APP 01

GOOD

1) Explicar como funciona la aplicación. Webview simple apuntando fuera.
2) ¿Porque se ha elegido un Webview? Compatibilidad para hacer apps en muchas plataformas.
3) Enseñar el código sin ofuscar.
4) Contexto: Subida en el Market. Firma propia => identificador unico e integro
5)

BAD

1) Abrir como ZIP y descomprimir. Explicar para que sirve cada fichero. Firma.
    1. META-INF: (mismo problema que el update.zip)
        1. MANIFEST < hashea ficheros de dentro
        2. CERT.SF < firma las 3 lineas de cada fichero
        3. CERT.RSA < genera clave
    2. Explicar como seria para saltarselo ("keys.inc")
2) Explicar apktool --> smali / baksmali
3) Explicar dex2jar.
4) Explicar dexdump. $ cd /mnt/sdcard; $ dexdump itis.dex > itis.txt
5) Compilación bydefault con simbolos de debugging, sin optimizar, ...
6) ¿Como se injectaria código malicioso?
    1. Reconstruir con apktool modificando el assets
    2. Reconstruir con la URL
7) Técnica de código dinámico -> mostrar código
    1. Serialize / Unserialize
    2. Descargar y ejecutar
8) Explicar que se podría hacer: aleatoriedad y fuera del control del Market
9) Decompilar el Ddream y explicar funciones principales
    1. Manifest.xml
    2. Firma
        1. CERT.RSA
    3. Assets
        1. exploid -> 2.1 NETLINK to udev -> setuid
        2. rageagainstthecage -> 2.2 NPROC – forks -> setuid() ADBD -> ADB
        3. /profile -> sh
        4. sqlite.db -> APK
    4. .dex
        1. AlarmReceiver -> instala profile
        2. Setting -> if (new File("/system/bin/profile").exists())
        3. Setting -> <ClientInfo><Partner>%s</Partner><ProductId>%s</ProductId><IMEI> %s</IMEI><IMSI>%s</IMSI><Modle>%s</Modle></ClientInfo></Request>
        4. sqlite.db_apk -> DownloadManager
10) Subir a black market
11)

APP 02

GOOD

1) Encender maquina virtual
2) Igual que la anterior, ofuscada con proguard
3) Añadir "proguard.config=proguard.cfg"
4) ¿Que es Androguard? -> Framework con herramientas (frontend)
    1. Queria: utilizar Androguard para buscar coincidencias -> Mostrar opcion risk 0.0
    2. Mostrar /output/
    3. Ejecutar ficheros, mostrar output
    4. Comentar otras opciones ->
        1. Diff entre versiones
        2. Graficos
        3. Reversing -> malware
        4. Permisos
        5. Riesgo
    5. http://code.google.com/p/androguard/wiki/Usage
5)

BAD

1) ¿Que ofrece el Proguard?
2) Maneras de coger la URL
    1. Reversing
    2. Usar Sniffer -> usa texto claro
3) Entrar a la web
4) Vector de ataque
    1. Posible SQL Injection -> webservices
    2. XSS script
    3. Marco de autorización -> admin.php
    4. files/ - List Files
5) Retrace -> Recordar app
6) /mnt/sdcard/stack.log
7) Enseñar ProguardGui - root\tools\android-sdk\tools\proguard\bin
8) keystore – Fuzzing y obtencion de acceso
9) cacerts.bks -> pass -> changeit/null
10)

APP 03

GOOD

1) Cambio a aplicación nativa DEX (sin JNI) - Ofuscada
2) Ahora va por SSL, no podemos ver en claro hacia donde va
3) Fatal error -> Admite cualquier SSL
4)

BAD

1) Sniffar 3G , GSM, bluetooth -> Taddong
2) Sniffar Wifi
    1. Al vuelo -> Arpspoofing & webmitm & ssldump
        1. Linux -> Modo Master
        2. Depende de la Tarjeta Wifi
        3. Conectar a la misma red
    2. Ataque del hotspot
    3. DNS falseado
        1. Versiones
            1. Cambiar DNS y apuntar a /, registrando Logs
            2. Crear el fichero a donde apunta y hacer que registre la peticion
        2. Wireshark
        3. Cambiar DNS en "wifi"
        4. cd C:\Users\Martes13\root\id\GTUG\app\dnspentest\bytecode
        5. java ServerKernelMain 178.33.118.102 192.168.1.4 (fail)
        6. matar proceso (TCPView)
        7. Poner el server WAMP a correr. Mode Online!!
        8. Certificados
        9. C:\wamp\www\gtug\auth.php
        10. ipconfig /flushdns
        11. ipconfig -> mirar ip
        12. java ServerKernelMain 178.33.118.102 192.168.1.4
        13. Reiniciar conexion Android
        14. Reiniciar "netsh wlan stop hostednetwork"
        15. Reiniciar "netsh wlan start hostednetwork"
        16. ipconfig /displaydns
        17. tcp.port eq 443
        18. Logs del servidor apache
3) Reversing en local

A)
getprop net.dns1
192.168.2.1
setprop net.dns1 x

B)
adb remount
adb push hosts /system/etc/hosts

C)
ip route list
ip route add 192.168.1.0/24 via 192.168.2.1 dev eth0

4) Analisis de datos
5) ¿Cuando se guardan?
    1. AndroidAuditTools
    2. C:\Users\Martes13\root\tools\android\usr_local_bin\androidAuditTools\bin

6) - Que guardan
    1. > adb shell
    2. $ tar zxvf gtug.third.backup.tgz
    3. $ sqlite3 -csv /mnt/sdcard/data/data/gtug.third/databases/GTUG
    4. > .dump
7) WhisperCore – Whisper sys
    1. TextSecure – SMS encriptados -> cache y aviso
    2. FlashBack – Backups en la nube
    3. RedPhone – Llamadas encriptadas
    4. Permisos, encriptacion, ... -> C:\Users\Martes13\root\id\GTUG\app\whispercore-n1-0.5.2\images\system
        1. build.prop -> 2.3.4
        2. apps

APP 04

GOOD

1) Applicación con protección a través de telefono (sólo miembros VIP)
2) BroadcastReceiver
3) Supuestamente ofuscada
4) Concepto equivocado del desarrollador (no es posible modificarlo desde el movil = no es modificable)

BAD

5) Probar un movil cualquiera -> Localizar un móvil valido
6) Buscar por Linkedin -> Fernando Cejas -> cambiado por 123456789 (num secreto)
7) Pasar al emulador
8) ERROR -> tecnica antidebugging -> Todas parcheables
    1. Comprobar DEVICE_ID (android-id == null)
    2. Comprobar IMSI (subscriber ID)
    3. Comprobar /proc/cpuinfo
    4. Comprobar sensores (vibrar)
    5. Comprobar Qemu
9) Localizar ficheros que tienen a ver con la emulación
    1. android-sdk\tools\emulator.exe
    2. android-sdk\platforms\
    3. android-sdk\platforms\android-8\images
    4. C:\Users\Martes13\.android
10) Modificar emulador.exe
11) Buscar: CIMI y CGSN
12) Reiniciar emulador
13) Aprender de los Custom errors
    1. Probar un numero cualquiera
    2. Probar el de Fernando
    3. Probar inputs
    4. Usar script de fuzzing
14) Mostrar código telnet_attack.py
15) Lanzarlo y ver resultado
16) Explicar DroidBox -> sandbox que logea
17) Explicar TaintDroid -> APK que muestra lo que se logea
18) GSoC 2011
19) pseudo.SOLUCION: incluir librerias criticas al APK (like Whatsapp)