Ports & Firewalls

Ports:

* MySQL: Port - 3306
* SQL Server: Port - 1433
* Oracle: Port – 1521
* Importance of knowing ports:
  + Security – Knowing the ports allows you to configure your firewall to only allow traffic on those specific ports.
  + Troubleshooting – If you encounter connectivity issues with your database, knowing the port can help diagnose the problem.
  + Configuration – Some applications require you to specify the port number when connecting a database.
  + Performance – Allows you to monitor ports to help identify bottlenecks and optimize resource allocation.
* Netstat findings:
  + SQL Server: PID – 5964
  + MySQL: PID - 5896
  + Oracle: PID – 5992
* List one port in use tied to ports that you didn’t know was running.
  + I didn’t expect my Fn keys on my laptop to be a process that has to run port - 9060

Firewall: Opening a database port on a firewall

**** Increased **Vulnerability:** Opening a database port exposes the database server to the internet, making it more vulnerable to unauthorized access. Hackers could attempt to exploit vulnerabilities in the database or launch brute force attacks to gain access.

**** Data **Breaches**: With an open database port, there's a higher risk of data breaches where sensitive information stored in the database could be compromised. This could lead to financial losses, legal repercussions, and damage to the organization's reputation.

**** Denial **of Service (DoS) Attacks**: Attackers could flood the database server with a high volume of requests, causing it to become overwhelmed and unresponsive. This could result in a denial of service (DoS) situation where legitimate users are unable to access the database services.

 Resource **Exhaustion:** Opening a database port could potentially lead to resource exhaustion on the server. If the server is not adequately configured to handle incoming connections, it could run out of resources such as memory, CPU, or network bandwidth, affecting the performance and stability of the system.