

TECHNICAL PRODUCT BRIEF

Internal network penetration testing

See how far an attacker could move inside your network.

Why customers use this service

Test representative internal access to expose weak trust boundaries, credentials, services and privilege paths that could turn one compromised device into broader control.

What we assess

Internal exposure	Reachable systems, services and administrative interfaces.
Identity and credentials	Weak authentication, reusable credentials and credential material.
Privilege escalation	Paths from ordinary access to local or domain privilege.
Lateral movement	Trust relationships and services that enable movement between systems.
Segmentation	Whether sensitive environments resist access from lower-trust locations.
Legacy protocols	Insecure or relayable protocols that increase compromise impact.
Operational visibility	Security events available to trace representative activity.

Engagement outcome

A prioritised technical report showing validated compromise paths, affected systems, remediation actions and retest results.

How the engagement works

How we test or review

Damocles begins from the agreed internal foothold, maps reachable services and identity relationships, and safely validates representative lateral and privilege paths. Configuration review supports but does not replace observed host and network results; protected systems and disruptive actions remain excluded.

Testing and review perspectives

Assumed internal foothold

Operates from the supplied internal network position without assuming credentials beyond those authorised.

Included when: Used to establish discovery and reachability available after an initial internal compromise.

Access: A test host or connection, source subnet, expected trust zone, approved ranges and exclusions.

Limitations: Represents one foothold and cannot establish access from every internal segment.

Supplied standard user or workstation

Uses a controlled standard identity and workstation to inspect credential, service, lateral-movement and local privilege conditions.

Included when: Used where user or endpoint context materially changes reachable services or permissions.

Access: A dedicated domain or local identity, representative workstation and expected user rights.

Limitations: Does not represent other builds, groups, cached sessions or privileged identities.

Privileged-path and configuration reviewer

Analyses network, host and directory evidence to connect permissions, management paths and trust relationships.

Included when: Used to substantiate attack paths or compare observed behaviour with intended controls.

Access: Relevant ACLs, firewall and routing exports, directory evidence, system inventories and access models.

Limitations: Evidence review cannot prove every live path and validation stops at the minimum safe proof.

Customer access or evidence typically required

A test host or connection, source subnet, expected trust zone, approved ranges and exclusions.; A dedicated domain or local identity, representative workstation and expected user rights.; Relevant ACLs, firewall and routing exports, directory evidence, system inventories and access models.

What you receive

A prioritised technical report showing validated compromise paths, affected systems, remediation actions and retest results.

Detailed technical coverage

Assumed internal foothold

What is assessed	Damocles records the supplied network position, host context, identity and expected trust zone, then establishes the discovery and reachability available from that foothold.
Perspective / access	Assumed internal foothold. Assessment requires approved ranges, supplied footholds, test hosts, identities, flow expectations and relevant network, host or directory evidence, selected specifically for assumed internal foothold.
Evidence	Evidence records the host, service, connection, credential, permission or attack-path evidence relevant to assumed internal foothold.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Assumed internal foothold when the relevant internal system, identity or trust boundary is included.
Limitations	The conclusion is limited to the sampled assumed internal foothold; results cover supplied footholds and test points; protected systems and disruptive actions remain excluded.

Internal service discovery

What is assessed	Damocles enumerates reachable hosts, listening ports, service indicators and administrative protocols within the approved internal ranges.
Perspective / access	Assumed internal foothold. Approved ranges, names, locations and the expected asset or interface inventory.
Evidence	A discovered-item register with address, service, version or location and reconciliation status.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed for customer-owned ranges, names, locations or interfaces listed in the authorised inventory.
Limitations	Discovery is point-in-time and cannot establish ownership or absence outside the approved inventory; intrusive enumeration stops at the agreed boundary.

Network trust zones

What is assessed	Damocles maps intended trust zones to routing, firewall and ACL evidence and identifies representative boundary paths for validation.
Perspective / access	Privileged-path and configuration reviewer. Assessment requires approved ranges, supplied footholds, test hosts, identities, flow expectations and relevant network, host or directory evidence, selected specifically for network trust zones.
Evidence	Evidence records the host, service, connection, credential, permission or attack-path evidence relevant to network trust zones.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Network trust zones when the relevant internal system, identity or trust boundary is included.
Limitations	The conclusion is limited to the sampled network trust zones; results cover supplied footholds and test points; protected systems and disruptive actions remain excluded.

