Operating System Security

Day 3: OS Security, Encryption & Secure Access

Password Security: The Human Factor

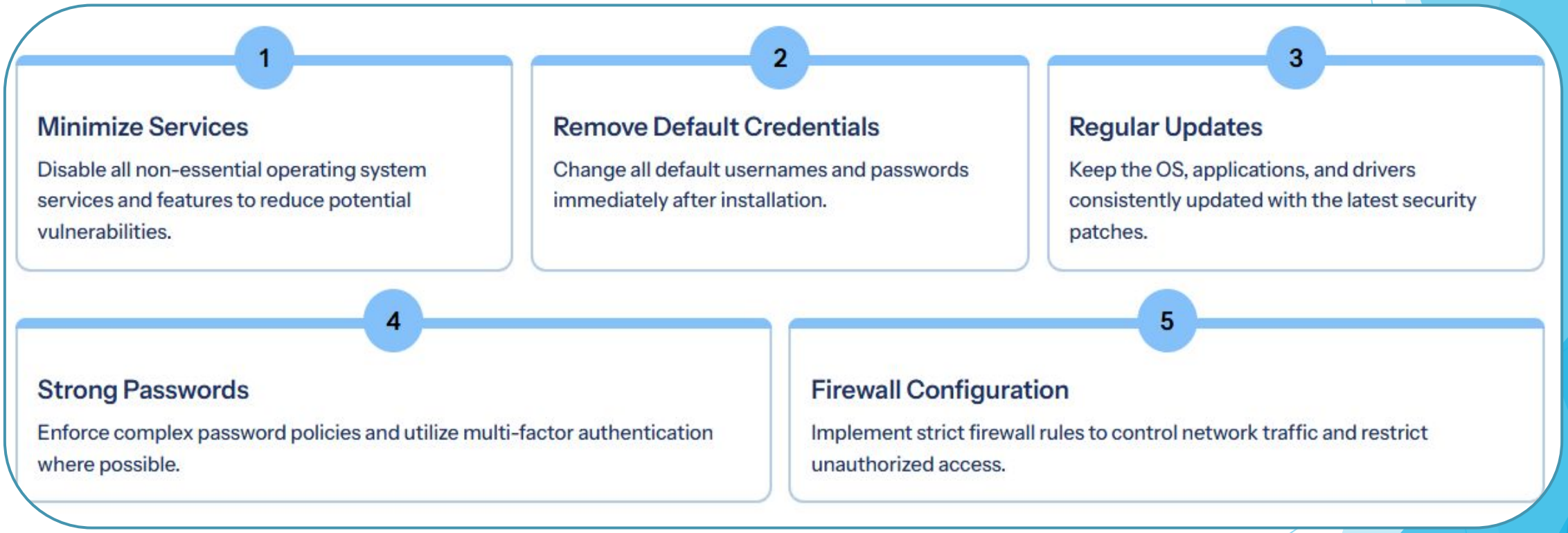
- **Weak Passwords:**
  - Short or predictable passwords (like "123456") are cracked in seconds using automated tools.
- **Common Attack Vectors:**
  - **Brute Force**: Testing every possible character combination.
  - **Credential Stuffing:** Using passwords stolen from other leaked databases.
- **Best Practices**: Use long, unique phrases and a Password Manager to eliminate reuse across different services.

OS Hardening: Fortifying the Foundation

- **Attack Surface Reduction:**
  - Disable or uninstall any software or services that aren't critical to the system's operation.
- **Account Hygiene:**
  - Remove dormant or "ghost" user accounts to prevent attackers from using them as a backdoor.
- **The Golden Rule:**
  - **Patching and Updates.** Regularly updating the OS is the single most effective way to close known security loopholes.

