Privilege Escalation Incident Report

This project demonstrates a real-world privilege escalation scenario caused by a misconfigured Group Policy Object (GPO) in an Active Directory environment.

A low-privileged domain user gained **local administrator privileges** on a Windows client due to incorrect GPO linking.

The project focuses on:

- Active Directory misconfiguration
- GPO abuse
- Security event analysis
- SOC detection and mitigation

Attack Scenario

Initial State

- User `alice.hr` is a standard domain user
- No administrative privileges on Windows 10

Misconfiguration

- A GPO configuring **Local Administrators group membership** was mistakenly linked to the **HR OU**

Result

- `alice.hr` was automatically added to the local Administrators group on the client machine

Detection & Log Analysis

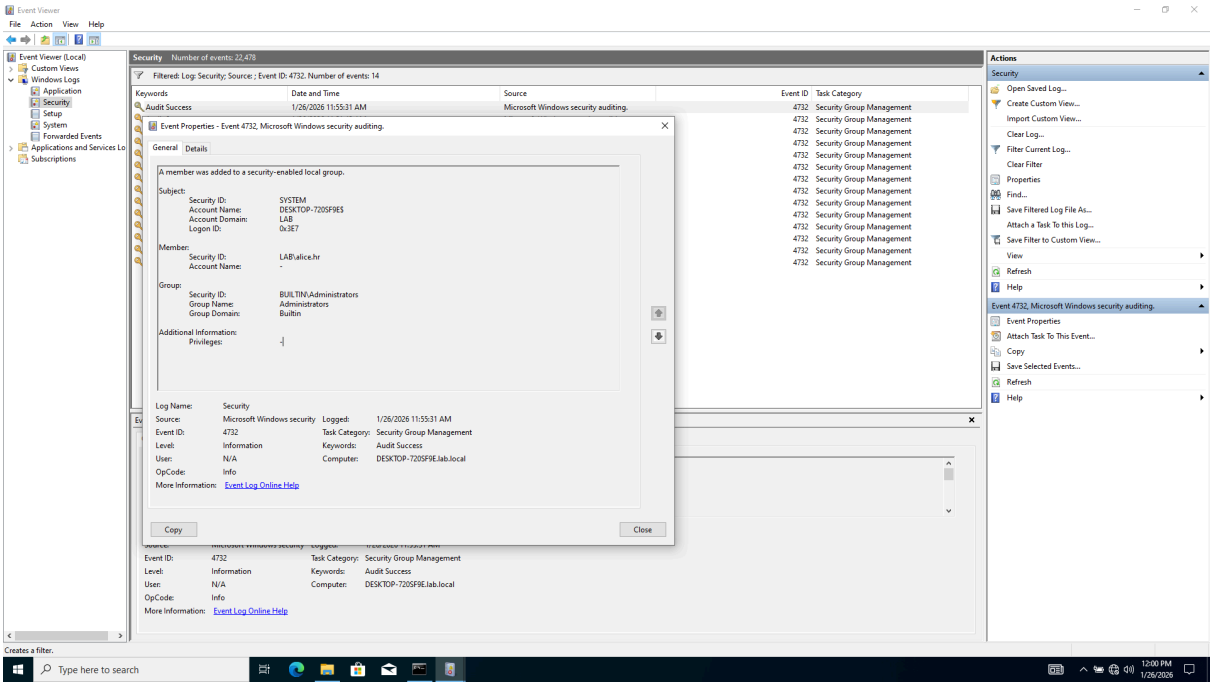
Windows 10 — Event ID 4732

Description: A member was added to a security-enabled local group

Key findings:

- User: `LAB\alice.hr`
- Group: `Administrators`
- Subject: `SYSTEM` (indicates GPO enforcement)

