Here is a **comprehensive and professionally formatted sentence-by-sentence breakdown** of the document **“Insider Threat Notes.docx”**. This is aligned with **CompTIA A+ 220-1102 (Core 2)**, especially under **Objective 2.5: Threats, vulnerabilities, and attacks**.

This version is structured to be pasted **directly into Word** with minimal formatting required — using tight bullet spacing and clean organization.

**🕵️‍♂️ Insider Threat – Detailed Study Notes**

**CompTIA A+ 220-1102 | Domain 2.0: Security | Objective 2.5: Threats, vulnerabilities, and attacks**

**✅ 1. What Is an Insider Threat?**

* An **insider threat** is a current or former employee, contractor, vendor, or partner who:
  + Has **authorized access** to internal systems
  + **Misuses that access** to harm the organization
* Example: An employee like “Tom in sales” downloads the company’s **entire CRM database** to sell it to a competitor — this is **insider abuse**.
* These threats are particularly dangerous because:
  + The attacker has **valid credentials** (username and password)
  + They can access **servers, files, and apps** just like a normal employee
  + They are **difficult to detect** using traditional security tools

**🛑 2. Why Are Insider Threats Hard to Detect?**

* Unlike external threats, insiders already have:
  + **Network access**
  + **Permissions and privileges** to do damage
* Security systems typically trust authenticated users, making **malicious insiders** hard to spot unless unusual behavior is observed.

**🔍 3. Detecting Insider Threats**

* Best detection method is through **active observation and a security-aware culture**.
* Encourage employees to:
  + **Monitor each other’s actions**
  + Ask questions like:

“Hey, why are you downloading 10GB of files at 2 a.m.?”

* This raises awareness of behaviors that don’t align with **normal business needs**.

**🚩 4. Behavioral Indicators**

* Warning signs may include:
  + Open **discontent with the company**
  + Verbal threats or wishing harm on the organization
  + Disgruntled attitude or desire for revenge
* If a person expresses anger or intent to hurt the company:
  + They should be **carefully offboarded**
  + Their network access must be revoked immediately

**🎬 5. Pop Culture Example: Jurassic Park**

* The movie offers a fictional but useful insider threat example:
  + A **disgruntled IT admin** creates a **logic bomb** in the system
* **Logic bomb** = a type of malware that:
  + Executes based on a **trigger** (like a time or event)
  + In this case: a **script** runs daily to check for an input code
* If no code is entered (e.g., employee is absent or leaves):
  + The system **automatically releases dinosaurs** by opening cage doors
  + Spoiler: The admin is killed, the system fails, and chaos follows
* This logic bomb was meant to **punish the organization** after the employee left.

**💣 6. Logic Bombs Explained**

* A logic bomb is malicious code designed to:
  + Activate under certain conditions (e.g., on a specific **date** or after a **missed input**)
  + Cause intentional damage (e.g., delete files, leak data, or shut down systems)
* Real-world logic bomb examples may:
  + **Wipe a hard drive**
  + **Encrypt data (ransomware style)**
  + **Leak sensitive files to public sources** (e.g., WikiLeaks)

**🧾 7. Summary Table – Insider Threat vs Logic Bomb**

| **Concept** | **Definition** |
| --- | --- |
| Insider Threat | A person with legitimate access who misuses it for sabotage or data theft |
| Logic Bomb | Malicious code triggered by a time or event to cause disruption or destruction |
| Disgruntled Employee | A common insider threat profile — may deploy logic bombs or steal data |
| Detection Strategy | Culture of questioning unusual behavior, monitoring login activity |
| Prevention | Least privilege, auditing, access revocation at termination |

**📘 8. CompTIA A+ 220-1102 Exam Relevance**

✅ **Yes – Insider threats and logic bombs are directly included in Objective 2.5.**

You must be able to:

* Recognize behaviors and risks of insider threats
* Understand what a logic bomb is and how it operates
* Know methods to detect, mitigate, and prevent insider misuse

Let me know if you’d like a **CompTIA-style 10-question quiz** based on this content — formatted professionally for Word just like this!

Based on the content of **“Insider Threat Notes.docx”**, here is a professionally formatted **10-question multiple-choice quiz** aligned with the **CompTIA A+ 220-1102 (Core 2)** exam — specifically **Objective 2.5: Compare and contrast common threats, vulnerabilities, and attacks**.

This quiz is designed for **easy pasting into Microsoft Word** — compact formatting, minimal spacing, and clear structure.

