

PREVIEW · FICTITIOUS DATA

Technical report

Internal penetration test

Example Client, Inc. (fictitious client)

Client / Organization	Example Client, Inc. (fictitious)
Assessment	Internal penetration test
Execution period	September 1–19, 2026 (example dates)
Version	Sample 1.0
Prepared by	SoluProTec
Issue date	October 12, 2026

CONFIDENTIAL. A real report carries this notice on its cover and is distributed on a restricted basis. This preview is public and **all of its data is fictitious**: no client, asset, address or result is real.

About this sample

This preview brings together 6 of the 25 pages of the SoluProTec sample technical report, with made-up data: the cover, these notes, the executive summary with the attack chain and one complete finding. It shows how we present what was found, how serious it is and what to do first.

What is fictitious

All of it. The client, people and job titles, host and domain names (`.test`), IP addresses (the documentation ranges `192.0.2.0/24` , `198.51.100.0/24` and `203.0.113.0/24` , reserved for examples), dates, figures and findings. The CVSS scores are, however, computed with the official formula from each vector.

What changes in a real report

- It is a condensed version: a real report includes the full asset inventory, the evidence (screenshots and outputs) in annexes and more findings.
- Secrets (passwords, hashes, tokens) still appear redacted, unless the client asks otherwise in writing.
- The close-out includes a results meeting and, if contracted, validation of the fixes.

Want a report like this for your organization? Write to us at info@soluprotec.org and tell us what you want to protect.

Document control

This copy	Public preview: 6 of the 25 pages of the sample report
Version	Sample 1.0
Date	October 12, 2026
Status	Final (sample)
Quality review (QA / peer review)	Done by a second assessor before issue (in a real report)
Distribution	General management, IT management and security officer of Example Client, Inc. (fictitious roles)

1 Executive summary

1.1 Overview

SoluProTec carried out an internal penetration test for Example Client, Inc. between September 1 and 19, 2026 (example dates). The test started from a user workstation connected to the corporate network with no credentials, and set out to answer one question: **what could someone achieve who gains that first foothold?** For example, reaching critical information, taking control of the corporate identity or preventing recovery after an incident.

6 findings were identified: 1 critical, 3 high, 1 medium and 1 low. Three of them (H-03, H-02 and H-01) form a chain: from a workstation with no credentials, a domain account was obtained, then an account with administrative rights over servers and, in addition, access to the backup console. **The overall risk level is HIGH.**

Controls that work well were also verified (section 5.4 of the full report): the VPN requires multi-factor authentication, endpoint detection reacted to offensive tools and the guest network is isolated.

1.2 Distribution by severity

Severity is derived strictly from each finding's CVSS v3.1 base score (section 4 of the full report).

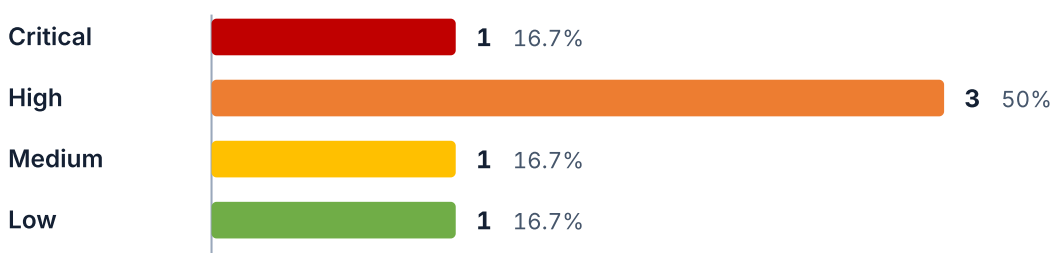


Figure 1. Findings by severity (total: 6).

Severity	Count	%	Executive reading	Priority
Critical	1	16.7%	Compromises critical systems with little technical effort. Fix immediately.	P0
High	3	50%	Allows privilege escalation or access to sensitive information with few preconditions.	P1
Medium	1	16.7%	Needs additional conditions to be taken advantage of; weakens the overall posture.	P2
Low	1	16.7%	Limited impact; hygiene and defense-in-depth improvement.	P3
Total	6	100%		

1.3 Main attack chain

The findings are not isolated: **H-03** delivers the first domain account, **H-02** turns it into administrative control of servers and **H-01** leaves the organization with no way to recover. **H-01** can also be reached directly from the user network, without going through the other two.

