LINUX SYSTEM SECURITY AUDIT (BEGINNER LEVEL)

DATE- 17.01.2026

NAME-SUHANI KULSHRESTHA

STATUS-COLLEGE STUDENT

OBJECTIVE

The objective of this project is to analyze basic security settings of a Linux system such as users, permissions, and sudo access and identify common security risks.

TOOLS USED

1. LINUX OS(KALI)
2. TERMINAL
3. BASIC LINUX COMMANDS (`ls`, `chmod`, `whoami`, `sudo`, `man`)

STEPS PERFORMED

- Checked current user using whoami command
- Listed all users from /etc/passwd
- Created test files to analyze permissions
- Changed file permissions using chmod command
- Checked sudo privileges using `sudo -l`

METHODOLOGY

The following steps were followed during the audit:

- Identify insecure permissions
- Analyze associated security risks
- Apply corrective actions based on least privilege principle

FINDINGS

- File permissions were found in the format `-rw-r--r--`
- Some files had overly permissive access such as 777
- Ownership of files was verified
- Users with sudo access were identified

RISKS

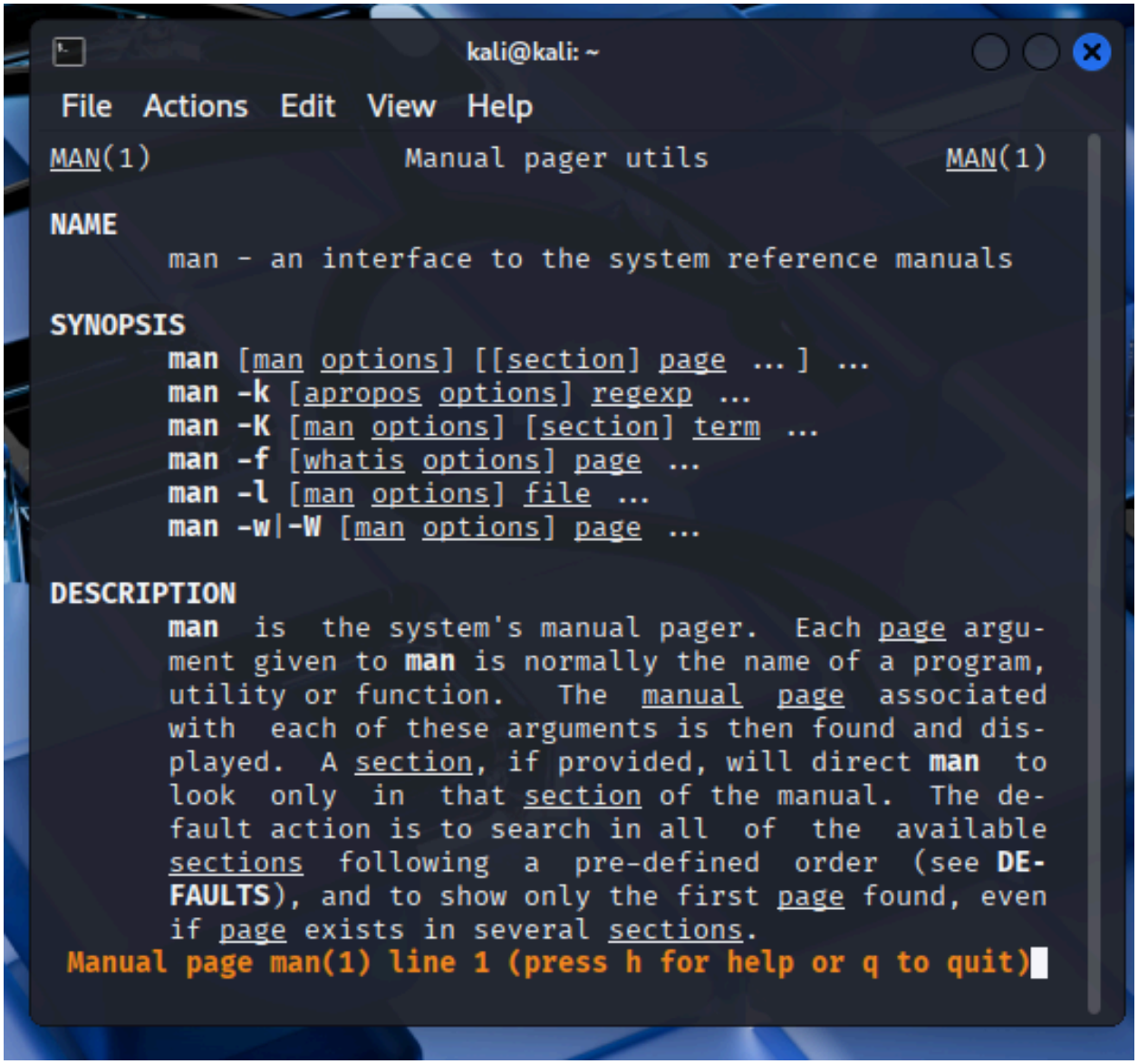
- Files with `777` permissions allow any user to read, write, or execute them
- Misconfigured permissions can allow attackers to modify or delete files
- Excessive sudo access can lead to privilege escalation

