# **CTF Topic: Domain Enumeration Cisco Talos**



# **Introduction**

In this CTF challenge, participants have to perform Domain enumeration that involves gathering information about a domain, its associated subdomains, IP addresses, DNS records, and other relevant data. This process is crucial in cybersecurity, penetration testing, and competitive intelligence to understand the digital footprint of a target.

# **Tools and requirements**

* [Cisco Talos](https://talosintelligence.com/)

# **Scenario**



Imagine you are a cybersecurity analyst tasked with investigating the domain [www.blanxer.com](http://www.blanxer.com). Your objective is to gather detailed information about the domain, including its subdomains, IP addresses, DNS records, and any security-related data that can help in assessing the domain's security posture.

# **Process to Perform**

* Navigate to the Cisco Talos Intelligence website: <https://talosintelligence.com/>
* Enter the target domain [blanxer.com](http://www.blanxer.com)) in the search bar to retrieve detailed information.

# **Let's Begin The Challenge**

# **Question**

Flag1: What is the Registry Domain ID?

Answer: 2740751208\_DOMAIN\_COM-VRSN

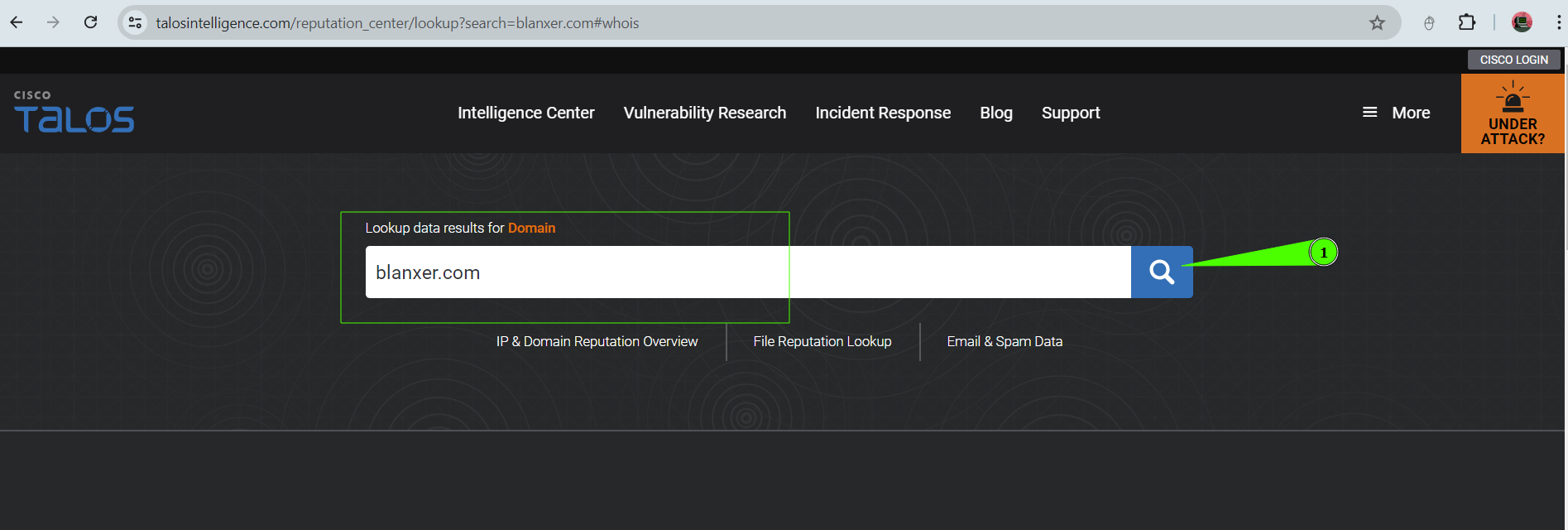
Flag2: Find 1st name server?

