HP-UX 11i Provisioning and Hardening Checklist

General Information

Name of Individual Performing the HP-UX 11i Provisioning and Hardening				
Last Name	**First Name**	**Middle Name**	**Title**	**Date of Review**

Additional Information			
Department	**Division**	**Office**	**Immediate Supervisor**

Server Information		
(1). Hostname of Server		**Additional Information:**
(2). Type of Application(s) on server		
(3). IP Address of Server		
(4). Function of Server		
(5). Other Vital Information		
(6). FIPS Security Category		
(7). Data | Info. Classification Level		

Vulnerability Severity Codes	
Severity 1	**Vulnerabilities which when exploited lead to immediate superuser access, unauthorized access to a machine, or allow an attacker to bypass security controls.**
Severity 2	**Vulnerabilities which provide an attacker information with a high probability of allowing unauthorized access to a machine, or to bypass security controls.**
Severity 3	**Vulnerabilities which grant an attacker information that may possibly lead to the compromise of a machine, or the bypassing of existing security controls**
Severity 4	**Vulnerabilities which generally degrade the overall security of a system when left unresolved.**

Configuration

	Task	Severity Code	Date Completed	Signature
(1).	Ensure that the most up to date and vendor supported version of HP-UX is installed. Ensure all hotfixes and patches are installed.	1		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(2).	Remove all applications, and listening ports which are not required for operations.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(3).	Ensure that default and unnecessary accounts such as “gopher ”,“ games” and “news” have been removed from the system. Additionally ensure that necessary accounts do not have blank passwords.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(4).	Ensure that the server has been configured to run in “Trusted Mode”. This can be accomplished with the following command: *tsconvert*	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(5).	The /etc/securetty file should be owned by a privileged account such as root, bin, or sys. Non-privileged access can lead to compromise. Additionally the permissions of this file should be set to 0640 or more restrictive.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(6).	The /etc/securetty file should not contain any extended ACLs as this can lead to unauthorized modification of the file.	2		
Additional Information:	**This will prevent removable storage devices from running executables with the same permissions as the owner.**			

	Task	Severity Code	Date Completed	Signature
(7).	Ensure that the system requires authentication when booting into single-user or maintenance mode. This can accomplished by verifying that the BOOTAUTH11i product is installed, and that the /etc/default/security file is root owned, and contains the BOOT_AUTH=1 flag.	2		
Additional Information:	**find / -xattr –print -exec runat {} ls –al \;**			

	Task	Severity Code	Date Completed	Signature
(8).	Ensure that the /etc/default/security file has permissions set to 0644 or more restrictive.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(9).	The system should be configured to lock accounts after a certain number of unsuccessful login attempts. This number should reflect organizational or regulatory requirements. The following files will need to have the timeout parameter modified:	2		
Additional Information:	**/opt/hpsmh/lbin/envvars** **/opt/hpsmh/conf.common/smhpd.xml** **/opt/hpsmh/conf/timeout.conf**			

	Task	Severity Code	Date Completed	Signature
(10).	Graphical deskstop sessions should be configured to time-out and lock the screen after a period of inactivity which is in compliance with organizational or regulatory standards. This setting can be configured in the /etc/dt/config/C/sys.resources file. The following parameter should bet set:	2		
Additional Information:	**dtsession*lockTimeout: <InactivityTimeout >**			

	Task	Severity Code	Date Completed	Signature
(11).	Ensure that the /etc/default/security file has the MIN_PASSWORD_LENGTH, PASSWORD_MIN_UPPER_CASE_CHARS, PASSWORD_MIN_LOWER_CAS_CHARS, PASSWORD_MIN_DIGIT_CHARS, PASSWORD_MIN_SPECIAL_CHARS, and the PASSWORD_HISTORY_DEPTH variables set to a value which is compliant with organizational or regulatory requirements.	3		
Additional Information:				

