

Auditoria informatica a Twitter



Jorge González

Profesor: Maximiliano Vega

29/ 11 /2017

Creadores e historia

-fundador

Jack Dorsey 21 de marzo del 2006.

-Twitter surgió como proyecto
de investigación dentro de Obvious.

-una pequeña
compañía situada en San Francisco.

-Consejo
de Administración está formado por
Dorsey, Evan Williams y Biz Stone.



Datos técnicos



Escrita en Ruby on Rails

Se caracteriza por su interfaz sencilla.
Todos los mensajes de Twitter van a parar al servidor servidor de un software programado en Scala la API está totalmente abierta a desarrolladores

Datos Específicos

- Localización San Francisco, California
- País de origen Estados Unidos
- Área de servicio Mundial
- Fundador(es):
 - Jack Dorsey
 - Noah Glass
 - Biz Stone
 - Evan Williams
- Presidente Omid Kordestani

Hackeo ético

- Hats, hackers
de sombrero blanco, o hacker éticos
- Black Hat o ciberdeluente



Exploit

Que es un Exploit?:
aprovecha de un agujero de seguridad



Medidas de protección

- Mantener todas nuestras aplicaciones y sistemas actualizados.
- Mitigar los efectos de posibles exploits usados en nuestra contra.
- Contar con una solución de seguridad avanzada como.

algunos ejemplos

- Análisis dinámico.
- Comunicación con el servidor
- Estudio de la estructura de protección del almacenamiento de datos.
- Decompilación de la aplicación.
- Revisión del código fuente.



aplicacion por Auditar

The screenshot displays a mobile application interface for Twitter. At the top, there are three header bars showing the time as 6:28 PM, 6:29 PM, and 6:29 PM respectively. Below the headers, the Twitter logo is visible.

The main screen features a sidebar on the left with the following icons and labels:

- Tweets (132)
- Mentions
- Direct messages
- #2010YearOf
- Lists
- Retweets
- My profile

The central area shows a feed of tweets. The first tweet is from **Annajane** (@jesusdiaz), which reads:
"giving me some cyber love, linking to the long awaited Nightline spot! RT @gizmodo Not-So-Old Technology... <http://bit.ly/bEUq6j>"
The tweet was posted 22 minutes ago via TweetMeme.

Below the tweet are four interaction buttons: Reply, Retweet, Favorite, and Share.

The right side of the screen shows a "Create Tweet" interface with a text input field containing "What's happening?". At the bottom right are "Update" and "Cancel" buttons. A virtual QWERTY keyboard is displayed at the very bottom.

Más de 32 millones de cuentas de Twitter fueron
hackeadas



Pruebas con exploits





decompilado de la aplicacion

APK Downloader

Home Comment DMCA Report

Package name or Google Play URL [Visit Play Store](#)

com.twitter.android

Package Name: com.twitter.android [Play Store]
File Size: 34.2 MB
QR Code: [View](#)
MD5 File Hash: e803a8f19ac3ddda5acccbc6db87dd2e4
Last Fetched: 2017-06-14 05:06:52
Version: 7.0.0 (7110078)

