Root Cause Analysis

Problem Statement

Unauthorized authentication attempts were detected against SSH in the environment.

5 Whys

Why 1 — Why did brute-force occur?

Because SSH was reachable and allowed repeated attempts without blocking.

Why 2 — Why was SSH reachable?

Because the service was exposed on the network without access control restrictions.

Why 3 — Why were there no restrictions (firewall/rate-limits)?

Because a security hardening baseline was not enforced in the lab build.

Why 4 — Why was a baseline not enforced?

Because deployment did not include a checklist requiring minimum controls (firewall rules, SSH hardening).

Why 5 — Why was there no checklist/process?

Because security configuration governance (standards and validation) was not part of the setup process.

Root Cause (final)

Lack of a hardened baseline and access governance for exposed services enabled repeated authentication attempts.

Fishbone Analysis

People

No defined “minimum secure config” checklist was applied during setup.

Process

No exposure review step (which ports should be reachable? from where?).

Technology

- SSH allowed repeated authentication failures without rate limiting.
- No allowlist-based access control.

Environment

Flat lab networks make discovery and targeting easy.

Monitoring/Response

Monitoring existed (Elastic), but prevention controls were not pre-applied.

Corrective Actions

- Apply firewall default-deny and allow only necessary ports
- Restrict SSH to known admin IPs
- Add rate limiting / lockout policies
- Run periodic vulnerability and configuration checks