- **How to bypass Root Detection with several techs?**

  Hook isRooted function

  Magisk : change app name

  Zygisk : deny application

  Frida Scripts

  Medusa Tool

- **How to bypass SSL Pinning with several techs?**

  Hook IsEncrypted function

  NSC File

  Trust Manager

  Frida Scripts

  Medusa

  Downgrade app to 6.0 version

- **What are the tools you are using?**

  ApkTool

  MobSF

  Medusa

  Frida Scripts

  Drozer

  Objection

  IDA, JadX

- **What is the diff between arm and x64/x86?**

  x64/x86 => Emulator

  arm => physical device

- **What will you do if you found source code obfuscated?**

  Automated tools like:

  ProGuard Deobfuscator

  Bytecode Viewer

  Simplify

  Revenge

  Xenotix APK Decompiler

- **How do you know there is native lib?**

  function name = native , then use frida spawn :enumexportssync to search for info about the library, then hooking the library by using frida inspector to the lib address in the code.

- **What are android permissions?**
  android.permission.INTERNET
  android.permission.ACCESS_NETWORK_STATE
  android.permission.RECORD_AUDIO
  android.permission.READ_EXTERNAL_STORAGE
  android.permission.WRITE_EXTERNAL_STORAGE
  android.permission.RECIEVE
- **What are diff between static and dynamic broadcast receivers with functions?**
  static: run anytime , OnRecieve
  dynamic: run in runtime only , EmailBroadCastRecv
- **How does Zygisk work?**
  zygisk use ptrace function to trigger all the calls and bypassing root detection, bypass SafetyNet
- **Explain a dynamic scenario?**
  change NSC File to trust user certificate, then rebuild the file with apktool and resign the app.