Lynis-2

Auditing, system hardening, compliance testing

To be
Presented to
St. Louis Unix Users Group
May 8, 2019
Graybar Electric Company Inc.
By
David Forrest

Who am I?

David Forrest graduated from Oregon State University in BA, Finance Emphasis, Physics & Mathematics. Lifelong hobbyist in IT from IBM 1401, Model 20, Model 30, Model 85, Sigma 7, XDS 7, SWTP 6800, M6809, 8080, 80286, 80386, OS2, and on to currently running XP, CentOS6/7, Raspbian, Mint, and Chrome on various local and cloud machines.

Lynis is a security auditing tool for a system based on UNIX like Linux, macOS, BSD, and others. It performs an in-depth security scan and runs on the system itself. The primary goal is to test security defenses and provide tips for further system hardening.

It will also scan for general system information, vulnerable software packages, and possible configuration issues. Lynis was commonly used by system administrators and auditors to assess the security defenses of their systems. Besides the "blue team", nowadays penetration testers also have Lynis in their toolkit.

So what is lynis?

Lynis ~~2.6.6~~ 2.7.4

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

(Linux, macOS, BSD, and others)

2007-2019, CISOfy - https://cisofy.com/lynis/

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

https://www.tecmint.com/scan-linux-for-malware-and-rootkits/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+tecmint+%28Tecmint%3A+Linux+Howto%27s+Guide%29

Why?

- To simplify my current data collection script as it started over a dozen years ago and has become difficult for an older guy to update.
- Currently I still use the script to collect information; it’s a bit easier to just demonstrate by showing it in another window.

Why?

I have run rkhunter for years but it is due for an upgrade anyway and my script is using a newer release which I will display in real time.

This requires an IPv6 ssh connection so I may have to go through a cloud machine I have in Chicago that is dual hosted. Alternatively, I'll have a back-up current flash drive and put it in Google Drive.

The lynis report

- Since it is now running from a root crontab at 3AM daily; we'll look at this morning's report as it is a continuing update but usable as a working document.
- And we'll look over the configuration processes for lynis and rkhunter. My machines are selinux enabled and dual IPv6 & IPv4 internally but only marginally accessible via IPv4 externally.

SSH?

- Security is important and I primarily use Open SSH on my various machines so let’s just look at how to check that configuration:
- Avoid Configuration Weaknesses: The first SSH protocol (SSH-1) was vulnerable to man-in-the-middle attacks, so eavesdroppers could intercept your communications and read your (supposedly secure) traffic. Most distributions’ SSH setups allow only SSH-2, but it’s a good idea to confirm that Protocol 2 is included in your configuration file and Protocol 1 is disabled.

SSH (cont.)

- Although not common today, rhosts sometimes was used to authenticate systems. Disable that by adding IgnoreRhosts yes to SSH's configuration file.
- If you won't be doing X11 forwarding, set X11Forwarding no to impede possible attacks.
- Set DSA Authentication to no to disable weak DSA authentication.

SSH (cont.)

- Don’t ever allow users to work without passwords: set PermitEmptyPasswords no .
- Set PermitRootLogin no so nobody can log in as root. Users who need to connect and work as root should log in as common users (that is, unprivileged, and as restricted as possible) and then use sudo.

SSH

- So just how does one check? Individually? Who checks the checker? All of the various items are found in the /etc/ssh/sshd_config file. ???
- So we'll just let rkhunter check as I have for years.

Rkhunter and lynis

- Rkhunter is run by lynis for me and its config files are defaulted to /etc/rkhunter as: /etc/rkhunter.conf and /etc/rkhunter.conf.local
- Lynis uses the profile files in /etc/lynis as default.prf, custom.prf, and also the output of rkhunter.
- We’ll look at those a bit.

