			General Info	rmation					
	Name of Individual Performing the HP-UX 11i Provisioning and Hardening								
Last Name First Name Middle Name Tit							Date of Review		
	Additional Information								
Demonst		Division							
Depart	ment	Division	Office	Imm	ediate Supervisor				
			Server Infor	mation					
_``	stname of Server			Addi	tional Information	:			
	pe of Application(s)	on server							
	Address of Server nction of Server								
	her Vital Informatio	n							
	S Security Category								
(7). Da	ta Info. Classificati	ion Level	Vulnerability Sev	erity Codes					
C	Vulnerabil	ities which when	exploited lead to immed			norized access to	o a machine,		
Severi	or allow an		ass security controls.	-	-		-		
Severi			de an attacker informati ypass security controls.	ion with a hig	gh probability of	allowing unaut	horized		
Severi	Vulnerabil	ities which grant	an attacker information security controls	n that may po	ossibly lead to th	e compromise o	f a machine,		
Severi			ally degrade the overall	security of a	system when lef	t unresolved.			
			Configura	ation					
		-	Task		Severity Code	Date	Signature		
(1).	Ensure that the most up to date and vendor supported version of HP-UX is			1	Completed				
	installed. Ensure a	ll hotfixes and patch	nes are installed.		1				
Addi	ional Information:								
Auun									
		-	Task		Severity Code	Date	Signature		
(2).	Demons all anali			a aution of face	Seventy couc	Completed	oignature		
	operations.	Remove all applications, and listening ports which are not required for operations			2				
						I			
Addit	ional Information:								
		1	Task		Severity Code	Date Completed	Signature		
(3).	Ensure that default and unnecessary accounts such as "gopher "," games" and								
			system. Additionally ensure to passwords	that	2				
necessary accounts do not have blank passwords.									
Additional Information:									
		-	Task		Severity Code	Date Completed	Signature		
(4).		rver has been config vith the following co	gured to run in "Trusted Moc ommand: <i>tsconvert</i>	le". This can	2				
					L	I	I		
Addit	Additional Information:								

HP-UX 11i Provisioning and Hardening Checklist

		Task	Severity Code	Date Completed	Signature
(5).	bin, or sys. Non-privi	e should be owned by a privileged account such as root, leged access can lead to compromise. Additionally the le should be set to 0640 or more restrictive.	2		
Addi	tional Information:				
(-)		Task	Severity Code	Date Completed	Signature
(6).	The /etc/securetty fil unauthorized modifie	le should not contain any extended ACLs as this can lead to cation of the file.	2		
Addi	tional Information:	This will prevent removable storage device same permissions as the owner.	ces from runnin	g executables	with the
		Task	Severity Code	Date Completed	Signature
(7).	or maintenance mod BOOTAUTH11i produ	m requires authentication when booting into single-user e. This can accomplished by verifying that the ict is installed, and that the /etc/default/security file is tains the BOOT_AUTH=1 flag.	2		
Addi	tional Information:	find / -xattr –print -exec runat {} ls –al \;			
(0)		Task	Severity Code	Date Completed	Signature
(8).	Ensure that the /etc/ restrictive.	default/security file has permissions set to 0644 or more	2		
Addi	tional Information:				
		Task	Severity Code	Date Completed	Signature
(9).	unsuccessful login at	e configured to lock accounts after a certain number of tempts. This number should reflect organizational or ents. The following files will need to have the timeout	2		
Addi	tional Information:	/opt/hpsmh/lbin/envvars /opt/hpsmh/conf.common/smhpd.xml /opt/hpsmh/conf/timeout.conf			
		Task	Severity Code	Date Completed	Signature
(10).	screen after a period regulatory standards	essions should be configured to time-out and lock the of inactivity which is in compliance with organizational or . This setting can be configured in the resources file. The following parameter should bet set:	2		
Addi	tional Information:	dtsession*lockTimeout: <inactivitytimeout></inactivitytimeout>			
		Task	Severity Code	Date Completed	Signature
(11).	PASSWORD_MIN_UP PASSWORD_MIN_LO PASSWORD_MIN_SP	default/security file has the MIN_PASSWORD_LENGTH, PER_CASE_CHARS, WER_CAS_CHARS, PASSWORD_MIN_DIGIT_CHARS, ECIAL_CHARS, and the PASSWORD_HISTORY_DEPTH ue which is compliant with organizational or regulatory	3		
Addi	tional Information:		·		

