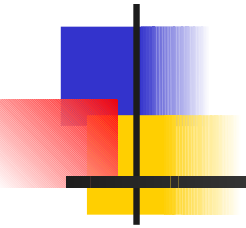


SEC520

System Hardening

Today's Objectives

System Hardening Overview:

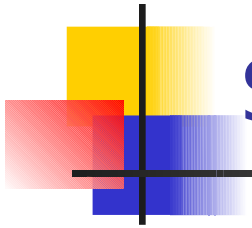
- Purpose
- Rules of Internet Security

Rule of Preventative Action:

- Patches, User Account Administration, Human Issues

Rules of Least Privilege / Trust:

- Lock-down booting options / Separate Partitions
- Separate Servers
- Turning off Unnecessary Open Ports (Services)
- AAA Protocol (Authentication)



System Hardening

- Now that you can confirm that there are vulnerabilities in your Linux and Windows servers, we need to "**harden**" these servers to make them **less vulnerable**. We will concentrate on hardening your Linux server in the next 2 weeks, and then harden your Windows server later in this course.

- Instead of "getting spun-off" with vulnerability testing, we need to consistently follow a **set of procedures, guidelines or rules** to help make our servers more secure.

- Believe it not, **the biggest weakness of any server is associated with humans**, and how they fails to adopt a solid framework used to make servers more secure.

8 Rules of Internet Security

From "*Inside the Security Mind: Making the Tough Decisions*", Kevin Day

Rules	Description
1. **Rule of Least Priviledge**	Allow only as much access as is required to do the job, nothing more.
2. **Rule of Change**	Any change must be managed, coordinated, and considered for possible security implications.
3. **Rule of Trust**	Understand the full effect before extending trust to anyone or anything.
4. **Rule of the Weakest Link**	Focus must be evenly "spread-out" in all aspects of security, not just on specific areas.
5. **Rule of Separation**	Diversity server tasks (don't put all eggs in one basket)
6. **Rule of 3-Fold Process**	Implementation, Monitoring, Maintenance
7. **Rule of Preventative Action**	Stay current, Regular testing, Find vulerablities
8. **Rule of Response**	Response plan, React quickly, Enforce Rules, Education

Rule of Preventative Action

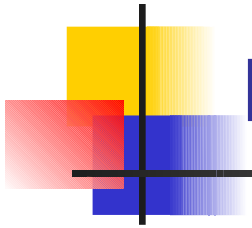
Ironically, the most common weaknesses facing Internet security are **human error.** For Example:

- Not Implementing **BIOS boot password** / **Grub boot password**.
- Not downloading/installing **security patches**.
- Failing to consider **Internet security issues when implementing a modification or change to the system**.
- Not **removing accounts of terminated employees**.
- Not having a **comprehensive, systematic plan for Internet security**.
- **Concentrating too much on "Attack"** as opposed to viewing "big picture" to better protect system.

Rule of Separation

These elements tend to be more technical in nature, although it is important to contain these elements within a **consistent Internet Security framework**:

- Boot Lock-down / Keep Separate Partitions
- Servers for Limited, Specific Purposes
- Close Unnecessary Open Ports (Services)
- Adopt AAA Protocol / Adopt Encryption Protocols



