Lesson 3.

OS Security

Bảo mật HĐH

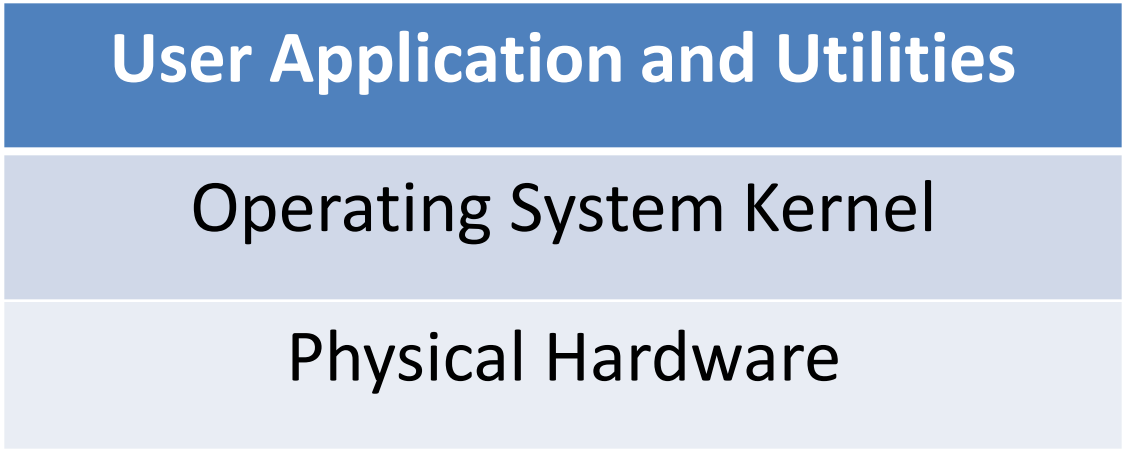
Contents

- Introduction
- OS Security security layers
- OS Security planning
- OS Security hardening
- Security maintenance
- Practice - Nmap
- Summary

Introduction

- *An operating system is a set of programs designed to run other programs on a computer.*
- Security of an OS depends upon how the system is being used by the administrator and how well it is maintained.
- Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.
- OS security encompasses many different techniques and methods which **ensure safety from threats and attacks**.

Operating system security layers



Each layer needs measures in place to provide appropriate security services

OS security issues

Among the issues to be considered these are the important ones:

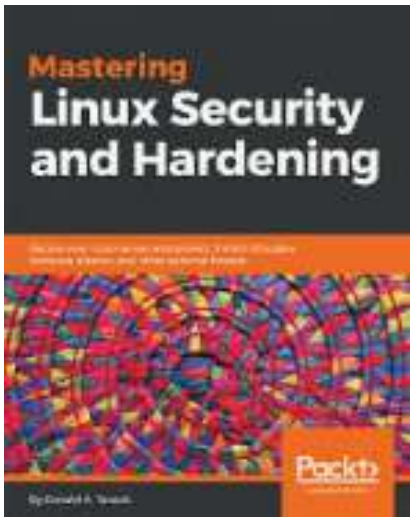
- Physical security
- Authentication
- Software Vulnerabilities
- Malwares

Security planning

1. The purpose of the system, the type of information stored, the applications and services provided, and their security requirements
2. The categories of users of the system, the privileges they have, and the type of information they can access
3. **How** the users are authenticated
4. **How** access to the information stored on the system is managed
5. What access the system has to information stored on other hosts, such as file or database servers, and how it is managed
6. **Who** will administer the system, and **how** they will manage the system (via local or remote access)
7. Any additional security measures required on the system: host firewall, anti-virus,..

Operating Systems Hardening

- Installing and patching
- Configuring
  - Remove unnecessary applications, services and protocols
  - Users, groups, controls and privileges
- Install additional software (anti-virus, firewall, intrusion detection system, etc.)
- Test the system security
  - Ensure previous security configuration steps are correctly implemented
  - Identify any possible vulnerabilities



Installing and patching

- **Installation**
  - Machines should not connect to network until secured
  - Limited network (firewall) is acceptable
  - Install only required services and drives (from trusted sources)
  - Set up automatic updates (only if update time is not issue)
- **Booting**
  - Protect BIOS changes with password
  - Disable some bootable media
  - Cryptographic hardware drives? Pros and Cons

Remove unnecessary services, applications, protocols

- Software have vulnerabilities,
  hence **more software** = **more vulnerabilities**
- **Better to not install it at all**
  - Uninstallers sometimes fail to clean all dependency
  - Disable software may be enabled by an attacker upon control acquisition

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

- **Define user types and privileges**
  - Admin (ideally only temporary)
  - Normal
  - Limited
- **Authentication**
  - Force default password change
  - Password definition
  - Password lifespan

- Remove or disable old accounts
- Allow for remote connections?

