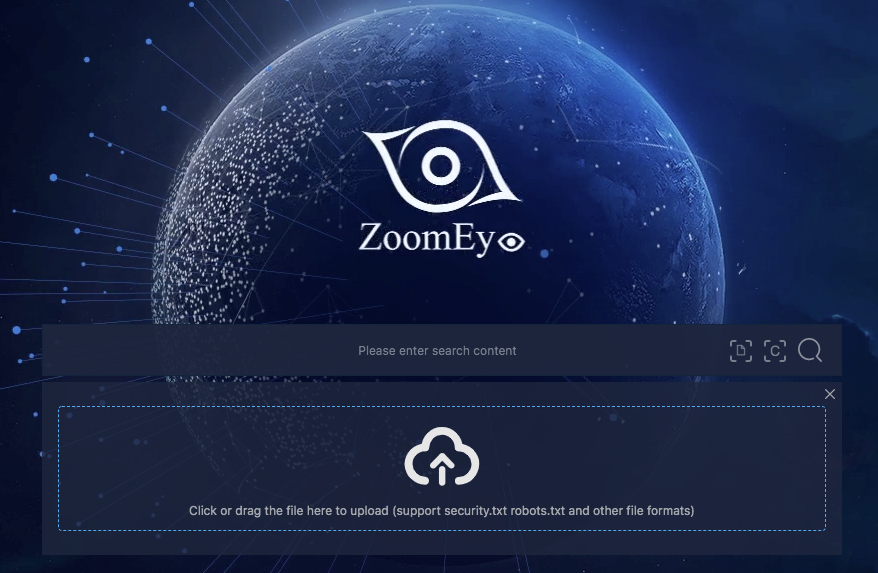
# **CTF Topic: ZoomEye Web View**



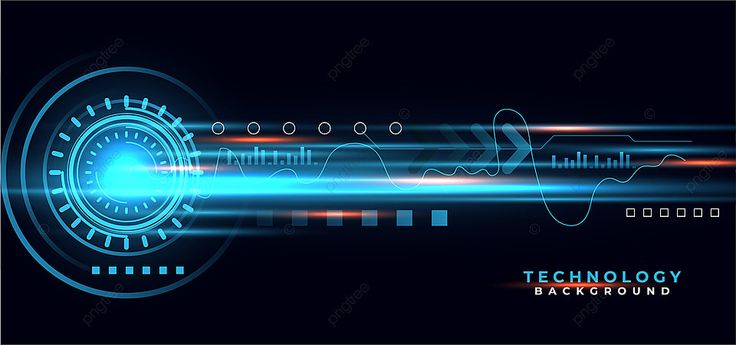
# **Introduction**

ZoomEye is a cybersecurity search engine, similar to Shodan, used to find information on devices and services connected to the internet. It allows users to search for and analyze various networked devices and services. This guide will walk you through using ZoomEye to gather information on a target IP address (137.74.187.102) for a Capture The Flag (CTF) challenge.

# **Tools and requirements**

[ZoomEYE](https://www.zoomeye.hk/pricing)

# **Scenario**



Assuming you participate in a CTF challenge, you will use the information gathered on the target IP address. Here are some possible steps:

# 

# 

# **Process to Follow while Performing CTF**

Step 1: Go through the zoomeye tool: [ZoomEYE](https://www.zoomeye.hk/pricing)

Step 2: then enter the target IP **137.74.187.102**  on the search box

Step 3: Now identify the flag and solve it

# **Let's Begin The Challenge**

# **Question**

Flag1: What is the Organization name of a target?

Answer: **staff hack this site**

Flag2: mae of ISP provider?

