The Different types of Ports with the vulnerability if they are open are:

- Port No 20 (FTP- Data):This is a port that lets user to send and receive files from servers
  The different attacks that can happen if it is open are:
  - Brute-forcing passwords
  - Anonymous authentication
  - Cross-site scripting
  - Directory traversal attacks
- Port No 21(FTP): This is also a port that lets users to send and receive files from servers
  The different attacks that can happen are:
  - Brute-forcing passwords
  - Anonymous authentication
  - Cross site Scripting
  - Directory traversal attacks
- Port No 22 (SSH):It is for secure shell(SSH). It provides secure access to the servers. Hackers can exploit port 22 by using the following:
  - SSH Keys
  - Brute-forcing credentials
- Port No 23(Telnet):This is a TCP protocol that connects users to remote computers.The vulnerabilities that can be performed are:
  - Credential brute-forcing
  - Spoofing
  - Credential sniffing
- Port No 25(SMTP):This is a simple mail transferring protocol port that is used for receiving and sending mails.The vulnerabilities that can be performed by are:
  - Spoofing
  - Spamming
- Port No 53(DNS):This is for Domain Name System(DNS).It's a UDP and TCP port for queries and transfers,respectively.This port is particularly vulnerable to:
  - DDoS
- Port No 69(TFTP):This is for booting UNIX or UNIX-like systems that do not have a local disk and for storing and retrieving configuration files for devices such as Cisco routers and switches.It is vulnerable to:
  - DoS Attacks
  - Password Spraying
- Port No 80(HTTP):HTTP stands for HyperText Transfer Protocol. They are generally used for sending and receiving encrypted web pages.It is the most widely used on web pages.It is generally vulnerable to:
  - SQL Injection
  - Cross-site Scripting
  - Cross-site request forgery
- Port No 110(POP3):It uses the protocol POP3 and is used for unencrypted access to electronic mails.The port is vulnerable to following attacks:
  - Brute force attacks

    - DoS
- Port No 123(NTP):The NTP stands for Network Time Protocol.It is used for synchronizing the clocks of computers and network devices in a network. It help to ensure time consistency.It has the following vulnerabilities:
    - DDoS
    - Time Spoofing
- Port No 143(IMAP):IMAP stands for Internet Message Access Protocol.It is a protocol used for accessing and managing email messages stored on a mail server.It unlike port 110 not only allows user to download and remove messages but also allows users to view,organize and manage their mails.The vulnerabilities that can be performed if left open are:
    - Man-In-The Middle Attacks
    - DoS
    - Brute-force attacks
- Port No 443(HTTPS):HTTPS stands for HyperText Transfer Protocol secured It is the most widely used on web pages.It is generally vulnerable to:
    - SQL Injection
    - Cross-site Scripting
    - Cross-site request forgery

.