1. 1.Implement and test simple symmetric encryption algorithms like AES and DES
   2.Create a simple application vulnerable to buffer overflow and demonstrate how to exploit it.

2. 1.Implement RSA encryption to demonstrate the concept of public and private keys.
   2.Investigate the functioning of a rootkit and demonstrate techniques to detect it.

3. 1.Set up and configure a basic firewall using tools like iptables on Linux.
   2.Investigate the functioning of a rootkit and demonstrate techniques to detect it.

4. 1.Demonstrate DNS spoofing and DNS cache poisoning attacks.
   2.Set up a basic IDS like Snort and test its effectiveness in detecting different types of attacks.

5. 1.Set up a proxy server and demonstrate how attackers can use proxies to hide their tracks.
   2.Create a simple application vulnerable to buffer overflow and demonstrate how to exploit it.

6. 1.Perform SQL injection on a test website and then implement measures to prevent it.
   2.Implement an XSS attack on a test web application and demonstrate ways to mitigate such attacks.

7. 1.Implement and test simple symmetric encryption algorithms like AES and DES.
   2.Create a simple application vulnerable to buffer overflow and demonstrate how to exploit it.

8. 1.Implement RSA encryption to demonstrate the concept of public and private keys.
   Investigate the functioning of a rootkit and demonstrate techniques to detect it.

9. 1.Set up and configure a basic firewall using tools like iptables on Linux.
   2.Investigate the functioning of a rootkit and demonstrate techniques to detect it.

10. 1.Demonstrate DNS spoofing and DNS cache poisoning attacks.
    2.Set up a basic IDS like Snort and test its effectiveness in detecting different types of attacks.