Unit 1

Index

Basics

Things that attackers usually want are PII (Personally Identifiable Information).

One thing that all security thingies should is the CIA triad. Confidentiality, Integrity, Availability.

Confidentiality: Only those who should have access have that access. **Integrity:** Data is edited by the right people. **Availability:** Making sure shit is useable/ available.

The AAA:

Authentication

Authorization

Accountability

There are ten security principles

Privileged Programs:

2 main types:

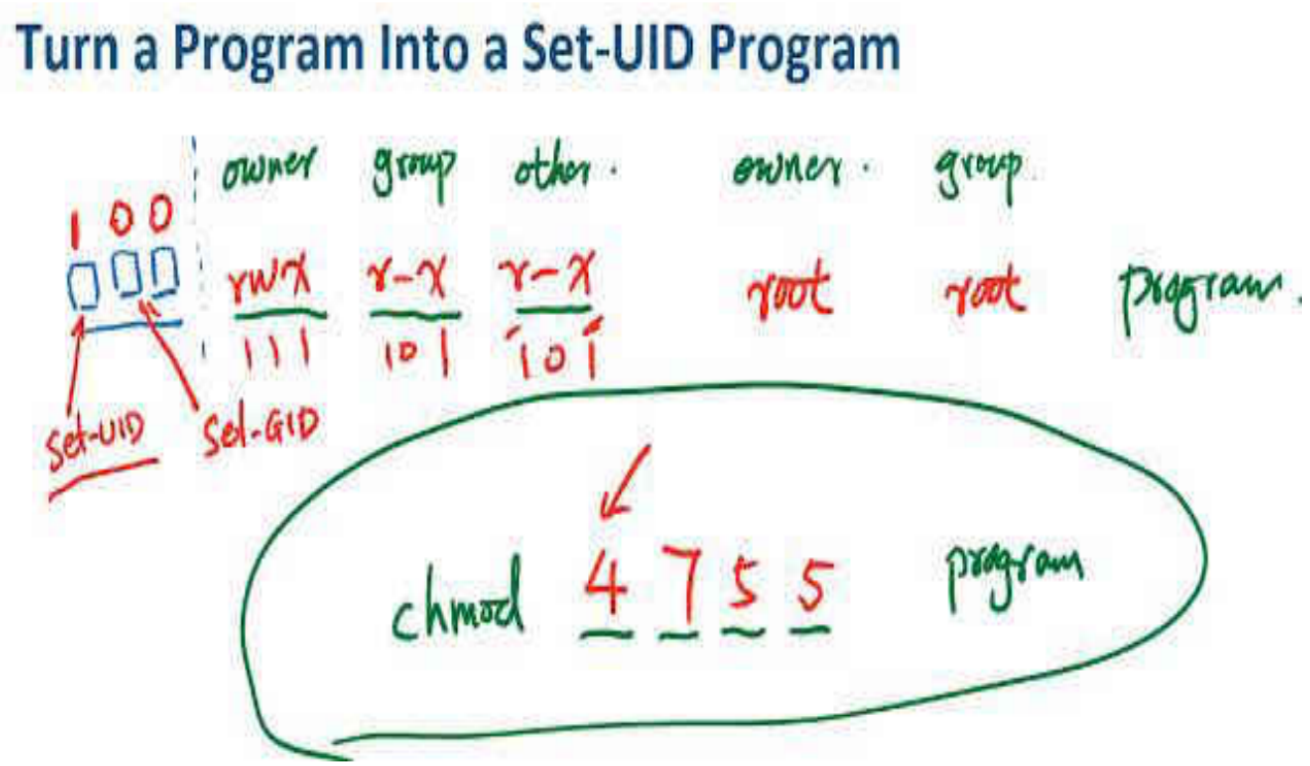
Daemon: This is when call another program to do the privileged action

Set-UID: This is where we upgrade our permissions.

Set-UID:

Every process has 2 IDs. Real UID and effective UID. Access control is based on **Effective UID**.

During regular execution RUID = EUID. During privileged run we change EUID.



Risk Analysis

We preform risk analysis based on different parts of the program.

Attack Surface

This is the places where a potential attack can happen.

User Inputs

- Format String Vulnerability
- Buffer Overflow
- Change Shell
- Bad Sanitization

System Inputs

dunno

Environment Variables

This is usually where we have malicious env vars being called.

These vars are usually called through fork() and execve().

Shell variables are not environment variables. The shell variables copy the required env vars according to the program that is running. These are inherited by child processes created by fork().

Dynamic linking is the real time walla one.

Capability Leaking

This is where we downgrade our privileges but we retain rights to some files n stuff.

Invoking programs

This is where we allow users to define the entire command they want to run.

To combat this we use execve(). This has 3 inputs, the command name, data and env vars. Here we separate the command name and data so there is no mismatch.