

Auditoria informatica a Twitter:,Segundo incremental



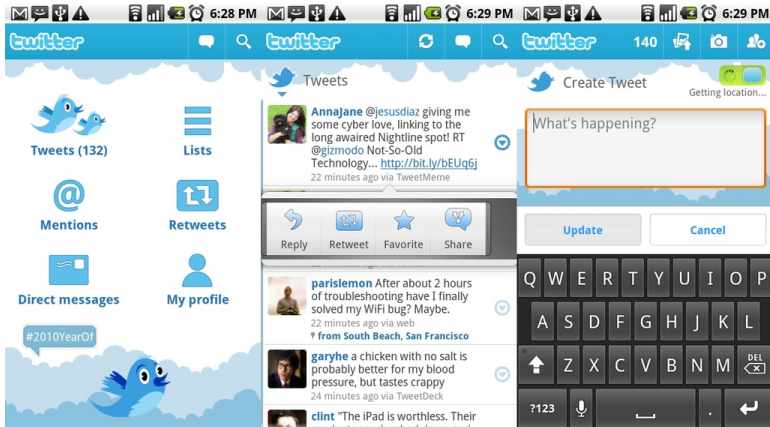
UNIVERSIDAD
Finis Terrae
VINCE IN BONO MALUM

Jorge Gonzlez

Profesor: Maximiliano Vega

Octubre / 11 /2017

aplicacion por Auditar



Ms de 32 millones de cuentas de Twitter fueron
hackeadas



Pruebas con exploits

The screenshot displays the 'Hackear Twitter' website. On the left is a dark sidebar with a login form containing fields for 'Identificador' (with a 'Generar Aleatoriamente' button), 'URL Opcional', and 'Usuario o E-mail Opcional'. The main content area has a blue header with navigation links and a central box titled 'Hackear Twitter Aqui ↓' with instructions for using the tool. To the right, a terminal window shows a Kali Linux command prompt with a command to exploit a Twitter account. At the bottom, a blue banner contains several informational boxes about the system's features and updates.

Hackear Twitter

Identificador [Generar Aleatoriamente](#)

ejemplo123

El identificador es tu "clave secreta" para obtener acceso

■ Recordar identificador

Si utilizas XPLOITZ con frecuencia te sugerimos recordarlo

URL Opcional

<http://google.com/>

Redireccionaremos a tu victima a la URL que introduzcas

Usuario o E-mail Opcional

correo@ejemplo.com

El usuario o e-mail será mostrado en el scam para que tu víctima caiga

Idioma

[Español](#)

HACKEAR FACEBOOK

Hackear Twitter Aqui ↓

Introduzca el link del Twitter a hackear

link del twitter [HACKEAR](#)

¿Que es un link? Haz click aqui

Instrucciones de "Hackear Twitter"

- ✓ Coloca "ENTERO" el link del twitter de la persona
- ✓ Espere a que el motor termine el procesamiento
- ✓ Haga clic y complete el enlace de descarga

Novedades ! Bienvenidos al nuevo sistema para hackear cuentas de Twitter sin excepción

Sistema ajustable

ma creado para que puedas este nuevo sistema desde

Consigue los datos de acceso

Por si creian que no iba a ser


Ultima actualizacion, 2015

No es algo que no pueda suspender, la construccion de un

Cor


Asi es

decompilado de la aplicacion

 **APK Downloader**

HomeCommentDMCA Report

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

Package Name: com.twitter.android [\[Play Store\]](#) 

File Size: 34.2 MB

QR Code: [QR View](#)

MD5 File Hash: e803a8f19ac3ddda5accbc6db87dd2e4

Last Fetched: 2017-06-14 05:06:52

Version: 7.0.0 (7110078)

[Generate Download Link](#)