	The login session is not operating with roo			
	The display station is located within a cont	rolled access area.		
	Task	Severity Code	Date Completed	Signature
(12).	If required the Password Hashing Interface should be installed. Additionally ensure that the /etc/default/security file has the CRYPT_DEFAULT paramete set to a value which reflects the organizationally or regulatory required encryption algorithm strength.	r 2		
Addit	tional Information:			
	Task	Severity Code	Date Completed	Signature
(13).	Ensure that the /etc/default/security file has the SU_ROOT_GROUP parameters 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		
Addit	tional Information:			
(4.4)	Task	Severity Code	Date Completed	Signature
(14).	Only the root account should have a UID of 0. Other accounts with this UID whave root privileges.	vill 2		
Addit	tional Information:			
(45)	Task	Severity Code	Date Completed	Signature
(15).	The root accounts home directory should not have extended ACLs and shoul have permissions set to 0700.	^d 2		
Addit	tional Information:			
	Task	Severity Code	Date Completed	Signature
(16).	The root accounts environmental PATH variable should only contain absolut paths. These will begin with a /. Additionally none of these directories should be world writable.			
Addit	tional Information:			
	Task	Severity Code	Date Completed	Signature
(17).	Unless otherwise required for operations, the root account should be restric to directly logging on only from the system console. This can be configured be ensuring that <i>console</i> or <i>/dev/null</i> are the only contents of the /etc/securett file.	by a		
Addit	tional Information:			
	Task	Severity Code	Date Completed	Signature
(18).	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.	d 2		
Addit	tional Information:			

	Task	Severity Code	Date	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	Completed	Signature
Addit	tional 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		
Addit	tional 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		
Addit	tional 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		
Addit	tional 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		
Addit	tional 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		
Addit	tional 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		
Addit	tional Information: kctune executable_stack=0			
(26).	Task	Severity Code	Date Completed	Signature
	Disable rlogin/rsh access by removing /etc/hosts.equiv, /.rhosts,	2		

	and all of the "r" commands in /etc/inetd.conf, unless they are require for operations.	d		
Addi	tional Information:			
	Auditing			
	Task	Severity Code	Date	Signature
(1).	Ensure that the /etc/rc.config.d/auditing file has the AUDOMON_ARGS flags s to -p 20, -t 1, -w 90. This provides for at least some modicum of useful forensi data to be collected for auditing purposes.		Completed	
Addi	tional Information:			
	Task	Severity Code	Date Completed	Signature
(2).	Ensure that the syslog startup script is enabled in order to require the auditin of successful and unsuccessful login and logout attempts.	g 2		
Addi	tional 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.			
Addi	tional 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		
Addi	tional 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		
Addi	tional 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		
Addi	tional Information:			
(2)	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		