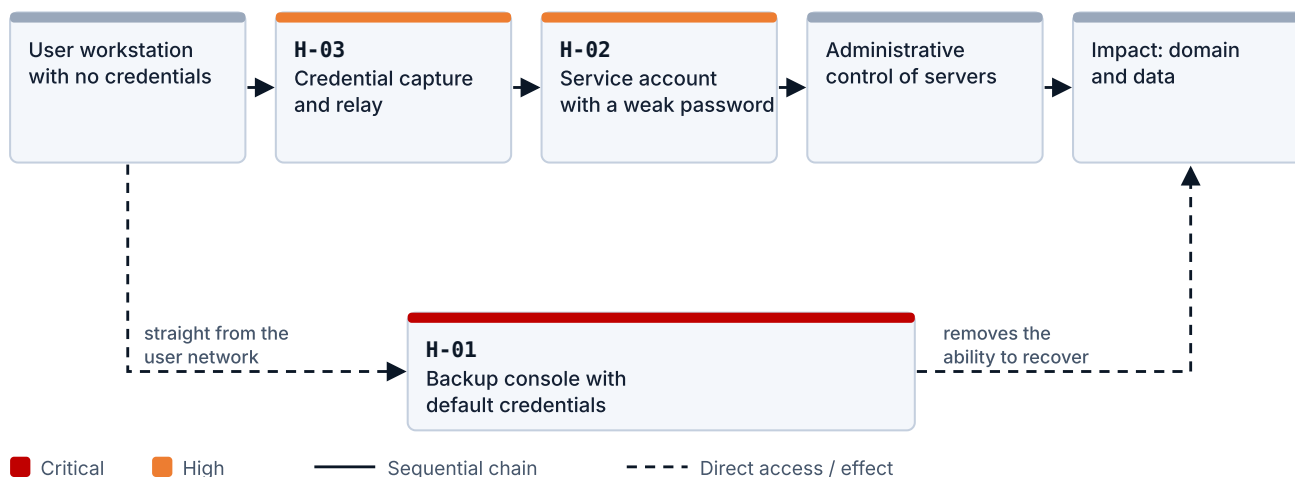


Figure 2. Main attack chain. The top color of each box indicates the severity.

1.4 Positive indicators identified

Control	What was verified
VPN with mandatory MFA	It could not be bypassed with the authorized techniques.
Endpoint detection (EDR)	Detected and alerted on 2 of 3 attempts to run common offensive tools.
Guest network isolation	No route to the corporate network from the guest Wi-Fi.

1.5 Message for management

The risk is not at the perimeter, which held, but on the internal network: legacy protocols, service accounts with weak passwords and an unprotected backup console. These are known problems with contained fixes.

Three actions concentrate the greatest risk reduction and can be completed in 15 days: change the backup console credentials and restrict its access (**H-01**); disable LLMNR/NBT-NS and require SMB signing (**H-03**); and rotate the service account password and remove its privileges (**H-02**). With them, the main chain is no longer possible.

One complete finding

Of the 6 findings in the sample report, this is the sheet of the most severe one (H-01), as it is delivered: risk data, attack chain, description, justification, countermeasures, references, steps to reproduce it and evidence.

H-01 Backup console reachable with default credentials

Risk rating	Critical Critical · P0
Status	Open — immediate response required
CVSS v3.1 base / vector	9.8 — CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE / MITRE ATT&CK	CWE-1392: Use of Default Credentials · MITRE ATT&CK T1078.001
Tools used	Nmap; web browser (manual validation)
Category	Default credentials
Affected assets	bkp01 · 198.51.100.20 · 8443/tcp (backup administration web console)
Identified by / method	Enumeration of web consoles in the server segment and manual validation of access.

Continuity and attack chain

- **Precursor vulnerability (origin):** None. It is an independent vector: it only needs network connectivity to the console.
- **Sequential vulnerability (continued impact):** Allows backups and their retention policies to be deleted or altered, and the backed-up data of every system to be copied.
- **Connecting vector:** Last link of the impact chain: without intact backups, a ransomware incident cannot be recovered from. It is reached directly from the user network and also from the server control obtained with H-02.

Description of the vulnerability

The web console of the backup system accepted the administrator account with the factory credential that the vendor publishes in its documentation (not reproduced here). With that session, the jobs, repositories and retention policies were listed. No backup was modified, downloaded or deleted: validation was limited to reading. The console is reachable from the user network because there is no filtering between that segment and the server network for this port.

Risk justification

Confidentiality, integrity and availability: high impact. Whoever reaches the console can delete or encrypt the repositories and retention policies, or copy the backed-up data of every system at once. It is the highest-priority finding because taking advantage of it needs no technical knowledge and it removes the organization's ability to recover.

Countermeasures and mitigation (step by step)

1. Change the default credential immediately and rotate the console's other credentials (local, service and integration accounts).
2. Restrict access to the console to an administration network and a bastion host, with an allow-list of addresses.
3. Administer the backups with named accounts and multi-factor authentication (MFA); disable the generic account.
4. Enable immutable repositories and an offline copy, or one in another identity domain, so a compromised account cannot delete every recovery point.
5. Log sign-ins and retention changes, and alert on any administrative access outside the usual window.

External references

- [CWE-1392](https://cwe.mitre.org/data/definitions/1392.html) · <https://cwe.mitre.org/data/definitions/1392.html>
- [MITRE ATT&CK T1078.001](https://attack.mitre.org/techniques/T1078/001/) · <https://attack.mitre.org/techniques/T1078/001/>
- Hardening guide from the backup system's vendor.

Proof of concept (PoC) and steps to reproduce

```
$ nmap -sV -p 8443 198.51.100.20
8443/tcp open  ssl/https    (backup administration web console)
```

Manual validation (read-only):

1. Sign-in at <https://bkp01.corp.example.test:8443> with the factory user and its default credential [REDACTED].
2. Result: valid administrator session.
3. Actions taken: listing jobs and repositories. No changes.

Summary of what was done, with no secrets. Full commands and outputs go in the evidence annex of a real report.

Digital evidence

- [EV-H01-01] Screenshot: console with an administrative session (not included in the sample).
- [EV-H01-02] Port scan output: 198.51.100.20:8443.

Want to see the full report?

This preview shows 6 of the 25 pages. The full report adds the scope and rules of engagement, the methodology, the severity scale, all 6 findings with their evidence, the technical observations, the prioritized remediation roadmap, the conclusions and the annexes.

Ask for it with the "Request the full report" button at www.soluprotec.org/en/services/penetration-testing or write to info@soluprotec.org. Our team reviews each request and we reply within one business day; the report is sent by email.