lynis Asset Report

created by lynis_report

lynis info	host info	network info	security Info	boot info	kernel info
filesystem/journalling info	service info	installed packages			

host findings:

hardening index: 67 Auditor: [Not Specified]

warnings (4):

Test ID	Description	Details	Solution
FIRE-4512	iptables module(s) loaded, but no rules active	NA	-

suggestions (34):

Test ID	Description	Details	Solution
ACCT-9622	Enable process accounting	-	-
ACCT-9626	Enable sysstat to collect accounting (no results)	-	-
ACCT-9628	Enable auditd to collect audit information	-	-
AUTH-9230	Configure password hashing rounds in /etc/login.defs	-	-
AUTH-9282	When possible set expire dates for all password protected accounts	-	-
AUTH-9286	Configure maximum password age in /etc/login.defs	-	-
AUTH-9286	Configure minimum password age in /etc/login.defs	-	-
AUTH-9328	Default umask in /etc/login.defs could be more strict like 027	-	-
BANN-7126	Add a legal banner to /etc/issue, to warn unauthorized users	-	-
BANN-7130	Add legal banner to /etc/issue.net, to warn unauthorized users	-	-
BOOT-5122	Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password)	-	-
BOOT-5264	Consider hardening system services	Run '/usr/bin/systemd-analyze security SERVICE' for each service	-
FILE-6310		-	-

	To decrease the impact of a full /home file system, place /home on a separate partition		
FILE-6310	To decrease the impact of a full /tmp file system, place /tmp on a separate partition	-	-
FILE-6310	To decrease the impact of a full /var file system, place /var on a separate partition	-	-
FILE-7524	Consider restricting file permissions	See screen output or log file	text:Use chmod to change file permissions
FINT-4350	Install a file integrity tool to monitor changes to critical and sensitive files	-	-
HRDN-7222	Harden compilers like restricting access to root user only	-	-
HRDN-7230	Harden the system by installing at least one malware scanner, to perform periodic file system scans	-	Install a tool like rkhunter, chkrootkit, OSSEC
KRNL-5820	If not required, consider explicit disabling of core dump in /etc/security/limits.conf file	-	-
KRNL-6000	One or more sysctl values differ from the scan profile and could be tweaked		Change sysctl value or disable test (skip-test=KRNL-6000:)
LOGG-2154	Enable logging to an external logging host for archiving purposes and additional protection	-	-
LOGG-2190	Check what deleted files are still in use and why.	-	-
NAME-4028	Check DNS configuration for the dns domain name	-	-
NETW-3200	Determine if protocol 'dccp' is really needed on this system	-	-
NETW-3200	Determine if protocol 'rds' is really needed on this system	-	-
NETW-3200	Determine if protocol 'sctp' is really needed on this system	-	-
NETW-3200	Determine if protocol 'tipc' is really needed on this system	-	-
PKGS-7346	Purge old/removed packages (3 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts.	-	-
PKGS-7370	Install debsums utility for the verification of packages with	-	-

	known good database.		
PKGS-7394	Install package apt-show-versions for patch management purposes	-	-
PRNT-2307	Access to CUPS configuration could be more strict.	-	-
TOOL-5002	Determine if automation tools are present for system management	-	-
USB-1000	Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft	-	-

manual checks:

- Make sure an explicit deny all is the default policy for all unmatched traffic
- Verify all traffic is filtered the right way between the different security zones
- Verify if a list is available with all required services
- Verify if there is a formal process for testing and applying firewall rules

deleted files (647):

lynis info:

lynis version:	3.0.8	lynis tests done:	263
lynis update available:	false	license key:	
report version:		1.0	
test category:	all	test group:	all
number of plugins enabled:	1	plugin directory:	./plugins
phase 1 plugins enabled:	name: pam version: 1.0.5 name: systemd version: 1.0.4		
report start time:	2022-08-03 14:15:12	report end time:	2022-08-03 14:16:11
hostid:	0ac128493b4005a8705959d8815c1c561b8aa341		
hostid:			

Plugin-processes: discovered processes:

host info:

hostname:	mike	domainname:		resolv.conf domain:	
os:	Linux	os fullname:	Ubuntu 22.04 LTS	os_version:	22.04
GRSecurity:	false	SELinux:	false	memory:	16298104 kB
linux version:	Ubuntu	pae enabled:	true	nx enabled:	true
Available shells:		locate db:		uptime (days):	5