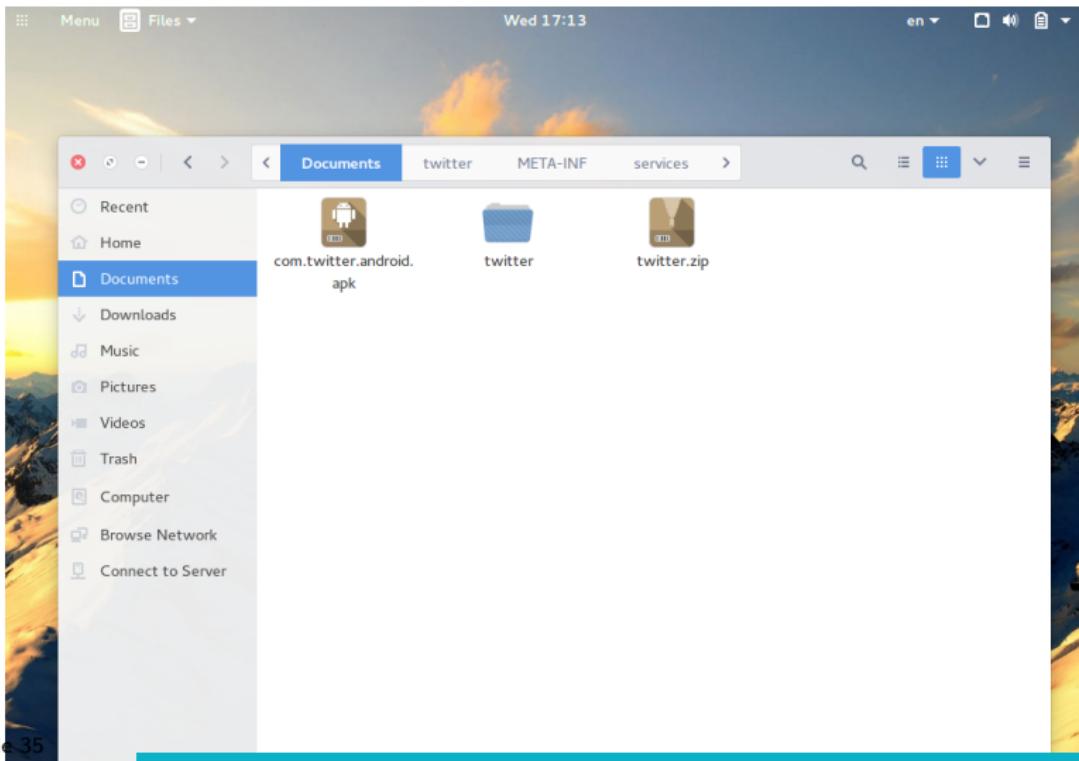
[Generate Download Link](#)

[Click here to download com.twitter.android now](#)

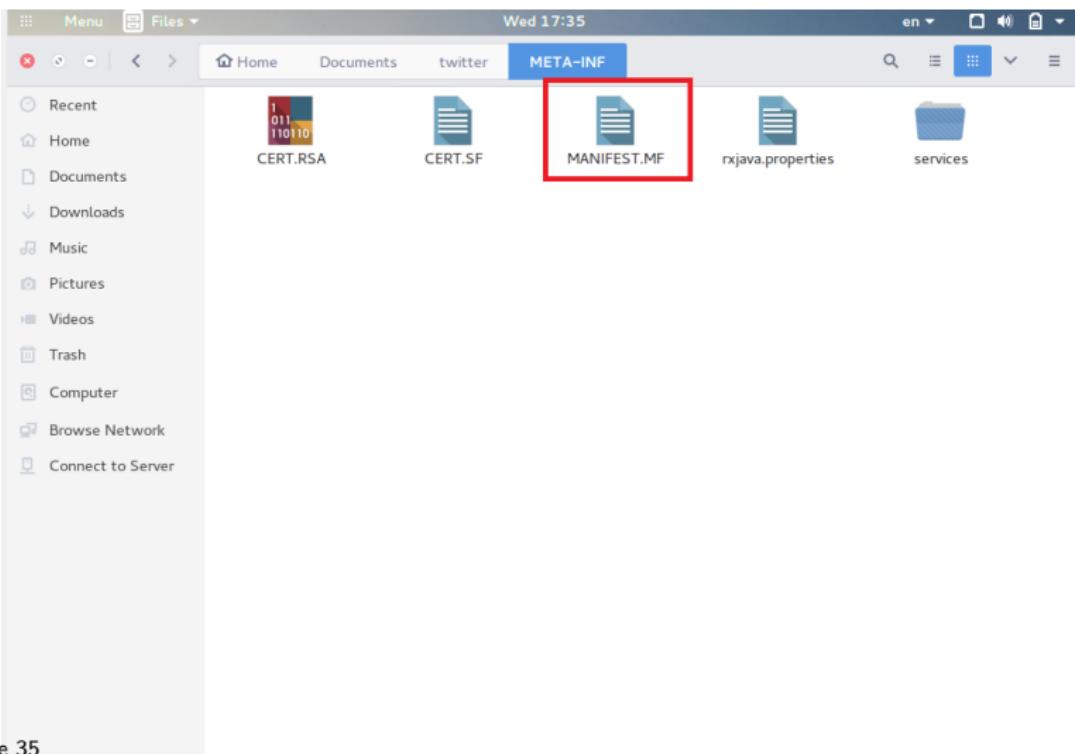
Request Update ▾

Have you ever wanted to get your hands on the latest game, only to find that the Google Play thought it wasn't compatible with your phone? Maybe you don't have a snapdragon device, but you're pretty sure an old device could handle it still. Or the app is not available in your country? Until now you've been stuck, but a new online service called APK Downloader will allow you to download an apk file from the Google Play directly to your desktop and your device.