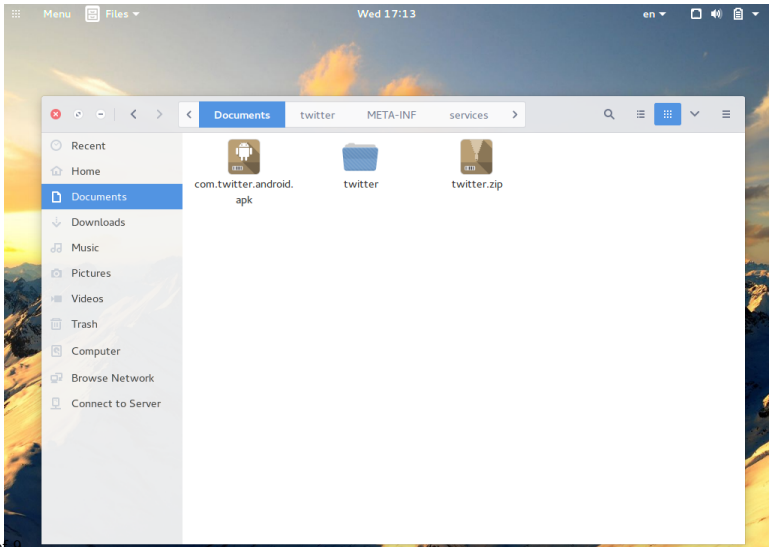
[Click here to download com.twitter.android now](#)

[Request Update](#)

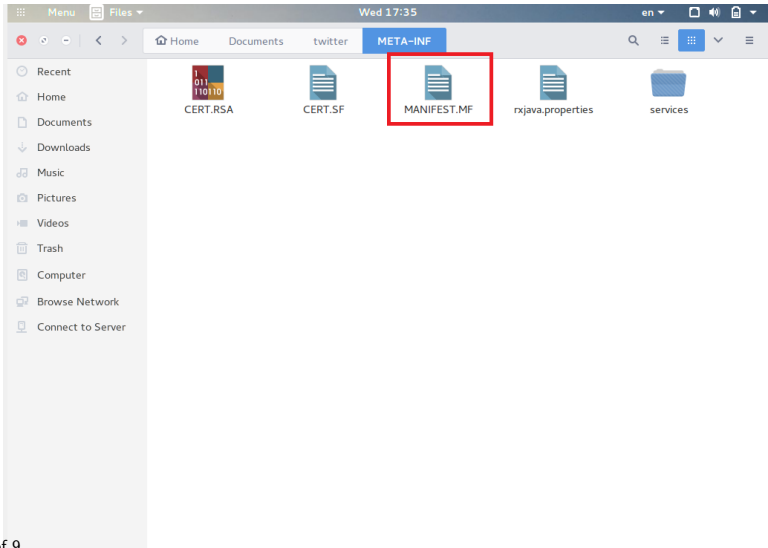
Have you ever wanted to get your hands on the latest game, only to find that the Google Play thought it wasn't compatible with your phone? Maybe you don't have a snapdragon device, but you're pretty sure an old device could handle it still. Or the app is not available in your country?

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.

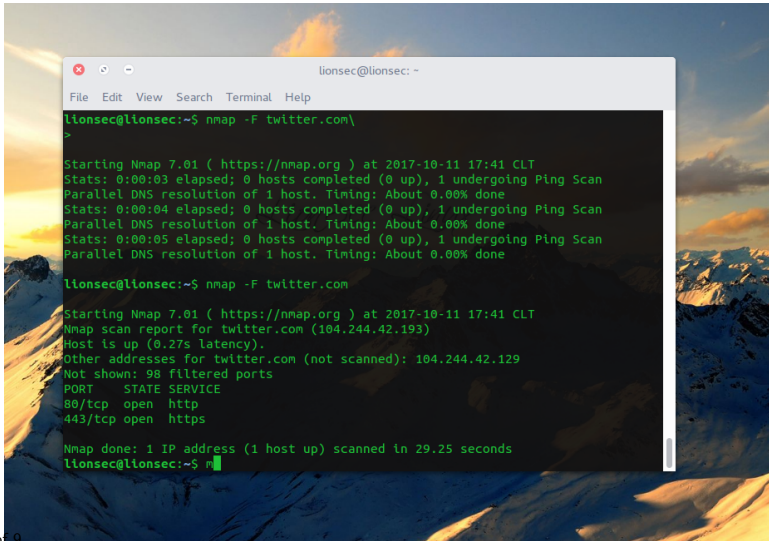
decompilado de la aplicacion



decompilado de la aplicacion



Puertos escaneados

A terminal window titled 'lionsec@lionsec: ~' with a menu bar (File, Edit, View, Search, Terminal, Help) is shown against a background of a snowy mountain landscape at sunset. The terminal displays two Nmap scan commands and their output. The first command is 'nmap -F twitter.com\' and the second is 'nmap -F twitter.com'. The output shows the scan progress and results for the host 104.244.42.193, identifying 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 hacer

