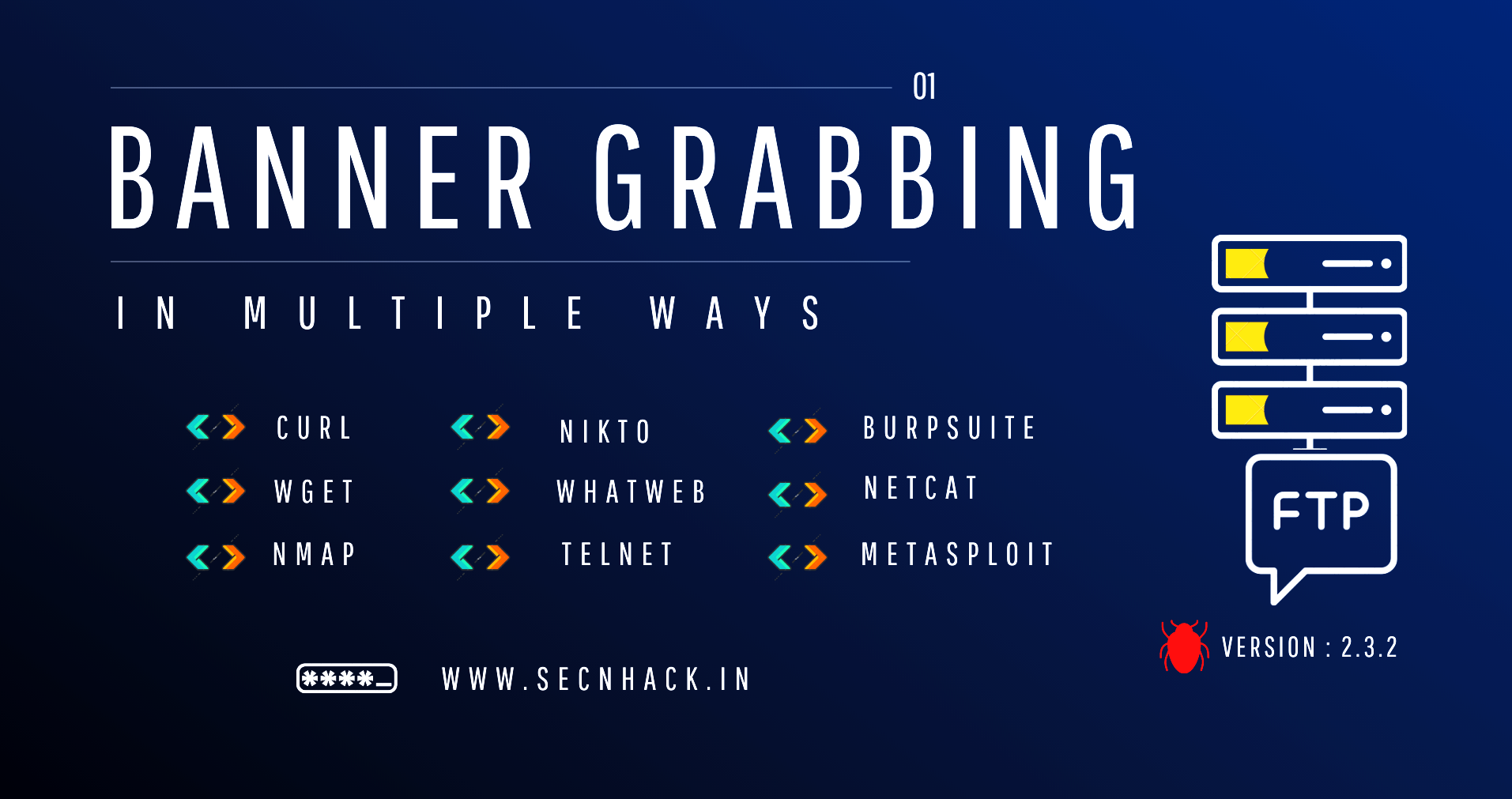
**CTF Topic: Banner Grabbing with HackerTarget**

