TEST REPORT SEAPATH DEBIAN

Receiver: SEAPATH

Contact: <seapath@savoirfairelinux>

10 March 2025, 08:12:47 UTC

Table of Contents

Test reports

Tests common for vmtest12

Test ID	Tests	Results
SEAPATH-00078	no paging error	PASS
SEAPATH-00079	no rcu stall	PASS
SEAPATH-00080	no backtraces	PASS
SEAPATH-00075	kernel is PREEMPT RT	PASS
SEAPATH-00076	kernel is realtime	PASS
SEAPATH-00081	kernel is >= 4.19.106	PASS
SEAPATH-00083	syslog-ng service is running	PASS
SEAPATH-00084	syslog-ng is configured to send log on network	PASS

- number of tests: 8
- number of failures: 0

Tests common security for vmtest12

Test ID	Tests	Results
SEAPATH-00198	No unrecognized packages installed	PASS
SEAPATH-00215	auditd service is active	PASS
SEAPATH-00216	auditd is configured to output in syslog	PASS
SEAPATH-00217	insmod call is logged	PASS
SEAPATH-00217	kmod call is logged	PASS
SEAPATH-00217	modprobe call is logged	PASS
SEAPATH-00217	rmmod call is logged	PASS
SEAPATH-00218	modification in /etc/ is logged	PASS
SEAPATH-00219	mount/umount call is logged	PASS
SEAPATH-00220	ioperm call is logged	PASS
SEAPATH-00220	prctl call is logged	PASS
SEAPATH-00220	ptrace call is logged	PASS
SEAPATH-00221	file deletion is logged	PASS
SEAPATH-00222	open monitoring is logged	PASS
SEAPATH-00222	openat monitoring is logged	PASS
SEAPATH-00222	unlink monitoring is logged	PASS
SEAPATH-00106	Check /etc/shadow permissions	PASS
SEAPATH-00107	Check /etc/passwd permissions	PASS
SEAPATH-00108	Check /etc/syslog-ng/cert.d/clientkey.pem permissions	PASS
SEAPATH-00049	Check /etc/ssh/ssh_host_ed25519_key permissions	PASS
SEAPATH-00090	Check /etc/ssh/ssh_host_rsa_key permissions	PASS

Test ID	Tests	Results
SEAPATH-00192	All files have a known owner and group	PASS
SEAPATH-00193	All directories writable by all users have the sticky bit	PASS
SEAPATH-00194	All directories writable by all users are owned by root	PASS
SEAPATH-00195	Ceph OSD are owned by ceph	PASS
SEAPATH-00196	No unexpected file has setuid/setgid enabled	PASS
SEAPATH-00088	root password was randomized at boot	PASS
SEAPATH-00089	root password is randomized at each boot	PASS
SEAPATH-00091	root password is encrypted with a cryto at least equivalent as sha512	PASS
SEAPATH-00092	bash timeout is set read-only to 300s	PASS
SEAPATH-00093	sshd forbids setting environment variables	PASS
SEAPATH-00094	sshd server time-out is set to 300s of client inactivity	PASS
SEAPATH-00095	shadow encrypts passwords with SHA512 by default	PASS
SEAPATH-00096	shadow encryption uses at least 65536 rounds	PASS
SEAPATH-00097	pam password authentication uses sha512 with 65536 rounds or yescrypt	PASS
SEAPATH-00098	password set to expire after 90 days	PASS
SEAPATH-00099	'su' is denied	PASS
SEAPATH-00100	/etc/securetty is empty	PASS
SEAPATH-00101	PAM securetty module is active in 'login' policy	PASS
SEAPATH-00202	grub root superuser is set in /boot/grub/grub.cfg	PASS
SEAPATH-00203	grub root superuser is password protected	PASS
SEAPATH-00204	main menuentry is unrestricted in /boot/grub/grub.cfg	PASS
SEAPATH-00205	TMPDIR env var is defined and readonly	PASS
SEAPATH-00206	TMPDIR is set with 700 mode and root as owner and group	PASS
SEAPATH-00225	Umask is set correctly set	PASS
SEAPATH-00227	AppArmor processes are confined in enforce mode	PASS
SEAPATH-00050	Linux kernel 'hardening' : SECURITY_YAMA is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : DEBUG_WX is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : SECURITY_DMESG_RESTRICT is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : LEGACY_VSYSCALL_NONE is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : SLAB_FREELIST_RANDOM is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : SLAB_FREELIST_HARDENED is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : HARDENED_USERCOPY is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : FORTIFY_SOURCE is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : PAGE_POISONING is enabled	PASS
SEAPATH-00170	Wipe slab and page allocations enabled on cmdline	PASS
SEAPATH-00174	Randomize kstack offset in on	PASS
SEAPATH-00175	Disable slab usercopy fallback	PASS
SEAPATH-00201	LSM Yama is enabled	PASS
SEAPATH-00210	MCE is disabled	PASS
SEAPATH-00211	rng_core.default_quality is set to 500	PASS