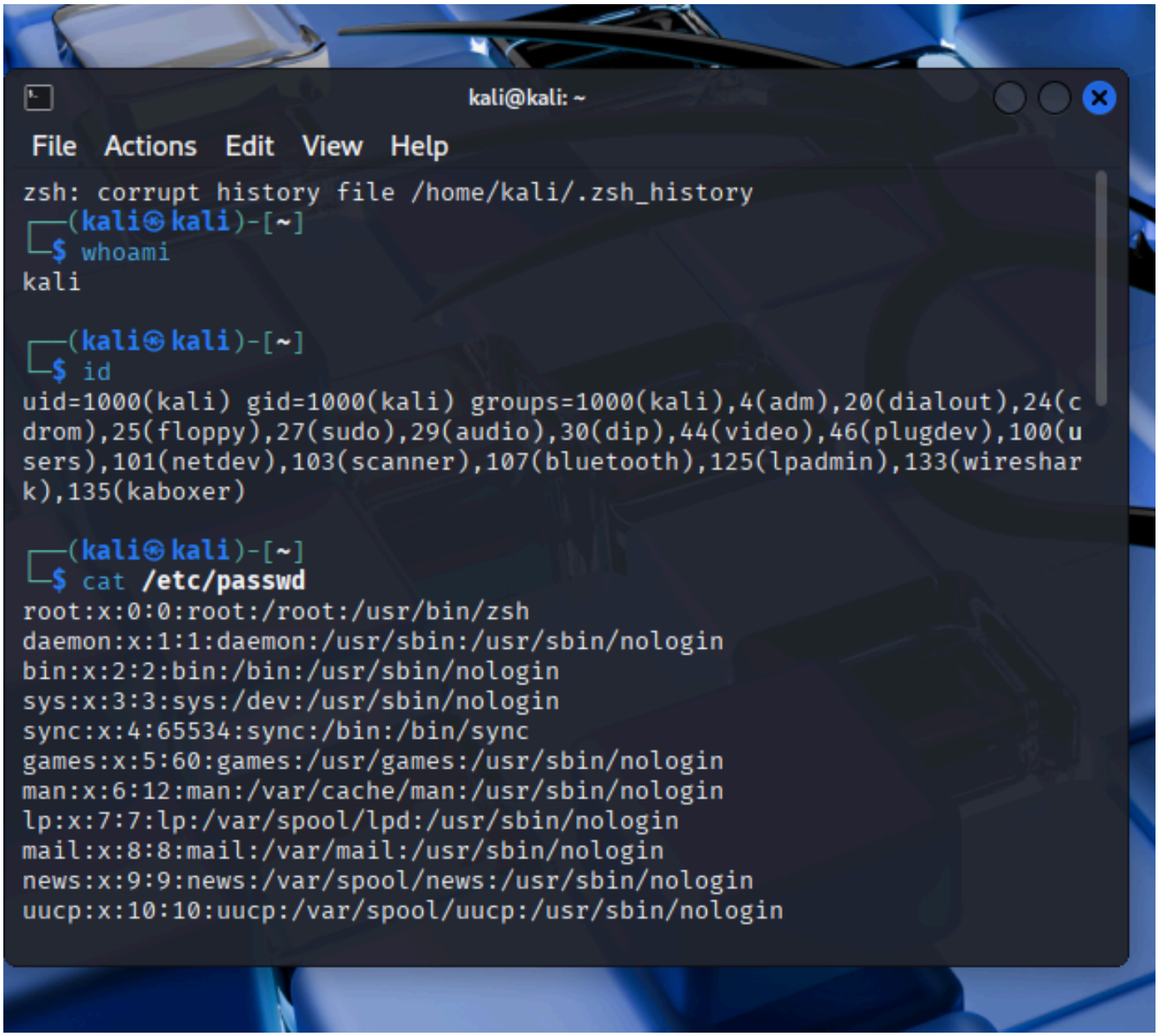
RECOMMENDATIONS

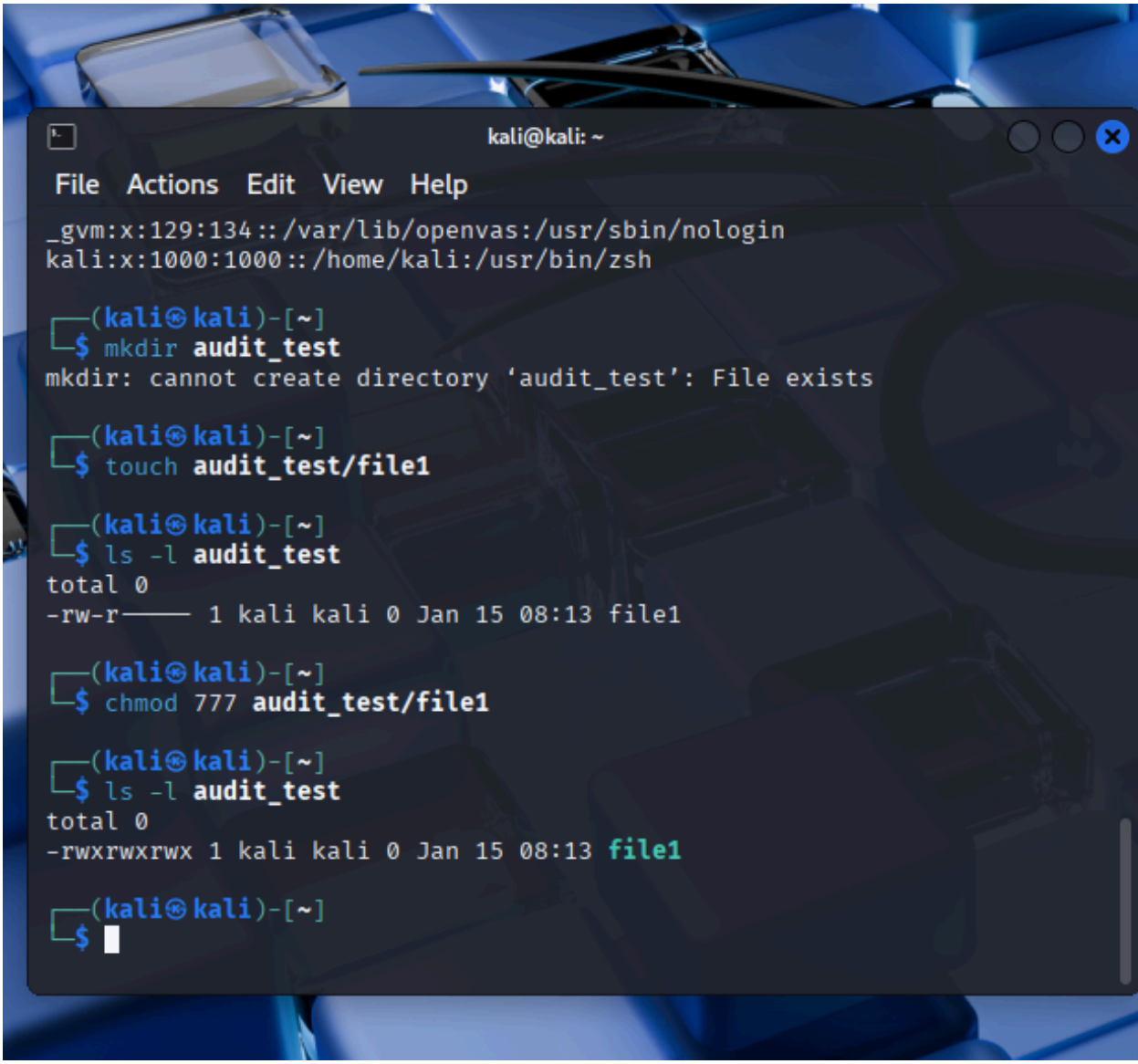
- Use restrictive permissions such as `644` or `640` for files
- Limit sudo access to required users only
- Applied the principle of least privilege

