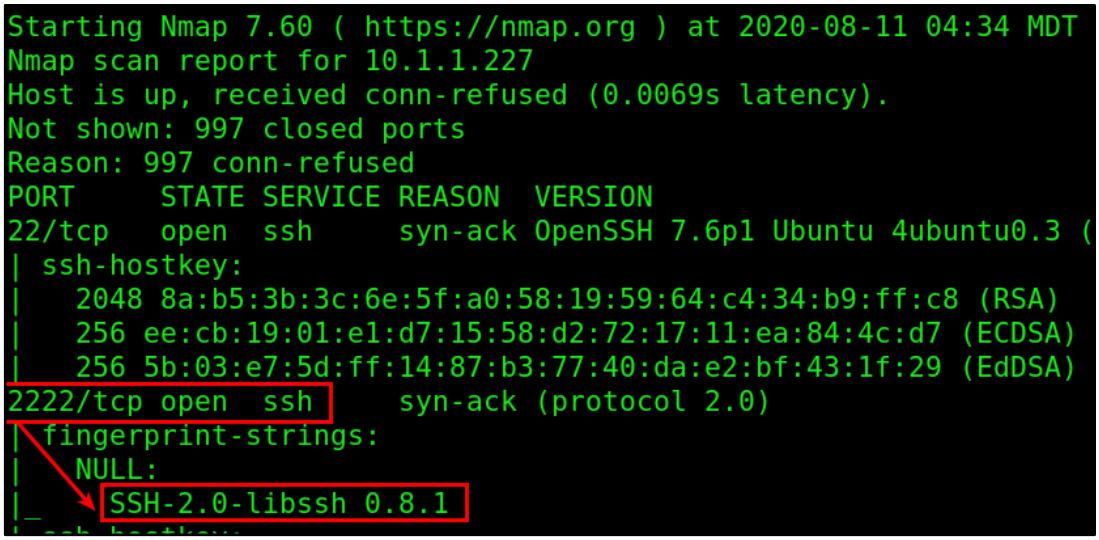
<For each vulnerability, make sure to:

- Identify the risk priority
- Describe the vulnerability
- Provide a screenshot that is centered, bordered, and has a caption
- Add a Discussion section under the screenshot>

Example of a vulnerability finding:

HIGH-RISK Vulnerability

The student found that both the LibSSH and Elasticsearch packages contained vulnerabilities directly associated with the lack of patching.



Example of a machine with LibSSH Missing Software Patches

Discussion:

<In your discussion, be sure to mention:

- Vulnerabilities were discovered <in what? why?>
- Are there any links available to discuss?

Appendix A: Security Analysis Methodology

The methodology the analyst used for the vulnerability assessment is provided below.

Assessment Tools Selection

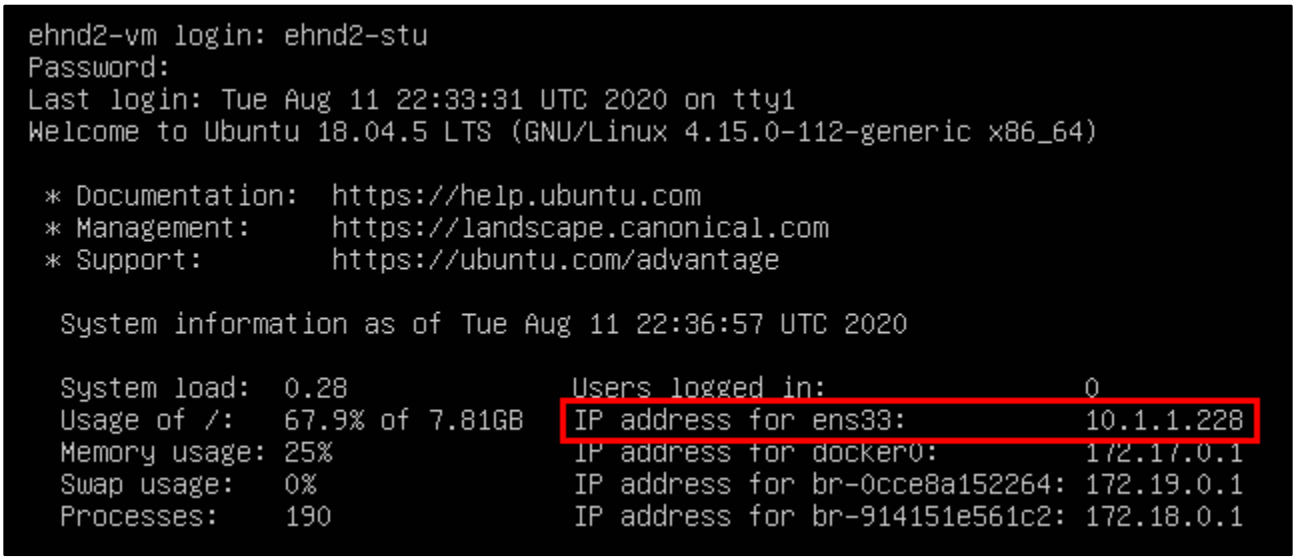
Noting the scope of the engagement was focused on a web application, the security analyst chose relevant web-application security analyst tools. The analyst created a Kali Virtual Machine which had many included tools. Tools used during this engagement included:

