

Proyecto Ciberseguridad Control remoto de un dispositivo Android ASIR

Proyecto fin de Ciclo Formativo

Autor: Orestes Palomino León



ÍNDICE DEL CONTENIDO:

- 1) Introducción al proyecto pág.2**
- 2) Objetivos del proyecto pág.3**
- 3) Ampliación de conceptos pág.4**
- 4) Explicación breve de la herramienta pág.5**
- 5) Requisitos necesarios Parte1 pág.6**
- 5.1) Requisitos necesarios Parte 2 pág.7**
- 6) Pasos realizados en las pruebas pág.8-22**
- 7) Opciones de la aplicación pág. 23-24**
- 9) Errores encontrados pág. 25-28**
- 10) Bibliografía utilizada pág. 29**

Introducción al Proyecto

Este proyecto con fines académicos está orientado a mostrar los conocimientos, tanto prácticos como teóricos, adquiridos a lo largo del grado.

El tema principal de este proyecto es la Ciberseguridad, aplicado en dispositivos móviles, nace de la necesidad de informar y demostrar las fortalezas y debilidades de los sistemas operativos para móviles Android, puesto que nuestros datos/conocimientos pueden ser objeto de manipulación para buscar un beneficio económico por ello o hacernos daño, hay un gran número de usuarios que utilizan este SO y están expuestos a los peligros de las redes sin muchas veces tener conocimiento de las vulnerabilidades que tienen.

Con este proyecto conseguiré tomar el control remoto de un dispositivo Android(móvil) con la ayuda de una herramienta de control remoto llamada L3MON.

Objetivos del proyecto

El objetivo principal de este proyecto es controlar de manera segura y rápida un dispositivo Android. Para ello haré uso práctico de una herramienta de control remoto llamado L3MON.

Esta herramienta estará instalada en una MV Debian con el SO Kali Linux.

Para establecer conexión remota con la app, utilizaré un servidor web (Nginx), conectándome vía localhost a la interfaz de la aplicación.

Para conseguir el control remoto de un dispositivo Android, una vez dentro de la aplicación, generaré un archivo APK que será instalado en el dispositivo víctima, pudiendo acceder a todo el sistema y controlar toda su información.

Toda esta práctica se realizará de manera didáctica y segura para poder gestionar el control absoluto de un dispositivo Android de la mejor forma posible.

Ampliación de conceptos

A continuación, haré un pequeño glosario de algunos conceptos interesantes utilizados en mi proyecto:

- a) Seguridad informática:** Disciplina que se encarga de proteger la integridad y privacidad de la información almacenada en un sistema informático de posibles ataques internos o externos, ya que, no existe técnica que asegure la inviolabilidad de un sistema. Se sustenta en 3 principios fundamentales: CIA(Confidencialidad-Integridad-Accesibilidad).
- b) Herramientas de control remoto:** Son instrumentos prácticos, utilizados para que mediante el control remoto de un ordenado se pueda resolver problemas/incidencias a distancia (Conexión a la nube, fallos de internet, errores en las cuentas, etc.). Sirven para realizar tareas de soporte técnico a distancia. No obstante, un mal uso de ellas puede considerarse delito y peligraría la integridad de éstas en el mundo de la seguridad informática
- c) RAT (Remote Access Trojans):** Son aplicaciones, aparentemente genuinas, que contienen malware y que pueden descargarse involuntariamente en un dispositivo, permitiendo el control absoluto sobre el dispositivo infectado. Afecta a los principios de la seguridad.
- d) Malware:** término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.

Explicación breve de la herramienta

Empezamos con la siguiente pregunta: ¿Qué es L3MON?, L3MON es una suite de gestión remota que nos permite acceder a cualquier smarthphone Android. También es considerado un RAT de Android (Herramienta de administración remota). ¿Cómo funciona la herramienta? Esta herramienta es gratuita y de fácil uso e instalación. Funciona de la siguiente manera: El usuario que la usa instala la herramienta en su ordenador y se conecta vía localhost a la interfaz web de L3MON. Una vez conectado, la herramienta se sirve de un generador de archivos maliciosos APK para poder tomar el control completo de un dispositivo. Una vez generado el archivo el atacante buscará la forma más rápida y eficaz de engañar a sus víctimas para que se descarguen dicho archivo y pueda controlar sus dispositivos móviles. Ya sea a través de una página web que simule ser una página de phishing, un mensaje promocional con un enlace malicioso entre otros métodos de captación. Este software está basado en JavaScript y utiliza una versión antigua de JAVA 8(version 1.8).

REQUISITOS NECESARIOS (Parte 1)

Para la realización de este experimento, dividiré los requisitos en dos partes:

1) Una MV con el SO Debian y la ISO de Kali Linux (versión actualizada) y que cumpla con el tipo de arquitectura que tengamos. La capacidad que utilizaremos es 2 GB.

1. Para una mayor comodidad podemos modificar los siguientes parámetros de la MV(Opcional):

a) En la opción SISTEMA, entramos a la opción Procesador y aumentamos el número de procesadores que nos permita, para una mayor velocidad del sistema (Utilizaré 2 procesadores).

b) En la opción PANTALLA, podemos subir la resolución gráfica de nuestra MV, aumentando la capacidad de la Memoria de vídeo y habilitando la opción 3D.

c) En la opción RED, modificamos el adaptador que mejor se ajuste a nuestras necesidades y prioridades (Opcional: Adaptador puente).

2) Para la instalación de la aplicación necesitaremos:

a) Una versión antigua de Java 8 (versión 1.8), ya que el generador de APK, no funciona con una versión reciente.

b) Esta aplicación trabaja con JavaScript y necesita el ejecutador de código JS, llamado NODE.js (tiene que estar instalado previamente).

3) Por último para la conexión remota utilizaremos un servidor web (Apache o Nginx). Utilizaré un servidor Nginx.

REQUISITOS NECESARIOS (Parte 2)

Si bien con los anteriores requisitos serían suficiente, podríamos tener algunos fallos con la paquetización de la ISO de KALI LINUX o con su instalación.

A continuación, escribiré los requisitos utilizados:

1) Para evitar posibles fallos, podemos utilizar una OVA de KALI LINUX sobre el SO Debian ya creada. Podemos descargarlas de Internet. Las características de la MV, serán iguales a las descritas anteriormente.

2) Para la instalación de la aplicación necesitaremos:

a) Una versión antigua de Java 8 (versión 1.8), ya que el generador de APK que utiliza no funciona con una versión reciente.

b) Esta aplicación trabaja con JavaScript y necesita el ejecutador de código JS, llamado NODE.js (tiene que estar instalado previamente).

3) Por último para la conexión remota utilizaremos un servidor web (Apache o Nginx). Utilizaré un servidor Nginx. Funciona en ambos.

PASOS REALIZADOS EN LAS PRUEBAS

A continuación, detallaré los pasos que seguí durante la fase prueba del proyecto.

1) Una vez instalada la MV con los requisitos mencionados anteriormente, iniciamos nuestra MV y empezamos con la configuración necesaria para la herramienta L3MON. Para hacer estas configuraciones, necesitaremos ser superusuario.



The screenshot shows a terminal window with a dark background. At the top, it displays the user 'root@kali: /home/orestes'. Below the prompt, the command '\$ sudo su' is entered. A message from the local System Administrator follows, stating: 'We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:' followed by a list of three items: '#1) Respect the privacy of others.', '#2) Think before you type.', and '#3) With great power comes great responsibility.' After this, the password for the user 'orestes' is requested with '[sudo] password for orestes:', and finally, the root prompt 'root@kali: /home/orestes' is shown again.