Confirms **local privilege escalation**



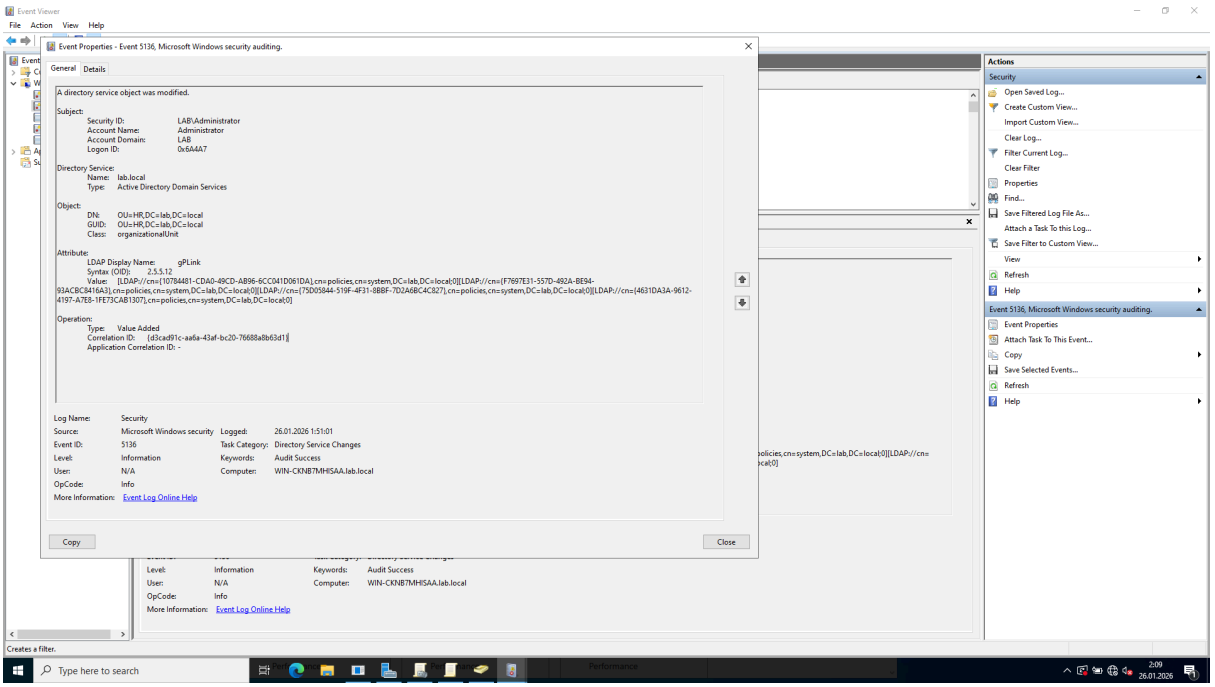
Domain Controller — Event ID 5136

Description: A directory service object was modified

Key findings:

- Attribute modified: `gPLink`
- Target object: `OU=HR`
- Operation: `Value Added`