Authentication

Authentication:

- Verifies user identity
- Permits access to the operating system

- **Physical authentication**
  - Allows physical entrance to company property
  - Magnetic cards and biometric measures
- Digital authentication: verifies user identity by digital means

User administration

- Create user accounts
- Set password policies
- Grant privileges to users
- Best practices:
  - Use a consistent naming convention
  - Always provide a password to an account and force the user to change it at the first logon
  - Protect passwords
  - Do not used default passwords

Configure resource controls

- Once the users and groups are defined, appropriate permissions can be **set** on data and resources

Authorization

- Process that decides whether users are permitted to perform the functions they request
- Authorization is not performed until the user is authenticated
- Deals with privileges and rights

Additional security and Testing

- Anti-virus software
- Host-based Firewalls, IDS/IPS
- Application white-listing

Test the system security

- Run some test cases which attempt to break security
- Ensure previous security configuration steps are correctly implemented
- Identify any possible vulnerabilities

Application Security

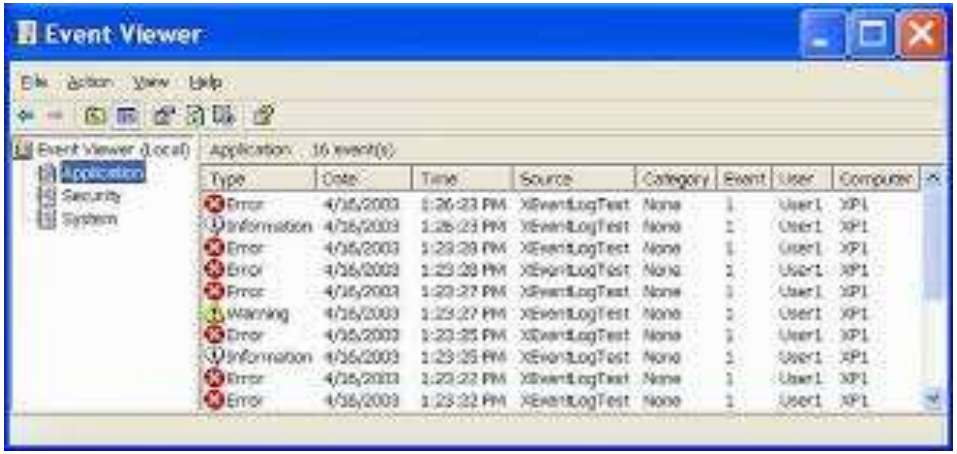
- Configure applications properly
- Use **encryption** when possible as seen earlier
  - For storing
  - For transmit
- **Limit privileges** as with users
- Applications may provide backdoors if not configure properly

Security Maintenance

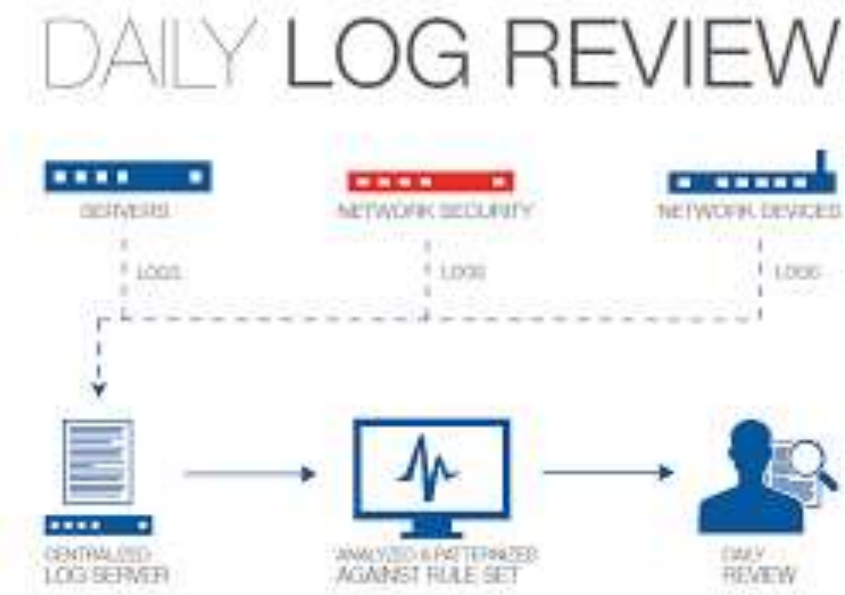
- Process of maintaining security is continuous
- This involves:
  - Monitoring and analyzing logging information
  - Performing regular **backups**
  - **Recovering** from security compromises
  - Regular testing for security
  - Patch, update, and revise critical software

