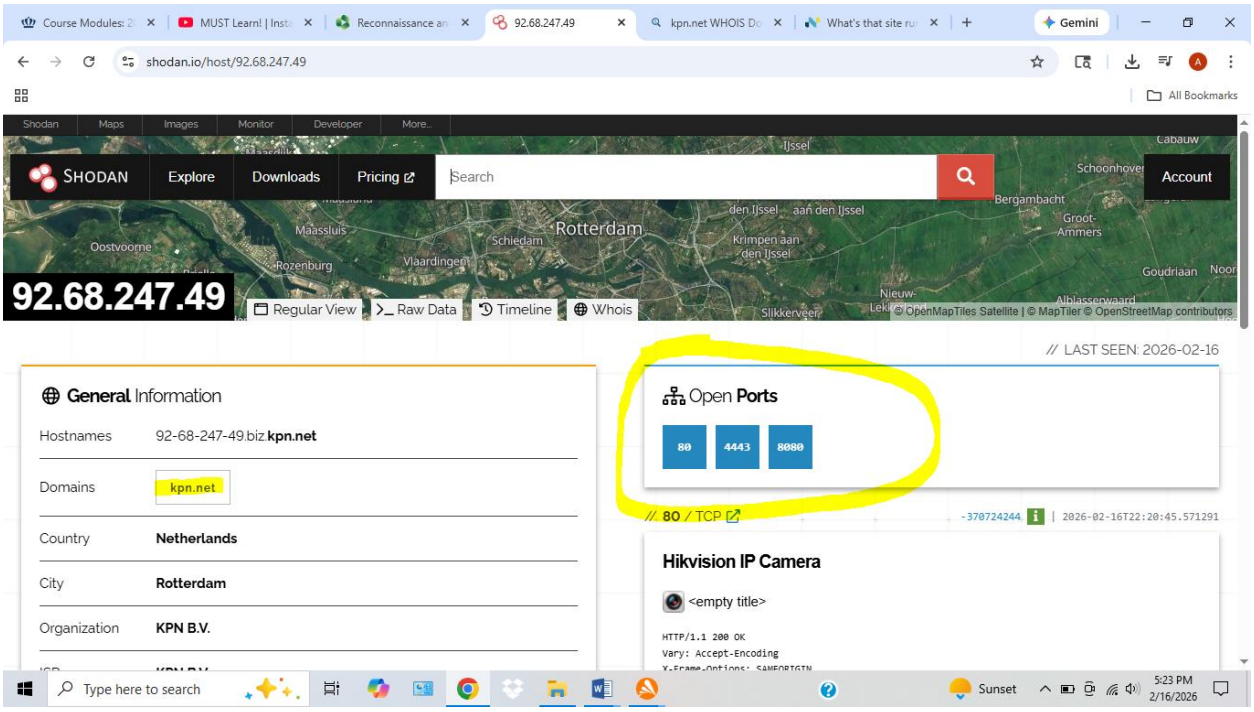
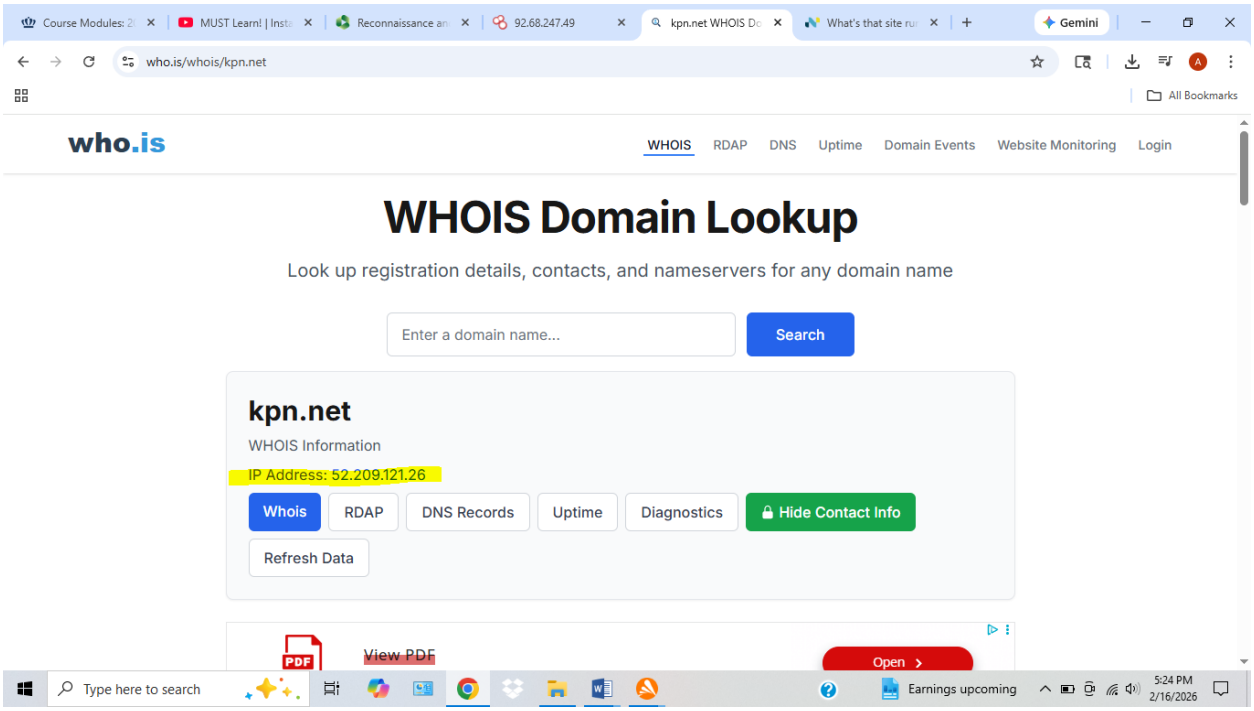
Lab 3 Passive Reconnaissance