****

**1. Introduction**

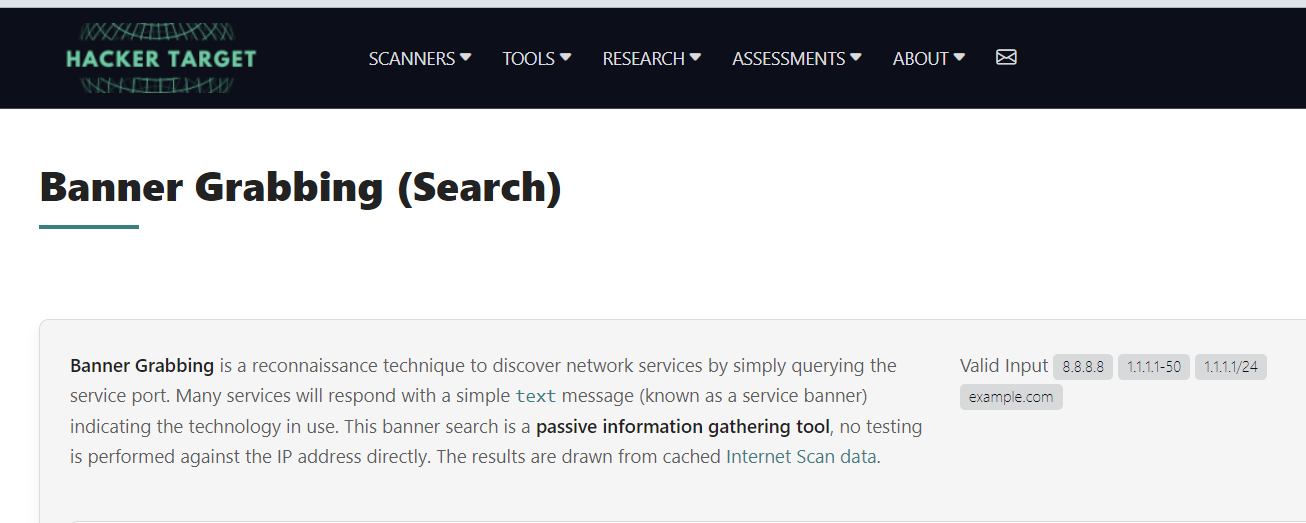
****

Banner grabbing is a technique used to gather information about network services by capturing banners or headers that servers send back when contacted. HackerTarget provides a web-based tool for performing banner grabbing across various services like HTTP, FTP, SSH, Telnet, SMTP, and more. This technique is essential for surveillance in cybersecurity to identify operating systems, software versions, and potential vulnerabilities.

**2. Tools and Requirements**

Access to [HackerTarget Banner Grabbing Tool  
- Web browser to access the tool [<https://hackertarget.com/banner-grabbing/> ]

**3. Scenario**

****

As a cybersecurity beginner, your task is to use the HackerTarget banner grabbing tool to analyze different services and answer questions based on the retrieved information. This exercise will help you understand the importance of banner grabbing in cybersecurity assessments.

**4. Process to Follow While Performing CTF**

**Step 1:** Go to the link and copy the ip address given in the information box. <https://traff.co/6fm03hg4>

**Step 2:** Visit the HackerTarget banner grabbing tool using the provided link: <https://hackertarget.com/banner-grabbing/>

**Step 3:** And perform banner grabbing on various services. Answer the following questions based on your findings.

**Questions**

**Flag 1: What is the banner information retrieved from an HTTP service running on 8.8.8.8.com?**

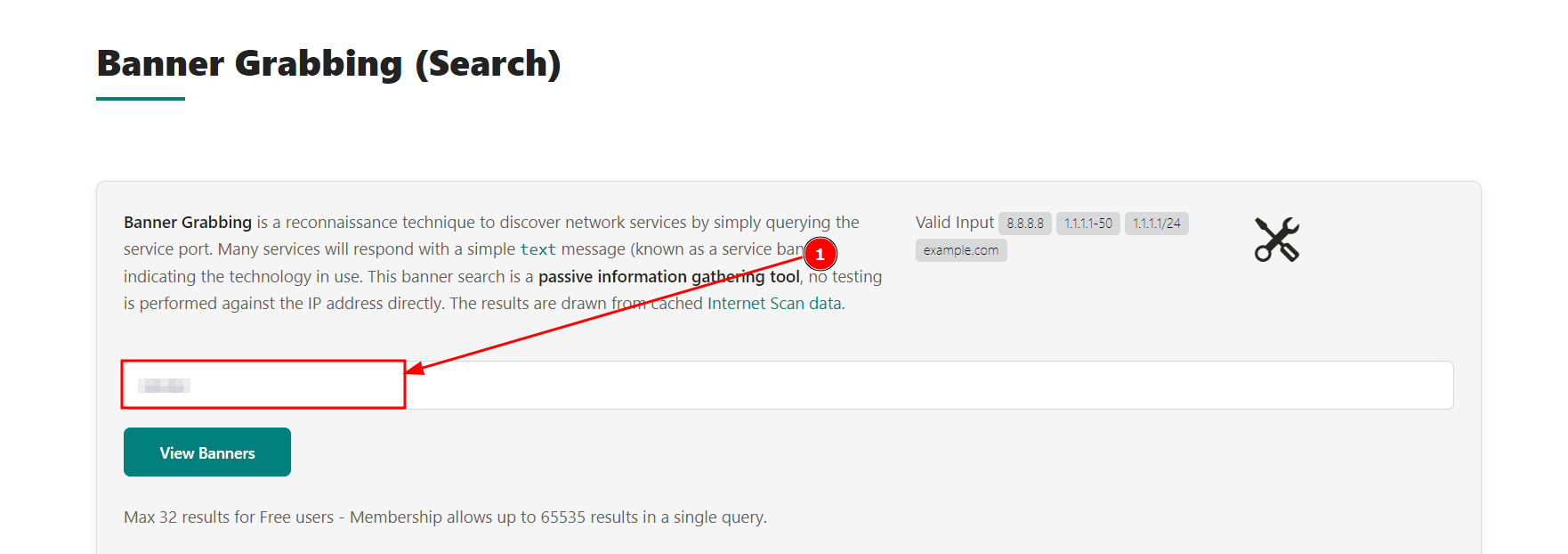
**Answer: HTTP 302 Moved**

**Flag 2: What is the HTTP CN used?**

**Answer: dns.google**

**Flag Captured.**

Hint





Use the HackerTarget banner grabbing tool to connect to different services and analyse the banners returned. Pay attention to the information provided in the banners to answer the questions accurately.