NETWORK SECURITY AND CRYPTOGRAPHY LAB

COURSE CODE:20CT1116

L	T	P	C
0	0	3	1.5

Course Outcomes: At the end of the Course the student shall be able to

CO1: Apply symmetric key cryptographic algorithms (L3)

CO2: Experiment with various asymmetric key cryptographic algorithms (L3)

CO3: Apply public key concepts to generate hash codes (L3)

CO4: Demonstrate intrusion detection mechanisms and network security attacks (L3)

CO5: Demonstrate web security analysis and SQL injection attacks (L3)

LIST OF EXPERIMENTS:

Implement the following techniques/algorithms:

1. Caesar Cipher
2. Hill Cipher
3. Simple-DES
4. RSA Algorithm
5. Diffie-Hellman Key exchange algorithm
6. SHA-1
7. Implement the NIST Digital Signature Algorithm

Demonstrate following mechanisms using Linux Platform (prefer kali Linux):

1. Exploit SQL injection flaws on a sample website.
2. Perform web security analysis on a sample website.
3. Demonstrate how to sniff for router traffic on a sample network.
4. Demonstrate Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
5. Assess Wi-Fi network security
6. Simulate and test, real-world phishing attacks
7. Demonstrate Intrusion Detection System (IDS)
8. Verify vulnerabilities, test known exploits, and perform security assessment on a given script file.

Additional Experiments (Optional) :

1. Implement Playfair cipher
2. Implement Simple-AES algorithm
3. Implement MD5 & SHA-512 algorithms

4. Explore the functionality of Kerberos package
5. Implement the dual signature concept in secure electronic transaction
6. Explore the features of Security-Enhanced Linux (SELinux)

TEXT BOOKS:

1. William Stallings, "*Cryptography and Network Security-Principles and Practice*" 7th Edition, Pearson Education, 2017
2. William Stallings, "*Network Security Essentials-Applications and Standards*", 6th Edition, Pearson Education, 2018

WEB-REFERENCES:

1. https://tools.kali.org/tools-listing
2. https://pypi.org/project/pykerberos/
3. https://github.com/SELinuxProject