	/bin/sh /bin/bash /usr/bin/bash /bin/rbash /usr/bin/rbash /usr/bin/sh /bin/dash /usr/bin/dash /usr/bin/tmux				
vm:	host	vm_type:		uptime (secs):	442396
is notebook/laptop:	false	is Docker container:	false		
binary paths:	/snap/bin,/usr/bin,/usr/sbin,/usr/local/bin,/usr/local/sbin	valid certificates:			
authorized default USB devices:	/sys/bus/usb/devices/usb3 /sys/bus/usb/devices/usb1 /sys/bus/usb/devices/usb4 /sys/bus/usb/devices/usb2	expired certificates:			
certificate count:	0	certificates:	/etc/ssl/certs/ca-certificates.crt|0|cn:subject= = ACCVRAIZ1, OU = PKIACCV, O = ACCV, C = ES;notafter:Dec 31 09:37:37 2030 GMT;| /etc/ssl/certs/ssl-cert-snakeoil.pem|0|cn:sub = ubuntu;notafter:Jul 11 06:53:57 2032 GMT;| /usr/local/share/ca-certificates/certificate.cr = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FG201ETK19903375, emailAddress = support@fortinet.com;notafter:Jun 27 09:32:36 2029 GMT;|		
world executable compiler(s):					

cron jobs:

logging info:

log rotation tool:	logrotate	log rotation config found:	true
syslog daemon detected:	true		
syslog daemon(s):	systemd-journal rsyslog		

log directories:

open log files:

open empty log files:

network info:

IPv6 Mode:	auto	IPv6 Only:	false
network interfaces:		lo enp2s0 enp3s0	
localhost mapped to:		::1	
ipv4 addresses:		127.0.0.1 192.168.103.150	
ipv6 addresses:		::1 fe80::5cb8:70c2:8be3:cb9b	
Default Gateway			
MAC Address:	00:e0:4c:68:0b:55 50:7b:9d:a1:a4:05	Name Cache Used:	false
name servers:		127.0.0.53	
resolv.conf search domain:		concords.com.tw	

Open Ports:

IP Address	Port	Protocol	Daemon/Process	???

security info:

Host Firewall Installed:	true	Firewall Software:		Firewall Empty Ruleset:	true	Firewall Active:	true
Package Audit Tools Found:	true	Package Audit Tool:	apt-check	Vulnerable Packages Found:	0	Package Manager:	dpkg
Two-Factor Authentication Enabled:	false	Two-Factor Authentication Required:	false	LDAP PAM Module Enabled:	false	LDAP Auth Enabled:	false
Minimum Password Length:	0	Maximum Password Days:	-1	Minimum Password Days:	-1	Maximum Password Retries:	3
Password Complexity Score:	0b1111	PAM Cracklib Found:	false	Password Strength Tested:	true	PAM Password Quality:	ARRAY(0x56516c8b5e88)
File Integrity Tools Installed:	false	File Integrity Tool:	NA	Automation Tool	false	Automation Tool:	

				Present:			
Malware Scanner Installed:	false	Malware Scanner(s):		compiler installed:	true	compilers:	
IDS/IPS Tooling		Failed Logins Logged:	1	fail2ban config file(s):		fail2ban enabled service(s):	
AppArmor Enabled:	false	AppArmor Policy Loaded:	false	SELinux Status:	false	SELinux mode:	
Group Names Unique	true	Group IDs Unique	true				

real users: **home directories:**

name	uid
root	0
mike	1000

PAM Modules:

> show <

boot info:

UEFI booted:	true	UEFI booted secure:	false
default runlevel:	5	boot service tool:	systemctl

services started at boot:

kernel info:

kernel version:	#46-Ubuntu SMP Tue Jul 12 10:30:17 UTC 2022	full kernel version:	5.15.0-43-generic
kernel release version:	5.15.0-43-generic	kernel IO scheduler:	
linux kernel type:	modular	number of kernels available:	

kernel modules loaded:

> show <

filesystem/journalling info:

oldest boot date:	2022-07-14	journal errors:	false
journal disk size:	456.0M	last cordumps:	0
filesystems:	/|ext4|	swap partitions:	/swapfile /swapfile
LVM volume group(s):		LVM volume(s)	

journal boot log found:

journal metadata:

> show <

```
Filepath:                  /var/log/journal/8b17349953d942a2bd14d0ae54a3b314/user-1000.journal
FileID:                    a9866b3df399415bbad66edf9bc4cc9b
MachineID:                 8b17349953d942a2bd14d0ae54a3b314
BootID:                    17d7ade5bc8a4d69a5622f8fab1d59ff
SequentialnumberID:        16ac98ca1c514ea3832ba8f0e11fbc66
State:                     ONLINE
Compatibleflags:
Incompatibleflags:         COMPRESSED-ZSTDKEYED-HASH
Headersize:                256
Arenasize:                 75497216
Datahashtablesize:         233016
Fieldhashtablesize:        333
Rotatesuggested:           no
Headsequentialnumber:      347506(54d72)
Tailsequentialnumber:      426062(6804e)
Headrealtimetimestamp:     Mon2022-08-0113:42:31CST(5e527774bb4fd)
Tailrealtimetimestamp:     Wed2022-08-0314:15:11CST(5e55027d4bdcc)
Tailmonotonictimestamp:    5d2h52min53.760s(66ff87e635)
Objects:                   152946
Entryobjects:              77314
Dataobjects:               74271
Datahashtablefill:         31.9%
Fieldobjects:              44
Fieldhashtablefill:        13.2%
Tagobjects:                0
Entryarrayobjects:         1315
Deepestfieldhashchain:     1
Deepestdatahashchain:      4
Diskusage:                 72.0M
|:
Filepath:                  /var/log/journal/8b17349953d942a2bd14d0ae54a3b314/system@da8d75110b3a40f0bfd04b
FileID:                    49d53be1262b41a8893f979501960f72
MachineID:                 8b17349953d942a2bd14d0ae54a3b314
BootID:                    17d7ade5bc8a4d69a5622f8fab1d59ff
SequentialnumberID:        da8d75110b3a40f0bfd04b0077fb91d3
State:                     ARCHIVED
```

```
Compatibleflags:
Incompatibleflags:       COMPRESSED-ZSTDKEYED-HASH
Headersize:              256
Arenasize:               16776960
Datahashtablesize:       233016
Fieldhashtablesize:      333
Rotatesuggested:         no
Headsequentialnumber:    226961(37691)
Tailsequentialnumber:    343935(53f7f)
Headrealtimetimestamp:   Mon2022-07-2509:42:22CST(5e4974b8b6ca9)
Tailrealtimetimestamp:   Mon2022-08-0113:37:49CST(5e52766767c64)
Tailmonotonictimestamp:  3d2h15min30.888s(3e3e29a4cd)
Objects:                 35053
Entryobjects:            8201
Dataobjects:             19330
Datahashtablefill:       8.3%
Fieldobjects:            125
Fieldhashtablefill:      37.5%
Tagobjects:              0
Entryarrayobjects:       7395
Deepestfieldhashchain:   2
Deepestdatahashchain:    2
Diskusage:               16.0M
|:
Filepath:                /var/log/journal/8b17349953d942a2bd14d0ae54a3b314/user-1000@16ac98ca1c514ea3832b
FileID:                  16ac98ca1c514ea3832ba8f0e11fbc66
MachineID:               8b17349953d942a2bd14d0ae54a3b314
BootID:                  17d7ade5bc8a4d69a5622f8fab1d59ff
SequentialnumberID:      16ac98ca1c514ea3832ba8f0e11fbc66
State:                   ARCHIVED
Compatibleflags:
Incompatibleflags:       COMPRESSED-ZSTDKEYED-HASH
Headersize:              256
Arenasize:               134217472
Datahashtablesize:       233016
Fieldhashtablesize:      333
Rotatesuggested:         no
Headsequentialnumber:    227103(3771f)
Tailsequentialnumber:    347505(54d71)
Headrealtimetimestamp:   Mon2022-07-2509:42:50CST(5e4974d3bba2b)
Tailrealtimetimestamp:   Mon2022-08-0113:42:31CST(5e527774bb478)
Tailmonotonictimestamp:  3d2h20min13.297s(3e4efedce1)
```

```
Objects:                  220027
Entryobjects:             112344
Dataobjects:              103647
Datahashtablefill:        44.5%
Fieldobjects:             54
Fieldhashtablefill:       16.2%
Tagobjects:               0
Entryarrayobjects:        3980
Deepestfieldhashchain:    1
Deepestdatahashchain:     4
Diskusage:                128.0M
l:
Filepath:                 /var/log/journal/8b17349953d942a2bd14d0ae54a3b314/user-1000@cd14d3eceb944648939
FileID:                   cd14d3eceb9446489397b913fd498e28
MachineID:                8b17349953d942a2bd14d0ae54a3b314
BootID:                   a0e64054b1534c6a9ddbcb8cc47d4a7c
SequentialnumberID:       cd14d3eceb9446489397b913fd498e28
State:                    ARCHIVED
Compatibleflags:
Incompatibleflags:        COMPRESSED-ZSTDKEYED-HASH
Headersize:               256
Arenasize:                134217472
Datahashtablesize:        233016
Fieldhashtablesize:       333
Rotatesuggested:          no
Headsequentialnumber:     2036(7f4)
Tailsequentialnumber:     165173(28535)
Headrealtimetimestamp:    Thu2022-07-1415:12:47CST(5e3bea0fcc4cd)
Tailrealtimetimestamp:    Thu2022-07-2116:36:35CST(5e44c9d8ae5f8)
Tailmonotonictimestamp: 6d5h42min56.123s(7d7d7af9a6)
Objects:                  220522
Entryobjects:             135244
Dataobjects:              77650
Datahashtablefill:        33.3%
Fieldobjects:             54
Fieldhashtablefill:       16.2%
Tagobjects:               0
Entryarrayobjects:        7572
Deepestfieldhashchain:    1
Deepestdatahashchain:     3
Diskusage:                128.0M
l:
```

```