Test ID	Tests	Results
SEAPATH-00226	Test AppArmor is enabled	PASS
SEAPATH-00223	All sockets are bound to an interface	PASS
SEAPATH-00224	IPv6 is disabled	PASS
SEAPATH-00164	sudo requires password for group operator (operator)	PASS
SEAPATH-00165	sudo requires password for group maintenance-N1 (maint-n1)	PASS
SEAPATH-00166	sudo requires password for group maintenance-N3 (maint-n3)	PASS
SEAPATH-00167	sudo requires password for group administrator (admincluster)	PASS
SEAPATH-00168	sudo requires password for group super-administrator (adminsys)	PASS
SEAPATH-00103	/usr/bin/sudo exists	PASS
SEAPATH-00104	/usr/bin/sudo belongs to group privileged	PASS
SEAPATH-00105	/usr/bin/sudo has permissions 4750	PASS
SEAPATH-00148	sudoers files include directive noexec	PASS
SEAPATH-00148	sudoers files include directive requiretty	PASS
SEAPATH-00148	sudoers files include directive use_pty	PASS
SEAPATH-00148	sudoers files include directive umask=0027	PASS
SEAPATH-00148	sudoers files include directive ignore_dot	PASS
SEAPATH-00148	sudoers files include directive env_reset	PASS
SEAPATH-00149	sudo commands don’t target privileged user	PASS
SEAPATH-00150	all commands require authentication	PASS
SEAPATH-00152	EXEC option is not used	PASS
SEAPATH-00153	rules are not defined by negation	PASS
SEAPATH-00154	sudo commands always specify arguments	PASS
SEAPATH-00154	no user can run all commands as root	PASS
SEAPATH-00155	sudo commands don’t use wildcard * argument	PASS
SEAPATH-00156	/etc/sudoers - /etc/sudoers is owned by root:root with 0440 permissions	PASS
SEAPATH-00156	/etc/sudoers.d/admin - /etc/sudoers.d/admin is owned by root:root with 0440 permissions	PASS
SEAPATH-00156	/etc/sudoers.d/00-security - /etc/sudoers.d/00-security is owned by root:root with 0440 permissions	PASS
SEAPATH-00171	Check coredumps are disabled	PASS
SEAPATH-00172	Check kexec is disabled	PASS
SEAPATH-00173	Check binfmt_misc is disabled	PASS
SEAPATH-00176	Check kptr_restrict is set to 2	PASS
SEAPATH-00177	Check dmesg_restrict is set to 1	PASS
SEAPATH-00178	Check pid_max is set to 4194304	PASS
SEAPATH-00179	Check perf_cpu_time_max_percent is set to 1	PASS
SEAPATH-00180	Check perf_event_max_sample_rate is set to 1	PASS
SEAPATH-00181	Check perf_event_paranoid is set to 2	PASS
SEAPATH-00182	Check randomize_va_space is set to 2	PASS
SEAPATH-00183	Check sysrq is set to 0	PASS
SEAPATH-00184	Check unprivileged_bpf_disabled is set to 1	PASS

