Traffic module using Android X86 emulator

It modifies some files of traffic module to deploy the platform by using the emulator Android X86, which is able to operate with the proxy configured in transparent mode.

Prerequisites

An internal network between the host machine and the emulator needs to be created. Follow this procedure or execute the script Config/config.sh

Pull image

1. Login to Docker Hub
   $ docker login
2. Pull the image
   $ docker pull dan2ysgl/privapp:demo

Run container

The following command will run the container:

```
docker run --network host -e LANG=C.UTF-8 dan2ysgl/privapp:demo
```

After the command has finished the control server will be listening in port 4000 of the local machine and the proxy will listen in port 8080.

Demo test

Use the traffic analysis wrapper (Config/traffic.py)

```
t = Traffic("192.168.1.50", "4000", "192.168.3.17", "/path/emoji.editor.apk")
        #Where: 192.168.1.50 and 4000 is the IP and port of your host,
192.168.3.17 is the emulator IP, and "/path/emoji.editor.apk” is the APK’s
path.
print(t.configure())#configure the target emulator IP and the target
application package name
print(t.upload()) #upload the target APK
print(t.phaseOne(10,False, False))  #start the capture of traffic by 10
seconds, grant_permissions =FALSE, reboot_before_capture = FALSE
print(t. analysis())
print(t. result())  #retrieve the results
```

Config files

api.conf

```
access_key: <ipstack access key>
fields: country_name,location.is_eu
```

categories

```
<category 1>: <PII type 1>;<PII type 2>;...
<category 2>: <PII type 3>;<PII type 4>;...
...
```

info.device

```
<PII type 1>: <PII 1>;<PII 2>;<PII 3>;...
<PII type 2>: <PII 4>
<PII type 3>: <PII 5>;<PII 6>
...
```

pinning_cases.js

```
Here new hook functions can be added to bypass further library-based
pinning implementations
...
```

inspect_request.py

```
One change from the original file:
- While in a physical device the command "netstat" shall be run with
root privileges, it is not necessary in Android X86, so 'su -c' has
been be removed from the function "configure".
...
```

start.sh

```
One change from the original file:
- Mitmproxy should be set to "Transparent" mode as the Android X86
emulator does not allow configuring an explicit proxy.
...
```