



NxSAM Red Teaming — Quick Guide

Quick reference guide for the Red Teaming module

Product release	**NxSAM 2026.09**
Verified against code on	**2026-09-10**
Document revision	**b441b08-dirty**
Audience	**End users**
Document owner	**eSec Forte Technologies — Product Documentation**

Screenshots are taken from a demonstration data set. Figures are illustrative.

eSec Forte Technologies

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Table of Contents

Red Teaming

- Overview
- Red Teaming: every screen, column and action
- Red Teaming: find the right screen

Reference

- Glossary

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Red Teaming

Red Teaming

Red teaming records adversarial exercises — assessments that test whether an attacker could achieve a specific objective, rather than enumerating weaknesses.

How it differs from penetration testing

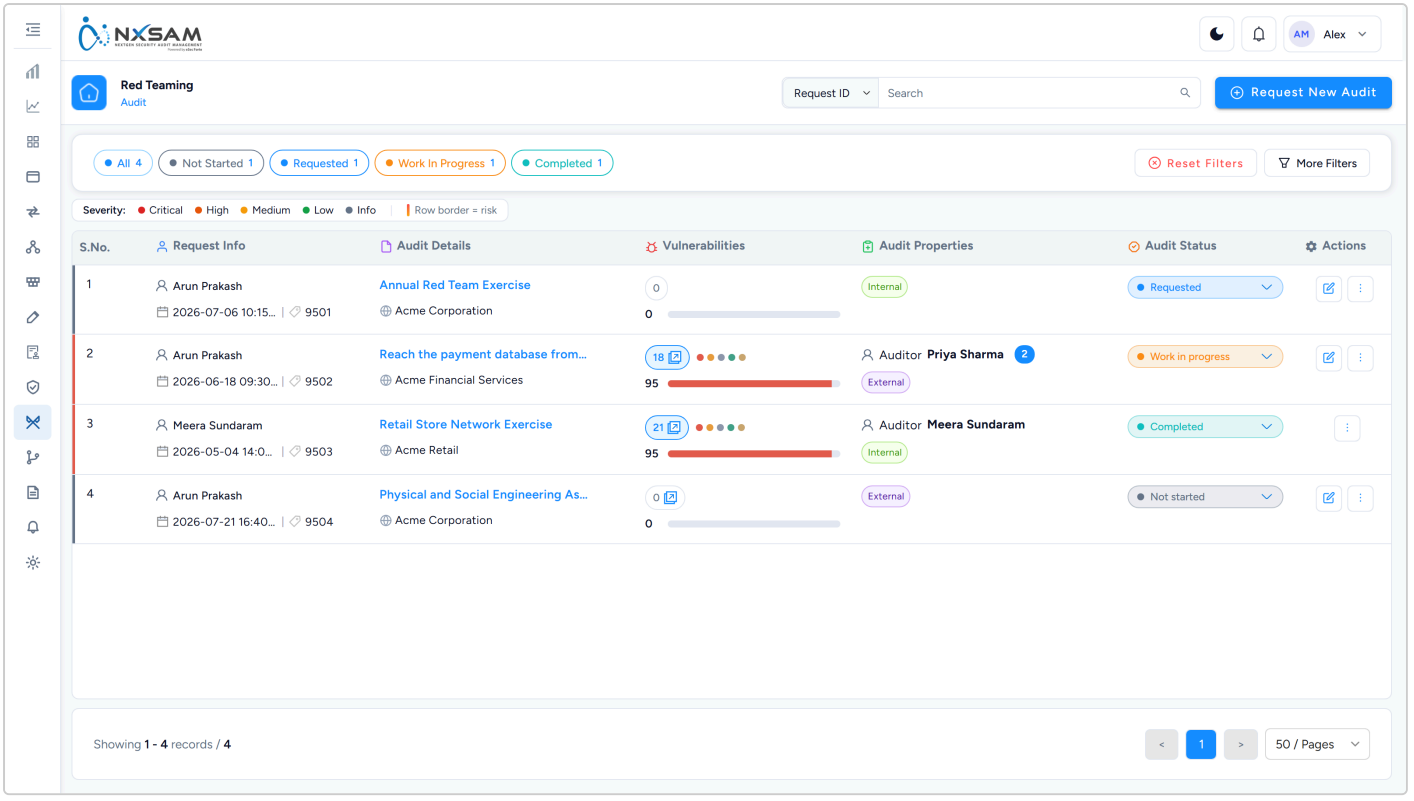
The two are often conflated, and the distinction shapes what the findings look like.

