Help Desk Simulation

Incorrect Password Attempts and Account Lockout Resolution

Objective

The purpose of this simulation is to demonstrate how failed domain login attempts and account lockouts are identified, investigated, and resolved in an Active Directory environment.

Environment

• Domain Controller: Windows Server 2022

• Client OS: Windows 10 (domain-joined)

• Domain Services: Active Directory Domain Services (AD DS)

• Tools Used:

- Event Viewer
- Active Directory Users and Computers
- Group Policy Management

Ticket Summary

Issue: User unable to log in due to account lockout
Category: Access / Authentication
Priority: Medium

Reported Issue

- User reported being unable to log in to their domain account.
- System displayed "Incorrect password" after multiple login attempts.
- After repeated attempts, the system displayed:
  "The referenced account is currently locked out and may not be logged on to."

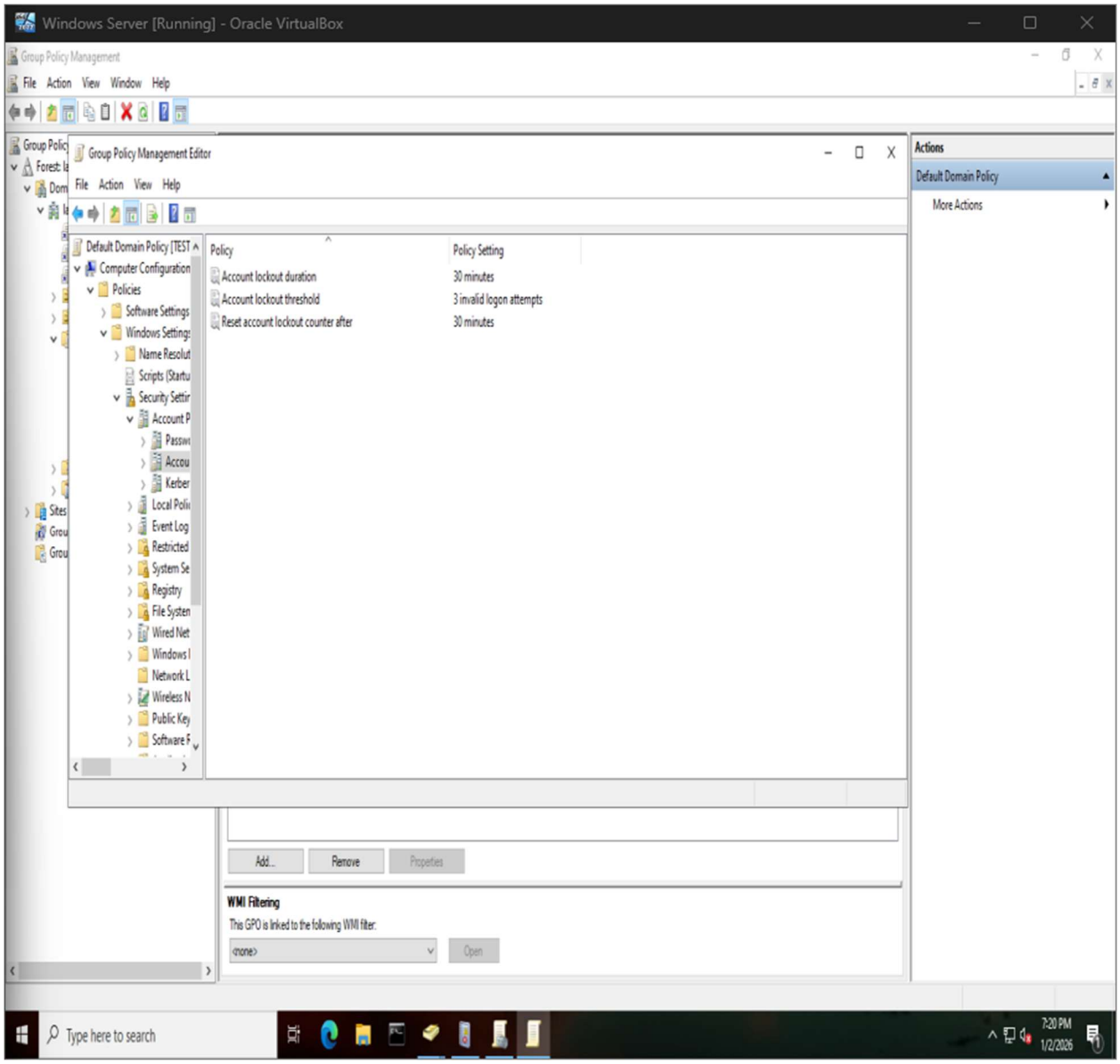
Troubleshooting & Investigation

- Verified user identity according to support procedures.
- Confirmed the correct username format with the user.
- Checked account status in Active Directory.
- Identified that the user account was locked due to multiple failed login attempts.
- Unlocked the account in Active Directory Users and Computers.
- Asked the user whether they preferred to reset the password independently or with assistance; the user chose to reset it themselves.

