Lynis

Auditing, system hardening, compliance testing

To be
Presented to
St. Louis Unix Users Group
September 12, 2018
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.

So what is lynis?

Lynis 2.6.6

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

(Linux, macOS, BSD, and others)

2007-2018, 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.

SSH → vp1 → dave

```
[drf@dave:~]$ sudo ss -n -o state established '( dport = :1941 or sport = :1941 )'
[sudo] password for drf:
Netid Recv-Q Send-Q          Local Address:Port                                  Peer Address:Port
tcp   0      0                192.168.1.73:47774                                198.58.98.128:1941       timer(keepalive,119min,0)
tcp   0      0      2602:100:6023:b392:e23f:49ff:fe7f:ad78:33270   2602:100:6023:b392:1e1b:dff:fe13:e4d5:1941   timer:(keepalive,31min,0)
tcp   0      0       2602:100:6023:b392:e23f:49ff:fe7f:ad78:1941   2600:3c00::f03c:91ff:fe56:7e17:38780        timer:(keepalive,119min,0)

[drf@dave:~]$ host 2600:3c00::f03c:91ff:fe56:7e17
7.1.e.7.6.5.e.f.f.f.1.9.c.3.0.f.0.0.0.0.0.0.0.0.0.0.0.0.c.3.0.0.6.2.ip6.arpa domain name pointer vp1.maplepark.com.
[drf@dave:~]$
```

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.

Why?

- 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 DSAAuthentication 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 look 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 /usr/local/lynis default.prf, custom.prf, and 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;
```

And if we Didn't connect??

I’ll show the data now from an archived mode. But if we did, let’s talk a bit more about security concerns.

NATTING


DILBERT • By Scott Adams
I INVENTED A DEVICE THAT CAN READ YOUR THOUGHTS AND TURN THEM INTO COMPUTER COMMANDS.
NOTHING IS HAPPENING.
IS IT BROKEN?
THAT'S ONE OF MY TOP TWO THEORIES.

FIN

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