Essential OS Hardening Practices

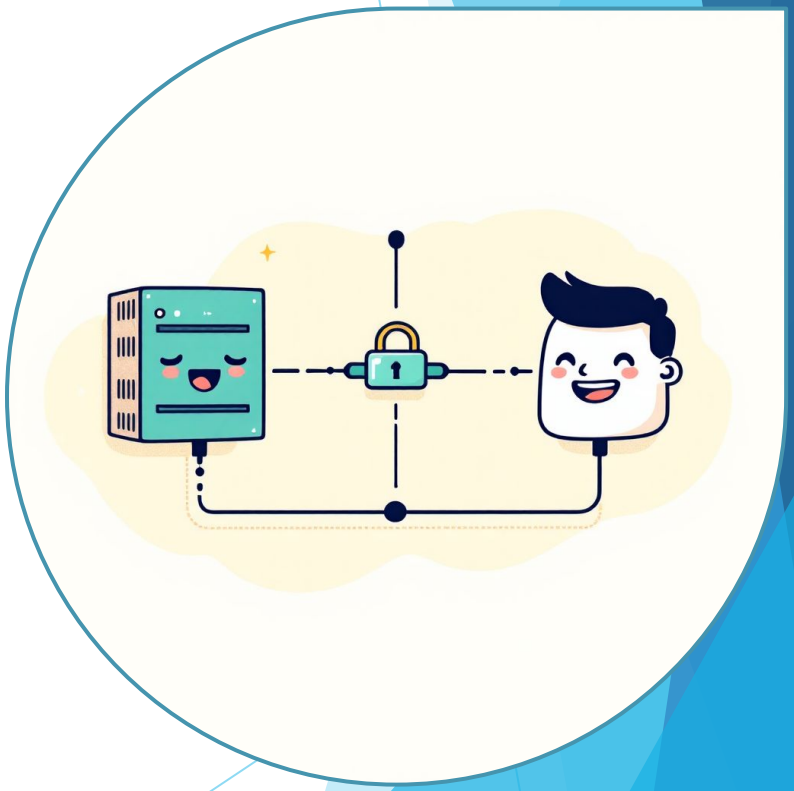
- A checklist of critical steps to ensure your operating system is configured with a robust security posture, reducing its attack surface and mitigating risks.



Secure Remote Access with OpenSSH (Secure Shell)

SSH: The Backbone of Secure Management

- SSH (Secure Shell) is the industry-standard protocol for managing servers, network devices, and cloud infrastructure over unsecured networks.
- It provides Confidentiality (encryption), Integrity (prevents data tampering), and Authentication (proves identity), effectively killing "Man-in-the-Middle" attacks.
- SSH operates on Port 22 by default. Changing this is a common "security by obscurity" tactic to reduce automated bot scans.



Authentication Methods

- **Password-Based:** The simplest method, but vulnerable to Brute Force and Credential Stuffing. Generally discouraged for high-security systems.
- **SSH Key-Based (Recommended):** Uses a Public Key (on the server) and a Private Key (on your laptop). It is nearly impossible to crack and eliminates the need for passwords.
- **Multi-Factor Authentication (MFA):** Many organizations now require an SSH key plus a one-time code (OTP) from an app like Google Authenticator.

Key Security Hardening

- **Disable Root Login:** Never allow the "Root" user to log in directly via SSH. Log in as a standard user and use sudo instead.
- **Disable Password Auth:** Once SSH keys (2048 bit) are set up, turn off password logins entirely to stop 100% of brute-force attacks.
- **Use a Passphrase:** Always protect your **Private Key** with a passphrase. If your laptop is stolen, the thief still can't use your key without it.
- **Monitor Logs:** Check /var/log/auth.log frequently to see who is attempting to "knock on the door" of your server.

Cryptography

- **The Art of Secrets:**
  - Cryptography is the science of secure communication when bad guys might be listening.
- **Not Just Encryption:**
  - It's about more than just hiding messages; it also proves identity and ensures data hasn't been changed.
- **Core Goals:**
  - Confidentiality: Keeping data secret.
  - Integrity: Ensuring data hasn't been tampered with.
  - Authentication: Proving who you are.

Symmetric Encryption (One Key for All)

Like a single house key that both locks and unlocks the front door. Everyone who needs to access the house has an identical copy.

