**CTF: Network Scanning with Hacker Target’s Nmap Online Port Scanner**

A blue eye with a blue background

Description automatically generated with medium confidence

**Introduction**



HackerTarget's Nmap Online Port Scanner is a powerful tool used for network discovery and security auditing. In this challenge, you will use HackerTarget's Nmap Online Port Scanner to scan the IP address "104.26.8.250" and uncover information about open ports, services, and other network details.

**Tools and Requirements**

To perform this CTF, you will need the following tools and resources:

* A web browser (e.g., Chrome)
* HackerTarget's Nmap Online Port Scanner: <https://hackertarget.com/nmap-online-port-scanner/>
* The target IP address: 104.26.8.250

**Scenario**

****

You are a cybersecurity analyst tasked with evaluating the network security of a target IP address. Your mission is to use HackerTarget's Nmap Online Port Scanner to scan the IP address "104.26.8.250" and answer specific questions based on the scan results.

**Process to Perform**

**Step 1: Visit HackerTarget's Nmap Online Port Scanner**

* Open <https://hackertarget.com/nmap-online-port-scanner/> in your browser.

**Step 2: Perform a Network Scan**

* Enter the target IP address "104.26.8.250" into the provided field.
* Initiate the scan and wait for the results to be generated.

**Step 3: Analyze the Results**

* Review the detailed report the Nmap Online Port Scanner provided about the target IP address.
* Look for open ports, services running on those ports, and any notable findings.
* Note any significant findings such as port numbers, service names, and vulnerabilities.

**Let's Begin the Challenge**

Let's dive into the challenge with the tools and techniques outlined above. Use HackerTarget's Nmap Online Port Scanner to scan the target IP address and document your findings.

**Questions**

1. What is the status of port 80 on the IP address 104.26.8.250?

- Answer: open

2. Which service is running on port 443?

- Answer: https

3. Is there any DNS service detected on the IP address 104.26.8.250?

- Answer: No

4. What is the IP address identified in the Nmap scan?

- Answer: 104.26.8.250

**Happy hunting!**

**Hint**

****