# Audits User accounts and permissions in a simulated environment

### Findings from the user account and permissions audits

### Summary of Audit

A review of the RBAC (Role-Based Access Control) environment setup at Basetech Corp revealed several issues related to user group memberships, directory ownership, and file permissions. These findings highlight both intentional misconfigurations (for demonstration) and potential security risks if applied in a production setting.

### Detailed Findings

### User Accounts and Group Memberships

- Correct groups `admin`, `staff`, and `guest` were created.
- Users were assigned appropriately to their primary groups.
- However:
    - **Cross-department group memberships were added:**
        - `susan_guest` (a guest user) was added to the `guest` group again (potentially redundant).
        - `fatima_admin` (an admin user) was added to the `guest` group, which may violate role segregation policies.

### Directory Ownership and Permissions

- Department directories were created under `/company/`:
    - `/company/admin` owned by `root:admin`, permission `770` ✅
    - `/company/staff` owned by `root:staff`, permission `770` ✅
    - **/company/guest was initially owned by `root:guest`, but then changed to `jude_admin` (an admin user)** ❌
        - This is a violation of least privilege principles and role boundaries.

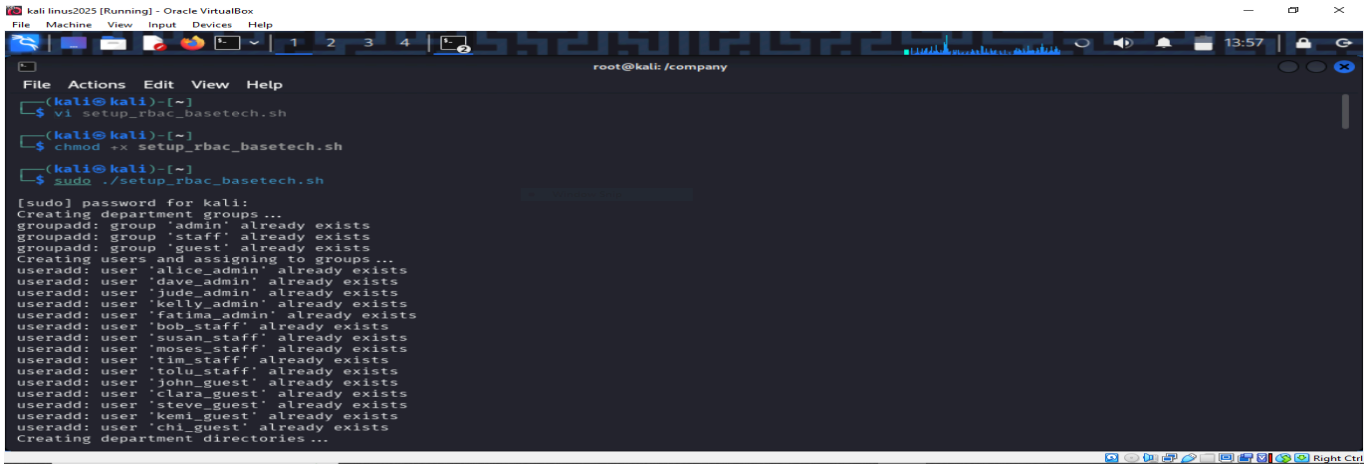
**File Permissions**

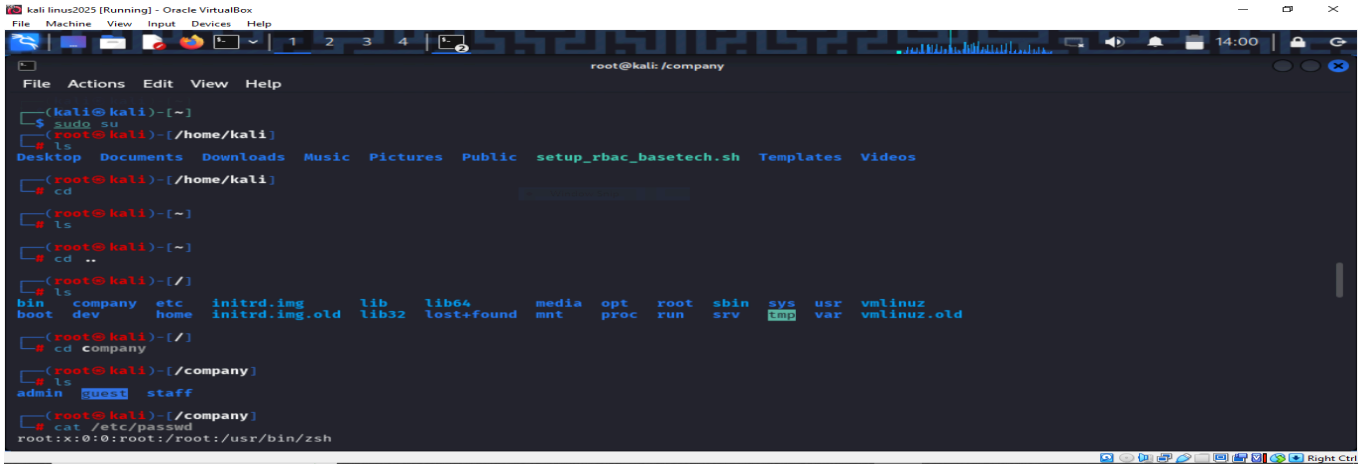
- Departmental files were created appropriately, but permissions were overly permissive in several places:

    1. **`/company/guest` folder set to `777` (world-readable, writable, and executable) ❌**
        - This allows any user to read, modify, or delete files within.
    2. **`/company/staff` set to `755` (world-readable) ❌**
        - Allows all users to read staff review files, breaching confidentiality.
    3. **`/company/admin/source_code.py` set to `666` (world-readable and writable) ❌**
        - High-risk — any user can modify critical code files.

**Summary of Misconfigurations**

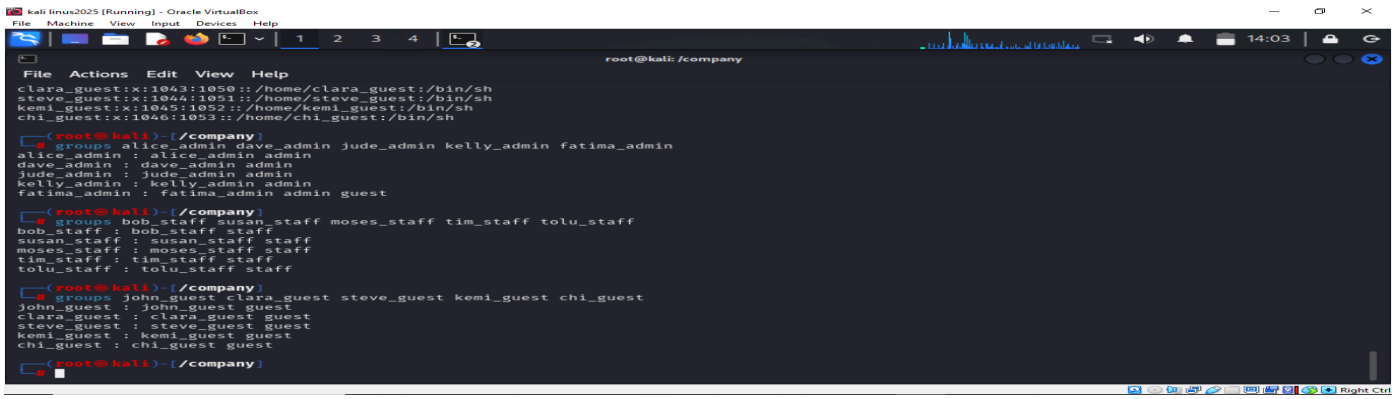
| Issue | Description | Impact |
|---|---|---|
| Directory Ownership | `/company/guest` owned by `jude_admin` | Bypasses department boundaries |
| Overly Permissive Folder | `/company/guest` permission `777` | Allows all users full access |
| Overly Permissive Folder | `/company/staff` permission `755` | Exposes sensitive staff files |
| Overly Permissive File | `/company/admin/source_code.py` permission `666` | Allows unauthorized code changes |
| Inconsistent Group Membership | `fatima_admin` in `guest` group | Breaks separation of duties |