Test ID	Tests	Results
SEAPATH-00185	Check panic_on_oops is set to 1	PASS
SEAPATH-00186	Check kernel.yama.ptrace_scope is set to 2	PASS
SEAPATH-00187	Check suid_dumpable is set to 0	PASS
SEAPATH-00188	Check protected_fifos is set to 2	PASS
SEAPATH-00189	Check protected_regular is set to 2	PASS
SEAPATH-00190	Check protected_symlinks is set to 1	PASS
SEAPATH-00191	Check protected_hardlinks is set to 1	PASS
SEAPATH-00082	/var/log is mounted on a separate partition	PASS
SEAPATH-00085	syslog-ng can not acquire new privileges	PASS
SEAPATH-00086	syslog-ng capabilities are bounded	PASS
SEAPATH-00087	syslog-ng system calls are filtered	PASS
SEAPATH-00199	No systemd service failed	PASS
SEAPATH-00200	No unrecognized service enabled	PASS

- number of tests: 112
- number of failures: 0

Tests common for vmtest12s

Test ID	Tests	Results
SEAPATH-00078	no paging error	PASS
SEAPATH-00079	no rcu stall	PASS
SEAPATH-00080	no backtraces	PASS
SEAPATH-00075	kernel is PREEMPT RT	PASS
SEAPATH-00076	kernel is realtime	PASS
SEAPATH-00081	kernel is >= 4.19.106	PASS
SEAPATH-00083	syslog-ng service is running	PASS
SEAPATH-00084	syslog-ng is configured to send log on network	PASS

- number of tests: 8
- number of failures: 0

Tests common security for vmtest12s

Test ID	Tests	Results
SEAPATH-00198	No unrecognized packages installed	PASS
SEAPATH-00215	auditd service is active	PASS
SEAPATH-00216	auditd is configured to output in syslog	PASS
SEAPATH-00217	insmod call is logged	PASS
SEAPATH-00217	kmod call is logged	PASS
SEAPATH-00217	modprobe call is logged	PASS

Test ID	Tests	Results
SEAPATH-00217	rmmod call is logged	PASS
SEAPATH-00218	modification in /etc/ is logged	PASS
SEAPATH-00219	mount/umount call is logged	PASS
SEAPATH-00220	ioperm call is logged	PASS
SEAPATH-00220	prctl call is logged	PASS
SEAPATH-00220	ptrace call is logged	PASS
SEAPATH-00221	file deletion is logged	PASS
SEAPATH-00222	open monitoring is logged	PASS
SEAPATH-00222	openat monitoring is logged	PASS
SEAPATH-00222	unlink monitoring is logged	PASS
SEAPATH-00106	Check /etc/shadow permissions	PASS
SEAPATH-00107	Check /etc/passwd permissions	PASS
SEAPATH-00108	Check /etc/syslog-ng/cert.d/clientkey.pem permissions	PASS
SEAPATH-00049	Check /etc/ssh/ssh_host_ed25519_key permissions	PASS
SEAPATH-00090	Check /etc/ssh/ssh_host_rsa_key permissions	PASS
SEAPATH-00192	All files have a known owner and group	PASS
SEAPATH-00193	All directories writable by all users have the sticky bit	PASS
SEAPATH-00194	All directories writable by all users are owned by root	PASS
SEAPATH-00195	Ceph OSD are owned by ceph	PASS
SEAPATH-00196	No unexpected file has setuid/setgid enabled	PASS
SEAPATH-00088	root password was randomized at boot	PASS
SEAPATH-00089	root password is randomized at each boot	PASS
SEAPATH-00091	root password is encrypted with a cryto at least equivalent as sha512	PASS
SEAPATH-00092	bash timeout is set read-only to 300s	PASS
SEAPATH-00093	sshd forbids setting environment variables	PASS
SEAPATH-00094	sshd server time-out is set to 300s of client inactivity	PASS
SEAPATH-00095	shadow encrypts passwords with SHA512 by default	PASS
SEAPATH-00096	shadow encryption uses at least 65536 rounds	PASS
SEAPATH-00097	pam password authentication uses sha512 with 65536 rounds or yescrypt	PASS
SEAPATH-00098	password set to expire after 90 days	PASS
SEAPATH-00099	'su' is denied	PASS
SEAPATH-00100	/etc/securetty is empty	PASS
SEAPATH-00101	PAM securetty module is active in 'login' policy	PASS
SEAPATH-00202	grub root superuser is set in /boot/grub/grub.cfg	PASS
SEAPATH-00203	grub root superuser is password protected	PASS
SEAPATH-00204	main menuentry is unrestricted in /boot/grub/grub.cfg	PASS
SEAPATH-00205	TMPDIR env var is defined and readonly	PASS
SEAPATH-00206	TMPDIR is set with 700 mode and root as owner and group	PASS
SEAPATH-00225	Umask is set correctly set	PASS
SEAPATH-00227	AppArmor processes are confined in enforce mode	PASS

