System Hardening and Baselines

A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.

News

- https://blog.qualys.com/vulnerabilities-threat-research/2023/10/03/cve-2023-4911-looney-tunables-local-privilege-escalation-in-the-glibcs-ld-so
- https://www.cisa.gov/news-events/news/joint-advisory-top-cyber-misconfigurations-highlights-urgency-software-manufacturers-incorporate

Controls Standards

The foundation of your work

CIS - 18 Critical Controls

- 1. Inventory and Control of Enterprise Assets
- 2. Inventory and Control of Software Assets
- 3. Data Protection
- 4. Secure Configuration of Enterprise Assets and Software
- 5. Account Management
- 6. Access Control Management
- 7. Continuous Vulnerability Management
- 8. Audit Log Management
- 9. Email and Web Browser Protections

Source: https://www.cisecurity.org/controls/cis-controls-navigator/

18 Critical Controls continued

- 10. Malware Defenses
- 11. Data Recovery
- 12. Network Infrastructure Management
- 13. Network Monitoring and Defense
- 14. Security Awareness and Skills Training
- 15. Service Provider Management
- 16. Application Software Security
- 17. Incident Response Management
- 18. Penetration Testing

Source: https://www.cisecurity.org/controls/cis-controls-navigator/

Secure Configuration of Enterprise Assets and Software

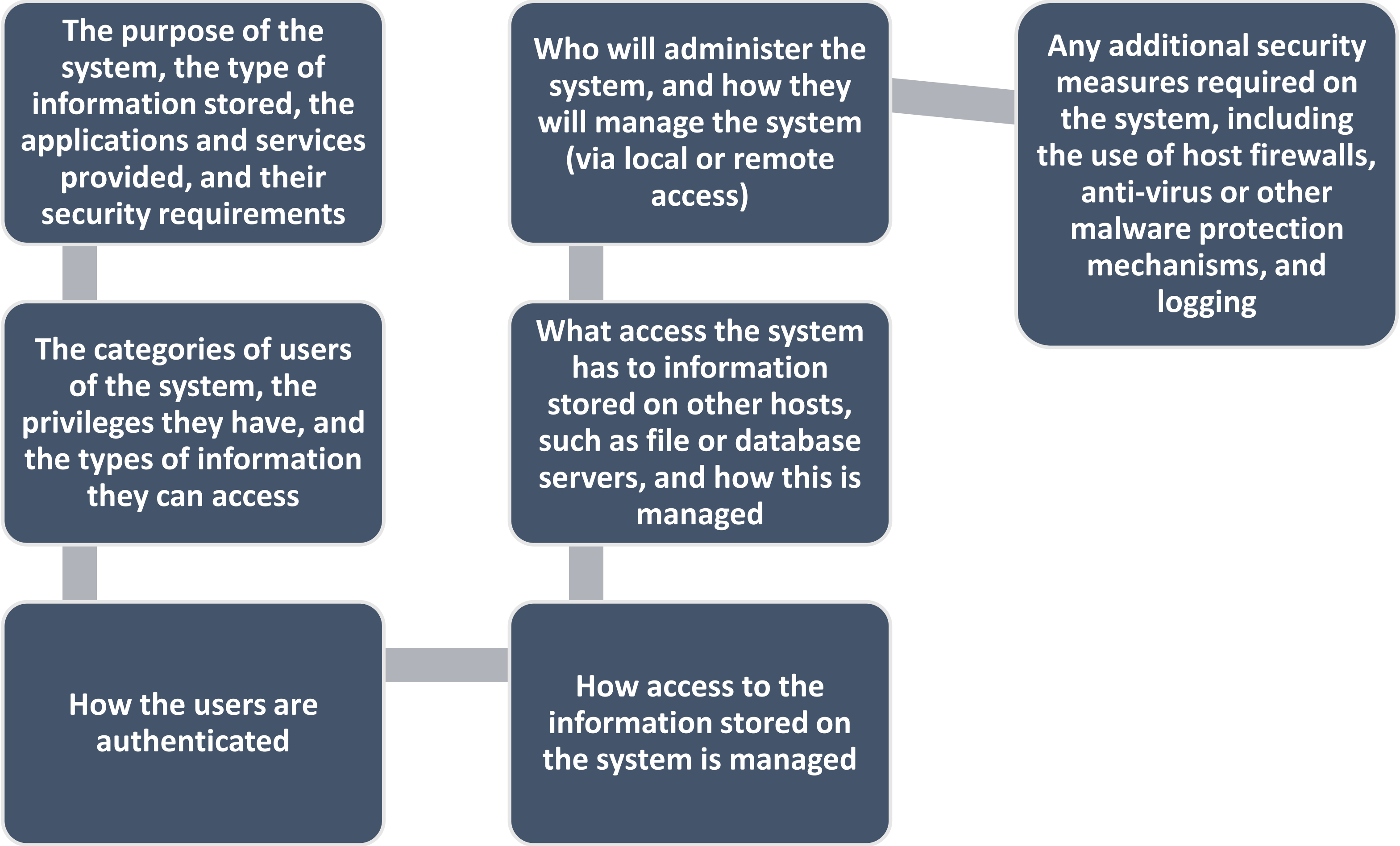
Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.
Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.
Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Operating System Hardening

