CTF Training Camp
Topic 4: Miscellaneous

WANG Xianbo

Outline

□ Basic Digital Forensic

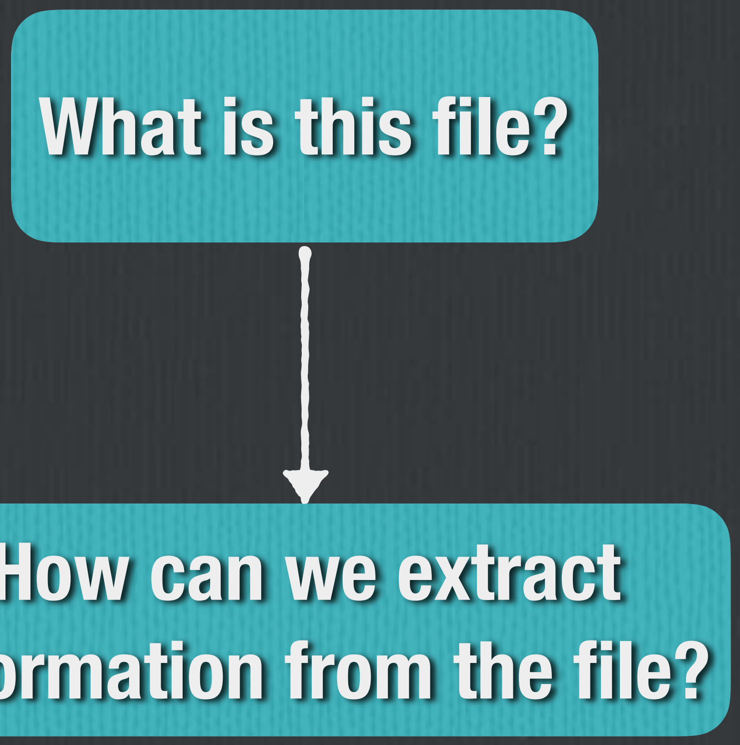
□ Basic Infrastructure Hacking

□ Basic Android Security

Digital Forensic

- □ File analysis
- □ Network trace analysis
- □ Disk/Memory image analysis

File Analysis



What is this file?

How can we extract information from the file?

Identify File Type

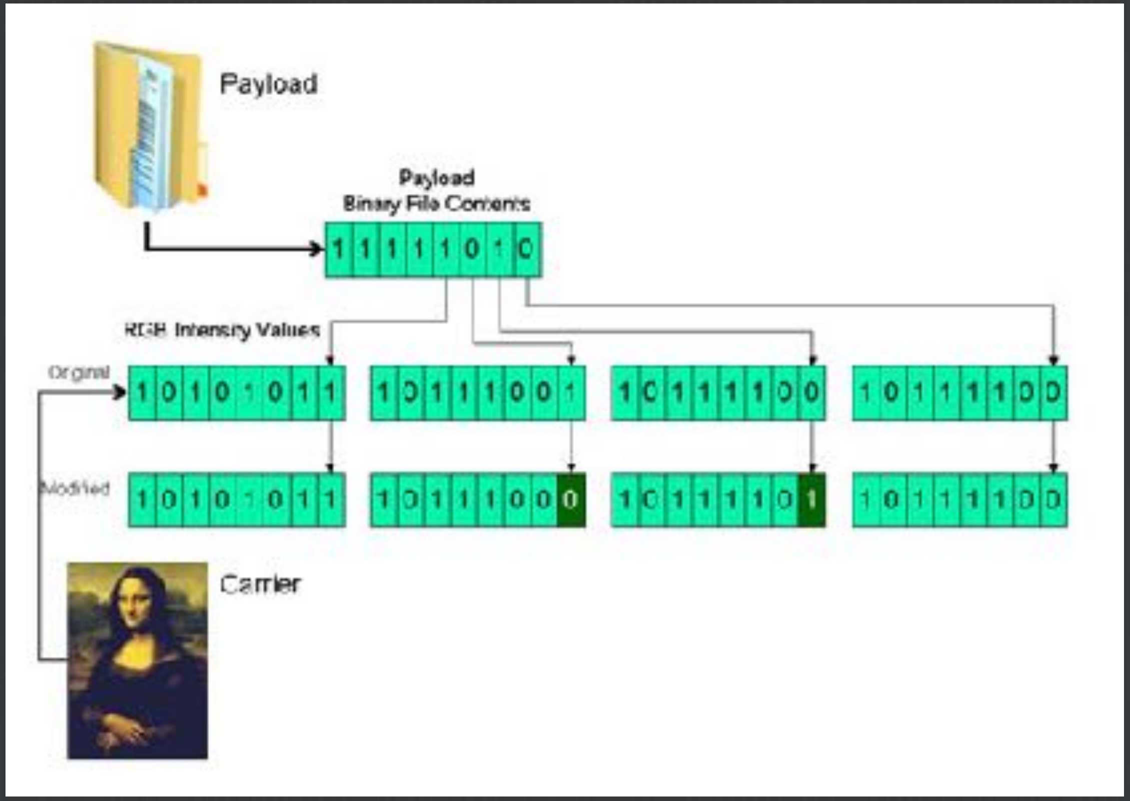
- File signature: a piece of special data at the beginning of file
  - List of common file signatures
- Demo: file command
- Multiple file signatures?
  - Tools: binwalk, foremost