Test ID	Tests	Results
SEAPATH-00050	Linux kernel 'hardening' : SECURITY_YAMA is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : DEBUG_WX is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : SECURITY_DMESG_RESTRICT is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : LEGACY_VSYSCALL_NONE is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : SLAB_FREELIST_RANDOM is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : SLAB_FREELIST_HARDENED is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : HARDENED_USERCOPY is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : FORTIFY_SOURCE is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : PAGE_POISONING is enabled	PASS
SEAPATH-00170	Wipe slab and page allocations enabled on cmdline	PASS
SEAPATH-00174	Randomize kstack offset in on	PASS
SEAPATH-00175	Disable slab usercopy fallback	PASS
SEAPATH-00201	LSM Yama is enabled	PASS
SEAPATH-00210	MCE is disabled	PASS
SEAPATH-00211	rng_core.default_quality is set to 500	PASS
SEAPATH-00226	Test AppArmor is enabled	PASS
SEAPATH-00223	All sockets are bound to an interface	PASS
SEAPATH-00224	IPv6 is disabled	PASS
SEAPATH-00164	sudo requires password for group operator (operator)	PASS
SEAPATH-00165	sudo requires password for group maintenance-N1 (maint-n1)	PASS
SEAPATH-00166	sudo requires password for group maintenance-N3 (maint-n3)	PASS
SEAPATH-00167	sudo requires password for group administrator (admincluster)	PASS
SEAPATH-00168	sudo requires password for group super-administrator (adminsys)	PASS
SEAPATH-00103	/usr/bin/sudo exists	PASS
SEAPATH-00104	/usr/bin/sudo belongs to group privileged	PASS
SEAPATH-00105	/usr/bin/sudo has permissions 4750	PASS
SEAPATH-00148	sudoers files include directive noexec	PASS
SEAPATH-00148	sudoers files include directive requiretty	PASS
SEAPATH-00148	sudoers files include directive use_pty	PASS
SEAPATH-00148	sudoers files include directive umask=0027	PASS
SEAPATH-00148	sudoers files include directive ignore_dot	PASS
SEAPATH-00148	sudoers files include directive env_reset	PASS
SEAPATH-00149	sudo commands don’t target privileged user	PASS
SEAPATH-00150	all commands require authentication	PASS
SEAPATH-00152	EXEC option is not used	PASS
SEAPATH-00153	rules are not defined by negation	PASS
SEAPATH-00154	sudo commands always specify arguments	PASS
SEAPATH-00154	no user can run all commands as root	PASS
SEAPATH-00155	sudo commands don’t use wildcard * argument	PASS
SEAPATH-00156	/etc/sudoers - /etc/sudoers is owned by root:root with 0440 permissions	PASS