Segmentation enforcement

What is assessed	Damocles attempts approved allowed and denied connections between actual source and destination test points and records the enforcement result.
Perspective / access	Assumed internal foothold. Assessment requires approved ranges, supplied footholds, test hosts, identities, flow expectations and relevant network, host or directory evidence, selected specifically for segmentation enforcement.
Evidence	Evidence records the host, service, connection, credential, permission or attack-path evidence relevant to segmentation enforcement.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Segmentation enforcement when the relevant internal system, identity or trust boundary is included.
Limitations	The conclusion is limited to the sampled segmentation enforcement; results cover supplied footholds and test points; protected systems and disruptive actions remain excluded.

Credential exposure

What is assessed	Damocles inspects authorised endpoints, shares, service configuration and protocol behaviour for reusable credentials or credential material without bulk harvesting.
Perspective / access	Assumed internal foothold. Assessment requires approved ranges, supplied footholds, test hosts, identities, flow expectations and relevant network, host or directory evidence, selected specifically for credential exposure.
Evidence	Evidence records the host, service, connection, credential, permission or attack-path evidence relevant to credential exposure.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Credential exposure when the relevant internal system, identity or trust boundary is included.
Limitations	The conclusion is limited to the sampled credential exposure; results cover supplied footholds and test points; protected systems and disruptive actions remain excluded.

Lateral movement

What is assessed	Damocles validates representative remote-management, service, trust or credential paths between approved systems and stops after minimum evidence of additional access.
Perspective / access	Supplied standard user or workstation. Assessment requires approved ranges, supplied footholds, test hosts, identities, flow expectations and relevant network, host or directory evidence, selected specifically for lateral movement.
Evidence	Evidence records the host, service, connection, credential, permission or attack-path evidence relevant to lateral movement.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Lateral movement when the relevant internal system, identity or trust boundary is included.
Limitations	The conclusion is limited to the sampled lateral movement; results cover supplied footholds and test points; protected systems and disruptive actions remain excluded.

Local privilege escalation

What is assessed	Damocles examines local groups, rights, services, scheduled tasks, stored credentials, installed software and host configuration for a safe path to local administrative access.
-------------------------	--

Perspective / access	Supplied standard user or workstation. Assessment requires approved ranges, supplied footholds, test hosts, identities, flow expectations and relevant network, host or directory evidence, selected specifically for local privilege escalation.
Evidence	Evidence records the host, service, connection, credential, permission or attack-path evidence relevant to local privilege escalation.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Local privilege escalation when the relevant internal system, identity or trust boundary is included.
Limitations	The conclusion is limited to the sampled local privilege escalation; results cover supplied footholds and test points; protected systems and disruptive actions remain excluded.

Domain privilege escalation

What is assessed	Damocles analyses directory groups, ACLs, delegation, service accounts and identity relationships for a safe path to increased domain privilege.
Perspective / access	Supplied standard user or workstation. Assessment requires approved ranges, supplied footholds, test hosts, identities, flow expectations and relevant network, host or directory evidence, selected specifically for domain privilege escalation.
Evidence	Evidence records the host, service, connection, credential, permission or attack-path evidence relevant to domain privilege escalation.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Domain privilege escalation when the relevant internal system, identity or trust boundary is included.
Limitations	The conclusion is limited to the sampled domain privilege escalation; results cover supplied footholds and test points; protected systems and disruptive actions remain excluded.

Administrative protocols

What is assessed	Damocles tests approved administrative protocols for authentication, signing, encryption and access restrictions from the supplied foothold.
Perspective / access	Assumed internal foothold. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed when current configuration evidence and a representative endpoint or device are included in the review.
Limitations	A configuration snapshot cannot prove continuous enforcement across excluded nodes; validation avoids changes unless implementation work is authorised.

