Part 1

Task 1

```
#!/bin/bash
# Print greeting and system info
echo "Hello, Security World!"
date
uptime
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ chmod 600 hello.sh

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ bash hello.sh
Hello, Security World!
Thu Oct  2 11:33:09 PM PDT 2025
 23:33:09 up 10 min,  0 users,  load average: 0.14, 0.16, 0.13

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$
```

Task 2

```
#!/bin/bash
ls /etc /home > /tmp/file_list.log
echo "File list saved to /tmp/file_list.log"
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ bash hello.sh
Hello, Security World!
Thu Oct  2 11:33:09 PM PDT 2025
 23:33:09 up 10 min,  0 users,  load average: 0.14, 0.16, 0.13

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ vim task2.sh

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ chmod 600 task2.sh

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ bash task2.sh
File list saved to /tmp/file_list.log

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ cat /tmp/file_list.log
/etc:
adduser.conf
alternatives
apache2
apparmor
apparmor.d
apt
arp-scan
audit
avahi
bash.bashrc
bash_completion
bash_completion.d
bindresvport.blacklist
binfmt.d
bluetooth
ca-certificates
ca-certificates.conf
chatscripts
chromium
chromium.d
cifs-utils
cloud
colord
```

Task 3

```
#!/bin/bash
DIR="/tmp/testdir"
if [ ! -d "$DIR" ]; then
        mkdir $DIR
        echo "Directory $DIR created"
else
        echo "Directory $DIR already exists"
fi
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ chmod 600 task3.sh

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ bash task3.sh
Directory /tmp/testdir created

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ bash task3.sh
Directory /tmp/testdir already exists

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$
```

Task 4

```
#!/bin/bash
echo "recent login attempts:"
last -n 5
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ chmod 600 task4.sh

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$ bash task4.sh
recent login attempts:
kali     tty7         :0               Fri Sep 26 10:47 - still logged in
kali     tty7         :0               Fri Sep 26 09:23 - still logged in
kali     tty7         :0               Fri Sep 26 09:14 - still logged in
kali     tty7         :0               Thu Sep 25 15:32 - still logged in
kali     tty7         :0               Thu Sep 25 15:25 - 15:31  (00:05)

wtmpdb begins Thu Sep 25 15:25:44 2025

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part1]
└─$
```

Part 2

Task 1

```
#!/bin/bash
chmod 644 /etc/passwd
chmod 600 /etc/shadow
echo "File permissions corrected"
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part2]
└─$ chmod 600 task1.sh

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part2]
└─$ bash task1.sh
chmod: changing permissions of '/etc/passwd': Operation not permitted
chmod: changing permissions of '/etc/shadow': Operation not permitted
File permissions corrected

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part2]
└─$ sudo bash task1.sh
File permissions corrected

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part2]
└─$
```

Task 2

```
#!/bin/bash
FAILURES=$(grep "Failed password" /var/log/auth.log | tail -n 10 | wc -1)
if [ $FAILURES -gt 3 ]; then
        echo "Alert: More than 3 failed login attempts"
fi
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part2]
└─$ grep "Failed password" /var/log/auth.log | tail -n 10 | wc -l
grep: /var/log/auth.log: No such file or directory
0
```

Task 3

```
#!/bin/bash
USER="testuser"
if id "$USER" &>/dev/null; then
        echo "User '$USER' exists";
else
        sudo useradd -m "$USER" && echo "User '$USER' created";
fi

LAST_LOGIN=$(lastlog2 -u testuser | tail -n1 | grep -o '\*\*Never logged in\*\*')
if [ "$LAST_LOGIN" == "**Never logged in**" ]; then
        sudo usermod -L $USER
        echo "User $USER disabled"
fi
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part2]
└─$ bash task3.sh
User 'testuser' exists
User testuser disabled

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part2]
└─$
```

Task 4

```
#!/bin/bash
tail -n 10 /var/log/auth.log | grep sudo
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part2]
└─$ bash task4.sh
tail: cannot open '/var/log/auth.log' for reading: No such file or directory
```

Kali does not have auth.log, distribution issues

Part 3

Task 1

```
#!/bin/bash
BACKUP_DIR="/tmp/etc_backup"
WRITE="/tmp/world_writable.txt"
REPORT="/tmp/security_report.txt"

for file in "$WRITE" "$REPORT"; do
        if [ ! -f "$file" ]; then
                echo "File $file not exist, create file"
                touch "$file"
        else
                echo "File $file exist"
        fi
done

mkdir -p $BACKUP_DIR
sudo cp -r /etc/* $BACKUP_DIR
find /home -type f -perm -o+w 2>/dev/null > /tmp/world_writable.txt
echo "Backup and security scan complete" > /tmp/security_report.txt
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part3]
└─$ bash task1.sh
File /tmp/world_writable.txt exist
File /tmp/security_report.txt exist

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part3]
└─$ cat /tmp/world_writable.txt

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part3]
└─$ cat /tmp/security_report.txt
Backup and security scan complete

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part3]
└─$
```

Task 2

```
#!/bin/bash
grep -i "error\|fail\|unauthorized" /var/log/auth.log > /tmp/suspicious_activity.log
echo "Suspicioud activities saved to /tmp/suspicious_activity.log"
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part3]
└─$ bash task2.sh
grep: /var/log/auth.log: No such file or directory
Suspicioud activities saved to /tmp/suspicious_activity.log
```