- Kali Operating System
  - https://www.kali.org/
  - Description
- Python Environment
  - https://www.python.org/
  - Description
- Nmap
  - https://nmap.org/
  - Description
- Others
  - Link
  - Description

Example:

Description of what/why you did

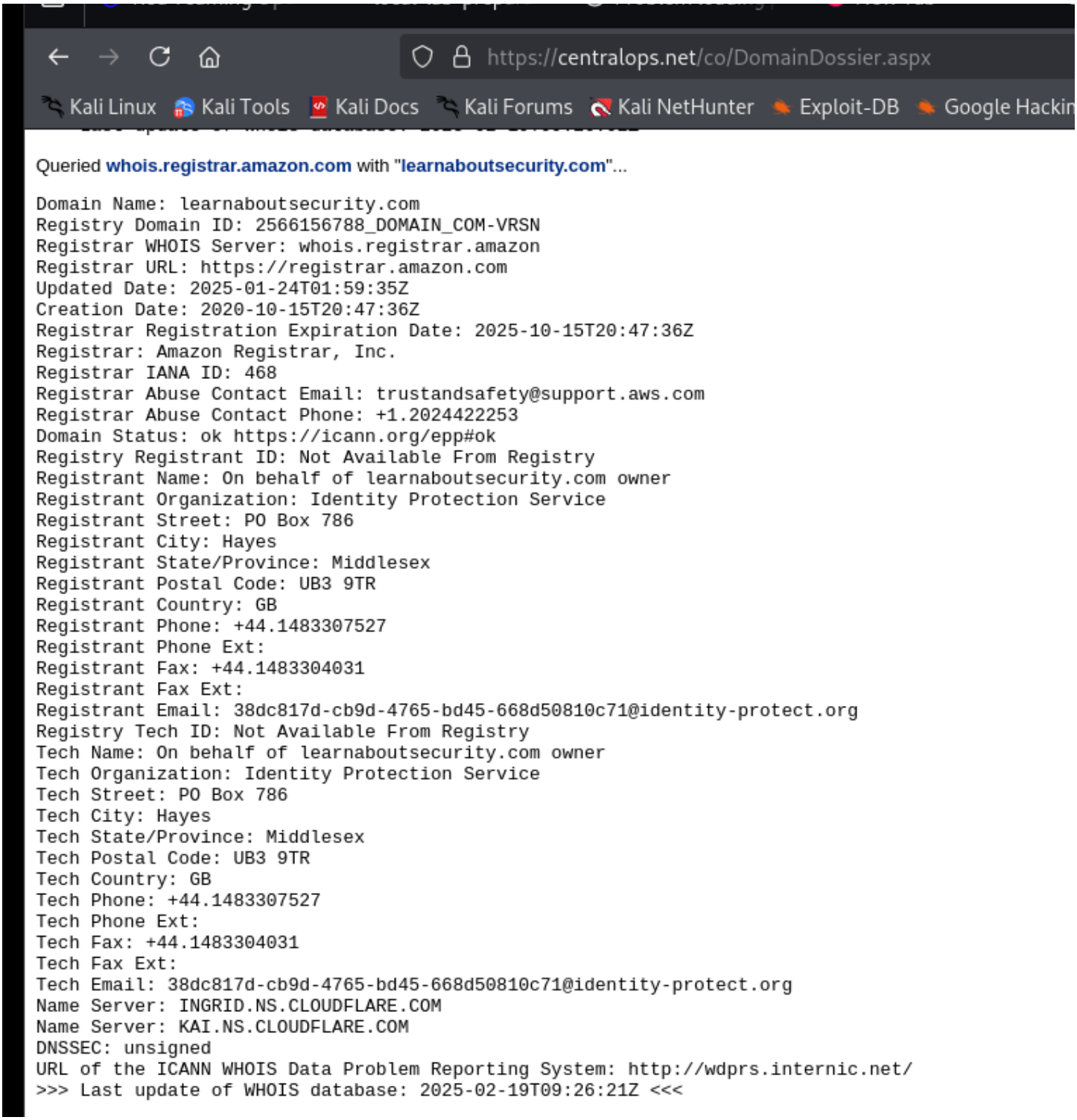