Answer: **OVH SAS**

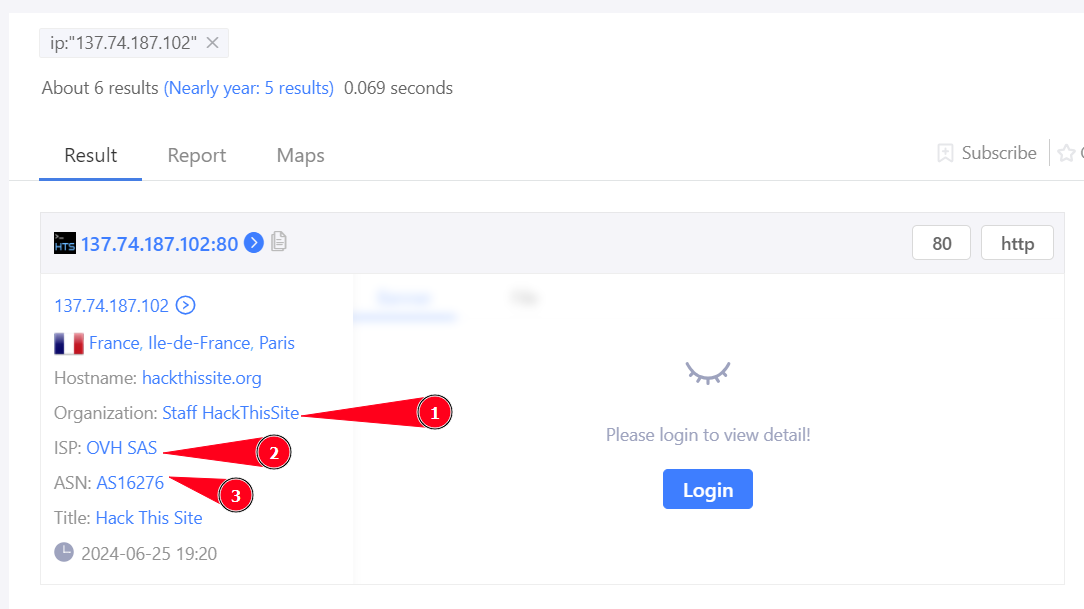
Flag3: What is the ASN number of the target system?

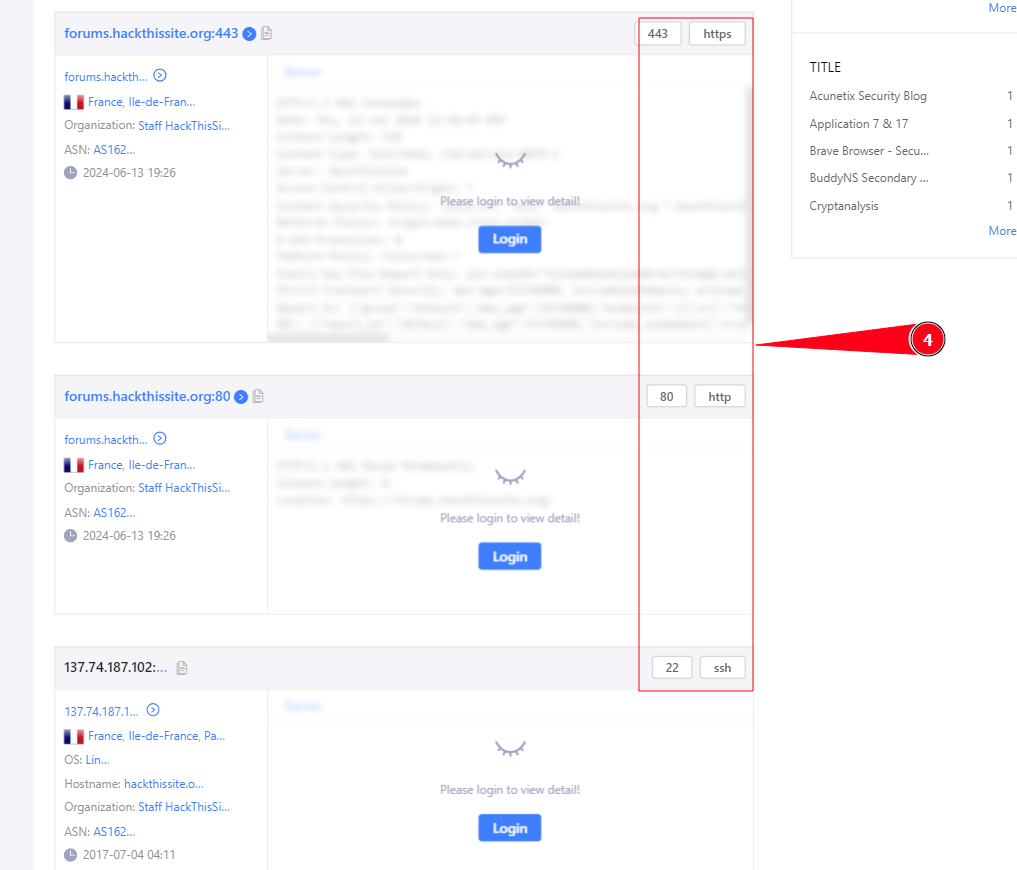
Answer: **AS16276**

Flag 4: How many Ports are open?

Answer: **3**

# **Hint**



****