- **How it Works:**
  - Sender uses a **Shared Secret Key** to encrypt the message.
  - Receiver uses the **EXACT SAME Shared Secret Key** to decrypt it.
- **Pros:** Very fast, efficient for large amounts of data.
- **Cons:** The biggest challenge is **how to securely share the key** with the other person without anyone else finding it.
- **Example Algorithms:** AES (Advanced Encryption Standard), DES.
- **Real-World Use:** Encrypting hard drives, securing VPN tunnels once keys are exchanged.

Asymmetric Encryption (Two Keys, One Pair)

The "Padlock and Key" system.

- **Public Key:** An open padlock you give to everyone. Anyone can lock a message for you.
- **Private Key:** The only key that can open that specific padlock. You keep it secret!
- **How it Works:**
  - Each person has a unique Public Key (shared) and a Private Key (secret).
  - To send a secret message to Ali, Khan uses Ali's Public Key to encrypt it.
  - Only Ali's Private Key can decrypt that message.
- **Pros:** Solves the key sharing problem, great for digital signatures (proving who sent something).
- **Cons:** Much slower than symmetric encryption.
- **Example Algorithms:** RSA, ECC (Elliptic Curve Cryptography).
- **Real-World Use:**
  - Securing your connection to websites (SSL/TLS Handshake), SSH key authentication.

Configuring & Testing Secure SSH

- Practical application is key to mastering secure remote access.

Generate Key Pairs

Students will generate their own SSH public and private key pairs on their local machines.

Deploy Public Key

The public key will be securely transferred to a designated Linux virtual machine.

Test Key-Based Login

Attempt to log in to the Linux VM using the newly generated key, verifying successful key-based authentication.

Monitor Failures

Learn to monitor and identify failed SSH login attempts, a crucial step in detecting potential attacks.

OpenSSH – Password vs Key-Based Authentication

- Commands / Hands-on:
  - ssh-keygen -t rsa -b 4096 # Generate key pair
  - ssh-copy-id user@server # Copy public key to server
  - ssh user@server # Login using key
- Configure a Secure SSH Server
  - Edit /etc/ssh/sshd_config:
    - PermitRootLogin no
    - PasswordAuthentication no
- Restart SSH service:
  - sudo systemctl restart ssh

Update Kali Linux & Upgrade System

- sudo apt update # Update package repository list
- sudo apt upgrade -y # Upgrade installed packages
- sudo apt full-upgrade -y # Upgrade including kernel and dependencies
- sudo apt autoremove -y # Remove unused packages

Installing Cybersecurity Packages

- sudo apt install nmap # Network scanning
- sudo apt install wireshark # Packet analysis
- sudo apt install john # Password cracking
- sudo apt install metasploit-framework # Exploitation framework
- sudo apt install hydra # Brute force tool

Hands-On Lab Activity

- Update and upgrade Kali Linux
- Install at least 3 cybersecurity tools
- Verify installation using:
  - which nmap
  - nmap --version

Disk Encryption Fundamentals

- **Encryption at Rest:**
  - Protects data when the computer is turned off or the drive is removed.
- **The Master Key:**
  - The OS uses a complex "Master Key" to encrypt every bit of data on the disk.
- **The User Passphrase:**
  - You don't use the Master Key directly. Instead, you use a passphrase to "unlock" the Master Key, which then decrypts the data on the fly.
- **Transparent Operation:**
  - Once the disk is unlocked at boot, the encryption happens in the background. The user and applications see files normally.

Why Encrypt Disks?

- **Physical Theft:**
  - If a laptop is stolen, a thief can pull out the hard drive and read the files on another computer. Encryption makes the data unreadable "garbage" without the key.
- **Data Privacy:**
  - Ensures that sensitive information (passwords, private photos, medical records) remains private even if the hardware falls into the wrong hands.
- **Regulatory Compliance:**
  - Many laws (like HIPAA or GDPR) require businesses to encrypt disks to protect client data.
- **Decommissioning Drives:**
  - When you throw away or sell an old SSD, encryption ensures that even if you didn't "wipe" it perfectly, the data is unrecoverable.