SSH ↔ rkhunter

A little coordination is necessary. This was a warning that caused me a misunderstanding about the interactions

---------- Start Rootkit Hunter Scan ----------
Warning: The SSH and rkhunter configuration options should be the same:
SSH configuration option 'PermitRootLogin': no
Rkhunter configuration option 'ALLOW_SSH_ROOT_USER': unset
---------- End Rootkit Hunter Scan ----------

```
2 3 * * * /usr/bin/echo "As of $(date)"  >/var/tmp/lynisreport; /usr/local/bin/lynis --cronjob 2>&1
 >>/var/tmp/lynisreport;
```

+] SSH Support

- Checking running SSH daemon [FOUND]
- Searching SSH configuration [FOUND]
- SSH option: AllowTcpForwarding [SUGGESTION]
- SSH option: ClientAliveCountMax [SUGGESTION]
- SSH option: ClientAliveInterval [OK]
- SSH option: Compression [SUGGESTION]
- SSH option: FingerprintHash [OK]
- SSH option: GatewayPorts [OK]
- SSH option: IgnoreRhosts [OK]
- SSH option: LoginGraceTime [OK]
- SSH option: LogLevel [SUGGESTION]
- SSH option: MaxAuthTries [SUGGESTION]
- SSH option: MaxSessions [SUGGESTION]
- SSH option: PermitRootLogin [OK]
- SSH option: PermitUserEnvironment [OK]
- SSH option: PermitTunnel [OK]
- SSH option: Port [OK]
- SSH option: PrintLastLog [OK]
- SSH option: StrictModes [OK]
- SSH option: TCPKeepAlive [SUGGESTION]
- SSH option: UseDNS [SUGGESTION]
- SSH option: VerifyReverseMapping [NOT FOUND]
- SSH option: X11Forwarding [SUGGESTION]
- SSH option: AllowAgentForwarding [SUGGESTION]
- SSH option: UsePrivilegeSeparation [OK]
- SSH option: AllowUsers [NOT FOUND]
- SSH option: AllowGroups [NOT FOUND]

Lynis-2

- Its been six months since I did the first lynis presentation and I now connect through an updated lynis from the cisofy open-source site:
- https://cisofy.com/documentation/lynis/get-started/
- I had used the CentOS package site but couldn’t update it as I needed some “enterprise” modules so I reloaded it using the github distribution and now am using version 2.74 and update often.

New warnings from new tests

- Now in a separate directory, I first got some new warnings and only one was not satisfied by simple configuration changes (and used my old config files). My new cronjob:
- /usr/bin/echo "As of $(date) Use sudo rkhunter --propupd to OK" >/var/tmp/lynisreport; /usr/local/lynis/lynis --cronjob 2>&1 >>/var/tmp/lynisreport;”
- I changed the called binary from bin/ to local/lynis/

+] Networking

- Checking IPv6 configuration [ENABLED]
Configuration method [AUTO]
IPv6 only [NO]
- Checking configured nameservers
- Testing nameservers
Nameserver: 192.168.1.1 [OK]
Nameserver: 8.8.8.8 [OK]
Nameserver: 2001:4860:4860::8888 [OK]
Nameserver: 2001:4860:4860::8844 [OK]
- Minimal of 2 responsive nameservers [OK]
- Checking default gateway [DONE]
- Getting listening ports (TCP/UDP) [DONE]
* Found 28 ports
- Checking promiscuous interfaces [WARNING]
- Checking waiting connections [OK]
- Checking status DHCP client [RUNNING]
- Checking for ARP monitoring software [NOT FOUND]

Lynis-2

- -[Lynis 2.7.4 Results]-
-
- Warnings (1):
- ----------------------------
- ! Found promiscuous interface [NETW-3015]
- - Details : virbr0-nic
- - Solution : Determine if this mode is required or whitelist interface in profile
- https://cisofy.com/lynis/controls/NETW-3015/
-
- Suggestions (29):
- ----------------------------

NETW-3015

[root@dave:~]$ /usr/local/lynis/lynis show details NETW-3015

2019-04-19 11:39:39 Performing test ID NETW-3015 (Checking promiscuous interfaces (Linux))