2) A continuación descargamos y actualizamos los paquetes de Debian pendiente. Esta tarea es recomendable siempre que podamos y trabajemos con un SO nuevo.

```
(root@kali)-[~/home/orestes]
# apt update
Des:1 http://kali.download/kali kali-rolling InRelease [30,6 kB]
Des:2 http://kali.download/kali kali-rolling/main amd64 Packages [18,2 MB]
Des:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [42,0 MB]
Des:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Des:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [158 kB]
Des:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [214 kB]
Des:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [1.006 kB]
Descargados 61,8 MB en 8s (7.271 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 1508 paquetes. Ejecute «apt list --upgradable» para verlos.

(root@kali)-[~/home/orestes]
#
```

```
Aplicaci... Lugares Terminal 9 de may 18:21
(root@kali)-[~/home/orestes]
# apt upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  fonts-roboto-slab gnome-screenshot libabsl20200923 libavif13 libfam0
  libgit2-1.1 libhttp-parser2.9 libllvm12 libmbedtls3 libmbedtls7
  libmbedtls12 libmbedtls14 libmbdx509-0 libmbdx509-1 libmms0 libmozjs-78-0
  libofao libperl5.32 libplacebo157 libpoppler102 libproj22 libwebrtc6
  libwmf-0.2-7 libwmf0.2-7 libx264-160 libyara8 perl-modules-5.32
  python3-ipaddr python3-mistune python3-singledispatch python3-twisted-bin
  ruby2.7 ruby2.7-dev
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  evil-winrm gcc-12-base gnome-bluetooth-common gnome-icon-theme
  libabsl20210324 libavif14 libflashrom1 libfreeaptx0 libftdi1-2
  libgweather-4-0 libgweather-4-common libicu71 libkf5syndication5abi1
  libldacbt-enc2 libldap-2.5-0 libldap-common libmbedtls7 libmbedtls14
  libmbdx509-1 libmozjs-91-0 libnma-gtk4-0 libopenh264-6 libosinfo-l10n
  libperl5.34 libplacebo192 libpoppler118 libproj25 libpskc0 libpython3.10
  libtiff5 libtiff5abi1 libtiff5dev libtiff5abi1abi1 libtiff5abi1dev libtiff5abi1abi1dev

$ _   _   _   _   _   _   _   _
```

3) Si queremos trabajar de forma remota con el repositorio, dónde se encuentra el programa, podemos clonarlo en nuestro sistema de archivos local. Después comprobamos si aparece.

```
[root@kali]~/home/orestes]
# git clone https://github.com/D3VL/L3MON.git
Clonando en 'L3MON'...
remote: Enumerating objects: 788, done.
remote: Total 788 (delta 0), reused 0 (delta 0), pack-reused 788
Recibiendo objetos: 100% (788/788), 18.77 MiB | 5.87 MiB/s, listo.
Resolviendo deltas: 100% (316/316), listo.
```

```
[root@kali]~/home/orestes]
# ls -l
total 36
drwxr-xr-x 2 orestes orestes 4096 may  9 18:16 Descargas
drwxr-xr-x 2 orestes orestes 4096 may  9 18:16 Documentos
drwxr-xr-x 2 orestes orestes 4096 may  9 18:16 Escritorio
drwxr-xr-x 2 orestes orestes 4096 may  9 18:16 Imágenes
drwxr-xr-x 7 root    root   4096 may  9 19:08 L3MON
drwxr-xr-x 2 orestes orestes 4096 may  9 18:16 Música
drwxr-xr-x 2 orestes orestes 4096 may  9 18:16 Plantillas
drwxr-xr-x 2 orestes orestes 4096 may  9 18:16 Público
drwxr-xr-x 2 orestes orestes 4096 may  9 18:16 Vídeos
```

4) Como cité en los requisitos necesitaremos instalar la versión de java 8. Continuamos con la instalación del paquete java 8. Usamos el siguiente comando.

```
[root@kali]~/home/orestes]
# apt install openjdk-8-jre
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete openjdk-8-jre no está disponible, pero algún otro paquete hace referencia
a él. Esto puede significar que el paquete falta, está obsoleto o sólo se encuentra disponible desde alguna otra fuente
Sin embargo, los siguientes paquetes lo reemplazan:
  nvidia-openjdk-8-jre

E: El paquete «openjdk-8-jre» no tiene un candidato para la instalación
```

Nota: La versión del manual que utilzo para la instalación de L3MON no está actualizado así que me sale esta captura.

5) Nos pedirá que instalemos el paquete disponible para la aplicación.

```
[root@kali] [/home/orestes]
# apt install nvidia-openjdk-8-jre
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
fonts-roboto-slab gnome-screenshot libabsl20200923 libavif13 libfam0
libgit2-1.1 libhttp-parser2.9 libllvm12 libmbcrypto3 libmbcrypto7
libmbdtls12 libmbdtls14 libmbdx509-0 libmbdx509-1 libmms0 libmozjs-78-0
libofa0 libperl5.32 libplacebo157 libpoppler102 libproj22 libwebp6
libwmf-0.2-7 libwmf0.2-7 libx264-160 libyara8 perl-modules-5.32
python3-ipaddr python3-mistune python3-singledispatch python3-twisted-bin
ruby2.7 ruby2.7-dev
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  nvidia-openjdk-8-jre
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 93 no actualizados.
Se necesita descargar 28,1 MB de archivos.
Se utilizarán 103 MB de espacio de disco adicional después de esta operación.
Des:1 http://http.kali.org/kali kali-rolling/non-free amd64 nvidia-openjdk-8-jre
  amd64 9.+8u312-b07-1-11.4.3-2+b1 [28,1 MB]
Descargados 28,1 MB en 3s (10,8 MB/s)
```

6) En caso de no tener instalado Node.js, lo instalamos y comprobamos la versión. Esta parte es opcional.

```
[root@kali] [/home/orestes]
# apt install nodejs
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
fonts-roboto-slab gnome-screenshot libabsl20200923 libavif13 libfam0
libgit2-1.1 libhttp-parser2.9 libllvm12 libmbcrypto3 libmbcrypto7
libmbdtls12 libmbdtls14 libmbdx509-0 libmbdx509-1 libmms0 libmozjs-78-0
libofa0 libperl5.32 libplacebo157 libpoppler102 libproj22 libwebp6
libwmf-0.2-7 libwmf0.2-7 libx264-160 libyara8 perl-modules-5.32
python3-ipaddr python3-mistune python3-singledispatch python3-twisted-bin
ruby2.7 ruby2.7-dev
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  libnode83 nodejs-doc
Paquetes sugeridos:
  npm
Se instalarán los siguientes paquetes NUEVOS:
  libnode83 nodejs nodejs-doc
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 93 no actualizados.
Se necesita descargar 11.3 MB de archivos.
```

```
[root@kali] [/home/orestes]
# nodejs -v
v14.19.1
```