decompilado de la aplicacion

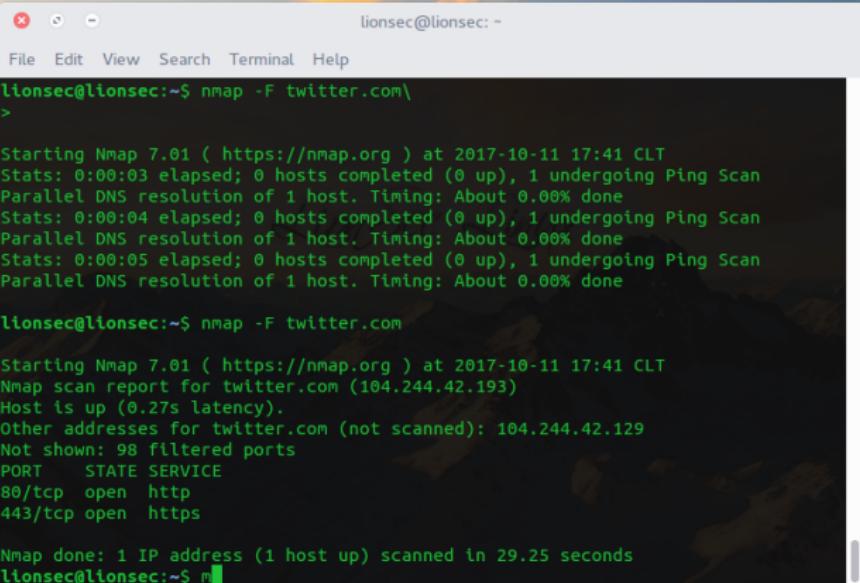


decompilado de la aplicacion





Puertos escaneados



A terminal window titled "lionsec@lionsec: ~" running on a Mac OS X desktop. The window displays the output of an Nmap port scan against the Twitter website (twitter.com). The scan shows that the host is up and identifies two open ports: 80/tcp (HTTP) and 443/tcp (HTTPS).

```
lionsec@lionsec:~$ nmap -F twitter.com
>

Starting Nmap 7.01 ( https://nmap.org ) at 2017-10-11 17:41 CLT
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done

lionsec@lionsec:~$ nmap -F twitter.com

Starting Nmap 7.01 ( https://nmap.org ) at 2017-10-11 17:41 CLT
Nmap scan report for twitter.com (104.244.42.193)
Host is up (0.27s latency).
Other addresses for twitter.com (not scanned): 104.244.42.129
Not shown: 98 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 29.25 seconds
lionsec@lionsec:~$
```

que es SQLmap

Pruebas de inyecciones SQL

¿Que es SQLmap? Sqlmap es una herramienta desarrollada en el lenguaje python y es muy util para hacer inyecciones sql automatizados.