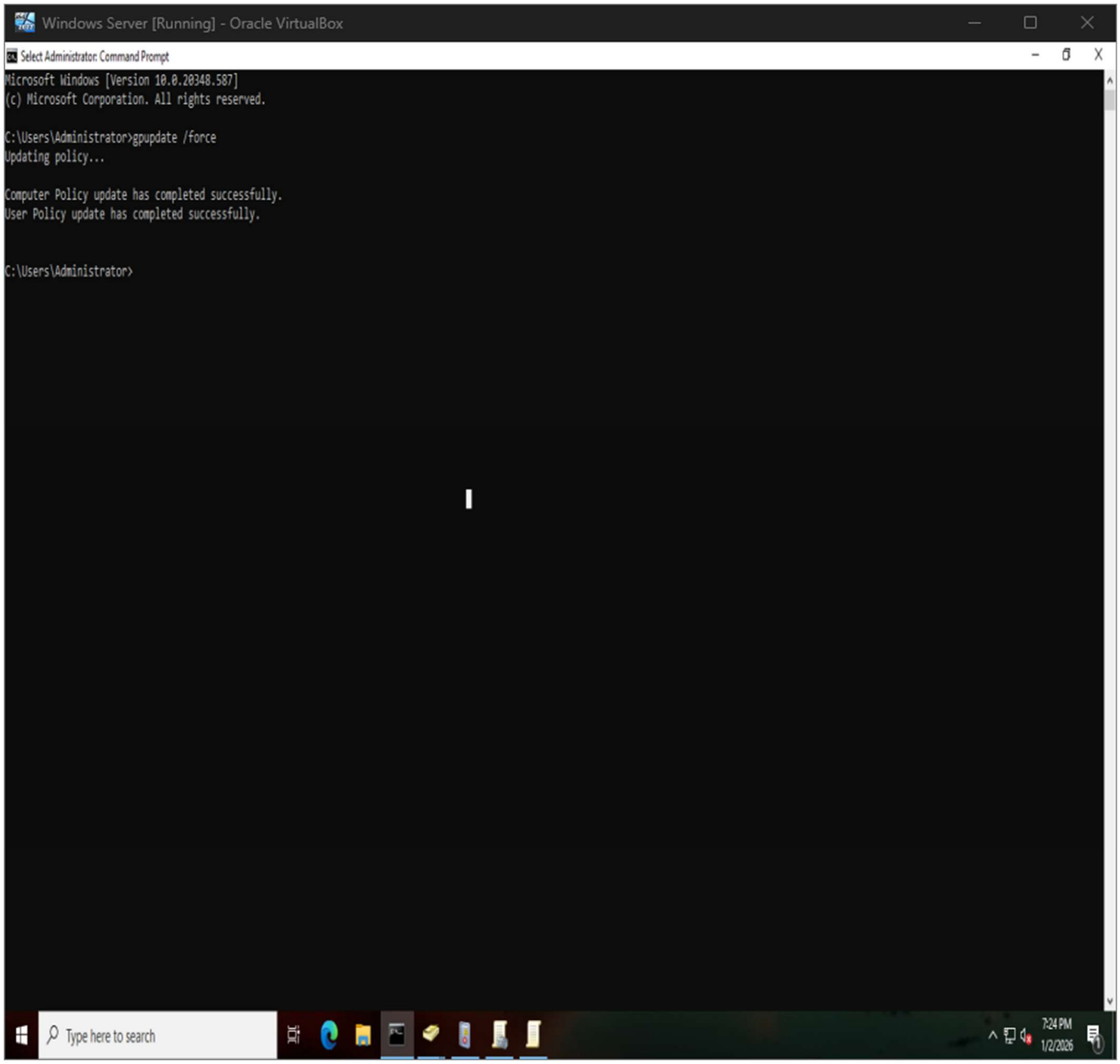
Resolution

- Guided the user through the password reset process.
- Allowed the user to create a new secure password.
- Confirmed successful login after password reset.
- Educated the user on best practices to avoid future lockouts (e.g., verifying credentials before repeated attempts).

