Perform Internal Penetration Test

ON THIS PAGE

Goals

Actions

Level 1 and Level 2 Maturities

Level 3 Maturity

Cost-Effective Tools

Learn More

Mapping to CIS Controls and Safeguards

Mapping to CIS Handbook Best Practices

Internal penetration testing can provide valuable and objective insights about the existence of vulnerabilities in enterprise assets and humans, and the efficacy of defenses and mitigating controls to protect against adverse impacts to the enterprise. They are part of a comprehensive, ongoing program of security management and improvement. They can also reveal process weaknesses, such as incomplete or inconsistent configuration management, or end-user training.

Penetration tests are expensive, complex, and potentially introduce their own risks. Experienced individuals from reputable organizations must conduct them. Accordingly, it is rare that this expertise already exists within an election office. Some risks include unexpected shutdown of systems that might be unstable, exploits that might delete or corrupt data or configurations, and the output of a testing report that needs to be protected itself, because it gives step-by-step instructions on how to break into the enterprise to target critical assets or data.

Goals

1. Conduct a penetration test of internal jurisdiction assets with capable and trustworthy organizations (Level 3 maturity)
2. Understand and correct findings of the results report in a timely manner (Level 3 maturity)

Actions

Level 1 and Level 2 Maturities

There are no actions for Level 1 and Level 2.

Level 3 Maturity

1. Identify high and low-value election assets requiring internal penetration testing.
2. Identify a suitable organization for performing the testing. These resources may be available via a state agency, university, or third-party company. Note that it is rare that this expertise already exists within an election organization.

Cost-Effective Tools

- OWASP Penetration Testing Methodologies: 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

- 18.1: Establish and Maintain a Penetration Testing Program
- 18.4: Validate Security Measures
- 18.5: Perform Periodic Internal Penetration Tests

Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

Previous
Remediate Penetration Test Findings

Next
Network Segmentation Based on Sensitivity