
Post-testing procedures

Remediation measures, corrective steps, and recommendations are all terms referring to the post testing procedures. During this procedure, you act as an advisor to the remediation team at the target organization. In this capacity, you may be required to interact with a number of technical people with different backgrounds, so keep in mind that your social appearance and networking skills can be of great value here.

Additionally, it is not possible to hold all sets of knowledge required by the target IT environment unless you are trained for it. In such situations, it is quite challenging to handle and remediate every single piece of vulnerable resource without getting any support from the network of experts. We have constituted several generic guidelines that may help you in pushing critical recommendations to your client:

- Revisit the network design and check for exploitable conditions at vulnerable resources pointed in the report.
- Concentrate on the edge-level or data centric protection schemes to reduce the number of security threats before they strike with backend servers or workstations simultaneously.
- Client-side or social engineering attacks are nearly impossible to resist but can be reduced by training the staff members with the latest countermeasures and awareness.
- Mitigate system security issues as per the recommendations provided by the penetration tester may require additional investigation to ensure that any change in a system should not affect its functional characteristics.
- Deploy verified and trusted third-party solutions (IDS/IPS, firewalls, content protection systems, antivirus, IAM technology, and so on) where necessary, and tune the engine to work securely and efficiently.
- Use the divide-and-conquer approach to separate the secure network zones from insecure or public-facing entities on the target infrastructure.
- Strengthen the skills of developers in coding secure applications that are a part of the target IT environment. Assessing application security and performing code audits can bring valuable returns to the organization.
- Employ physical security countermeasures. Apply a multilayered entrance strategy with a secure environmental design, mechanical and electronic access control, intrusion alarms, CCTV monitoring, and personnel identification.
- Update all the necessary security systems regularly to ensure their confidentiality, integrity, and availability.
- Check and verify all the documented solutions provided as a recommendation to eliminate the possibility of intrusion or exploitation.