Management-plane exposure

What is assessed	Damocles determines whether standard footholds can reach network, security, hypervisor, backup or infrastructure management interfaces contrary to the intended model.
Perspective / access	Privileged-path and configuration reviewer. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results.
References	Technical Guide to Information Security Testing and Assessment SP 800-115

Applicability	Performed when current configuration evidence and a representative endpoint or device are included in the review.
Limitations	A configuration snapshot cannot prove continuous enforcement across excluded nodes; validation avoids changes unless implementation work is authorised.

Sensitive-system reachability

What is assessed	Damocles attempts named required and forbidden protocols to approved high-value destinations from representative footholds.
Perspective / access	Assumed internal foothold. Named source and destination test points, expected flow matrix and a safe test window.
Evidence	Source-to-destination results linked to rule, route or boundary evidence; the record names the tested sensitive-system reachability object, path or control and its observed result.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed when both ends of the network path and the enforcing device are owned or expressly authorised for testing.
Limitations	Results cover the tested source, destination, protocol and route; testing stops on instability and does not authorise third-party or denial-of-service activity.

Attack-path chaining

What is assessed	Damocles joins observed foothold, credential, privilege, lateral-movement and sensitive-system reachability evidence into a reproducible attack chain.
Perspective / access	Assumed internal foothold. Named source and destination test points, expected flow matrix and a safe test window.
Evidence	Source-to-destination results linked to rule, route or boundary evidence; the record names the tested attack-path chaining object, path or control and its observed result.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed when both ends of the network path and the enforcing device are owned or expressly authorised for testing.
Limitations	Results cover the tested source, destination, protocol and route; testing stops on instability and does not authorise third-party or denial-of-service activity.

Protected and excluded systems

What is assessed	Damocles marks protected and excluded systems in the test inventory, prevents active interaction with them and records how each exclusion constrains discovery or path conclusions.
Perspective / access	Assumed internal foothold. Assessment requires approved ranges, supplied footholds, test hosts, identities, flow expectations and relevant network, host or directory evidence, selected specifically for protected and excluded systems.
Evidence	Evidence records the host, service, connection, credential, permission or attack-path evidence relevant to protected and excluded systems.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Protected and excluded systems when the relevant internal system, identity or trust boundary is included.

Limitations	The conclusion is limited to the sampled protected and excluded systems; results cover supplied footholds and test points; protected systems and disruptive actions remain excluded.
-------------	--

Methodologies and standards

Technical Guide to Information Security Testing and Assessment SP 800-115 — Uses NIST SP 800-115 guidance to plan, execute, analyse and report the authorised procedure.

Information Security Manual June 2026 — Provides ASD ISM control context only for the declared mapping and observed behaviour.

Common Weakness Enumeration 4.20 — Classifies confirmed weakness types using CWE 4.20.

Common Vulnerability Scoring System 4.0 — Calculates technical severity and records a CVSS 4.0 vector separately from customer impact.

Standards and control mappings

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — contextual

References: Framework-level mapping

Assessed: The engagement produces point-in-time technical evidence about the configured and observed security behaviour within the authorised Internal network penetration testing scope.

Evidence: Coverage status, procedure results and findings can inform the customer’s control assessment and risk treatment records.

Applicability: Framework-level context is provided when the customer uses NIST SP 800-53 to organise its security control program.

Limitations: No individual NIST control is published as verified; organisational implementation, continuous operation, governance and complete catalogue coverage remain outside the engagement.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Internal network penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Coverage matrix

Records coverage matrix produced from the authorised Internal network penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Retest and residual-risk record

Records retest and residual-risk record produced from the authorised Internal network penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Internal service inventory

Records internal service inventory produced from the authorised Internal network penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Lateral-movement path record

Records lateral-movement path record produced from the authorised Internal network penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Privilege-path evidence

Records privilege-path evidence produced from the authorised Internal network penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Scope and safety limitations

- Only expressly authorised assets, identities, locations and activities are assessed.
- Higher-risk, disruptive, destructive and third-party activity requires separate written authority.
- Point-in-time evidence cannot establish continuous operation or conditions outside the engagement.

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

Review metadata

Owner: Technical Assurance

Last reviewed: 2026-08-10

Next review due: 2026-12-10

Scope this engagement with Damocles Security
damocles.com.au/contact

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

This brief supports engagement scoping. The authorised scope, rules of engagement and applicable agreement govern delivery.