- Command used



Screenshot of <COMMAND> and results

Reconnaissance

<Provide a screenshot from the OSINT tool, and a description of the findings>



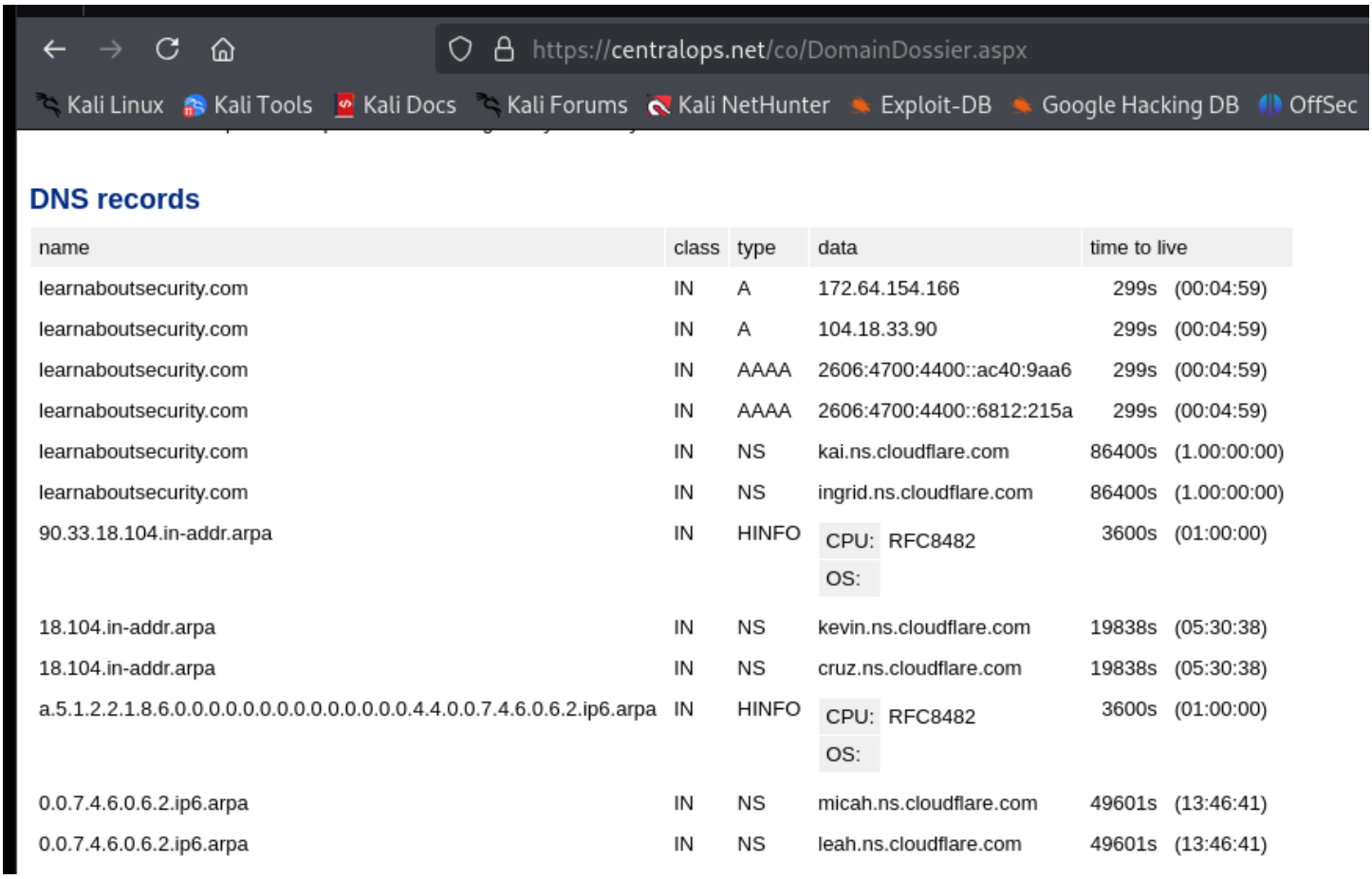
This means the domain is registered through Amazon, privacy-protected, and uses Cloudflare for DNS management.

