SAMPLE REPORT · FICTITIOUS CLIENT

CYBER ERA OS

OFFENSIVE SECURITY

Internal Network, Active Directory & Web Application Penetration Test

Northgate Ltd (fictitious organisation) · Final report with retest results

CLIENT
Northgate Ltd (fictitious)

REPORT VERSION
1.1 · Final, retest included

PREPARED BY
Cyber Era Offensive Security · cybereraos.com

TESTING WINDOW
6–12 October 2026

CLASSIFICATION
Confidential: client and tester only

CONTACT
contact@cybereraos.com

About this document

This is a sample report. It shows how Cyber Era OS reports a penetration test. Northgate Ltd is a fictitious organisation and every host, account, file and password in this document is invented. The testing itself is real: it was carried out against an isolated training lab built to behave like a small company network, and recorded live on video.

Document control

Version	Date	Change
1.0	12 Oct 2026	Findings reported to the client
1.1	12 Oct 2026	Retest results added; all findings closed

Distribution	Role
Northgate Ltd: IT Manager (fictitious)	Report owner, remediation
Cyber Era Offensive Security	Tester

Contents

1. Executive summary
2. Scope, rules of engagement and approach
3. How findings are rated
4. Summary of findings
5. Detailed findings F-01 to F-08
6. What is already done well
7. Remediation roadmap

Appendix A: Tools · Appendix B: Evidence handling · Appendix C: Glossary

1. Executive summary

Cyber Era OS tested Northgate's internal network, its Active Directory domain and its online shop between 6 and 12 October 2026. The goal was to answer two questions: **what can someone on the office network reach without any account**, and **what can one ordinary employee account see**, for example after a phishing email steals it.

1	4	3	8 / 8
CRITICAL	HIGH	MEDIUM	FIXED & RETESTED

What this means for the business

Without any account, a person plugged into the office network could read and change the shop's cache server, read the password of a backup service account straight from the domain directory, and find a deployment account's password in a script on a file share anyone can open. Any one of these is a foothold an attacker would use first.

With one ordinary staff login, the same person could read the HR share (payroll, salary bands, disciplinary cases and scanned passports), see that a former contractor's account still holds full Domain Admin rights with a password that never expires, and guess passwords against every account without ever being locked out.

On the online shop, the product search could be made to run attacker-controlled database queries, and any customer could read other customers' orders, including names and addresses.

Where Northgate stands now

All eight findings were reported the same day they were confirmed. Northgate's IT team fixed all of them, and every fix was **retested and confirmed closed** from the same network position. The most important remaining work is process, not technology: an owner and an expiry date for every privileged account, and a periodic review of who can read which share (section 7).

How we work. Every finding was proven, never exploited further than needed to prove it. Credentials found during the test were masked in the same command that read them and were **never used**. Sensitive files were listed by name, **never opened or downloaded**. No data was changed and no service was disrupted.

2. Scope, rules of engagement and approach

In scope

Target	Address	Tested as
Internal network	`10.10.10.0/24`	No account (unauthenticated)
Active Directory domain `northgate.local` (dc-01)	`10.10.10.10`	No account, then one ordinary staff account supplied by the client (assumed breach)
File server (files-01)	`10.10.10.30`	Guest, then the supplied account
Cache server (cache-01)	`10.10.10.20`	No account
Online shop (shop-01)	`10.10.10.50:3000`	No account, then a test customer account

Out of scope: anything outside 10.10.10.0/24, denial of service, social engineering, physical access, and password guessing of any kind.

Rules of engagement (agreed in writing before testing)

Testing window	6–12 October 2026, from source address 10.10.10.4 only
Credentials	If found: masked on capture, never used, reported to the client the same hour
Sensitive data	Listed by name only; never opened, copied or downloaded
Changes	None. Read-only testing; no configuration or data altered
Critical findings	Reported immediately, not held for the final report

Approach

The test followed one loop for every finding: **find** (discovery and enumeration), **prove** (the smallest action that shows the issue is real), **stop** (no further exploitation), **report** (same day), and **retest** (after the client's fix). It covered:

Phase	What was done
Discovery	Host and service discovery across the range; version identification of exposed services
Unauthenticated checks	Anonymous access to directory (LDAP), file shares (SMB) and the cache service; web application testing without an account
Assumed breach	What one ordinary employee account can read: domain users and groups, password policy, privileged groups, file share permissions
Web application	Input handling in the search, access control on the order API, error handling
Retest	Every finding re-checked from the same position after the client's fix

3. How findings are rated

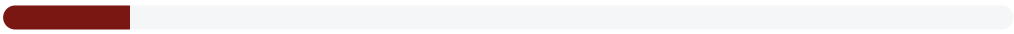
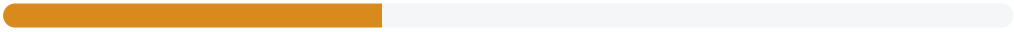
Each finding gets a **CVSS 3.1 base score**, the industry-standard way to rate the technical severity of a weakness, with its vector shown so the score can be checked. We score **what was proven**, not what might happen next; possible follow-on impact is described in words under *Impact*. Where the business impact is clearly higher than the technical score, for example because personal data is exposed, we state an adjusted **risk** and explain why.

