8.6.11 NoSQL Security Facts

A *NoSQL* (Not Only SQL) database is a type of non-relational database designed to deal with big data storage and retrieval. NoSQL uses different terminology than traditional relational databases, such as Microsoft SQL and MySQL. For example:

NoSQL Term	SQL Equivalent Term
Collection	Table
Document	Record
Field	Column

In a typical NoSQL database, a collection holds one or more documents, and each document can have one or more fields.

Because NoSQL is a newer database architecture and less mature than traditional SQL, there are several key security issues that you need to be familiar with:

- Most NoSQL database implementations do not require authentication by default, even for the admin user. User account passwords must be manually configured after installation by the database administrator. Otherwise, anyone can access the database and view the information it contains without supplying a password.
- In most NoSQL database implementations, any logged in user can access every collection on the server by default. The database administrator must manually configure access controls to prevent unauthorized access to the information in the database.
- Most NoSQL database implementations do not implement data encryption for either data at rest or data in transit.
- Because NoSQL does not support most aspects of the SQL language, NoSQL databases are less susceptible to SQL injection attacks when compared to traditional SQL database implementations.

To harden a NoSQL implementation, perform the following:

- Configure user accounts and assign strong passwords to them.
- Disable anonymous access and require authentication.
- Configure access controls to restrict access to data based on user account.
- Encrypt data using an Application-layer protocol prior to saving it in the database.
- Encrypt data in transit using SSL.
- Because of its minimal security controls, NoSQL database servers should only be implemented in a hardened, secure environment protected by traditional network security mechanisms such as firewalls, VLANs, and ACLs.