Inyección SQL

Pruebas de inyecciones SQL



Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

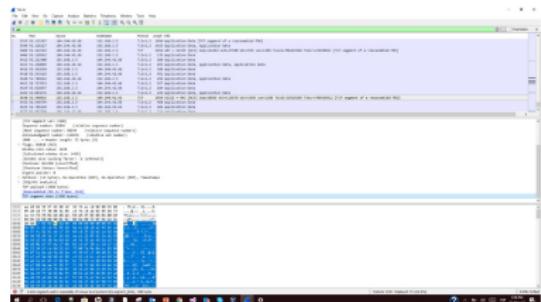
Prueba de Man in the middle

punto de acceso al computador



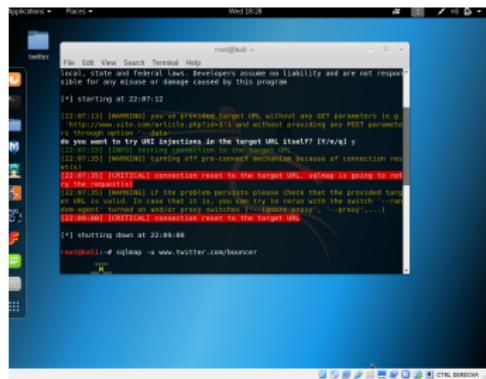
Prueba de Man in the middle

Prueba
de man in the middle con wireshark



Pruebas con SQLmap

Pruebas de inyecciones SQL



```
root@kali:~# ./sqlmap -u www.twitter.com/account
[!] Starting at 22:07:22
[File, Edit, View, Search, Terminal Help]
[local], state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] Starting at 22:07:22

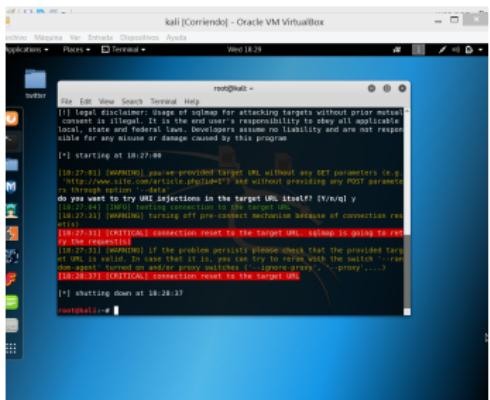
[22:07:31] [WARNING] you've provided target URL without any GET parameters (e.g.
http://www.site.com/article.php?id=1) and without providing any POST parameter
to --data. Do you want to try URL injections in the target URL itself? [Y/n]y
[22:07:31] [INFO] testing connection to the target url...
[22:07:31] [WARNING] Target URL pre-configured because of connection reusing
[*] [22:07:31] [WARNING] connection reset to the target url... please a proxy [http]
[22:07:31] [INFO] If the problem persists please check that the provided target URL is correct and that the target URL is accessible from the system. The --user-agent turned on and/or proxy switched. [-l|--user-agent], ...--proxy'....]
[22:08:00] [WARNING] connection reset to the target url...
[*] Shutting down at 22:08:00
root@kali:~#
```

escaneos de las cuentas con SQLmap
la la direccion twitter.com/account

Pruebas con SQLmap

Pruebas de inyecciones SQL

escaneos de las cuentas
con SQLmap con twitter.com/follow



```
root@kali: ~ [Comiendo] - Oracle VM VirtualBox
root@kali: ~ [Terminal] - Wed 18:29
[*] starting at 18:27:08
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 18:27:08
[0:27.01] [WARNING] you've provided target URL without any GET parameters (e.g. http://www.site.com/article.php?id=5) and without providing any POST parameters
do you want to try URL injections in the target URL itself? [Y/n/q] y
[0:27.04] [INFO] testing connection to the target URL
[0:27.01] [WARNING] turning off pre-connect mechanism because of connection reusing
[0:27.01] [WARNING] connection reset to the target URL (attempt is going to ret)
[0:27.01] [WARNING] if the problem persists please check that the provided target URL is correct and that the target is up. If you're still trying to connect with the switch --rand-agent turned on make sure web browser matches (e.g. proxy, ...), proxy ....)
[0:28.37] [CRITICAL] connection reset to the target URL
[*] shutting down at 18:28:37
root@kali: ~ [
```



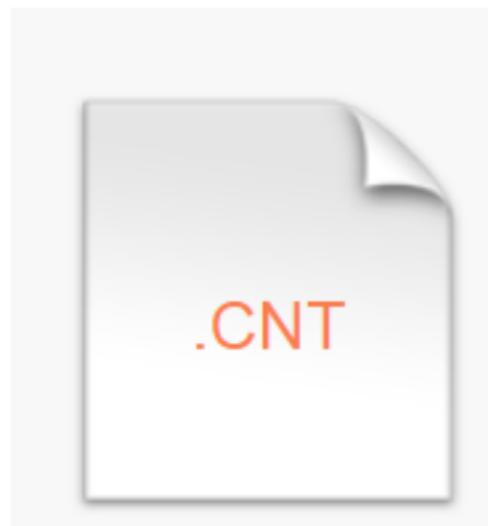
archivos en el telefono

carpetas internas de twitter

Todos los archivos		
/Android/data/com.twitter.android/cache		
http-responses	02/11/2017	
image_cache	02/11/2017	
photos	02/11/2017	