	Penetration test	Red team exercise
Question asked	What weaknesses exist in this system?	Could an attacker achieve this objective?
Scope	A defined system	Whatever the objective requires
Success measure	Coverage of the target	Whether the objective was reached
Also tests	The system	The system *and* whether anyone noticed

A red team exercise may reach its objective through a chain of individually unremarkable weaknesses. No single finding looks severe; the path is what matters.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

What findings look like here



Red team engagements, tracked as audits with their own findings.

Red team findings are narrative. They describe a route: this access led to that credential, which permitted this movement, which reached the objective.

Two consequences for how they are handled:

- **Severity reflects the path, not the step.** A finding rated Critical may involve several individually minor weaknesses. Do not down-rate the parts.
- **Fixing one step may break the chain** — but usually only that chain. The underlying weaknesses often remain available for a different route.

Detection matters as much as prevention

A red team exercise also tests whether your monitoring noticed. "The objective was achieved and nothing alerted" is a finding in its own right, and often the more important one, because it applies to every future attack rather than one path.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Working with the results

1. **Read the narrative before the findings list.** The list without the story loses the point.
2. **Address the chain, not only its steps.** Ask what else the same weakness enables.
3. **Treat detection gaps as findings.** They deserve owners and dates like any other.
4. **Re-run periodically.** A red team result is a statement about one point in time against one objective.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Red Teaming: every screen, column and action

The smallest module in the product, and deliberately so — a red team engagement produces a handful of findings that matter rather than a list to work through.

The audit list

An engagement is tracked as an audit, with the same columns as the other assessment modules:

Column	What it holds
Request Info	Who commissioned the engagement, when, and the request ID
Audit Details	The engagement name and its target
Vulnerabilities	How many findings it produced, with the severity split
Audit Properties	Type, cycle, scope and whether the engagement is considered
Audit Status	The engagement's state

Row actions — five

Action	What it does
View Vulnerabilities	The findings from this engagement
Assign Auditors	Who runs the engagement
Edit Audit Details	Name, dates, scope and properties

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Action	What it does
View Status History	Every status change, with who made it
Delete Audit	Soft delete

The menu is shorter than VA's or AppSec's on purpose. There is no re-audit, no audit chain and no severity configuration, because a red team engagement is a discrete exercise rather than a repeating scan — you commission a new one, you do not re-run the old one.

The findings list

Column	What it holds
VID	The finding's identifier, to quote in discussion
Vulnerability	What was achieved and how
Risk	The team's own rating
Status	Where the finding has got to

The only row action is **Delete Vulnerability**. Findings are entered by the team as they work and edited in place, so there is no separate edit dialog to open.

Validation statuses `Saved`, `Submitted`, `Approved`, `Closed`, `False Positive` — the same five as

Application Security, in this module's own table.

Why the findings read differently

A scanner finding names a weakness. A red team finding names an **outcome** — domain admin obtained, customer data reachable, a payment altered — and then explains the path that produced it.

That has two consequences for anyone supporting this module:

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

- **Risk is judged, not derived.** There is no CVSS score behind it. The team rates the finding on what it let them do, so two findings with identical technical severity can be rated differently and both be right.
- **The path matters more than the endpoint.** A finding that chains four low-severity weaknesses is the point of the exercise, and closing any one link resolves it. Reading only the individual weaknesses misses what was actually demonstrated.

Detection is part of the result

A red team engagement tests the response as much as the estate. Whether the activity was noticed, by what, and how quickly, is recorded with the findings — and an engagement where nothing was detected is a significant result even if few technical weaknesses were found.

