Vulnerability Scanning Procedures and Guidelines

Purpose

To provide a common set of methodologies and requirements to standardize vulnerability scans on campus servers and networking infrastructure.

Background

Vulnerability scans provide a mechanism for system administrators to assess the security posture of the servers they manage by probing the systems for open ports, services and application and operating system patch levels. Open ports are queried for information regarding what services are listening and each service is compared against a database of known vulnerabilities or issues. System Administrators can utilize vulnerability scan reports to assess the security posture of their system and outline remediation tasks required to bring the system into compliance.

There are two primary types of vulnerability scans: assessment and maintenance.

Assessment Scans

Assessment scans involve scanning a system as it exists to a computer or user outside the systems firewall. Assessment scans typically run without credentials and with or without exceptions in firewall rules. Port assessment scans provide reports on what ports are visible, what services are running on the open ports and any known vulnerabilities for each service. Full assessment scans provide similar reports to the port assessment scans but include information for services running on all system ports.

Maintenance Scans

Maintenance scans are similar to assessment scans but typically produce more in-depth scanning reports. Maintenance scans typically run with credentials and exceptions in host firewall rules. Port maintenance scans provide reports on what services are running on each port and any known vulnerabilities for each service, application and operating system. Full maintenance scans provide similar reports to the port assessment scan, but report on all system ports. This report is a key component for determining remediation requirements for the System Administrator.

Credentialed versus Non-Credentialed Scans

One of the critical components of a Maintenance Scan is the use of system credentials. The scanning engine utilizes these credentials to login to the system to enumerate services, applications and patch levels. The information obtained by using credentials during a maintenance scan allows administrators to perform a more comprehensive assessment of the security posture of their system, verify the performance of their patching mechanisms, check service configurations and discover erroneously or maliciously installed services.

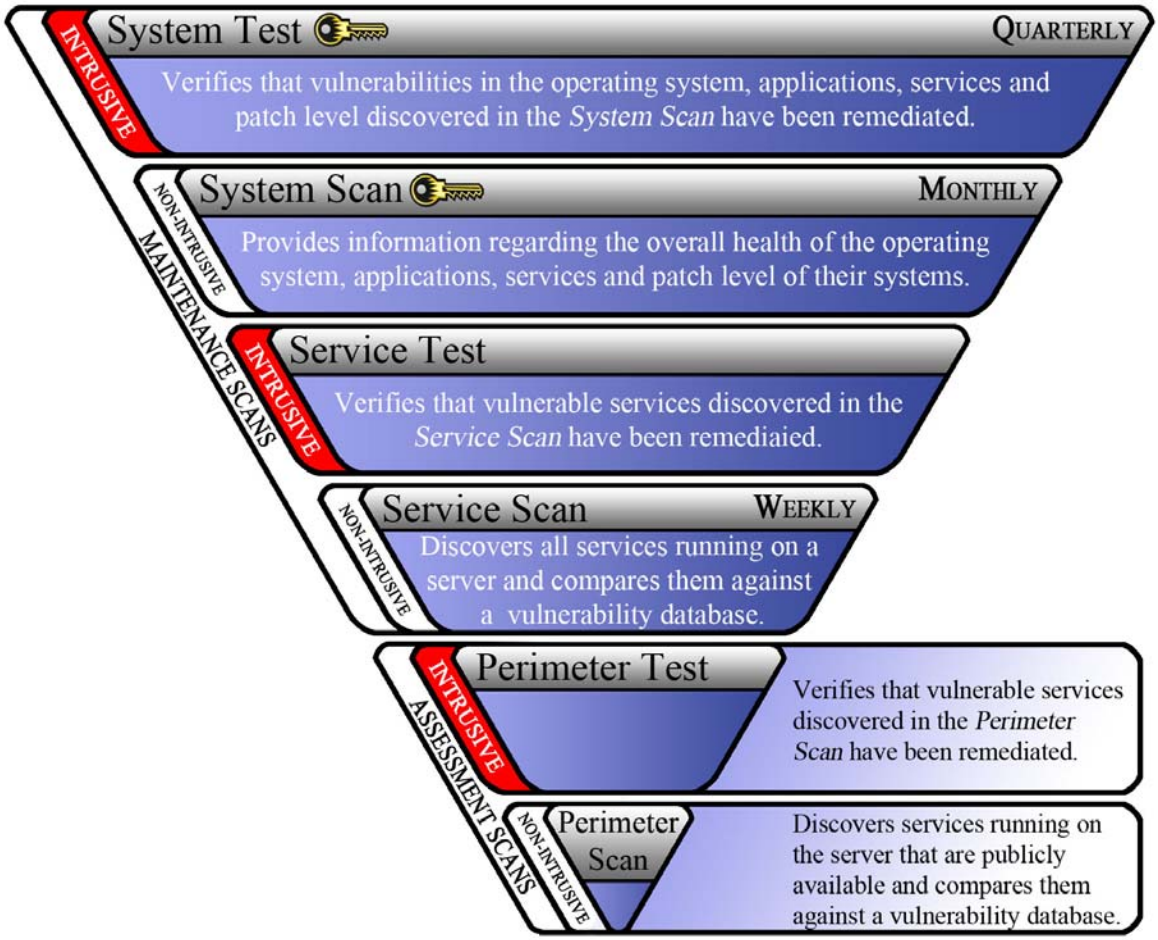
SECURITY NOTE: To protect against piggyback attacks originating from an owned scanning engine, it is recommended that firewall exceptions and user credentials used in performing maintenance scans be deactivated when not in use.

