NYSERNet Scan+

Frequently Asked Questions

What is the Scan+ service?

Security vulnerability scanning is a process through which devices connected to a network are tested for available points of access which could lead to security exposures. NYSERNet's Scan+ service uses the Nessus Vulnerability Scanner software and its knowledge base to identify exposures found in an institution's assets. NYSERNet performs unauthenticated external scans of an institution's network, which are run on a weekly basis. These scans originate from the NYSERNet network, providing visibility into the security posture of an institution's network from its perimeter. A highlights report of the results is delivered via email and its data is managed via the Scan+ Portal. The Scan+ Portal allows designated staff to prioritize identified risks, track changes in risk posture over time, and assign attributes to those risks, such as mitigation status, responsible parties, and planned remediation dates.

What types of scans are possible?

An external scan is run from outside of an institution's network perimeter, where a firewall typically resides. Such a scan reflects which devices and services they offer are visible to those outside of the institution's network. An internal scan is run from inside an institution's network or from a scanner authorized to bypass any institutional firewall controls. This type of scan reflects which devices and services are visible from within an institution's network.

How does a scan work?

The Nessus scanning software transmits connection requests to every requested IP address within an institution's network, identifying accessible devices. These requests attempt to identify TCP, UDP and ICMP ports on each device which offer a response, indicating some type of a server application is running and is accessible. There are 65,536 possible ports available for both TCP,UDP and ICMP on any networked device.

Does Scan+ perform internal scans?

We are working to enhance the Scan+ service to perform unauthenticated internal scans of an institution's network. At this time, institutions which perform their own authenticated or unauthenticated internal scans can upload those scan results into the Scan+ Portal. Clients can then manage the status of risks identified by the internal scans alongside the results of Scan+ external scans.

Can a scan harm my networked devices?

Scan+ scans do not attempt to enter a networked device or its applications nor access any data contained within the device. As networks are routinely subject to scans from the Internet, external scans from Scan+ should not pose any greater risk of harm. As internal scans are not blocked by a firewall, however, those scans may connect to applications on devices not typically accessed otherwise. Scans can be tailored to limit device impact as needed.

NYSERNet Scan+

Frequently Asked Questions

What are the components of the Scan+ service?

- NYSERNet-run external vulnerability scanner using the Nessus security product to identify vulnerabilities
- A database for maintaining scan data
- The Scan+ Portal for analyzing the scan data and managing vulnerabilities
- Email-based reporting of the scan results and current security posture
- Facility for importing third-party scans:
    - Institution-run internal scans
    - External scans performed by the Department of Homeland Security (DHS)
- NYSERNet-run internal vulnerability scanning (please contact us)

How large of a network does Scan+ support?

Vulnerability scanning can be a challenge for research and academic institutions, which often have substantial campus networks with large volumes of IP addresses. The Scan+ service does not place a limit on the number of IPv4 addresses scanned and processed.

Does Scan+ support IPv6?

Unlike IPv4 addresses, the number of IPv6 addresses available to an institution is virtually limitless. An individual /64 IPv6 subnet (equivalent to an IPv4 /24 subnet on a typical LAN) has a theoretical capacity of 2^64 (1.8446744e+19) addresses. An institution's /48 IPv6 address block, for example, has sufficient capacity for 65,536 /64 subnets. Given the sheer volume of IPv6 addresses available within such a network, it is impossible to conduct an effective scan of an IPv6 address block. Support for scanning individual IPv6 addresses, however, may be made available in a future version of Scan+.

What security safeguards are in place within Scan+?

The web server is behind a firewall and client access is protected by certificate-based encrypted HTTPS communications. We also offer multi-factor authentication (MFA) access to the Scan+ portal, which can be optionally enabled by clients. The Scan+ databases are on a protected network with highly restricted access. The Scan+ data is stored on encrypting hard drives, and service backup images are also maintained on encrypted storage. All supporting infrastructure is maintained within secure facilities with restricted access.

Which institutions are eligible to participate?

Any Research and Education institution is eligible to participate in this service. NYSERNet membership is not required. Please contact us for additional information.

What is included with the Scan+ service?

The Scan+ Service provides external vulnerability scanning of an institution's entire IPv4 address space and access to the Scan+ Portal. The ability to import third party scan results (internal institution scans, or external DHS scans) is available at an additional cost. Participation in NYSERNet's Security Users Group.

NYSERNet Scan+

Frequently Asked Questions

What service term lengths are available?

The service term is (14) months from service commencement with the first two (2) months considered a "proof-of-concept" period at no charge.

How can I learn more about Scan+?

For additional information please contact membership@nysernet.org.