Confirms **GPO was linked to HR OU**



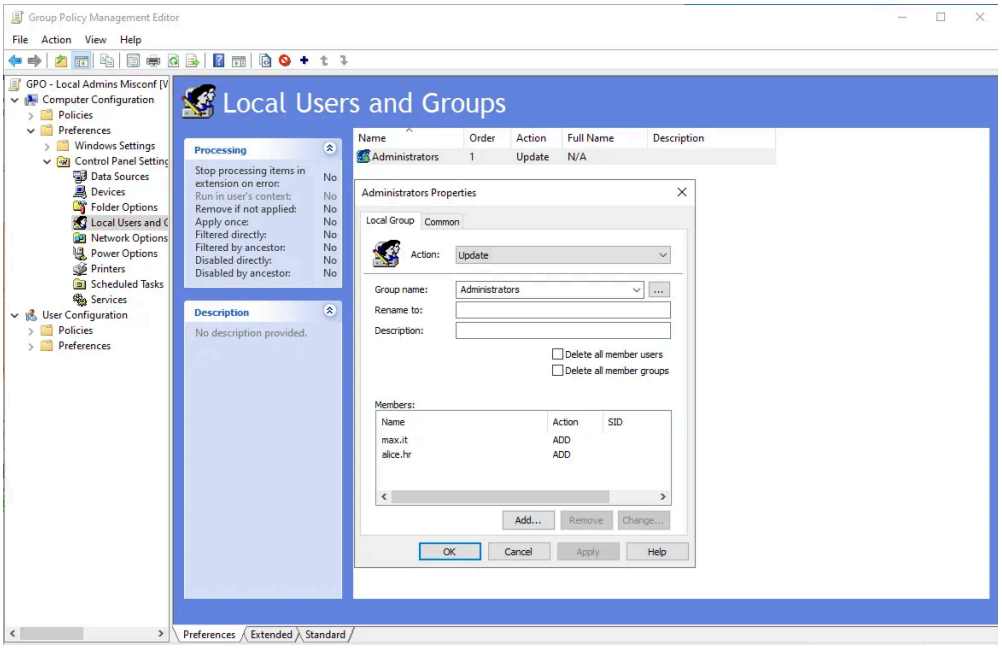
Impact Assessment

- User gained full local administrative access
- Ability to install software, disable security controls, and dump credentials
- Potential lateral movement risk

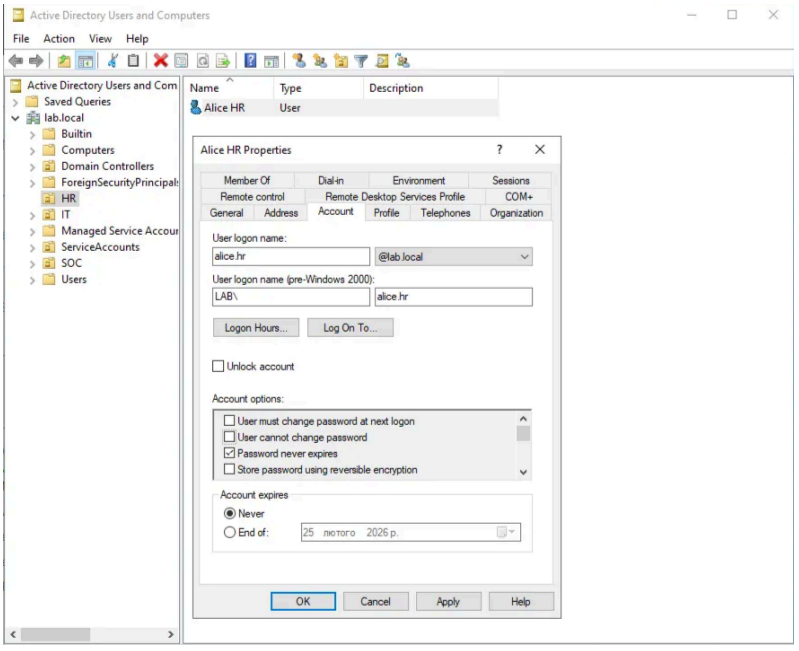
Mitigation & Recommendations

- Review GPO scope before linking
- Separate administrative GPOs
- Restrict GPO editing permissions
- Monitor:
  - Event ID 5136 (GPO changes)
  - Event ID 4732 (local admin changes)