Logging

- **Keep** a record of important events in the computer



- *Problems*
  - Need to make sure to have enough space
  - Manual analysis is hard, so these logs should contain a format such that a program can parse messages

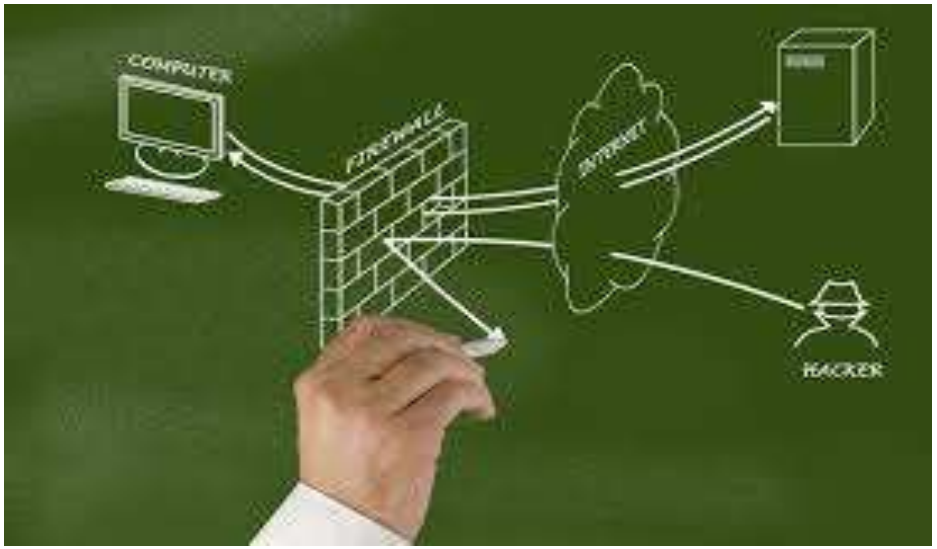


Data backup

- Backup us the act of creating copies of information such that it may be recovered
- Archive is to keep these backups for a long period of time in order to meet some legal aspects

- Should the backup be kept online or offline?
  - ✓ Online makes easier access, faster recover
  - ✓ Offline is more secure, harder to recover
  - ✓ Why not both?. Users should keep their own offline backups, in case online backup gets removed
- Data may be lost accidentally (hardware failures, human mistake) or intentionally

Network protection



- The connectivity of operating systems to the Internet also signaled the start of a rapid increase in reported vulnerabilities.

- Many OSes have built firewalls into their operating systems to reduce the ability of attackers to access network services and applications that they should not.

