EXPERIMENT LIST SH-2025

SECURITY LAB SEM : V

1. Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.
2. Poly alphabetic Substitution cipher using Play Fair & Vigenere technique.
3. Study the use of network reconnaissance tools like WHOIS, dig, traceroute, ns lookup to gather information about networks and domain registrars.
4. Study of packet sniffer tools wireshark: -. Observer performance in promiscuous as well as non-promiscuous mode. Show the packets can be traced based on different filters.
5. Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan,udp port scan.
6. Encrypt long messages using various modes of operation using AES or DES.
7. Cryptographic Hash Functions and Applications (HMAC): to understand the need, design and applications of collision resistant hash functions.(SHA 256 & SHA 512).
8. Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA.
9. Study of Keylogger attack using a keylogger tool.
10. Study of Network security tool Snort and study the logs

Subject in-Charge

(FARIDA ATTAR)