**Assignment Summary**

This initial report is part of the assignment 'Foot printing and Reconnaissance.' As the penetration testing phase begins, there are six steps defined by the CEH council.

RECONNAISSANCE

SCANNING

VULNERABILITY ASSESSMENT

EXPLOITATION

REPORTING

In this part, the first step will be started and continued towards the report phase. The purpose of this phase is to determine the victim network status, gather information, and document all findings.

**Approach**

The first step of this pentest report starts with reconnaissance. Search engines will be used to gather as much information from the internet as possible. This might include simple information about the domain up to the server being used in the victim environment. Testing was performed remotely over the internet via a host with a normal Windows 11 running laptop. Each step is done manually and documented for possible findings.

**Scope**

The scope of this assessment is a live website used for practice.

**In-Scope Assessment**

| HOST/URL/IP Address | Description |

| www.hackthebox.com | Targeted website |

**Assessment Overview**

During the initial phase of the reconnaissance phase, four tools were used:

[1]. **whois**

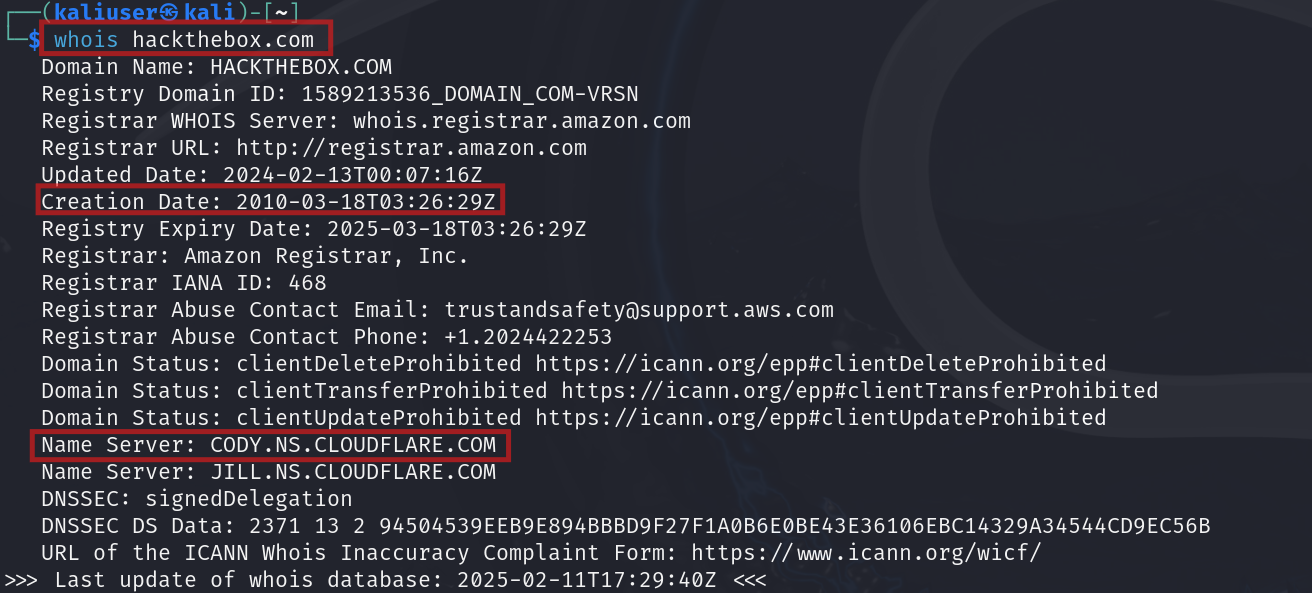