Open the File

- □ Google tools to open the file
  - □ e.g. compressed: decompressor, db file: db viewer
- □ Cannot open? Repair it !
  - □ Read file format specification: file header, metadata
  - □ Tool: 010 Editor's Template Engine

Find Hidden Information

- □ Hide in metadata
  - □ Documents, media files
  - □ Tools: strings, exiftool
- □ Steganography (隱寫術)
  - □ Media files: image, radio
  - □ Tools: stegsolve, Audacity



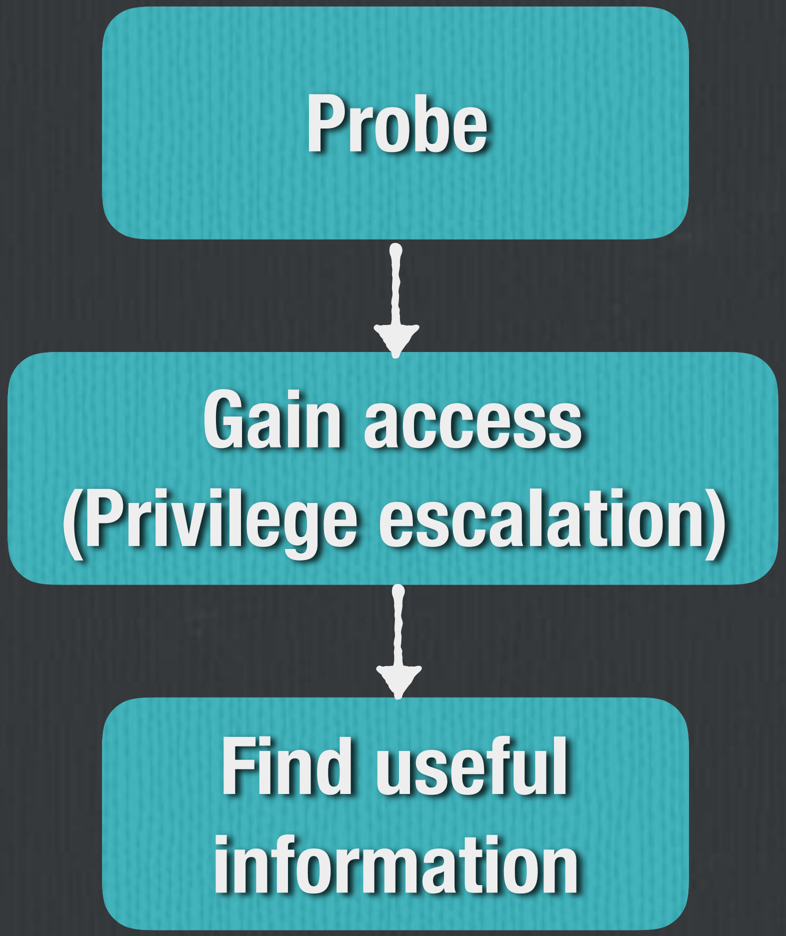
Network Trace Analysis

- □ One tool for all: Wireshark
  - □ Read plaintext traffics
  - □ Extract files from traffics
  - □ Decrypt encrypted traffics
- □ strings, binwalk sometime give you a shortcut !!

Disk/Memory Image Analysis

- Disk image
    - Tools: The Sleuth Kit
        - https://wiki.sleuthkit.org/index.php?title=TSK_Tool_Overview
    - Identify file system: fsstat
    - Browse file: fls, mount or load in VM
    - File recovery: icat, testdisk, extundelete
- Memory image
    - Tools: volatility
        - https://github.com/volatilityfoundation/volatility

Infrastructure Hacking



Probe

Gain access (Privilege escalation)

Find useful information

Probe

- Nmap
  - Host discovery: nmap -sn 192.168.1.0/24
  - Port scan: nmap -p22,80,400-500
  - Service fingerprint: nmap -sV
  - Advanced: nmap —script

Gain Access

- Tools: metasploit, exploit-db
- Remote exploit
  - Find vulnerable service / program
    - e.g. SMB, Web Applications, FTP
  - Weak password, brute-force
- Privilege escalation
  - Local: kernel exploit, misconfiguration, password crack
  - Intranet: ssh keys, domain controller, remote desktop

