

## Server Recommendations

Questions and additional information requested include:

1. Please identify which servers are teaching and research related (as opposed to “production” servers).
2. For each server for which you are responsible, what identified services **need** to be visible from the Internet?
3. Who are the server administrators? Please let us know what academic/administrative group actually takes care of the servers.
4. What type of information is being housed on these servers? (Whether that information is meant to be accessible over the Internet or not.)
5. Who has access to the information on the servers and how is that process managed?
6. Please verify ports and services that on are *meant* to be turned on, i.e., SMTP, IMAP, POP3.

## Practices to make the servers on the campus less vulnerable

Based on the audit report:

*Default services that should not be enabled include:*

1. WebDAV – (Distributed authoring and versioning) Allows for remote changes to Web Server
2. Default server installations (not configured)
3. Front page extensions - Allows for remote changes to Web Server
4. All sample (and example) files should be removed, as they present vulnerabilities.
5. Debugging turned off (Trace and Track)
6. Internet Printing
7. .HTR file processing

## Practices which will reduce the risks for any system serving up information, whether internal or external:

1. Userid/passwords non-obvious combinations (For any server which contains any data of personal nature - however slight - see #3 below)
2. Web servers, which access database services allow for the possibility of SQL injection attacks, these should be protected per userid/passwords, and evaluated for off-campus use.
3. If a given server has been set up for convenience in administration, use VPN when needed for administration from off campus.
4. Keep all patches and revision levels up to date at *least* once a year by scheduling a formal review of your servers. More often is preferable, and campus server scans will catch new vulnerabilities as they are identified.

**Practices which will assist University Computing in case of problems with, or complaints about, the server:**

1. If your server is performing a service Web, Mail, Database, etc, it should have a known DNS name and contact person.
2. In which building/room is the system housed?

Please contact [network@sjsu.edu](mailto:network@sjsu.edu), with any questions you may have.