**🧾 Cybersecurity Portfolio**

**Scan for Open Ports from a Remote Computer**

**🔍 Objective**

To simulate a rogue access point scenario by remotely connecting to a compromised internal device and scanning the internal network for open ports using Zenmap/Nmap. This tests how exposed the network is to internal threats.

**🛠️ Tools Used**

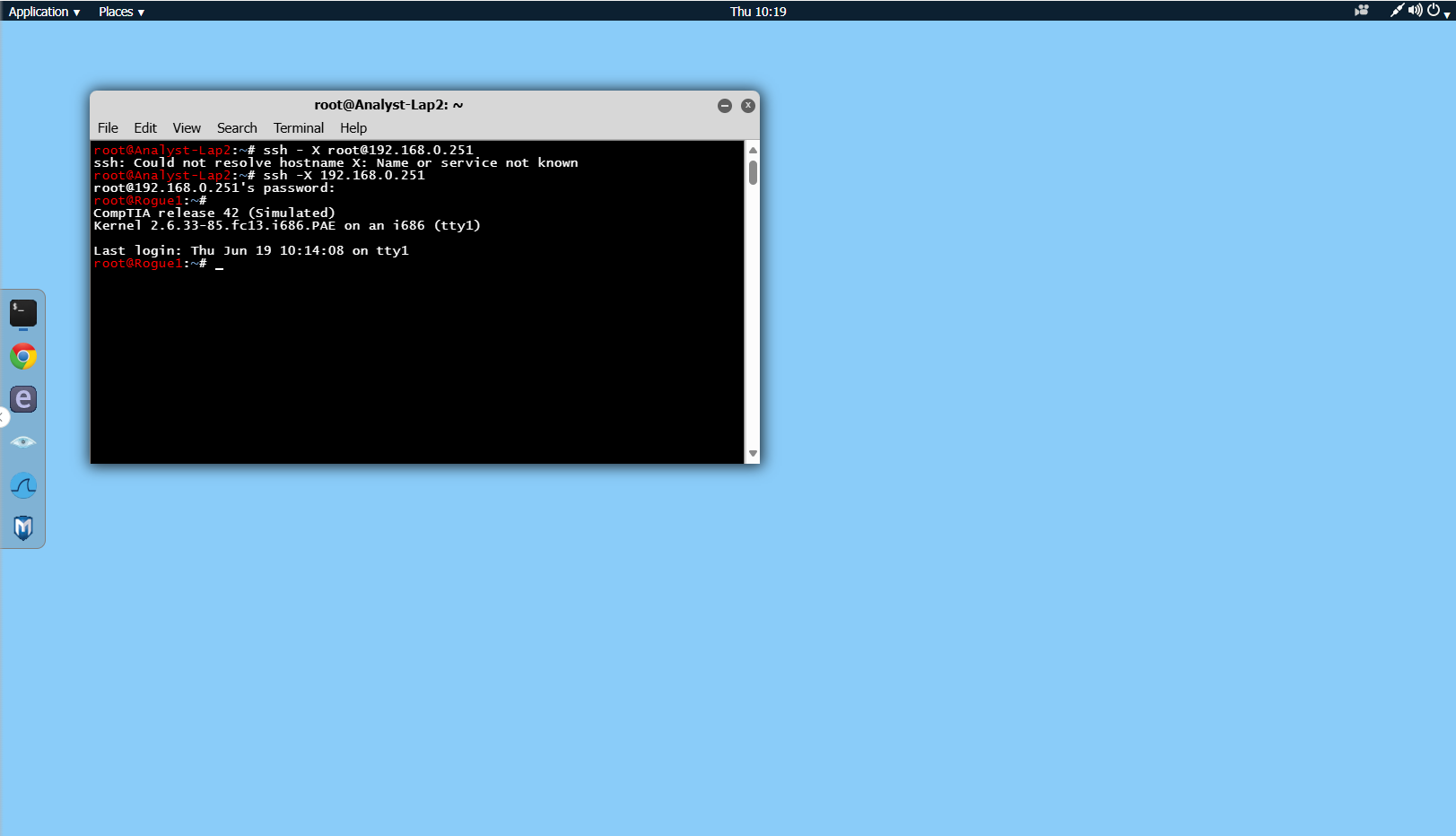
* Kali Linux (attacker machine)
* SSH
* Zenmap or Nmap
* Internal Rogue Computer IP: 192.168.0.251
* Target Subnet: 192.168.0.0/24
* Password for SSH: 1worm4b8