7) Instalamos el gestor de procesos de nodejs(pm2). Esto nos permitirá controlar mejor la herramienta. Usamos el siguiente comando. Para que reconozca el comando nos pedirá que instalemos npm primero.

```
(root@kali)-[~/home/orestes]
# npm install pm2 -g
Command 'npm' not found, but can be installed with:
apt install npm
Do you want to install it? (N/y)
apt install npm
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
fonts-roboto-slab gnome-screenshot libabsl20200923 libavif13 libfam0 libgit2-1.1
libhttp-parser2.9 libllvm12 libmbcrypto3 libmbcrypto7 libmbedtls12
libmbedtls14 libmbedx509-0 libmbedx509-1 libmms0 libmozs-78-0 libofa0 libperl5.32
libplacebo157 libpoppler102 libproj22 libwevp6 libwmf-0.2-7 libwmf0.2-7
libx264-160 libyara8 perl-modules-5.32 python3-ipaddr python3-mistune
python3-singledispatch python3-twisted-bin ruby2.7 ruby2.7-dev
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
gyp handlebars libjs-async libjs-events libjs-inherits libjs-prettify libjs-psl
libjs-regenerate libjs-source-map libjs-sprintf-js libjs-util libnode-dev
libssl-dev node-abab node-abbrev node-agent-base node-ampproject-remapping
node-ansi-escapes node-ansi-regex node-ansi-styles node-ansistyles node-anymatch
node-aproba node-archy node-are-we-there-yet node-argparse node-arrify node-asap
node-assert node-async node-async-each node-asynckit node-auto-bind
node-babel-plugin-add-module-exports node-babel-plugin-lodash node-babel7
node-babel7-runtime node-balanced-match node-base node-binary-extensions
```

```
Configurando node-globby (13.1.1+~cs16.24.39-8) ...
Configurando node-del (6.0.0-1) ...
Configurando node-find-cache-dir (3.3.2+~3.2.1-1) ...
Configurando node-babel7 (7.17.11+~cs214.263.190-1) ...
update-alternatives: utilizando /usr/bin/babeljs-7 para proveer /usr/bin/babeljs (babeljs) en modo automático
update-alternatives: utilizando /usr/bin/babeljs-7-external-helpers para proveer /usr/bin/babeljs-external-helpers (babeljs-external-helpers) en modo automático
update-alternatives: utilizando /usr/bin/babeljs-7-node para proveer /usr/bin/babeljs-node (babeljs-node) en modo automático
update-alternatives: utilizando /usr/bin/babeljs-7-parser para proveer /usr/bin/babeljs-parser (babeljs-parser) en modo automático
Configurando node-babel-plugin-lodash (3.3.4+~cs2.0.1-5) ...
Configurando node-jest-debbundle (27.5.1-ds+-~cs69.51.22-7) ...
Configurando node-debbundle-es-to-primitive (1.2.1+~cs9.7.25-2) ...
Configurando node-es-abstract (1.19.2+~cs16.20.24-1) ...
Configurando node-deep-equal (2.0.5+~cs32.11.68-3) ...
Configurando node-util (0.12.4+~1.0.10-1) ...
Configurando node-assert (2.0.0+~cs2.4.2-1) ...
Configurando node-parse-json (5.2.0+~cs5.1.7-1) ...
Configurando node-read-pkg (5.2.0-2) ...
Configurando node-istanbul (0.4.5+repack10+-~cs97.25.57-3) ...
Configurando node-tap (15.2.3+ds+-~cs33.7.17-3) ...
Procesando disparadores para kali-menu (2022.2.0) ...
Procesando disparadores para man-db (2.10.2-1) ...
```

```
(root@kali)-[~/home/orestes]
# apt install npm
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
npm ya está en su versión más reciente (8.8.0~ds1-1).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  fonts-roboto-slab gnome-screenshot libabsl20200923 libavif13 libfam0 libgit2-1.1
  libhttp-parser2.9 libllvm12 libmbcrypto3 libmbcrypto7 libmbdtls12
  libmbdtls14 libmbdex509-0 libmbdex509-1 libmms0 libmozjs-78-0 libofa0 libperl5.32
  libplacebo157 libpoppler102 libproj22 libwebp6 libwmf-0.2-7 libwmf0.2-7
  libx264-160 libyara8 perl-modules-5.32 python3-ipaddr python3-mistune
  python3-singledispatch python3-twisted-bin ruby2.7 ruby2.7-dev
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 93 no actualizados.
```

8) Proseguimos con la instalación de pm2.

```
(root@kali)-[~/home/orestes]
# npm install pm2 -g
npm WARN deprecated uuid@3.4.0: Please upgrade to version 7 or higher. Older versions may use Math.random() in certain circumstances, which is known to be problematic. See https://v8.dev/blog/math-random for details.

added 182 packages, and audited 183 packages in 20s

12 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```

9) Lo siguiente será descargar la última versión de la herramienta del repositorio github y la descomprimiremos en una carpeta posteriormente creada.

```
(root@kali)-[~/home/orestes]
# wget https://github.com/D3VL/L3MON/releases/download/1.1.2/L3MON-v1.1.2.zip
--2022-05-09 20:36:03-- https://github.com/D3VL/L3MON/releases/download/1.1.2/L3MON-v1.1.2.zip
Resolviendo github.com (github.com)... 140.82.121.3
Conectando con github.com (github.com)[140.82.121.3]:443... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Localización: https://objects.githubusercontent.com/github-production-release-asset-2e65be/207894535/29e37c00-8b45-11ea-8902-1412988bb303?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNYAX4CSVEH53A%2F20220509%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220509T183603Z&X-Amz-Expires=300&X-Amz-Signature=b2d2243af9bf5e6dde974b3ae58cc1dbbc10654162ef2d0370d418dfbcf649f&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=207894535&response-content-disposition=attachment%3B%20filename%3DL3MON-v1.1.2.zip&response-content-type=application%2Foctet-stream [siguiendo]
--2022-05-09 20:36:03-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/207894535/29e37c00-8b45-11ea-8902-1412988bb303?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNYAX4CSVEH53A%2F20220509%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220509T183603Z&X-Amz-Expires=300&X-Amz-Signature=b2d2243af9bf5e6dde974b3ae58cc1dbbc10654162ef2d0370d418dfbcf649f&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=207894535&response-content-disposition=attachment%3B%20filename%3DL3MON-v1.1.2.zip&response-content-type=application%2Foctet-stream
Resolviendo objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.110.133, ...
Conectando con objects.githubusercontent.com (objects.githubusercontent.com)[185.199.109.133]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 18632710 (18M) [application/octet-stream]
Grabando a: «L3MON-v1.1.2.zip»
```

Comprobamos el archivo descargado y lo descomprimimos en una carpeta creada. Para ello usamos los siguientes comandos.

```
(root㉿kali)-[~/home/orestes]
└─# ls
Descargas Escritorio L3MON          Música          Plantillas Videos
Documentos Imágenes  L3MON-v1.1.2.zip package-lock.json Público

(roots@kali)-[~/home/orestes]
└─# unzip L3MON-v1.1.2.zip -d /home/orestes/L3MON-v1.1.2
Archive: L3MON-v1.1.2.zip
  inflating: /home/orestes/L3MON-v1.1.2/app/factory/apktool.jar
  inflating: /home/orestes/L3MON-v1.1.2/app/factory/base.apk
  inflating: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/AndroidManifest.xml
  inflating: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/apktool.yml
  inflating: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/build/apk/AndroidManife
st.xml
  inflating: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/build/apk/classes.dex
  inflating: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/build/apk/res/layout/ac
tivity_main.xml
  inflating: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/build/apk/res/layout-v1
7/activity_main.xml
  extracting: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/build/apk/res/mipmap-hd
pi/ic_launcher.png
  extracting: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/build/apk/res/mipmap-md
pi/ic_launcher.png
  extracting: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/build/apk/res/mipmap-xh
dpi/ic_launcher.png
  extracting: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/build/apk/res/mipmap-xx
hdpi/ic_launcher.png
  inflating: /home/orestes/L3MON-v1.1.2/app/factory/decompiled/build/apk/res/mipmap-xx
xhdpi/ic_launcher.png
```

10) Una vez descomprimido, se nos creará una carpeta y tendremos que situarnos en la ruta de la carpeta para continuar con la instalación de L3MON.

```
(root㉿kali)-[~/home/orestes]
└─# ls
Descargas Escritorio L3MON          L3MON-v1.1.2.zip  package-lock.json  Público
Documentos Imágenes  L3MON-v1.1.2  Música          Plantillas          Videos

(roots@kali)-[~/home/orestes]
└─# cd L3MON-v1.1.2

(roots@kali)-[~/home/orestes/L3MON-v1.1.2]
└─# ls
app  assets  clientData  includes  index.js  package.json  package-lock.json
```

Continuamos con la instalación de las dependencias del gestor de procesos(npm).

```
[root@kali]~[/home/orestes/L3MON-v1.1.2]
# npm install
npm WARN old lockfile
npm WARN old lockfile The package-lock.json file was created with an old version of npm,
npm WARN old lockfile so supplemental metadata must be fetched from the registry.
npm WARN old lockfile
npm WARN old lockfile This is a one-time fix-up, please be patient...
npm WARN old lockfile
npm WARN deprecated debug@4.1.1: Debug versions >=3.2.0 <3.2.7 || >=4 <4.3.1 have a low-severity ReDos regression when used in a Node.js environment. It is recommended you upgrade to 3.2.7 or 4.3.1. (https://github.com/visionmedia/debug/issues/797)

added 118 packages, and audited 119 packages in 18s

10 vulnerabilities (2 moderate, 6 high, 2 critical)

To address issues that do not require attention, run:
  npm audit fix

To address all issues (including breaking changes), run:
  npm audit fix --force

Run `npm audit` for details.
```

Nota: Los paquetes descargados son antiguos y pueden descargarse como contenido malicioso para nuestro SO.

Para ello al instalar npm nos da la opción, recomendable, de depurar los paquetes con los siguientes comandos.