Question 1:

Task 1:



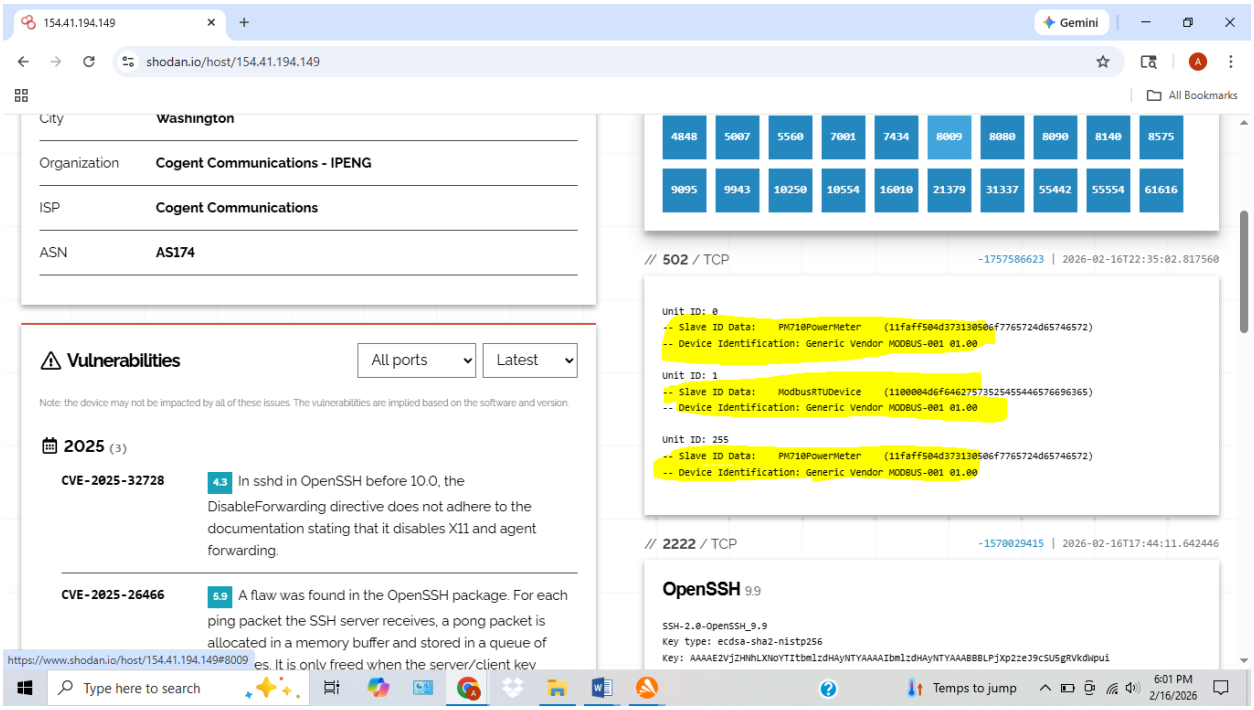
Task 2:

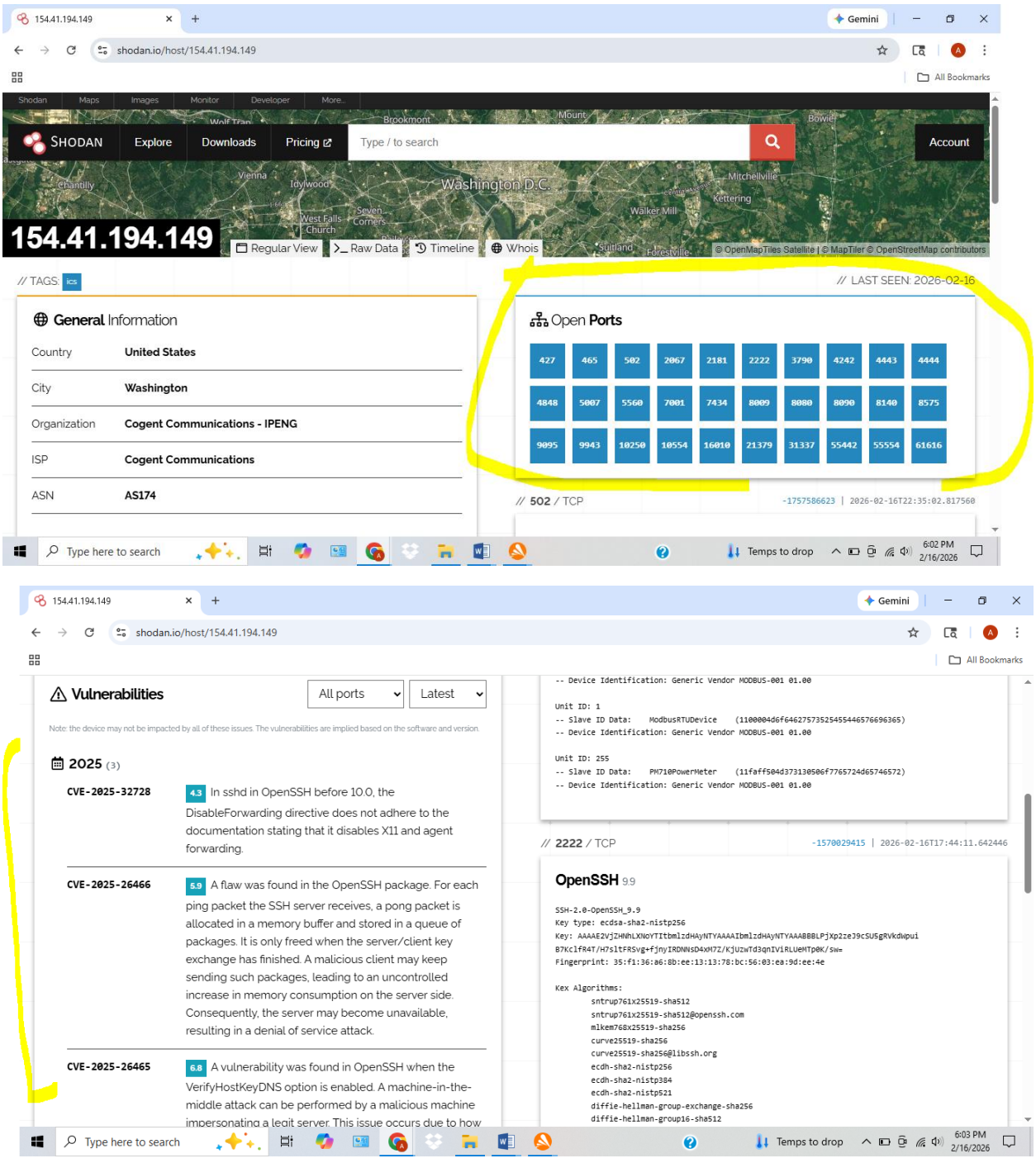


The IP addresses for the nameservers are exposed which can allow for attacks such as DNS spoofing or flooding of the nameservers. The registrar name being available can be a vulnerability because attackers can use the information for social engineering or finding vulnerabilities in the registrar's system. The expiration date of the domain being this year is a weakness because an attacker can prepare to take over the domain as soon as it expires.