Auth.log does not exist on kali

Task 3

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part3]
└─$ bash task3.sh
no crontab for kali - using an empty one
/usr/bin/select-editor: 12: cannot create /home/kali/.selected_editor: Permission denied
Unable to create directory /home/kali/.local/share/nano/: Permission denied
It is required for saving/loading search history or cursor positions.

crontab: installing new crontab
```

Task 4

```
#!/bin/bash
SUMMARY="/tmp/security_summary.txt"

echo "Security Summary: " > $SUMMARY
wc -l /tmp/world_writable.txt >> $SUMMARY
wc -l /tmp/suspicious_activity.log >> $SUMMARY
echo "Summary saved to: '$SUMMARY'"
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part3]
└─$ bash task1.sh
File /tmp/world_writable.txt not exist, create file
File /tmp/security_report.txt not exist, create file

┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part3]
└─$ bash task4.sh
Summary saved to: '/tmp/security_summary.txt'
```

Part 4

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part4]
└─$ sudo bash enforce_policy.sh
Enforcing Security Policy
Changing Home directories permissions
Password Requirement applying
Last 3 password non reusable
Password aging limit
Update PAM...
File & directory permissions
default umasks
Enabling account monitoring
SElinux enforcing mode
SELinux is already in enforcing mode.
Done
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part4]
└─$ sudo cat /var/log/secure
Username         Port     From                                Latest
alice            tty8     :1                                  Fri Oct  3 00:21:03 -0700 2025
kali             tty7     :0                                  Fri Oct  3 09:24:26 -0700 2025
lightdm          tty7     :0                                  Fri Oct  3 09:24:21 -0700 2025
```

```
┌──(kali㉿dhcp-10-65-64-234)-[~/bash_lab/part4]
└─$ cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1759515775.757:1): op=start ver=4.1.2 format=enriched kernel=6.12.38+kali-amd64 auid=429
4967295 pid=52366 uid=0 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=successAUID="unset" UID="root"
type=SERVICE_START msg=audit(1759515775.761:6152): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r
:init_t:s0 msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'U
ID="root" AUID="unset"
type=USER_END msg=audit(1759515775.769:6153): pid=52360 uid=1000 auid=1000 ses=1 subj=unconfined_u:unconfined_r:unco
nfined_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_limits,pam_permit,pam_umask,pam_unix,pam_winbind acct
="root" exe="/usr/bin/sudo" hostname=dhcp-10-65-64-234 addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=CRED_DISP msg=audit(1759515775.769:6154): pid=52360 uid=1000 auid=1000 ses=1 subj=unconfined_u:unconfined_r:unc
onfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo" hostname=dhcp-10-65
-64-234 addr=? terminal=/dev/pts/0 res=success'UID="kali" AUID="kali"
type=AVC msg=audit(1759515775.793:6155): avc:  denied  { read } for  pid=52382 comm="auditctl" name="audit" dev="sda
1" ino=1177464 scontext=system_u:system_r:auditctl_t:s0 tcontext=system_u:object_r:auditd_log_t:s0 tclass=dir permis
sive=1
type=SYSCALL msg=audit(1759515775.793:6155): arch=c000003e syscall=257 success=yes exit=5 a0=ffffff9c a1=5589f67cd42
0 a2=90800 a3=0 items=0 ppid=52381 pid=52382 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:auditctl_t:s0 key=(null)A
RCH=x86_64 SYSCALL=openat AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="
root" FSGID="root"
type=PROCTITLE msg=audit(1759515775.793:6155): proctitle=617564697463746C002D73
type=AVC msg=audit(1759515775.793:6156): avc:  denied  { read } for  pid=52382 comm="auditctl" name="audit.log" dev=
"sda1" ino=1177431 scontext=system_u:system_r:auditctl_t:s0 tcontext=system_u:object_r:auditd_log_t:s0 tclass=file p
ermissive=1
type=AVC msg=audit(1759515775.793:6156): avc:  denied  { open } for  pid=52382 comm="auditctl" path="/var/log/audit/
audit.log" dev="sda1" ino=1177431 scontext=system_u:system_r:auditctl_t:s0 tcontext=system_u:object_r:auditd_log_t:s
0 tclass=file permissive=1
type=SYSCALL msg=audit(1759515775.793:6156): arch=c000003e syscall=257 success=yes exit=5 a0=ffffffffffffff9c a1=7ff
f18f2a59b a2=0 a3=0 items=0 ppid=52381 pid=52382 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsg
id=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:auditctl_t:s0 key=(nu
ll)ARCH=x86_64 SYSCALL=openat AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SG
ID="root" FSGID="root"
type=PROCTITLE msg=audit(1759515775.793:6156): proctitle=617564697463746C002D73
type=CONFIG_CHANGE msg=audit(1759515775.797:6157): op=set audit_backlog_limit=8192 old=8192 auid=4294967295 ses=4294
967295 subj=system_u:system_r:auditctl_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1759515775.797:6157): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffcb25f8ce0 a2=3c
 a3=0 items=0 ppid=52370 pid=52386 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none
) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:auditctl_t:s0 key=(null)ARCH=x86_64
 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGI
D="root"
type=PROCTITLE msg=audit(1759515775.797:6157): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F6
1756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1759515775.797:6158): op=set audit_failure=1 old=1 auid=4294967295 ses=4294967295 subj=
system_u:system_r:auditctl_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1759515775.797:6158): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffcb25f8cf0 a2=3c
 a3=0 items=0 ppid=52370 pid=52386 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none
```

Part 5