```
[root@kali]~[/home/orestes/L3MON-v1.1.2]
# npm audit fix
npm WARN deprecated debug@4.1.1: Debug versions >=3.2.0 <3.2.7 || >=4 <4.3.1 have a low-severity ReDos regression when used in a Node.js environment. It is recommended you upgrade to 3.2.7 or 4.3.1. (https://github.com/visionmedia/debug/issues/797)
npm WARN deprecated debug@4.1.1: Debug versions >=3.2.0 <3.2.7 || >=4 <4.3.1 have a low-severity ReDos regression when used in a Node.js environment. It is recommended you upgrade to 3.2.7 or 4.3.1. (https://github.com/visionmedia/debug/issues/797)

added 4 packages, removed 4 packages, changed 19 packages, and audited 119 packages in 4s

# npm audit report

ejs <3.1.7
Severity: high
Template injection in ejs - https://github.com/advisories/GHSA-phwq-j96m-2c2q
fix available via `npm audit fix --force`
Will install ejs@3.1.7, which is a breaking change
node_modules/ejs

engine.io <4.0.0
Severity: high
Resource exhaustion in engine.io - https://github.com/advisories/GHSA-j4f2-536g-r55m
fix available via `npm audit fix --force`
Will install socket.io@4.5.0, which is a breaking change
node_modules/engine.io
  socket.io 1.0.0-pre - 2.4.1
    Depends on vulnerable versions of engine.io
```

```
[root@kali) [/home/orestes/L3MON-v1.1.2]
# npm audit fix --force
npm WARN using --force. Recommended protections disabled.
npm WARN audit Updating ejs to 3.1.7, which is a SemVer major change.
npm WARN audit Updating socket.io to 4.5.0, which is a SemVer major change.

added 17 packages, removed 22 packages, changed 12 packages, and audited 114 packages
in 3s

2 packages are looking for funding
  run 'npm fund' for details

found 0 vulnerabilities
```

11) Una vez depurados las dependencias de npm, tenemos que iniciar el script de inicio de la app. También haremos que la app se inicie automáticamente en cada sesión.

```
[PM2] Spawning PM2 daemon with pm2_home=/root/.pm2
[PM2] PM2 Successfully daemonized
[PM2] Starting /home/orestes/L3MON-v1.1.2/index.js in fork_mode (1 instance)
[PM2] Done.
```

<code>id</code>	<code>name</code>	<code>mode</code>	<code>o</code>	<code>status</code>	<code>cpu</code>	<code>memory</code>
0	index	<code>fork</code>	0	<code>online</code>	0%	11.6mb

```
(root@kali)-[~/home/orestes/L3MON-v1.1.2]
└─# pm2 startup
[PM2] Init System found: systemd
Platform systemd
Template
[Unit]
Description=PM2 process manager
Documentation=https://pm2.keymetrics.io/
After=network.target

[Service]
Type=forking
User=root
LimitNOFILE=infinity
LimitNPROC=infinity
LimitCORE=infinity
Environment=PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games:/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
Environment=PM2_HOME=/root/.pm2
PIDFile=/root/.pm2	pm2.pid
Restart=on-failure

ExecStart=/usr/local/lib/node_modules/pm2/bin/pm2 resurrect
ExecReload=/usr/local/lib/node_modules/pm2/bin/pm2 reload all
ExecStop=/usr/local/lib/node_modules/pm2/bin/pm2 kill

[Install]
WantedBy=multi-user.target
```

12) A continuación, modificamos el archivo maindb.js para crear un usuario y contraseña, en formato md5(Podemos utilizar cualquier conversor de contraseñas). Una vez, hecho esto podremos iniciar la interfaz de L3MON en el navegador.

Primero paramos el script iniciado anteriormente, para poder modificar dicho archivo.

```
(root@kali)-[~/home/orestes/L3MON-v1.1.2]
└─# pm2 stop index
[PM2] Applying action stopProcessId on app [index](ids: [ 0 ])
[PM2] [index](0) ✓
```

id	name	mode	o	status	cpu	memory
0	index	fork	15	stopped	0%	0b

```

root@kali:/home/orestes/L3MON-v1.1.2
GNU nano 6.3                               maindb.json *

{
  "admin": {
    "username": "orestes",
    "password": "4d186321c1a7f0f354b297e8914ab240",
    "loginToken": "",
    "logs": [],
    "ipLog": []
  },
  "clients": []
}

^G Ayuda      ^O Guardar      ^W Buscar      ^K Cortar      ^T Ejecutar      ^C Ubicación
^X Salir      ^R Leer fich.  ^N Reemplazar  ^U Pegar       ^J Justificar  ^/ Ir a linea

```

Nota: Cuando editamos el archivo maindb.js, por defecto aparece en username, el usuario “admin”, podemos modificarlo y crear nuestro propio usuario. El campo “password”, hay que rellenarlo con el correspondiente valor en MD5 que tengamos.

13) Una vez modificado y guardado la información del archivo maindb.js, debemos reiniciar el script para que los cambios funcionen. Lo hacemos de la siguiente forma.

```

[root@kali]~ [~/home/orestes/L3MON-v1.1.2]
# pm2 restart all
Use --update-env to update environment variables
[PM2] Applying action restartProcessId on app [all](ids: [ 0 ])
[PM2] [index](0) ✓



| id | name  | mode | ø  | status | cpu | memory |
|----|-------|------|----|--------|-----|--------|
| 0  | index | fork | 15 | online | 0%  | 11.7mb |