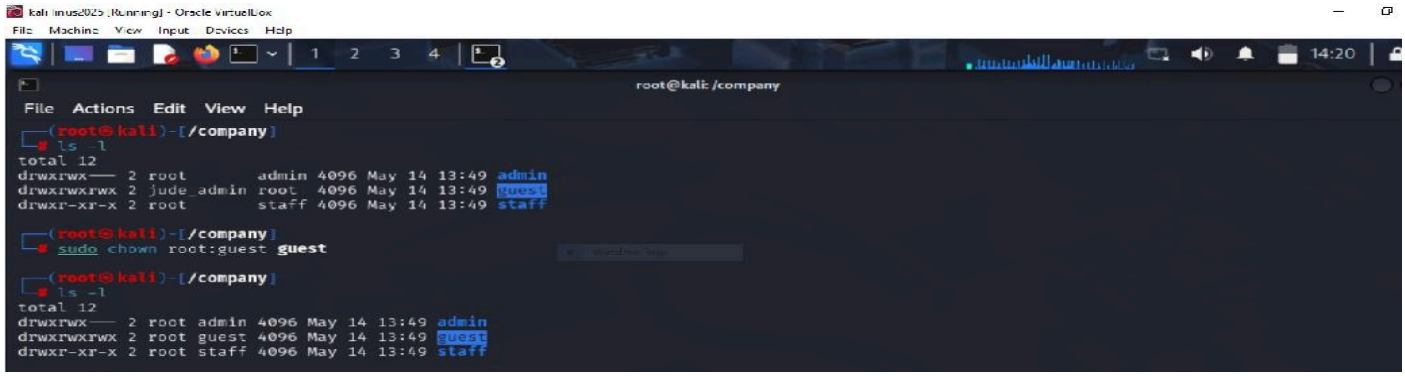

kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
13:57
root@kali: /company
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ vi setup_rbac_basetech.sh
┌──(kali㉿kali)-[~]
└─$ chmod +x setup_rbac_basetech.sh
┌──(kali㉿kali)-[~]
└─$ sudo ./setup_rbac_basetech.sh
[sudo] password for kali:
Creating department groups...
groupadd: group 'admin' already exists
groupadd: group 'staff' already exists
groupadd: group 'guest' already exists
Creating users and assigning to groups...
useradd: user 'alice_admin' already exists
useradd: user 'dave_admin' already exists
useradd: user 'jude_admin' already exists
useradd: user 'kelly_admin' already exists
useradd: user 'fatima_admin' already exists
useradd: user 'bob_staff' already exists
useradd: user 'susan_staff' already exists
useradd: user 'moses_staff' already exists
useradd: user 'tim_staff' already exists
useradd: user 'tolu_staff' already exists
useradd: user 'john_guest' already exists
useradd: user 'clara_guest' already exists
useradd: user 'steve_guest' already exists
useradd: user 'kemi_guest' already exists
useradd: user 'chi_guest' already exists
Creating department directories...
Right Ctrl