Name server ((INGRID.NS.CLOUDFLARE.COM, KAI.NS.CLOUDFLARE.COM), which suggests security measures like DDoS protection and CDN services.

DNSSEC (Domain Name System Security Extensions) is not enabled, meaning DNS spoofing or cache poisoning attacks could be a concern.

Another interesting fact, expiration date of the site, which could be used by malicious actors to revendicate the ownership of the site before the owner and then ask a financial pay in order to transfer the ownership right.

<DNS Information, including at least the names to IP mappings>



DNS records

name	class	type	data	time to live
learnaboutsecurity.com	IN	A	172.64.154.166	299s (00:04:59)
learnaboutsecurity.com	IN	A	104.18.33.90	299s (00:04:59)
learnaboutsecurity.com	IN	AAAA	2606:4700:4400::ac40:9aa6	299s (00:04:59)
learnaboutsecurity.com	IN	AAAA	2606:4700:4400::6812:215a	299s (00:04:59)
learnaboutsecurity.com	IN	NS	kai.ns.cloudflare.com	86400s (1.00:00:00)
learnaboutsecurity.com	IN	NS	ingrid.ns.cloudflare.com	86400s (1.00:00:00)
90.33.18.104.in-addr.arpa	IN	HINFO	CPU: RFC8482 OS:	3600s (01:00:00)
18.104.in-addr.arpa	IN	NS	kevin.ns.cloudflare.com	19838s (05:30:38)
18.104.in-addr.arpa	IN	NS	cruz.ns.cloudflare.com	19838s (05:30:38)
a.5.1.2.2.1.8.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.4.0.0.7.4.6.0.6.2.ip6.arpa	IN	HINFO	CPU: RFC8482 OS:	3600s (01:00:00)
0.0.7.4.6.0.6.2.ip6.arpa	IN	NS	micah.ns.cloudflare.com	49601s (13:46:41)
0.0.7.4.6.0.6.2.ip6.arpa	IN	NS	leah.ns.cloudflare.com	49601s (13:46:41)

These records map the domain name learnaboutsecurity.com to IP addresses: 172.64.154.166, 104.18.33.90

