Generic Hardening Checklist- Queen's University - SCOP

How to use the checklist

Print the checklist and check off each item you complete to ensure that you cover the critical steps for securing your server. The Security Officer uses this checklist during risk assessments as part of the process to verify that servers are secure.

How to read the checklist

Steps (√) - This is for administrators to check off when she/he completes this portion.

To Do - Basic instructions on what to do to harden the respective system

Note - The QU Note at the bottom of the page provides additional detail about the step for the university computing environment. If there is a “Note” for this step.

Server Information

MAC Address	
IP Address	
Machine Name	
Date	

Steps √	To Do	Notes
A. Preparation and Installation		
	1. record system details: IP, Machine Name, MAC Address for system 2. If machine is a new install, protect it from hostile network traffic, until the ož 3. Set a BIOS/firmware password and/or - Configure the device boot order to prevent unauthorized booting from alternate media. 4. physically securing the cpu and storage media	1
B. e and Initial Lockdown		
	1. Ož 2. Configure SSH, disabled all non-secure ! , Telnet) 3. Configure and enable firewall 4. Enable and test OS and Applications logg] 5. Enable VM encryption if available. 6. Configure an NTP server . 7. .	SSH 2 DNS, NTP 3

	8. Record notes on dependencies/reasons installed	

B.1 Anti-Virus Considerations

	1. Install and enable anti-virus software. 2. Configure to update signature daily on AV. 3. Integrity checking of critical operating system files should be enabled and tested. Third-party tools may also be used to implement this.	

C. Minimize services (network) / Accounts / Tuning

	1. Disable any services, ports, applications and/or user accounts that are not being utilized 2. Limit connections to services running on the host to authorized users of the service (utilize firewall technology, AD/LDAP Roles)	

D. Logging

	1. All administrator or root access must be logged. 2. Capture messages sent to syslog AUTH facility. 3. Log files on non-system disks or remote server 4. Review Logs for unauthorized access to system	

E. Files/Directory Permissions/Access

	1. Set daemon umask 2. Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.	

F. System Access, Authentication, and Authorization

	1. Ensure that system is configuration in a secure way (LDAP over SSL, local accounts not listed, firewall enable). 2. Configure a screen-saver to lock the console's screen automatically, if the host is left unattended. Require passwora	

4. review of accounts

- http://www.securityfocus.com/
- Clam AntiVirus is an open source (GPL) anti-virus toolkit for UNIX, designed especially for e-mail scanning on mail gateways. http://www.clamav.net/
- http://www.linuxsecurity.com/
- Published flaws and exploits: http://www.milw0rm.com/

Queen's Hardening Checklist

- Solaris Hardening Checklist
- Red Hat Linux Hardening Checklist
- Macintosh OS X Hardening Checklist
- Windows Server Hardening Checklist

---

return to