Here is a **comprehensive sentence-by-sentence study note breakdown** of the uploaded document **“157. Vulnerabilities Notes.docx”**, written in **high-yield bullet point format** to ensure **no critical information is omitted**. This breakdown is tailored specifically for **CompTIA A+ 220-1102 (Core 2) Exam — Domain 2.0: Security**.

**✅ 1. Concept Overview**

A **vulnerability** is a **flaw or weakness** in a system that a **threat actor** can exploit to harm devices, data, or networks.

This document covers five key types of system vulnerabilities:

* **Non-compliant systems**
* **Unpatched systems**
* **Unprotected systems**
* **End-of-life operating systems**
* **BYOD (Bring Your Own Device)**

**📘 2. Exam Relevance**

* **CompTIA A+ 220-1102**
* **Domain 2.0: Security**
* **Objective 2.5: Compare and contrast common threats, vulnerabilities, and social engineering attacks**

Key understanding:

* How vulnerabilities increase risk
* How to mitigate each type
* Real-world examples of each vulnerability type

**📋 3. Sentence-by-Sentence Note Breakdown**

**🔐 What is a Vulnerability?**

* A vulnerability is a **flaw or weakness** in a system.
* Can be **exploited by a threat actor** (e.g., hackers or malicious groups).
* Often caused by:
  + Missing security patches
  + Improper configurations
  + Using outdated software/hardware

**⚠️ 1. Non-Compliant Systems**

* A **non-compliant system** is one that **no longer follows the approved configuration baseline**.
* A **baseline** is the approved:
  + OS version
  + Application versions
  + Security patches
  + Configuration settings
    - Configuration Baseline: Set if recommendations for deploying a computer in a hardened configuration.
* Purpose of baseline: ensure **uniform security posture** across all systems.

A **configuration baseline** is a **standard setup** for computers in a company that tells you **exactly how each system should be configured** to stay **secure and consistent**.

**🔍 Think of it like this:**

* It’s a **blueprint or checklist** for:
  + Which operating system version to use
  + What software must be installed
  + Which security patches should be applied
  + What settings (like password rules or firewalls) must be enabled

**🧠 Memory Trick:** “A configuration baseline is the company-approved setup for every system.”

**🖥️ Real-Life Example:**

* Your company says every laptop must run **Windows 10 with the August 2022 security patch KB6616**, Microsoft Word 2021, and antivirus turned on.
* That’s your **baseline**.
* If a user installs extra software or skips updates, the system becomes **non-compliant** — and now it may be **vulnerable** to attacks.

**🧾 Exam Tip:** If you see a question about **“approved security configurations”** or **“ensuring consistency across devices,”** the answer likely involves **configuration baselines**.

**🔧 Real-World Example:**

* If Windows 10 patch **KB6616** (August 2022) is required in the **configuration baseline**:
  + Any system missing that patch is **non-compliant**.
* A user installs **Microsoft Word** without IT knowledge:
  + System might not get **security patches** for Word.
  + **New attack surface** is introduced.
* Sharing folders via **SMB** can make the system vulnerable due to **SMB protocol weaknesses**.

**🧠 Key Point: Non-compliant = outside of hardened, approved configuration = increased vulnerability**

**🩹 2. Unpatched Systems**

* An **unpatched system** has known security updates available — **but they haven’t been installed**.
* Many attacks exploit **known vulnerabilities** where a patch exists.
* **Example:**
  + Microsoft Word is installed but **not updated** → attacker uses known exploit.
* Delay in patching = **window of opportunity** for attackers.

**🧠 Key Point: If a patch exists and isn’t installed, the system is vulnerable — and attackers know it.**

**🛡️ 3. Unprotected Systems**

* Systems lacking **security defenses**:
  + No antivirus or anti-malware
  + No firewall
  + No IDS/IPS
* Unprotected systems are **easy targets** for:
  + Malware
  + Direct attacks
  + Phishing attachments

**📧 Email Scenario:**

* Malware arrives as an attachment.
  + No antivirus? You might open it and get infected.
  + With antivirus? Malware is quarantined automatically.

**🔥 Firewall Scenario:**

* No firewall? Attackers can **connect directly** to your system.
* Software firewall blocks **unauthorized access**.

**🔍 Windows Defender:**

* Includes both **firewall** and **anti-malware**.
* Recommended for **Windows 10/11** as a free built-in defense.

**🧠 Key Point: Protection requires both detection (antivirus) and prevention (firewall).**

**⌛ 4. End-of-Life (EOL) Operating Systems**

* **End-of-life OS**: No longer supported by the vendor.
* No more **security patches**, even when vulnerabilities are discovered.

**🧓 EOL Examples:**

* Windows XP
* Windows Vista
* Windows 7

→ All are **no longer patched** by Microsoft.

**🎯 Mitigation:**

* Upgrade to a **modern OS** like Windows 11 (if hardware allows).

**🧠 Key Point: EOL systems are permanently vulnerable. Upgrading is the only fix.**

**💼 5. BYOD (Bring Your Own Device)**

* Employees bring **personal devices** (phones, tablets, laptops) into the work environment.
* These devices often:
  + Lack antivirus
  + Aren’t patched
  + Don’t have firewalls
  + Use unknown or untrusted configurations

**🕳️ Security Risk:**

* BYOD devices can introduce **unpatched, unprotected systems** to the network.
* **One weak device** can compromise the entire network.
  + “A network is only as secure as its **least secure** device.”

**✅ Best Practice:**

* **Avoid BYOD**
* Instead, have IT **issue company-approved devices**:
  + Properly configured
  + Patched
  + Protected

**🧠 Key Point: BYOD = unpredictable security posture = higher risk to the entire network**

**🧩 4. Real-Life Implementation Examples**

**🔧 Example 1: Non-Compliant System**

* A sales rep installs unapproved Chrome plugins → opens up new vulnerabilities.

**🔧 Example 2: Unpatched System**

* HR PC running outdated Adobe Reader gets infected through a PDF exploit.

**🔧 Example 3: Unprotected System**

* An employee disables antivirus to “speed up” the system — gets infected via phishing.

**🔧 Example 4: End-of-Life OS**

* Warehouse uses Windows 7 → ransomware hits it hard because there are no security updates.

**🔧 Example 5: BYOD**

* Intern connects personal phone to Wi-Fi → phone has malware → starts beaconing outbound traffic.

**🧾 5. Exam Inclusion Notification**

✅ **Yes, all of these topics are directly included in the CompTIA A+ 220-1102 exam**, specifically in:

* **Domain 2.0: Security**
* **Objective 2.5:** Compare and contrast common social engineering attacks, threats, and **vulnerabilities**

**You are expected to:**

* Identify and describe **types of vulnerabilities**
* Understand how to **protect systems** from them
* Match real-world examples to their **corresponding vulnerability**