



Gonzaga University Information Technology Policy and Procedure

SUBJECT: Vulnerability Scanning

Policy Number	Date Issued	Date Reviewed
IT109		

PURPOSE:

Gonzaga University is committed to implementing formal procedures for guarding against, detecting, and reporting malicious software and vulnerabilities. As such, the University will continually assess potential risks and vulnerabilities and develop, implement and maintain appropriate administrative, physical, and technical security measures to ensure the integrity of University services and information.

Vulnerability scanning is a process by which devices connected to the campus network are probed in an attempt to identify security related issues including, but not limited to, missing or weak passwords, insecure software installations, missing patches, updates and service packs, software with known security issues, and back-door administration programs installed on compromised hosts.

SCOPE:

This policy applies to all faculty, staff, students, temporary employee, and other personnel within Gonzaga, including employees of affiliated third-party organizations. This policy applies to all equipment that is owned, leased, operated, maintained, or connected to the Gonzaga University network, including personally owned equipment.

POLICY:

All computers, servers, routers, switching equipment, and other electronic devices connected to the campus network shall be scanned regularly for vulnerabilities.

Vulnerability scanning will only be conducted by the University Information Security team or its designees.

The Information Security Team will provide communication to appropriate personnel at least 24 hours prior to any vulnerability scan. In the event the vulnerability scan is in response to an incident or security breach, communication of the scan may take place after the scan.

Vulnerability scan results and statistics will be produced on at least a bimonthly basis by the IT Asset Manager or other member of the Information Security Team.

Faculty, staff and students suspecting a malicious software infection should immediately contact the Help Desk by phone or walk-in.

Individuals responsible for computer equipment that present serious or critical security vulnerabilities must correct those vulnerabilities in a timely manner before connecting to the campus network.

Computers with security vulnerabilities that threaten the integrity or performance of the campus network may be denied access to campus computing resources at the discretion of the Information Security Team. This may include but is not limited to connection to the campus network.

Notification of scanning activities will be automated when possible.

DEFINITIONS:

Analyze – Through this process, current patch levels must be determined and a minimum baseline policy should be defined.

Critical Vulnerability – Defined as any vulnerability which is identified as “critical” by the US Department of Energy Computer Incident Advisory Capability (CIAC) vulnerability assessment or as determined by the vendor of the impacted software.

Information Security Team – The group of University IT staff responsible for identifying security vulnerabilities, conducting vulnerability scans, and responding to security incidents.

Lead Technician – The technician responsible for a specified group of target machines.

Remediate – To “remedy” the vulnerabilities found by bringing systems up to date, best accomplished via policy based solutions.

Report – Reporting conducts a change review and verifies successful deployment of patches. Reporting should also include enough review, analysis, and adjustment to close the loop and begin cycle again automatically (see Patch Management Best Practices)

Security Vulnerability – Those software and/or hardware issues that typically affect default installations of software that are susceptible to attack or malicious activity.

PROCEDURE:

- I. Individual areas may scan their assigned IP address ranges.
- II. Notification must be sent to Network Support and the Help Desk x5550 prior to conducting scans
- III. The following information must be included in the notification:
 - a. Scheduled Date and Time of the scan
 - b. Originating IP address
 - c. Estimated duration of scan

- d. Target IP address – range
- IV. Machines conducting regular or scheduled scans must be registered with Network Support Service.
- V. Determine the components within the University that process, transmit, or store information and are vulnerable to malicious software. Such components may include:
 - a. Workstations
 - b. Servers
 - c. Firewalls
 - d. Palmtops
 - e. Laptops.
- VI. Enterprise vulnerability detection software will be used to conduct vulnerability scans against the campus network and devices on a regular basis. Multiple software packages will be utilized for the purposes of cross-checking accuracy.
- VII. Various reporting mechanisms will be used to produce vulnerability scan results and statistical information.
- VIII. In the event that scan notification is not possible via an automated process, it is the responsibility of the technician conducting the scan to send appropriate notifications.
- IX. Lead Technicians will review the reports and remediate any critical vulnerability that cannot be remedied using alternate methods.
- X. Any critical vulnerability that cannot be remedied should be tracked in the Help Desk Management software and referenced to the specific device.
- XI. Any device that remains in a vulnerable state by the next scan date may be removed from the network.

ENFORCEMENT:

Any University personnel found to have violated this policy may be subject to disciplinary action, at the discretion of their supervisor, as described in the university's **Personnel Policies and Procedures Manual**.

Date:	President or Designee