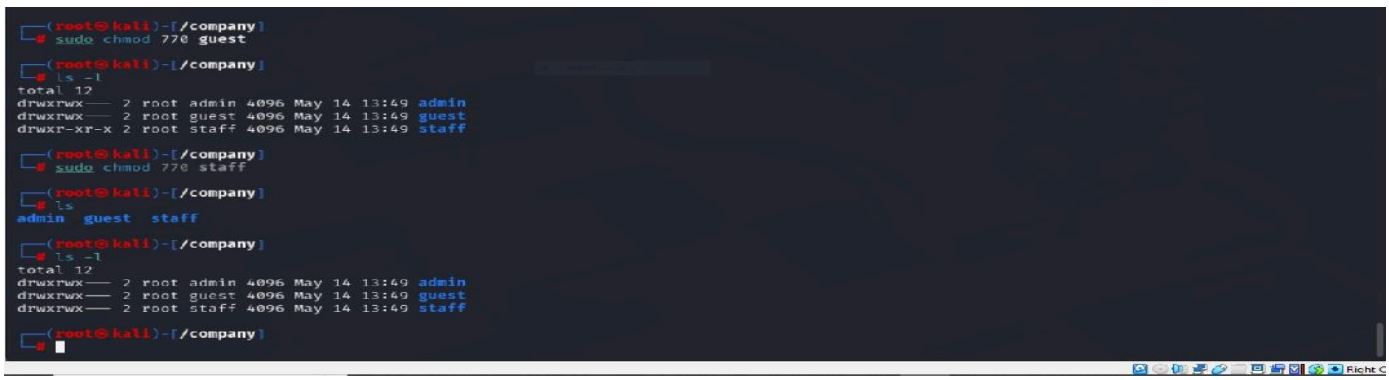

kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
14:00
root@kali: /company
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop Documents Downloads Music Pictures Public setup_rbac_basetech.sh Templates Videos
┌──(root㉿kali)-[/home/kali]
└─# cd
┌──(root㉿kali)-[~]
└─# ls
┌──(root㉿kali)-[~]
└─# cd ..
┌──(root㉿kali)-[/]
└─# ls
bin company etc initrd.img lib lib64 media opt root sbin sys usr vmlinuz
boot dev home initrd.img.old lib32 lost+found mnt proc run srv tmp var vmlinuz.old
┌──(root㉿kali)-[/]
└─# cd company
┌──(root㉿kali)-[/company]
└─# ls
admin guest staff
┌──(root㉿kali)-[/company]
└─# cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
Right Ctrl


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
14:02
root@kali: /company
File Actions Edit View Help
┌──(root㉿kali)-[/]
└─# ls
bin company etc initrd.img lib lib64 media opt root sbin sys usr vmlinuz
boot dev home initrd.img.old lib32 lost+found mnt proc run srv tmp var vmlinuz.old
┌──(root㉿kali)-[/]
└─# cd company
┌──(root㉿kali)-[/company]
└─# ls
admin guest staff
┌──(root㉿kali)-[/company]
└─# 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
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
Right Ctrl


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
14:02
root@kali: /company
File Actions Edit View Help
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
_gophish:x:104:105::/var/lib/gophish:/usr/sbin/nologin
iodine:x:105:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:106:106::/nonexistent:/usr/sbin/nologin
tcpdump:x:107:107::/nonexistent:/usr/sbin/nologin
miredo:x:108:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin
redis:x:110:110::/var/lib/redis:/usr/sbin/nologin
mosquitto:x:111:113::/var/lib/mosquitto:/usr/sbin/nologin
redsocks:x:112:114::/var/run/redsocks:/usr/sbin/nologin
stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
Debian-snmp:x:114:115::/var/lib/snmp:/bin/false
sslh:x:115:117::/nonexistent:/usr/sbin/nologin
postgres:x:116:118:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:117:119:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
Right Ctrl


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
14:03
root@kali: /company
File Actions Edit View Help
clara_guest:x:1043:1050::/home/clara_guest:/bin/sh
steve_guest:x:1044:1051::/home/steve_guest:/bin/sh
kemi_guest:x:1045:1052::/home/kemi_guest:/bin/sh
chi_guest:x:1046:1053::/home/chi_guest:/bin/sh
┌──(root㉿kali)-[/company]
└─# groups alice_admin dave_admin jude_admin kelly_admin fatima_admin
alice_admin : alice_admin admin
dave_admin : dave_admin admin
jude_admin : jude_admin admin
kelly_admin : kelly_admin admin
fatima_admin : fatima_admin admin guest
┌──(root㉿kali)-[/company]
└─# groups bob_staff susan_staff moses_staff tim_staff tolu_staff
bob_staff : bob_staff staff
susan_staff : susan_staff staff
moses_staff : moses_staff staff
tim_staff : tim_staff staff
tolu_staff : tolu_staff staff
┌──(root㉿kali)-[/company]
└─# groups john_guest clara_guest steve_guest kemi_guest chi_guest
john_guest : john_guest guest
clara_guest : clara_guest guest
steve_guest : steve_guest guest
kemi_guest : kemi_guest guest
chi_guest : chi_guest guest
┌──(root㉿kali)-[/company]
└─#
Right Ctrl