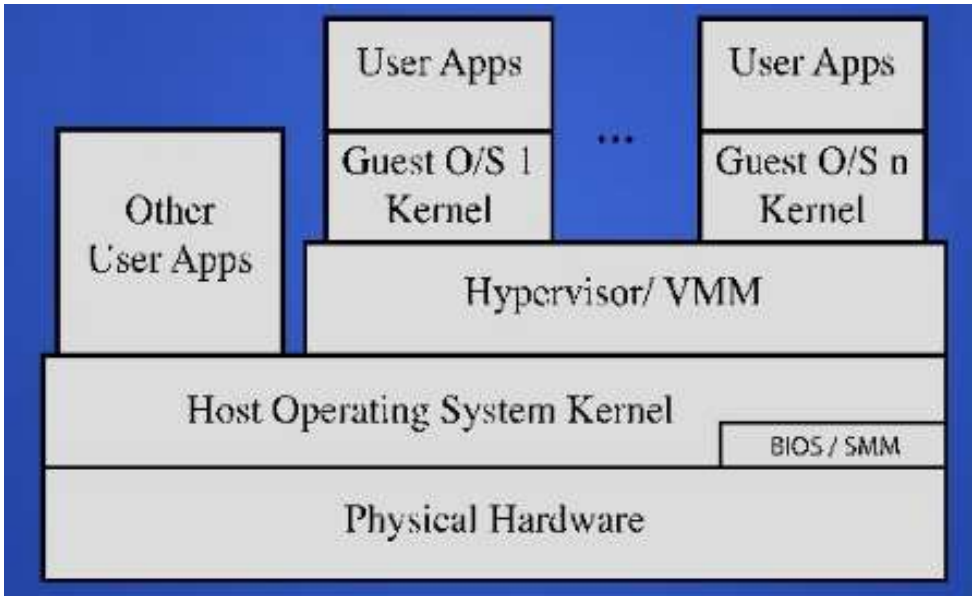
Malware protection

- **Malware** has become an increasing issue for operating systems to deal with as users need and want to access and exchange files and applications through a variety of means, such as web portal, messaging/chat systems and social media.

- Application verification and control.
- Application separation - sandboxing

Virtualization security layers

- Carefully plan the security of the virtualized system
- Guest OS isolation
- Virtualized environment security



OS must protect users from each other

- Memory protection
- File protection
- General control and access to objects
- User authentication

The components of an OS security environment

- Three components
  - Services
  - Files
  - Memory

Services

- Main component of operating system security environment
- Used to gain access to the OS and its features
- Include
  - User authentication
  - Remote access
  - Administration tasks
  - Password policies

Files

- Common threats
  - File permission
  - File sharing
- Files must be protected from unauthorized reading and writing actions

File permissions

- Read, write, and execute privileges
- In Windows:
  - Change permission on the Security tab on a file's Properties dialog box
  - Allow indicates grant; Deny indicates revoke

Sharing Files

- Naturally leads to security risks and threats
- peer-to-peer programs: allow users to share files over the Internet
- Reason for blocking file sharing:
  - Malicious code
  - Adware and spyware
  - Privacy and confidentiality
  - Copyright issues

Memory

- Hardware memory available on the system can be corrupted by badly written software
- Can harm data integrity
- Two options:
  - Stop using the program
  - Apply a patch (service pack) to fix it

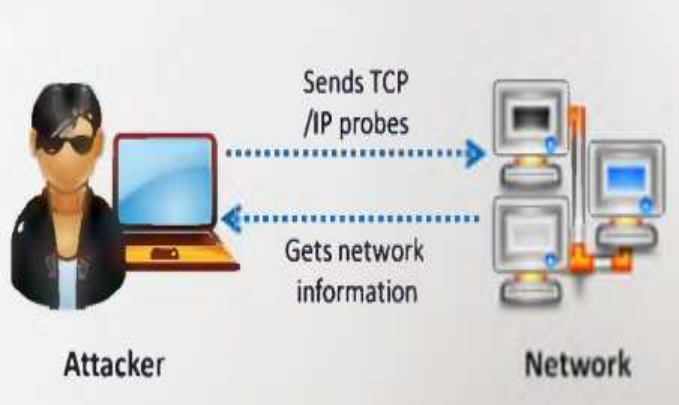
Summary

- Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.
- OS security encompasses many different techniques and methods which **ensure safety from threats and attacks**.
  - System security planning
  - Operating systems hardening
    - Initial setup and patching
    - Remove unnecessary services
    - Configure users and groups
    - Test system security
  - Application security
    - Application configuration
    - Encryption technology
    - Security maintenance
    - Data backup
  - Virtualization security

Scanning network - NMAP

- **Network Discovery and Security Scanning**
- Guide: https://nmap.org/book/toc.html

Network scanning



- Network scanning refers to a set of procedures for identifying hosts, ports, and services in a network.
- Network scanning is one of the components of intelligence gathering an attacker uses to create a profile of the target organization

