# Task 8 — Comprehensive Reporting & Debriefing (Full Report)

Author: MALEPATI SAMSKAR REDDY

Date: September 19, 2025

Scope: Produce PTES-compliant red team reports, executive briefings, findings tables, and visual attack-path diagrams.

Note: Screenshots are referenced by filename in the Week 4 mapping; this document contains only content (no embedded images).

---

## 1. Objective

Create professional, repeatable red-team deliverables including a PTES-style technical report, executive summary (100 words), non-technical brief (100 words), findings table with CVSS and remediation, and attack-path visualizations for stakeholders. Ensure outputs are clear for both technical teams and executives.

## 2. Report Structure (PTES-aligned)

Recommended sections and content for the full PTES-compliant report:

- Cover page: Engagement name, client, author, date, scope, and disclaimers.

- Executive Summary (100 words): high-level findings and critical remediation items.

- Scope & Rules of Engagement: Targets, boundaries, timelines, and permitted actions.

- Methodology: Tools, lab setup, attack flow, and commands (redacted as needed).

- Findings & Evidence: Detailed findings mapped to MITRE ATT&CK, CVSS scores, evidence references (filenames), and screenshots saved separately.

- Impact Analysis & Risk Rating: Business impact, likelihood, and suggested prioritization.

- Recommendations & Remediation Roadmap: Technical fixes, short-term mitigations, and long-term improvements.

- Detection & Response Gaps: SOC observations, tuning advice, and playbook suggestions.

- Appendices: Commands.txt, logs, timeline, and artifact inventory.

## 3. Executive Summary (100 words) — Template

[100-word executive summary template — replace placeholders]  
During a controlled red-team engagement, multiple critical vulnerabilities were identified that enabled unauthorized access and data exfiltration. Key issues include overprivileged IAM roles, publicly exposed S3 buckets, and script-based in-memory execution enabling C2 beaconing. Immediate actions: enforce MFA, restrict S3 ACLs, apply least-privilege to IAM roles, and enable enhanced PowerShell and network telemetry. These measures will reduce attacker dwell time and protect sensitive assets while technical remediation and SOC tuning are executed.

## 4. Non-Technical Brief (100 words) — Template

[100-word non-technical brief — for executives]  
A simulated attack showed attackers could access sensitive systems and copy mock data due to misconfigurations and weak controls. We recommend immediate steps: enable multi-factor authentication, lock down cloud storage, and review user privileges. These actions reduce business risk quickly. A technical remediation plan is attached for the engineering team with prioritized fixes and estimated effort.

## 5. Findings Table (example)

Provide a compact table of findings (example rows):

| Finding ID | Summary | MITRE TTP | CVSS | Risk | Remediation (high level) |  
|------------|------------------------------|---------------|------|---------|----------------------------------------|  
| FID001 | Overprivileged IAM role | T1078.004 | 9.0 | Critical| Apply least-privilege; audit & rotate |  
| FID002 | Public S3 bucket | T1580/T1537 | 8.0 | High | Block public access; enable logging |  
| FID003 | PowerShell fileless execution| T1059/T1086 | 7.0 | Medium | Enable script block logging, AMSI |  
| FID004 | Obfuscated payloads detected | T1027/T1071 | 6.5 | Medium | Behavioral EDR & egress filtering |

## 6. Metrics, KPIs & Executive Dashboards

Suggested KPIs to include in debriefs:

- Detection Rate (%) per TTP / Attack Phase

- Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR)

- Number of compromised hosts / assets

- Phishing click-through and credential capture rates

- Time to privilege escalation and time to exfiltration (seconds/minutes)

## 7. Recommendations for Presenting to Stakeholders

- Technical Appendix for SOC: full command logs, evidence filenames, SIEM queries, and remediation steps.

- Executive Brief: focus on risk, business impact, and prioritized remediation (top 3).

- Visual Attack Path Diagram: simple step boxes showing exploit chain (no technical jargon) for executives; detailed graph for technical teams.

- Actionable Remediation Plan: short-term (hours/days), medium-term (weeks), and long-term (months).

## 8. Sample 200‑Word PTES Technical Report (Template)

[200-word technical summary — include in full report]  
An end-to-end red-team engagement validated multiple attack vectors enabling unauthorized access and mock data exfiltration within a controlled lab. Reconnaissance exposed S3 buckets and IAM metadata; phishing operations captured credentials enabling initial access. PoshC2/Cobalt-style HTTPS beacons and fileless PowerShell stages permitted in-memory execution and remote command execution. Pacu modules revealed overprivileged roles and facilitated assume-role escalation, enabling broad access to S3 and configuration data. Automated orchestration (Caldera/RTA) replicated multi-stage campaigns and highlighted gaps in telemetry correlation between host and cloud logs. Detection was triggered in Wazuh for PowerShell anomalies and CloudTrail events for S3 PutObject; however, lag in correlation allowed the simulated exfiltration to complete. We advise urgent enforcement of MFA, immediate remediation of public S3 ACLs, least-privilege role reviews, activation of CloudTrail data event logging, and EDR tuning for script-based behaviors. A prioritized remediation roadmap, SIEM queries for hunting, and a post-engagement validation plan are provided in appendices.