Severity	CVSS 3.1	Meaning for Northgate
CRITICAL	9.0–10.0	Exploitable without an account; fix immediately
HIGH	7.0–8.9	Serious exposure; fix within days
MEDIUM	4.0–6.9	Real weakness with a precondition; fix within weeks
LOW	0.1–3.9	Limited impact; fix in normal maintenance

4. Summary of findings

ID	Finding	Host	Severity	CVSS	Status
F-01	Cache server accepts commands without a password	cache-01	CRITICAL	9.8	Closed
F-02	Former contractor account still in Domain Admins, password never expires	dc-01	HIGH	8.1	Closed
F-03	Anonymous directory read exposes all users and a service account password	dc-01	HIGH	7.5	Closed
F-04	Guest-readable share holds a deployment account password	files-01	HIGH	7.5	Closed
F-05	SQL injection in the shop's product search	shop-01	HIGH	7.5	Closed
F-06	HR share readable by every domain user (payroll, passports)	dc-01	MEDIUM risk: High	6.5	Closed
F-07	Any customer can read any other customer's order	shop-01	MEDIUM	6.5	Closed
F-08	No account lockout; 7-character minimum password length	dc-01	MEDIUM	5.3	Closed

Severity at a glance

Critical (1)	
High (4)	
Medium (3)	
Closed after retest	

F-01 Cache server accepts commands without a password

Severity	CRITICAL CVSS 3.1 **9.8** · `AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
Affected	cache-01 · `10.10.10.20:6379` (Redis 7.0.15)
Status	**Closed: retest passed**

Description

The Redis cache service answers commands from any address on the network without authentication.

Impact

Anyone on the internal network can read and change every key in the cache and change the server's configuration while it runs. The shop depends on this cache. No keys or configuration were changed during testing.

Evidence

```
# nmap -sV -p 6379 10.10.10.20
6379/tcp open  redis   Redis key-value store 7.0.15
# redis-cli -h 10.10.10.20 PING
PONG                      ← answered with no password
```

Recommendation

Require authentication (Redis ACLs with one user per application, or at least `requirepass`). Bind to the application interface only, keep protected mode on, and allow port 6379 only from the application servers.

Retest (12 Oct 2026)

```
# redis-cli -h 10.10.10.20 PING
(error) NOAUTH Authentication required.
```

The application still reaches the cache with its own credentials. **Closed.**

F-02 Former contractor account still in Domain Admins

Severity	HIGH CVSS 3.1 **8.1** · `AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H`
Affected	dc-01 · domain `northgate.local` · account `it.temp`
Status	**Closed: retest passed**

Description

An account created for an IT contractor is still a member of **Domain Admins**, the group that controls the whole domain. Its own description says it should have been removed when the project ended. Its password is set to never expire.

Impact

Anyone who obtains this one password, through reuse, phishing of the former contractor, or guessing (see F-08), controls every computer and account in the domain. Because nobody owns the account, misuse is unlikely to be noticed. The score reflects that the password itself was not exposed (attack complexity high).

Evidence (read with the ordinary staff account, over encrypted LDAP)

```
# $L '(memberOf=CN=Domain Admins,CN=Users,DC=northgate,DC=local)' sAMAccountName | grep ^sAM
sAMAccountName: Administrator
sAMAccountName: it.temp
# $L '(sAMAccountName=it.temp)' description userAccountControl | grep -v ^dn
description: IT contractor, migration project. Remove when project ends.
userAccountControl: 66048   ← 512 normal account + 65536 password never expires
```

Recommendation

Remove `it.temp` from Domain Admins and disable it until someone confirms it is still needed. Give every privileged account a named owner and an expiry date, and review Domain Admins membership monthly.

Retest

```
sAMAccountName: Administrator          ← only member left
userAccountControl: 66050              ← +2 = account disabled
```

Closed.