Filepath:                 /var/log/journal/8b17349953d942a2bd14d0ae54a3b314/system.journal
FileID:                   740bba0af60f4a96a4441b6809922d20
MachineID:                8b17349953d942a2bd14d0ae54a3b314
BootID:                   17d7ade5bc8a4d69a5622f8fab1d59ff
SequentialnumberID:       da8d75110b3a40f0bfd04b0077fb91d3
State:                    OFFLINE
Compatibleflags:
Incompatibleflags:        COMPRESSED-ZSTDKEYED-HASH
Headersize:               256
Arenasize:                8388352
Datahashtablesize:        233016
Fieldhashtablesize:       333
Rotatesuggested:          no
Headsequentialnumber:     348379(550db)
Tailsequentialnumber:     426058(6804a)
Headrealtimetimestamp:    Mon2022-08-0113:42:59CST(5e52778fc204f)
Tailrealtimetimestamp:    Wed2022-08-0314:13:42CST(5e5502286f3a1)
Tailmonotonictimestamp:   5d2h51min24.776s(66fa3a1c0b)
Objects:                  6326
Entryobjects:             1243
Dataobjects:              3215
Datahashtablefill:        1.4%
Fieldobjects:             71
Fieldhashtablefill:       21.3%
Tagobjects:               0
Entryarrayobjects:        1795
Deepestfieldhashchain:    1
Deepestdatahashchain:     1
Diskusage:                8.0M
|:
Filepath:                 /var/log/journal/8b17349953d942a2bd14d0ae54a3b314/system@da8d75110b3a40f0bfd04b
FileID:                   da8d75110b3a40f0bfd04b0077fb91d3
MachineID:                8b17349953d942a2bd14d0ae54a3b314
BootID:                   a0e64054b1534c6a9ddbcb8cc47d4a7c
SequentialnumberID:       da8d75110b3a40f0bfd04b0077fb91d3
State:                    ARCHIVED
Compatibleflags:
Incompatibleflags:        COMPRESSED-ZSTDKEYED-HASH
Headersize:               256
Arenasize:                33554176
Datahashtablesize:        233016
Fieldhashtablesize:       333
```

```
Rotatesuggested:          no
Headsequentialnumber:     1(1)
Tailsequentialnumber:     142986(22e8a)
Headrealtimetimestamp:    Thu2022-07-1415:09:01CST(5e3be937d6e52)
Tailrealtimetimestamp:    Thu2022-07-2116:36:32CST(5e44c9d67546a)
Tailmonotonictimestamp:   6d5h42min53.792s(7d7d576817)
Objects:                  99334
Entryobjects:             29929
Dataobjects:              52745
Datahashtablefill:        22.6%
Fieldobjects:             143
Fieldhashtablefill:       42.9%
Tagobjects:               0
Entryarrayobjects:        16515
Deepestfieldhashchain:    2
Deepestdatahashchain:     2
Diskusage:                32.0M
l:
Filepath:                 /var/log/journal/8b17349953d942a2bd14d0ae54a3b314/user-1000@cd14d3eceb944648939
FileID:                   e2ae37d4a80f47e2a6687576bb51d553
MachineID:                8b17349953d942a2bd14d0ae54a3b314
BootID:                   2f863502659f49bb8dab27e0e73a9d81
SequentialnumberID:       cd14d3eceb9446489397b913fd498e28
State:                    ARCHIVED
Compatibleflags:
Incompatibleflags:        COMPRESSED-ZSTDKEYED-HASH
Headersize:               256
Arenasize:                58720000
Datahashtablesize:        233016
Fieldhashtablesize:       333
Rotatesuggested:          no
Headsequentialnumber:     165174(28536)
Tailsequentialnumber:     224706(36dc2)
Headrealtimetimestamp:    Thu2022-07-2116:36:35CST(5e44c9d8ae630)
Tailrealtimetimestamp:    Mon2022-07-2509:29:35CST(5e4971dd594dc)
Tailmonotonictimestamp:   1w2d22h35min56.081s(c7fdc5a88a)
Objects:                  76932
Entryobjects:             56712
Dataobjects:              18928
Datahashtablefill:        8.1%
Fieldobjects:             47
Fieldhashtablefill:       14.1%
```

```
Tagobjects:                 0
Entryarrayobjects:          1243
Deepestfieldhashchain:      1
Deepestdatahashchain:       2
Diskusage:                  56.0M
|:
Filepath:                   /var/log/journal/8b17349953d942a2bd14d0ae54a3b314/system@da8d75110b3a40f0bfd04b
FileID:                     c25f9ef5f0c646d5b1a72f7f647c9737
MachineID:                  8b17349953d942a2bd14d0ae54a3b314
BootID:                     2f863502659f49bb8dab27e0e73a9d81
SequentialnumberID:         da8d75110b3a40f0bfd04b0077fb91d3
State:                      ARCHIVED
Compatibleflags:
Incompatibleflags:          COMPRESSED-ZSTDKEYED-HASH
Headersize:                 256
Arenasize:                  16776960
Datahashtablesize:          233016
Fieldhashtablesize:         333
Rotatesuggested:            no
Headsequentialnumber:       182215(2c7c7)
Tailsequentialnumber:       226960(37690)
Headrealtimetimestamp:      Thu2022-07-2116:36:40CST(5e44c9dd25133)
Tailrealtimetimestamp:      Mon2022-07-2517:42:21CST(5e49e001c062d)
Tailmonotonictimestamp:     49.153s(2ee05d7)
Objects:                    22346
Entryobjects:               5075
Dataobjects:                12302
Datahashtablefill:          5.3%
Fieldobjects:               119
Fieldhashtablefill:         35.7%
Tagobjects:                 0
Entryarrayobjects:          4848
Deepestfieldhashchain:      2
Deepestdatahashchain:       2
Diskusage:                  16.0M
```

