Cybersecurity Assignment 3

Name: Deep Ghadiyali

Roll Number: CS17B011

Q2. Explain differences between DES and Blowfish.

- DES and Blowfish both are symmetric block cipher.
- In DES, the key size is 64 bits from which 56 bits are used. Blowfish can use huge keys and so, it is more secure and provides a good encryption rate.
- In DES, block size is 64 bits and in Blowfish block size varies from 32 bits to 448 bits.
- DES is based on Fiestel network, so is Blowfish but with larger S-boxes
- DES was designed for hardware whereas Blowfish was designed for software.
- Blowfish is significantly faster than DES.

Q3. Point out commonalities and differences with Microsoft SSLDC and OWASP SAMM.

- The Security Development Lifecycle (SDL) consists of a set of practices that support security assurance and compliance requirements. The SDL helps developers build more secure software by reducing the number and severity of vulnerabilities in software.
- Microsoft SSLDC goes through six different phases:
  Training, Requirements, Design, Implementation, Verification, Release and Response.
- OWASP SAMM defines business functions as:
  Governance, Design, Implementation, Verification, Operations with its standard practices.
- They are prescriptive methodology.
- These approaches acknowledge that everyone on the team should be aware of the importance of security and also basics of security engineering.
- Governance includes Strategy & Metrics, Policy & Compliance, Education & Guidance. In Microsoft SSLDC Training phase include education and guidance part and other parts are not mentioned.
- SDL has two additional testing activities:
  - The security pushes
  - The final security reviews.

- In the Implementation, testing and Verification phase, SDL focuses more on SDL testing while emphasizes more on white box testing.
- SAMM supports the complete software lifecycle and is technology and process agnostic.
- SAMM is built to be evolutive and risk-driven in nature, as there is no single recipe that works for all organizations.