F-03 Anonymous directory read exposes users and a password

Severity	HIGH CVSS 3.1 **7.5** · `AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`
Affected	dc-01 · `10.10.10.10:389` (LDAP) · account `svc_backup`
Status	**Closed: retest passed**

Description

The domain controller answers directory queries from anyone on the network without a login. One service account has a password typed into its description field.

Impact

Without any account, an attacker gets the full list of usernames (a ready-made target list) and a working domain password. The password was masked on capture and **never used**; reading it is the proof.

Evidence

```
# ldapsearch -x -H ldap://10.10.10.10 -b DC=northgate,DC=local '(sAMAccountName=svc_backup)' desc
ription \
    | sed -E 's/(password: ).*/\1********/I' | grep ^desc
description: Backup service. Temp password: ********
```

Recommendation

Block anonymous LDAP operations (restore the default dSHeuristics) and remove the Anonymous Logon read permission on the domain. Clear the description and **rotate the svc_backup password**, because it has been readable for as long as it was there. Never store secrets in directory attributes.

Retest

```
Operations error: 000004DC: LdapErr: ... Operation unavailable without authentication
```

The public rootDSE still answers, as it should. **Closed.**

F-04 Guest-readable share holds a deployment password

Severity	HIGH CVSS 3.1 **7.5** · AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Affected	files-01 · 10.10.10.30 · public/IT/deploy/map-drives.ps1 · account svc_deploy
Status	**Closed: retest passed**

Description

A file share is readable as guest (no account). It contains a drive-mapping script with the svc_deploy account's password in plain text, the account that opens the restricted shares.

Impact

Anyone on the network can obtain a working service account password and, with it, the contents of shares that guest cannot open. The script was read through a filter so the password never reached the screen; it was **never used**.

Evidence

```
# smbclient //10.10.10.30/public -N -c 'get IT/deploy/map-drives.ps1 -' 2>/dev/null \
    | sed -E 's/(pass = ")[^"]*(")/\1********\2/'
...
$pass = "********"        ← svc_deploy's password, masked as it was read (other lines abridged)
```

Recommendation

Disable guest access (map to guest = Never, guest ok = no). Remove credentials from scripts and use the signed-in user's identity or a managed service account. **Rotate svc_deploy now.**

Retest

```
NT_STATUS_ACCESS_DENIED   ← guest refused; svc_deploy password rotated
```

Closed.

F-05 SQL injection in the product search

Severity	HIGH CVSS 3.1 **7.5** · `AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`
Affected	shop-01 · `10.10.10.50:3000` · `/api/search?q=`
Status	**Closed: retest passed**

Description

The search builds its database query by pasting the visitor's search text into it, so the text can change what the query does.

Impact

An unauthenticated visitor can run queries with the application's own database access. The same database holds customers' orders and addresses. This was established with a minimal true/false test; **no records were extracted**.

Evidence

```
q=laptop'          → HTTP 500, database syntax error returned to the browser
q=laptop' OR '1'='1 → normal results
q=laptop' AND '1'='2 → no results         ← the query logic follows the input
```

Recommendation

Use parameterised queries for every database call. Return generic error messages. Give the application a database account that can read only what it needs, as defence in depth.

Retest

The quote no longer causes an error, the always-true condition returns nothing, and a normal search still works. **Closed.**

F-06 HR share readable by every domain user

Severity	MEDIUM CVSS 3.1 **6.5** · `AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N` · **Risk adjusted to High**
Affected	dc-01 · share `\\dc-01\HR`
Status	**Closed: retest passed**

Description

The HR share is meant for the HR Staff group, but its permissions also grant **read to Domain Users**, which is every account in the domain.

Impact

Every employee, and anyone who steals one employee's password, can read payroll, salary bands, performance reviews, disciplinary cases and scanned passports. The technical score is Medium because a login is required; the **risk is raised to High** because the share holds personal and identity data that would be reportable if exposed. Files were **listed only, never opened or downloaded**.

Evidence (ordinary IT staff account)

```
# smbclient //dc-01.northgate.local/HR -A ~/.creds/l.novak.auth -c ls
  payroll-2026-Q3.xlsx   salary-bands-2026.xlsx   performance-reviews-2026.docx
  disciplinary-cases.docx   passport-scans/
# smbcacls //dc-01.northgate.local/HR / -A ~/.creds/l.novak.auth
ACL:NORTHGATE\HR Staff:ALLOWED/OI|CI/RWXD
ACL:NORTHGATE\Domain Users:ALLOWED/OI|CI/READ   ← the cause
```

Recommendation

Remove Domain Users from the HR share; keep HR Staff. Review every share for broad groups (Domain Users, Authenticated Users, Everyone) and repeat the review quarterly.