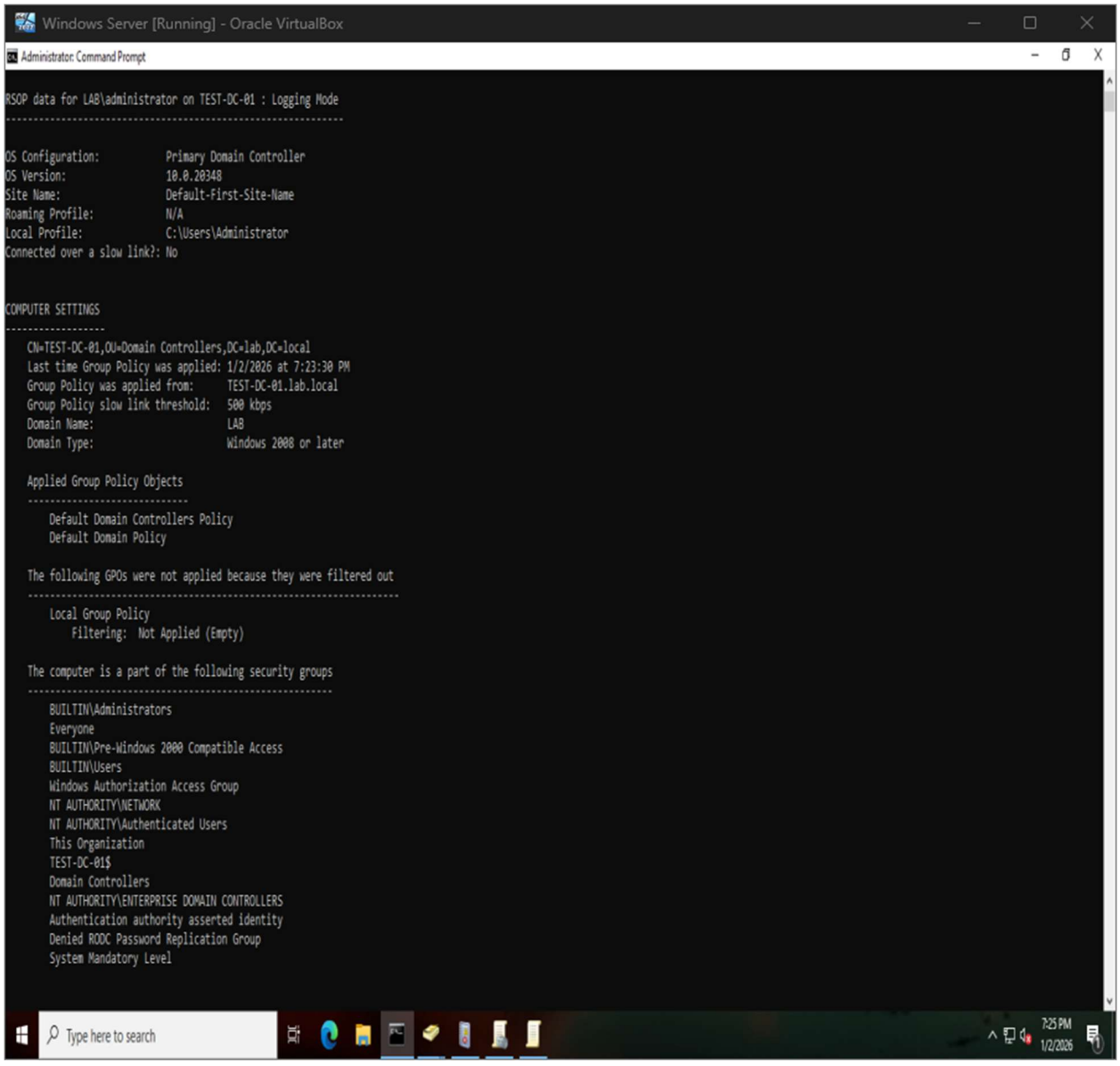
1. Created account lockout policies in Group Policy to set the threshold for invalid login attempts.