**🕵️‍♂️ Insider Threat & Logic Bombs – Quiz (CompTIA A+ 220-1102)**

**Instructions:** Choose the best answer for each question.

**1. Which of the following best defines an insider threat?**

a) A script that triggers based on system activity

b) A person without network access attempting to breach a firewall

c) An individual with authorized access who misuses it

d) A malicious third-party app downloaded by a user

**2. Why are insider threats often difficult to detect?**

a) They rely on encryption to hide their activity

b) Insider threats bypass antivirus programs automatically

c) They have legitimate credentials and permissions

d) They only attack external-facing systems

**3. Which of the following is an example of insider threat behavior?**

a) Sending phishing emails from a fake domain

b) Accessing CRM data at 2 a.m. without business justification

c) Spoofing a MAC address to access Wi-Fi

d) Launching a DDoS attack from outside the network

**4. What type of malware is activated based on a specific time or event?**

a) Worm

b) Trojan

c) Logic bomb

d) Keylogger

**5. What is the main function of a logic bomb?**

a) Continuously scan for vulnerabilities in a network

b) Create encrypted tunnels for secure communications

c) Trigger malicious actions when specific conditions are met

d) Lock out user accounts after failed login attempts

**6. Which behavior might indicate a disgruntled employee posing an insider threat?**

a) Reporting security concerns to management

b) Asking IT for a password reset

c) Making verbal threats or expressing harmful intent

d) Logging out of systems before leaving the office

**7. What’s the best prevention strategy for limiting insider threat damage?**

a) Use WPA3 encryption

b) Limit file sharing over email

c) Implement least privilege and revoke access at termination

d) Require biometric login for all users

**8. In the Jurassic Park scenario, what did the logic bomb do?**

a) Crashed the payroll system

b) Disabled the network firewall

c) Opened the dinosaur cages after no input was detected

d) Changed all root passwords on the server

**9. What is one way to detect a potential insider threat?**

a) Running a virus scan every hour

b) Monitoring system performance metrics

c) Observing employee behavior that deviates from norms

d) Disabling macros in email attachments

**10. Which of the following is NOT an example of logic bomb activity?**

a) A script that deletes files after an employee is terminated

b) A program that leaks files to the public at midnight

c) A phishing campaign to collect login credentials

d) A timer-based script that encrypts company data

**✅ Graded Answer Sheet – Insider Threat & Logic Bombs Quiz**

**CompTIA A+ 220-1102 | Domain 2.0: Security | Objective 2.5**

| **#** | **Your Answer** | **Correct?** | **Correct Answer** | **Explanation** |
| --- | --- | --- | --- | --- |
| 1 | c | ✅ | c | An insider threat is someone **with authorized access** who abuses it to harm the organization. |
| 2 | c | ✅ | c | Insider threats are difficult to detect because they operate using **valid user credentials**. |
| 3 | b | ✅ | b | Accessing large amounts of data outside of business hours is **suspicious insider behavior**. |
| 4 | c | ✅ | c | A **logic bomb** is malware triggered by a specific event or condition (e.g., a date, a missed login). |
| 5 | c | ✅ | c | Logic bombs are designed to **perform malicious actions** only when a certain **condition is met**. |
| 6 | c | ✅ | c | A disgruntled employee making verbal threats is a classic **early warning sign** of insider threat risk. |
| 7 | c | ✅ | c | **Least privilege** and **access revocation** at termination are the best practices to limit insider damage. |
| 8 | c | ✅ | c | In Jurassic Park, the logic bomb **opened dinosaur cages** when the input code was missing. |
| 9 | c | ✅ | c | Observing **behavioral deviations** is an effective insider threat detection strategy. |
| 10 | c | ❌ | **c** | A phishing campaign is **not** a logic bomb — it’s a **social engineering attack**. Logic bombs are **trigger-based scripts** like file deletion or encryption. |

**🎯 Final Score: 9 out of 10 – Excellent!**

**❌ Missed Question Review**

**Question 10**

* **Your answer:** c
* **Correct answer:** **c**
* **Why it’s incorrect:**

While phishing is a common threat, it’s **not triggered by system conditions** and is **not automated code** like a logic bomb. Logic bombs include scheduled scripts or code that runs on events (e.g., logout, date/time, missed check-in).

**💡 Summary Tip**

To distinguish phishing from logic bombs:

* Phishing = **user interaction required** (emails, fake sites)
* Logic Bomb = **silent malware** that activates automatically when triggered

Would you like a **scenario-based follow-up quiz**, or a **visual chart comparing insider threat types** for study? Let me know!