Please utilize masscan and perform a complete on finding out what sensitive ports are open. The ports list are as follows:

Commonly Abused Ports

* Port 20,21 – FTP. An outdated and insecure protocol, which utilizes no encryption for both data transfer and authentication.
* Port 22 – SSH. Typically, it is used for remote management. While it is generally considered secure, it requires proper key management.
* Port 23 – Telnet. A predecessor to SSH, is no longer considered secure and is frequently abused by malware.
* Port 25 – SMTP. If not properly secured, it can be abused for spam e-mail distribution.
* Port 53 – DNS. Very often used for amplification DDoS attacks.
* Port 139 – NetBIOS. Legacy protocol is primarily used for file and printer sharing.
* Ports 80,443 – Used by HTTP and HTTPS. HTTP servers and their various components are very exposed and often sources of attacks.
* Port 445 – SMB. Provides sharing capabilities of files and printers. Used in the 2017 WannaCry attack.
* Ports 1433,1434, and 3306 – SQL Server and MySQL default ports – used for malware distribution.
* Port 3389 – Remote Desktop. Utilized to exploit various vulnerabilities in remote desktop protocols, as well as [weak user authentication](https://portal.alnafi.com/manage/courses/2970751/contents/61248252). Remote desktop vulnerabilities are commonly used in real-world attacks, with the last example being the BlueKeep vulnerability.

Please ensure that you only submit a single text file down below. Your grading will be assessed and those who pass the assignment will be informed in 6 weeks after submission.