Retest

```
NT_STATUS_ACCESS_DENIED listing \*
NT_STATUS_ACCESS_DENIED listing \passport-scans\*   ← the fix reached the files inside
```

The Public share still works for everyone, as intended. **Closed.**

F-07 Any customer can read any other customer's order

Severity	MEDIUM CVSS 3.1 **6.5** · `AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`
Affected	shop-01 · `/api/orders/<id>`
Status	**Closed: retest passed**

Description

The order API checks that the caller is signed in, but not that the order belongs to them (an insecure direct object reference).

Impact

Any customer account can read other customers' orders, including names and delivery addresses, by changing one number. One other customer's record was read to prove it; nothing was changed.

Evidence

```
GET /api/orders/1042   (tester's own order)   → 200
GET /api/orders/1041   (another customer)     → 200, returned with the same session
```

Recommendation

Check ownership in the handler and return 404 on a mismatch. Build the check into the data-access layer so every route gets it. Avoid sequential identifiers in URLs.

Retest

Order 1041 now returns 404 for the tester account; order 1042 still returns 200. **Closed.**

F-08 No account lockout and a short minimum password

Severity	MEDIUM CVSS 3.1 **5.3** · `AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`
Affected	dc-01 · domain password policy
Status	**Closed: retest passed**

Description

The domain never locks an account after wrong passwords, and the minimum length is seven characters.

Impact

Passwords can be guessed against every account indefinitely, and nothing stops or alerts on it. Next to F-02 this matters more: one guessed password could belong to a Domain Admin. Per the rules of engagement **no password guessing was performed**; the policy setting itself is the evidence.

Evidence

```
# $L -s base '(objectClass=*)' minPwdLength lockoutThreshold pwdProperties | grep -v ^dn
lockoutThreshold: 0
minPwdLength: 7
pwdProperties: 1
```

Recommendation

Lock accounts after 5 wrong attempts for 15 minutes, raise the minimum length to 12 or more (or adopt passphrases), and alert on repeated failures.

Retest

```
lockoutThreshold: 5
minPwdLength: 12
```

Closed.

6. What is already done well

Control	Why it matters
Plain-text LDAP logins are refused ("Transport encryption required")	Passwords cannot be sniffed from directory logins on the network
SMB signing required on the domain controller	Blocks relay attacks against the most important server
The IT admins' share refuses ordinary staff accounts	Least privilege works where it was configured; the HR share (F-06) was the exception
Same-day response and complete fixes	Every finding was fixed and passed retest within the testing window

7. Remediation roadmap

All technical findings are closed. These process changes stop the same weaknesses from coming back:

When	Action	Prevents
Now	Give every privileged and service account a named owner and an expiry date	F-02, F-03, F-04
Monthly	Review Domain Admins and other privileged groups	F-02
Quarterly	Review share permissions for broad groups (Domain Users, Everyone, guest)	F-04, F-06
Every release	Code review checklist: parameterised queries, ownership checks on every object	F-05, F-07
Ongoing	Secret scanning of shares and scripts; no passwords in descriptions or files	F-03, F-04
In 6–12 months	Repeat the test to confirm the controls hold	All

Appendix A: Tools

Tool	Used for
Kali Linux	Testing platform
nmap	Host and service discovery, version identification
ldapsearch (OpenLDAP)	Directory queries, anonymous and authenticated over LDAPS
smbclient, smbcacls (Samba)	Share listing and share permissions
redis-cli	Cache service authentication check
Burp Suite, curl	Web application requests and responses

Appendix B: Evidence handling

Raw evidence (command output and HTTP exchanges) was saved as text with timestamps and source address. Credentials were masked before being written anywhere. Evidence is kept encrypted for the period agreed with the client and then deleted; a deletion confirmation is provided on request.

Appendix C: Glossary

Active Directory (AD)	Microsoft's directory of users, computers and groups that controls logins across a company network
Domain Admins	The AD group with full control of every computer and account in the domain
LDAP / LDAPS	The protocol used to query the directory; LDAPS is the encrypted version
SMB share	A shared network folder on a Windows or Samba server
Assumed breach	Testing from the position of an attacker who already has one ordinary employee account
CVSS	Common Vulnerability Scoring System, the standard 0–10 technical severity score
Retest	Re-checking a finding after the fix, from the same position, to confirm it is closed

Cyber Era Offensive Security · penetration testing, scoping to retest · cybereraos.com · contact@cybereraos.com
Tester certifications: OSCP, OSCP+, CPENT, LPT (Master), CEH Master.
Sample report. Northgate Ltd is fictitious; all hosts, accounts, files and passwords are invented and were tested in an isolated lab.