Operating System Security

- Building and deploying a system should be a planned process designed to counter a compromise before installation
- Process must:
  - Assess risks and plan the system deployment
  - Secure the underlying operating system and then the key applications
  - Ensure any critical content is secured
  - Ensure appropriate network protection mechanisms are used
  - Ensure appropriate processes are used to maintain security

System Security Planning Process
NIST SP 800-123



The purpose of the system, the type of information stored, the applications and services provided, and their security requirements

The categories of users of the system, the privileges they have, and the types of information they can access

How the users are authenticated

How access to the information stored on the system is managed

What access the system has to information stored on other hosts, such as file or database servers, and how this is managed

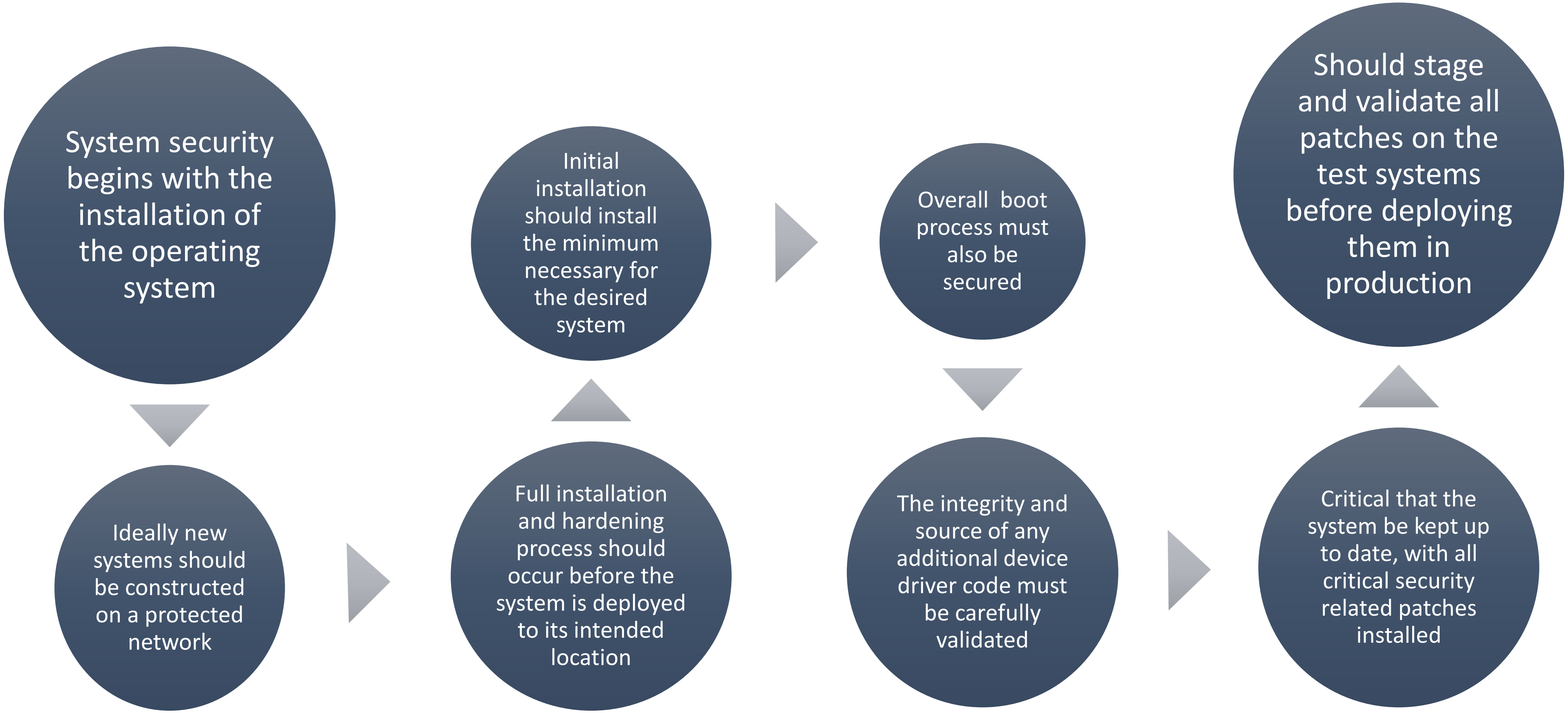
Who will administer the system, and how they will manage the system (via local or remote access)

