Mini Project

Business Logic:

Nowadays, most companies are looking for penetration testers and ethical hackers to secure their networks and web applications from Black Hat Hackers. Most of the companies are doing projects on web applications and creating a network for start-ups. They perform penetration testing and hand over network reports to the client if the application or network is hacked. This helps the companies to understand the importance of cybersecurity and penetration testing.

Consideration/Scenario:

A web development company configured its network with many devices and started working on website development. They hired you as a penetration tester, and you need to perform penetration testing on all of their client's systems, mobiles, and websites. To test the systems' security, you must verify the system by creating a virus/trojans and injecting it into the system. This will help you analyze how the system is getting affected by the virus.

After these tests are completed, you also need to ensure that the information transferred through email by the employees of the organization is also safe. For that purpose, you need to perform data encryption and steganography techniques to hide the information.
Make a report of all the tests and share it with the administrator to take further actions.

To start with the testing, we need to gather information about the website. To do so, perform the below tasks:

1. **Information Gathering on Websites**
   - Create a lab with Oracle Virtual Box or VMware with Kali Linux OS, Windows 7, and Windows XP.
   - Gather information about Instagram (website).

After information gathering, we need to test the company's security network as well. To do so, we will test their local system and its operating system (operating system). So, we need to perform enumeration and penetration testing on the company system.

2. **Penetration Testing on System**
   - Test the Windows security using the ProRat and get access to the key logs. Delete the files from desktop or C drive and execute the commands to create a new folder in desktop and upload any file from your system.

Now, after testing the system/network, we must test the antivirus in their system. To do so, we will create a virus and inject it in their system to determine/exploit the vulnerabilities of it.

3. **Malware Creation, Exploitation, and Mobile Hacking**
    - Create a virus using Tetrabit Virus Maker and execute the virus in the victim machine.
    - Hack the mobile device using online tool MTF, gather the call list contacts, and access the camera.

After exploiting the system's vulnerabilities, we must also test and exploit the vulnerabilities of the client websites. To do so, we need to perform penetration testing and DOS injection attack on their websites.

4. **Website Penetration Testing**
    - Perform a DOS attack on windows 7 virtual machine using the LOIC tool and check the performance.
    - Test the website using BlindSQL to Bypass Admin panel Authentication manually for https://demo.testfire.net/ website.

After testing the systems and websites, one possibility that can steal sensitive information is from the communication medium, that is, email communications. We need to secure this transmission of messages by performing data encryption and hiding secret messages.

5. **Data Encryption, Decryption, and Hiding of Secret Messages.**
    - Hide the secret text file in the image using command prompts and SNOW tool.

Summary:

You will perform all the tests and create a report of the vulnerabilities found and provide it to the concerned department so that the loopholes can be fixed. Once this is done, you will help the company hide their secret information/conversations by encrypting the information and storing it in an image form.

Tools Covered in the Project:

- ProRat
- Tetrabit Virus Maker
- LOIC Tool
- Mobile Tracker Free (MTF)
- SNOW Tool
- Manual Footprinting and BlindSQL Authentication Injection