**📜 Steps Taken**

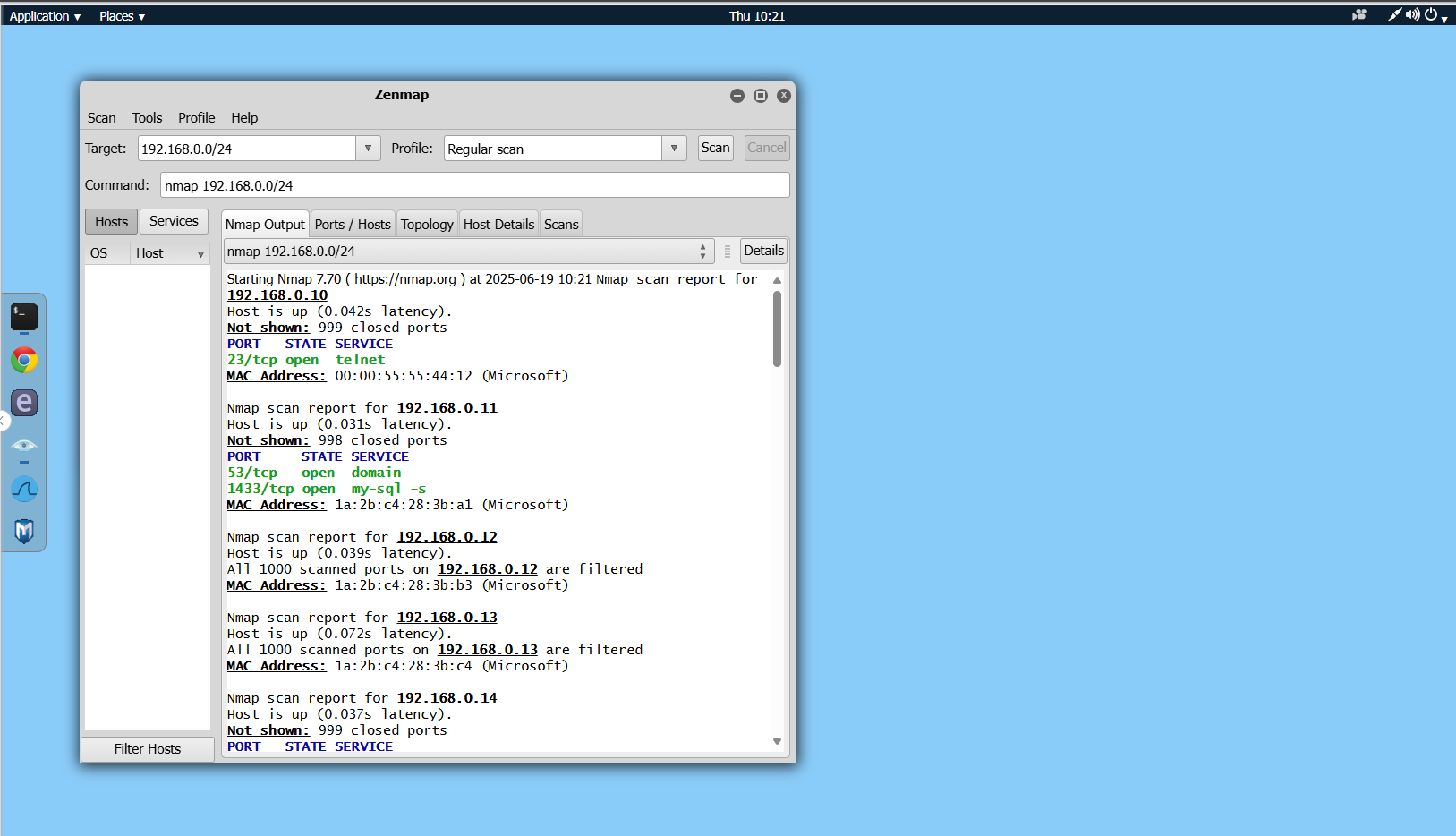
1. **Connected to the Rogue Computer:**
   * Used SSH to access the rogue system installed on the internal network:

ssh -X 192.168.0.251

* + Logged in successfully with the password 1worm4b8.



1. **Ran a Network Scan using Zenmap:**
   * Opened Zenmap on the rogue computer.
   * Set **Target** as 192.168.0.0/24.
   * Used scan profile: Intense scan, all TCP ports.



1. **Analyzed the Scan Results:**
   * Identified open ports and services for each host.
   * Looked for:
     + **HTTP (port 80)** to identify a **web server**
     + **Telnet (port 23)** to identify **unencrypted text communication**

**✅ Results**

* **Web Server Detected:**  
  192.168.0.15 had port **80** open, indicating it is hosting a web server.
* **Unencrypted Communication Detected:**  
  192.168.0.10 had port **23** (Telnet) open, which transmits data in cleartext and is considered insecure.

**💬 Reflections / Lessons Learned**

This lab highlights how dangerous a rogue device can be when placed inside a network. Even with no physical access, an attacker could identify critical systems and unencrypted services like Telnet. Regular internal scans and the disabling of insecure protocols are crucial to maintaining network security.