[2]. **nslookup**

[3]. **maltego**

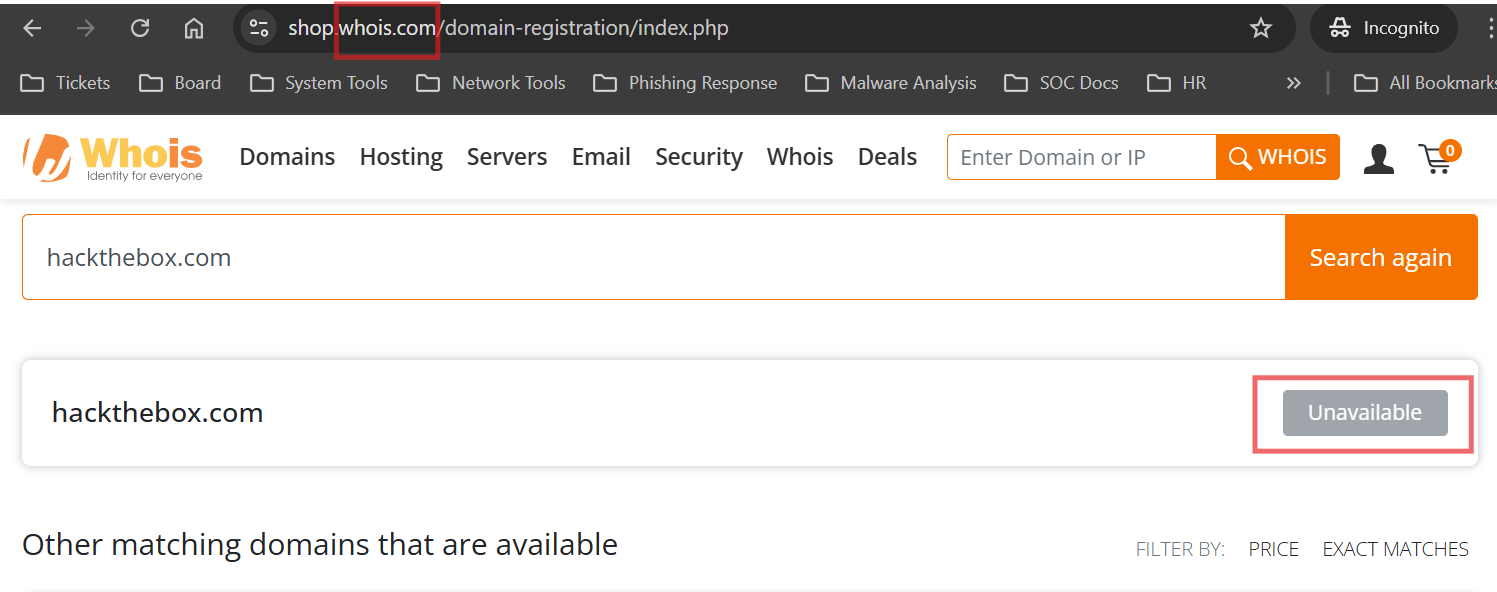
[4]. **wappalyzer**

[1]. **whois**: Using the whois tool, information on the domain creation date, name server, and registrar URL was gathered.

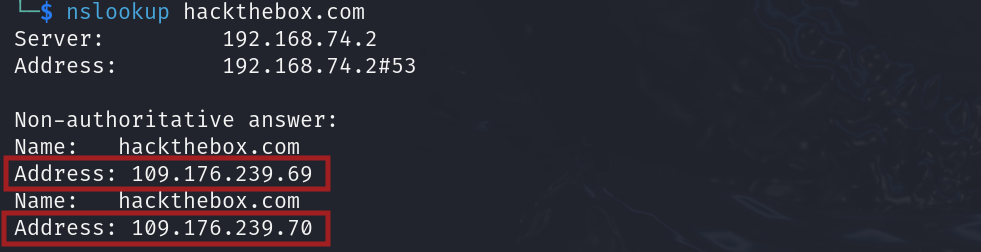
$ whois hackthebox.com



The above information couldn't be found from the browser, so the whois tool on Linux was better in this aspect.



[2]. **nslookup**: Searching for DNS records, A records. During the nslookup command for the 'hackthebox' website, two Domain Name System (DNS) servers that host this website were found. This can also be referenced to the server responsible for load balancing.



The responsible mail address (MX).

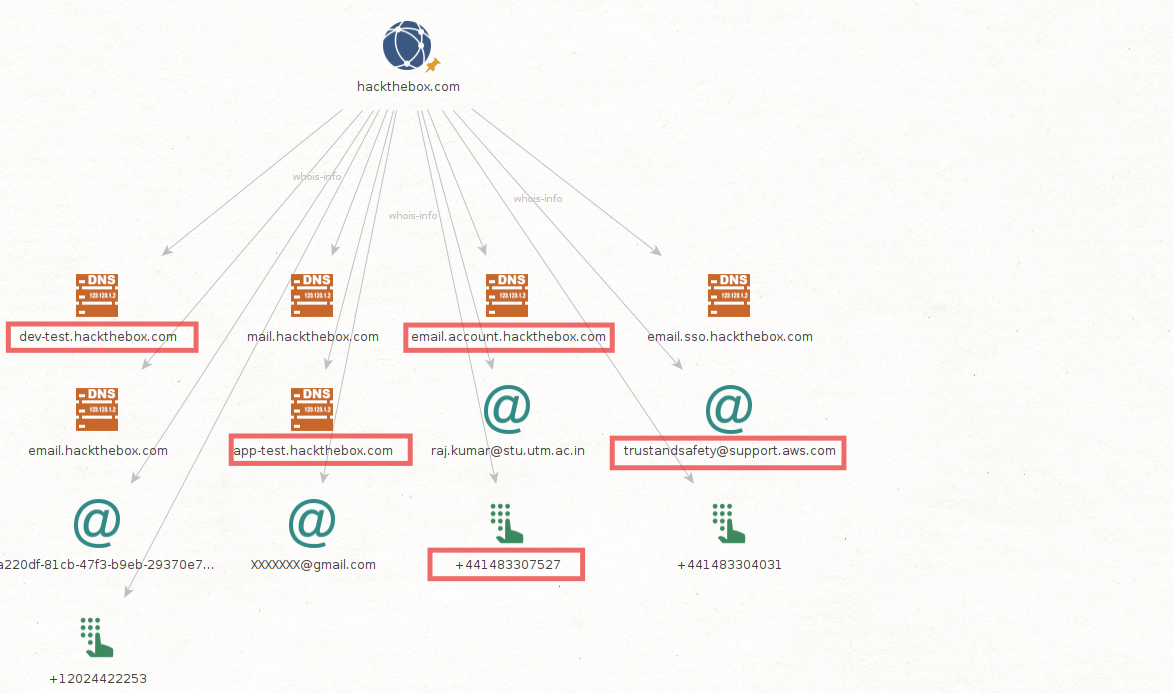
>nslookup

> set type=MX

> www.hackthebox.com



[3]. **maltego**: Using this tool, subdomains, phone numbers, and email addresses related to this domain were queried. This tool was helpful to put a graphical representation of the relationship between the parent-child entity and findings using the transform tools. Some findings are as follows:



[4]. **wappalyzer**: It is a cloud-based tool to find the CMS of a website. The aggregate information shows the domain is using Cloudflare for its content delivery network service.