(1) To discover live hosts, IP address, and open ports of live hosts

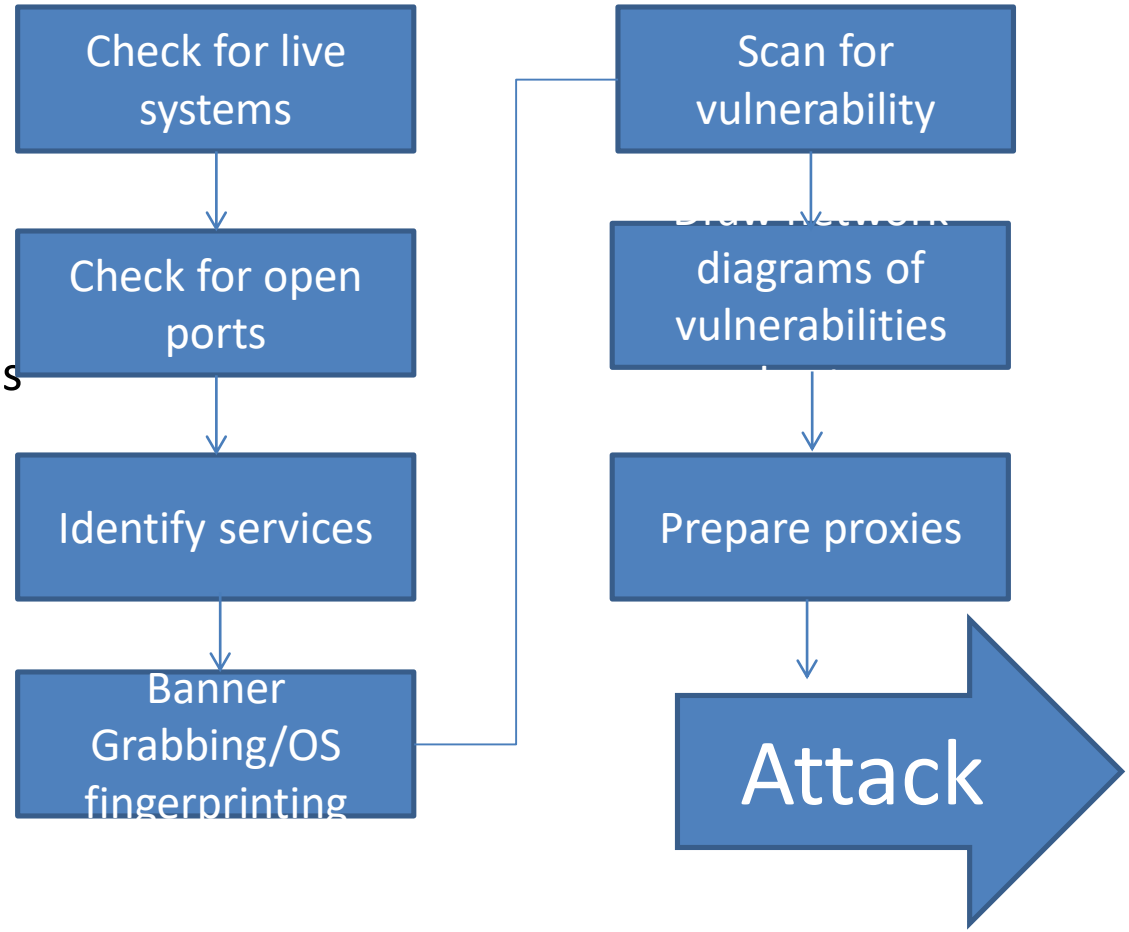
(2) To discover operating systems and system architecture

(3) To discover services running on hosts

(4) To discover vulnerabilities in live hosts

Scanning methodology

1) Check for live systems
2) Check for open ports
3) Scanning beyond IDS
4) Banner grabbing
5) Scanning for vulnerabilities
6) Draw network diagrams
7) Prepare proxies
8) Scanning Pen Testing



OS detection, Service discovery

- Sudo nmap –F <network>
- sudo nmap -O <IP-target>
- sudo nmap -sV <IP-target>
- sudo nmap <IP-target> -A

Nmap vulscan

- CVE stands for Common Vulnerabilities and Exposures
- git clone https://github.com/scipag/vulscan scipag_vulscan
- Sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
- nmap -sV --script=vulscan/vulscan.nse www.example.com

https://securitytrails.com/blog/nmap-vulnerability-scan

```
git clone https://github.com/scipag/vulscan scipag_vulscan
ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
```

```
nmap -sV --script=vulscan/vulscan.nse www.example.com
```

Q&A