SOURCE CODE FILE

```
========================================
BRUTE FORCE ATTACK ANALYSIS - SOURCE CODE
========================================
Environment: Kali Linux
Logs: CentOS SSH authentication logs (secure files)
----------------------------------------
```

1. Navigation and Directory Setup

```
cd ~/Downloads
cd ~/Downloads/bruteforce
cd ~/Downloads/bruteforce/securelogs
ls
```

---

2. Extract All Usernames From Failed SSH Logins

```
grep "Failed password for" secure* | grep -v "invalid user" | awk '{print
$9}' > usernames.log
```

To verify:

```
cat usernames.log
```

---

3. Extract All Invalid Usernames

```
grep "Invalid user" secure* | awk '{print $8}' | sort -u > abc.txt
```

Verify:

```
cat abc.txt
```

---

4. Cross-Reference Script (testtheusers_1.sh)

FINAL WORKING VERSION (safe, correct, no formatting errors)

```
#!/bin/bash

while read user; do
    if grep -q "^$user:" /etc/passwd; then
        echo "EXISTS: $user"
    else
        echo "NOT FOUND: $user"
    fi
done < abc.txt
```

---

5. Create Script Automatically (to avoid nano formatting issues)

(This is the exact fix used to generate a clean script.)

```
printf '%s\n' '#!/bin/bash' '' 'while read user; do' '    if grep -q
"^$user:" /etc/passwd; then' '        echo "EXISTS: $user"' '    else' '
echo "NOT FOUND: $user"' '    fi' 'done < abc.txt' > testtheusers_1.sh
```

---

6. Make Script Executable

```
chmod +x testtheusers_1.sh
```

---

7. Run Script

```
./testtheusers_1.sh
```

---

8. Optional Analysis Commands (Used During Investigation)

Count number of failed brute-force attempts:

```
grep -i "Failed password" secure* | wc -l
```

Show attacker IPs:

```
grep "Failed password for" secure* | awk '{print $11}' | sort -u
```

Show frequency of login attempts per username:

```
grep "Failed password" secure* | awk '{print $9}' | sort | uniq -c
```

Show all lines containing failed SSH logins:

```
grep -i "failed" secure*
```

---

9. Security Hardening Configuration (DOCUMENTATION ONLY – NOT EXECUTED)

These are entries for `/etc/ssh/sshd_config`:

```
PermitRootLogin no
```

```
PasswordAuthentication no
```

Restart SSH service (for documentation only):

```
sudo systemctl restart sshd
```