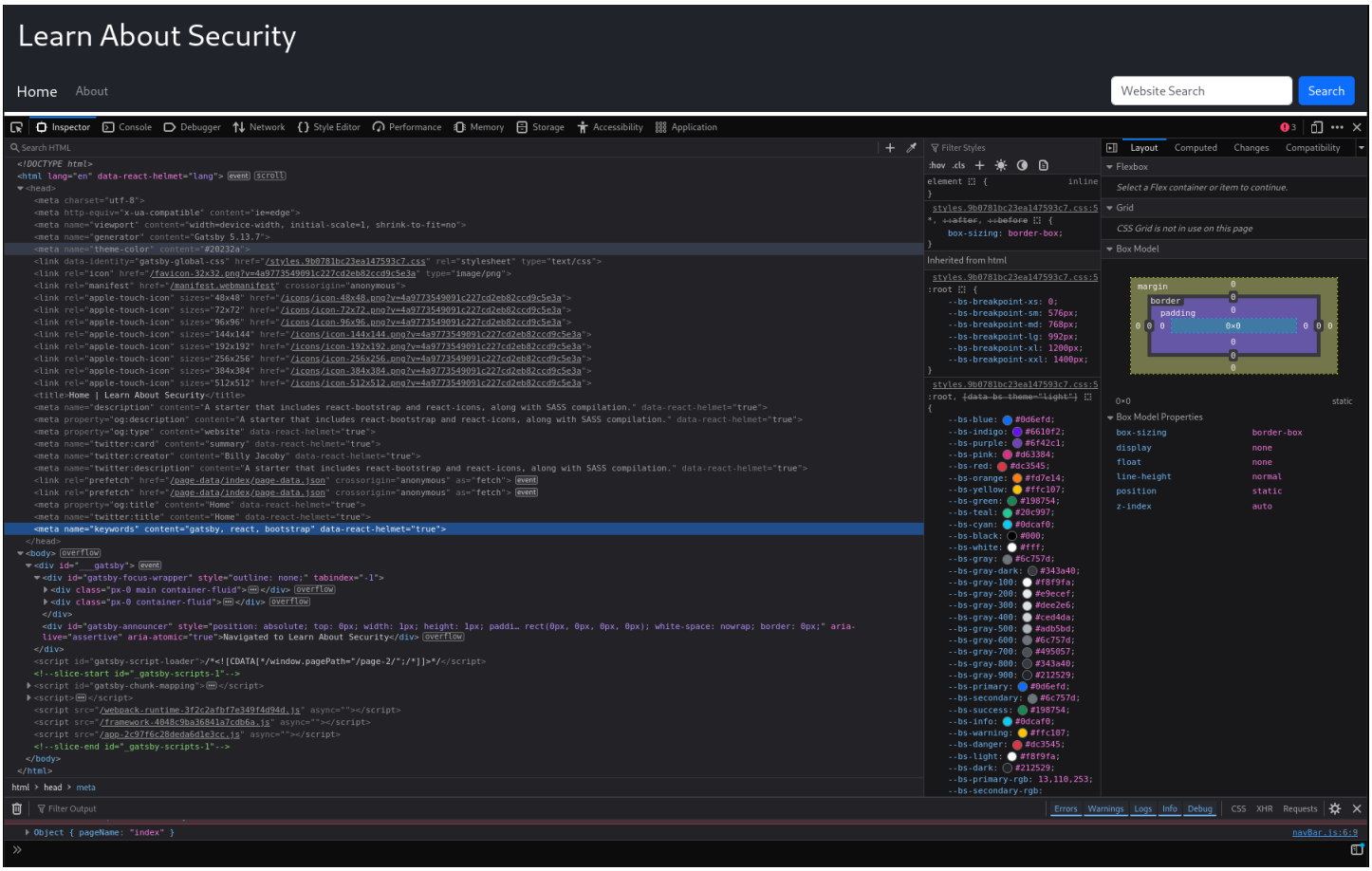
These records map the domain to IPv6 addresses: 2606:4700:4400::ac40:9aa6 , 2606:4700:4400::6812:215a

Name servers managing the domain's DNS: kai.ns.cloudflare.com, ingrid.ns.cloudflare.com

