Hardening refers to providing various means of protection in a computer system. Protection is provided in various layers and is often referred to as defense in depth.
Hardening: **WHAT**

- Eliminate as many risks and security threats as possible
  - Strong passwords, no disclosure of personal secrets
  - Firewall, IDs, disabling unnecessary services to reduce points of access to the system
  - Keeping the system patched, and so on...

- Hardening on multiple layers, we’re going to harden *system calls!*
Two basic approaches used to deal with security vulnerabilities:

**REACTIVE VS PROACTIVE**

Finding and patching vulnerabilities is a good thing for the good guys (us), but...

...what about **0-day** exploits?
Windows O-Day Exploit
Selling @ $90,000
Hardening: **HOW**

- Linux: ownership and permissions
- Will my mail server *ever* need to acquire my paypal credentials?
- The goal is to implement a **fine-grained** security
Hardening: **HOW**

- Three specific examples:
  - apache2 policy generation
  - VerySecureFTPDaemon 2.3.4 smiley backdoor
  - Apache exploitation - ShellShock CGI vector
Hardening: **SO WHAT?**

Our goal is to show how ad-hoc **policies** can successfully prevent an exploited process to damage our system, **no matter what the exploit is!**
Hardening: **SO WHAT?**

Many security suites to fit our needs...
Hardening: *SO WHAT?*

...Is there a best one?

Today we will show the tools and how to use them... the rest is up to you.