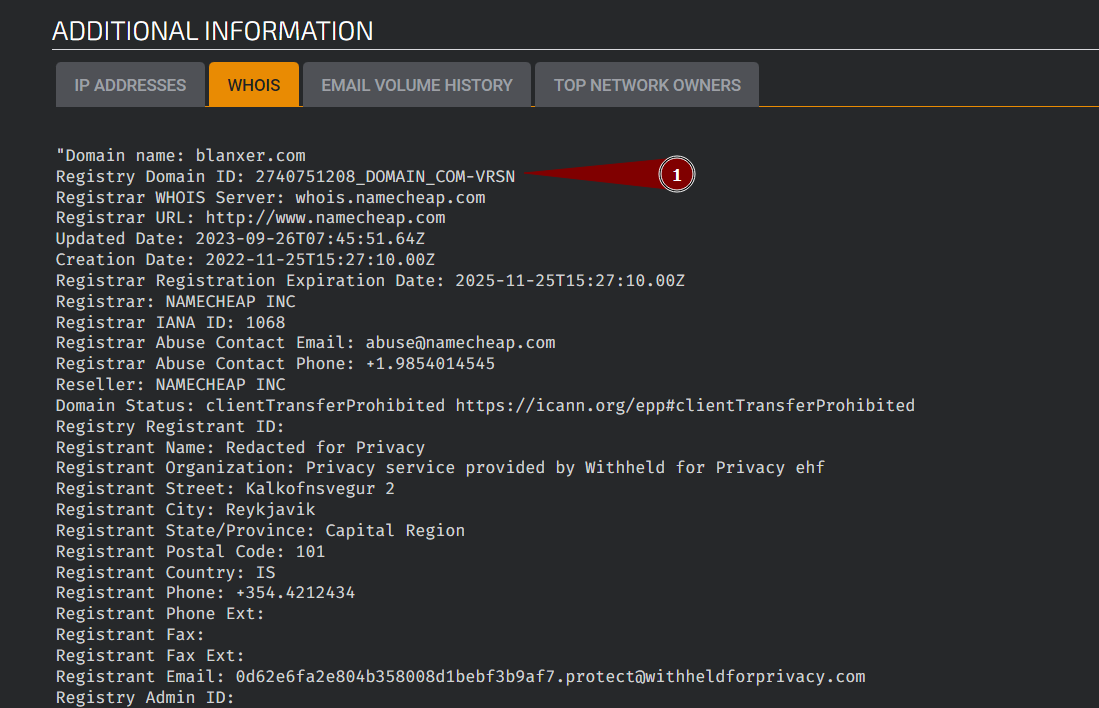
Answer: liberty.ns.cloudflare.com

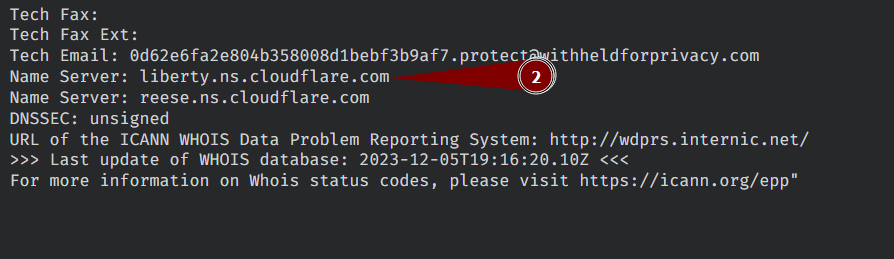
Flag3: How many mail servers are there?

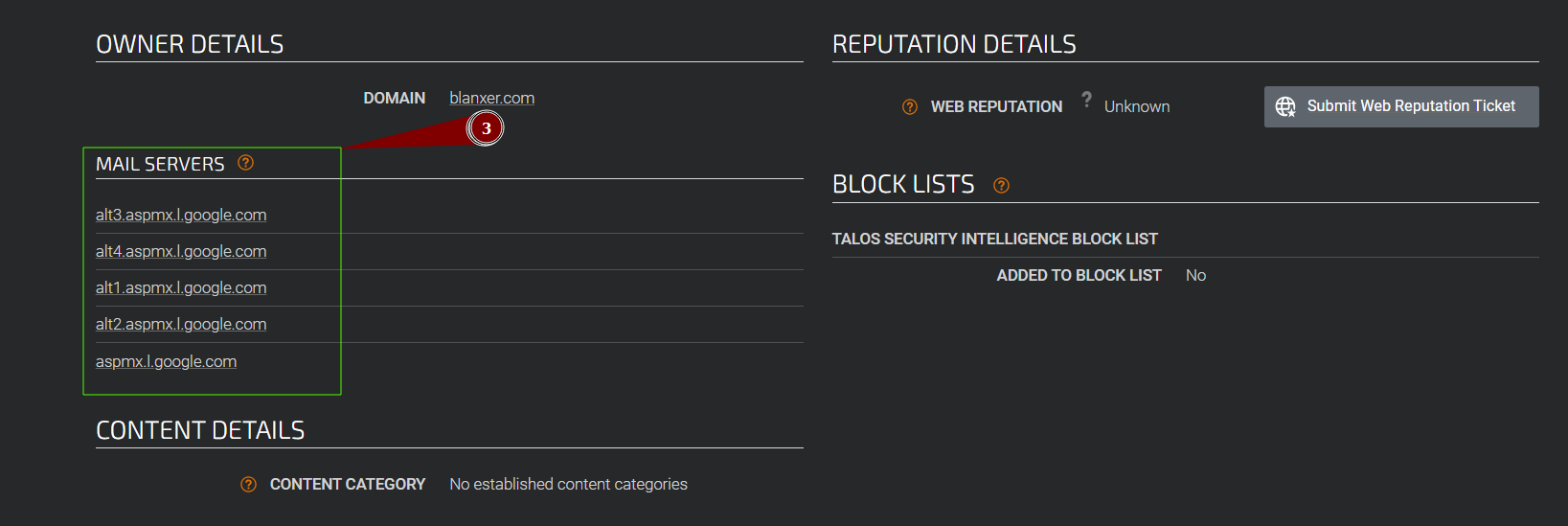
Answer: 4

# **Hint**



****

****

****