Additional Information: Task Severity Code Date Completed Signature (4). The /etc/hosts file should be owned by root. This will prevent unauthorized in the entropy of		should have permiss	ions set to 0644 or more restrictive, and not have an			
Task Severity Code Date Completed (4). The /etc/hosts file should be owned by root. This will prevent unauthorized modification of system's predetermine host addresses. Additionally, this file petterned ACL. 2 Image: Completed Additional Information: Image: Completed 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 Date Completed Signature (6). The /etc/fnsawtfiles should be owned by root. These files are visit on the system's and rest should be rookup proct. These files are visit on the system's automatication processes and access should be arrich; controlled. Additionally, these files should be owned by root. These files are visit on the system's automatication processes and access should be arrich; controlled. Additionally, these files should be owned by root. These files are visit on the system's automatication processes and access should be arrich; controlled. Additionally, these files should be owned by root. These files are visit of the owned of the system, and access to 1664 or more restrictive, and not have an extended ACL. Severity Code Date Completed Signature (7). The /etc/shadow file should be owned by root. The shadow file contains the encrypted authentication information of the system, and access to 1616 file should be strictly controlled. Additionally, this the should have permissions set to 0400 or more restrictive, and non thave an extended ACL. Severity Code		extended ACL.				
Task Severity Code Completed Signature (4). The /etc/hots file should be wored by root. This will prevent unauthorized act. 2	Addi	tional Information:				
(4). The / etc/hosts file should be owned by root. This will prevent unsutforized addresses. Additionally, this file should have permission set to 0644 or more restrictive, and not have an extended ACL. 2 2 2 Additional information: Task Severity Code Date Completed Signature (5). The / etc/inswitch.conf file should be owned by root. This file controls the system* account and host lookup procedures. Additionally, this file should have permissions set to 0644 or more restrictive, and not have an extended ACL. 2 Date Completed Signature (6). The / etc/group and / etc/grossw files should be owned by root. This file controls the value of the system? authonitization processes and access should be strictly out to the system? authonitization processes and access should be strictly out to the system? authonitization processes and access should be strictly out to the system? authonitization processes and access to to 0644 or more restrictive, and not have an extended ACL. Additional information: 2 Date Completed Signature (7). The / etc/group and / etc/grossw file should be owned by root. The shadow file contains the encrypted authentication information for the system, and access to this file should be completed ACL. Additional information: 2 Date Completed Signature (7). The / etc/group and / etc/grossw file should be comed by root. The shadow file contains the encrypted authentication information for the system, and access to this file should be acticly wand to the system?			Task	Severity Code		Signature
Image: constraint of the structure of the	(4).	modification of syste should have permiss	m's predetermine host addresses. Additionally, this file	2		
Instrument Itsik Severity Code Completed Signature (5). The fetr/nswitch.conf file should be owned by root. This file controls the system's account and host lookup procedures. Additionally, this file should have permission set to 0644 or more restrictive, and not have an extended ACL. 2 Date Signature Additional Information: Task Severity Code Date Signature (6). The fetr/group and /etr/passwd files should be owned by root. These files are vital to the system's aurotexases and access should be strictly controlled. Additionally, these files should have permission set to 0644 or more restrictive, and not have an extended ACL. 2 Date Signature (7). The fetr/should file should be owned by root. The shadow file contains the encrypted authentication information information for the system, and acces to this file should be strictly controlled. Additionally, this file should have permission set to 0604 or more restrictive, and not have an extended ACL. Additional information: 2 Date Signature (7). The fetr/shadow file should be comfigured in /etr/pam.conf, as this allows hosts which are identified in the file to remotely access the system 2 Date Signature (8). Ther fosts_auth module should not be configured in /etr/pam.conf, as this allows hosts which are identified in the file to remotely access the system 2 Signature (9). Task Severity Code Completed Signature (9).	Addi	tional Information:				
(5). The /etc//nswitch.com file should be owned by root. This file controls the date 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 Image: Completed in the file 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 Image: Completed is completed in the file or more restrictive, and not have an extended ACL. Additional Information: Task Severity Code is completed in 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 Image: Completed is completed in the file to remotely access the system in allows hosts which are identified in the file to remotely access the system is allows hosts which are identified in the file to remotely access the system is allows hosts which are identified in the file to remotely access the system is allows hosts which are identified in the file to remotely access the system is allows hosts which are identified in the file toremotely access the syst			Task	Severity Code		Signature
