**Misconfigurations**

A configuration, of any kind, that allows an attacker to get a foot-hold into the machine

* Anything from config files to permissions on the system

So knowing how to set up Apache

* Knowing where the logs the ae
* Knowing how it should be configured

Are all important as a red teamer when trying to find exploits

**Why is this important?**

* Difference between gaining access or not
* Ability to escalate privileges
* Can allow for password disclosure

**Examples**

* /etc/passwd (holds hashed) having global write
  + With global write permissions, you can add a usr to passwd then you can gain access to the machine
* Config file for a webservice, viewable without authentication from outside the host
  + Don’t just dump config.ini onto your webservice in cleartext, good to use .php or have it encrypted and decrypted on the webservice with certificates, or another interpreted language
* Sticky bits enabled on a binary that can be used to elevate privileges, such as VI or Man
* Usr and pwd left on defaults is also technically a misconfig