Intrusive versus Non-Intrusive Scans

There are two classes of vulnerability scans, intrusive and non-intrusive. Simply put, non-intrusive scans have little to no system impact when run. Intrusive scans however, have a possibility of disrupting a service or taking a system offline. Non-intrusive scans are the standard for examining systems and discovering services and vulnerabilities. Intrusive scans are similar to non-intrusive scans but also test remediation efforts.

Full Scan versus Port Scans

The degree of access a system grants to the vulnerability-scanning engine determines the comprehensiveness of a scan. Port scans are scans initiated against a firewalled system testing only those ports open to the public. Port scans are the least comprehensive scan type as they provide a superficial view of the system. Full scans are scans initiated against a firewalled system testing all 65,535 ports. Full scans provide a comprehensive view of the system that allows system administrators to check services not available to the general user and discover services running erroneously or maliciously.



Vulnerability Scanning Requirements

The following requirements standardize the vulnerability scanning of systems on the campus network. All systems must meet the requirements outlined in the following sections.

Scan Type and Schedule

System Administrators must perform, analyze, remediate or document exceptions and report on all maintenance scans completed on their systems.

The Information Security Office requires the following types of vulnerability scans for ensuring the security of a system:

- Each stage of the Server Implementation Lifecycle
  - *Operating System Installation*
  - *Application Installation*
  - *Database Installation*
  - *Move to Production Environment (GO-Live)*
- Weekly trusted assessment scans
- Monthly maintenance scans
- Periodic assessment scans

Of these types, moving a server from development to production and monthly maintenance scans require the use of intrusive credentialed scans to provide the greatest depth of testing and assurance. Weekly assessment scans do not require intrusive scans or credentials, but must run within the trusted zone in order to provide System Administrators with in-depth reports for comparisons against the system's security baseline. System Administrators may schedule additional assessment scans at their discretion.

All server administrators must meet the following minimum vulnerability scanning requirements.

Scan Activity	Intrusive	Credentialed	Full Scan
Each stage of the Server Implementation Lifecycle	YES	YES	YES
Weekly Assessment Scans	NO	NO	YES
Monthly Maintenance Scans	NO	YES	YES
Quarterly Maintenance Scan	YES	YES	YES
Assessment Scans	NO	NO	YES/NO

Scan Review

The System Administrator or designated department scan analyst must review all vulnerability scans for a system within 24 hours of scanning. If a scan occurs during the weekend or on a holiday, scan review must occur on the first business day following the scan.

Remediation

System Administrators are responsible for remediating vulnerabilities identified during vulnerability scanning. System Administrators must evaluate vulnerabilities identified as critical by the scan engine or high-risk through analysis within 24 hours of discovery. System Administrators must report their evaluation and remediation options to the System Owner or designee upon completion of evaluation.

System Administrators must evaluate and report remediation options for important vulnerabilities to the System Owner or designee, within 5 days. System Administrators will evaluate informational items identified by the vulnerability scans and report options to System Owners or designee at their discretion. Any critical or high-risk vulnerabilities remaining un-remediated after 48 hours or important vulnerabilities remaining un-remediated after 10 days must have a signed exception document on file with the System Owner.

The System Administrator as must document mitigating action that reduce the risk of exposure but do not remediate the original vulnerability. An example of a mitigating action is moving a vulnerable service port behind a host-based firewall. This action simply protects the system against exposure of the vulnerability but does not remediate the vulnerability, but applying a patch would.

Following remediation steps, the System Administrator must run a follow-up scan targeting the vulnerability to confirm remediation.

Vulnerability Type	Evaluate	Remediate	Document Exception
Critical or High-Risk	Within 24 hours	Within 48 hours	After 48 hours
Important	Within 5 days	Within 10 days	After 10 days
Information	At System Administrator's discretion		

Exception Handling

The System Administrator will document any critical/high-risk or important vulnerabilities remaining un-remediated past the timelines established in the Remediation section of this document. This exception document must include the vulnerability and the risk to the system while un-remediated. The System Owner or designee must accept and sign the exception document and maintain a system log for review by the Information Security Office during the annual vulnerability assessment.

Reporting

The System Administrator must document and report any exceptions on their systems to the System Owner or designee at completion of evaluation or remediation. The System Administrator will include Application, Database and Data Owners as needed on a per scan basis. The System Administrator may provide the Information Security Office a report at their discretion.

If reporting involves a designee of the System Owner, the designee must provide a monthly summary of scanning activity and exception documents to the System Owner.

Audience	Report	Frequency
System Owner/Designee	Exception Documents	Every Scan
System Owner	Summary Report from Designee	Monthly
Application Owner	Vulnerability Report	As Needed per Scan
Database Owner	Vulnerability Report	As Needed per Scan
Data Owner	Vulnerability Report	As Needed per Scan
Information Security Office	All Reports	As Needed

Information Security Office Vulnerability Scans

The Information Security Office will perform periodic assessment scans against systems on the campus network. These periodic scans will be non-intrusive and non-credentialed. Information Security Office personnel will generate reports for internal use. The Information Security Office will also review the Monthly Vulnerability Scans completed by System Administrators on a quarterly basis and report discrepancies to system owners.

The Information Security Office will work closely with System Administrators to perform an intrusive non-credentialed assessment scan annually. The System Administrator, the System Owner and the Information Security Officer will receive a report documenting the results of the annual vulnerability assessment and exceptions.