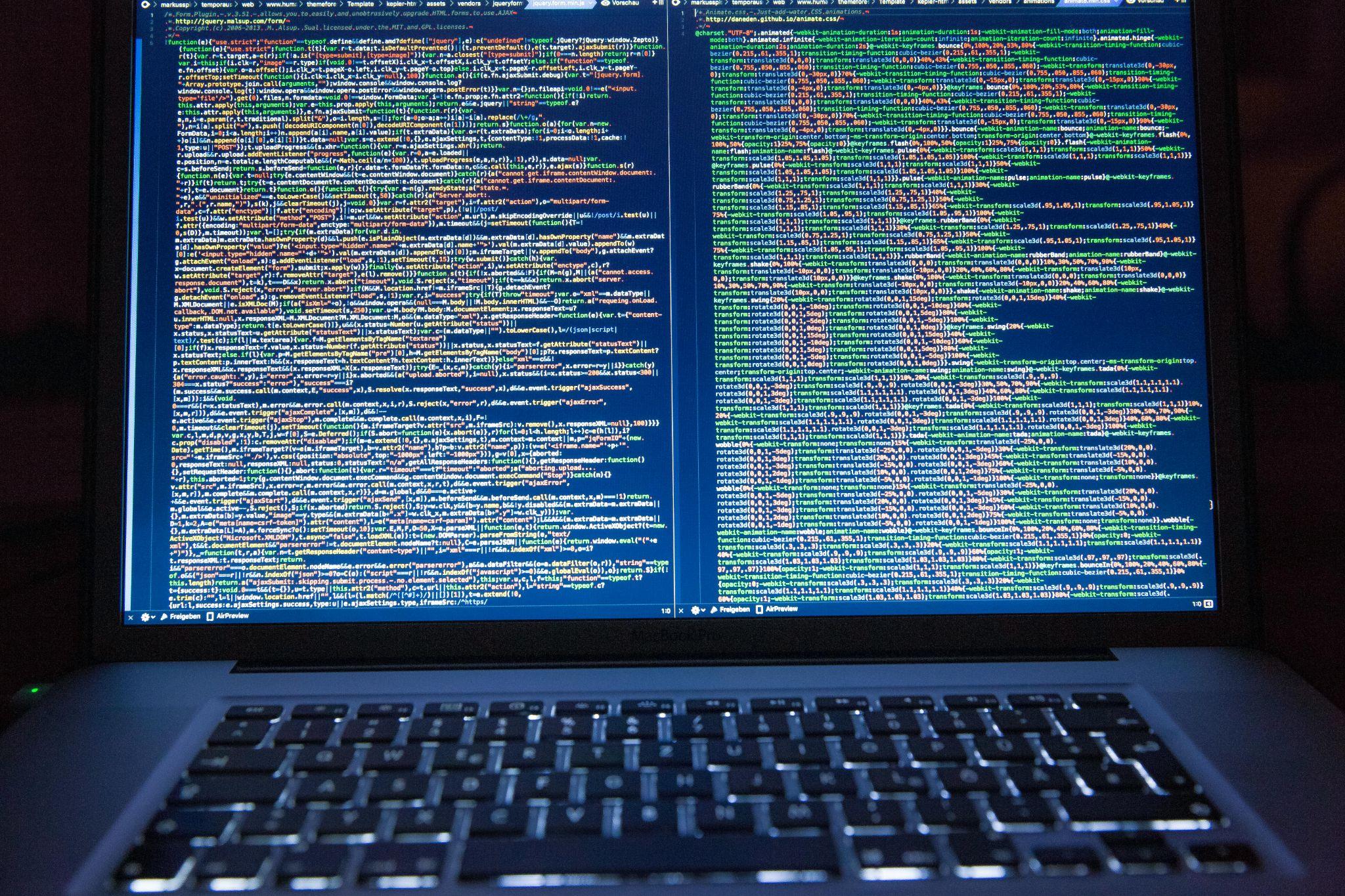
**CTF Challenge: Ethical Hacking - Using HackerTarget.com**



# **1. Introduction**



HackerTarget.com provides a suite of online tools for network reconnaissance and scanning. This challenge will introduce you to using these tools to gather information about a target server.

# **2. Tools and requirements**

Access to the internet and open **Hacker target**  website

# **3. Scenario**



You are an ethical hacker tasked with gathering information about a target server using the online tools provided by HackerTarget.com. Your job is to perform a basic scan and report on the open ports and services.

# **4. Process to follow while doing CTF**

* Go to the Browser and click on the provided link: [**https://hackertarget.com/**](https://hackertarget.com/)
* Navigate to the scanners drop down menu and click Nmap Online Port Scanner.
* Enter the IP address **44.228.249.3** and perform the scan.
* Identify the open ports from the scan results.

# **5. Let’s Begin the Challenge**

**Flag 1: What are the open ports and services found for Provided IP Address using HackerTarget.com?**

**Answer: 80/tcp http**

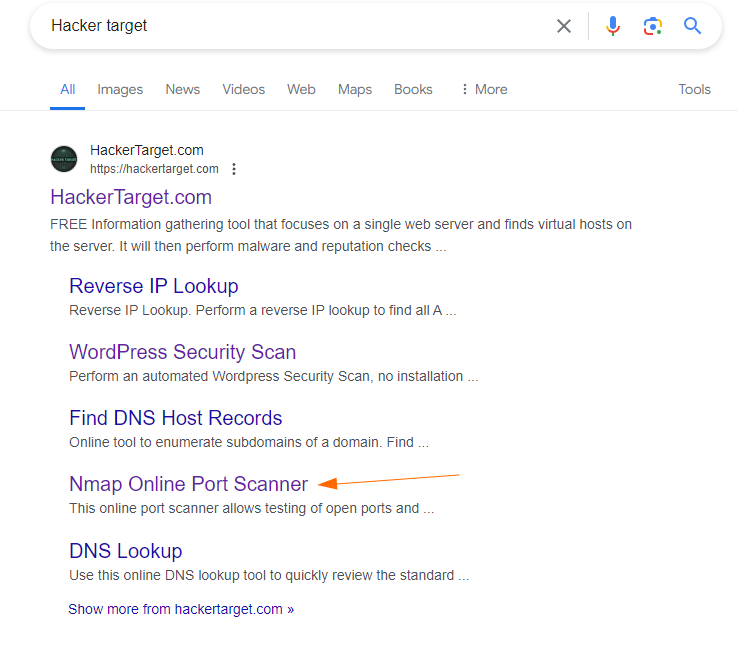
**Flag Captured**

**Flag 2: Which service is open on port 3389/tcp?**

**Answer: ms-wbt-server**

**Flag Captured**

**Hint:**



A screenshot of a computer program

Description automatically generated