CTF Writeup: SFTP Triple-Layer Access Control

This CTF demonstrates defense-in-depth through three independent access control mechanisms: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC). The flag is protected by all three layers simultaneously, requiring an attacker to bypass multiple security policies to gain access.

Flag details:

- Flag: FLAG{group_CS_triple_layer_victory}
- Location: /confidential/admin/secrets/.hidden/flag.txt
- Protection: Triple-layer (DAC ∧ MAC ∧ RBAC)

Design Rationale:

- Hidden directory (.hidden)
- Requires all 3 policies to allow
- Defense-in-depth approach

Protection Layers:

- DAC (Discretionary Access Control):
    - Owner: annie, Group: admins, Mode: 0o400
    - Only owner can read, no write allowed
- MAC (Mandatory Access Control):
    - Clearance levels: public < internal < confidential
    - Annie: confidential, James: internal, Bob: public
    - No read up, no write down
- RBAC (Role-Based Access Control):
    - Roles: intern, analyst, admin
    - /confidential/admin/* requires admin role
    - Only Annie has admin role

  Composition: Final = DAC ∧ MAC ∧ RBAC (all must allow)

Attack 1: Bob - Unauthorized Access

Objective: User with insufficient permissions attempts to read flag

```
Username: bob
Password:
Connecting to localhost:2222 as bob...
✓ SSH connection established
✓ Host key verified (TOFU)
✓ Password authentication successful
✓ SFTP subsystem started

=== SFTP session active ===
Available commands: pwd, ls [path], mkdir <path>, stat <path>, get <rpath> [lpath], put <lpath> <rpat
h>, quit
sftp> ls /confidential/admin/secrets/.hidden/
Error listing directory: DAC: DENY, other lacks permission on /confidential (mode=0o750) | MAC: DENY,
 no read up (public < confidential) | RBAC: DENY, no matching role permission
sftp> get /confidential/admin/secrets/.hidden/flag.txt
Error downloading file: DAC: DENY, other lacks permission on /confidential (mode=0o750) | MAC: DENY,
no read up (public < confidential) | RBAC: DENY, no matching role permission
sftp> quit
Exiting SFTP session.
```

Result: BLOCKED by all three layers

- DAC: other lacks permission (mode=0o750)
- MAC: no read up (public < confidential)
- RBAC: no admin role

Audit Evidence: {"user": "bob", "operation": "read", "path": "...flag.txt", "allowed": false, "reason": "DAC: DENY... | MAC: DENY... | RBAC: DENY..."}

Attack 2: James - Role Violation

Objective: Analyst attempts to access admin-only resource

```
Username: james
Password:
Connecting to localhost:2222 as james...
✓ SSH connection established
✓ Host key verified (TOFU)
✓ Password authentication successful
✓ SFTP subsystem started

=== SFTP session active ===
Available commands: pwd, ls [path], mkdir <path>, stat <path>, get <rpath> [lpath], put <lpath> <rpat
h>, quit
sftp> ls /confidential/admin/secrets/.hidden/
Error listing directory: DAC: DENY, other lacks permission on /confidential (mode=0o750) | MAC: DENY,
 no read up (internal < confidential) | RBAC: DENY, no matching role permission
sftp> get /confidential/admin/secrets/.hidden/flag.txt
Error downloading file: DAC: DENY, other lacks permission on /confidential (mode=0o750) | MAC: DENY,
no read up (internal < confidential) | RBAC: DENY, no matching role permission
sftp> quit
Exiting SFTP session.
```

Result: BLOCKED

- DAC: other lacks permission
- MAC: no read up (internal < confidential)
- RBAC: lacks admin role

Audit Evidence: {"user": "james", "operation": "read", "path": "...flag.txt", "allowed": false, "reason": "..."}

