Lab 9: Traffic Interception

Overview

One of the most important operations in Penetration Testing is traffic interception so we will learn how to intercept HTTPS traffic using Burp Suite, to do that we need to trust the Burp certificate as a system certificate, to trust any certificate as a system certificate we need a rooted device or a rooted emulator for example Genymotion, when you trust the certificate as a system certificate you can intercept HTTPS connections that don't use SSL pinning , and in case there is an SSL pinning we will disable it using Frida, in our hack app there are two connections the first one using HTTPS and the second using HTTPS with SSL pinning, now we will intercept these connections to get the flags

Steps

1. In the terminal navigate to labs > traffic_interception folder
    - you will find APk File which is hack.apk you can use it for this lab or open the Hack project in Android Studio and switch to the traffic_interception branch
      `git checkout traffic_interception`
      and build a new release app

2. Export the Burp certificate and install it in Android System
    - open burp and click proxy > proxy settings then export the certificate in der format and save it in the traffic_interception folder
    - now drag the certificate to your Android

3. install the certificate as a user certificate
    - In order to trust it in your Android go to the Settings > Security > Encryption & Credentials > then click install a certificate, select CA certificate, ANSTALL ANYWAY, and select the burp certificate from the downloads
    - now if you check the Trusted Credentials you will find it as a user certificate so you have to move it to the system certificates

4. Move the certificate to the system certificates store
    - go to the shell as a super user
      ```
      adb shell
      su
      ```
    - mount the system directories so you can move the certificate
      ```
      mount -o rw,remount /
      ```

- now move it from the user certificates to the system certificates store
  `mv /data/misc/user/0/cacerts-added/{certificate-name.0} /syatem/etc/security/cacerts`
- now you will find it in the Trusted Credentials as a system certificate

5. Configure the proxy setting

- open a new terminal in the traffic_interception folder and show the IP Address using this command
  - **for Windows**
    - `ipconfig`
  - **for Linux**
    - `ifconfig`
- from the result, copy the IP Address (IPv4)
- listen on this IP in burp, from proxy settings, and under the proxy listeners click add then select spicific address and define the same IP that you see in the terminal, also define the port to 8081
- config your Android to use the same IP and port number
  from the Wi-Fi setting click on the edit icon, then proxy and select manual, now enter the IP and the port

6. Intercept HTTPS using Burp

- now we can intercept the HTTPS connection just send the first request using HTTPS
- in burp check HTTPS history you will find the request which is a call to info API method, click on it to show the response
- great, the flag is in the response, use it to access the Info Activity
  now we have solved the CTF challenge level 4

7. Bypass SSL pinning using Frida

- if you send the second request, burp will not be able to intercept it because of SSL certificate pinning so we will use frida to disable this certificate check
- run frida server, from the shell navigate to the tmp folder
  `cd data/local/tmp`
  and run it
  `./frida-server &`

- after that, open the JavaScript file which is disable_ssl.js and go to the Frida CodeShare from this link copy the code and paste it into the script then save the file
- now run frida and pass the script
  `frida -U -l disable_ssl.js -f com.afif.hack`
- it will launch the app and will listen for the SSL pinning classes and methods so when SSL verification starts it will hook it to bypass SSL pinning

8. Intercept HTTPS & SSL using Frida & Burp

- now we can intercept the second connection because frida disabled SSL pinning, send the request using HTTPS + SSL
- check HTTPS history you will find the request which is a call to infossl API method
- great, the flag is in the response, use it to access the Info Activity as in the previous challenge now we have solved the CTF challenge level 5, which is one of the most important challenges in Android Penetration Testing