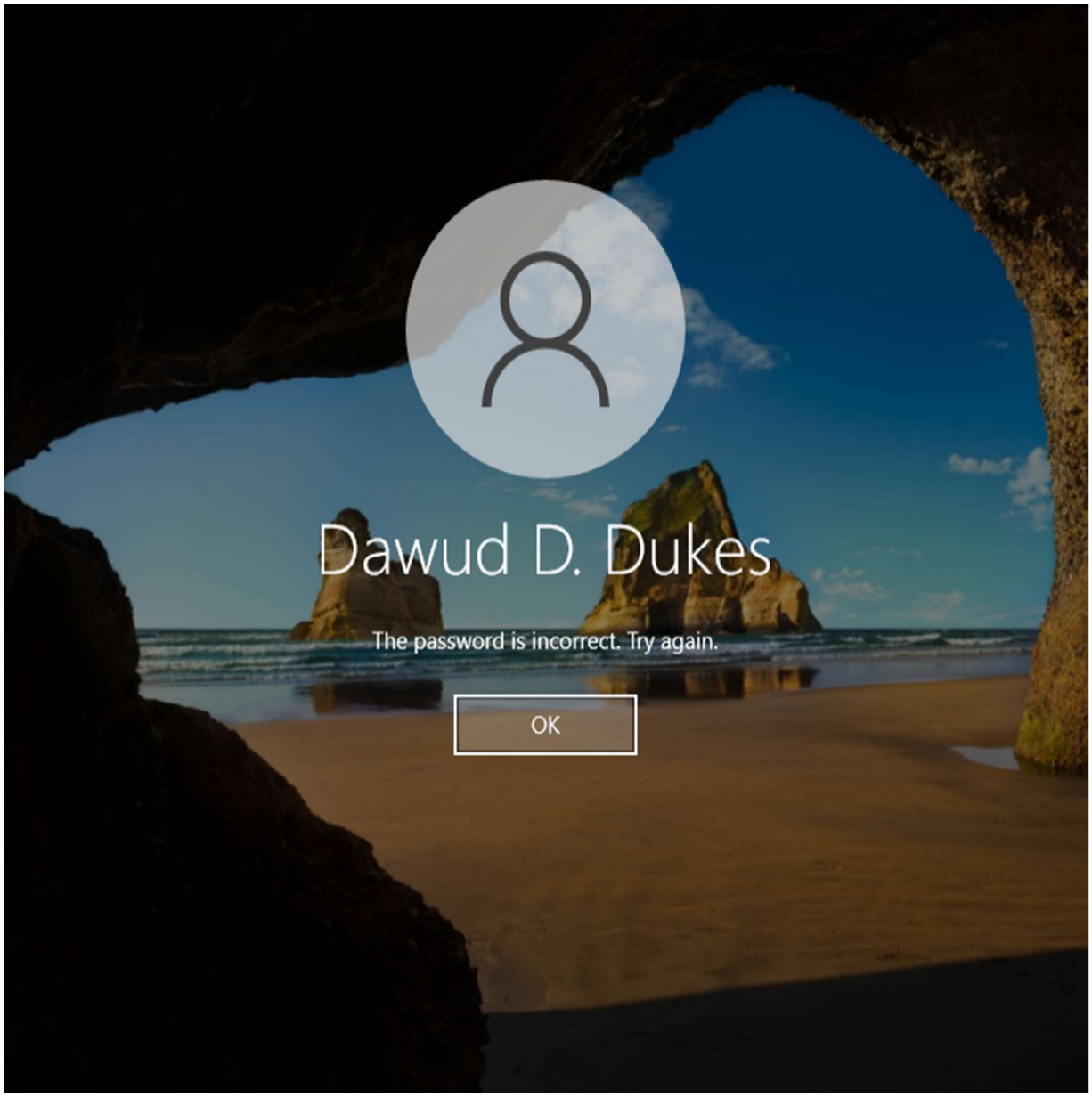
2. Group Policy was manually refreshed using the gpupdate /force command to ensure the latest domain security and lockout policies were applied and enforced.



