Vulnerability Assessment life cycle

The Process of Vulnerability Assessment:

The process of Vulnerability Assessment is divided into four stages. Let us discuss them one by one.

Testing or Vulnerability Identification: All the aspects of a system like networks, servers, and databases are checked for possible threats, weaknesses, and vulnerabilities. The goal of this step is to get a list of all the possible loopholes in the security of the system. The testing is done through machines as well as manually and all parameters are kept in mind while doing so.

Analysis: From the first step, we get a list of vulnerabilities. Then, it is time that these are analyzed in detail. The goal of this analysis is to identify where things went wrong so that rectification can be done easily. This step aims at finding the root cause of vulnerabilities.

Risk Assessment: When there are many vulnerabilities, it becomes important to classify them on the basis of risks they might cause. The main objective of this step is to prioritize vulnerabilities on the basis of data and systems they might affect. It also gauges the severity of attacks and the damage they can cause.

Rectification: Once if have a clear layout of the risks, their root cause, and their severity, we can start making corrections in the system. The fourth step aims at closing the gaps in security by introducing new security tools and measures.