Periodic Network Vulnerability Scan Process

The list of target IP blocks / addresses is input into our automated scan system.

Then, *Nessus Professional* is scheduled for periodically scanning the target systems and services for vulnerabilities.

Results of the last vulnerability scan is compared to the results of the previous scan. A differential report is automatically generated and emailed to the recipient.

The differential report only contains information about the closed findings, new findings and changed findings. This is an ideal way of keeping a tab on

- the newly discovered vulnerabilities on the existing systems and services
- new vulnerabilities due to software installs, configuration changes, reverts from backup and other changes
- vulnerabilities discovered in the new systems, which were added to the designated IP blocks after the last scan
- changes to the severity level of existing vulnerabilities
- fixed vulnerabilities since the previous report (verification)

Therefore, periodic vulnerability scans is concise and is easy-to-process, helping the security teams and admins to keep a tab on the current security posture of the internet-facing systems.