Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor & Associate Dean
School of Cyber Security and Digital Forensics
National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in

Objection Framework

- Objection is runtime mobile exploration toolkit built on top of frida which is used in Android and iOS pentesting.

- We can use Objection to perform numerous functions like SSLPinning bypass, root detection bypass, performing memory tasks, heap tasks and more without even being root/ jailbroken.

- However, it is to be noted that to take full advantage of all the functions it is recommended for **the device to be root.**

- some of the functions demonstrated will require root and some may not.

- It is recommended to test the application on a root device.

- Install Frida server in the Genimotion and client in the Kali Linux.

- Run the Frida serve in the genymotion and test Frida with kali Linux.

- Install objection

  Pip3 install objection

- Now, the packages (apps) installed in an android device are referred to as **gadget** in objection and to interact with an application to test, we'll have to inject our objection agent in the app. To do so:

  objection –gadget jakhar.aseem.diva explore

  ping // to check that target agent responds ok

  objection >> - - help // to see the help

  objection >> <tab> // to check the complete help

  objection >>   - - help android / ios /…..

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor & Associate Dean
School of Cyber Security and Digital Forensics
National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in