**Hardening:**

Hardening is the process of securely deploying systems with the practice of ‘least privilege’. Hardening includes:

* Understanding what you actually need to run on the system
* Documentation (Policy, Standards & Guidelines)
* Operating systems
* Virtual servers
* Coding
* Application settings
* Database setup & configuration
* Network devices
* Portable device

**Platform hardening:**

Platforms are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the platforms are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service

DEFINITIONS

* Hardened System
  + (H) Is the final state we are trying to achieve
* Baseline OS Hardening
  + (Bos) Is the Baseline Operating System hardening
* Application / System Function Hardening
  + (Af) Is any hardening of applications that may reside on top of the operating system, such as Apache, IIS, Oracle or specific functions, such as File/Print, DNS/DHCP, etc
* Base Hardening
  + Base hardening = Baseline Operating System Hardening + Application or System Function hardening
  + (B) = (Bos) + (Af)
* Custom Hardening
  + (C)Is any additional hardening applied to the system, such as’ Specialized Security Limited Functionality’ settings, DMZ settings, addition system service settings (KIOSK, Bastion Host, etc), custom OS specific security controls(TCPWrappers, Bastille, etc.)
* Virtual System (Needs Host OS)
  + (C)Is the Virtual Machine hardening
* Is the Virtual Machine hardening
  + (VOS) Is the Virtual Server hardening - VM Ware ESXi

**Hardening Formula**

Putting System Hardening into a mathematical formula:

H = Hardened System

B = Base Hardening

C = Custom Hardening

So…

H = B+C

Hardened System or Secure Deployment

Custom Hardening

Application / Function Hardening

In the layered security

Hardened System or Secure Deployment

Baseline OS Hardening

Baseline OS Hardening

**Hardening Virtual Systems**

For Virtual Operating System:

H = Hardened System

Vos = Virtual OS Hardening

B = Base Hardening

C = Custom Hardening

So…

H = Vos+B+C

Also stated as layered security:

Hardened System or Secure Deployment

Virtual OS Hardening