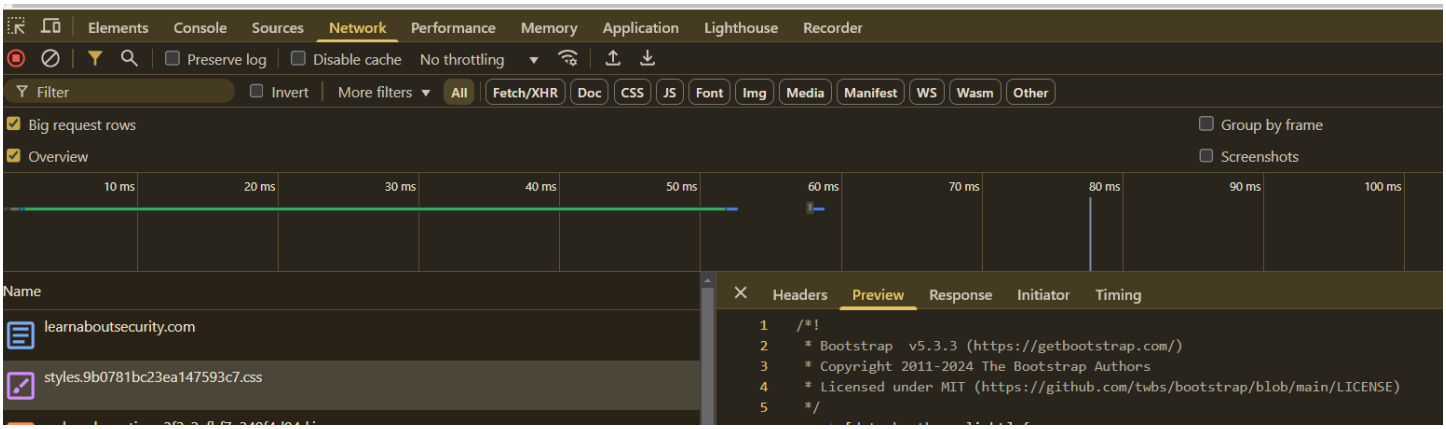
Host Information are not available due RFC482 standard for privacy (and security)

<Web technologies used by the website, with a screenshot of the identification >

Using Dev tools from Google Chrome we learn:

