DAY -42, DAILY REPORT, 13- 01 -2022 (THURSDAY)

Today, I had an experience. When I woke up in the morning it gave me a positive vibe, and the cab came to the apartment and I went to the office. In the first session I had a meeting with a security team. After that I did my internship work. Redis is an open-source, highly replicated, performant, non-relational kind of database and caching server. It works **by mapping keys to values with a sort of predefined data model**. Mapped key-value-based caching system, almost comparable to memcached. The **ability to work with different types of data** is what really makes Redis an especially powerful tool. A key value could be just a string as is used with Memcached.All of the data is stored in RAM, so the speed of this system is phenomenal, often performing even better than Memcached. While Redis is **an in-memory (mostly) data store** and it is not volatile, Memcached is an in-memory cache and it is volatile. Also Memcached is limited to the LRU (least recently used) eviction policy whilst Redis supports six different policies: No eviction returning an error the memory limit is reached. Redis can be used with streaming solutions such as Apache Kafka and Amazon Kinesis as an in-memory data store to ingest, process, and analyze real-time data with sub-millisecond latency. Redis is an ideal choice for **real-time analytics use cases** such as social media analytics, ad targeting, personalization, and IoT. As Redis is an in-memory storage, you cannot store large data that won't fit your machine's memory size. Redis **usually works very badly when** the data it stores is larger than 1/3 of the RAM size. So,

this is the fatal limitation of using Redis as a database. Redis has two persistence mechanisms: RDB and AOF. RDB uses a scheduler global snapshotting and AOF writes updates to an append-only log file similar to MySql. You can use one of them or both. **Redis has low security on its own**, so it's important to set up a firewall. Setting up a proper firewall configuration will prevent any unauthorized incoming traffic. Some commands are considered dangerous and could be run by mistake or by an unauthorized user. In general, compliance is defined as the following rules and meeting requirements. In cyber security, compliance means creating a program that establishes risk - based controls to protect the integrity, confidence, and accessibility of information stored, processed or transferred. Security compliance in the context of IT security, compliance means ensuring that your organization meets the standards for data privacy and security that apply to your specific industry. In security compliance has different types like CIS controls (Center for internet security controls) and ISO - (International Organization for stamdardization) and HIPAA - Health Insurance protability and accountability) and HITECH - has the omni bus rule. PCI DSS - The payment card industry data security standards. The center for internet security (CIS) benchmarks are a set of best pratice in cybersecurity standards for the range of IT systems and products. CIS benchmarks provide the baseline configurations to ensure compliance with industry - and agreed cybersecurity

standards. That's all about today, thank you.