

Security Scans on NYU-NET

NYU Network and Security staff run periodic network scans to test the integrity of portions of NYU-NET and equipment attached to the network. Such equipment may include (but is not limited to) desktop computers, minicomputers, file servers, print servers, and network infrastructure devices.

What is a scan?

A scan in this context is a program which examines a system's network presence by sending it various sorts of packets and analyzing the replies, making connections to the service ports on the system and seeing what information it offers and presenting it with various forms of input and seeing what the response is. Based on a machine's reactions we can conclude something about the system and software it is running and the flaws present in that software.

Scans range from simple inventories up to nondestructive versions of the attacks that outsiders constantly launch against NYU-NET. Well over a thousand different tests are routinely run during an serious ITS scan of a system.

Can I run a scan?

Because attackers often scan as a precursor to attack, because a poorly written or configured scanner can cause problems on the network, and because there are no legitimate reasons to scan a network that can not be satisfied in other ways only ITS Network Services may scan NYU-NET. Any tool which can perform "autodiscovery" of client or servers is probably a scanner and must be configured NOT to perform such autodiscovery. Please contact [ITS Technology Security Services](#) for assistance in understanding this requirement.

Does ITS Scan?

Scans are routinely run to conduct an inventory of devices that are attached to NYU-NET, to make note of services offered by systems on the network, and to identify vulnerabilities that might allow a malicious person to break into the system.

Systems can also be tested for vulnerabilities to Denial of Service attacks which try to make the system or service crash or hang. It is important that public servers stand up to such attacks since they are used as part of some two step efforts to deface or subvert systems. Testing for this class of vulnerability is done less often to minimize the

disruptions of testing but it is expected that all such systems will be patched and configured to survive a brief Denial of Service attack such as the test includes.

Why does ITS scan?

As part of its duty to manage the network ITS Communications & Computing Services must both inventory and test the systems on the network. Scanning allows ITS to efficiently detect when machines are running outdated or vulnerable versions of software (such as sendmail) that might risk the security of the system. Scanning also allows ITS to identify systems that are running inappropriate services (such as desktop computers offering Domain Name Service), or that are not properly registered with the NYU Network Operations Center (NOC).

When ITS finds a problem someone on the staff will contact the responsible person for that system or network so they can fix it. This also highlights why it is important to keep up-to-date the "responsible person" information for each registered host and why every host on NYUNET must be registered. If no responsible person can be contacted the system in question must be taken off the network.

Where are scans announced?

Most general network scans are announced on the Security Alerts Forum (send a blank email to join-security-alerts@forums.nyu.edu to subscribe). The technical person responsible for managing the systems in a given department or subnet is expected to join this list.

In order to get a picture of the real state of the network, not all scans are or can be announced. We may also do a scan targeted at particular issues when there is a vulnerability which is being actively exploited so that we notify owners of affected systems as quickly as possible. When we receive a problem report or discover a problem with a individual machine, it may well be scanned intensely as part of the problem diagnosis.

What are those things in my log file?

Most scans are performed non-intrusively, so that while they may cause events to be logged on systems that support event logging, they are not destructive or harmful.

Will a scan break my machine?

In the course of a scan, conditions can arise with systems and configurations which can result in momentary disruptions of service. These may result in distress or panic in system

operators, administrators and users who are unaware of these scans. As a matter of policy, it is important that potentially affected parties be aware of the nature and purpose of the security scans.

None of the tests performed routinely are actively destructive. Many tests are performed which "push the envelope" of the system's operation, looking for known bugs and vulnerabilities. Because we test for bugs, malfunctions, and vulnerabilities, it is possible to uncover a previously unknown vulnerability which results in an interruption of service. This is rare but not impossible.

When such an event does occur, it becomes critical to analyze the interruption of service. If it proves to really be a newly discovered vulnerability, actions then need to be taken to notify respective vendors and security agencies for corrective actions and advisories. In such cases, NOC and Security staff work with the manager of the system involved to conduct an appropriate analysis.

If you have a problem or simply want to verify that your system was scanned by ITS rather than by a would be attacker, please contact the ITS Technology Security Services at security@nyu.edu.

When appropriate, certain systems may be allowed to *temporarily* "opt out" of wide-ranging scans, if special needs, circumstances, or justifications, such as imminent upgrades, are made known and agreed to in advance. Those systems can then be specially and individually monitored until the systems are properly secured.

Questions or comments? Send email to security@nyu.edu.

All contents copyright

© New York University

All rights reserved

Page last revised: **August 23, 2004**

Page last reviewed: August 22, 2006