Unicorn IT Group

External Network Penetration Test Report

Perimeter security assessment of public-facing infrastructure

Prepared for: Sample Engineering Pty Ltd

Date: 28 August 2026

Classification: CONFIDENTIAL

1300 904 635 | hello@uitg.com.au | www.uitg.com.au

Document Information

Document title	Sample Penetration Test Report
Version	1.0
Author	Unicorn IT Group Security Team
Classification	Confidential
Contact	hello@uitg.com.au | 1300 904 635

This is a sample report for demonstration purposes. Names, IP addresses and findings have been fictionalised.

Executive Summary

This sample report summarises the results of an external network penetration test performed against the client's public IP ranges. Testing identified one critical and one high-risk issue that could allow unauthorised remote access to the internal network. Immediate remediation is recommended for the exposed RDP service and outdated VPN appliance. The remaining findings are medium and low risk but should be addressed to reduce overall attack surface.

Metric	Value
Test type	External network penetration test
Targets	Public IP ranges and external services
Duration	3 business days
Critical findings	1
High findings	1
Medium findings	1
Low findings	1

Findings Overview

ID	Finding	Risk	Status
EXT-001	Exposed RDP service with weak credentials	Critical	Open
EXT-002	Outdated VPN appliance with public exploit	High	Open
EXT-003	Missing DMARC email policy	Medium	Open
EXT-004	Information disclosure in public web directory	Low	Open

Detailed Findings

EXT-001 — Exposed RDP service with weak credentials

Risk rating: Critical

Description

A Remote Desktop service was reachable from the internet on TCP/3389 and accepted authentication with a common username/password combination. Successful login granted full interactive access to an internal workstation.

Evidence

Nmap scan identified open port 3389. Hydra brute-force succeeded with administrator / Summer2024!. Screenshot shows interactive desktop session.

Recommendation

Disable external RDP, enforce VPN-only access, enable account lockout and require MFA for all remote access.

EXT-002 — Outdated VPN appliance with public exploit

Risk rating: High

Description

The edge VPN appliance is running firmware with a known CVE that allows unauthenticated command injection. A public proof-of-concept is available.

Evidence

Shodan query and banner grab confirmed version. CVE-2023-XXXX matches the observed build.

Recommendation

Patch VPN appliance to the latest vendor-supported firmware and review remote-access architecture.

EXT-003 — Missing DMARC email policy

Risk rating: Medium

Description

The organisation's DNS records do not include a DMARC policy, increasing the risk of spoofed emails being delivered to staff and customers.

Evidence

DNS query for _dmarc.example.com returned NXDOMAIN.

Recommendation

Publish a DMARC record with p=quarantine and align SPF/DKIM records.

EXT-004 — Information disclosure in public web directory

Risk rating: Low

Description

A directory listing on the public web server exposed backup file names and internal folder structure.

Evidence

GET /old/ returned an Apache directory index with file listings.

Recommendation

Disable directory indexing and remove or restrict legacy public folders.

Scope & Methodology

Scope

- Public IP ranges assigned to the organisation
- Externally reachable web services and VPN endpoints
- Email security configuration (SPF, DKIM, DMARC)
- DNS and public-facing infrastructure

Methodology

Testing combined automated vulnerability scanning with manual validation. Where weaknesses were found, we attempted safe exploitation only to confirm impact and never disrupted production services.

Standards & Frameworks

- PTES (Penetration Testing Execution Standard)
- NIST SP 800-115
- OWASP Testing Guide
- ACSC Essential Eight

Remediation Tracker

ID	Action	Owner	Target
EXT-001	Disable external RDP, enforce VPN-only access, enable account lockout and require MFA for all remote access.	IT Team	30 days
EXT-002	Patch VPN appliance to the latest vendor-supported firmware and review remote-access architecture.	IT Team	30 days
EXT-003	Publish a DMARC record with p=quarantine and align SPF/DKIM records.	IT Team	30 days
EXT-004	Disable directory indexing and remove or restrict legacy public folders.	IT Team	30 days

Unicorn IT Group can assist with remediation, re-testing and ongoing security management. Contact us at hello@uitg.com.au or 1300 904 635.