Attack 3: Bob - Path Traversal

Objective: Bypass jail using /../ sequences

```
Username: bob
Password:
Connecting to localhost:2222 as bob...
✓ SSH connection established
✓ Host key verified (TOFU)
✓ Password authentication successful
✓ SFTP subsystem started

=== SFTP session active ===
Available commands: pwd, ls [path], mkdir <path>, stat <path>, get <rpath> [lpath], put <lpath> <rpat
h>, quit
sftp> get /../confidential/admin/secrets/.hidden/flag.txt
Error downloading file: DAC: DENY, no matching rule for path | MAC: DENY, no read up (public < confid
ential) | RBAC: DENY, no matching role permission
sftp> get /./../../confidential/admin/secrets/.hidden/flag.txt
Error downloading file: DAC: DENY, no matching rule for path | MAC: DENY, no read up (public < confid
ential) | RBAC: DENY, no matching role permission
sftp> quit
Exiting SFTP session.
```

Mitigation: safe_join() function:

- Normalizes paths
- Resolves .. and symlinks
- Ensures result stays within jail root

Result: BLOCKED - path canonicalization prevents escape

Successful Access: Annie

```
Username: annie
Password:
Connecting to localhost:2222 as annie...
✓ SSH connection established
✓ Host key verified (TOFU)
✓ Password authentication successful
✓ SFTP subsystem started

=== SFTP session active ===
Available commands: pwd, ls [path], mkdir <path>, stat <path>, get <rpath> [lpath], put <lpath> <rpat
h>, quit
sftp> get /confidential/admin/secrets/.hidden/flag.txt ./flag_annie.txt
Downloaded '/confidential/admin/secrets/.hidden/flag.txt' to './flag_annie.txt'
sftp> quit
Exiting SFTP session.
```

```
cat flag_annie.txt
```

```
FLAG{group_CS_triple_layer_victory}
```

Authorization Success:

- MAC: confidential clearance
- DAC: file owner with read permission
- RBAC: admin role

