What is vulnerability scanning?

Vulnerability Scanning is a technique where a scanner scans an interface to detect any open ports, service running and the versions of the services, if the service is outdated and is prone to attack then it is tagged as a risk, the scanning tool often output the results in the CVSS score.

Difference between vulnerability scanning and penetration testing?

Penetration Testing is a process where the whole process of finding vulnerabilities, identifying risks, determining the level of the risk and reporting, whereas vulnerability scanning is a subprocess of penetration testing which involves scanning an interface like IP, Servers, ports, etc. To find any outdated or services which are prone to risks.

What are some common vulnerabilities in personal computers?

Some common vulnerabilities of a personal computers are lack of SSL certificates in a third party browser this uses HTTP instead of HTTPS, enabled FTP services and not SFTP for file sharing through local servers, using repeated passwords or passwords with common words this is exploited with a simple Brute Force attack, using old versions of Operating System for example the previous versions of Windows are susceptible for Eternal Blue vulnerability.

How do scanners detect vulnerabilities?

Vulnerability scanners detect weaknesses by examining systems and comparing their findings with databases of known flaws. They identify software versions, services, and operating systems (fingerprinting), then check if these match vulnerable versions. They also analyse configurations for weak settings like open ports or default passwords, and in some cases, perform safe simulated exploits to confirm issues.

What is CVSS?

CVSS (Common Vulnerability Scoring System) is a framework used to measure the severity of security vulnerabilities in software and systems. It gives each vulnerability a score from 0 to 10, based on factors like how easy it is to exploit, what impact it can have on confidentiality, integrity, and availability, and whether fixes exist.

How often should vulnerability scans be performed?

Vulnerability scans should ideally be performed on a regular schedule, such as monthly or quarterly, and after major events like system upgrades, new software deployments, or security incidents. High-risk environments may scan more frequently, even weekly or daily, to catch new threats quickly.

What is a false positive in a vulnerability scanning?

A false positive in vulnerability scanning occurs when a scanner flags a system, service, or application as vulnerable, even though the reported vulnerability is not truly present or exploitable. This usually happens due to inaccurate fingerprinting, outdated vulnerability databases, or overly generic detection signatures.

How do you prioritise vulnerability scanning?

Vulnerabilities are prioritized using a combination of severity scores and business context. Security teams usually start with CVSS scores to gauge technical risk, then factor in elements like exploit availability, exposure to the internet, the sensitivity of the affected asset, and potential business impact if compromised.