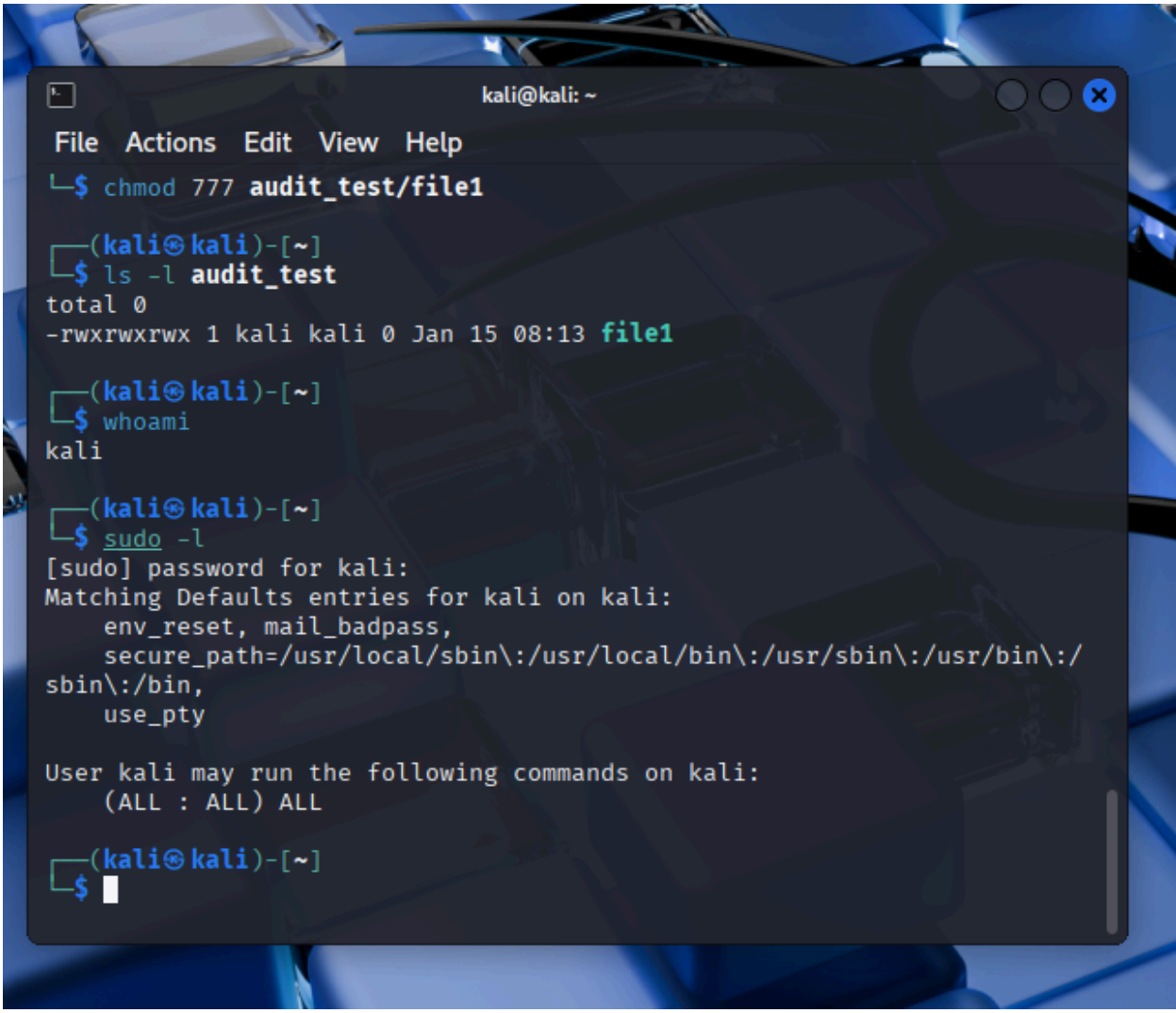
PROOFS / REFERENCES

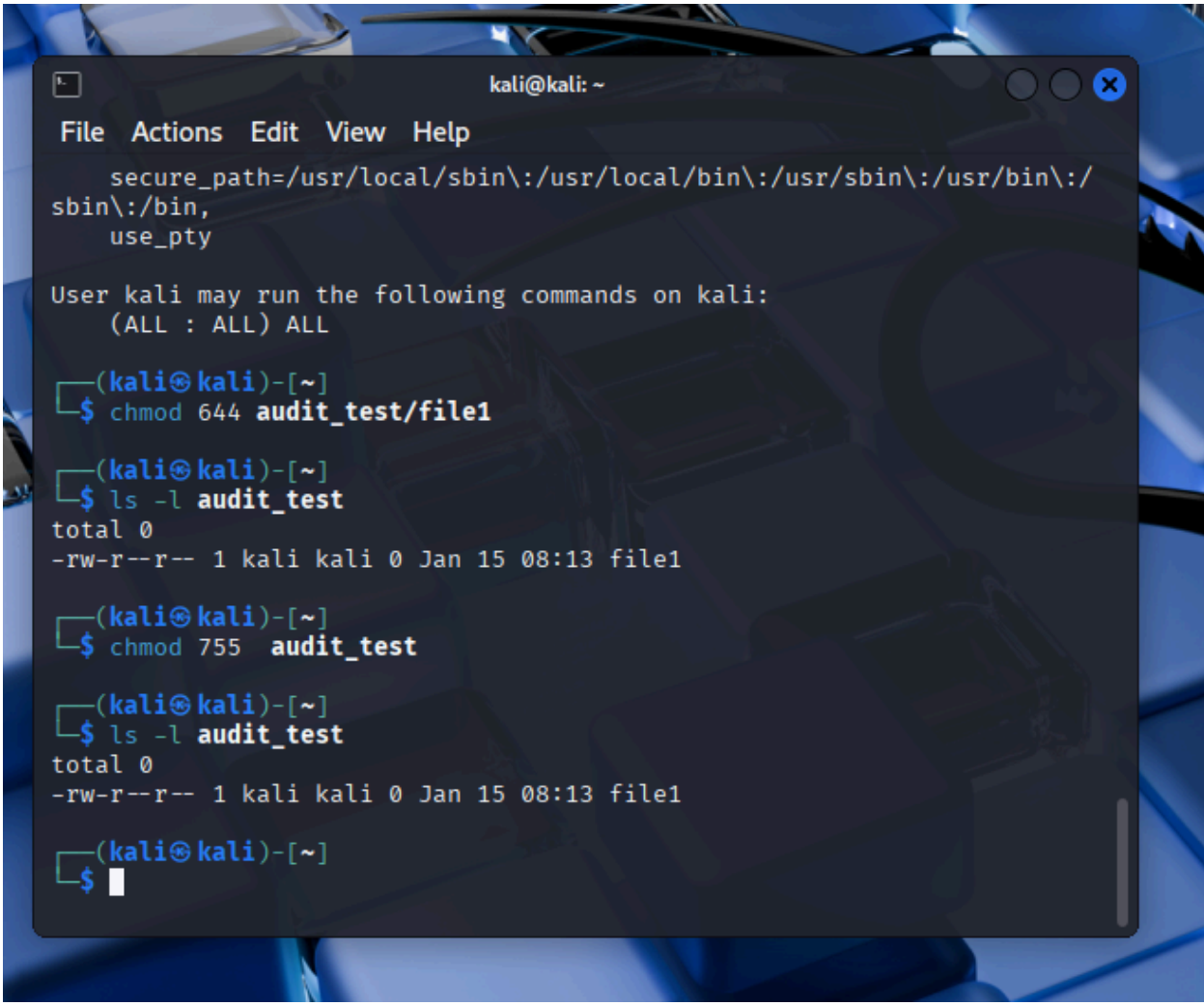
• Linux manual pages were used using the man command to understand commands and options.


