CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

REMOTE PENETRATION TESTING

The CISA team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA's Remote Penetration Test (RPT) utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways. RPTs are similar to risk and vulnerability assessments but focus only on externally accessible systems with a tradeoff made for more service capacity at the expense of assessment scope. As a remote service, it is less costly and more scalable than on-site offerings; however, it is more limited in organizational insight and context.

SCENARIOS

External Penetration Test: Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.

External Web Application Test: Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.

Phishing Assessment: Testing the stakeholder email infrastructure through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.

Open Source Information Gathering: Identify publicly available information about the stakeholder environment which may be useful in preparing for an attack.

ASSESSMENT OBJECTIVES

- Conduct assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways.
- Simulate the tactics and techniques of real-world threats and malicious adversaries.
- Test centralized data repositories and externally accessible assets/resources.
- Avoid causing disruption to the customer’s mission, operation, and network infrastructure.

ASSESEMENT TIMELINE

Pre-Planning

- Request RPT
- Receive RPT Capabilities Brief
- Sign and return RPT Rules of Engagement
- Determine RPT services, scope, and logistics during pre-assessment call(s)

Planning

- Confirm schedule
- Establish trusted points of contact

Execution (Up to Six Weeks)

- Dependent on resource availability
- Critical findings are immediately disclosed

Reporting

- Briefing and initial recommendations
- Final report review and receipt – 10 days

ABOUT

Our Team

The CISA team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA's security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **vulnerability_info@cisa.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*