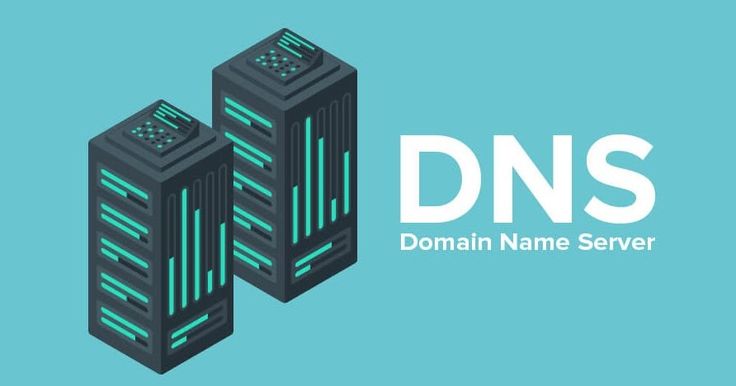
# **CTF Topic: DNS recon & research**



# **Introduction**

DNS reconnaissance is a crucial step in the information-gathering phase of a penetration test or a cybersecurity investigation. It involves collecting information about the DNS records of a target domain, which can reveal valuable insights about the target's infrastructure and potential vulnerabilities.

# **Tools and requirements**

1. [dnsdumpster](https://dnsdumpster.com/) web site

# **Link**

Target : blanxer.com

# **Scenario**

In this scenario, we will perform DNS reconnaissance on the target domain "blanxer.com" using DNSDumpster. The goal is to gather as much information as possible about the domain's DNS records.

# **Process to Perform**

* [Access DNSDumpster website](http://dnsdumpster.com)
* Then scan the target website

# **Let's Begin The Challenge**

# **Question**

Flag1: What is the IP of  **rees.np.cloudflare.com ?**

Answer: 108.162.195.1187

Flag2: Which mail server belongs to IP **142.250.27.26 ?**

Answer: alt3.aspmx.l.googlr.com

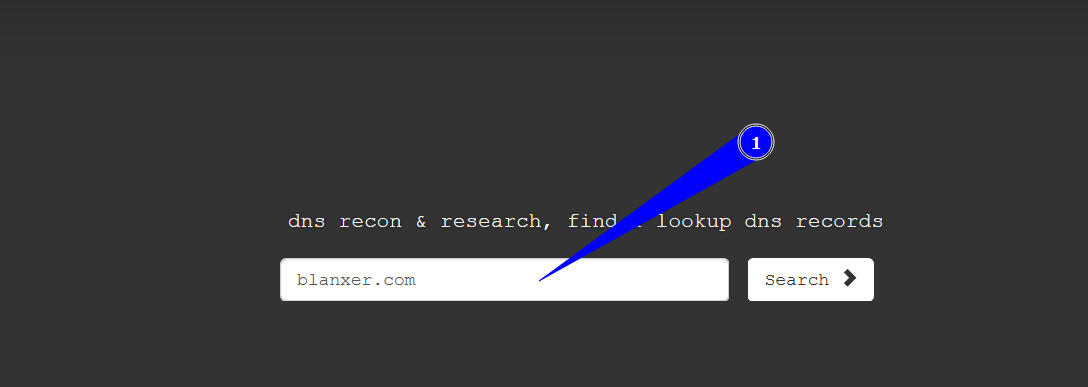
Flag3:What is the full form of MX ?

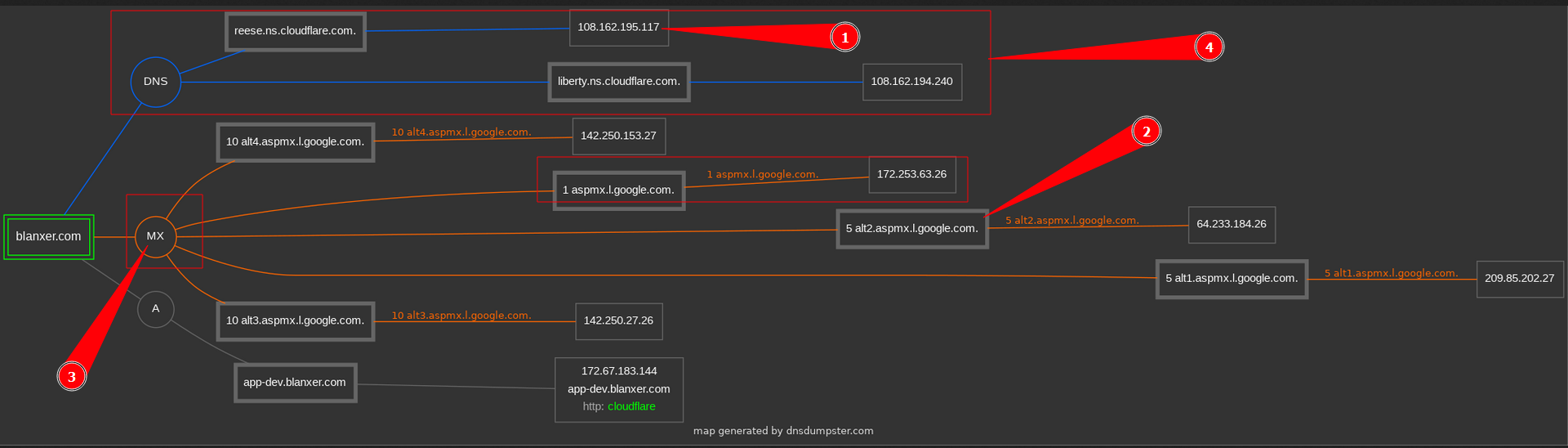
Answer: Mail server

Flag3: How many DNS name server are there ?

Answer: 2

# **Hint**



****