archivos en el telefono

archivos en android de twitter



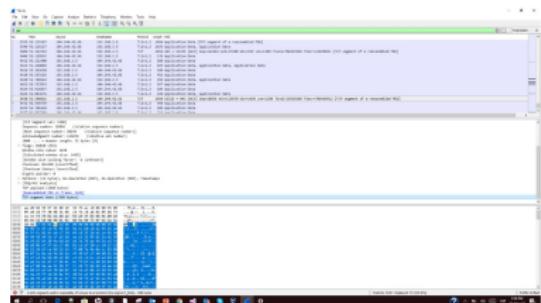
Prueba de Man in the middle

punto de acceso al computador



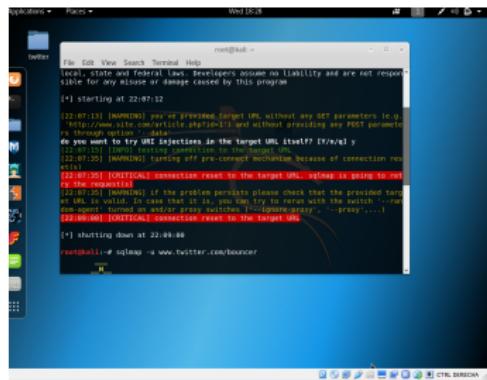
Prueba de Man in the middle

Prueba
de man in the middle con wireshark



Pruebas con SQLmap

Pruebas de inyecciones SQL



```
root@kali:~# ./sqlmap -u www.twitter.com/account
[!] Starting at 22:07:22
[File, Edit, View, Search, Terminal Help]
[local], state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] Starting at 22:07:22

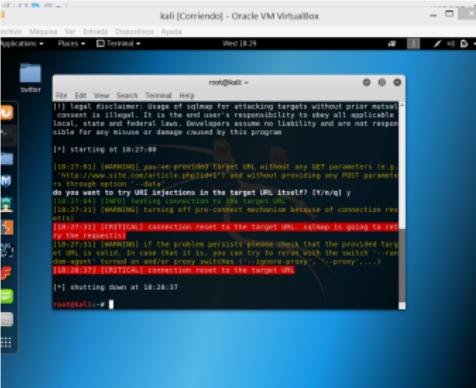
[22:07:31] [WARNING] you've provided target URL without any GET parameters (e.g.
http://www.site.com/article.php?id=1) and without providing any POST parameter
to --data. Do you want to try URL injections in the target URL itself? [Y/n]y
[22:07:31] [INFO] testing connection to the target url...
[22:07:31] [WARNING] Target URL pre-configured because of connection reusing
[*] [22:07:31] [WARNING] connection reset to the target url... please a proxy [http]
[22:07:31] [INFO] If the problem persists please check that the provided target URL is correct and that the target URL is accessible from the system. The --user-agent turned on and/or proxy switched. [-l|--user-agent], ...--proxy'....]
[22:08:00] [WARNING] connection reset to the target url...
[*] Shutting down at 22:08:00
root@kali:~#
```

escaneos de las cuentas con SQLmap
la la direccion twitter.com/account

Pruebas con SQLmap

Pruebas de inyecciones SQL

escaneos de las cuentas
con SQLmap con twitter.com/follow



```
root@kali: ~ [Comiendo] - Oracle VM VirtualBox
root@kali: ~ [Terminal] - Wed 18:29
[*] starting at 18:27:08
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 18:27:08
[18:27:08] [INFO] you've provided target URL without any GET parameters (e.g. http://www.site.com/article.php?id=5) and without providing any POST parameters
[*] do you want to try URL injections in the target URL itself? [Y/n]qj y
[18:27:08] [INFO] testing connection to the target URL
[18:27:08] [WARNING] turns off pre-connect mechanism because of connection restrictions
[18:27:08] [WARNING] connection reset to the target URL (attempt is going to re-connect)
[18:27:08] [WARNING] if the problem persists please check that the provided target URL is correct and that the target is up. If you're behind a proxy, turn off proxy with the switch --proxy=none or --proxy=off
[18:28:37] [WARNING] connection reset to the target URL
[*] shutting down at 18:28:37
root@kali: ~ [
```