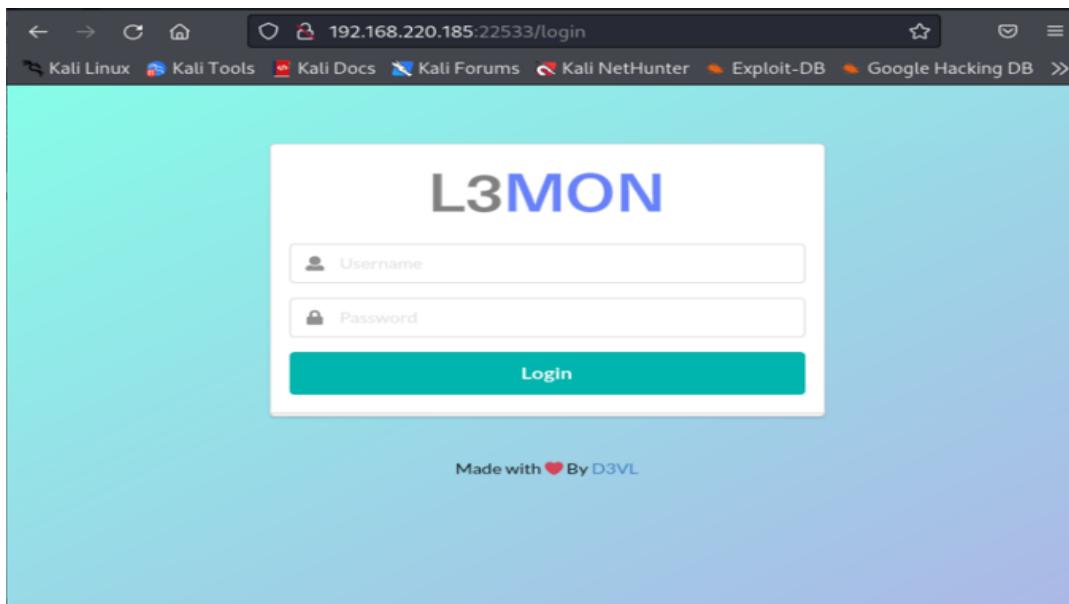

```

14) Como indiqué en los requisitos para que la app funcione y nos conectemos a la interfaz web, necesitamos un servidor web local, en este caso utilizaré Nginx, aunque sirve cualquier otro. Levantamos el servicio Nginx y comprobamos su estado.

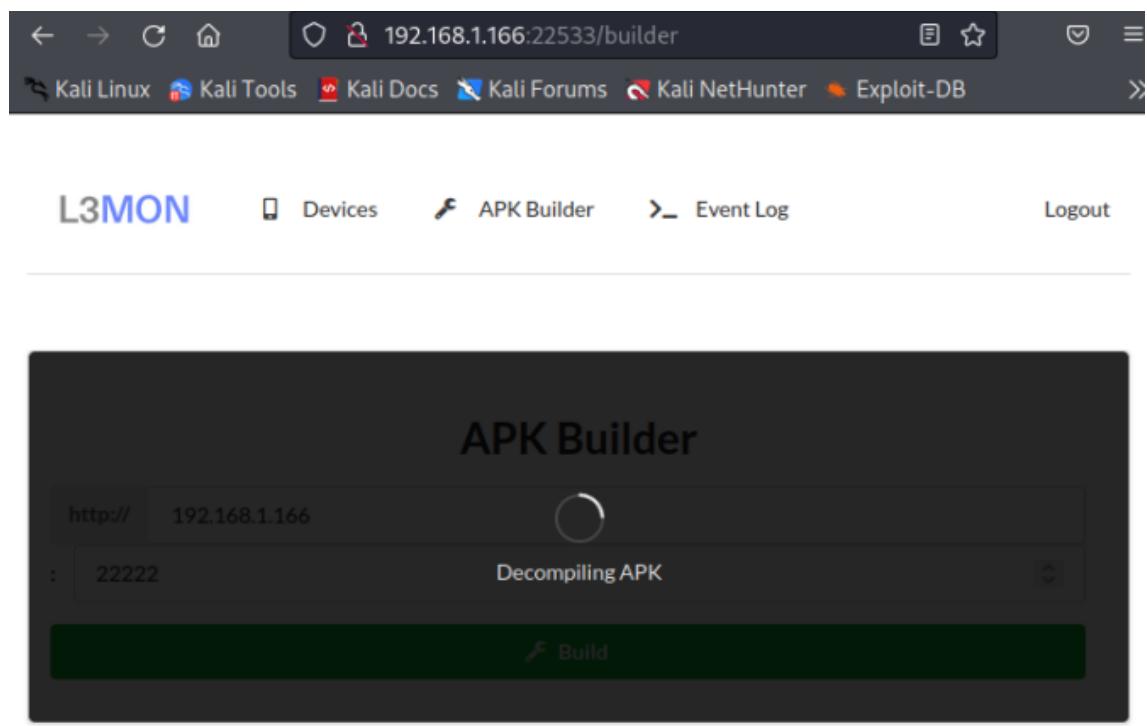
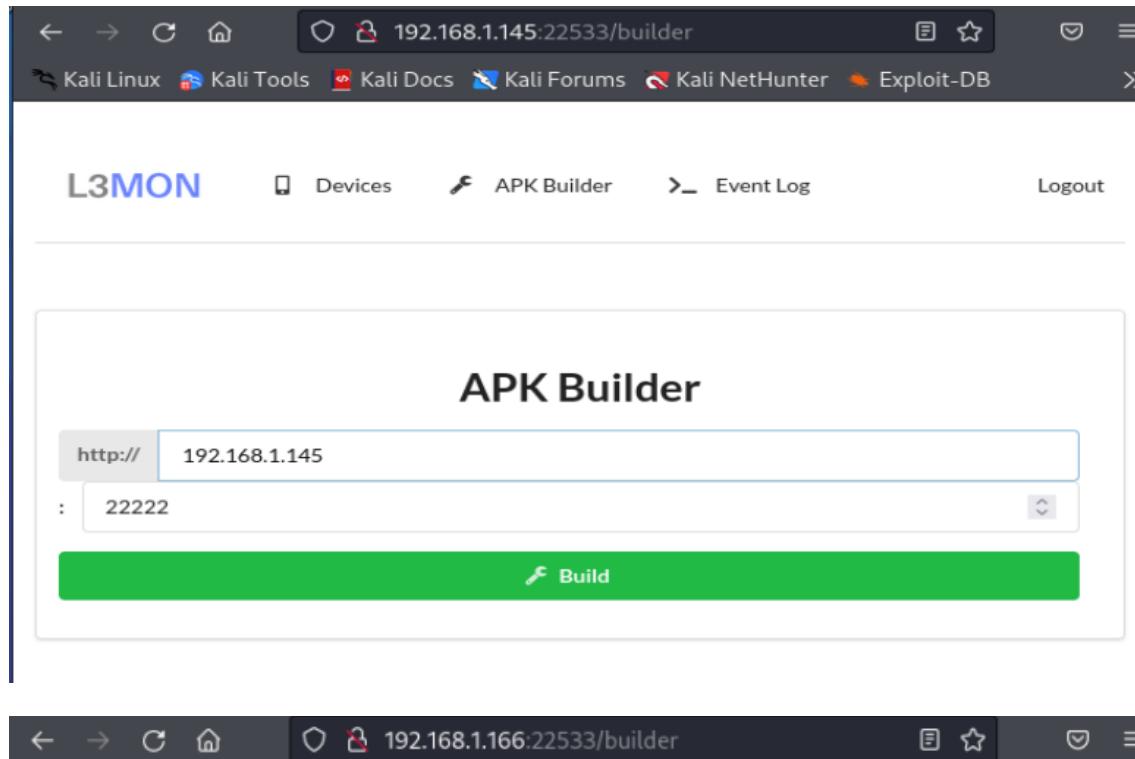
```
(orestes㉿kali)-[~]
$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-05-09 21:09:20 CEST; 36s ago
     Docs: man:nginx(8)
 Process: 63847 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on>
 Process: 63848 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0)
 Main PID: 63849 (nginx)
    Tasks: 3 (limit: 2275)
   Memory: 7.5M
      CPU: 33ms
     CGroup: /system.slice/nginx.service
             ├─63849 "nginx: master process /usr/sbin/nginx -g daemon on; master_process"
             ├─63850 "nginx: worker process"
             ├─63851 "nginx: worker process"