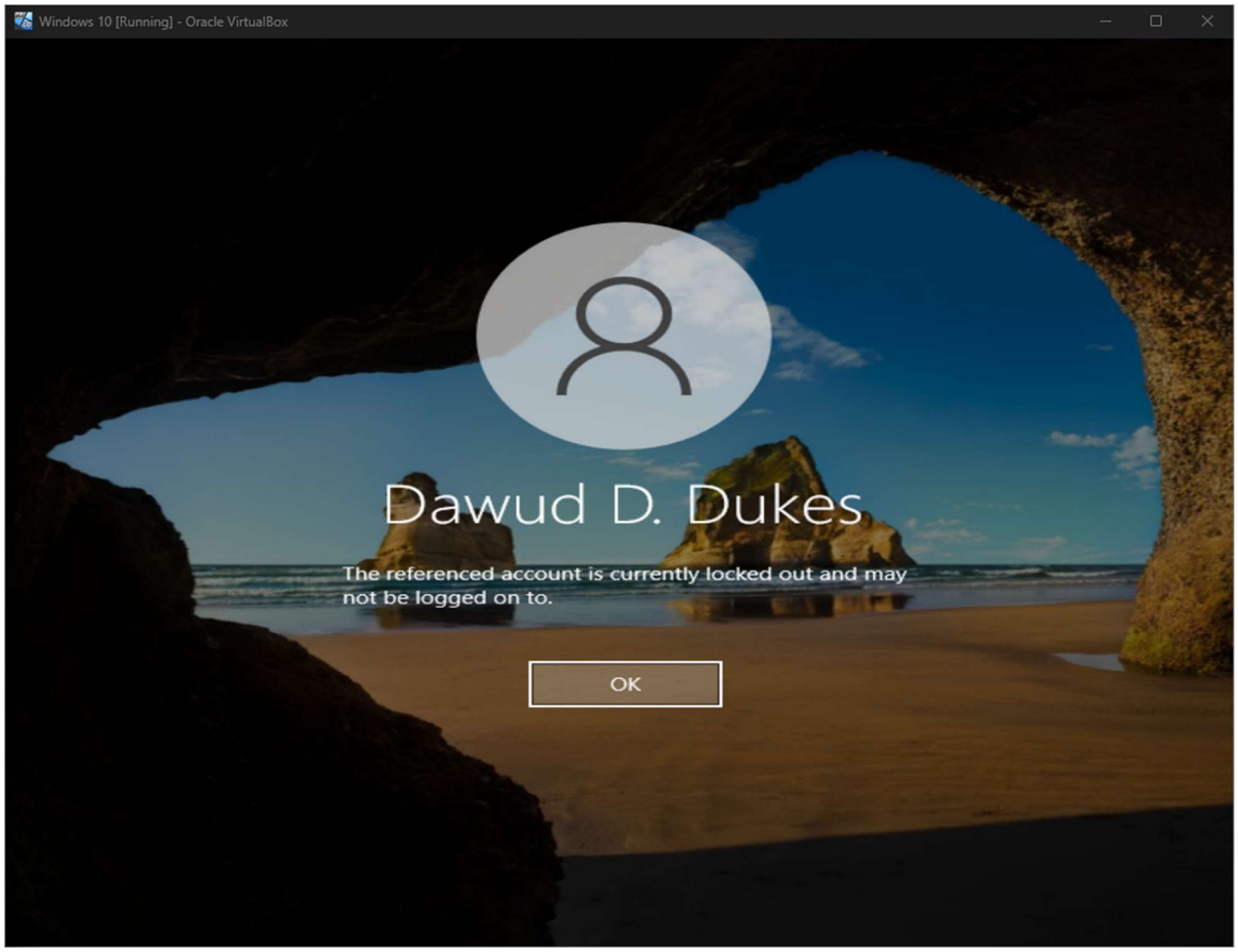
3. The applied Group Policy settings were verified using the gpresult command to confirm that account lockout policies were successfully applied to the system.



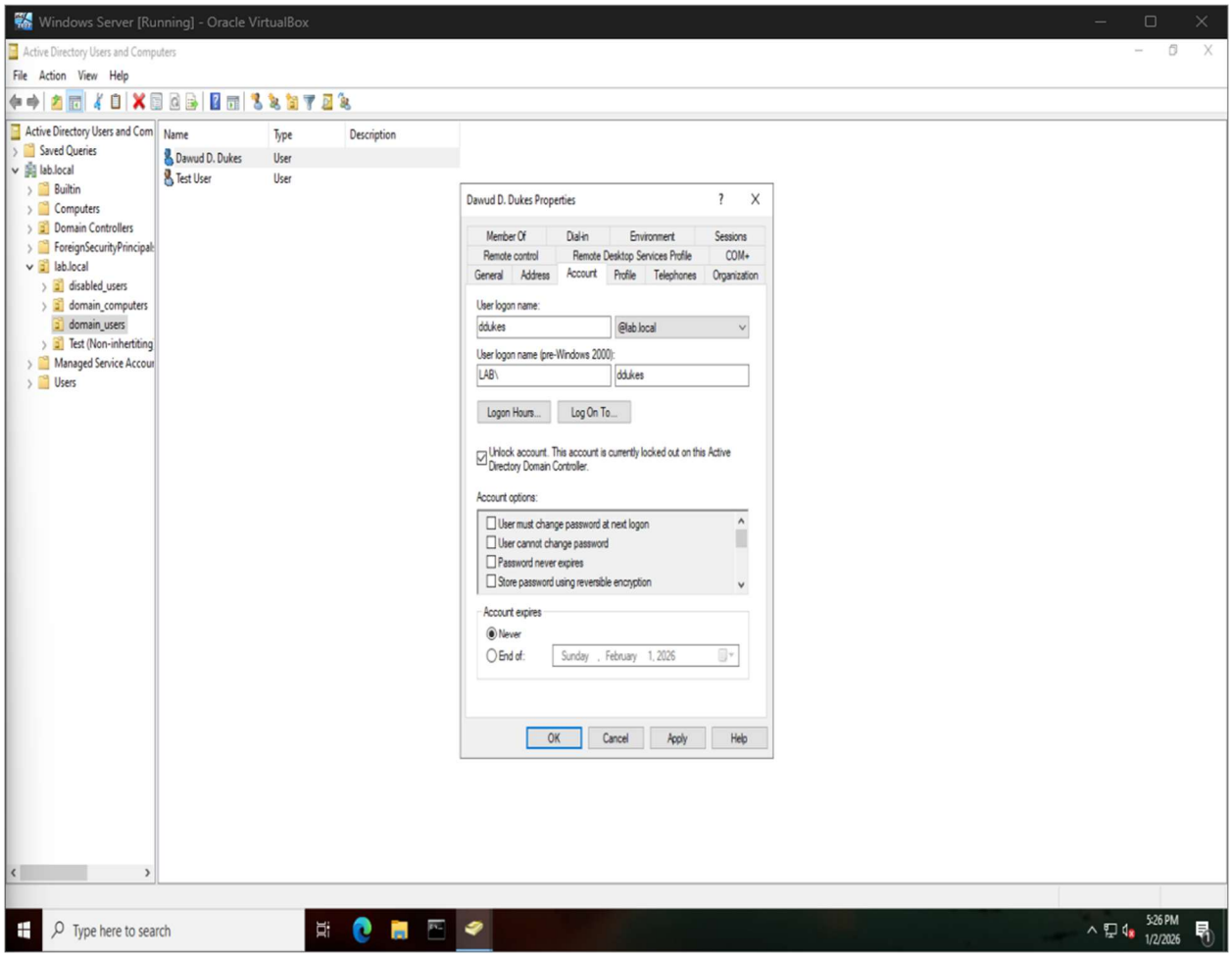
4. The user attempted to log in to their domain account using an incorrect password, resulting in a failed authentication attempt at the workstation.



