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



# **Introduction**



In this CTF challenge, participants have to perform Domain enumeration 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.

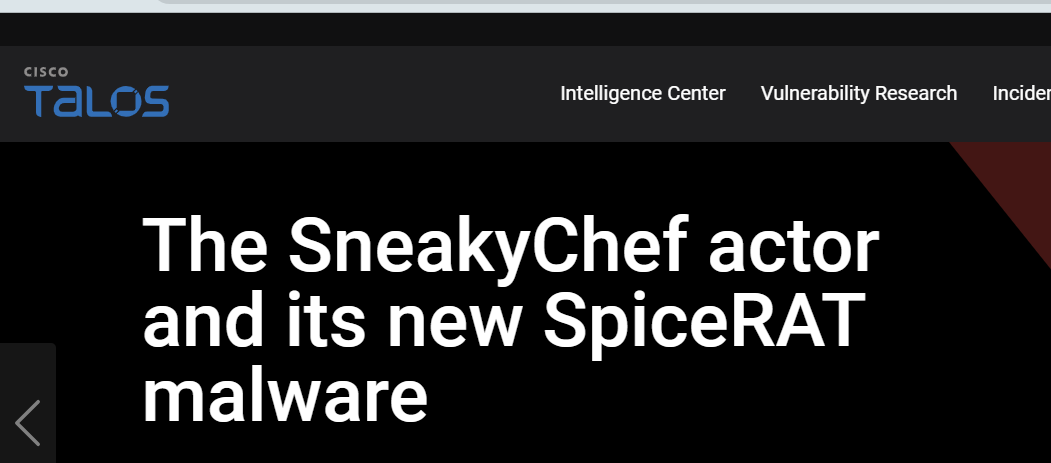
# **Tools and requirements**

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

# **Link (File)**

Target:[blanxer.com](http://www.blanxer.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, DNS records, and any security-related data to help assess its security posture.

# **Process to Perform**

* Navigate to the Cisco Talos Intelligence website
* Enter the target domain ([blanxer.com](http://www.blanxer.com)) in the search bar to retrieve detailed information.
* Click on the hostname option and select whois.
* Capture the flag

