Security & Access Troubleshooting Case Studies for CloudOps Engineers

10 Real-world Linux Security and Access Control Scenarios with Commands, Logs, and Resolutions

Case 1: SSH Key Authentication Failure

Problem: User unable to log in using SSH key on production node.
Investigation:

```
$ ssh -v user@server
debug1: Offering public key: id_rsa RSA SHA256:abc...
debug1: Authentications that can continue: password
$ ls -ld ~/.ssh && ls -l ~/.ssh/authorized_keys
Permissions incorrect on .ssh directory
```

Root Cause: Incorrect file permissions on .ssh directory prevented SSH key auth.
Resolution: Fixed permissions with `chmod 700 ~/.ssh` and `chmod 600 ~/.ssh/authorized_keys`.
Prevention: Ensure correct SSH permissions during provisioning with automation scripts.

Case 2: Locked User Account (PAM Policy)

Problem: Developer unable to log in; message: 'Account locked due to too many login failures'.
Investigation:

```
$ pam_tally2 --user devuser
Login Failures: 5 Denied access
$ faillock --user devuser
```

Root Cause: Account automatically locked by PAM after consecutive failed attempts.
Resolution: Unlocked using `pam_tally2 --user devuser --reset`.
Prevention: Configure PAM faillock policy thresholds appropriately for internal accounts.

Case 3: Incorrect File Permissions Breaking Service Startup

Problem: Nginx service failed to start after recent deployment.
Investigation:

```
$ systemctl status nginx
nginx: [emerg] open() '/var/www/html/index.html' failed (13: Permission denied)
$ ls -l /var/www/html
```

Root Cause: File permissions too restrictive for Nginx user.
Resolution: Updated ownership with `chown -R nginx:nginx /var/www/html`.
Prevention: Implement deployment checks for file permissions.

Case 4: Sudo Access Revoked Unexpectedly

Problem: Admin user unable to run sudo commands: 'is not in the sudoers file'.
Investigation:

```
$ su - root
$ visudo
User entry missing in /etc/sudoers
```

Root Cause: Sudoers entry removed during configuration management run.
Resolution: Re-added user to /etc/sudoers or admin group.
Prevention: Automate sudoers management through Ansible with validation checks.

Case 5: SELinux Denial Preventing Web Service Access

Problem: Web app returned 403 errors even with correct file permissions.
Investigation:

```
$ ausearch -m avc -ts recent
type=AVC msg=audit(1719.3:231): denied { read } for pid=2134 comm='nginx'
name='index.html'
$ getenforce
```

Root Cause: SELinux context on web directory mismatched expected policy.
Resolution: Restored context with `restorecon -Rv /var/www/html`.
Prevention: Add SELinux context restore step to deployment pipelines.

Case 6: Firewalld Blocking Required Port

Problem: New service unreachable externally though running locally.
Investigation:

```
$ ss -tuln | grep 8080
LISTEN 0 128 *:8080 *:*
$ firewall-cmd --list-all | grep 8080
```

Root Cause: Firewalld missing port rule for application service.
Resolution: Added rule with `firewall-cmd --permanent --add-port=8080/tcp && firewall-cmd --reload`.
Prevention: Document all required ports in service onboarding checklists.

Case 7: Expired SSL Certificate on Production Site

Problem: HTTPS requests failed with certificate expiration error.
Investigation:

```
$ openssl x509 -in /etc/ssl/certs/app.crt -noout -enddate
notAfter=Sep 29 12:00:00 2025 GMT
```

Root Cause: Expired SSL certificate not renewed before expiration date.
Resolution: Renewed certificate via Let's Encrypt and reloaded web server.
Prevention: Implement automatic certificate renewal and monitoring alerts.

Case 8: Cron Job Failing Due to Restricted PATH

Problem: Cron job running script failed: 'command not found'.
Investigation:

```
$ grep CRON /var/log/syslog
sh: myscript.sh: command not found
$ crontab -l
```

Root Cause: Cron environment lacked PATH to custom binaries.
Resolution: Added full path to script or PATH variable in crontab entry.
Prevention: Always define absolute paths in cron jobs to avoid environment issues.

Case 9: Auditd Log Rotation Failure

Problem: Audit logs consumed full disk space on system partition.
Investigation:

```
$ ls -lh /var/log/audit
audit.log 25G
$ systemctl status auditd
```

Root Cause: Auditd log rotation misconfigured, preventing automatic cleanup.
Resolution: Manually rotated and updated `/etc/audit/auditd.conf` to enable rotation.

Prevention: Monitor disk space usage and validate logrotate configurations.

Case 10: Rootkit Detection and Recovery

Problem: Strange network connections found on production VM.
Investigation:

```
$ netstat -antp | grep ESTABLISHED
$ chkrootkit
Warning: Suspicious file '/usr/bin/ssh2'
```

Root Cause: Rootkit infection altered system binaries.
Resolution: Isolated system, reinstalled clean OS image, and restored from verified backups.
Prevention: Enforce image integrity checks and centralized security scanning.