Major Project

Business Logic:

A few years ago, not many companies were aware of the need for Ethical hacking/penetration testing. With the increase in cybercrimes, nowadays, most of the companies have their focus on data security. Apart from developers and testers, the companies are now looking for ethical hackers or are giving their network/data security as a contract to other ethical hacking companies, who would perform penetration testing and other methods to protect and secure their data.

Consideration:

You are hired as a penetration tester in a company. You have been asked to secure their network, systems, employee mobiles, etc. To accomplish this, it is also important for you to determine the network's existing phase and understand the awareness of cybersecurity amongst the employees. To determine this, you need to perform phishing attacks on employees and gather all the necessary information. Later with this, you create awareness amongst the employee about the data-stealing that has taken place and how important it is to secure their network.

Now once you understood that the network is insecure and may have a lot of loopholes. You decide to test the network completely (systems, websites, and mobile phones). To do so, you perform penetration testing and find the vulnerabilities on the host's systems that are live and running.

After determining the loopholes, you need to create a detailed analysis report and share it with the concerned department to fix them.

Steps to Perform:

To determine the awareness amongst the employee, you must perform a phishing attack on them. As a part of a phishing attack, host a login page and send it to all the employees such that it seems original, and if anyone logs in to the website, you can gather their login credentials.

To accomplish this, follow the tasks given below:

Host a server and scan the network using various tools and commands.

- To determine the live system, to which you will be sharing the login phishing website, use the Advanced IP Scanner to scan the LAN network and find the systems connected to the same network. Also, determine their IP Address, System names, and MAC address.
- Use the WAMP server to convert a normal system to a server and host a login phishing website, using which you can capture the user credentials (Any website as per your wish)

After completing the previous task, you get the employee's login credentials, using which you create awareness amongst them about how data can be stolen using a phishing attack. By this, they understand that hackers can also steal the data sent through emails(online) in the same manner.

You need to perform system/network penetration testing to determine the security of the network and find out the vulnerabilities in the network. As a part of it perform the tasks below:

Scan the host and exploit the systems using Metasploit.

- Use the NMAP tool to scan the system in a network and find the ports opened and services running on machine and OS fingerprint.
- Perform testing on windows7 by Metasploit using reverse TCP payload, bypass the admin privileges, and change the administrator's password without knowing the old one.

Now once you are done with the system penetration testing and determined the loopholes, you perform website penetration testing and find the loopholes in the website that is hosted on their server. To do so, perform the tasks below:

Website penetration testing

- Hack the website by using Sql Injection on http://testphp.vulnweb.com/

Once you have determined the vulnerabilities on the website, you have to perform penetration testing to determine the security of the employees' mobiles. To do so, perform the tasks below:

Mobile Testing:

- Exploit an android mobile phone using Metasploit and access the camera. Take snapshots and download the images from mobile.

Once you determine all the loopholes, you have to find ways to secure the data transmitted through them using encryption and steganography. To do so, perform the tasks below:

Data Encryption tasks

- Try to extract the WinRAR file from the given image and extract email id, name, phone number, and IP address of the server and username and password from file.
- Decrypt the username and password of the database along with the IP address from the extracted file from Steganography task. Use cryptography online websites resources to crack the hashes.

These tasks will help you determine how to secure the transfer of sensitive data over the internet. This will also help you determine how to find the data, in case of any malicious data transferred using steganography.

Tools Covered in the Project:

- WAMP Server
- Advanced IP Scanner
- NMAP Tool
- Metasploit
- Data encryptions (Online)