**🧾 Cybersecurity Portfolio**

**Perform Enumeration of MSSQL with Metasploit**

**🔍 Objective**

To identify which non-default TCP port Microsoft SQL Server is using on a target machine (192.168.10.14) by utilizing Metasploit’s MSSQL scanner module. This helps detect hidden services that may have been moved from their standard ports.

**🛠️ Tools Used**

* Kali Linux
* Metasploit Framework (msfconsole)
* Target IP: 192.168.10.14
* Metasploit Module: auxiliary/scanner/mssql/mssql\_ping

**📜 Steps Taken**

1. **Launched Metasploit Framework:**
   * In terminal:

msfconsole

1. **Selected the Correct Scanner Module:**
   * Entered:

use auxiliary/scanner/mssql/mssql\_ping

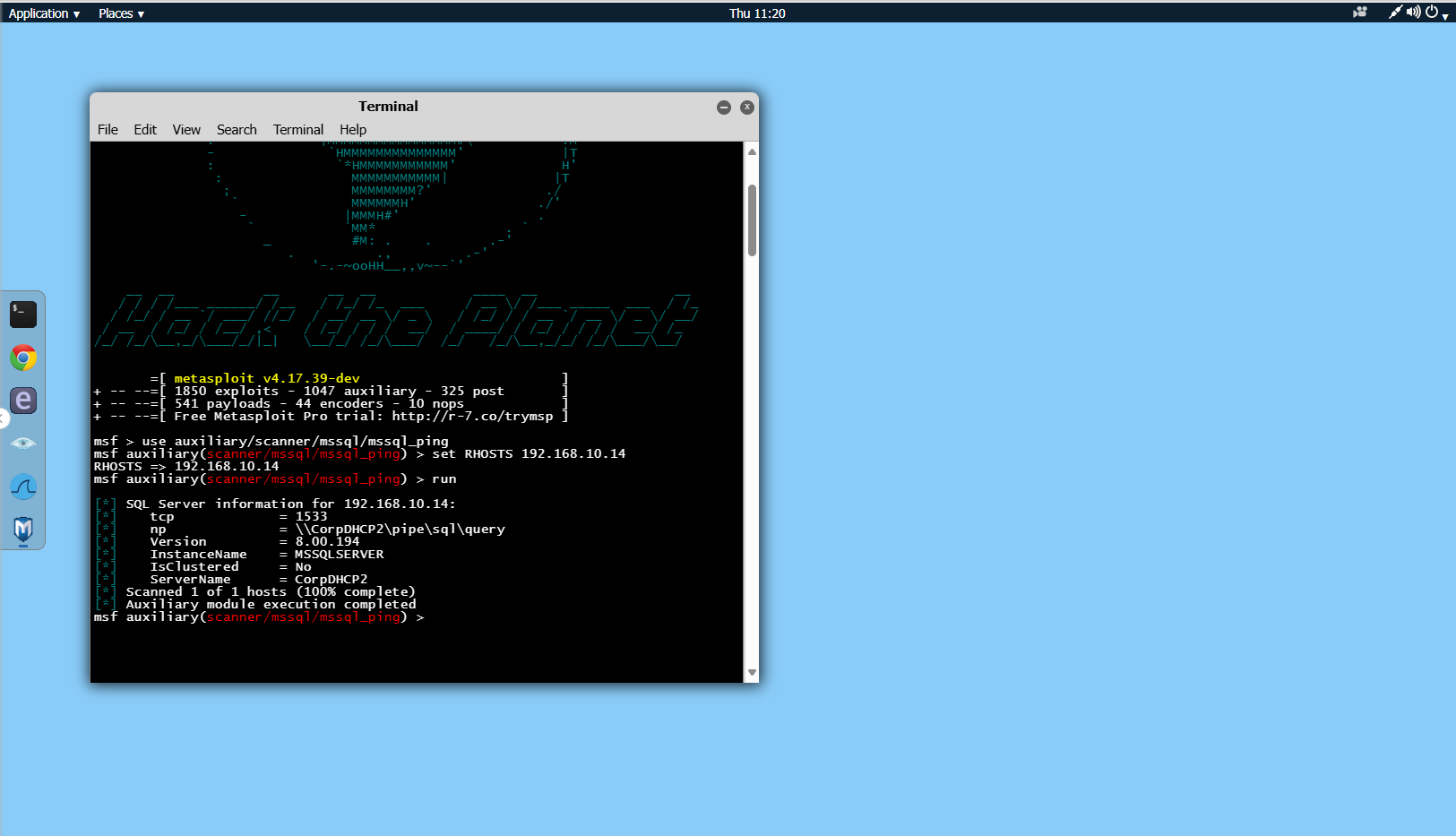
1. **Set the Target Host:**

set RHOSTS 192.168.10.14

1. **Executed the Scan:**

Run

1. **Interpreted the Results:**
   * The output indicated that the SQL Server was detected and provided the **specific TCP port** it was listening on **1533**



**✅ Results**

* **MSSQL Server Detected:**  
  The Microsoft SQL Server was found running on a **non-default port**.

**💡 Reflections**

This lab demonstrated how attackers or defenders can use Metasploit modules to enumerate non-standard services. MSSQL services running on alternate ports may be hidden from basic scans, but tools like mssql\_ping can still detect them through deeper analysis of protocol behavior.