Any additional security measures required on the system, including the use of host firewalls, anti-virus or other malware protection mechanisms, and logging

Operating Systems Hardening

- First critical step in securing a system is to secure the base operating system:
    - Install and patch the operating system
    - Harden and configure the operating system to adequately address the indentified security needs of the system by:
        - Removing unnecessary services, applications, and protocols
        - Configuring users, groups, and permissions
        - Configuring resource controls
    - Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)
    - Test the security of the basic operating system to ensure that the steps taken adequately address its security needs

Initial Setup and Patching



System security begins with the installation of the operating system

Ideally new systems should be constructed on a protected network

Full installation and hardening process should occur before the system is deployed to its intended location

Initial installation should install the minimum necessary for the desired system

Overall boot process must also be secured

The integrity and source of any additional device driver code must be carefully validated

Critical that the system be kept up to date, with all critical security related patches installed

Should stage and validate all patches on the test systems before deploying them in production

Remove Unnecessary Services, Applications, Protocols

- If fewer software packages are available to run the risk is reduced
- System planning process should identify what is actually required for a given system

- When performing the initial installation the supplied defaults should not be used
  - Default configuration is set to maximize ease of use and functionality rather than security
  - If additional packages are needed later they can be installed when they are required

Configure Users, Groups, and Authentication

- Not all users with access to a system will have the same access to all data and resources on that system
- Elevated privileges should be restricted to only those users that require them, and then only when they are needed to perform a task

- System planning process should consider:
  - Categories of users on the system
  - Privileges they have
  - Types of information they can access
  - How and where they are defined and authenticated
- Default accounts included as part of the system installation should be secured
  - Those that are not required should be either removed or disabled
  - Policies that apply to authentication credentials configured
  - https://ubuntu.com/server/docs/security-users

Configure Resource Controls

- Once the users and groups are defined, appropriate permissions can be set on data and resources
- Many of the security hardening guides provide lists of recommended changes to the default access configuration

Install Additional Security Controls

- Further security possible by installing and configuring additional security tools:
  - Anti-virus software
  - Host-based firewalls
  - IDS or IPS software
  - Application white-listing

Test the System Security

- Final step in the process of initially securing the base operating system is security testing
- Goal:
  - Ensure the previous security configuration steps are correctly implemented
  - Identify any possible vulnerabilities

- Checklists are included in security hardening guides
- There are programs specifically designed to:
  - Review a system to ensure that a system meets the basic security requirements
  - Scan for known vulnerabilities and poor configuration practices
- Should be done following the initial hardening of the system
- Repeated periodically as part of the security maintenance process