may 09 21:09:20 kali systemd[1]: Starting A high performance web server and a reverse proxy...
may 09 21:09:20 kali nginx[63847]: nginx: [warn] duplicate extension "woff", content type >
may 09 21:09:20 kali nginx[63848]: nginx: [warn] duplicate extension "woff", content type >
may 09 21:09:20 kali systemd[1]: Started A high performance web server and a reverse proxy...
lines 1-19/19 (END)
```

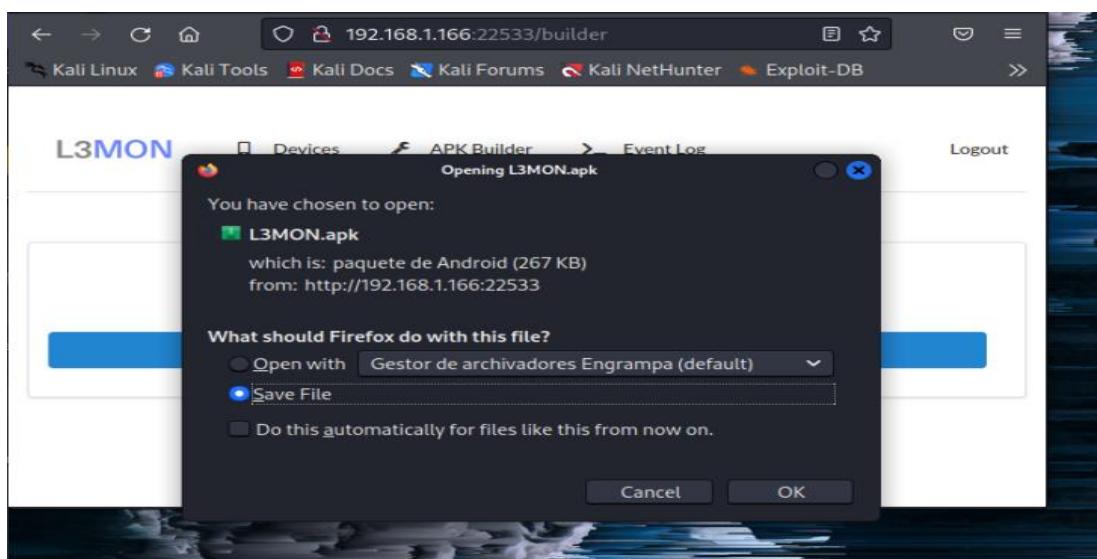
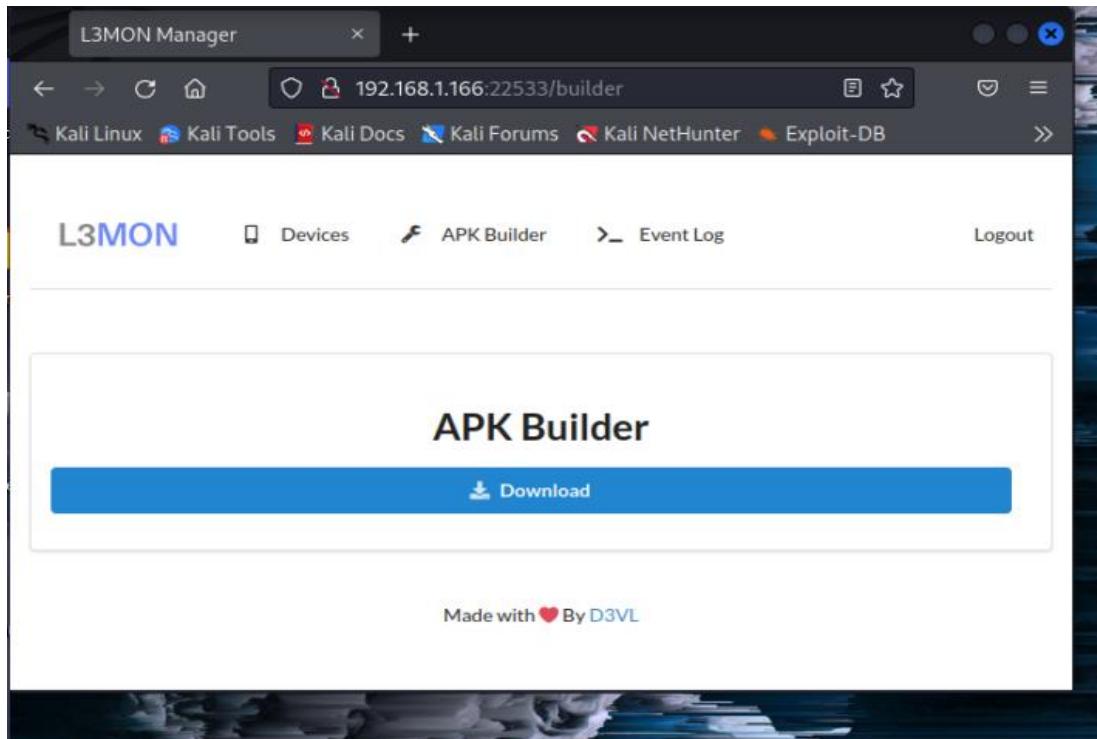
15) Nos conectamos a la interfaz de la app vía local y con la ip que dispongamos. Nos logueamos con el usuario y contraseña corriente (no valor md5), modificado anteriormente a través del puerto 22533, que es el que utiliza L3MON.



16) Una vez dentro de la interfaz podremos crear el archivo apk con el cuál controlaremos el dispositivo móvil. Para ello vamos a la opción “APK Builder” y con la ip local de nuestra máquina generamos el archivo APK, que nos permitirá controlar el dispositivo móvil.



17) Una vez generado el archivo, podremos descargarlo en nuestra máquina y podremos enviarlo a un móvil y controlarlo remotamente. Para poder controlar el dispositivo diseñé una página web gancho que servirá de engaño para el usuario y poder instalar el apk en el móvil.



The screenshot shows a web application running on Kali Linux. The URL in the address bar is 192.168.220.185:22533. The page displays two tables: one for 'Online' devices and one for 'Offline' devices. The 'Online' table has columns: Name, Country, IP, Device, Last Seen, and Manage. The 'Offline' table has columns: Name, Country, IP, Device, Last Seen, and Manage. Two devices are listed in the 'Offline' table.

Name	Country	IP	Device	Last Seen	Manage
225304585bf1c244	?	192.168.1.150	samsung (SM-G988N)	02/05/2022, 19:44:32	<button>Manage</button>
530cef99b4ba9492	?	192.168.220.27	OPPO (CPH2195)	07/05/2022, 15:35:23	<button>Manage</button>

Made with ❤ By D3VL

The screenshot shows a Firefox browser window titled 'Descarga Juegos'. The address bar shows 'localhost/descargas.html'. A download dialog box is open, titled 'Opening Juego_demo'. It says: 'You have chosen to open: Juego_demo which is: paquete de Android (267 KB) from: http://localhost'. The dialog asks: 'What should Firefox do with this file?'. The 'Save File' option is selected. There is also a checkbox 'Do this automatically for files like this from now on.' At the bottom are 'Cancel' and 'OK' buttons.

