Here is a **comprehensive, bullet-point-based study note breakdown** of the document titled **“Threats and Vulnerabilities Notes”**, tailored for **CompTIA A+ 220-1102 (Core 2)** exam preparation. This breakdown follows a **sentence-by-sentence analysis**, ensuring no critical detail is missed and aligns with the exam’s **Objective 2.5: Compare and contrast common threats, vulnerabilities, and social engineering attacks**.

**✅ 1. Concept Overview**

This section introduces foundational concepts in cybersecurity focusing on **threats**, **vulnerabilities**, and **risk**—core elements in evaluating security posture. It also introduces distinctions between **information security**, **information system security**, and the practical **balance between security and convenience**.

**📘 2. Exam Relevance**

**Relevant Exam Domain:** Core 2 — **Domain 2.0: Security**, especially **Objective 2.5**

**Key Topics Covered:**

* CIA Triad (Confidentiality, Integrity, Availability)
* Threat vs. Vulnerability
* Internal vs. External Threats
* Zero-Day Exploits
* CVEs (Common Vulnerabilities and Exposures)
* Exploit definition and lifecycle
* Patching systems and system hardening
* Risk calculation (Likelihood × Impact)
* Real-world examples of risk scenarios

**📋 3. Note Breakdown**

**Detailed Sentence-by-Sentence Bullet Notes:**

**🔐 Security vs. Convenience**

* Cybersecurity always involves a **trade-off between convenience and protection**.
* Users prioritize ease of access, while IT admins prioritize securing systems.
* Example: Long, complex Wi-Fi passwords are more secure but less convenient.
* This **friction leads to vulnerabilities** in organizational setups.
* Choosing **convenience over security** can lead to **costly data breaches**.
* Average cost of a breach in 2022: **$4.2 million per incident**.

**📉 Definitions: Threat, Vulnerability, Risk**

* **Threat:** An entity or event that can negatively impact resources (e.g., hackers, hurricanes).
  + A **threat** is *anything* that could potentially **harm your computer, network, or data**.
  + A hurricane can cause harm to physical systems harming the network.
* **Vulnerability:** A weakness that can be exploited by a threat (e.g., outdated software).
  + A **vulnerability** is a **weakness** in a computer, system, or software that could let a threat cause harm.
* **Risk:** The **likelihood and impact** of a threat exploiting a vulnerability.
  + **Risk** is the **chance** that a threat will use a vulnerability to cause harm.
  + Risk = Threat × Vulnerability
* If either a threat or a vulnerability is missing, **no actual risk exists**.

**🔁 Examples of Risk Calculation**

* Leaving a door unlocked is a vulnerability.
  + If no one tries to enter (no threat), **risk is zero**.
* Sending ransomware for Windows OS is ineffective against a **macOS** system.
  + If the system isn’t vulnerable, **no risk occurs**, even if the threat is real.

**🔐 Info Security vs. Info System Security**

* **Information Security:** Protects the data itself (e.g., files, databases).
* **Information System Security:** Protects systems **that store/process** that data (e.g., servers, smartphones).
* Subtle distinction: **Data vs. Devices**

**👥 Internal vs. External Threats**

* **Internal Threats:**
  + Originate from inside the organization (employees, contractors).
  + Can be **malicious** (insider stealing data) or **accidental** (employee opening malware).
* **External Threats:**
  + Come from **outside** the organization (e.g., hackers, natural disasters).
  + Includes **hacktivists** or **environmental issues** (e.g., wildfires).

**📘 CIA Triad (Core Cybersecurity Principle)**

* **Confidentiality:** Only authorized users access the data.
* **Integrity:** Data remains accurate and unaltered.
* **Availability:** Systems and data must be accessible when needed.

**⚠️ Common Vulnerabilities**

* **Non-compliant systems:** Do not follow security policies.
* **Unpatched systems:** Lacking recent security updates.
* **Unprotected systems:** Missing security tools (antivirus, firewalls).
* **Delayed systems:** Late response to known issues.
* **BYOD (Bring Your Own Device):**
  + Increases vulnerability surface (unmanaged devices on corporate networks).

**🧨 Common Threats (Objective 2.5)**

* **Zero-day attacks:** Exploit unknown vulnerabilities.
* **DoS/DDoS:** Overload systems to deny access.
* **Spoofing:** Falsify identity (IP, MAC, email).
* **On-path (MITM):** Intercept data between two parties.
* **SQL Injection:** Inject malicious SQL into queries.
* **Cross-site Scripting (XSS):** Inject scripts into websites.
* **Cross-site Request Forgery (CSRF):** Exploit user authentication to perform unwanted actions.
* **Password cracking:** Automated tools to guess user credentials.
* **Insider threats:** Malicious or accidental internal actors.
* **Supply chain attacks:** Compromise a vendor or service provider.

**🧠 CVE (Common Vulnerabilities and Exposures)**

* **CVE database**: Centralized list of publicly disclosed software vulnerabilities.
* Format: CVE-YYYY-NNNN (e.g., CVE-2017-0144 = 144th vuln in 2017).
* Example: **EternalBlue** (CVE-2017-0144)
  + Exploited by **WannaCry ransomware**
  + Affected Windows Vista → Windows 10, and Server 2008 → 2016.

**⏳ Zero-day Vulnerabilities**

* Not yet known or documented vulnerabilities.
* Once reported → assigned a CVE and no longer considered “zero-day.”

**💻 Exploits & Patching**

* **Exploit**: Software/code that takes advantage of a vulnerability.
* Software vendors issue **patches** to fix vulnerabilities.
* **Attackers reverse-engineer patches** to discover vulnerabilities and create exploit code.
* Delay in patching = **window of opportunity** for attackers.
* Example: An exploit created after Microsoft issues a patch, targeting systems that haven’t yet updated.

**🔄 Security Maintenance Best Practices**

* Always keep systems **patched and updated**.
* Use **anti-malware and antivirus** software.
* Monitor for **new CVEs** and apply patches rapidly to close vulnerabilities.

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

* **Example 1: BYOD Policy**
  + An employee brings their own smartphone infected with malware.
  + The device connects to the corporate Wi-Fi and infects internal systems.
  + Solution: Implement **Mobile Device Management (MDM)** and restrict BYOD access.
* **Example 2: EternalBlue/WannaCry**
  + A hospital using unpatched Windows 7 machines was hit by WannaCry.
  + Medical devices and patient records became inaccessible.
  + Cost: millions in downtime and breach response.
  + Prevention: Regular patching, network segmentation.
* **Example 3: Insider Threat**
  + Disgruntled employee downloads client list before quitting.
  + Organization suffers customer loss to competitor.
  + Solution: Implement **access logging**, **data loss prevention (DLP)**, and **least privilege access**.
* **Example 4: Environmental Threat**
  + A server room with no backup power loses electricity during a storm.
  + No UPS or generator = complete downtime.
  + Mitigation: Ensure **redundant power**, **UPS systems**, and **disaster recovery plans**.

**🧾 5. Exam Inclusion Notification**

✅ **Yes, this content is explicitly covered in the CompTIA A+ 220-1102 exam**, particularly in:

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

**Justification:**

* CVEs, exploits, and patching are fundamental to maintaining security.
* Understanding threats vs vulnerabilities is critical to assessing risk.
* Internal vs external threats are explicitly listed in exam subdomains.
* Real-world attacks like **Zero-day**, **SQL injection**, and **DDoS** are all referenced in CompTIA’s exam objectives.