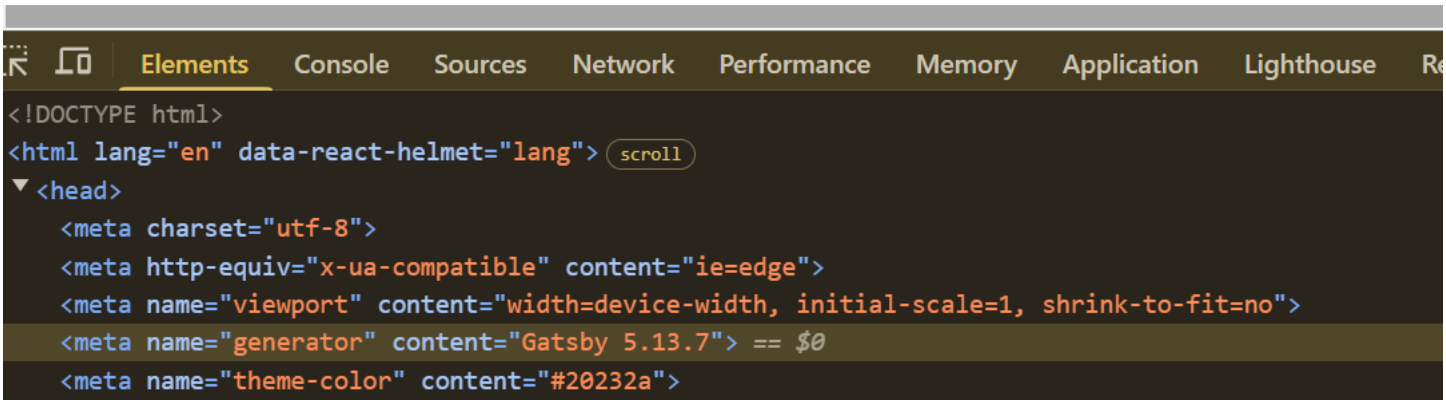


Use HTML for web structuring,

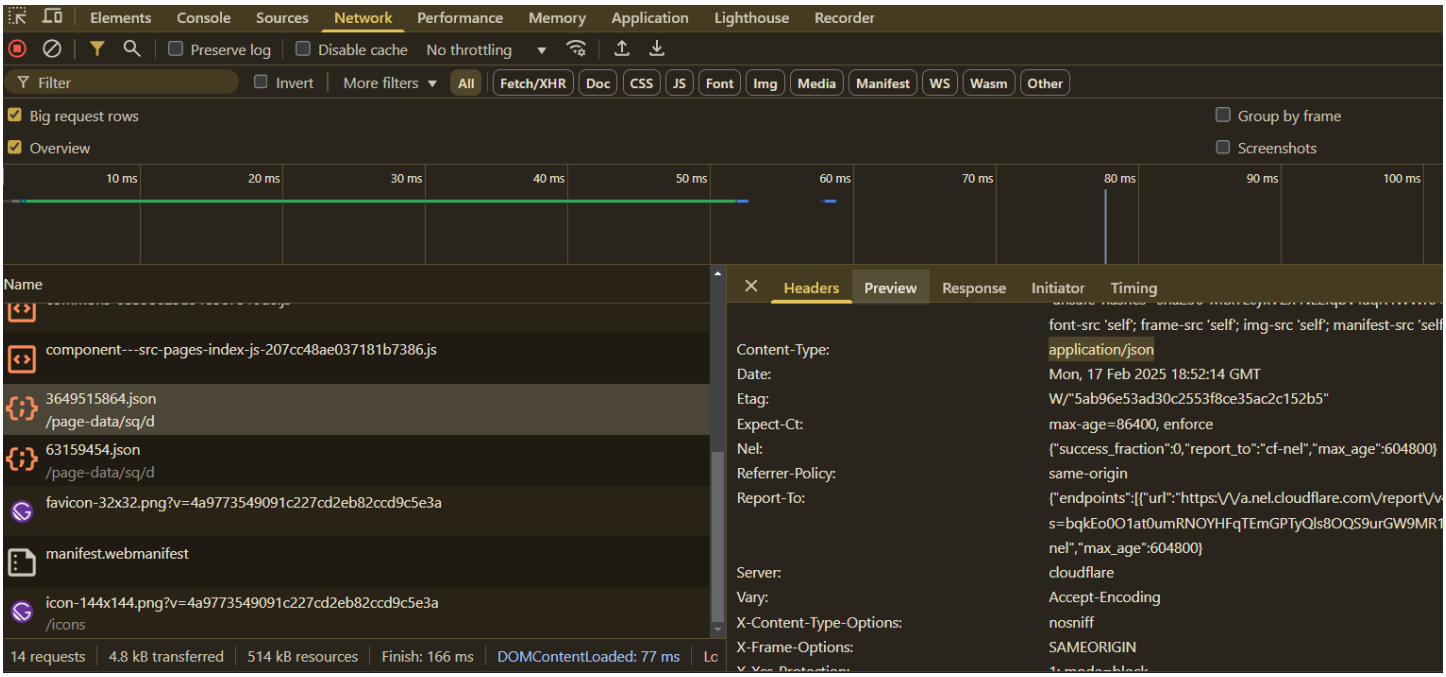


Use CSS for styling (with Bootstrap v5.3.3 libraries)

Use JavaScript for interaction (with react 19)



Use Gatsby 5.13.7 version used as a framework



Use Json to send/receive data via API.

