### **CTF Topic: Open Port Scanning Using yougetsignal**

Introduction

#### Open port scanning is a crucial step in the reconnaissance phase of a security assessment. It involves identifying open ports on a target server to determine which services are running and potentially accessible from the internet. Each open port represents a possible entry point for attackers, and understanding which ports are open can help security professionals identify potential vulnerabilities. Common services include HTTP (port 80), HTTPS (port 443), SSH (port 22), and FTP (port 21). Open port scanning is typically performed using specialised tools that can quickly scan a range of ports and report which ones are open.

#### 

#### **Tools and Requirements**

* Browser
* Online port scanner (YouGetSignal)

#### 

#### **Scenario**

#### Anna is learning about network security and penetration testing. She has been assigned the task of scanning a server to identify open ports. This task will help her understand the importance of port scanning in the context of network security and how it can be used to uncover potential vulnerabilities. By identifying which ports are open, she can infer what services the server is running and assess their potential risks. For this exercise, Anna will use an online port scanner to perform the scan and gather information about the target server.

#### 

#### **Process**

1. Access YouGetSignal ( <https://www.yougetsignal.com/>).
2. Then, click on the port forwarding tester.
3. Enter the server IP address **202.63.241.174** on the remote address portion and perform a port scan on the right side.
4. After that