Test ID	Tests	Results
SEAPATH-00156	/etc/sudoers.d/admin - /etc/sudoers.d/admin is owned by root:root with 0440 permissions	PASS
SEAPATH-00156	/etc/sudoers.d/00-security - /etc/sudoers.d/00-security is owned by root:root with 0440 permissions	PASS
SEAPATH-00171	Check coredumps are disabled	PASS
SEAPATH-00172	Check kexec is disabled	PASS
SEAPATH-00173	Check binfmt_misc is disabled	PASS
SEAPATH-00176	Check kptr_restrict is set to 2	PASS
SEAPATH-00177	Check dmesg_restrict is set to 1	PASS
SEAPATH-00178	Check pid_max is set to 4194304	PASS
SEAPATH-00179	Check perf_cpu_time_max_percent is set to 1	PASS
SEAPATH-00180	Check perf_event_max_sample_rate is set to 1	PASS
SEAPATH-00181	Check perf_event_paranoid is set to 2	PASS
SEAPATH-00182	Check randomize_va_space is set to 2	PASS
SEAPATH-00183	Check sysrq is set to 0	PASS
SEAPATH-00184	Check unprivileged_bpf_disabled is set to 1	PASS
SEAPATH-00185	Check panic_on_oops is set to 1	PASS
SEAPATH-00186	Check kernel.yama.ptrace_scope is set to 2	PASS
SEAPATH-00187	Check suid_dumpable is set to 0	PASS
SEAPATH-00188	Check protected_fifos is set to 2	PASS
SEAPATH-00189	Check protected_regular is set to 2	PASS
SEAPATH-00190	Check protected_symlinks is set to 1	PASS
SEAPATH-00191	Check protected_hardlinks is set to 1	PASS
SEAPATH-00082	/var/log is mounted on a separate partition	PASS
SEAPATH-00085	syslog-ng can not acquire new privileges	PASS
SEAPATH-00086	syslog-ng capabilities are bounded	PASS
SEAPATH-00087	syslog-ng system calls are filtered	PASS
SEAPATH-00199	No systemd service failed	PASS
SEAPATH-00200	No unrecognized service enabled	PASS

- number of tests: 112
- number of failures: 0

Tests common for vmtest12rt

Test ID	Tests	Results
SEAPATH-00078	no paging error	PASS
SEAPATH-00079	no rcu stall	PASS
SEAPATH-00080	no backtraces	PASS
SEAPATH-00075	kernel is PREEMPT RT	PASS
SEAPATH-00076	kernel is realtime	PASS

Test ID	Tests	Results
SEAPATH-00081	kernel is >= 4.19.106	PASS
SEAPATH-00083	syslog-ng service is running	PASS
SEAPATH-00084	syslog-ng is configured to send log on network	PASS

- number of tests: 8
- number of failures: 0

Tests common security for vmtest12rt

Test ID	Tests	Results
SEAPATH-00198	No unrecognized packages installed	PASS
SEAPATH-00215	auditd service is active	PASS
SEAPATH-00216	auditd is configured to output in syslog	PASS
SEAPATH-00217	insmod call is logged	PASS
SEAPATH-00217	kmod call is logged	PASS
SEAPATH-00217	modprobe call is logged	PASS
SEAPATH-00217	rmmod call is logged	PASS
SEAPATH-00218	modification in /etc/ is logged	PASS
SEAPATH-00219	mount/umount call is logged	PASS
SEAPATH-00220	ioperm call is logged	PASS
SEAPATH-00220	prctl call is logged	PASS
SEAPATH-00220	ptrace call is logged	PASS
SEAPATH-00221	file deletion is logged	PASS
SEAPATH-00222	open monitoring is logged	PASS
SEAPATH-00222	openat monitoring is logged	PASS
SEAPATH-00222	unlink monitoring is logged	PASS
SEAPATH-00106	Check /etc/shadow permissions	PASS
SEAPATH-00107	Check /etc/passwd permissions	PASS
SEAPATH-00108	Check /etc/syslog-ng/cert.d/clientkey.pem permissions	PASS
SEAPATH-00049	Check /etc/ssh/ssh_host_ed25519_key permissions	PASS
SEAPATH-00090	Check /etc/ssh/ssh_host_rsa_key permissions	PASS
SEAPATH-00192	All files have a known owner and group	PASS
SEAPATH-00193	All directories writable by all users have the sticky bit	PASS
SEAPATH-00194	All directories writable by all users are owned by root	PASS
SEAPATH-00195	Ceph OSD are owned by ceph	PASS
SEAPATH-00196	No unexpected file has setuid/setgid enabled	PASS
SEAPATH-00088	root password was randomized at boot	PASS
SEAPATH-00089	root password is randomized at each boot	PASS
SEAPATH-00091	root password is encrypted with a cryto at least equivalent as sha512	PASS
SEAPATH-00092	bash timeout is set read-only to 300s	PASS
SEAPATH-00093	sshd forbids setting environment variables	PASS