Linux Encryption with LUKS

- **What is LUKS?**
  - Stands for **Linux Unified Key Setup**. It is the standard specification for Linux hard disk encryption.
- **The LUKS Header:**
  - A small area at the start of the drive that stores the encryption metadata and "Key Slots."
- **Multiple Key Slots:**
  - LUKS allows up to 8 (or 32 in LUKS2) different passphrases or key files to unlock the same drive. Useful for teams or emergency backups.
- **dm-crypt:**
  - The actual engine in the Linux Kernel that performs the encryption; LUKS is the "manager" that handles the keys.
- **The Boot Process:**
  - When a Linux system starts, it pauses and asks for the LUKS passphrase before it can even load the operating system files.

BitLocker: Windows Disk Encryption

- **Proprietary Encryption:** A full-disk encryption feature included with professional and enterprise versions of Windows.
- **AES Encryption:** Uses the **Advanced Encryption Standard (AES)** algorithm (usually 128-bit or 256-bit) to ensure data is unreadable to unauthorized users.
- **Ease of Use:** Integrated directly into Windows Explorer; once enabled, it operates seamlessly as you save and open files.
- **Recovery Key:** Generates a 48-digit numerical password that acts as a "safety net" if you forget your password or the hardware changes.

The Role of the TPM (Hardware Security)

- **What is a TPM?** The Trusted Platform Module is a dedicated microchip on the motherboard used to store encryption keys securely.
- **Boot Integrity:** The TPM checks if the computer's hardware or boot files have been tampered with before releasing the Master Key.
- **Hands-Free Unlocking:** With a TPM, your computer can automatically unlock the drive as soon as it confirms the hardware is safe, allowing you to go straight to the login screen.
- **Anti-Hammering**: TPM chips have built-in protection against "Brute Force" attacks by slowing down or locking out attempts after too many wrong guesses.

BitLocker Authentication Modes

- **TPM-Only:** Automatically unlocks the drive when it detects the correct, untampered hardware. No user action is needed until the Windows login.
- **TPM + PIN:** Requires the user to enter a secret PIN before the computer even starts loading Windows. This is the most secure method.
- **TPM + Startup Key:** Requires a physical USB flash drive containing a key file to be plugged in to "turn the ignition" and start the OS.
- **Password Mode:** Used on older computers without a TPM chip or for removable USB "BitLocker To Go" drives.

BitLocker vs. LUKS: A Comparison

Feature	BitLocker (Windows)	LUKS (Linux)
Philosophy	"Ease of Use" & Hardware Integration	"Full Control" & Customization
Primary Storage	Uses TPM Chip on motherboard	Uses Header on the disk partition
Format	NTFS (Proprietary)	Ext4, Btrfs, etc. (Open Source)
Recovery	48-digit Recovery Key	Backup of the "Header" file
Multi-User	Managed via Active Directory/Accounts	Up to 32 independent Key Slots

Hands-On Lab: Encrypting a Disk

This practical lab consolidates theoretical knowledge into tangible skills, allowing students to directly apply disk encryption techniques on virtual machines.

Encrypt Linux Partition

Utilize LUKS and `cryptsetup` to encrypt a designated partition on a Linux virtual machine, experiencing the process firsthand.

Test Encrypted Access

Attempt to access the encrypted drives to confirm proper functionality and security protocols.

Enable BitLocker on Windows

Activate BitLocker on a Windows virtual machine's drive, following recommended security practices.

Explore Recovery Keys

Locate and understand the role of recovery keys, discussing their security implications and storage best practices.

Optional Challenge: Data in Jeopardy

- This challenge provides a powerful demonstration of the importance of disk encryption by simulating a real-world data breach scenario.

- **Simulate Data Theft:** What happens if an encrypted disk is physically removed from the machine without proper decryption?
- **Observation:** Students will attempt to access the data on the "stolen" encrypted disk using another system.
- **Outcome:** Witness firsthand the inability to retrieve information from the encrypted drive, even with direct access to the hardware.