Here is a sentence-by-sentence study note breakdown of the document **“128. Configuration Files Notes.docx”**, restructured into **detailed bullet points** to maximize clarity and exam readiness. This aligns with **CompTIA A+ 220-1102 Objective 1.8**, which includes **basic Linux file and command knowledge**.

**🧠 Study Notes – Common Linux Configuration Files**

**🗂️ What Are Configuration Files?**

* Linux systems rely on **configuration files** to manage **functionality** and **smooth operation**.
* These files control:
  + User settings
  + Device interactions with the OS
  + System services and security
* Understanding these files is **crucial for system management and troubleshooting**.

**📚 The 5 Most Common Linux Configuration Files:**

| **File** | **Purpose** |
| --- | --- |
| /etc/passwd | Stores user account information |
| /etc/shadow | Stores encrypted user password data |
| /etc/hosts | Maps IP addresses to hostnames |
| /etc/fstab | Defines how file systems are mounted |
| /etc/resolv.conf | Configures DNS name resolution |

**1️⃣ /etc/passwd – User Account Info**

* Pronounced **“pass-wd”**, not “password”
* **Stores basic user account information**.
* Each line represents a user and includes:
  + username
  + UID (user ID)
  + GID (group ID)
  + home directory
  + Placeholder for password (not actual password)
* **Does NOT store passwords directly anymore** (for security reasons).
* Used by the system during **user authentication**:
  + Helps verify valid users trying to log in.

**2️⃣ /etc/shadow – Encrypted Passwords**

* Holds **actual password data** in encrypted format.
* Contains:
  + Encrypted password
  + Last password change date
  + Password expiration policies
* Every line corresponds to a user in /etc/passwd.
* This file is:
  + **Highly sensitive**
  + **Only accessible by the root user or administrator**
* Essential for maintaining **strong system security**.
* Admins must **manage this file carefully** to protect user credentials.

**3️⃣ /etc/hosts – Hostname to IP Mapping**

* Used to **locally resolve hostnames to IP addresses**.
* Historical use: Was the main method **before DNS existed**.
* Each line includes:
  + An IP address
  + One or more hostnames linked to that IP
* Often used for:
  + **Testing and troubleshooting**
  + Bypassing or overriding DNS
* Example use case:
  + Redirecting a hostname to a specific IP during testing
  + Accessing internal servers without DNS

**4️⃣ /etc/fstab – File System Mounting**

* Full name: **File System Table** (spelled "F-S-T-A-B")
* Controls **how storage devices and partitions are mounted**.
* Each entry in this file includes: Device, location, Mount Point, File System Type, Permissions.
  + Device ID or UUID
  + Mount point (where in the directory tree)
  + File system type (e.g., ext4, ntfs)
  + Mount options (e.g., read-only, read-write)
* Read during the **boot process**:
  + Ensures file systems auto-mount at startup
* To add new drives or modify mount options:
  + You **edit /etc/fstab**

**5️⃣ /etc/resolv.conf – DNS Settings**

* Spelled: R-E-S-O-L-V dot C-O-N-F
* Manages **DNS (Domain Name System) settings** on the Linux system.
* Tells the system which **DNS servers to use** to resolve hostnames to IP addresses.
* Each line starts with:
  + nameserver followed by the DNS server IP
* Incorrect settings here can cause:
  + Websites to **not load**
  + Loss of access to **network resources**
* Critical for **network connectivity and performance**

**🔁 Recap: Purpose of Each File**

| **File** | **Role** |
| --- | --- |
| /etc/passwd | Supports user authentication |
| /etc/shadow | Stores encrypted passwords securely |
| /etc/hosts | Maps hostnames locally to IPs |
| /etc/fstab | Mounts storage devices automatically |
| /etc/resolv.conf | Manages DNS servers for name resolution |

**🛠️ Why These Matter to You (as a tech/admin)**

* These files are used in:
  + **User management**
  + **Security hardening**
  + **Networking**
  + **Storage configuration**
* You should:
  + Know their locations
  + Understand their format and purpose
  + Be able to **read, interpret, and safely edit** them as part of troubleshooting

**🎯 CompTIA A+ 220-1102 Relevance (Objective 1.8)**

You’re expected to:

* Recognize and describe **Linux system files** like /etc/passwd, /etc/shadow, etc.
* Understand how these files affect:
  + **Authentication**
  + **Networking**
  + **Storage**
* Know how to use them during **system management and repair**

Would you like:

* A **Linux config file cheat sheet**?
* A **file format breakdown** (showing example content)?
* A **real-world troubleshooting scenario** using these files?

Just say the word and I’ll build it for you!