2019-04-19 11:39:39 Test: Using ip binary to retrieve network interfaces

2019-04-19 11:39:39 Test: Checking all interfaces to discover any with promiscuous mode enabled

2019-04-19 11:39:39 Result: Promiscuous interface: virbr0-nic

2019-04-19 11:39:39 Warning: Found promiscuous interface [test:NETW-3015] [details:virbr0-nic] [solution:text:Determine if this mode is required or whitelist interface in profile]

2019-04-19 11:39:39 Note: some tools put an interface into promiscuous mode, to capture/log network traffic

2019-04-19 11:39:39 ===--===

[root@dave:~]$ /usr/local/lynis/lynis show profiles

/etc/lynis/default.prf

Promiscuity ON! (but down)

```
[root@dave:~]$ ip -details  address show dev virbr0-nic
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN
group default qlen 1000
    link/ether 52:54:00:be:42:f7 brd ff:ff:ff:ff:ff:ff promiscuity 1
    tun
    bridge_slave state disabled priority 32 cost 100 hairpin off guard off root_block off fastleave off
learning on flood on port_id 0x8001 port_no 0x1 designated_port 32769 designated_cost 0
designated_bridge 8000.52:54:0:be:42:f7 designated_root 8000.52:54:0:be:42:f7 hold_timer
0.00 message_age_timer    0.00 forward_delay_timer    0.00 topology_change_ack 0
config_pending 0 proxy_arp off proxy_arp_wifi off mcast_router 1 mcast_fast_leave off
mcast_flood on numtxqueues 1 numrxqueues 1 gso_max_size 65536 gso_max_segs 65535
[root@dave:~]$
```

Just delete the test!

Added a custom.prf to adjust my profile!

```
########################################
# D. R. Forrest 4/28/19
# Not using virbr0-nic (disabled)
skip-test=NETW-3015
########################################
```

Now

-[Lynis 2.7.4 Results]-

Great, no warnings

Suggestions (28):

Rkhunter local configuration

- # 9/4/18 DRF :To add a mailing address for rkhunter execution warnings
- MAIL-ON-WARNING=drf@maplepark.com
- # 9/5/18 DRF :Create a new log file each run
- APPEND_LOG=0
- # 9/8/18 DRF :ALLOW ROOT USER NO (But I think it reflects on ALLOW ROOT USER as I set it unset it first run but I think it means
- # PermitRootLogin actually is NO.
- ALLOW_SSH_ROOT_USER=NO
- # 9/8/18 DRF :I do not use Protocol 1 and hope no one does
- ALLOW_SSH_PROT_V1=2
- # 4/26/19 re-implemented upon installation of new system this date

Updating file properties

```
[03:11:18]   /usr/bin/mailx                          [ OK ]
[03:11:19]   /usr/bin/kmod                           [ OK ]
[03:11:20]   /usr/bin/systemctl                      [ Warning ]
[03:11:20] Warning: The file properties have changed:
[03:11:20]         File: /usr/bin/systemctl
[03:11:20]         Current inode: 560719    Stored inode: 560720
[03:11:21]   /usr/sbin/adduser                       [ OK ]
[03:11:22]   /usr/sbin/chkconfig                     [ OK
(… and four more; init, ip, runlevel, systemd ...)

[drf@dave:~]$ less /usr/bin/systemctl
"/usr/bin/systemctl" may be a binary file.  See it anyway?
[drf@dave:~]$ sudo chmod o-x /usr/bin/systemctl
[drf@dave:~]$ sudo chmod o-r /usr/bin/systemctl
[drf@dave:~]$ sudo rkhunter --propupd
[ Rootkit Hunter version 1.4.6 ]
File updated: searched for 176 files, found 136
[drf@dave:~]$
```

Lynis local configuration

- Lynis doesn't have to be installed, so it can be used directly from a (removable) disk. If you want the program to be installed, use one of the methods from: https://cisofy.com
- Required permissions: root preferred, not needed- Other requirements: write access to /tmp
- So why not?

FIN

- Thanks for being here.
-
- What final Questions?