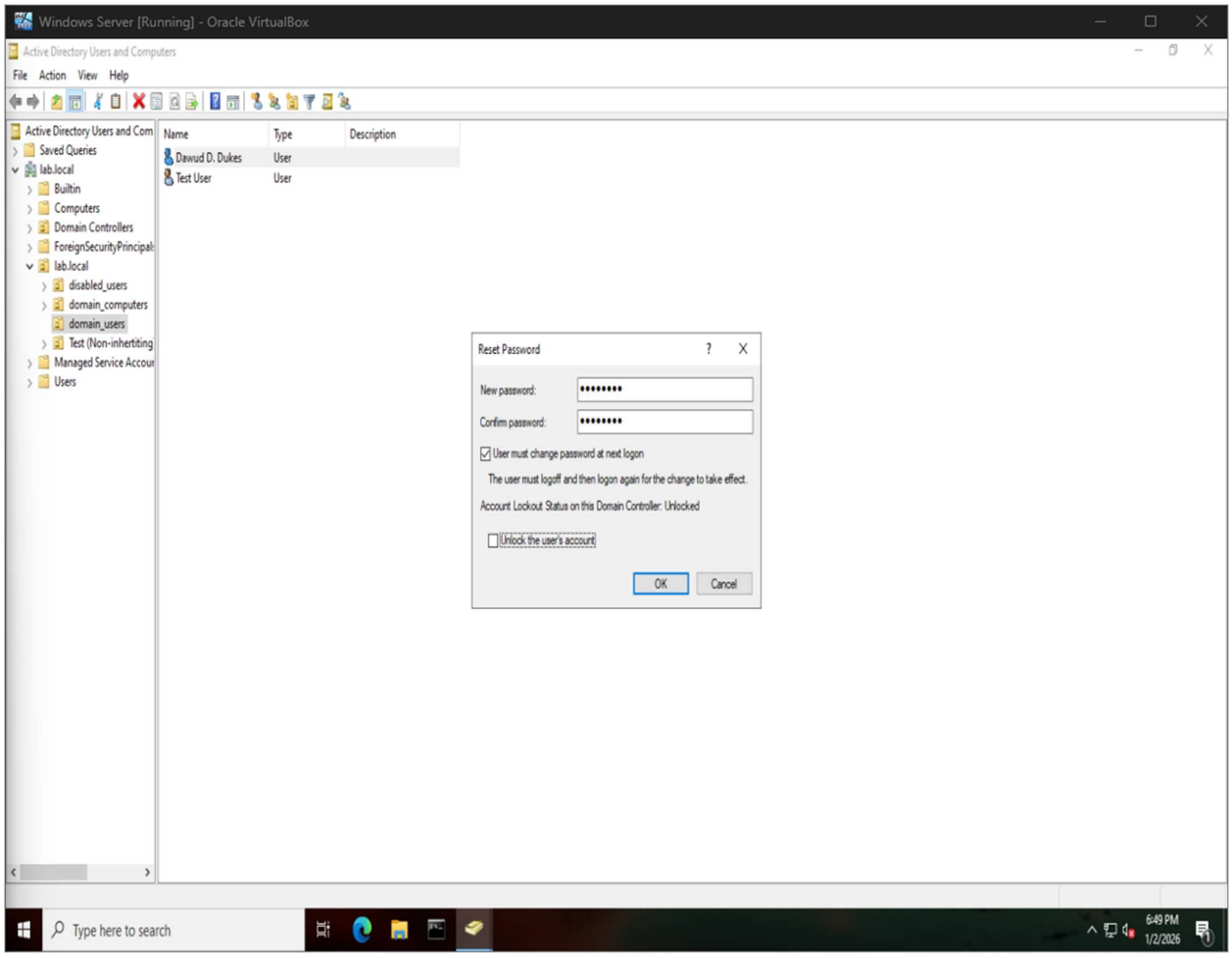
5. After exceeding the configured account lockout threshold defined by domain policy, the user account was automatically locked to prevent further unauthorized access attempts.