archivos en el telefono

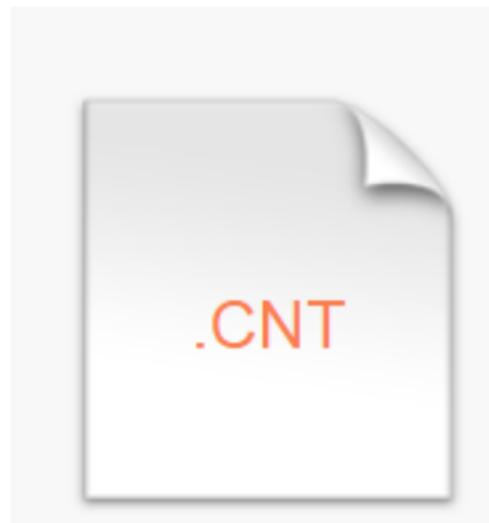
carpetas internas de twitter

A screenshot of a file manager interface. The top bar shows a back arrow, the text "Todos los archivos", a refresh icon, and a search icon. Below the bar, the path "/Android/data/com.twitter.android/cache" is displayed. Three folder entries are listed: "http-responses" (modified 02/11/2017), "image_cache" (modified 02/11/2017), and "photos" (modified 02/11/2017).

Folder	Name	Modified
http-responses	http-responses	02/11/2017
image_cache	image_cache	02/11/2017
photos	photos	02/11/2017

archivos en el telefono

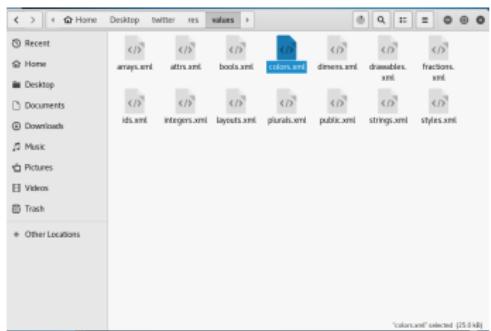
archivos en android de twitter



Compilación de la aplicación

Cambio de valores en la aplicación

archivo de
la aplicación que contiene los colores



Compilación de la aplicación

Cambio de valores en la aplicación

cambio dentro del archivo

```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <color name="app_background">@color/black</color>
    <color name="badge_protected">#000000</color>
    <color name="color_accentified">@color/twitter_blue</color>
    <color name="border_color">@color/tertiary</color>
    <color name="deep_gray">#ff657786</color>
    <color name="deep_gray_30">#4d657786</color>
    <color name="deep_gray_50">#80657786</color>
    <color name="faded_gray">#e0e0e0</color>
    <color name="faded_gray_50">#fffff1f1</color>
    <color name="focused_bg">@color/faded_gray</color>
    <color name="footer_logo">@color/medium_gray</color>
    <color name="global_ripple_selector_color">#1d000000</color>
    <color name="light_gray">#ffccdd00</color>
    <color name="list_bg">@color/clear</color>
    <color name="medium_gray">#ffaabb00</color>
    <color name="medium_gray_50">#80aab000</color>
    <!-- color for the bottom navigation bar -->
```

Compilación de la aplicación

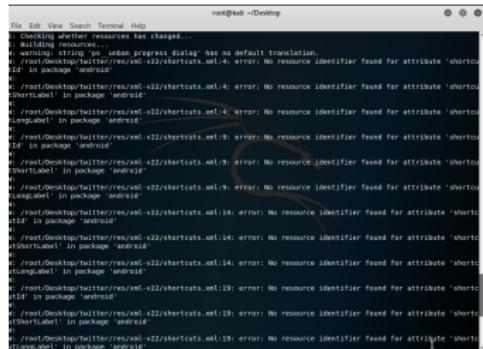


Cambio de valores en la aplicación
intento
de contracción de la aplicación

Compilación de la aplicación

Cambio de valores en la aplicación

fallo al intentar compilar una aplicación ya que detecto que habían archivos que tenían modificaciones



The screenshot shows a terminal window with the following text output:

```
root@kali:~/Desktop:  
File Edit View Search Terminal Help  
File Contents Terminal resources has changed...  
Building resources...  
warning: string 'ps_urban.progress_dialog' has no default translation.  
error: No resource identifier found for attribute 'shortcuts_id' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:4: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:4: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:9: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:9: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:9: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:9: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:9: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:14: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:14: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:14: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:19: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:19: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'  
error: /root/Desktop/twitter/res/xml/v22/sheretcats.xml:19: error: No resource identifier found for attribute 'shortcuts_label' in package 'android'
```

ataque Ddos

Investigación sobre ataque DDos

¿se puede realizar un ataque
de denegación de servicio a Twitter?



ataque Ddos

Investigación sobre ataque DDos

según
la revista especializada en informática
aproximadamente entre 250
y 500 computadores. (García, 2017)