Task Severity Code Date Completed Signature (6). The /etc/group and /etc/passwafiles 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 Date 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 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 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. Severity Code Date Completed Signature (9). Task Severity Code Date Completed Signature (9). Task Severity Code Date Completed Signature (9). Task	(5).	system's account an have permissions set	d host lookup procedures. Additionally, this file should	2	completed	
Iask Severity Code 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 2 2 2 Additional Information: Image: Severity Code Date Completed Signature 5 (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 2 1 Additional Information: 2 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 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 2 Date Completed Signature (9). Task Severity Code </td <td>Addi</td> <td>tional Information:</td> <td></td> <td></td> <td></td> <td></td>	Addi	tional Information:				
(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 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 an extended ACL. 2 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 Acce. 2 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 and inhout authentication. 2 Date Completed Signature (9). Task Severity Code Date Completed Signature (9). Task Severity Code Date Completed Signature (9). Task Severity Code Date Completed Signature Additional Information: ndd -s			Task	Severity Code		Signature
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 1 1 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 1 1 (9). Task Severity Code Date Completed Signature (9). Task Severity Code Date Completed Signature (1). Ensure that source routing has been disabled by issuing the following command: 3 1 1 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 Severity Code Completed Signature	(6).	vital to the system's controlled. Addition	authentication processes and access should be strictly ally, these files should have permissions set to 0644 or	2		
Task Severity Code 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 1 1 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 1 1 (9). Task Severity Code Date Completed Signature (9). Ensure that source routing has been disabled by issuing the following command: 3 1 1 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 1 1	Addi	tional Information:				
(7). 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: Image: Completed authentication information for the system, and access to this file should have permissions set to 0400 or more restrictive, and not have an extended ACL. 2 Additional Information: Image: Completed authentication information for the system, and access the system information in the file to remotely access the system information: 2 Image: Completed authentication information for the system, and access the system information: 2 (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 Image: Completed information: (9). Task Severity Code Date Completed Completed in formation: Signature information: Additional Information: Ind -set /dev/ip ip_forward_src_routed 0 Etit /etc/rc.config.d/nddconf and add/set: TRANSPORT_NAME[x] = ip NDD_NAME[x] = ip Additional Information: Ind -set /dev/ip ip_forward_src_routed 0 Etit /etc/rc.config.d/nddconf and add/set: TRANSPORT_NAME[x] = ip Image: Completed in the file in t			Task	Severity Code		Signature
Image: 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 2 1 1 Additional Information: 2 1 1 1 1 (9). Task Severity Code Date Completed Signature (9). Ensure that source routing has been disabled by issuing the following command: 3 1 1 Additional Information: Indd -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 NDD_VALUE[x] = 0 1 1	(7).	encrypted authentic should be strictly cor	ation information for the system, and access to this file ntrolled. Additionally, this file should have permissions set	2		
I ask Severity Code 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 1 1 Additional Information: 2 <	Addi	tional Information:				
(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: Image: Completed in the file to remotely access the system is a completed in the file to remotely access the system is allows hosts which are identified in the file to remotely access the system without authentication. 2 Additional Information: Task Severity Code is a completed in the file to remotely access the system is a completed in the file to remotely access the system without authentication. Date completed is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system without authentication. (9). Image: Task is a completed in the file to remotely access the following command: Date completed is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a completed in the file to remotely access the system is a			Task	Severity Code		Signature
(9). Task Severity Code Date Completed Signature Image: Signature 1 <td>(8).</td> <td>allows hosts which a</td> <td>re identified in the file to remotely access the system</td> <td>2</td> <td></td> <td></td>	(8).	allows hosts which a	re identified in the file to remotely access the system	2		
Item Task Severity Code Completed Signature (9). Ensure that source routing has been disabled by issuing the following command: 3 3 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 Image: Completed of the second of the	Addi	tional Information:				
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	(0)		Task	Severity Code		Signature
Additional Information: Edit /etc/rc.config.d/nddconf and add/set: TRANSPORT_NAME[x] = ip NDD_NAME[x] = ip_forward_src_routed NDD_VALUE[x] = 0	(9).		outing has been disabled by issuing the following	3		
(10). Task Severity Code Date Signature	Addi	tional Information:	Edit /etc/rc.config.d/nddconf and add/set: TRANSPORT_NAME[x] = ip NDD_NAME[x] = ip_forward_src_routed			
	(10).		Task	Severity Code	Date	Signature

		Completed		
Ensure that the system is protected from 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+, b Edit /etc/rc.config.d/nddconf and add/set: TRANSPORT_NAME[x]=tcp NDD_NAME[x]=tcp_syn_rcvd_max NDD_VALUE[x]=500	ased on availa	ble memory>	