service info:

```
arpwatch running:       false
audit_daemon running:   false
dhcp_client running:    false
```

linux_auditd running:	false
mysql running:	true
nginx running:	false
ntp_daemon running:	true
postgresql running:	false
redis running:	false
ssh_daemon running:	false

daemon info:

pop3 daemon:	
imap daemon:	
smtp daemon:	
printing daemon:	cups
ntp daemon:	systemd-timesyncd
scheduler(s):	crond anacron
service manager:	systemd
running service tool:	systemctl

running services:

ntp detail:

> show <

ntp config found:	false	ntp config file:	
ntp version:		unreliable peers:	
	NTP Config Type		
startup:	false	daemon:	true
scheduled:	false	event based:	false

nginx detail

main config file:	other config file(s):
log file:	

nginx config options:

> show <

-

SSL/TLS protocols enabled:

> show <

-

apache details:

> show <

apache version:

apache modules found:

> show <

systemd detail:

> show <

systemd version:	249	systemd status:	degraded
systemd builtin components:	+PAM,+AUDIT,+SELINUX,+APPARMOR,+IMA,+SMACK,+SECCOMP,+GCRYPT,+GNUTLS,		

systemd unit files:

> show <

unit file	status

systemd unit not found:

> show <

- â
- â
- â
- â
- â
- â
- â
- â
- â
- â
- â
- â
- â
- â
- â
- â
- â

- â
- â
- â

systemd service not found:

> show <

- auditd.service
- auto-cpufreq.service
- cloud-config.service
- connman.service
- console-screen.service
- kbd.service
- nslcd.service
- oem-config.service
- ovsdb-server.service
- system76-power.service
- systemd-hwdb-update.service
- systemd-update-done.service
- systemd-vconsole-setup.service
- tuned.service
- ua-auto-attach.service
- ubuntu-advantage-cloud-id-shim.service
- zfs-mount.service

Installed packages:

Number of packages installed: 1840 Number of binaries found: 2005

> show <