This is why the module has no SLA columns. A red team finding is not a queue item with a remediation clock; it is evidence for a decision about defensive capability.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

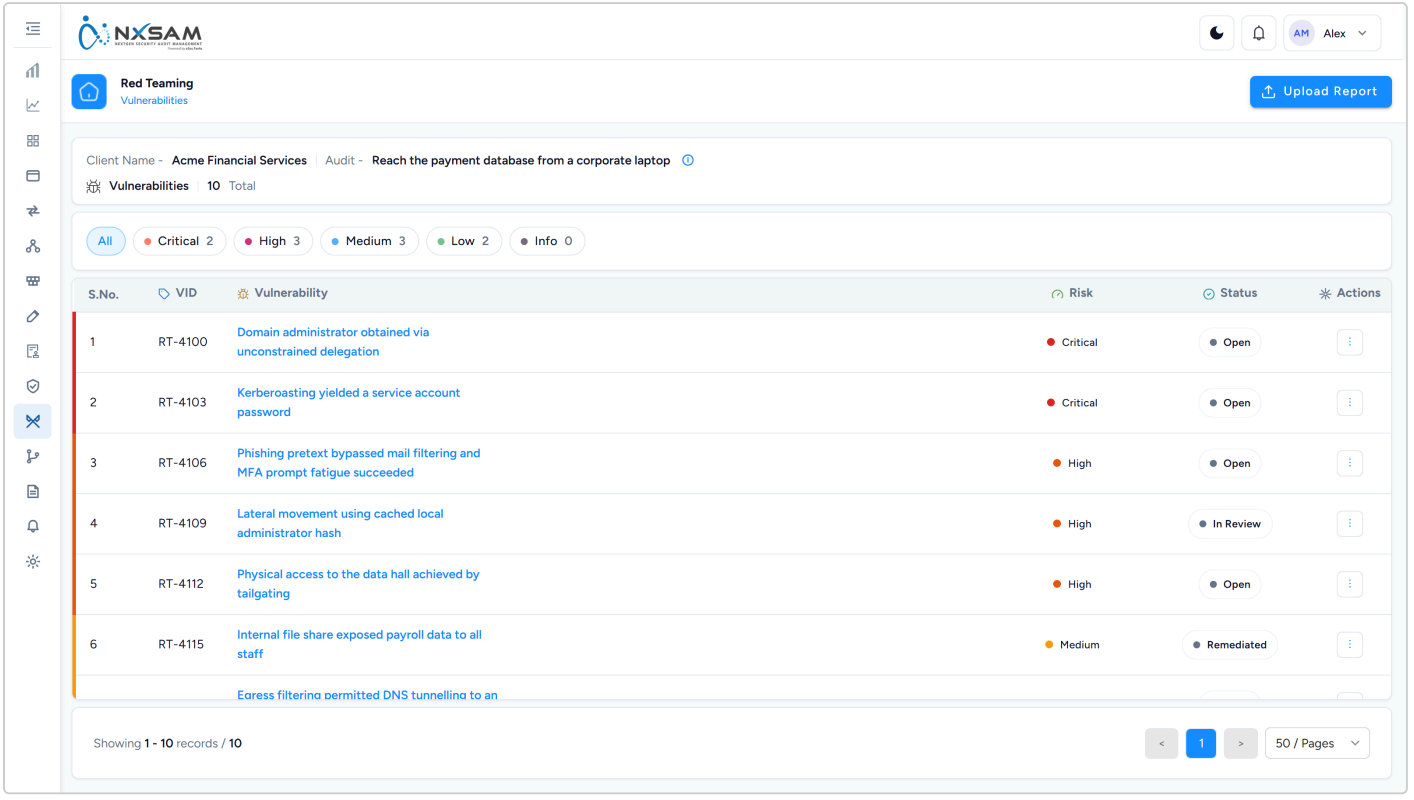
Red Teaming: find the right screen

Every screen in this module, what each one is for, and where it lives. Use it to find the right screen quickly, and to confirm you are on the one a colleague means — several screens in this product have similar names and different jobs.

Screenshots come from a demonstration data set, so the figures are illustrative. Click any screenshot to open it at full resolution.

Red Teaming Findings

What an engagement achieved and how — attack paths rather than a list of weaknesses.



Red Teaming → Red Teaming Findings

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Reference

Glossary

Terms as NxSAM uses them. Several are ordinary security words with a narrower meaning here, and those are the ones worth reading even if the term is familiar.

Assets and scope

Asset — anything that can hold a vulnerability: a web or mobile application, an API, a network host, a thick client, or a container image. Each type is a separate inventory with its own columns and its own licensed limit.

Asset property — an attribute recorded against an asset, such as criticality or whether it is internet-facing. Properties are more than description: they narrow SLA durations and feed the contextual risk score.

Bifurcation — splitting one application into separately assessed parts, so a large system can be tested module by module rather than as one unit.

