CYBER ASSESSMENT FACT SHEET
Remote Penetration Test

February 2022

OVERVIEW

CISA's Remote Penetration Test (RPT) utilizes a dedicated remote team to identify and assess vulnerabilities. The RPT team works with the stakeholder to test internet exposure to eliminate exploitable pathways. RPTs focus only on externally accessible systems. As a remote service, it is more scalable than on-site offerings.

RPT includes:

- **External Penetration Test** assesses open ports, protocols, and services in order to verify whether the stakeholder network is accessible from the public domain by an unauthorized user.
- **External Web Application Test** evaluates web applications for potential exploitable vulnerabilities and can include automated scanning, manual testing, or a combination of both methods.
- **Phishing Assessment** tests the stakeholder's email infrastructure through carefully crafted phishing emails—containing a variety of malicious payloads—sent to the stakeholder trusted points of contact.
- **Open-Source Information Gathering** identifies publicly available information about the stakeholder environment that may be useful to a malicious cyber actor in preparing for an attack.

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.

PHASES

Pre-Planning	Planning	Execution	Post-Execution
Stakeholder: • Requests RPT. • Receives RPT capabilities briefing. • Signs and returns Rules of Engagement.	**CISA:** • Confirms schedule. • Establishes stakeholder trusted points of contact. • Determines RPT services, scope, and logistics during pre-assessment calls with stakeholder.	• CISA immediately discloses critical findings. **Note:** Execution is dependent upon resource availability.	**CISA:** • Provides briefing and initial recommendations. • Provides final report within 10 days of RPT completion.

HOW TO GET STARTED

Contact vulnerability@cisa.dhs.gov to get started. Please keep in mind:

- CISA's assessments are available to both public and private organizations at no cost.
- Service availability is limited; service delivery timelines are available upon request. CISA prioritizes service delivery queues on a continuous basis to ensure no stakeholder/sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.