In conclusion:

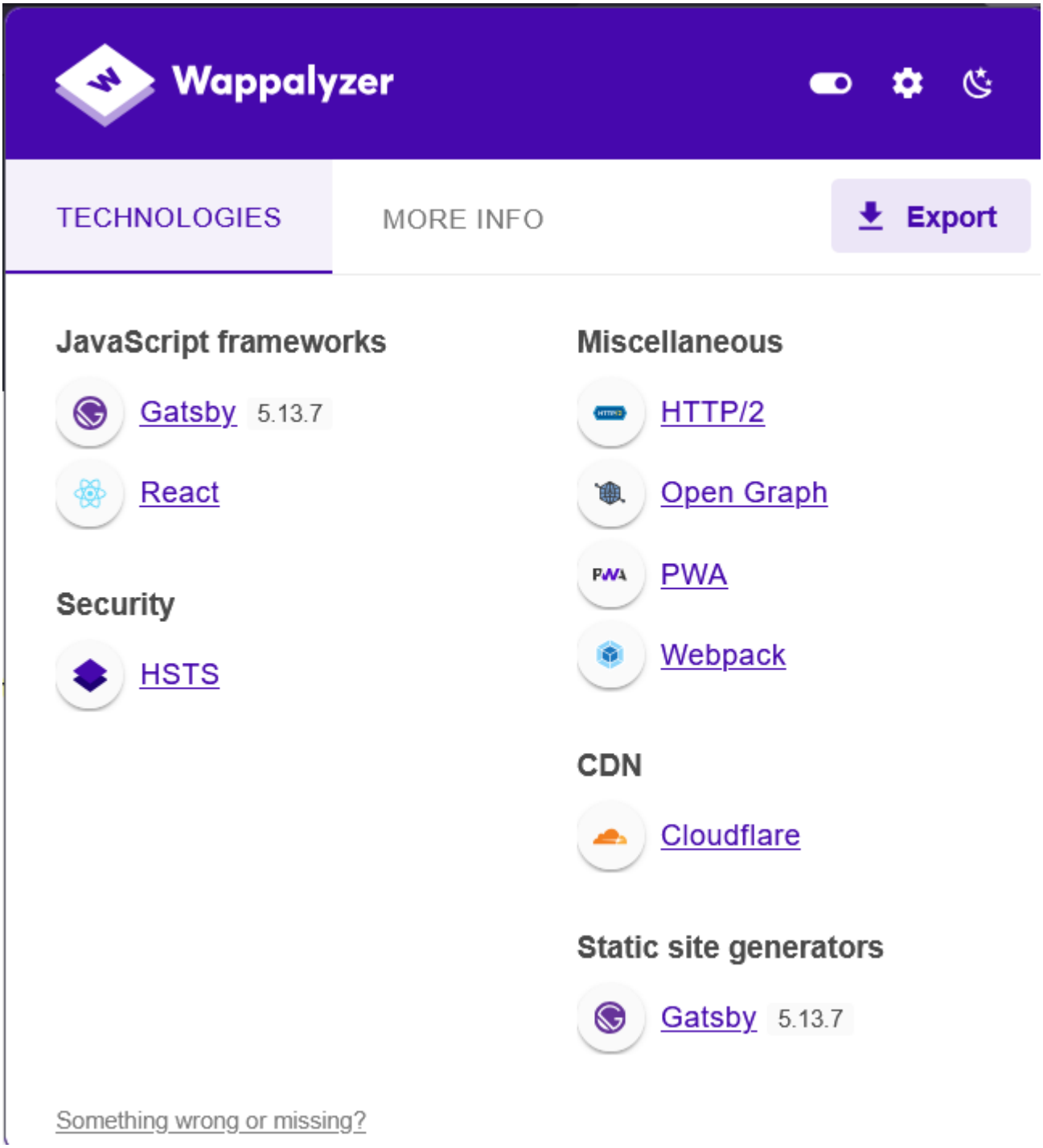
The site is React-based and likely built using Gatsby.

Uses Bootstrap for styling, meaning pre-designed UI elements.

Likely dynamically updates SEO/meta tags using React Helmet.

Variant 2:

Instaled Wappalyser as a extension and got this in less than 1 second!



Scanning

<Annotated screenshot and description of the nmap scans of each machine, one-by-one.>

Exploitation

<Successful exploits to gain access/ exfiltrate sensitive data>

<Exploit commands>

<Vulnerable software exploitation>

<Weak Password Cracks>

<provide the commands you used and screenshots for them, with the description as seen in the example>
