Ransomware Assessment Summary

Risk Assessment Summary:

Risk: High - Antivirus software is not installed.

Risk: High - Last backup was done 51 days ago, which is too long.

Suspicious encrypted files detected:

- /home/vethavarshini/Desktop/2-share_decrypt.jpeg.crypted
- /home/vethavarshini/Desktop/Tiger.jpeg.crypt
- /home/vethavarshini/Desktop/2-share_encrypt.jpeg.locked

MALICIOUS FILE DETECTED:POSSIBLY A RANSOMEWARE

- /home/vethavarshini/Desktop/Ransomware-Samples-main.zip

Lynis System Information:

[+] Networking

- Checking IPv6 configuration [ENABLED]

Configuration method [AUTO]

IPv6 only [NO]

- Checking configured nameservers

- Testing nameservers

Nameserver: 8.8.8.8 [OK]

- Minimal of 2 responsive nameservers [WARNING]

- Checking default gateway [DONE]

- Getting listening ports (TCP/UDP) [SKIPPED]

- Checking promiscuous interfaces [OK]

- Checking waiting connections [OK]

- Checking status DHCP client [NOT ACTIVE]

- Checking for ARP monitoring software [NOT FOUND]

- Uncommon network protocols [0]

- Checking cups daemon [NOT FOUND]

- Checking lp daemon [NOT RUNNING]

[+] Software: firewalls

- Checking iptables kernel module [FOUND]

- Checking iptables policies of chains [FOUND]

- Checking for empty ruleset [WARNING]

- Checking for unused rules [OK]

- Checking host based firewall [ACTIVE]

- Checking Apache (binary /usr/sbin/apache2) [FOUND]

Info: Configuration file found (/etc/apache2/apache2.conf)

Info: No virtual hosts found

* Loadable modules [FOUND (118)]

- Found 118 loadable modules

mod_evasive: anti-DoS/brute force [NOT FOUND]

mod_reqtimeout/mod_qos [FOUND]

ModSecurity: web application firewall [NOT FOUND]

- Checking nginx [NOT FOUND]

- Checking running SSH daemon [NOT FOUND]

- Checking running SNMP daemon [NOT FOUND]

No database engines found

- Checking OpenLDAP instance [NOT FOUND]

- Checking PHP [FOUND]

- Checking PHP disabled functions [FOUND]

- Checking expose_php option [OFF]

- Checking enable_dl option [OFF]

- Checking allow_url_fopen option [ON]

- Checking allow_url_include option [OFF]

- Checking listen option [OK]

[+] Squid Support

- Checking running Squid daemon [NOT FOUND]

- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NOT FOUND]
- Checking systemd journal status [FOUND]
- Checking Metalog status [NOT FOUND]
- Checking RSyslog status [NOT FOUND]
- Checking RFC 3195 daemon status [NOT FOUND]
- Checking minilogd instances [NOT FOUND]
- Checking logrotate presence [OK]
- Checking remote logging [NOT ENABLED]
- Checking log directories (static list) [DONE]
- Checking open log files [DONE]
- Checking deleted files in use [FILES FOUND]

- Installed inetd package [NOT FOUND]
- Installed xinetd package [OK]
- xinetd status [NOT ACTIVE]
- Installed rsh client package [OK]
- Installed rsh server package [OK]
- Installed telnet client package [OK]
- Installed telnet server package [NOT FOUND]
- Checking NIS client installation [OK]
- Checking NIS server installation [OK]

- Checking TFTP client installation [SUGGESTION]

- Checking TFTP server installation [SUGGESTION]

- /etc/issue [FOUND]

- /etc/issue contents [WEAK]

- /etc/issue.net [FOUND]

- /etc/issue.net contents [WEAK]

[+] Scheduled tasks

- Checking crontab and cronjob files [DONE]

[+] Accounting

- Checking accounting information [NOT FOUND]

- Checking sysstat accounting data [DISABLED]

- Checking auditd [NOT FOUND]

[+] Time and Synchronization

[+] Cryptography

- Checking for expired SSL certificates [0/149] [NONE]

[WARNING]: Test CRYP-7902 had a long execution: 49.213564 seconds

- Found 0 encrypted and 1 unencrypted swap devices in use. [OK]

- Kernel entropy is sufficient [YES]

- HW RNG & rngd [NO]

- SW prng [YES]

- MOR variable not found [WEAK]

[+] Virtualization

[+] Containers

[+] Security frameworks

- Checking presence AppArmor [FOUND]

- Checking AppArmor status [DISABLED]