# **Let's Begin The Challenge**

# **Question**

**Flag1: What is the Registry Domain ID?**

**Answer: 2740751208\_DOMAIN\_COM-VRSN**

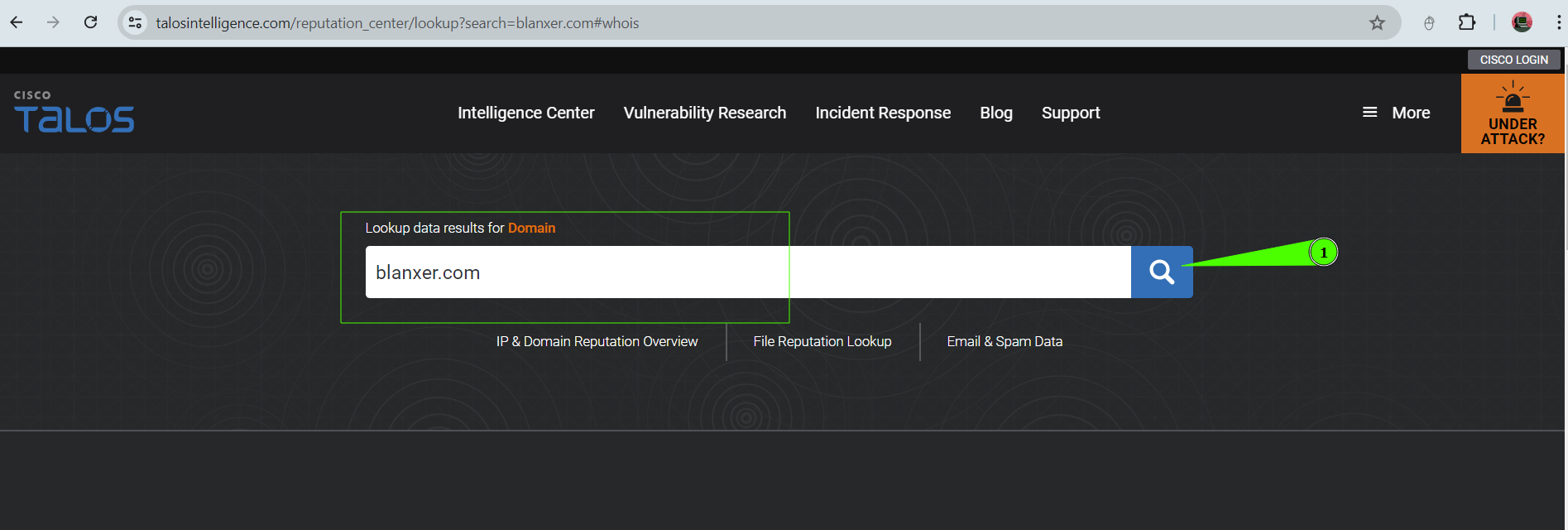
**Flag2: Find 1st name server?**

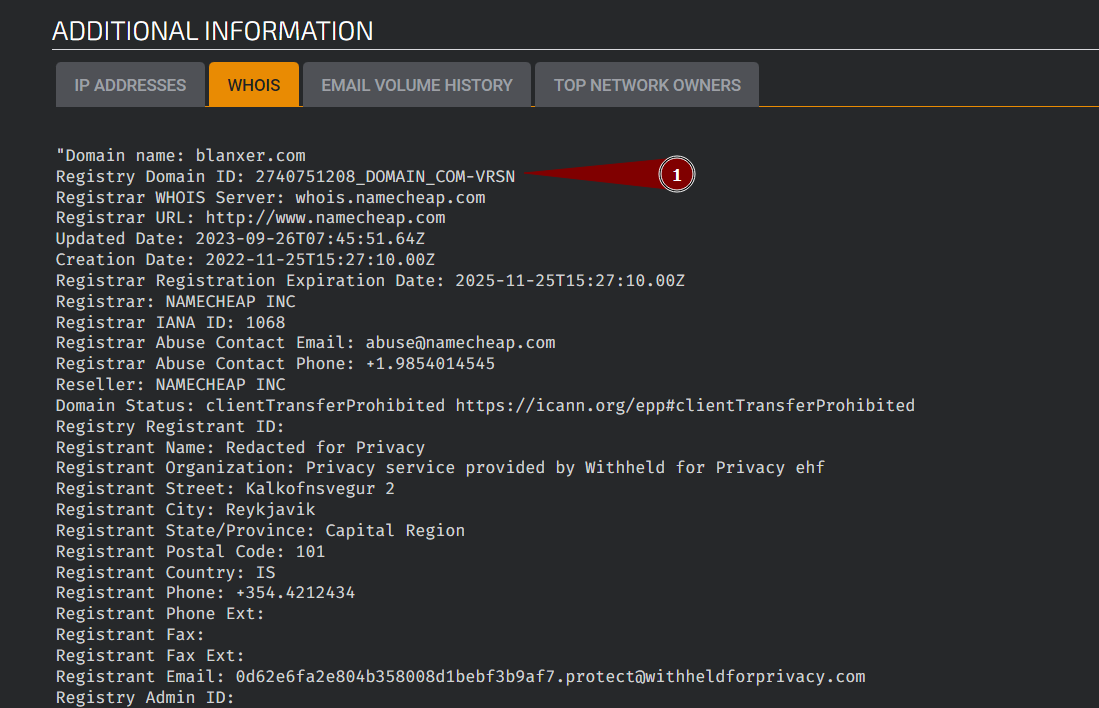
**Answer: liberty.ns.cloudflare.com**

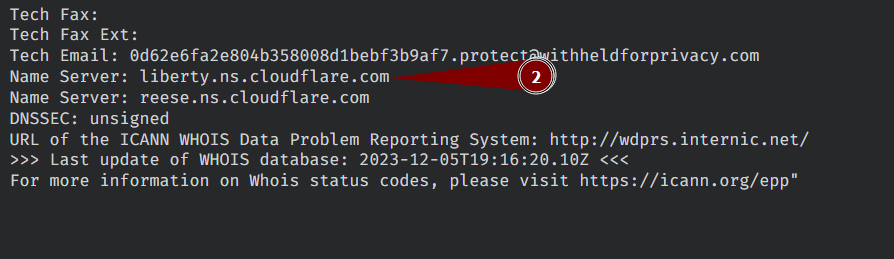
**Flag3: How many mail servers are there?**

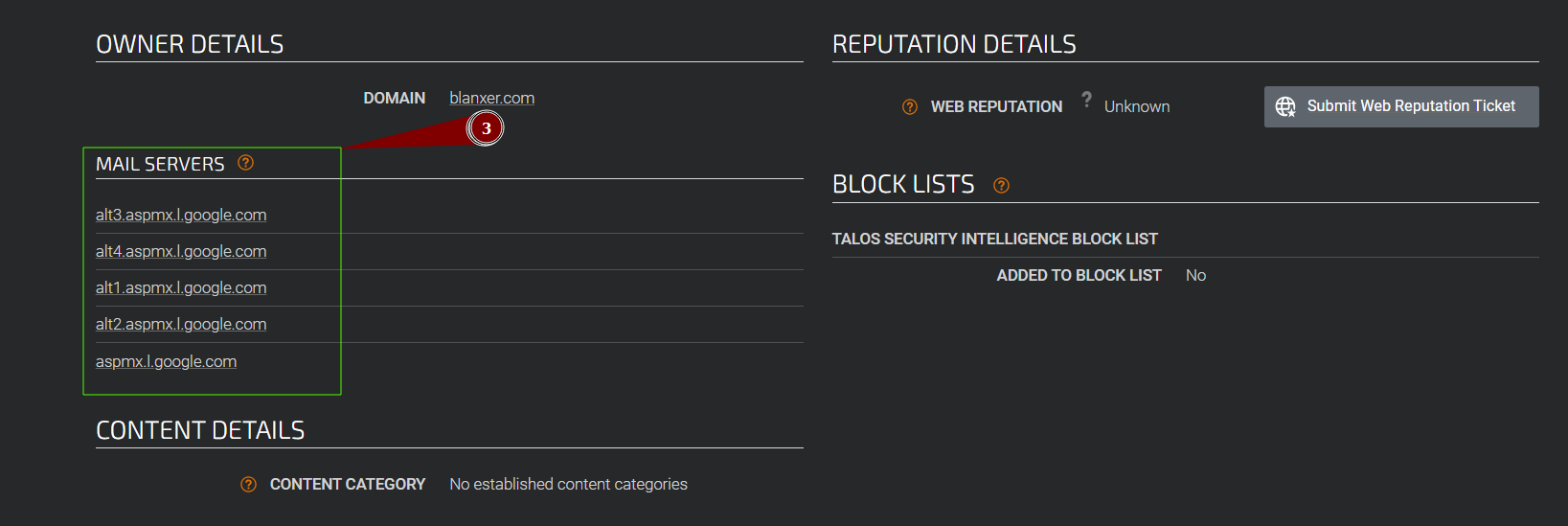
**Answer: 4**

# **Hint**



****

****

****