Android (App) Security

□ Traffic interception

□ APK reverse engineering

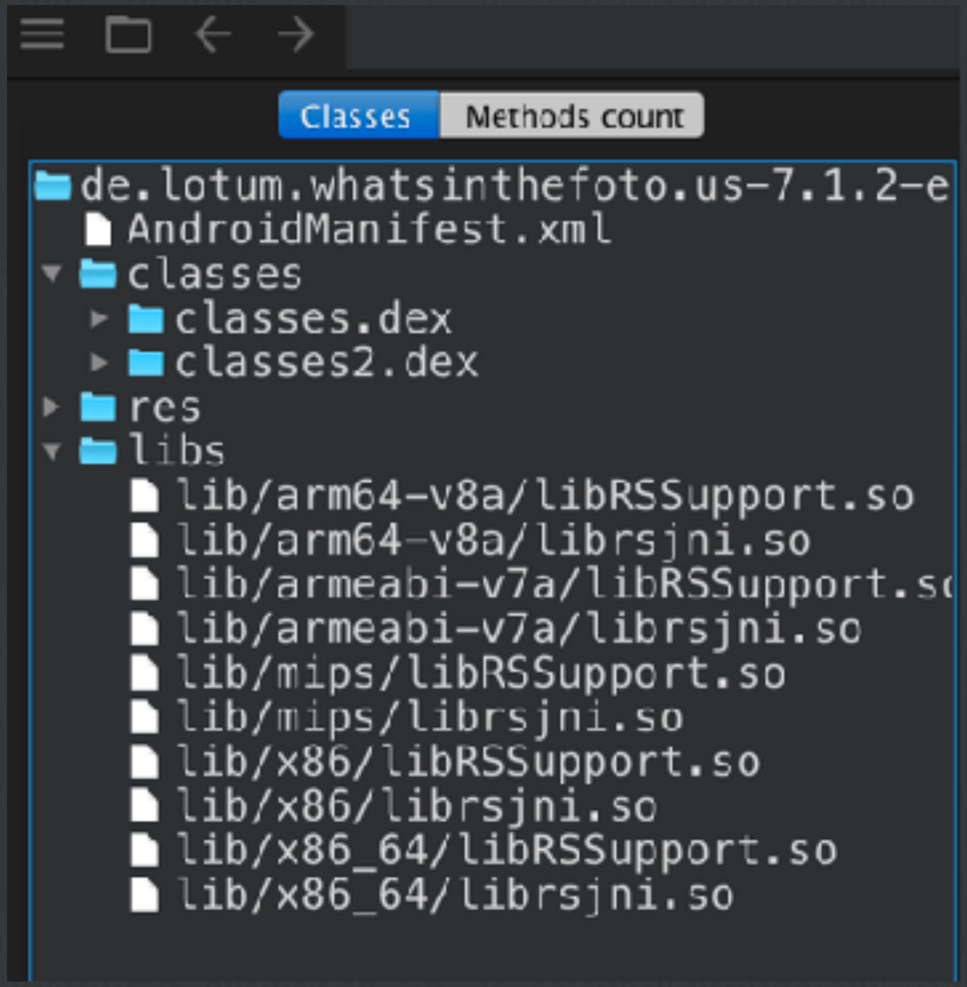
□ App hooking

Traffic Interception

- □ Set proxy: e.g. Burpsuite, mitmproxy
- □ HTTPS
  - □ Install custom certificate on mobile device
  - □ Certificate pinning: JustTrustMe

Reverse Engineering

- □ APK file is a ZIP package
- □ APK -> bytecode -> JAVA code
- □ Tools: jadx
- □ For .so files: IDA pro



```
de.lotum.whatsinthefoto.us-7.1.2-e
  AndroidManifest.xml
▾ classes
    ▸ classes.dex
    ▸ classes2.dex
▸ res
▾ libs
    lib/arm64-v8a/libRSSupport.so
    lib/arm64-v8a/librsjni.so
    lib/armeabi-v7a/libRSSupport.s
    lib/armeabi-v7a/librsjni.so
    lib/mips/libRSSupport.so
    lib/mips/librsjni.so
    lib/x86/libRSSupport.so
    lib/x86/librsjni.so
    lib/x86_64/libRSSupport.so
    lib/x86_64/librsjni.so
```

Hooking

- □ Tools: Xposed, Magisk
    - □ Xposed QuickStart
- □ Dynamic analysis
- □ Modify App
- □ Fun demo: game hacking

Future Training Plan, Q&A

□ We will host a mini CTF in CUHK in later March

□ Form team(s): participate weekend CTFs, weekly / biweekly review