- Checking presence SELinux [NOT FOUND]

- Checking presence TOMOYO Linux [NOT FOUND]

- Checking presence grsecurity [NOT FOUND]

- Checking for implemented MAC framework [NONE]

[+] Software: file integrity

- Checking file integrity tools

- Tripwire [FOUND]

- dm-integrity (status) [DISABLED]

- dm-verity (status) [DISABLED]

- Checking presence integrity tool [FOUND]

[+] Software: System tooling

- Checking automation tooling

- Automation tooling [NOT FOUND]

- Checking for IDS/IPS tooling [NONE]

[+] Software: Malware

- Checking ClamAV scanner [FOUND]

- Malware software components [FOUND]

- Active agent [NOT FOUND]

- Rootkit scanner [NOT FOUND]

[+] File Permissions

- Starting file permissions check

File: /boot/grub/grub.cfg [OK]

File: /etc/crontab [SUGGESTION]

File: /etc/group [OK]

File: /etc/group- [OK]

File: /etc/hosts.allow [OK]

File: /etc/hosts.deny [OK]

File: /etc/issue [OK]

File: /etc/issue.net [OK]

File: /etc/motd [OK]

File: /etc/passwd [OK]

File: /etc/passwd- [OK]

File: /etc/ssh/sshd_config [SUGGESTION]

Directory: /root/.ssh [OK]

Directory: /etc/cron.d [SUGGESTION]

Directory: /etc/cron.daily [SUGGESTION]

Directory: /etc/cron.hourly [SUGGESTION]

Directory: /etc/cron.weekly [SUGGESTION]

Directory: /etc/cron.monthly [SUGGESTION]

[+] Home directories

- Permissions of home directories [WARNING]

- Ownership of home directories [OK]

- Checking shell history files [OK]

[+] Kernel Hardening

- Comparing sysctl key pairs with scan profile

- dev.tty.ldisc_autoload (exp: 0) [DIFFERENT]

- fs.protected_fifos (exp: 2) [DIFFERENT]

- fs.protected_hardlinks (exp: 1) [OK]

- fs.protected_regular (exp: 2) [OK]
- fs.protected_symlinks (exp: 1) [OK]
- fs.suid_dumpable (exp: 0) [OK]
- kernel.core_uses_pid (exp: 1) [OK]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.dmesg_restrict (exp: 1) [DIFFERENT]
- kernel.kptr_restrict (exp: 2) [DIFFERENT]
- kernel.modules_disabled (exp: 1) [DIFFERENT]
- kernel.perf_event_paranoid (exp: 3) [OK]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFFERENT]
- kernel.unprivileged_bpf_disabled (exp: 1) [DIFFERENT]
- kernel.yama.ptrace_scope (exp: 1 2 3) [DIFFERENT]
- net.core.bpf_jit_harden (exp: 2) [DIFFERENT]
- net.ipv4.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv4.conf.all.bootp_relay (exp: 0) [OK]
- net.ipv4.conf.all.forwarding (exp: 0) [OK]
- net.ipv4.conf.all.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [OK]
- net.ipv4.conf.all.proxy_arp (exp: 0) [OK]
- net.ipv4.conf.all.rp_filter (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_source_route (exp: 0) [OK]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFFERENT]

- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [OK]

- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]

- net.ipv4.tcp_syncookies (exp: 1) [OK]

- net.ipv4.tcp_timestamps (exp: 0 1) [OK]

- net.ipv6.conf.all.accept_redirects (exp: 0) [DIFFERENT]

- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]

- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFFERENT]

- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]

[+] Hardening

- Installed compiler(s) [FOUND]

- Installed malware scanner [FOUND]

- Non-native binary formats [FOUND]

[+] Custom tests

- Running custom tests... [NONE]

==========

====

! Couldn't find 2 responsive nameservers [NETW-2705]

https://cisofy.com/lynis/controls/NETW-2705/

! iptables module(s) loaded, but no rules active [FIRE-4512]

https://cisofy.com/lynis/controls/FIRE-4512/

Suggestions (46):

---

* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]

https://cisofy.com/lynis/controls/LYNIS/

* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]

https://cisofy.com/lynis/controls/DEB-0280/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]

https://cisofy.com/lynis/controls/DEB-0810/

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]

https://cisofy.com/lynis/controls/DEB-0811/

* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]

https://cisofy.com/lynis/controls/DEB-0831/

* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]

https://cisofy.com/lynis/controls/DEB-0880/

* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

https://cisofy.com/lynis/controls/BOOT-5122/

* Consider hardening system services [BOOT-5264]

- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service

https://cisofy.com/lynis/controls/BOOT-5264/

* Configure password hashing rounds in /etc/login.defs [AUTH-9230]

https://cisofy.com/lynis/controls/AUTH-9230/

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]

https://cisofy.com/lynis/controls/AUTH-9262/

* When possible set expire dates for all password protected accounts [AUTH-9282]

https://cisofy.com/lynis/controls/AUTH-9282/

* Configure minimum password age in /etc/login.defs [AUTH-9286]

https://cisofy.com/lynis/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]

https://cisofy.com/lynis/controls/AUTH-9286/

* Default umask in /etc/login.defs could not be found and defaults usually to 022, which could be more strict like 027 [AUTH-9328]

https://cisofy.com/lynis/controls/AUTH-9328/

* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]

https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]

https://cisofy.com/lynis/controls/FILE-6310/

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]

https://cisofy.com/lynis/controls/USB-1000/

* Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]

https://cisofy.com/lynis/controls/STRG-1846/

* Check DNS configuration for the dns domain name [NAME-4028]

https://cisofy.com/lynis/controls/NAME-4028/

* Check RPM database as RPM binary available but does not reveal any packages [PKGS-7308]

https://cisofy.com/lynis/controls/PKGS-7308/

* Purge old/removed packages (4 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]

https://cisofy.com/lynis/controls/PKGS-7346/

* Install debsums utility for the verification of packages with known good database. [PKGS-7370]

https://cisofy.com/lynis/controls/PKGS-7370/

* Install package apt-show-versions for patch management purposes [PKGS-7394]

https://cisofy.com/lynis/controls/PKGS-7394/

* Consider using a tool to automatically apply upgrades [PKGS-7420]

https://cisofy.com/lynis/controls/PKGS-7420/

* Check your resolv.conf file and fill in a backup nameserver if possible [NETW-2705]

https://cisofy.com/lynis/controls/NETW-2705/

* Determine if protocol 'dccp' is really needed on this system [NETW-3200]

https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'sctp' is really needed on this system [NETW-3200]

https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'rds' is really needed on this system [NETW-3200]

https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'tipc' is really needed on this system [NETW-3200]

https://cisofy.com/lynis/controls/NETW-3200/

* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]

https://cisofy.com/lynis/controls/HTTP-6640/

* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]

https://cisofy.com/lynis/controls/HTTP-6643/

* Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via PHP [PHP-2376]

https://cisofy.com/lynis/controls/PHP-2376/

* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]

https://cisofy.com/lynis/controls/LOGG-2154/

* Check what deleted files are still in use and why. [LOGG-2190]

https://cisofy.com/lynis/controls/LOGG-2190/

* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-8318]

https://cisofy.com/lynis/controls/INSE-8318/

* Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [INSE-8320]

https://cisofy.com/lynis/controls/INSE-8320/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]

https://cisofy.com/lynis/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

https://cisofy.com/lynis/controls/BANN-7130/

* Enable process accounting [ACCT-9622]

https://cisofy.com/lynis/controls/ACCT-9622/

* Enable sysstat to collect accounting (disabled) [ACCT-9626]

https://cisofy.com/lynis/controls/ACCT-9626/

* Enable auditd to collect audit information [ACCT-9628]

https://cisofy.com/lynis/controls/ACCT-9628/

* Determine if automation tools are present for system management [TOOL-5002]

https://cisofy.com/lynis/controls/TOOL-5002/

* Consider restricting file permissions [FILE-7524]

- Details : See screen output or log file
- Solution : Use chmod to change file permissions

https://cisofy.com/lynis/controls/FILE-7524/

* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]

https://cisofy.com/lynis/controls/HOME-9304/

* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]

- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)

https://cisofy.com/lynis/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HRDN-7222]

https://cisofy.com/lynis/controls/HRDN-7222/

Follow-up:

- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

==

Lynis security scan details:

Hardening index : 64 [#############   ]

Tests performed : 268

Plugins enabled : 1

Components:

Components:

- Firewall [V]

- Firewall [V]

- Malware scanner [V]

- Malware scanner [V]

Scan mode:

Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:

- Compliance status [?]

- Security audit [V]

- Vulnerability scan [V]

Files:

- Test and debug information : /var/log/lynis.log

- Report data : /var/log/lynis-report.dat

==

Lynis 3.1.1

Auditing, system hardening, and compliance for UNIX-based systems

(Linux, macOS, BSD, and others)

Enterprise support available (compliance, plugins, interface and tools)

==

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)