	The login session is not operating with root privileges. **The display station is located within a controlled access area.**			
(12).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	If required the Password Hashing Interface should be installed. Additionally ensure that the /etc/default/security file has the CRYPT_DEFAULT parameter set to a value which reflects the organizationally or regulatory required encryption algorithm strength.	2		
Additional Information:				
(13).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Ensure that the /etc/default/security file has the SU_ROOT_GROUP parameter set to a value which reflects a “wheel” group. This will ensure that only authorized users are able to switch user to the root account, even if they manage to guess the root credentials.	2		
Additional Information:				
(14).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Only the root account should have a UID of 0. Other accounts with this UID will have root privileges.	2		
Additional Information:				
(15).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	The root accounts home directory should not have extended ACLs and should have permissions set to 0700.	2		
Additional Information:				
(16).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	The root accounts environmental PATH variable should only contain absolute paths. These will begin with a /. Additionally none of these directories should be world writable.	2		
Additional Information:				
(17).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Unless otherwise required for operations, the root account should be restricted to directly logging on only from the system console. This can be configured by ensuring that *console* or */dev/null* are the only contents of the /etc/securetty file.	2		
Additional Information:				
(18).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	System command files, such as /etc, /bin, /sbin, /usr/bin, should have permissions set to 0755 or more restrictive. This will protect the files from unauthorized modification. Additionally these files should not have extended ACLs.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(19).	Ensure that the NIS/NIS+/yp files are owned by a privileged account such as root, sys, or bin, as these files control the systems authentication processes. Additionally, these files should have permissions set to 0755 or more restrictive.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(20).	All global initialization files (IE, /etc/.login, /etc/bashrc, /etc/profile, etc) should have permissions set to 0644 or more restrictive in order to prevent unauthorized modification of user logon environments.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(21).	All skeleton files are contained within /etc/skel. These files should be owned by root, and have permissions set to 0644 or more restrictive as these files control user startup parameters. Additionally these files should not have extended ACLs.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(22).	Ensure that the default umask contained in the global initialization files is set to 077 or more restrictive. The umask will set the file permissions on all newly created files.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(23).	Only those crontab files which are required for operations should exist. All other should be disabled or removed. Crontabs which are required for operations should be owned by root and have permissions set to 0644 or more restrictive.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(24).	The cron.allow, cron.deny, at.allow, and at.deny files should be owned by root and have permissions set to 0644 or more restrictive, in order to protect against unauthorized job scheduling.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(25).	The system should be protected from stack based buffer overflows by preventing instructions from executing within the stack. This can be accomplished with the following command:	2		
Additional Information:	**kctune executable_stack=0**			
	Task	**Severity Code**	**Date Completed**	**Signature**
(26).	Disable rlogin/rsh access by removing `/etc/hosts.equiv, /.rhosts,`	2		

	and all of the "r" commands in `/etc/inetd.conf`, unless they are required for operations.			
Additional Information:				

Auditing

	Task	Severity Code	Date Completed	Signature
(1).	Ensure that the /etc/rc.config.d/auditing file has the AUDOMON_ARGS flags set to -p 20, -t 1, -w 90. This provides for at least some modicum of useful forensic data to be collected for auditing purposes.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(2).	Ensure that the syslog startup script is enabled in order to require the auditing of successful and unsuccessful login and logout attempts.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(3).	All system log files should have permissions set to 0640 or more restrictive in order to prevent unauthorized modification or tampering of the system audit trail. Additionally no system log or audit files should have extended ACLs.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(4).	System audit executables such as /sbin/audfilter and /sbin/auditdp should be owned by root, have permissions set to 0750 or more restrictive, and should not have extended ACLs.	2		
Additional Information:				

Availability

	Task	Severity Code	Date Completed	Signature
(1).	Within the /etc/default/security file ensure that the NUMBER_OF_LOGINS_ALLOWED parameter has been set to a number which reflects organizational or regulatory requirements and provides protection from resource exhaustion. For most organizations a setting of 10 will be sufficient.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(2).	Ensure that all network enabled daemons have permissions set to 0755 or more restrictive. This will protect them from unauthorized starting, stopping, or modification. Additionally, ensure that none of these daemons have extended ACLs.	2		
Additional Information:				

	Task	Severity Code	Date Completed	Signature
(3).	The /etc/resolv.conf file should be owned by root. This will prevent unauthorized modification of system's DNS resolver. Additionally, this file	2		

	should have permissions set to 0644 or more restrictive, and not have an extended ACL.			
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(4).	The /etc/hosts file should be owned by root. This will prevent unauthorized modification of system's predetermine host addresses. Additionally, this file should have permissions set to 0644 or more restrictive, and not have an extended ACL.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(5).	The /etc/nsswitch.conf file should be owned by root. This file controls the system's account and host lookup procedures. Additionally, this file should have permissions set to 0644 or more restrictive, and not have an extended ACL.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(6).	The /etc/group and /etc/passwd files should be owned by root. These files are vital to the system's authentication processes and access should be strictly controlled. Additionally, these files should have permissions set to 0644 or more restrictive, and not have an extended ACL.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(7).	The /etc/shadow file should be owned by root. The shadow file contains the encrypted authentication information for the system, and access to this file should be strictly controlled. Additionally, this file should have permissions set to 0400 or more restrictive, and not have an extended ACL.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(8).	The rhosts_auth module should not be configured in /etc/pam.conf, as this allows hosts which are identified in the file to remotely access the system without authentication.	2		
Additional Information:				
	Task	**Severity Code**	**Date Completed**	**Signature**
(9).	Ensure that source routing has been disabled by issuing the following command:	3		
Additional Information:	**ndd -set /dev/ip ip_forward_src_routed 0** **Edit /etc/rc.config.d/nddconf and add/set:** **TRANSPORT_NAME[x] = ip** **NDD_NAME[x] = ip_forward_src_routed** **NDD_VALUE[x] = 0**			
(10).	**Task**	**Severity Code**	**Date**	**Signature**

			Completed	
	Ensure that the system is protectedfrom TCP SYN flood attacks but implementing SYN cookies. This can be configured by issuing the following commands:	2		
Additional Information:	**ndd -set /dev/tcp tcp_syn_rcvd_max <500+, based on available memory>** **Edit /etc/rc.config.d/nddconf and add/set:** **TRANSPORT_NAME[x]=tcp** **NDD_NAME[x]=tcp_syn_rcvd_max** **NDD_VALUE[x]=500**			