Test ID	Tests	Results
SEAPATH-00094	sshd server time-out is set to 300s of client inactivity	PASS
SEAPATH-00095	shadow encrypts passwords with SHA512 by default	PASS
SEAPATH-00096	shadow encryption uses at least 65536 rounds	PASS
SEAPATH-00097	pam password authentication uses sha512 with 65536 rounds or yescrypt	PASS
SEAPATH-00098	password set to expire after 90 days	PASS
SEAPATH-00099	'su' is denied	PASS
SEAPATH-00100	/etc/securetty is empty	PASS
SEAPATH-00101	PAM securetty module is active in 'login' policy	PASS
SEAPATH-00202	grub root superuser is set in /boot/grub/grub.cfg	PASS
SEAPATH-00203	grub root superuser is password protected	PASS
SEAPATH-00204	main menuentry is unrestricted in /boot/grub/grub.cfg	PASS
SEAPATH-00205	TMPDIR env var is defined and readonly	PASS
SEAPATH-00206	TMPDIR is set with 700 mode and root as owner and group	PASS
SEAPATH-00225	Umask is set correctly set	PASS
SEAPATH-00227	AppArmor processes are confined in enforce mode	PASS
SEAPATH-00050	Linux kernel 'hardening' : SECURITY_YAMA is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : DEBUG_WX is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : SECURITY_DMESG_RESTRICT is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : LEGACY_VSYSCALL_NONE is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : SLAB_FREELIST_RANDOM is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : SLAB_FREELIST_HARDENED is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : HARDENED_USERCOPY is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : FORTIFY_SOURCE is enabled	PASS
SEAPATH-00050	Linux kernel 'hardening' : PAGE_POISONING is enabled	PASS
SEAPATH-00170	Wipe slab and page allocations enabled on cmdline	PASS
SEAPATH-00174	Randomize kstack offset in on	PASS
SEAPATH-00175	Disable slab usercopy fallback	PASS
SEAPATH-00201	LSM Yama is enabled	PASS
SEAPATH-00210	MCE is disabled	PASS
SEAPATH-00211	rng_core.default_quality is set to 500	PASS
SEAPATH-00226	Test AppArmor is enabled	PASS
SEAPATH-00223	All sockets are bound to an interface	PASS
SEAPATH-00224	IPv6 is disabled	PASS
SEAPATH-00164	sudo requires password for group operator (operator)	PASS
SEAPATH-00165	sudo requires password for group maintenance-N1 (maint-n1)	PASS
SEAPATH-00166	sudo requires password for group maintenance-N3 (maint-n3)	PASS
SEAPATH-00167	sudo requires password for group administrator (admincluster)	PASS
SEAPATH-00168	sudo requires password for group super-administrator (adminsys)	PASS
SEAPATH-00103	/usr/bin/sudo exists	PASS
SEAPATH-00104	/usr/bin/sudo belongs to group privileged	PASS