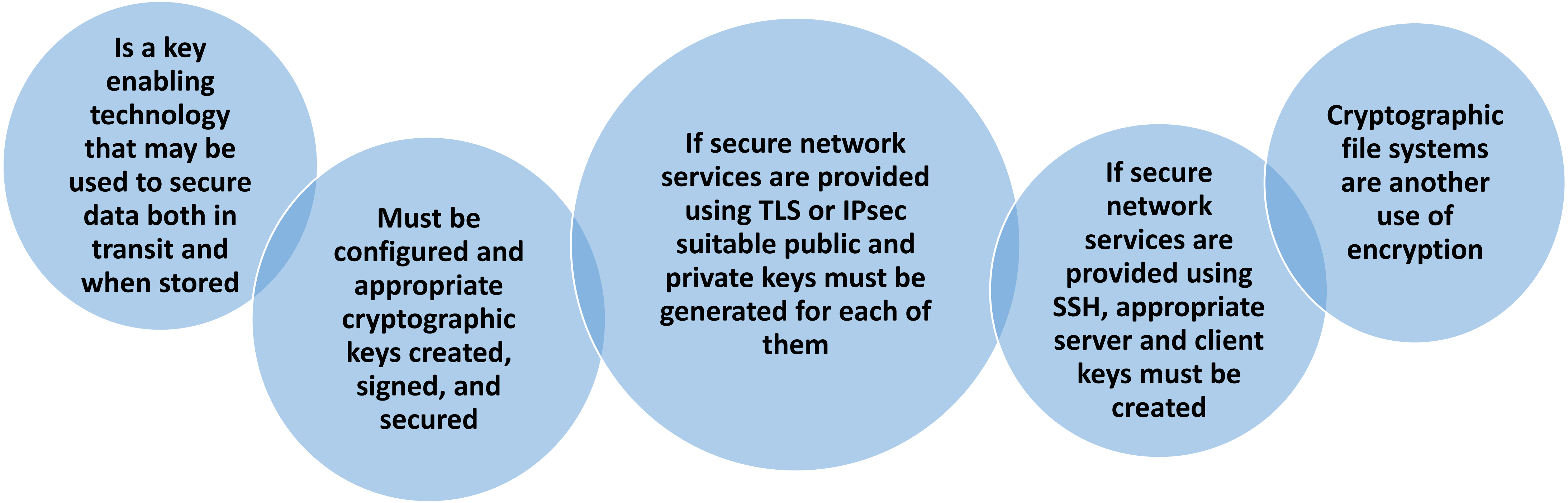
Example Policy Checklist

- https://security.utexas.edu/os-hardening-checklist/linux-7

Example Detailed Hardening Checklists

- Windows and Linux Examples in Canvas Learning Resources.

Configure Encryption



Is a key enabling technology that may be used to secure data both in transit and when stored

Must be configured and appropriate cryptographic keys created, signed, and secured

If secure network services are provided using TLS or IPsec suitable public and private keys must be generated for each of them

If secure network services are provided using SSH, appropriate server and client keys must be created

Cryptographic file systems are another use of encryption

Application/Encryption Security Policy Example

- https://security.ucop.edu/files/documents/policies/secure-software-configuration-standard.pdf

Security Maintenance

- Security maintenance is continuous and includes:
  - Monitoring and analyzing logging information
  - Performing regular backups 3-2-1
    - Create 3 backups on at least 2 different types of storage media, of which 1 copy is kept off-site
  - Recovering from security compromises
  - Regularly testing system security
  - Using appropriate software maintenance processes **to patch and update all critical software**, and to monitor and revise configuration as needed

Logging

Can only inform you about bad things that have already happened

In the event of a system breach or failure, system administrators can more quickly identify what happened

Key is to ensure you capture the correct data and then appropriately monitor and analyze this data

Information can be generated by the system, network and applications

Range of data acquired should be determined during the system planning stage

Generates significant volumes of information and it is important that sufficient space is allocated for them

Automated analysis is preferred

Data Backup and Archive

- Performing regular backups of data is a critical control that assists with maintaining the integrity of the system and user data
  - May be legal or operational requirements for the retention of data
- Backup
  - The process of making copies of data at regular intervals
- Archive
  - The process of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data
- Needs and policy relating to backup and archive should be determined during the system planning stage
  - Kept online or offline
  - Stored locally or transported to a remote site
    - Trade-offs include ease of implementation and cost versus greater security and robustness against different threats

File Integrity Management

- OSSEC - https://www.ossec.net/
- Tripwire article in Canvas
  - Limit noise by:
  - Identifying key files to track
  - Identifying who made changes – to know if the are authorized

“Poor Man’s” File Integrity Lab

Application Hardening

Application Configuration

- May include:
  - Creating and specifying appropriate data storage areas for application
  - Making appropriate changes to the application or service default configuration details
- Some applications or services may include:
  - Default data
  - Scripts
  - **User accounts**
- Of particular concern with remotely accessed services such as Web and file transfer services
  - Risk from this form of attack is reduced by ensuring that most of the files can only be read, but not written, by the server
- https://httpd.apache.org/security/vulnerabilities_24.html

Example for a Specific Application

- https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/index.html

Prep for Exercise

- https://portal.nice-challenge.com/

Windows Security

Windows Security

- Patch management
  - “Windows Update” and “Windows Server Update Service” assist with regular maintenance and should be used
  - Third party applications also provide automatic update support