GPMC — GPO Details

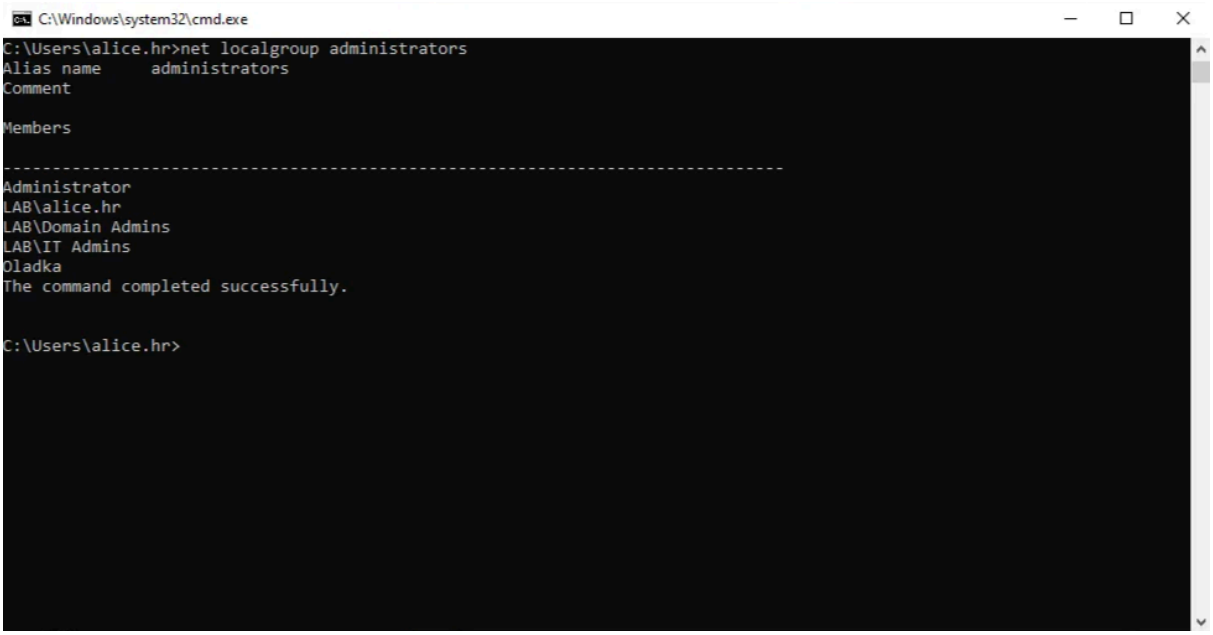


OU HR (ADUC)

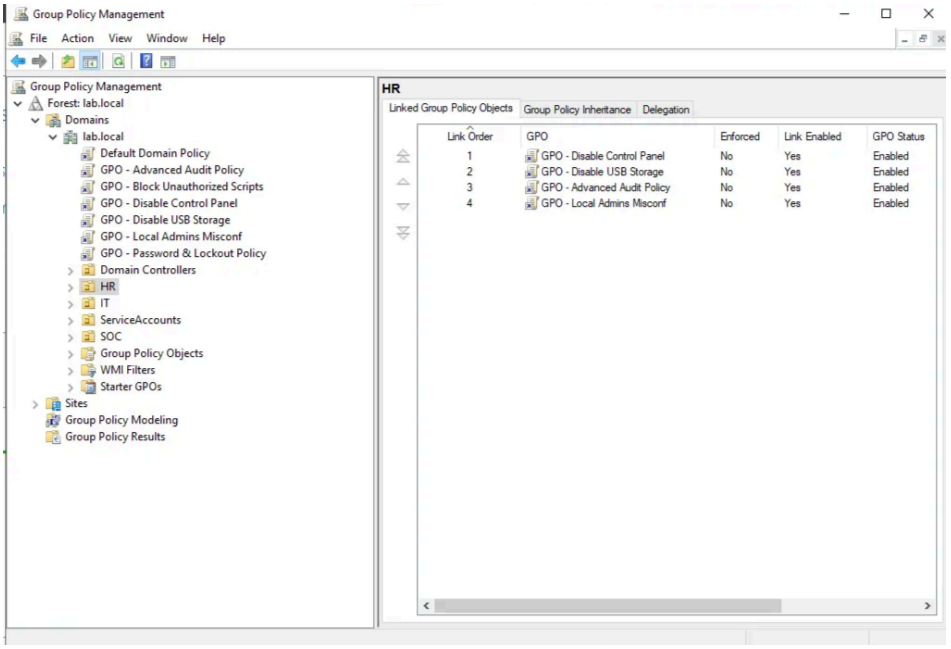


Client Verification

Windows 10 (alice.hr)


C:\Windows\system32\cmd.exe
C:\Users\alice.hr>net localgroup administrators
Alias name administrators
Comment
Members
Administrator
LAB\alice.hr
LAB\Domain Admins
LAB\IT Admins
Oladka
The command completed successfully.
C:\Users\alice.hr>

Linked GPO


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: lab.local
Domains
lab.local
Default Domain Policy
GPO - Advanced Audit Policy
GPO - Block Unauthorized Scripts
GPO - Disable Control Panel
GPO - Disable USB Storage
GPO - Local Admins Misconf
GPO - Password & Lockout Policy
Domain Controllers
HR
IT
ServiceAccounts
SOC
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
HR
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
1 GPO - Disable Control Panel No Yes Enabled
2 GPO - Disable USB Storage No Yes Enabled
3 GPO - Advanced Audit Policy No Yes Enabled
4 GPO - Local Admins Misconf No Yes Enabled