**Presentation topics**

**Database security:**

1. Using sqlmap to exploit sql injection
2. Sql injection to shell attack

**Malware analysis**

1. Mirai Botnet

**IDS/IPS**

1. Installation, Configuration and Demonstration of Snort IDS
2. Installation, Configuration and Demonstration of SnortSAM
3. Installation, Configuration and Demonstration of Suricata

**Ancient ciphers**

1. Substitution Ciphers (mono, poly-alphabetic, Vigenere cipher, One-time pad) -> Cryptanalysis
2. Transposition Ciphers (Rail Fence, Route, Columnar, Double transposition) -> Cryptanalysis

**Hash**

1. Cryptographic hash function features

* MD5,
* SHA

1. Message Authentication Code (MAC): NMAC, HMAC

**Symmetric-key Encryption**

**Block ciphers**

1. Feistel structure
2. DES
3. AES
4. Encrypting large message: ECB, CBC, CFB, …

**Public-Key Encryption**

1. Modulo arithmetic
2. RSA Algorithm, demo
3. Diffie-Hellman Key Exchange algorithm, demo