- User administration and access controls
  - Systems implement discretionary access controls resources
  - Mandatory integrity controls are available
    - Objects are labeled as being of low, medium, high, or system integrity level
    - System ensures the subject’s integrity is equal or higher than the object’s level

Windows Security

Application and service configuration

- Much of the configuration information is centralized in the Registry
  - Forms a database of keys and values that may be queried and interpreted by applications
- Registry keys can be directly modified using the “Registry Editor”
  - Can be dangerous if mistakes are made
  - More useful for making bulk changes

Windows Security

Other security controls

- Essential that anti-virus, anti-spyware, personal firewall, and other malware and attack detection and handling software packages are installed and configured
- Current generation Windows systems include basic firewall and malware countermeasure capabilities

Windows systems also support a range of cryptographic functions:

- Encrypting files and directories using the Encrypting File System (EFS)
- Full-disk encryption with AES using BitLocker

“Microsoft Baseline Security Analyzer”

- Free, easy to use tool that checks for compliance with Microsoft’s security recommendations

Evaluating Windows Policies

- Open Windows browser and search for Microsoft Security Compliance Toolkit
- Download PolicyAnalyzer.zip and Windows 11 Security Baseline.zip

Linux Security

Patch Management

- Keeping security patches up to date is a widely recognized and critical control for maintaining security
- Subscribe to service to be notified of patches
- Use a tool like [Landscape]() to identify machines needing the patch and distribute it
- Attempt to patch with minimal downtime
  - Update parts of a cluster at a time

Application and Service Configuration

- Most commonly implemented using separate text files for each application and service
- Generally located either in the /etc directory or in the installation tree for a specific application
- Individual user configurations that can override the system defaults are located in hidden "dot" files in each user's home directory
- Most important changes needed to improve system security are to disable services and applications that are not required

Linux Config Files

- On NCR:
- cd to etc directory
- ls –a to see config and . files

Users, Groups, and Permissions

- Access is specified as granting read, write, and execute permissions to each of owner, group, and others for each resource
- Guides recommend changing the access permissions for critical directories and files
- Local exploit
  - Software vulnerability that can be exploited by an attacker to gain elevated privileges
- Remote exploit
  - Software vulnerability in a network server that could be triggered by a remote attacker

Other Linux Hardening

- Remote access controls
  - Several host firewall programs may be used
  - Most systems provide an administrative utility to select which services will be permitted to access the system
- Logging and log rotation
  - Should not assume that the default setting is necessarily appropriate

chroot Jail

- chroot jail
  - Restricts the server's view of the file system to just a specified portion
  - Uses chroot system call to confine a process by mapping the root of the filesystem to some other directory
  - File directories outside the chroot jail aren't visible or reachable
  - Main disadvantage is added complexity and difficult troubleshooting
- Example exercise
  - https://www.geeksforgeeks.org/linux-virtualization-using-chroot-jail/
  - Can be broken: If program or user has root privileges, they can do another chroot

Windows and Linux Config Exercise

NICE Challenge – Calamitous Configurations

- Windows – eliminate unnecessary services
- Linux - Restrict root login

Group Policy Configurations

https://portal.nice-challenge.com/

Virtualization Security

Virtualized Systems

- In virtualized systems, the available hardware resources must be appropriately shared among the various guest OS’s
- These include CPU, memory, disk, network, and other attached devices
- CPU and memory are generally partitioned between these, and scheduled as required
- Disk storage may be partitioned, with each guest having exclusive use of some disk resources
- Alternatively, a “virtual disk” may be created for each guest, which appears to it as a physical disk with a full file-system, but is viewed externally as a single ”disk image” file on the underlying file-system
- Attached devices such as optical disks, or USB devices are generally allocated to a single guest OS at a time

Hypervisor

- Software that sits between the hardware and the VMs
- Acts as a resource broker
- It allows multiple VMs to safely coexist on a single physical server host and share that host's resources
- Virtualizing software provides abstraction of all physical resources and thus enables multiple computing stacks, called virtual machines, to be run on a single physical host
- Each VM includes an OS, called the guest OS
  - This OS may be the same as the host OS, if present, or a different one

Hypervisor Functions

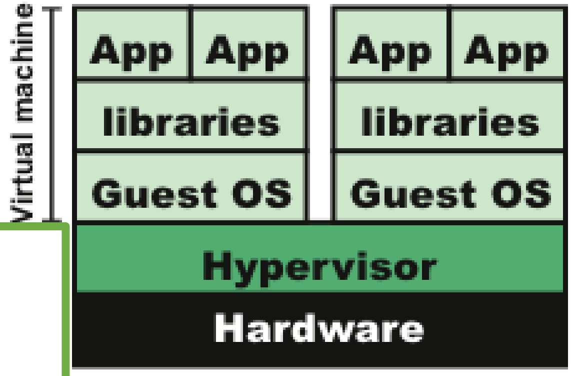
The principal functions performed by a hypervisor are:

