**Week 2: Network Commands & Tools**

**Objective:** Learn essential networking commands and tools.

**Task#03: Use Nmap to perform a network scan and list open ports on your machine.**

**Solution:**

The provided screenshot shows the results of an Nmap network scan initiated from a Kali Linux terminal. The command executed was nmap 192.168.213.128, targeting the local Kali Linux virtual machine itself.

Nmap successfully confirmed that the target host, 192.168.213.128, was "up" and reachable. The scan by default checks 1000 common TCP ports. In this instance, Nmap reported that "All 1000 scanned ports on 192.168.213.128 are in ignored states," meaning they were essentially closed.

However, despite the majority being closed, the detailed output clearly shows one significant open port: 22/tcp, which is associated with the "ssh" (Secure Shell) service. This indicates that the SSH server is running and listening for connections on the Kali Linux VM. The entire scan completed in 13.17 seconds, successfully identifying the status of the single scanned IP address. This result is typical for a Kali Linux installation, where few services are running by default for security, except for essential ones like SSH.