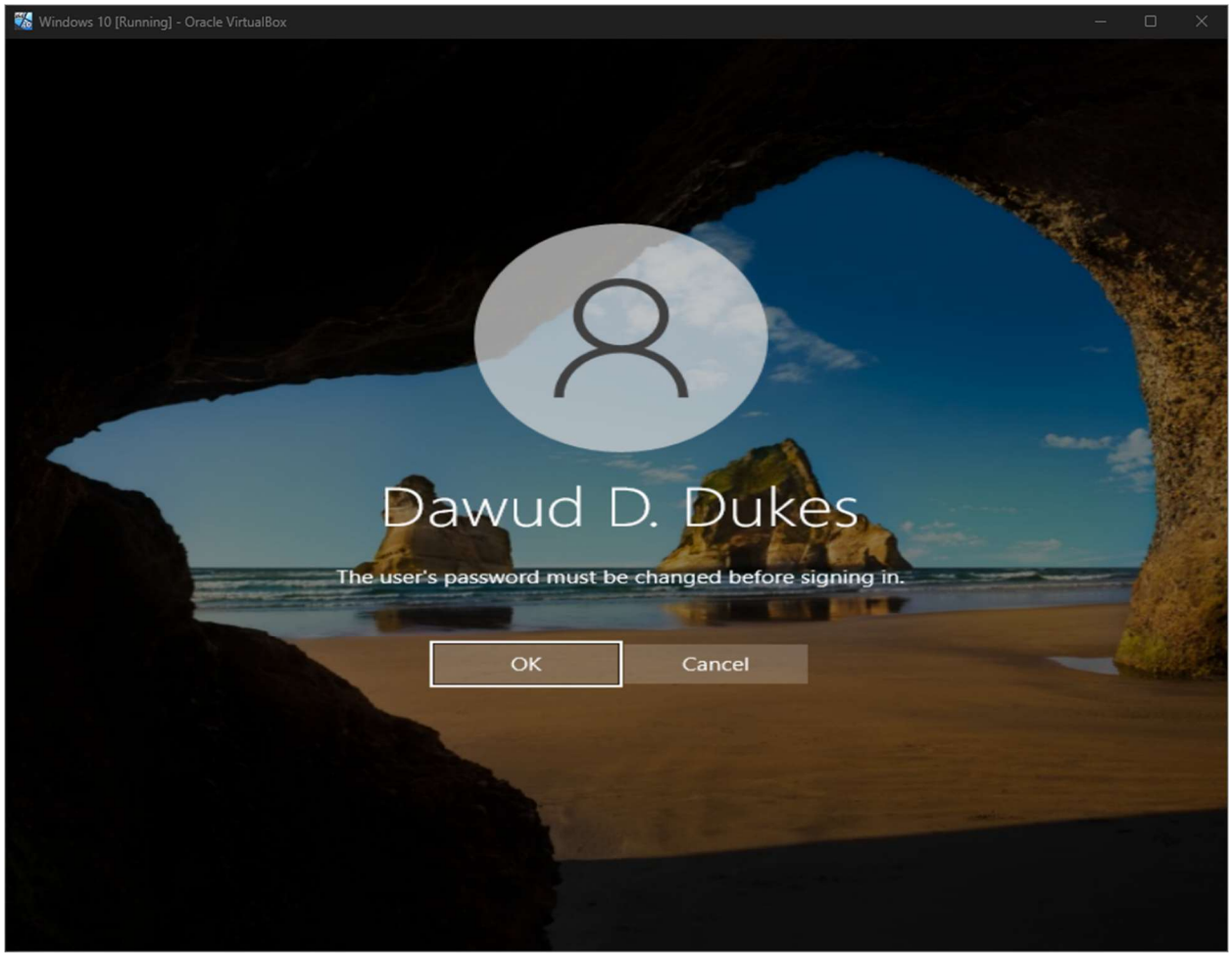
6. The locked user account was unlocked in Active Directory Users and Computers.