kali@kali: ~
File Actions Edit View Help
MAN(1) Manual pager utils MAN(1)
NAME
man - an interface to the system reference manuals
SYNOPSIS
man [man options] [[section] page ...] ...
man -k [apropos options] regexp ...
man -K [man options] [section] term ...
man -f [whatis options] page ...
man -l [man options] file ...
man -w|-W [man options] page ...
DESCRIPTION
man is the system's manual pager. Each page argument given to man is normally the name of a program, utility or function. The manual page associated with each of these arguments is then found and displayed. A section, if provided, will direct man to look only in that section of the manual. The default action is to search in all of the available sections following a pre-defined order (see DEFAULTS), and to show only the first page found, even if page exists in several sections.
Manual page man(1) line 1 (press h for help or q to quit)


kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ whoami
kali
┌──(kali㉿kali)-[~]
└─$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),103(scanner),107(bluetooth),125(lpadmin),133(wireshark),135(kaboxer)
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin


kali@kali: ~
File Actions Edit View Help
_gvm:x:129:134::/var/lib/openvas:/usr/sbin/nologin
kali:x:1000:1000::/home/kali:/usr/bin/zsh
┌──(kali㉿kali)-[~]
└─$ mkdir audit_test
mkdir: cannot create directory ‘audit_test’: File exists
┌──(kali㉿kali)-[~]
└─$ touch audit_test/file1
┌──(kali㉿kali)-[~]
└─$ ls -l audit_test
total 0
-rw-r——— 1 kali kali 0 Jan 15 08:13 file1
┌──(kali㉿kali)-[~]
└─$ chmod 777 audit_test/file1
┌──(kali㉿kali)-[~]
└─$ ls -l audit_test
total 0
-rwxrwxrwx 1 kali kali 0 Jan 15 08:13 file1
┌──(kali㉿kali)-[~]
└─$


kali@kali: ~
File Actions Edit View Help
└─$ chmod 777 audit_test/file1
┌──(kali㉿kali)-[~]
└─$ ls -l audit_test
total 0
-rwxrwxrwx 1 kali kali 0 Jan 15 08:13 file1
┌──(kali㉿kali)-[~]
└─$ whoami
kali
┌──(kali㉿kali)-[~]
└─$ sudo -l
[sudo] password for kali:
Matching Defaults entries for kali on kali:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/
sbin\:/bin,
use_pty
User kali may run the following commands on kali:
(ALL : ALL) ALL
┌──(kali㉿kali)-[~]
└─$


kali@kali: ~
File Actions Edit View Help
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
use_pty
User kali may run the following commands on kali:
(ALL : ALL) ALL
(kali㉿kali)-[~]
$ chmod 644 audit_test/file1
(kali㉿kali)-[~]
$ ls -l audit_test
total 0
-rw-r--r-- 1 kali kali 0 Jan 15 08:13 file1
(kali㉿kali)-[~]
$ chmod 755 audit_test
(kali㉿kali)-[~]
$ ls -l audit_test
total 0
-rw-r--r-- 1 kali kali 0 Jan 15 08:13 file1
(kali㉿kali)-[~]
$

FIXES APPLIED

- Changed insecure file permissions from 777 to 644 using chmod
- Restricted directory access by setting permission to 755
- Verified user privilege using sudo -l
- Applied the principles of least privilege to reduce security risk

WHAT I LEARNED

- How linux file permissions control access for users,groups and others
- Why insecure permissions can lead to security vulnerabilities
- How to identify and fix permission-related security issues
- Basic understanding of privilege escalation and sudo risks
- How to document security findings like a cybersecurity analyst