Collection — a grouping of container images that comes from the scanning platform rather than from NxSAM, and is not editable here.

Scope — what an assessment covers. For applications this is the application; for compliance it is a host list, which is why compliance scope disputes are settled with an exported list of addresses.

Assessments

Audit — one assessment of one asset. It has a type, a category, a cycle, a scope, and a status of its own, separate from any finding's status.

Audit cycle — which round of a recurring programme an audit belongs to.

Confirmatory audit — a re-test created against a parent audit to verify that fixes hold. It is evidence about the original rather than an independent assessment, so the two should not be counted as two rounds of testing.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

Considered — the marker deciding whether an audit contributes to aggregate figures. Normally the latest audit per asset that reached a final state. An audit that is *not* considered still shows its findings on the module screen while contributing to no dashboard or report.

Initial audit — a first assessment, as opposed to a confirmatory one.

Findings

Vulnerability (also *finding*, *issue*) — one weakness on one asset, found by one assessment.

Vulnerability master — the catalogue entry (title, description, remediation) inherited by every occurrence of that vulnerability everywhere. Editing the master changes all of them.

Posture — Policy Compliance's unit: one control checked against one host. Every check produces a posture whether it passed or failed, which is why this module's volumes dwarf the others.

Artifact — the evidence attached to a finding: the steps, description and images that let someone else reproduce it.

Instance — which occurrence, where the same control or finding applies more than once to the same asset.

Status

Validation status — whether a finding has been confirmed. Nothing is counted anywhere until this reaches *Approved*, which is also when **Discovered On** is populated.

Client status (also *current status*) — what is being done about the finding. Of its values, only two close it.

Closed type — the flag deciding whether a status stops something counting as open. It is configuration rather than a fixed rule, so a deployment can change what "closed" means.

Posture status — what a compliance check returned: pass, fail or **error**. Error means the check could not run — a scanner or credentials problem rather than a compliance result.

Sub status — the qualifier beneath a main status: which kind of acceptance, or which stage of an approval.

Time and SLA

SLA duration — how long a finding of a given severity on a given asset type may remain open. Configurable, and narrowable by asset property.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

SLA expiry — the resulting deadline. Changing an SLA duration re-derives expiry dates, which can make a batch of findings overdue with no data change at all.

Discovered On — when a finding was first observed. Blank until the finding is approved.

Last observed — the most recent sighting, which is how a finding is known still to exist.

Overdue — past SLA expiry and not closed.

Decisions

Deviation (also *risk acceptance*, *RA*) — a recorded decision not to fix something, with an approval chain and an expiry. It does **not** close the finding: the exposure is still live and still counts as open.

Exception — a status marking an agreed exception rather than a resolution. Reporting that conflates the two overstates remediation.

Auto reject end date — when a temporary acceptance lapses on its own.

Integrations and processing

Integration — a connection to a scanning tool, either pulling from its API or parsing an uploaded report.

Vulnerability key — the columns deciding whether an incoming finding is one already seen. Changing it redefines "the same finding" and splits history.

Queue — asynchronous work: imports, syncs, report generation. A screen that seems not to have updated usually has a queue entry that explains it.

Data process — how far a tool-fed audit has got through the import pipeline; the difference between "the upload finished" and "the data is ready".

Beat — a scheduled job maintaining derived data, such as recalculating SLA states as dates pass. A stopped beat produces figures wrong by a fixed interval and raises no error.

Governance

RLCM — Red Line Compliance Management: assessment of controls against frameworks, rather than of systems for weaknesses.

TPRM — Third-Party Risk Management: the same control assessment applied to suppliers. It shares screens with RLCM and differs by the audit's type.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.

UCF — Unified Control Framework: the mapping that lets one control satisfy several frameworks at once, so answering it once covers each of them.

Control — a requirement being assessed, as opposed to a weakness being found.

Standard — the framework a control belongs to, such as ISO/IEC 27001 or PCI DSS.

Reporting

Considered audit filter — the switch on Report Search that reproduces either the dashboard's numbers or the module screens'. Comparing the two settles most disagreements about counts.

Design template — the layout a report renders through, separate from the template that decides its content.

Share view against share copy — sharing a template as a view keeps one definition that your edits reach; sharing a copy creates an independent template that will drift.

Copyright 2010-2026 eSec Forte® Technologies Private Ltd.