

# Day 46

## Exploitation Analyst

### Firewalls and TCP wrappers:

### Lynis Audit Tool:

#### What is Lynis Audit tool?

Lynis is an open-source security auditing tool for Linux and Unix systems. It scans the system to check for misconfigurations, vulnerabilities, and compliance issues. Lynis evaluates things like:

- Installed software and packages
- File permissions and authentication settings
- Firewall, SSH, and logging configuration
- Security hardening opportunities

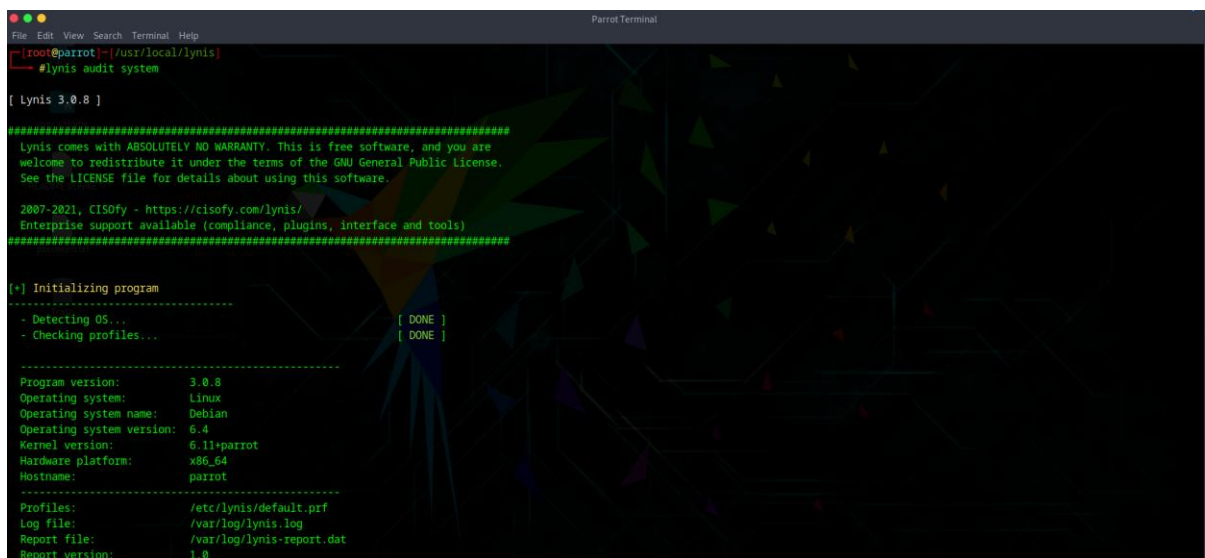
It's useful for penetration testers, system administrators, and auditors to quickly assess a system's security posture and get recommendations for hardening.

### Exploring Lynis Audit Tool:

Steps:

Command:

`sudo lynis audit system`

A screenshot of a terminal window titled "Parrot Terminal". The terminal shows the command `lynis audit system` being executed. The output includes a header for "Lynis 3.0.8", a disclaimer about the GNU General Public License, and system information. The initialization process is shown with progress bars for "Detecting OS..." and "Checking profiles...", both marked as "[ DONE ]". A detailed system profile is listed, including program version (3.0.8), operating system (Linux/Debian), kernel version (6.11+parrot), hardware platform (x86\_64), and hostname (parrot). Configuration files for profiles, log files, and report files are also displayed.

```
File Edit View Search Terminal Help
--[root@parrot:~/usr/local/lynis]
#lynis audit system

[ Lynis 3.0.8 ]

=====
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
=====

[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]

-----
Program version: 3.0.8
Operating system: Linux
Operating system name: Debian
Operating system version: 6.4
Kernel version: 6.11+parrot
Hardware platform: x86_64
Hostname: parrot
-----
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
```

```
ParrotTerminal
File Edit View Search Terminal Help
- Firewall [V]
- Malware scanner [X]

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 3.0.8

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2021, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====
[Tip]: Enhance Lynis audits by adding your settings to custom.prfl (see /etc/lynis/default.prfl for all settings)
```

This will scan your machine and generate a report with warnings, suggestions, and hardening tips.

Now, open the report:

```
[root@parrot]-[/usr/local/lynis]
#nano /var/log/lynis-report.dat
```

Following screen will appear: the report is ready.

```
ParrotTerminal
File Edit View Search Terminal Help
GNU nano 7.2 /var/log/lynis-report.dat
Lynis Report
report_version_major=1
report_version_minor=0
report_datetime_start=2025-08-26 04:59:42
auditor=[Not Specified]
lynis_version=3.0.8
os=Linux
os_name=Debian
os_fullname=Parrot Security 6.4 (lorikeet)
os_version=6.4
linux_version=Debian
os_kernel_version=6.11+parrot
os_kernel_version_full=6.11+parrot-amd64
hostname=parrot
test_category=all
test_group=all
plugin_directory=/etc/lynis/plugins
lynis_update_available=0
suggestion[]=LYNIS[This release is more than 4 months old. Check the website or GitHub to see if there is an update available.]--
binaries_count=4742
binaries_suid_count=/usr/bin/chfn /usr/bin/chsh /usr/bin/fusemount /usr/bin/fusemount3 /usr/bin/gpasswd /usr/bin/mailq /usr/bin/mount /usr/bin/newaliases /usr/bin/newgidmap /usr/bin/newgrp
binaries_sgid_count=/usr/bin/chage /usr/bin/crontab /usr/bin/dotlockfile /usr/bin/expiry /usr/bin/ssh-agent /usr/sbin/unix_chkpwd
binary_paths=/usr/bin,/usr/sbin,/usr/local/bin,/usr/local/sbin
vm=1
vmtype=virtualbox
container=0
notebook=1
system=1
plugin_enabled_phase1[]=debian[1.0.1]

[Read 728 lines]
Help Read File Replace Paste Go To Line Redo Copy Where Was Next
Exit Where Is Cut Execute Undo Set Mark To Bracket Previous Back Prev Word Next Word Home
```

--The End--