Audit Trial:

```
{"timestamp": "2025-11-17T17:10:46.996522", "user": "annie", "operation": "read", "path": "<file>", "
allowed": false, "reason": "DAC: DENY, no matching rule for path | MAC: ALLOW | RBAC: DENY, no matchi
ng role permission"}
{"timestamp": "2025-11-17T17:10:46.997512", "user": "annie", "operation": "read", "path": "<file>", "
allowed": false, "reason": "DAC: DENY, no matching rule for path | MAC: ALLOW | RBAC: DENY, no matchi
ng role permission"}
{"timestamp": "2025-11-17T17:11:53.788552", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-17T17:11:53.796334", "user": "annie", "operation": "read", "path": "<file>", "
allowed": false, "reason": "DAC: DENY, no matching rule for path | MAC: ALLOW | RBAC: DENY, no matchi
ng role permission"}
{"timestamp": "2025-11-17T17:11:53.796848", "user": "annie", "operation": "read", "path": "<file>", "
allowed": false, "reason": "DAC: DENY, no matching rule for path | MAC: ALLOW | RBAC: DENY, no matchi
ng role permission"}
{"timestamp": "2025-11-17T22:14:26.809980", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-17T22:20:46.541846", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-17T22:20:46.555322", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-17T22:20:46.558822", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-17T22:20:46.563031", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-17T22:20:46.568694", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-17T22:20:46.572098", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-17T22:22:00.647519", "user": "bob", "operation": "list", "path": "/confidentia
l\\admin\\secrets\\.hidden", "allowed": false, "reason": "DAC: DENY, other lacks permission on /confi
dential (mode=0o750) | MAC: DENY, no read up (public < confidential) | RBAC: DENY, no matching role p
ermission"}
```

```
{"timestamp": "2025-11-17T22:22:06.411685", "user": "bob", "operation": "read", "path": "/confidentia
l\\admin\\secrets\\.hidden\\flag.txt", "allowed": false, "reason": "DAC: DENY, other lacks permission
 on /confidential (mode=0o750) | MAC: DENY, no read up (public < confidential) | RBAC: DENY, no match
ing role permission"}
{"timestamp": "2025-11-17T22:22:30.475054", "user": "james", "operation": "list", "path": "/confident
ial\\admin\\secrets\\.hidden", "allowed": false, "reason": "DAC: DENY, other lacks permission on /con
fidential (mode=0o750) | MAC: DENY, no read up (internal < confidential) | RBAC: DENY, no matching ro
le permission"}
{"timestamp": "2025-11-17T22:22:35.901627", "user": "james", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": false, "reason": "DAC: DENY, other lacks permissi
on on /confidential (mode=0o750) | MAC: DENY, no read up (internal < confidential) | RBAC: DENY, no m
atching role permission"}
{"timestamp": "2025-11-17T22:23:19.422058", "user": "bob", "operation": "read", "path": "/..\\confide
ntial\\admin\\secrets\\.hidden\\flag.txt", "allowed": false, "reason": "DAC: DENY, no matching rule f
or path | MAC: DENY, no read up (public < confidential) | RBAC: DENY, no matching role permission"}
{"timestamp": "2025-11-17T22:23:31.139518", "user": "bob", "operation": "read", "path": "/..\\..\\con
fidential\\admin\\secrets\\.hidden\\flag.txt", "allowed": false, "reason": "DAC: DENY, no matching ru
le for path | MAC: DENY, no read up (public < confidential) | RBAC: DENY, no matching role permission
"}
{"timestamp": "2025-11-18T02:47:26.916459", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-18T02:47:26.952208", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-18T02:47:26.953585", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-18T02:47:26.956033", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-18T02:47:26.958399", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-18T02:47:26.959180", "user": "annie", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": true, "reason": "Allowed by all policies"}
{"timestamp": "2025-11-18T02:48:16.251351", "user": "bob", "operation": "list", "path": "/confidentia
l\\admin\\secrets\\.hidden", "allowed": false, "reason": "DAC: DENY, other lacks permission on /confi
dential (mode=0o750) | MAC: DENY, no read up (public < confidential) | RBAC: DENY, no matching role p
ermission"}
```

```
{"timestamp": "2025-11-18T02:48:21.074660", "user": "bob", "operation": "read", "path": "/confidentia
l\\admin\\secrets\\.hidden\\flag.txt", "allowed": false, "reason": "DAC: DENY, other lacks permission
 on /confidential (mode=0o750) | MAC: DENY, no read up (public < confidential) | RBAC: DENY, no match
ing role permission"}
{"timestamp": "2025-11-18T02:48:56.315350", "user": "james", "operation": "list", "path": "/confident
ial\\admin\\secrets\\.hidden", "allowed": false, "reason": "DAC: DENY, other lacks permission on /con
fidential (mode=0o750) | MAC: DENY, no read up (internal < confidential) | RBAC: DENY, no matching ro
le permission"}
{"timestamp": "2025-11-18T02:49:01.505315", "user": "james", "operation": "read", "path": "/confident
ial\\admin\\secrets\\.hidden\\flag.txt", "allowed": false, "reason": "DAC: DENY, other lacks permissi
on on /confidential (mode=0o750) | MAC: DENY, no read up (internal < confidential) | RBAC: DENY, no m
atching role permission"}
{"timestamp": "2025-11-18T02:49:33.557582", "user": "bob", "operation": "read", "path": "/..\\confide
ntial\\admin\\secrets\\.hidden\\flag.txt", "allowed": false, "reason": "DAC: DENY, no matching rule f
or path | MAC: DENY, no read up (public < confidential) | RBAC: DENY, no matching role permission"}
{"timestamp": "2025-11-18T02:49:39.169001", "user": "bob", "operation": "read", "path": "/..\\..\\con
fidential\\admin\\secrets\\.hidden\\flag.txt", "allowed": false, "reason": "DAC: DENY, no matching ru
le for path | MAC: DENY, no read up (public < confidential) | RBAC: DENY, no matching role permission
"}
```


Complete audit trail in data/audit_policy.jsonl shows:

- Annie's successful access (allowed: true)
- Bob's denied attempts (allowed: false)
- James's denied attempts (allowed: false)
- All decisions logged with timestamps and reasons

Conclusion

Defense-in-depth successfully protected the flag:

- 3 independent security layers (stronger than single-layer security)
- Each layer alone would block unauthorized access (default deny prevents unexpected access)
- Audit trail provides complete visibility
- Authorized user (Annie) can access as intended