University at Buffalo
Information Technology

Server Security and Hardening Standards
Appendix A: Server Security Checklist

Server Description

- Server DNS hostnames: _____
- System Administrator Names: _____
- What Services does the Server provide? _____
- Describe the data stored on the servers and it' categorization per: http://www.buffalo.edu/ubit/policies/it-policies-a-to-z/data-classification-standard.html:

  _____

  _____

  _____

Checklist

Check each item in the list that has been verified to be true.

Server Configuration

☐ The server does not provide more than one service.

☐ The server has a minimal operating system configuration.

☐ The server has been scanned with the CIS CAT tool and has been secured appropriately according to scanning results.

☐ The server has been scanned with a vulnerability scanner and has been secured appropriately according to the scanning results.

☐ The server is protected with a host based firewall.

☐ The server is protected with a network firewall at the edge of its network.

☐ Firewall rules are whitelist based.

☐ If possible, group based device policies are employed for firewall rules.

☐ Firewall rules and configurations are backed up.

☐ Remote administration access is secured with appropriate network encryption protocols.

☐ Remote access is disabled for built-in privileged system accounts such as root and Administrator.

☐ All hosts (laptops, workstations, mobile devices) used for system administration are secured as follows

- Secured with an initial password-protected log-on and authorization.
- Whole disk encryption required on portable devices
- Whole disk encryption is recommended on desktop workstations.
- Anti-malware software with the most up-to-date malware database.
- Separate local admin and user accounts.
- Up to date VPN software.
- Regular, timely, OS, and software updates.

☐ The OS installed on the server has been installed by the system administrator.

☐ Additional software components added above and beyond the base OS install are documented.

☐ Only software necessary for the server's primary function has been installed and enabled on the server.

☐ Superfluous services provided with the base OS install have been removed or disabled.

☐ Any compilers or development environments that were installed in order to install software have been removed.

☐ The server uses the appropriate NTP servers.

- Windows servers in UBAD: use domain controllers
- All other servers: use tick.acsu.buffalo.edu and/or tock.acsu.buffalo.edu

☐ OS and software patching will be performed either monthly or according to the vendor's patch release schedule.

- A patch management tool should be used if possible.

☐ If encryption is used only acceptable encryption standards are used.

☐ If used, private keys used in public-private key pairs of asymmetric cryptography are only be available to the individual associated with the private key's identity or an operational group responsible for the service.

☐ Server Data is properly backed up to another system.

Server Security Monitoring and Protection

☐ If the server has a Windows OS, it is running Intrusion Detection and Prevention Software approved by the Information Security Office.

☐ Logs are collected and monitored for security related events.

☐ Logs are replicated on a system other than the server generating the logs.

☐ Security related events are reported to the Information Security Office

☐ Audit trails of security related events are retained.

☐ The server will be scanned for vulnerabilities on a weekly basis and address in a timely manner.

Access Control

☐ Where possible access controls to files, data and applications follows a role-based model.

☐ Unneeded user accounts have been removed from the system.

☐ Elevated privileges are not granted to non administrative accounts.

- Tools such as sudo or runas may be used to temporarily elevate privileges of user accounts.

☐ Where possible administrative accounts are linked to a single individual.

☐ Shared administrative accounts have their passwords and use restricted and protected to the fullest extent possible.

☐ Passwords adhere to the UBIT password policy.

☐ The default Windows Administrator account has been disabled.

- A new administrator account may be created.

☐ Default passwords for built-in accounts have been disabled.

☐ Where possible automatic idle time-out log-off of administrative users sessions must be set to 10 minutes.

☐ Direct server login capability has been disabled for accounts that do not require it.

☐ Logon banners have been implemented for interactive logins, explaining appropriate system use and that user activities could be monitored.

☐ The number of failed login attempts to the server is limited to five. Upon five failed login attempts, the account is locked out of the system for at least one hour.

☐ User accounts of persons unaffiliated with UB (such as hired contractors and consultants) a limited to a specific period of time required for the purposes of their engagement or support assistance. These accounts provide only the necessary minimum level of access that is required for the task in which they have been contracted.