#### 

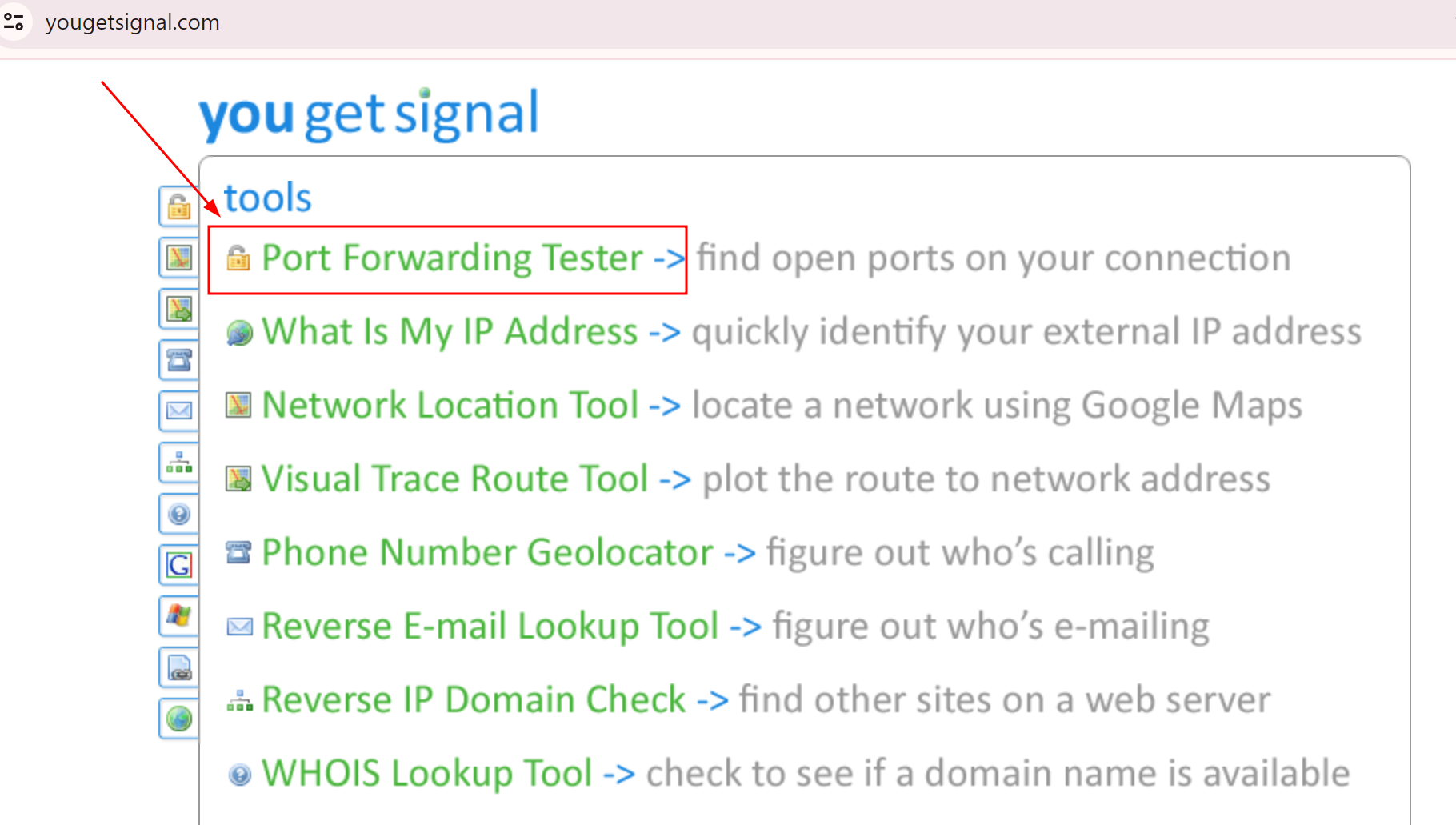
#### 

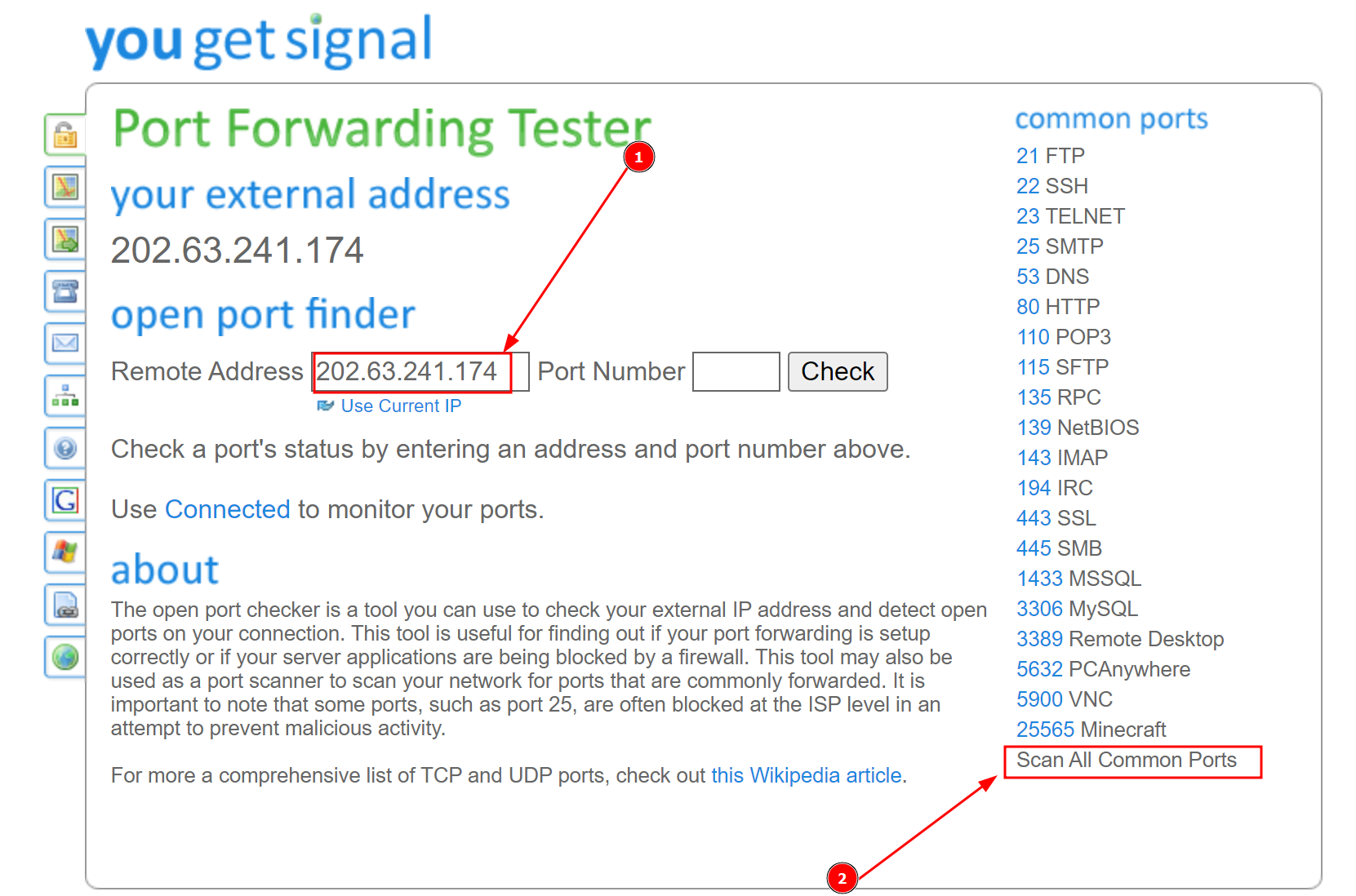
#### 

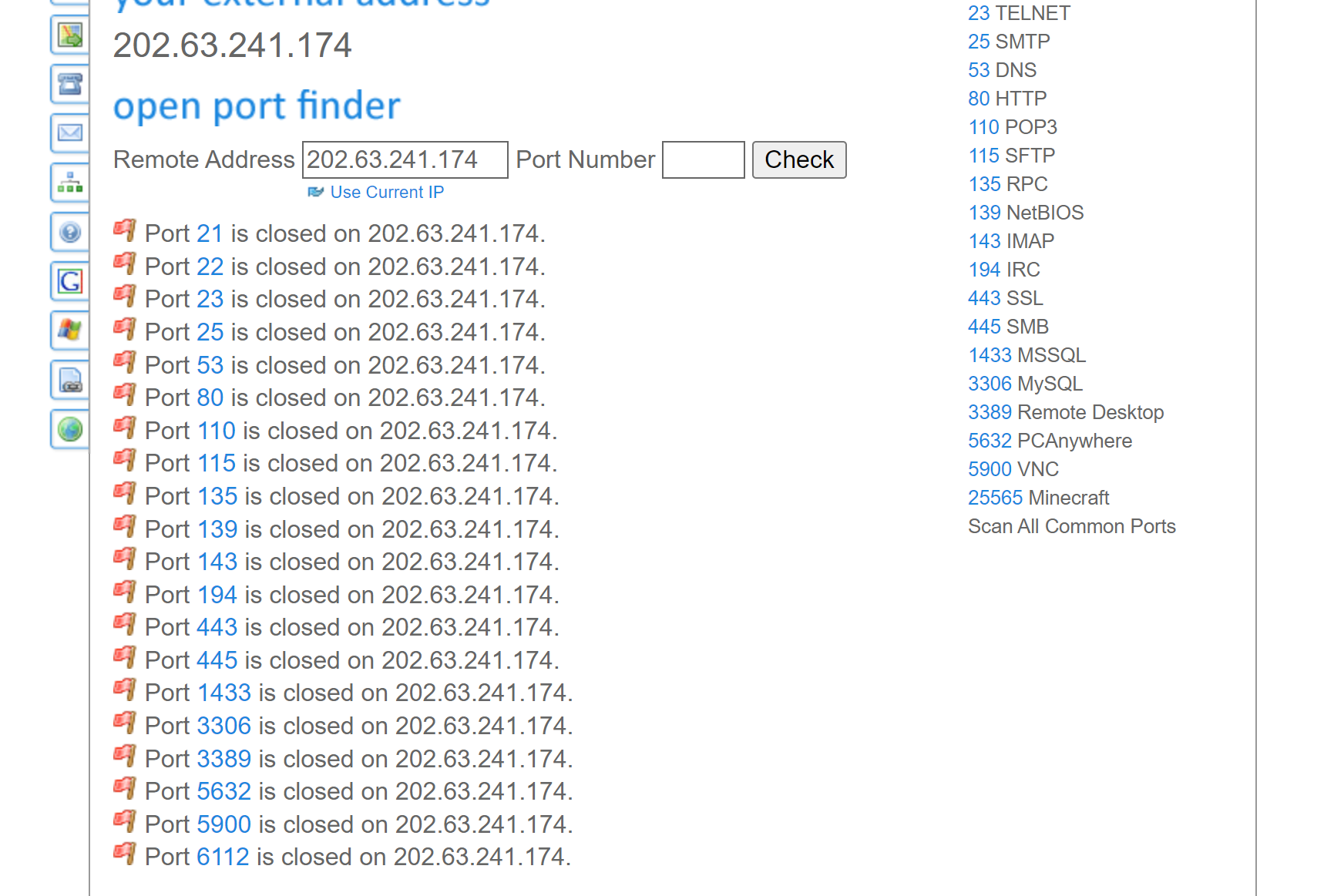
#### **Question**

* **Flag 1:** Are there any open ports found on the server?
  + **Answer:** No
  + **Flag Captured**.
* **Flag 2:** What service is running on port 80?
  + **Answer:** HTTP
  + **Flag Captured**.

**Hint**

****

****

****