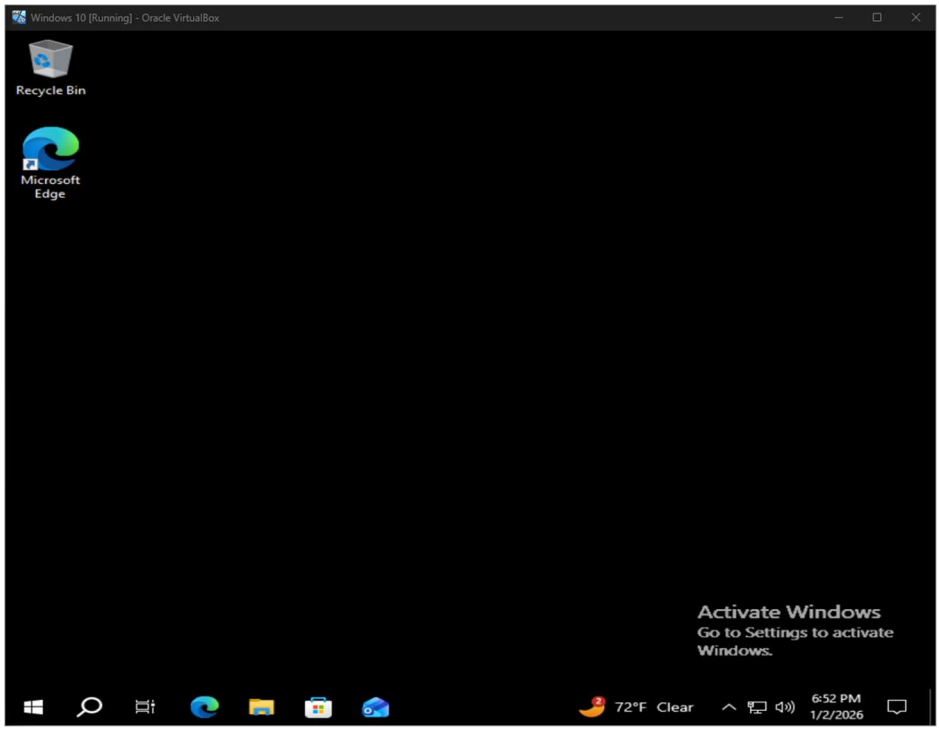
7. Temporary passwords were assigned to restore user access while maintaining security controls.

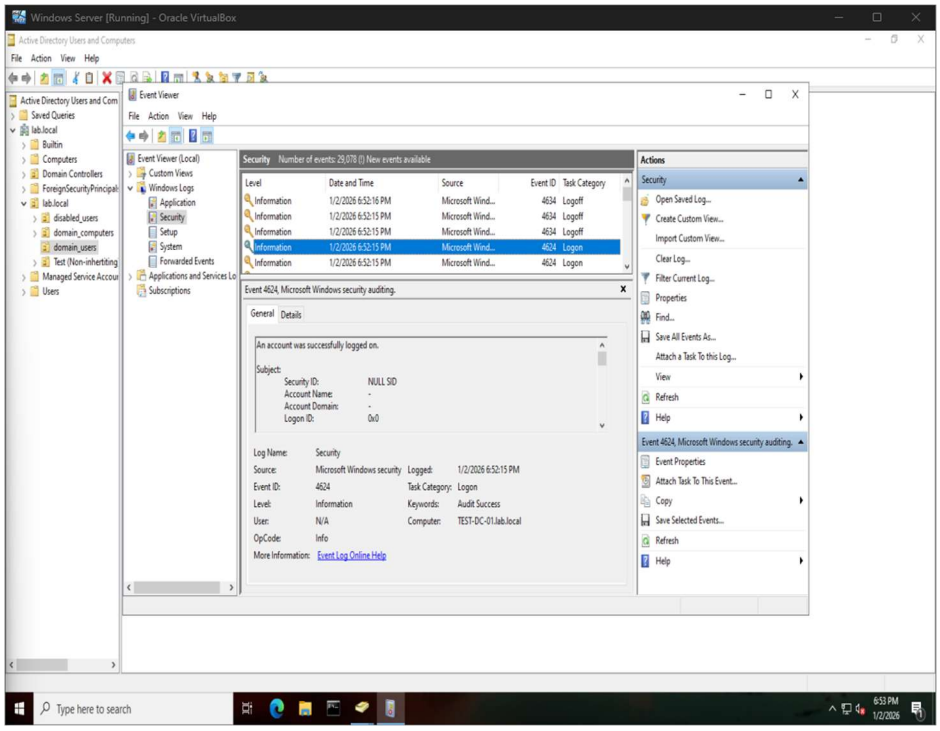


8. The user logged in using the temporary password and was prompted to create a new secure password.



9. Successful authentication confirmed that the account lockout issue had been fully resolved.





Resolution

The issue was resolved by identifying failed authentication attempts, confirming account lockout enforcement, restoring access through account unlock and password reset, and verifying successful login in the Active Directory domain environment.