Goal-Setting Examples for Entry-Level Pentester & SOC L1

A) Entry-Level Pentester / Security Analyst (Web & Network)

1) SMART Goal

Goal title: Deliver web & network pentests with measurable client impact by year-end.

Specific — What exactly will you do?
Lead/assist 3 scoped pentests (2 web apps, 1 external network), from testing to reporting, including retests and client readouts.

Measurable — How will you quantify success?

- 3 Workpaper fulfilled for the pentest.
- 3 Report is drafted and submitted for the manager review.
- Timely delivery completed without extending the project timeline.

Achievable — Why is this realistic?
Assigned to a mix of small/medium engagements with senior oversight; lab and tool access (Burp Pro, Nmap, Nessus, Nuclei) already provisioned.

Relevant — How does this support bigger priorities?
Improves practice quality, drives renewals, and strengthens reputation for impactful reports.

Time-bound — Deadline or timeframe:
1 Sep–31 Dec 2025.

Key milestones & dates:

- 15 Sep: personal web test checklist v1 finalized and peer-reviewed.
- 30 Sep: deliver 1 web pentest with 1 report submission.
- 30 Nov: perform first external network pentest end-to-end and report is submitted for manager's review.

Owner: Chintan Gurjar

Risks:

- Client website was down for 2 days dated XX-XX-XXXX.
    - Extended business hours to complete the testing within the timeframe.
- Credentials for the authenticated pentest was provided post 3 days of the engagement start.
    - Analyze the application depth and breath post login and it was identified that the testing can still be carried out within the timeline regardless of delay in access.

2) OKR (Q4 2025)

Objective (qualitative, inspiring): Deliver standout pentests that reveal meaningful risk and are effortless for clients to act on.

Key Results (outcome-based & numeric):

1. Raise average report readability score (internal rubric /10) from 7.2 → **9.0**.
2. Reduce false positives to **≤1 per engagement** (self-reported + reviewer sign-off).
3. Produce **12 new reusable findings write-ups** (with remediation & business impact) in the internal knowledge base.
4. Cut retest cycle time median from 10 business days → **5 business days**.

Initiatives/Projects (how you'll hit KRs):

- Build "business impact" boilerplates mapped to common web vulns (IDOR, auth bypass, SSRF, object storage misconfig, etc.).
- Create Nuclei templates for 5 recurring misconfig checks; peer review.
- Adopt a report check-down: evidence → reproduction → impact → remediation → references.
- Pair with senior on 2 client readouts for storytelling coaching.

Owner(s): You (primary), Senior Pentester (mentor).

Weekly confidence score (0–1.0): Start 0.6; update Fridays with notes.

Check-in cadence: Fridays 16:00–16:20.

Timeframe: 1 Oct–31 Dec 2025 (Q4).

B) SOC L1 Analyst

1) SMART Goal

Goal title: Level up SOC L1 triage quality, speed, and documentation by the end of Q4 2025.

Specific — What exactly will you do?
Handle first-line triage for minimum 30 Critical and High severity alerts across SIEM + EDR, create/maintain runbooks, and improve escalation quality.

Measurable — How will you quantify success?

- Mean Time To Triage (MTTT) from queue assignment: baseline 22 min → **target 12 min**.
- Escalation acceptance rate by L2/L3: baseline 78% → **target 92%**.
- Case notes completeness (internal rubric /10): baseline 6.5 → **target 9.0**.

Achievable — Why is this realistic?
Existing runbooks, mentoring, and lab tenants for practice; alert volumes stable.

Relevant — How does this support bigger priorities?
Improves detection response, reduces risk exposure, and boosts SOC credibility with stakeholders.

Time-bound — Deadline or timeframe:
1 Sep–31 Dec 2025.

Key milestones & dates:

- 10 Sep: draft phishing triage runbook v2 with improved decision tree.
- 30 Sep: complete 15 recorded mock triages in lab; hit ≤12-minute average.
- 31 Oct: pilot enriched case template including MITRE technique mapping + IoC context.
- 30 Nov: deliver dashboard for personal KPIs (MTTT, acceptance rate, notes score).
- 15 Dec: cross-train on 2 new use cases (lateral movement, suspicious OAuth consent).

Owner: Chintan Gurjar (SOC L1)

Risks & mitigations:

- Alert surge → use queue triage policy & priority tags.
- Tool access delays → confirm permissions with platform owner by 5 Sep.
- Documentation drift → schedule monthly runbook review.

---

2) OKR (Q4 2025)

Objective: Provide decisive, well-documented triage that L2 trusts immediately.

Key Results:

1. Reduce **average** MTTT to **≤12 minutes** in October, **≤10 minutes** by December.
2. Achieve **≤5%** reopened escalations due to missing evidence/context.
3. Create **6 new/updated runbooks** for top alert types (phishing, malware, failed logon storms, privilege escalation, suspicious PowerShell, OAuth app consent).
4. Deliver **weekly quality spot-checks** (5 cases/week) with a rolling average ≥9/10.

Initiatives/Projects:

- Introduce a “triage stoplight” summary in case notes (Green: benign, Amber: suspicious, Red: likely malicious) with justification.
- Build a copy-paste IoC enrichment block (VT, WHOIS, passive DNS) with placeholders to speed note-taking.
- Pair with L2 for 4 shadow sessions focused on escalation criteria.

Owner(s): You (primary); L2 mentor.

Weekly confidence score: Start 0.7; update Tuesdays at stand-up.

Check-in cadence: Monday 09:30 KPI review; Friday retro 15:45.

Timeframe: 1 Oct–31 Dec 2025.