NCCIC

National Cybersecurity and Communications Integration Center

NATIONAL CYBERSECURITY ASSESSMENTS AND TECHNICAL SERVICES (NCATS)

CYBER HYGIENE: VULNERABILITY SCANNING

The NCATS Cyber Hygiene: Vulnerability Scanning activities continuously assess the "health" of external stakeholder endpoints reachable via the Internet. Activities consist of voluntary target discovery, vulnerability scanning, and checks of web and email best practices.

Scanning Phases

Target Discovery

Process of identifying all active Internet accessible assets (networks, systems and hosts) to be scanned for vulnerabilities.

Vulnerability Scanning & Configuration Tests

Occurs as a continuous series of non-intrusive checks in order to identify existing or potential vulnerabilities and configuration weaknesses.

Scanning Objectives

- Maintain a continually updated enterprise view of the cybersecurity posture of stakeholder's Internet accessible systems
- Understand how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities and reduce risk

Scanning Timeline

[1] Pre-Planning

- Request service
- Receive Cyber Hygiene brief
- Provide target list (scope)
- Sign and return documents

[2] Planning

- Confirm scanning schedule
- Pre-scan notification

[3] Execution

- Initial scan of submitted scope
- Rescan scope based on detected vulnerability severity:
  - 12 hours for "critical"
  - 24 hours for "high"
  - 4 days for "medium"
  - 6 days for "low"
  - 7 days for "no vulnerabilities"

[4] Post-Execution

- Scanning summary report with Report Card
- Vulnerability mitigation recommendations
- Detailed findings included as exports
- Weekly reporting intervals

NCCIC

National Cybersecurity and Communications Integration Center

About

Our Team

NCATS is a group of highly trained information security experts within DHS NCCIC. Our mission is to measurably reduce the cybersecurity risks to our Nation's cybersecurity infrastructure.

DHS is responsible for protecting the Nation's infrastructure from physical and cyber threats, including those impacting business and government operations.

Our Work

A proactive, risk-based approach to analyzing stakeholder systems

Expertise in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance

Empowering stakeholders to increase speed and effectiveness of their cyber-attack response capabilities

Our Services

NCATS also offers the following services:

[+] Phishing Campaign Assessments

[+] Risk and Vulnerability Assessments

[+] Remote Penetration Testing

[+] Red Team Assessments

[+] Validated Architecture Design Review

[+] Training and Qualification for Third Party Assessment Organizations

Additional Information

NCATS security services are available at no-cost. Our stakeholders include Federal, State, Local, Tribal and Territorial levels of governments, as well as Critical Infrastructure Private Sector companies.

NCATS does not share attributable information collected during assessments without written and agreed consent from the stakeholder. However, anonymized data is used to develop non-attributed reports for trending and analysis purposes.

Assessments are not conducted in response to an incident, but to identify, mitigate, and remediate vulnerabilities prior to exploitation by an attacker.

Get Started

To learn more about NCATS or request service, contact us using the information below. Testing availability is limited so contact us soon to get started.

NCATS_INFO@HQ.DHS.GOV

In support of our national mission, the NCATS 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 many stakeholders that the NCCIC and NCATS support.