

Auditoria informatica a Twitter:Tercer incremental



UNIVERSIDAD
Finis Terrae
VINCE IN BONO MALUM

Jorge González

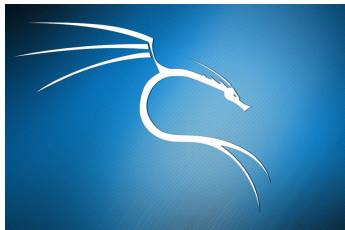
Profesor: Maximiliano Vega

Octubre / 25 /2017

Decompilación

Obtención de Archivos

Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría



Herramientas Para decompilar

Obtención de Archivos



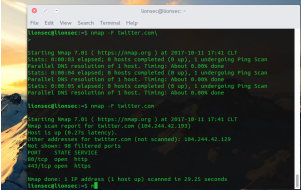
Apktool es una herramienta para la modificación de APKs

Escaneo de puertos

Obtención de Archivos

Escaneo de puertos con Nmap:

- Puerto 80 HTTP
- Puerto 443 HTTPS/SSL



```
lironex@lironex:~$ nmap -P -f twitter.com

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

lironex@lironex:~$ nmap -P -f twitter.com

Starting Nmap 7.01 ( https://nmap.org ) at 2017-10-11 17:41 CDT
Nmap scan report for twitter.com (104.244.42.120)
Host is up (0.17s latency).
Not shown: 99 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 20.25 seconds
lironex@lironex:~$
```

Decompilacion del APK

Obtención de Archivos

```
File Edit View Search Terminal Help
$ javac -h advanced -g prints advanced information.
$ javac -version prints the version then exits
$ aptool -i [install] -f framework [options] -o framework.apk
$ --framework-path <dir> Store framework files into <dir>.
$ --tag <tag> Tag frameworks using <tag>.
$ --apktool <dir> Optional file apk.
$ --force Force delete destination directory. (If you want to force)
$ --package <dir> The name of folder that only written. Default is apk.out
$ --framework-path <dir> Uses framework files located in <dir>.
$ --no-res Do not decode resources.
$ --no-ars Do not decode sources.
$ --framework-tag <tag> Uses framework files tagged by <tag>. (see this tag parameter apk -tag)
$ --apktool <dir> [optional] temp path.
$ --force-all Skip changes detection and build all files.
$ --package <dir> The name of apk that gets written. Default is dist/name.apk
$ --framework-path <dir> Uses framework files located in <dir>.

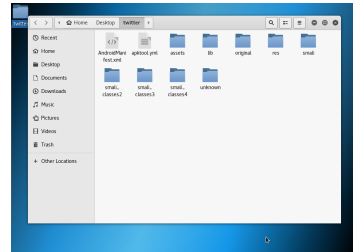
or additional info, see: http://l0b0p0ach0s.github.io/Apktool/
$ shell$ aptool -i -f http://github.com/Sec0ur1ty/Sec0ur1ty
$ shell$ aptool -i /root/.ssh/Sec0ur1ty/apk
$ aptool -i /root/.ssh/Sec0ur1ty/apk was not found or was not readable.
$ shell$ aptool -i /root/.ssh/Sec0ur1ty/apk
$ Using Apktool 2.2.4-dirty to twitter.apk
$ Loading resource table...
$ Decoding AndroidManifest.xml with resources...
$ Loading resource table from file: /root/.local/share/apktool/framework/1.apk
$ Merging manifest package...
$ Decoding file resources...
$ Decoding values */*.xml...
$ Baksmaling classes.dex...
$ Baksmaling classes2.dex...
$ Baksmaling classes3.dex...
$ Baksmaling classes4.dex...
$ Copying assets and libs...
$ Copying unknown files...
$ Copying original files...
$ shell$
```

aplicacion decompilada

Decompilación del APK

Obtención de Archivos

Carpetas
internas de la aplicación Twitter



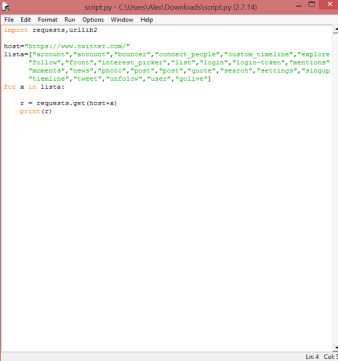
Android manifest xml

7 de 11

Busqueda de URLs

Obtención de Archivos

Script en python para la búsqueda de URLs validas con el host de twitter



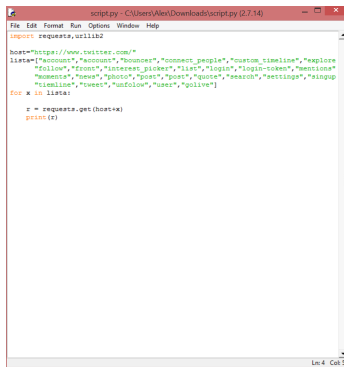
```
script.py - C:\Users\Alex\Downloads\script.py (2.7.14)
File Edit Format Run Options Window Help
import requests,urllib2

host="https://www.twitter.com/"
lista=["accounts","account","bounces","connect_people","custom_timeline","explore","follow","front","interest_picker","list","login","login-token","mentions","moments","news","photo","post","post","quote","search","settings","signup","timeline","tweet","unfollow","user","golive"]

for x in lista:
    z = requests.get(host+x)
    print(z)
```


Busqueda de URLs

Obtención de Archivos



```
File Edit Format Run Options Window Help
import requests,urllib2

host="https://www.twitter.com/"
lista=["account","account","bouncer","connect_people","custom_timeline","explore","follow","front","interest_picker","list","login","login-token","mentions","moments","news","photo","post","post","quote","search","settings","singup","timeline","tweet","unfollow","user","golive"]

for x in lista:

    z = requests.get(host+x)
    print(z)
```

Script en python para la búsqueda de URLs validas con el host de twitter

Obtención de Archivos

Script en python para la búsqueda de URLs validas con el host de twitter