- Execution management of VMs
- Devices emulation and access control
- Execution of privileged operations by hypervisor for guest VMs
- Management of VMs (also called VM lifecycle management)
- Administration of hypervisor platform and hypervisor software

Containers

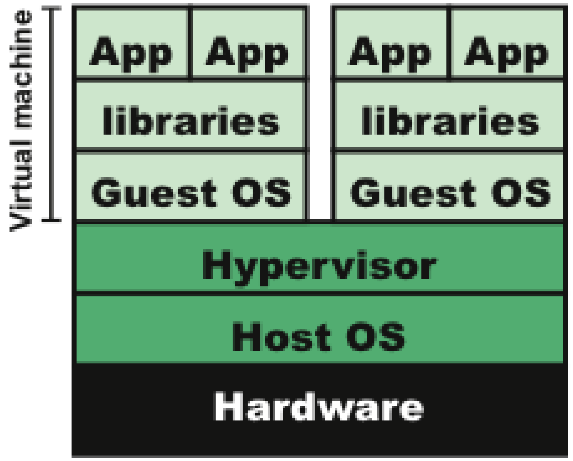
- In this approach, software known as a virtualization container, runs on top of the host OS kernel and provides an isolated execution environment for applications
- Unlike hypervisor-based VMs, containers do not aim to emulate physical servers
- All containerized applications on a host share a common OS kernel
- For containers, only a small container engine is required as support for the containers
- Containerization sits in between the OS and applications and incurs lower overhead, but potentially introduces greater security vulnerabilities

Comparison of Virtual Machine Containers



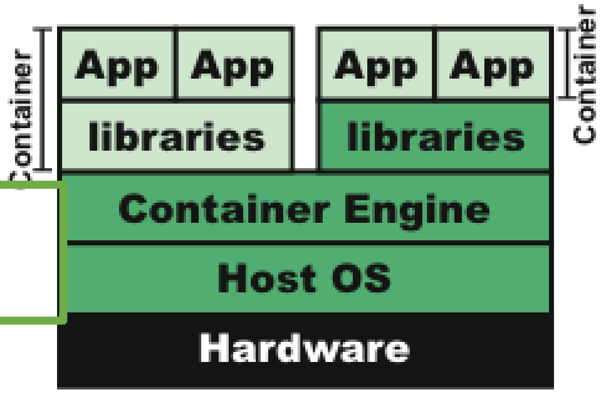
(a) Type 1 hypervisor
(native virtualization)

Proxmox
KVM
Hyper-V
Vmware Esxi



(b) Type 2 hypervisor
(hosted virtualization)

KVM
VirtualBox
Vmware Desktop



(c) Container (application virtualization)

Docker
Kubernetes

Virtualization Security Issues

- Security concerns include:
  - Guest OS isolation
    - Ensuring that programs executing within a guest OS may only access and use the resources allocated to it
  - Guest OS monitoring by the hypervisor
    - Which has privileged access to the programs and data in each guest OS
  - Virtualized environment security
    - image and snapshot management which attackers may attempt to view or modify
    - Shared folders and clipboards

Securing Virtualization Systems

Organizations using virtualization should:

- Carefully plan the security of the virtualized system
- Secure all elements of a full virtualization solution and maintain their security
- Ensure that the hypervisor is properly secured
- Restrict and protect administrator access to the virtualization solution

Hypervisor Security

- Should be
  - Secured using a process similar to securing an operating system
  - Installed in an isolated environment
  - Configured so that it is updated automatically
  - Monitored for any signs of compromise
  - Accessed only by authorized administration
- Ideally administration traffic should use a separate network with very limited access provided from outside the organization https://www.virtualbox.org/manual/ch13.html

Module 7 Assignment

- Modify the spreadsheet template to reflect ONLY the things in the scenario
- Your model will have fewer things in each category, but a good analysis of each
- List any assets that you think might be related to the vulnerability
- On threat sheet, estimate potential damage and probability
  - In mitigations, list what should be done to prevent or recover from attack
  - In issues give brief description of specific issues that could arise