El aspecto de la interfaz es el siguiente:

The screenshot shows a web-based interface for managing mobile devices. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and other sections. Below the bar, the title 'L3MON' is displayed, along with links for Devices, APK Builder, Event Log, and Logout.

The main area is divided into two sections: 'Online' and 'Offline'. The 'Online' section contains a table with one row of data:

Name	Country	IP	Device	Last Seen	Manage
530cef99b4ba9492	?	192.168.220.27	OPPO (CPH2195)	10/05/2022, 12:18:18	<button>Manage</button>

The 'Offline' section contains a table with one row of data:

Name	Country	IP	Device	Last Seen	Manage
225304585bf1c244	?	192.168.1.150	samsung (SM-G98BN)	07/05/2022, 16:04:26	<button>Manage</button>

Tiene 3 opciones:

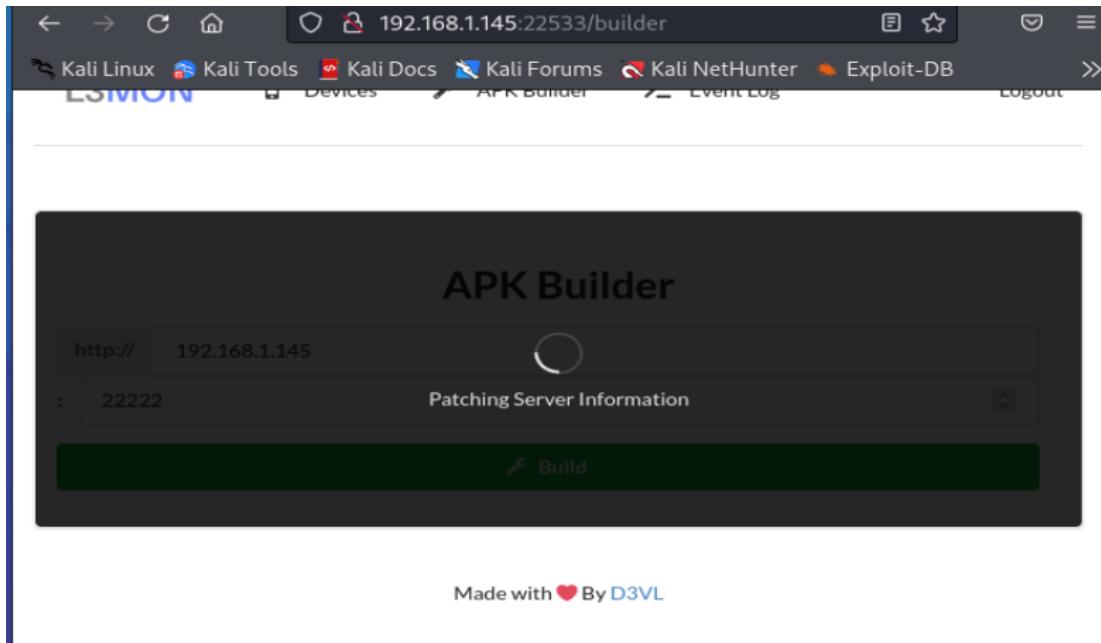
a) Devices: En este campo, podemos ver el estado de los dispositivos móviles que tengamos controlados (estado, fecha, ip, etc). Con la opción Manage, podremos entrar al dispositivo y controlarlo remotamente.

Una vez, controlado el dispositivo podremos navegar por las distintas opciones que ofrece la herramienta.

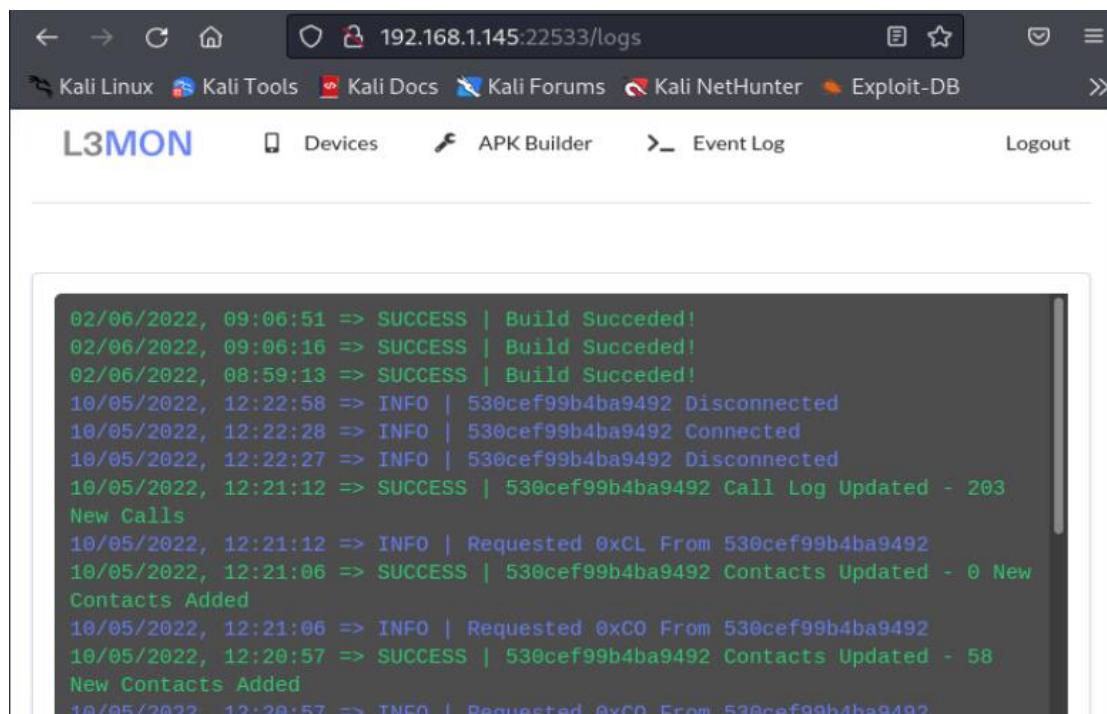
This screenshot shows the 'Info' screen for a selected device. On the left, a sidebar lists various options: Info (selected), GPS, Microphone, Contacts, Call Log, Clipboard Log, Notification Log, SMS Manager, WiFi Manager, Installed Apps, Allowed Permissions, File Explorer, and Downloads. The main content area displays the following information:

12:34 12:34
12/02/2019 12/02/2019
FIRST SEEN LAST SEEN

b) Opción APK Builder: Cómo comenté anteriormente esta app se sirve de la creación de un archivo apk para poder controlar el dispositivo, para ello ponemos la ip local que tengamos y se generará el archivo que podremos descargar.

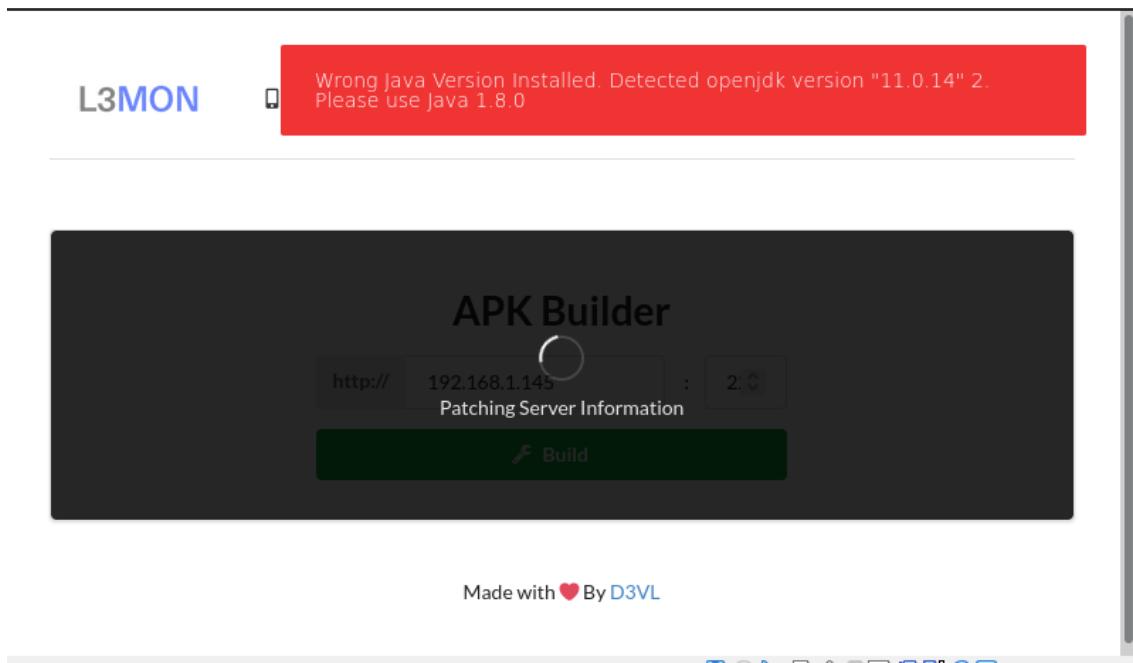


c) Opción Event Log en esta consola, se nos genera los logs de las acciones que vamos haciendo así cómo los dispositivos que controlemos.



Errores encontrados:

Mientras trasteaba en la aplicación, encontré un error al generar el apk con el apk Builder de la interfaz, resulta que este generador no funciona con una versión de Java superior a la 1.8. A continuación muestro el error generado y su solución.



Solución: Una solución a este problema es cambiar la versión de Java instalada en la MV a la versión 1.8 de forma manual.

1) Comprobamos la versión de Java que tenemos.

