Rooting Overview

You need to Modify Android OS because Stock Android OS doesn't provide root privilege to the user out of the box

Modify Android OS

After Booting into Android OS

Find Vulnerability in Android OS that escalate User Privilege

Gives root shell

Getting root shell is breakthrough, you can do whatever with root shell to Android file system

Before Booting into Android OS

Unlock Bootloader

Unlocked bootloader allows you to run your own OS by flashing the image file to specific Android Partition.

Change the entire Android System Image

Unpack Android System Image (system.img) or get it from manufacturer or trusted third party provider

Modify system image by changing build type or by adding some SUID su binary

Gives root shell

Commercial Android devices uses *User* build which disallows root access via shell. But It can be turned into the *userdebug* or *engineering* build which gives root access through the shell by setting *ro.secure = 0*.

Update Android System Image by applying OTA (Over The-Air) updates

Stock Recovery only allows you to apply OTA updates authorized by manufacturer. We need to replace Stock Recovery with Custom Recovery to apply our own OTA updates which bypasses signature verification

Replace Stock Recovery with Custom Recovery

Custom Recovery will run *update-binary* from the OTA package to apply updates

Basically *update-binary* is a binary file that runs *updater-script* that guides recovery to install files from OTA package to main Android OS to achieve rooting.

Gives root shell