Remediate Penetration Test Findings

Often, penetration tests are performed for specific purposes:

- As a “dramatic” demonstration of an attack, usually to convince decision-makers of their enterprise’s weaknesses
- As a means to test the correct operation of enterprise defenses (“verification”)
- To test that the enterprise has built the right defenses in the first place (“validation”)

This best practice looks to address what occurs once the penetration testing has been completed. The organization performing the penetration test will provide a written report of their results. It is becoming increasingly popular to conduct penetration tests through third-party legal counsel to protect the penetration test report from disclosure. Once a report is received, the security team and other affected parties within the organization should review the report to understand the findings. The organization performing the test is often available for questions to clarify issues documented in the report.

Issues within the report should then be priortized. As a simple method, some organizations may choose to use the Common Vulnerability Scoring System (term:*CVSS*) which can provide a severity rating for vulnerabilities. But CVSS severity ratings shoudln’t leveraged blindly; a 5/10 in a production system handling election data that is exposed to the internet is likely more important than a 7/10 in an internal testing system that lacks sesntive data.

Specific individuals working to fix issues from the report should report back that the fixes have been successfully completed so that they can be validated by the appropriate internal team.

Goals

1. Work to understand the results report from the penetration test. Create a plan to remediate findings in a logical manner, according to the severity of the findings (Level 3 maturity)

Actions

Level 1 and Level 2 Maturities

There are no actions for Level 1 and Level 2.

Level 3 Maturity

1. Review and understand the results of the penetration testing report with all IT and security staff that have responsibilities.
2. Ask questions of the organization that performed the penetration test to clarify any misunderstandings or concerns that may require an update to the report.
3. Create a list of items to fix.
4. Prioritize this list based on severity.
5. Assign list items to appropriate personnel.

Cost-Effective Tools

- OWASP Penetration Testing Methodologies: This link contains a collection of penetration testing methodologies.

Learn More

- PCI Security Standards Council: A set of standards used by the Payment Card Industry (PCI) for perfomring penetration testieng. Includes qualifications for testers and a technical methodology.

Mapping to CIS Controls and Safeguards

- 18.3: Remediate Penetration Test Findings
- 18.4: Validate Security Measures

Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.