```
(orestes㉿kali)-[~]
$ java -version
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
openjdk version "11.0.14.1" 2022-02-08
OpenJDK Runtime Environment (build 11.0.14.1+1-post-Debian-1)
OpenJDK 64-Bit Server VM (build 11.0.14.1+1-post-Debian-1, mixed mode, sharing)
```

2) De la página oficial de oracle, nos descargamos el paquete de instalación de open jdk 8. Lo encontraremos como “jdk-8u333-linux-x64.tar.gz”.

```
kali@kali: ~/Descargas
Archivo Acciones Editar Vista Ayuda
└──(kali㉿kali)-[~]
$ cd Descargas
└──(kali㉿kali)-[~/Descargas]
$ ls
INFORMACION jdk-8u333-linux-x64.tar.gz 'L3MON(1).apk' L3MON.apk
└──(kali㉿kali)-[~/Descargas]
$
```

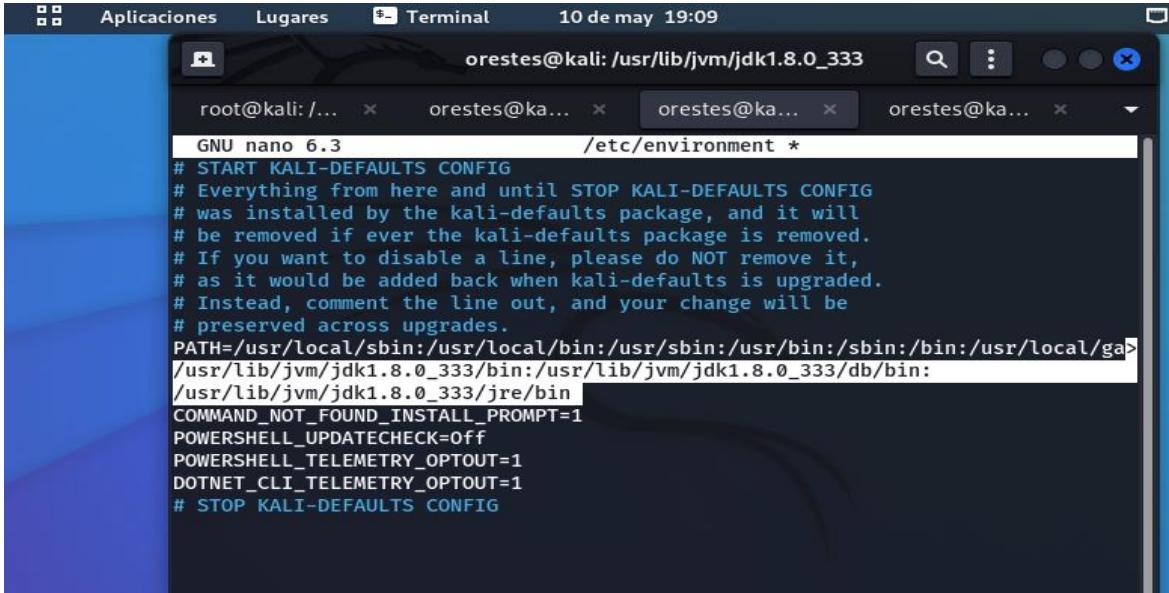
3) Entramos a la siguiente ruta y extraemos el zip de open jdk 8 con el siguiente comando:

```
└──(orestes㉿kali)-[~]
$ cd /usr/lib/jvm
└──(orestes㉿kali)-[/usr/lib/jvm]
$ sudo tar -xvzf ~/Descargas/jdk-8u333-linux-x64.tar.gz
[sudo] contraseña para orestes:
[jdk1.8.0_333/
[jdk1.8.0_333/COPYRIGHT
[jdk1.8.0_333/LICENSE
[jdk1.8.0_333/README.html
[jdk1.8.0_333/THIRDPARTYLICENSEREADME.txt
[jdk1.8.0_333/bin/
[jdk1.8.0_333/bin/java-rmi.cgi
[jdk1.8.0_333/bin/appletviewer
[jdk1.8.0_333/bin/extcheck
[jdk1.8.0_333/bin/idlj
[jdk1.8.0_333/bin/jar
[jdk1.8.0_333/bin/iarsigner
```

4) Una vez descomprimidos todos los archivos nos movemos al siguiente directorio:

```
└──(orestes㉿kali)-[/usr/lib/jvm]
$ ls
default-java          java-11-openjdk-amd64    java-8-openjdk-amd64
java-1.11.0-openjdk-amd64  java-1.8.0-openjdk-amd64  jdk1.8.0_333
└──(orestes㉿kali)-[/usr/lib/jvm]
$ cd jdk1.8.0_333
```

5) Lo siguiente que haremos es establecer la ruta de Java, cambiando la variable de entorno y editamso el archivo “environment” de la siguiente manera:



```
GNU nano 6.3
# START KALI-DEFAULTS CONFIG
# Everything from here and until STOP KALI-DEFAULTS CONFIG
# was installed by the kali-defaults package, and it will
# be removed if ever the kali-defaults package is removed.
# If you want to disable a line, please do NOT remove it,
# as it would be added back when kali-defaults is upgraded.
# Instead, comment the line out, and your change will be
# preserved across upgrades.
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/ga>
/usr/lib/jvm/jdk1.8.0_333/bin:/usr/lib/jvm/jdk1.8.0_333/db/bin:
/usr/lib/jvm/jdk1.8.0_333/jre/bin
COMMAND_NOT_FOUND_INSTALL_PROMPT=1
POWERSHELL_UPDATECHECK=off
POWERSHELL_TELEMETRY_OPTOUT=1
DOTNET_CLI_TELEMETRY_OPTOUT=1
# STOP KALI-DEFAULTS CONFIG
```

6) Instalamos Open jdk 8 como alternativa para que podamos cambiar fácilmente la versión de Java según nuestras necesidades.



```
(orestes㉿kali)-[~/Documents]
$ sudo update-alternatives --install "/usr/bin/java" "java" "/usr/lib/jvm/jdk1.8.0_333/bin/java" 0

(orestes㉿kali)-[~/Documents]
$ sudo update-alternatives --install "/usr/bin/javac" "javac" "/usr/lib/jvm/jdk1.8.0_333/bin/javac" 0

(orestes㉿kali)-[~/Documents]
$ sudo update-alternatives --set java /usr/lib/jvm/jdk1.8.0_333/bin/java
update-alternatives: utilizando /usr/lib/jvm/jdk1.8.0_333/bin/java para proveer /usr/bin/java (java) en modo manual

(orestes㉿kali)-[~/Documents]
$ sudo update-alternatives --set javac /usr/lib/jvm/jdk1.8.0_333/bin/javac
update-alternatives: utilizando /usr/lib/jvm/jdk1.8.0_333/bin/javac para proveer /usr/bin/javac (javac) en modo manual

(orestes㉿kali)-[~/Documents]
```

Nota: Con el comando utilizado configuramos el compilador de java y configuramos open jdk 8

7) Actualizamos el compilador y comprobamos que existe la opción de Java que utilizaremos. Por último, comprobamos si nuestra versión de Java se ha modificado.

```
(orestes㉿kali)-[/usr/lib/jvm/jdk1.8.0_333]
$ sudo update-alternatives --config java
Existen 3 opciones para la alternativa java (que provee /usr/bin/java).

  Selección    Ruta                               Prioridad  Estado
  -----
  0            /usr/lib/jvm/java-11-openjdk-amd64/bin/java  1111      modo auto
mático
  1            /usr/lib/jvm/java-11-openjdk-amd64/bin/java  1111      modo manu
al
  2            /usr/lib/jvm/jdk1.8.0_333/bin/java           0         modo manu
al
* 3            /usr/lib/jvm/jdk1.8.0_333/bin/javac          0         modo manu
al

Pulse <Intro> para mantener el valor por omisión [*] o pulse un número de selección: 2
update-alternatives: utilizando /usr/lib/jvm/jdk1.8.0_333/bin/java para proveer
/usr/bin/java (java) en modo manual
```

```
(orestes㉿kali)-[/usr/lib/jvm/jdk1.8.0_333]
$ java -version
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
java version "1.8.0_333"
Java(TM) SE Runtime Environment (build 1.8.0_333-b02)
Java HotSpot(TM) 64-Bit Server VM (build 25.333-b02, mixed mode)
```

Bibliografía utilizada:

Información sobre la herramienta y su instalación:

<https://github.com/D3VL/L3MON>

<https://hackwise.mx/como-acceder-a-dispositivos-android-de-forma-remota-con-l3mon/>

<https://muylinux.xyz/l3mon-acceso-remoto-a-dispositivos-android/>

<https://wikitecno.net/como-hackear-un-dispositivo-android-con-kali-linux/>

https://www.elespanol.com/elandroidelibre/aplicaciones/seguridad/20191124/hackeo-etico-importante-seguridad-android/446956010_0.html

<https://cienciasdelderecho.com/seguridad-informatica-beneficios/>

<https://www.tecmint.com/install-pm2-to-run-nodejs-apps-on-linux-server/>

Descargas del SO Kali Linux:

<https://www.profesionalreview.com/2019/01/02/instalar-kali-linux-virtualbox/>

<https://www.kali.org/get-kali/#kali-platforms>

Vídeos tutoriales empleados:

<https://www.youtube.com/watch?v=Onk48wHw1Mw>

<https://www.youtube.com/watch?v=WU43BsVXh5s>

<https://www.youtube.com/watch?v=Onk48wHw1Mw>

Solución al fallo de la versión de Java: <https://muylinux.xyz/como-instalar-manualmente-java-openjdk8-en-kali-linux/>

Conversores de contraseñas a MD5:

<https://www.infranetworking.com/md5>

<https://smallseotools.com/es/md5-generator/>