Test ID	Tests	Results
SEAPATH-00105	/usr/bin/sudo has permissions 4750	PASS
SEAPATH-00148	sudoers files include directive noexec	PASS
SEAPATH-00148	sudoers files include directive requiretty	PASS
SEAPATH-00148	sudoers files include directive use_pty	PASS
SEAPATH-00148	sudoers files include directive umask=0027	PASS
SEAPATH-00148	sudoers files include directive ignore_dot	PASS
SEAPATH-00148	sudoers files include directive env_reset	PASS
SEAPATH-00149	sudo commands don’t target privileged user	PASS
SEAPATH-00150	all commands require authentication	PASS
SEAPATH-00152	EXEC option is not used	PASS
SEAPATH-00153	rules are not defined by negation	PASS
SEAPATH-00154	sudo commands always specify arguments	PASS
SEAPATH-00154	no user can run all commands as root	PASS
SEAPATH-00155	sudo commands don’t use wildcard * argument	PASS
SEAPATH-00156	/etc/sudoers - /etc/sudoers is owned by root:root with 0440 permissions	PASS
SEAPATH-00156	/etc/sudoers.d/00-security - /etc/sudoers.d/00-security is owned by root:root with 0440 permissions	PASS
SEAPATH-00156	/etc/sudoers.d/admin - /etc/sudoers.d/admin is owned by root:root with 0440 permissions	PASS
SEAPATH-00171	Check coredumps are disabled	PASS
SEAPATH-00172	Check kexec is disabled	PASS
SEAPATH-00173	Check binfmt_misc is disabled	PASS
SEAPATH-00176	Check kptr_restrict is set to 2	PASS
SEAPATH-00177	Check dmesg_restrict is set to 1	PASS
SEAPATH-00178	Check pid_max is set to 4194304	PASS
SEAPATH-00179	Check perf_cpu_time_max_percent is set to 1	PASS
SEAPATH-00180	Check perf_event_max_sample_rate is set to 1	PASS
SEAPATH-00181	Check perf_event_paranoid is set to 2	PASS
SEAPATH-00182	Check randomize_va_space is set to 2	PASS
SEAPATH-00183	Check sysrq is set to 0	PASS
SEAPATH-00184	Check unprivileged_bpf_disabled is set to 1	PASS
SEAPATH-00185	Check panic_on_oops is set to 1	PASS
SEAPATH-00186	Check kernel.yama.ptrace_scope is set to 2	PASS
SEAPATH-00187	Check suid_dumpable is set to 0	PASS
SEAPATH-00188	Check protected_fifos is set to 2	PASS
SEAPATH-00189	Check protected_regular is set to 2	PASS
SEAPATH-00190	Check protected_symlinks is set to 1	PASS
SEAPATH-00191	Check protected_hardlinks is set to 1	PASS
SEAPATH-00082	/var/log is mounted on a separate partition	PASS
SEAPATH-00085	syslog-ng can not acquire new privileges	PASS
SEAPATH-00086	syslog-ng capabilities are bounded	PASS

Test ID	Tests	Results
SEAPATH-00087	syslog-ng system calls are filtered	PASS
SEAPATH-00199	No systemd service failed	PASS
SEAPATH-00200	No unrecognized service enabled	PASS

- number of tests: 112
- number of failures: 0

Compliance Matrix

Matrix include/ANSSI-BP28-Recommandations-M.csv

Requirement	Test id	Status

Matrix include/ANSSI-BP28-Recommandations-MI.csv

Requirement	Test id	Status

Matrix include/ANSSI-BP28-Recommandations-MIR.csv

Requirement	Test id	Status

About this documentation

This documentation uses the AsciiDoc documentation generator. It is a convenient format that allows using plain-text formatted writing that can later be converted to various output formats such as HTML and PDF.

In order to generate an HTML version of this documentation, use the following command (the asciidoc package will need to be installed in your Linux distribution):

```
$ asciidoc test-report.adoc
```

This will result in a README.html file being generated in the current directory.

If you prefer a PDF version of the documentation instead, use the following command (the dblatex package will need to be installed on your Linux distribution):

```
$ asciidoctor-pdf test-report.adoc
```