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
14:20
root@kali: /company
File Actions Edit View Help
┌──(root㉿kali)-[/company]
└─# ls -l
total 12
drwxrwx--- 2 root admin 4096 May 14 13:49 admin
drwxrwxrwx 2 jude_admin root 4096 May 14 13:49 guest
drwxr-xr-x 2 root staff 4096 May 14 13:49 staff
┌──(root㉿kali)-[/company]
└─# sudo chown root:guest guest
┌──(root㉿kali)-[/company]
└─# ls -l
total 12
drwxrwx--- 2 root admin 4096 May 14 13:49 admin
drwxrwxrwx 2 root guest 4096 May 14 13:49 guest
drwxr-xr-x 2 root staff 4096 May 14 13:49 staff


┌──(root㉿kali)-[/company]
└─# sudo chmod 770 guest
┌──(root㉿kali)-[/company]
└─# ls -l
total 12
drwxrwx--- 2 root admin 4096 May 14 13:49 admin
drwxrwx--- 2 root guest 4096 May 14 13:49 guest
drwxr-xr-x 2 root staff 4096 May 14 13:49 staff
┌──(root㉿kali)-[/company]
└─# sudo chmod 770 staff
┌──(root㉿kali)-[/company]
└─# ls
admin guest staff
┌──(root㉿kali)-[/company]
└─# ls -l
total 12
drwxrwx--- 2 root admin 4096 May 14 13:49 admin
drwxrwx--- 2 root guest 4096 May 14 13:49 guest
drwxrwx--- 2 root staff 4096 May 14 13:49 staff
┌──(root㉿kali)-[/company]
└─#

**Recommendations for addressing any misconfiguration**

1. **Restore correct ownership** of `/company/guest` to `root:guest`.
2. **Adjust permissions**:
    - `/company/guest` to `770`
    - `/company/staff` to `770`
    - `/company/admin/source_code.py` to `640`
3. **Review group memberships** and remove inappropriate cross-group assignments.
4. Implement **RBAC policy enforcement scripts** to detect and revert unauthorized changes.
5. Conduct **periodic audits** to maintain security posture

**Observations about the importance of regular audits:**

**Helps Identify Security Misconfigurations Early**: Regular audits allow administrators to catch mistakes like overly permissive file permissions, inappropriate user group memberships, or improper directory ownership before they can be exploited. In our recent audit, we identified several intentional misconfigurations that, if left unchecked, could have led to serious data leaks or unauthorized system changes.

**Enforces Compliance with Organizational Policies**: Every organization should have clearly defined RBAC (Role-Based Access Control) policies. Regular audits verify that these policies are consistently applied and enforced, helping

prevent privilege creep — where users accumulate access rights over time, increasing the attack surface.

**Supports Incident Response Readiness**: By maintaining a clear, up-to-date understanding of system configurations and access controls, regular audits improve an organization's ability to respond quickly to security incidents. Knowing who has access to what resources is crucial during a breach investigation.

**Provides Operational Assurance**: Audits ensure operational integrity by confirming that critical systems and sensitive files are only accessible by authorized personnel. This limits the risk of accidental modifications, intentional sabotage, or unauthorized disclosure.

**Aids in Regulatory Compliance**: Many industries are subject to regulatory frameworks (like GDPR, HIPAA, or ISO 27001) that mandate periodic access reviews and permission audits. Regular audits demonstrate due diligence and provide evidence of compliance during external assessments.

**Promotes a Culture of Accountability**: Knowing that audits occur regularly encourages system administrators and users to adhere to best practices. It cultivates a security-aware environment where permissions are granted and managed responsibly.

**Conclusion**

Regular user account and permissions audits are a critical component of good security hygiene. They not only help detect and correct misconfigurations but also reinforce organizational policy, support compliance efforts, and reduce the risk of insider and external threats.