

CYBERSECURITY TRAINING

(WEEK 3 – Day1)

ANDROID HACKING

1. Structure of Android OS

- **Linux Kernel:** It is the core part of the Android operating system that interacts directly with hardware and manages low-level system tasks like memory, process, and power management.
- **System Libraries:** These are essential libraries written in C/C++ that provide various functions such as graphics rendering (Skia), database support (SQLite), and web rendering (WebKit).
- **Application Framework:** It provides high-level building blocks and APIs used by

developers to build Android applications, such as Activity Manager, Window Manager, and Content Providers.

- **Android Runtime (ART):** It is responsible for running Android apps. It compiles app code from bytecode into native instructions at install time (ahead-of-time compilation).
- **Applications:** These are the user-installed apps or pre-installed system apps that run on top of the framework using Java/Kotlin.

2. Common Android Vulnerabilities

- **Insecure Data Storage:** Sensitive information like passwords, tokens, or user data is stored in unprotected files or preferences, which can be accessed by other apps or attackers.

- **Improper Access Control:** App components like Activities or Services are left exposed to other apps, allowing unauthorized access or functionality misuse.
- **Insecure Communication:** Apps transmit sensitive data over unencrypted channels (like HTTP), making it vulnerable to man-in-the-middle attacks.

3. Tools for Testing Android Applications

- **APKTool:** A reverse engineering tool used to decompile and recompile Android APK files. It helps analyze and modify app resources and code.
- **MobSF (Mobile Security Framework):** An automated tool that performs static and dynamic security analysis of Android apps to detect vulnerabilities.

Practical Implementation

```
C:\Windows\System32\cmd.exe
(c) Microsoft Corporation. All rights reserved.

C:\Users\bhavn\Downloads\platform-tools-latest-windows\platform-tools>adb devices
List of devices attached
084333127B020766      device

C:\Users\bhavn\Downloads\platform-tools-latest-windows\platform-tools>adb tcpip 5555
restarting in TCP mode port: 5555

C:\Users\bhavn\Downloads\platform-tools-latest-windows\platform-tools>adb connect 192.168.29.60
connected to 192.168.29.60:5555

C:\Users\bhavn\Downloads\platform-tools-latest-windows\platform-tools>adb shell am start -a android.intent.action.VIEW -d https://www.youtube.com
Starting: Intent { act=android.intent.action.VIEW dat=https://www.youtube.com/... }

C:\Users\bhavn\Downloads\platform-tools-latest-windows\platform-tools>adb shell am start -a android.settings.SETTINGS
Starting: Intent { act=android.settings.SETTINGS }
Warning: Activity not started, its current task has been brought to the front

C:\Users\bhavn\Downloads\platform-tools-latest-windows\platform-tools>adb shell am start -a android.intent.action.DIAL -d tel:7006009643
Starting: Intent { act=android.intent.action.DIAL dat=tel:xxxxxxxx }

C:\Users\bhavn\Downloads\platform-tools-latest-windows\platform-tools>adb shell am start -a android.intent.action.CALL -d tel:7006009643
Starting: Intent { act=android.intent.action.CALL dat=tel:xxxxxxxx }

C:\Users\bhavn\Downloads\platform-tools-latest-windows\platform-tools>adb disconnect
disconnected everything
```