**✅ Justify the Common Types of Attacks Which Recommender Systems Can Face at Manipulating Their Output or Degrading Their Performance**

**📘 Introduction**

Recommender systems help users by suggesting products, movies, or content based on preferences.  
But attackers can try to **manipulate these systems** to show fake results, promote unwanted items, or reduce system accuracy.

These attacks are called **"shilling attacks"** or **"profile injection attacks"**. They can **reduce trust**, **affect business**, and **harm user experience**.

**🛡️ Common Types of Attacks on Recommender Systems**

**1. ⭐ Push Attack (Promotion Attack)**

**🔹 What is it?**

The attacker tries to **promote a target item** to make it appear in more recommendations.

**🔹 How it works:**

* Fake users are created with **high ratings** for the target item.
* These users also rate other items to seem realistic.

**🔹 Purpose:**

* Make a product/movie appear more popular.
* Influence user buying decisions.

**🔹 Example:**

A seller wants to promote a poor-quality product. They create 100 fake users who all rate it 5 stars.

**2. ⛔ Nuke Attack (Demotion Attack)**

**🔹 What is it?**

The attacker tries to **downgrade a competitor's item** by giving it low ratings.

**🔹 How it works:**

* Fake users rate the target item with **very low scores**.
* They also give normal ratings to other items to hide the attack.

**🔹 Purpose:**

* Reduce the rank or popularity of a specific item.

**🔹 Example:**

A company targets a popular movie or product and creates fake accounts giving 1-star ratings.

**3. 👥 Random Attack**

**🔹 What is it?**

A type of attack where fake profiles are created with **random ratings** for normal items and **extreme ratings** for the target item.

**🔹 How it works:**

* Ratings on filler items are chosen randomly.
* The target item is rated either very high (for push) or very low (for nuke).

**🔹 Purpose:**

* Makes the fake profiles harder to detect.
* Blends in with average user behavior.

**4. 🧠 Average Attack**

**🔹 What is it?**

An advanced attack where fake users give ratings close to the **average rating** of each item (not random).

**🔹 How it works:**

* Filler item ratings = average item ratings.
* Target item rating = high or low depending on the attack goal.

**🔹 Purpose:**

* Avoid detection by appearing like a typical user.
* More successful than random attack.

**5. 👨‍👩‍👧‍👦 Group Attack (Sybil Attack)**

**🔹 What is it?**

Multiple fake user profiles act as a **group** to increase the effect of the attack.

**🔹 How it works:**

* Many fake users rate the target item and other items similarly.
* Coordinated behavior boosts the influence.

**🔹 Purpose:**

* Strengthen the attack impact using group behavior.

**🔹 Example:**

A music band creates 500 fake accounts to promote their new song.

**6. 🔁 Bandwagon Attack**

**🔹 What is it?**

Fake users rate the **target item** along with **popular items** to gain trust.

**🔹 How it works:**

* The attacker gives high ratings to trending/popular items.
* Also gives high rating to the item they want to promote.

**🔹 Purpose:**

* Link the target item with trending items.
* Makes it more likely to be recommended.

**7. 🧬 Segment Attack**

**🔹 What is it?**

Targets a **specific user group** by imitating their taste and injecting the target item.

**🔹 How it works:**

* Attacker studies user group behavior (e.g., teenagers).
* Fake profiles mimic that group and promote/demote the target.

**🔹 Purpose:**

* Precise targeting of a particular audience.

**⚠️ Impact of Attacks on Recommender Systems**

* 💔 **Reduces Recommendation Quality**
* ❌ **Shows wrong or harmful suggestions**
* 📉 **Decreases system accuracy and trust**
* 🧪 **Skews evaluation results**
* 💸 **Affects sales, reviews, and product visibility**
* 👤 **Harms user satisfaction**

**✅ Conclusion**

Recommender systems are powerful tools but **vulnerable to various attacks**.  
Attackers use fake profiles or biased ratings to **manipulate outputs** for personal or business gain.  
It is important to detect and prevent such attacks to keep the system **fair, reliable, and trustworthy**.