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 operating system is installed, patched and hardened. 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. Patches, Packages/Additional Software and Initial Lockdown		
	1. Operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures. 2. Configure SSH, disabled all non-secure access (FTP, Telnet) 3. Configure and enable firewall 4. Enable and test OS and Applications logging. 5. Enable VM encryption if available. 6. Configure an NTP server . 7. Enable automatic notification of patch availability.	SSH 2 DNS, NTP 3

8. Record notes on dependencies / versions 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 password to unlock.
3. Consider Configure TCP Wrappers.

G. User Accounts and Environment

1. Ensure Password Fields are Not Empty
2. Set quotas
3. Accounting on User accounts for auditing

H. Ongoing System Maintenance

1. security patches of OS and applications.
   update notes on dependencies / versions installed.
2. periodic audits
3. periodic reviews of logs (look for non-standard access / activities)

	4. review of accounts - disable/delete accounts no longer in use. 5. review of services - disable service no longer in use. And archive / securely erase data no longer needed for these disable services. System accounting gathers baseline system data (CPU utilization, disk I/O, etc.) every 10 minutes. Once a normal baseline for the system has been established, unauthorized activity (password crackers and other CPU-intensive jobs, and activity outside of normal usage hours) may be detected due to departures from the normal system performance curve.	
I. Warning Banners		
	1. Create warning banners for standard login services. Recommended Banner "This is a Queen's Univeristy computer resource and is intended to be used by authorised Queen's Univerity users only. If you are not an authorised user, please do not attempt to access. All access attempts are monitored. Any unauthorised access will be procesecuted by Law and University policy"	

Notes:

1. The machine should be behind a firewall that blocks all not allowed incoming traffic.
2. If you decide to utilize SSH, the ISO highly recommends the following:
   - Change the port from port 22 to something/anything else. There are scripts online that malicious hackers can use against an SSH server. These scripts always attack port 22 since most people do not change the default port.
   - Do not allow root logins via SSH.
   - If possible, use keys with passphrase instead of just passwords. To create rsa keys, follow these commands:

     ```
     ssh-keygen –t rsa
     ssh server “mkdir .ssh; chmod 0700 .ssh”
     scp ./ssh/ida_rsa.pub server:.ssh/authorized_keys2
     ```

3. On campus DNS and NTS server are:

   ```
   130.15.126.54, 130.15.126.52 - DNS
   time.queensu.ca
   ```

References:

See Queen's Hardening Checklist and CIS Benchmark for OS for details.

- The Center for Internet Security
- Benchmarks Tools
- Subscription information for the "@RISK: The Consensus Security Alert" weekly newsletter from SANS is at: http://www.sans.org/newsletters/

- 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 Main Index
Last Reviewed: 18 Feb 2009