Question 2:

Task 1:





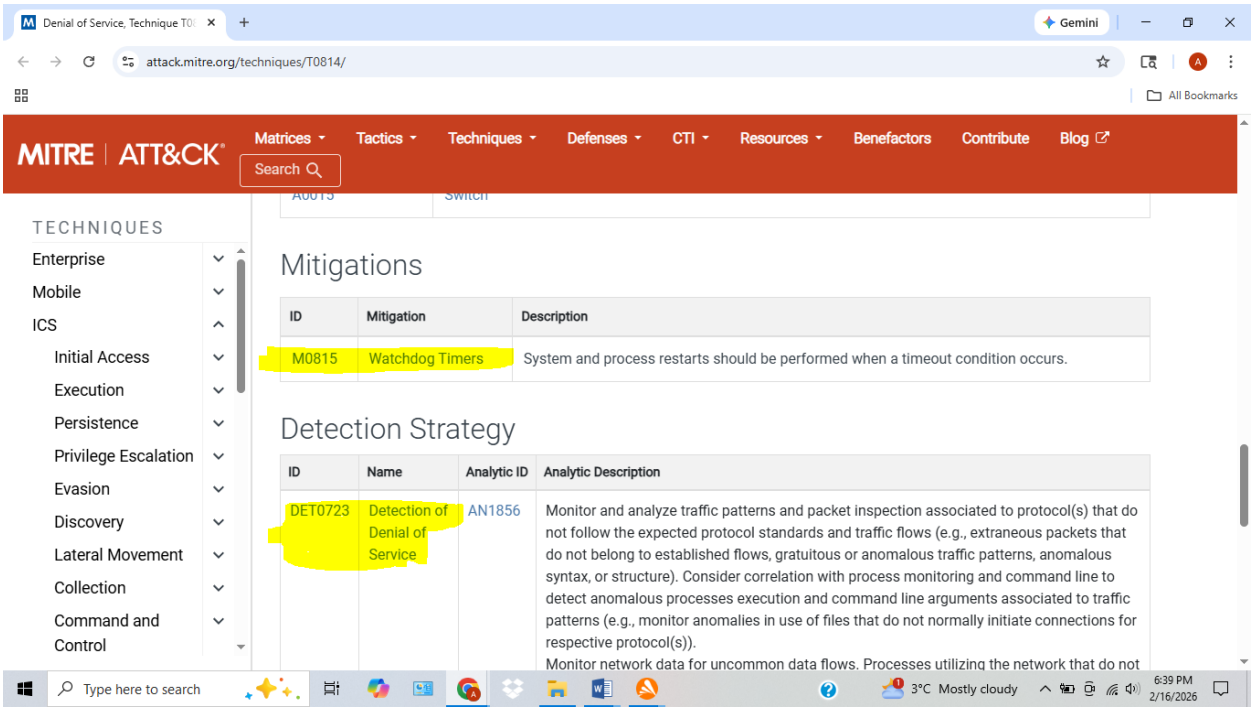
Task 2:

The device is a PM710 Power Meter that uses Modbus protocol and is manufactured by Schneider Electric. The power meter is part of the SCADA system. The power meter cannot encrypt or authenticate which results in the device being vulnerable to data theft and manipulation. Due to the lack of authentication, attackers can also modify and reconfigure the device for their own purposes. The device is vulnerable to denial of service attacks. The device

is very simple and is unable to filter the packets entering. Attackers will be able to flood the device easily with packets causing it to stop functioning.

Task 3:

The attack described in CVE-2025-26466 is a denial of service attack.



M0815 Watchdog Timers is a mitigation technique that uses watchdog timer devices. A watchdog timer allows the device to detect if a system is unresponsive. When watchdog timers are used, the organization can respond quickly to the attack. DET0723 Detection of Denial of Service involves monitoring the flow of traffic and the inspection of packets. Other aspects to monitor are application logging, network data, and operational data. The detection strategy monitors the device or system for any abnormalities which can indicate a denial of service attack is occurring.