Rule of Separation

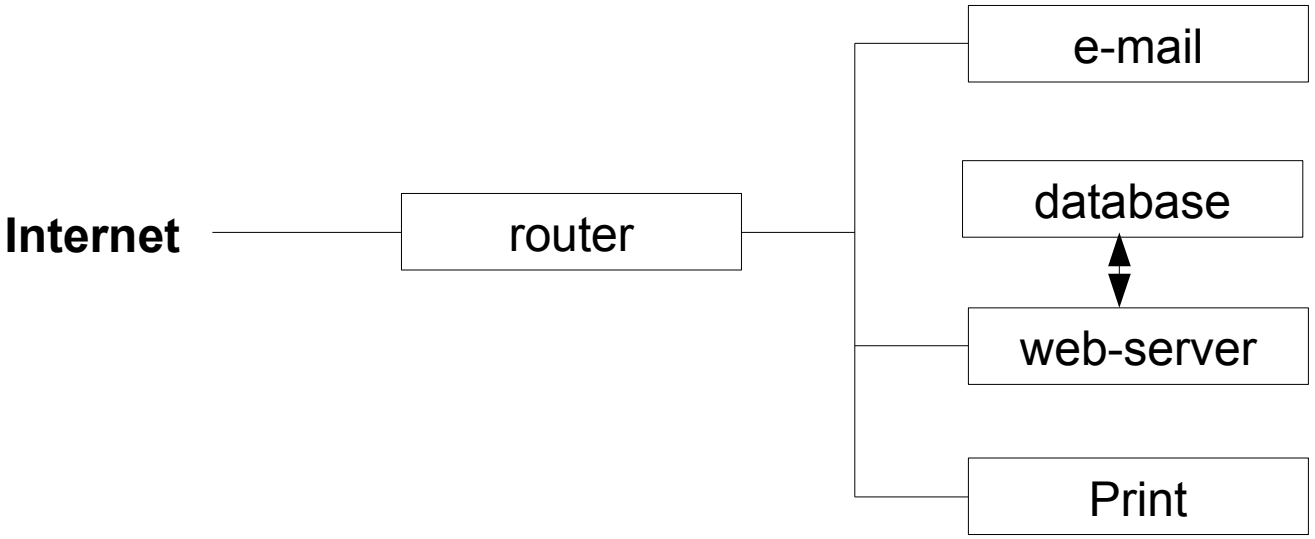
Boot Lock-down / Keep Separate Partitions:

- Set a **BIOS password** for server / clients.
- Set BIOS to **boot from hard disk** (not removable media)
- Set a **Grub Boot password**
  - If not, user could boot in **level 1** as **superuser** and have unrestricted access to the computer.
- Keep **Separate Linux Partitions** :
  - Eg: **/boot**, **/var**, **/tmp**, **/usr**

Rule of Separation

Servers for Limited / Specific Purposes:

Instead of setting up one server for many tasks, better to set-up several servers for specific tasks. Can use AAA protocol to protect access to critical servers.



Rule of Separation

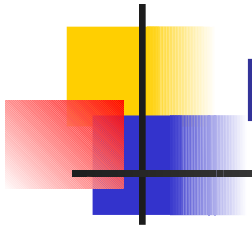
Close Unnecessary Open Ports (Services):

The motto for Backtrack Linux says it all:

"The quieter you are, the more you hear"

In other words, if your server is running too many ports (services), there are too many elements to try to monitor and protect. For example, try running the **netstat** or **nmap** command for multiple open ports.

By turning-off unwanted services, the more time to focus on keeping the running services less vulnerable to attacks. This can allow for running **IDS** (intrusion Detection System) to better report penetration attempts.

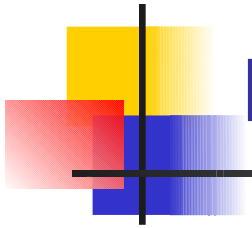


Rule of Separation

Adopt AAA Protocol:

AAA Protocol stands for:

Authorization, **Authentication**, **Accounting**



Rule of Separation

Adopt AAA Protocol (WikiPedia Definition):

Authentication

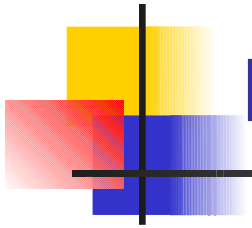
- Identity is authenticated (eg. passwords, one-time tokens, digital certificates).

Authorization

- whether a particular entity is authorized to perform a given activity.

Accounting

- tracking of network resource consumption by users for the purpose of capacity and trend analysis, cost allocation, billing.



Rule of Separation

Athentication Methods:

PKI

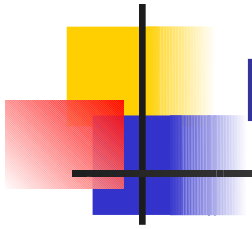
- Stands for **Public-Key Infastructure** which is a method/framework to store digital certificates (trust user). For example, public and private key cryptography (SSH)

PAM

- Stands for **Pluggable Authentication Module** which is a method to authenticate users when running APIs (Application Programming Interfaces). Rules are set in PAM configuration files (modules) to extend autentication to other application programming Interfaces (thus setting limits; for example, length of time).

Kerebos Protocol

- A protocol to **allow "nodes" to authenticate over unsecure networks**. Kerebos prevents against eavesdropping (eg. "man in the middle" attacks)



Lab Time

Start Working on:

Lab 4: Linux System Hardening (Part 1)