Auditing and Configuring Security in a Simulated Enterprise Environment

Nestor Alzate Mejia[1], Cano Beltrán, Jhon Haide[1]
nestor.alzatem@campusucc.edu.co ; jhon.canob@campusucc.edu.co,

1. Research Professor, Faculty of Engineering – Cali Campus
ESLINGA Research Group
Universidad Cooperativa de Colombia

Problem Description: This laboratory introduces students to the design, configuration, and auditing of Authentication, Authorization, and Accounting (AAA) services using the TACACS+ and RADIUS protocols within a Cisco Packet Tracer environment. AAA protocols are critical for strengthening access control in enterprise networks by centralizing identity management and ensuring accountability through activity logging.
The case study involves NetBank Ltd., a fictitious financial services company that has outgrown the limitations of traditional local passwords. The organization seeks to transition toward a centralized AAA solution to mitigate risks such as shared credentials, lack of access traceability, and limited administrative control. Students will configure routers to authenticate against TACACS+ and RADIUS servers, verify redundancy through local accounts, and audit system responses under normal and attack conditions.

Requirement:

NetBank Ltd., a mid-sized financial institution with three branch offices:
- Currently relies on local router passwords shared by multiple administrators.
- Issues: no traceability, ex-employees retaining access.
- Management requires migration to centralized AAA.

Requirements:
- Router R2 authenticates via TACACS+ server (192.168.2.2).
- Router R3 authenticates via RADIUS server (192.168.3.2).
- Local fallback accounts: Admin2 (R2), Admin3 (R3).
- Students must configure, validate, and audit results.

Phase 1 – TACACS+ on R2:
- Verify connectivity with ping.
- Configure local fallback Admin2.

- Configure TACACS+ server IP and key.
- Enable AAA new-model and define TACACS+ group.
- Apply AAA to console and VTY.
- Test login with remote and fallback accounts.

Phase 2 – RADIUS on R3:
- Configure local fallback Admin3.
- Configure RADIUS server IP and secret.
- Enable AAA with RADIUS.
- Apply AAA to console and VTY.
- Test login with valid and invalid credentials.

Phase 3 – Auditing:
- Attempt invalid logins, record responses.
- Check AAA server logs.
- Compare TACACS+ vs RADIUS log detail.

Guiding Questions

1. What risks arise if fallback local accounts are unmanaged?
2. Why does TACACS+ encrypt the entire payload but RADIUS only the password?
3. How does AAA support compliance frameworks?
4. What happens if AAA servers fail and no fallback exists?
5. In which scenarios is RADIUS more suitable than TACACS+?
6. How do AAA logs enhance accountability?
7. What recommendations would you make to NetBank's CISO?

Expected Outcomes

1. AAA Configurations – Verified running-config snippets from R2 (TACACS+) and R3 (RADIUS) demonstrating correct method lists, server definitions, and fallback users.
2. Connectivity Proofs – ICMP reachability evidence and screenshots of successful AAA server communication.
3. Authentication Test Matrix – Table of test cases (valid, invalid, fallback) with expected vs. observed results.
4. Log Collection & Analysis – TACACS+ and RADIUS logs exported, highlighting failed logins, privilege attempts, and user attribution.
5. Comparative Findings – Narrative comparing TACACS+ vs RADIUS features, encryption coverage, and audit suitability.
6. Recommendations Report – Structured advice to NetBank's CISO on improving availability (e.g., redundant AAA servers), managing fallback accounts, and tightening authorization policies.
7. Dataset Package – Zipped repository including configs, logs (anonymized), test results, and report, with complete metadata for Mendeley Data deposit.