**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **11-July-2020** | **Name:** | **Bhuvanesh M** |
| **Course:** | **Coursera** | **USN:** | **4AL16EC015** |
| **Topic:** | **SQL data types** | **Semester & Section:** | **8th sem & ‘A’ section** |
| **Github Repository:** | **Bhuvan** |  |  |

|  |  |  |
| --- | --- | --- |
| **FORENOON SESSION DETAILS** | | |
| **Image of session** |
| **Types of Data**  Has data really changed? Well technically no, data generated by computers and digital devices is still groups of 1s and 0s. That has not changed. What has changed is the quantity, volume, variety, and immediacy of the generated data.  Historically companies would have access to our information gathered from forms, spreadsheets, applications, credit card purchases and other types of files. Much of the information was stored and analyzed at a later date. Sensitive data was still collected, stored and analyzed but, historically, hackers were more interested in hacking into systems to obtain corporate or government secrets.  Today, gathered data is taking on new characteristics. The digitized world has opened the floodgates for data gathering. IoT sensor-enabled devices are collecting more and more data of a personal nature. Wearable fitness trackers, home monitoring systems, security cameras, and debit card transactions are all collecting personal data as well as business and environmental data. Data is often combined from different sources and users may be unaware of this. Combining fitness monitoring data with house monitoring data could produce data points to help map the movements or location of a homeowner. This changing type of data collection and aggregation can be used for good purposes to help the environment. It also increases the possibility of invasion of our privacy, identity theft, and corporate espionage.  Personally identifiable information (PII) or sensitive personal information (SPI) is any data relating to a living individual that can be used on its own or with other information to identify, contact, or locate a specific individual. The data gathered by companies and government institutions can also contain sensitive information concerning corporate secrets, new product patents, or national security.  Because we are gathering and storing exponential quantities of both sensitive and informational data, it has increased the need for extra security to protect this information from natural disasters, hackers, and misuse. **Who Wants our Data?** **The Good Guys**  Legitimate companies have an agreement in place that gives them permission to use the collected data about you for purposes of improving their business. Remember those “Terms and Conditions” or “Terms of Service and Agreements” documents that we say yes to but do not usually read? The next time that you are presented with one, take the time to read through it. The contents might surprise you.  Other legitimate users of our data would be companies that use sensors on their own devices or vehicles. Governments that have environmental sensors, and cities who have installed sensors on trains, busses or traffic lights also have a right to the data they generate.  Some hackers, called white hat hackers, are paid by legitimate companies and governments to test the security of a device or system. Their goal is not to steal or modify data but to help to protect it.  **The Bad Guys**  Other hackers, called black hat hackers, want access to collected data for many nefarious reasons:   * To sell the information to a third party. * To modify the data or disable functionality on a device. * To disrupt or to damage the image of a legitimate company. * To access devices, web pages, and data to create political unrest or to make a political statement. * To access user IDs and passwords to steal identities. * To access data to commit a crime. * To hack into systems to prove that they can do it.  **Lab - Internet Fingerprint** The purpose of this lab is to introduce the aspect of “fingerprinting” an individual using the worldwide web. The objective is to introduce various methods to extract as much information as possible using only the Internet browser and various sites effectively. **Security Best Practices** Securing the network involves all of the protocols, technologies, devices, tools, and techniques that secure data and mitigate threats. Network security is largely driven by the effort to stay one step ahead of ill-intentioned hackers. Just as medical doctors attempt to prevent new illnesses while treating existing problems, network security professionals attempt to prevent potential attacks while minimizing the effects of real-time attacks. Networks are routinely under attack. It is common to read in the news about yet another network that has been compromised.  Security policies, procedures, and standards must be followed in the design of all aspects of the entire network. This should include the cables, data in transit, stored data, networking devices, and end devices. **Physical Security** Today’s data centers store vast quantities of sensitive, business-critical information; therefore, physical security is an operational priority. Physical security not only protects access to the premises, but also protects people and equipment. For example, fire alarms, sprinklers, seismically-braced server racks, and redundant heating, ventilation, and air conditioning (HVAC) and UPS systems are in place to protect people and equipment.  Figure one shows a representation of a data center. Select each circle for more information.  Physical security within the data center can be divided into two areas, outside and inside.   * **Outside perimeter security** - This can include on-premise security officers, fences, gates, continuous video surveillance, and security breach alarms. * **Inside perimeter security** - This can include continuous video surveillance, electronic motion detectors, security traps, and biometric access and exit sensors.   Security traps provide access to the data halls where data center data is stored. As shown in Figure 2, security traps are similar to an air lock. A person must first enter the security trap using their badge ID proximity card. After the person is inside the security trap, facial recognition, fingerprints, or other biometric verifications are used to open the second door. The user must repeat the process to exit the data hall. **Challenges of Securing IoT devices** IoT devices are developed with the necessary network connectivity capabilities but often do not implement strong network security. Network security is a critical factor when deploying IoT devices. Methods must be taken to ensure the authenticity, integrity, and security of the data, the path from the sensor to the collector, and the connectivity to the device. |