Instal·lar programes detectors de spyware i stalkerware

7-8 minuts

Objectius

1. Instal·lar MVT i ISDI per analitzar des d'un portàtil amb un gnu/linux, telèfons Android en cerca de programari espia.

   No és un objectiu d'aquesta guia, però pot servir per allisar el camí per:

1. instal·lar els programes en mac, o en distribucions de linux no basades en debian com fedora (família red hat) o manjaro (família arch linux).
2. analitzar iphones. No ho cobrim, però tots dos programes hi són compatibles
3. analitzar via backups. Només farem servir l'opció de fer-ho en viu en mvt. isdi ho fa només així.

Comparació de MVT i ISDI

	MVT	ISDI
Autores	Amnistia Internacional i CitizenLab	Cornell Tech, Cornell University, and NYU
Orientació	Spyware polític	Stalkerware masclista
Instal·lació	Més senzilla	Més complexa
Anàlisi	SMS, historial web, aplicacions, +	Aplicacions instal·lades
Desenvolup.	Molt actiu	A mig gas
Estabilitat	Bona	Algun error

0. Requeriments previs

- Un ordinador amb Linux. En concret la guia és per Debian i derivats, és a dir, Ubuntu, Linux Mint, Trisquel, Tails, etc.
- Permisos d'administradora. Sinó, les ordres que comencin per `sudo` no faran efecte
- Una mínima seguretat amb la consola o curiositat i ganes.
- Connexió a internet a l'ordinado, però no descarregarem moltes megues.

- Un mòbil amb Android.

1. Habilitem el mode de depuració d'Android

Per comunicar el portàtil amb el mòbil, tots dos programes fan servir l'eina `adb`, o Android Debug. Permet fer el mateix que podem fer nosaltres des del mòbil, però des del portàtil, de forma molt més ràpida i eficient. Per exemple, revisar quines aplicacions estan instal·lades, instal·lar-les o desinstal·lar-les si en tenim permisos, fer backups, etc.

Aquests programes fan servir la funció de llistar aplicacions instal·lades i de fer backups.

Seguim les instruccions que ens donen des d'Android per:

1. Des del menú de configuració del sistema, habilitem les opcions de desenvolupament
2. Dins del menú d'opcions de desenvolupament, habilitem la depuració /adb

2. Comprovem que podem connectar

Instal·lem adb:

```
sudo apt install adb
```

Connectem el mòbil al portàtil per USB, obrim una consola/terminal i escrivim:

```
adb devices
```

Hauríem de veure una cosa així:

```
$ adb devices
* daemon not running; starting now at tcp:5037
* daemon started successfully
List of devices attached
0a388e93      unauthorized
```

Si mirem la pantalla del mòbil, hauríem de trobar una notificació que ens demana permís per connectar amb el portàtil. Si li diem que si, i tornem a executar:

```
$ adb devices
List of devices attached
0a388e93      device usb:1-1 product:razor model:Nexus_7
device:flo
```

Si hem arribat aquí, quan tinguem instal·lats els programes al portàtil ja podran consultar informació del mòbil

Per permetre els següents programes connectar-se a través d'adb, n'aturem el servei:

```
adb kill-server
```

3. Instal·lem python i dependències genèriques

Tant MVT com ISDI estan fetes amb el llenguatge de programació python. Això condiciona com s'instal·len i com s'executen.

Obrim una terminal i instal·lem python i 2 paquets relacionats

```
sudo apt install python3 python3-pip python3-venv git
```

4. Instal·lem mvt

Per variacions d'entorn (com analitzant un iphone), consulteu les instruccions d'instal·lació

Instal·lem dependències del sistema:

```
sudo apt install libusb-1.0-0 sqlite3
```

Instal·lem mvt a través dels paquets de python:

```
sudo pip3 install mvt
```

Comprovem que funciona. Executem això:

```
mvt-android
```

I si ens surt un missatge de "Usage, Options, Commands", és que ja podem fer-la servir.

5. Executem mvt

Amb el mòbil connectat, fem

```
mvt-android check-adb
```

I estem antentes al mòbil per confirmar les sol·licitud de permís d'accés del portàtil al mòbil.

El mòdul d'anàlisi de sms ens farà saltar una sol·licitud de backup/còpia de seguretat, i li direm que sí, sense posar-li contrasenya. Així el programa podrà buscar enllaços maliciosos que haguem pogut rebre.

Trigarà una estona i anirà escrivint informació a la consola. La informació més interessant anirà prefixada per lletres en vermell com **WARNING**.

Fa diverses comprovacions, com quines aplicacions tenen permisos excessius, quines aplicacions estan instal·lades i des de quina font (google play, navegador, fdroid, etc), els sms per si contenen enllaços maliciosos, si el mòbil està rootejat, etc.

Per aprendre millor a interpretar els resultats, consulta la documentació oficial de mvt o contacta el teu col·lectiu hacktivista de confiança ;)

Per permetre els següents programes connectar-se a través d'adb, n'aturem el servei:

```
adb kill-server
```

6. Instal·lem isdi

Si voleu analitzar un Android, podeu saltar aquest pas. Només si voleu analitzar iphones, instal·leu:

```
 sudo apt install expect libimobiledevice-utils
ideviceinstaller ifuse
```

En descarreguem el codi:

```
git clone https://github.com/stopipv/isdi.git
```

Preparem l'entorn del programa:

```
# entrem a la carpeta
cd isdi

# preparem un entorn virtual de python
#+ per descarregar les dependències en aquesta carpeta
#+ i no en tot el sistema
python3 -m venv venv

# activem l'entorn virtual
source venv/bin/activate

# instal·lem les dependències del programa
pip install -r requirements.txt
```

Alerta! Si encara no han arreglat un error, en python 3.9 i superiors, hi ha dependències que fallen a l'hora d'executar el programa. Si és el cas, obriu l'arxiu de requirements.txt amb un editor de text i canvieu-ne les versions que necessitem. Ho podem fer així:

```
# canviem el requeriment
sed -i 's/Flask-SQLAlchemy==2.4.0/Flask-SQLAlchemy==2.5.1/'
requirements.txt

# i actualitzem
pip install -r requirements.txt
```

Finalment, podem executar el programa així:

```
TEST=0 ./isdi
```

Ens obrirà una finestra al navegador. Quan haguem acabat, aturem el servei d'adb per permetre a mvt o altres programes de connectar-se al mòbil:

```
adb kill-server
```

7. Fem servir ISDI

L'execució d'isdi des de la consola ens obrirà una pàgina web que existeix només en el nostre ordinador mentre tinguem la consola oberta.

Per analitzar un dispositiu Android, fem:

1. Seleccionem que és un dispositiu Android
2. Posem un nom al dispositiu, qualsevol
3. Piquem el botó verd que posa SCAN

Esperem una mica, i s'omplirà la taula amb totes les aplicacions instal·lades en el sistema.

La columna de Flags ens diu coses sobre l'aplicació:

- *System app* vol dir que no es pot desinstal·lar de normal, com Google Play.

- *Dual use* vol dir que per bé que pot tenir un ús legítim, es pot abusar per fer mal, com un enregistrador de trucades
- *Regex rules* vol dir que no està llistada, però que en el nom conté “spy” o “tracker”, que en general indiquen recollida de dades, com LG Health Tracker
- *Spyware* vol dir que l’aplicació és coneguda per ser explícitament orientada a espiar sense ser detectada.

  Alerta, algunes funcionalitats no funcionen:

- la creueta per desintal·lar, no fa res
- l’avís de si el mòbil està rootejat, està desactualitzat