

Lab 1 – Active Directory Hardening & Account Lockout Policy Enforcement

Fuaineaitee Willie

Objective

The objective of this lab was to deploy a functional Active Directory domain environment and implement security controls designed to detect and mitigate brute-force authentication attempts. This lab emphasized identity management, centralized authentication, policy enforcement, and security log validation within a Windows-based enterprise infrastructure.

The project simulated foundational blue team responsibilities: implementing authentication hardening controls, validating policy enforcement, and analyzing Windows Security event logs.

Environment

- Windows Server 2022 (Domain Controller – DC01)
- Windows 10 Client (Domain-Joined Endpoint)
- Oracle VirtualBox
- Internal Network: 192.168.10.0/24
- Static IP Assignment (DC01: 192.168.10.10)

Security Architecture Overview

A Windows Server 2022 system was promoted to a Domain Controller hosting the lab.local domain. Organizational Units (IT, HR) were created to simulate departmental segmentation within an enterprise directory structure. Security groups were implemented to reflect role-based access control (RBAC) principles.

A Windows 10 endpoint was domain-joined to simulate a corporate workstation. Security hardening was applied through a custom Group Policy Object enforcing account lockout thresholds to mitigate password brute-force attacks.

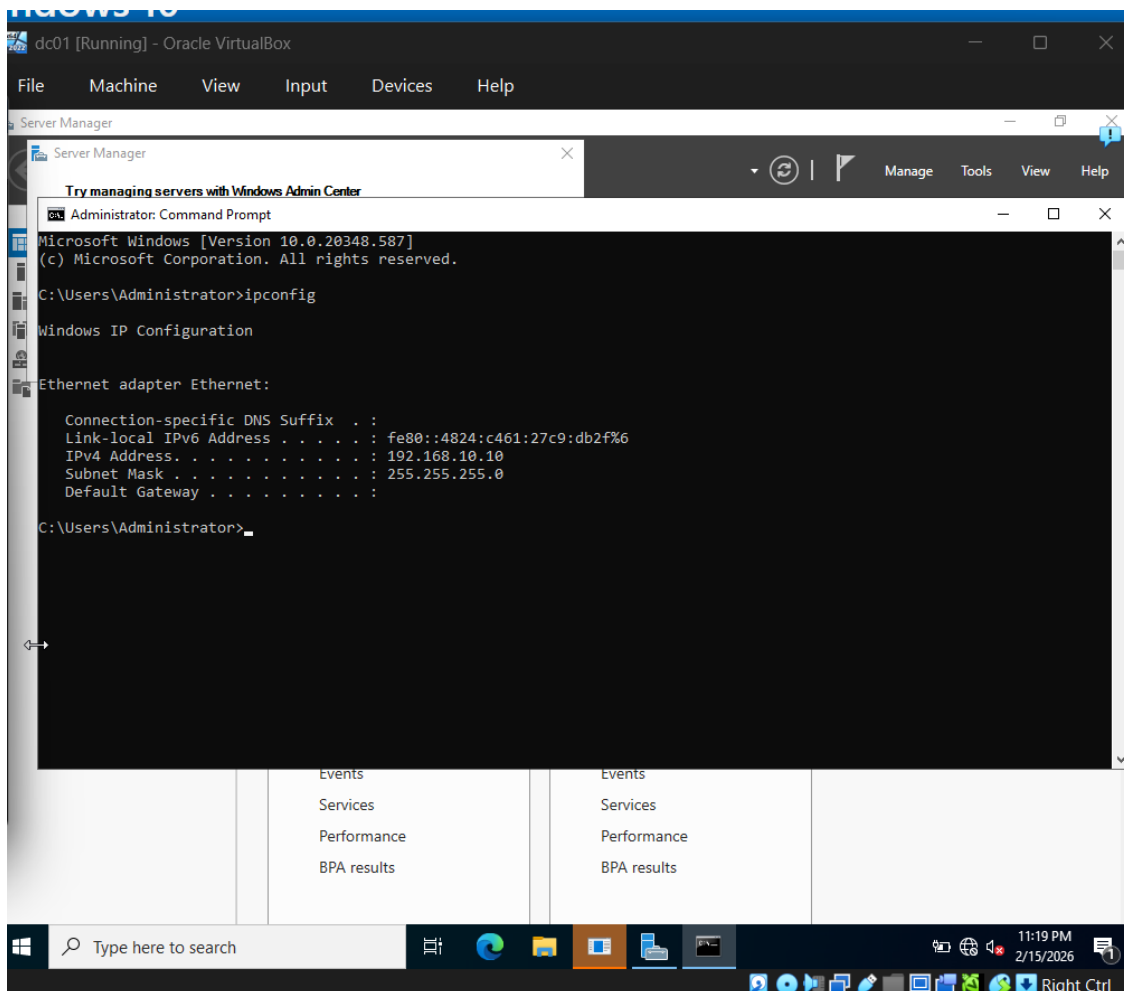
Policy enforcement and authentication integrity were validated using:

- gpupdate /force
- gpresult /r
- gpresult /h
- Event Viewer (Security Logs)

Security Control Implementation (Screenshot Evidence)

1. Domain Controller Static Configuration

Configured a static IP address (192.168.10.10) on DC01 to ensure reliable DNS resolution and authentication services. Domain Controllers must maintain consistent addressing to preserve identity infrastructure stability.

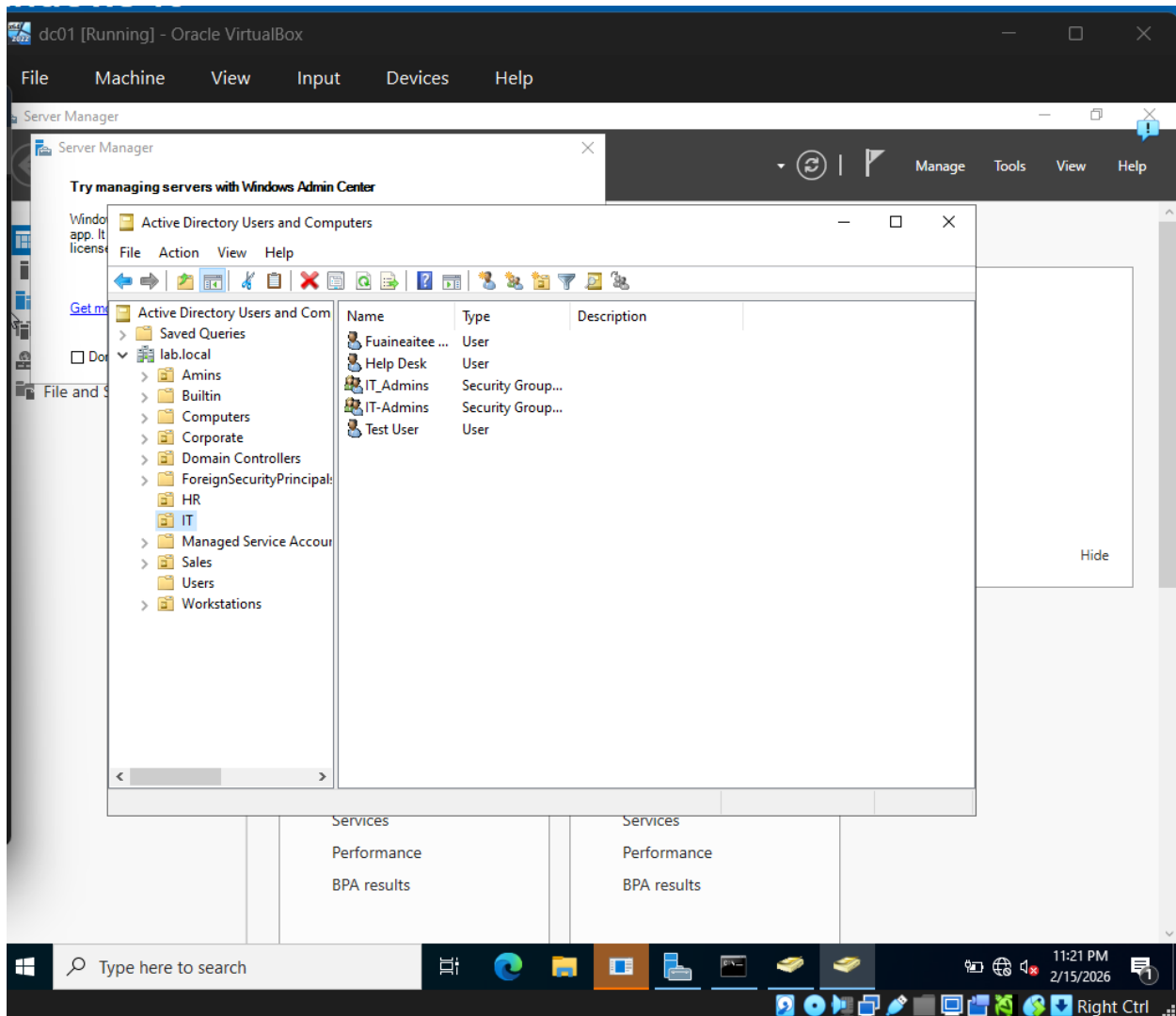


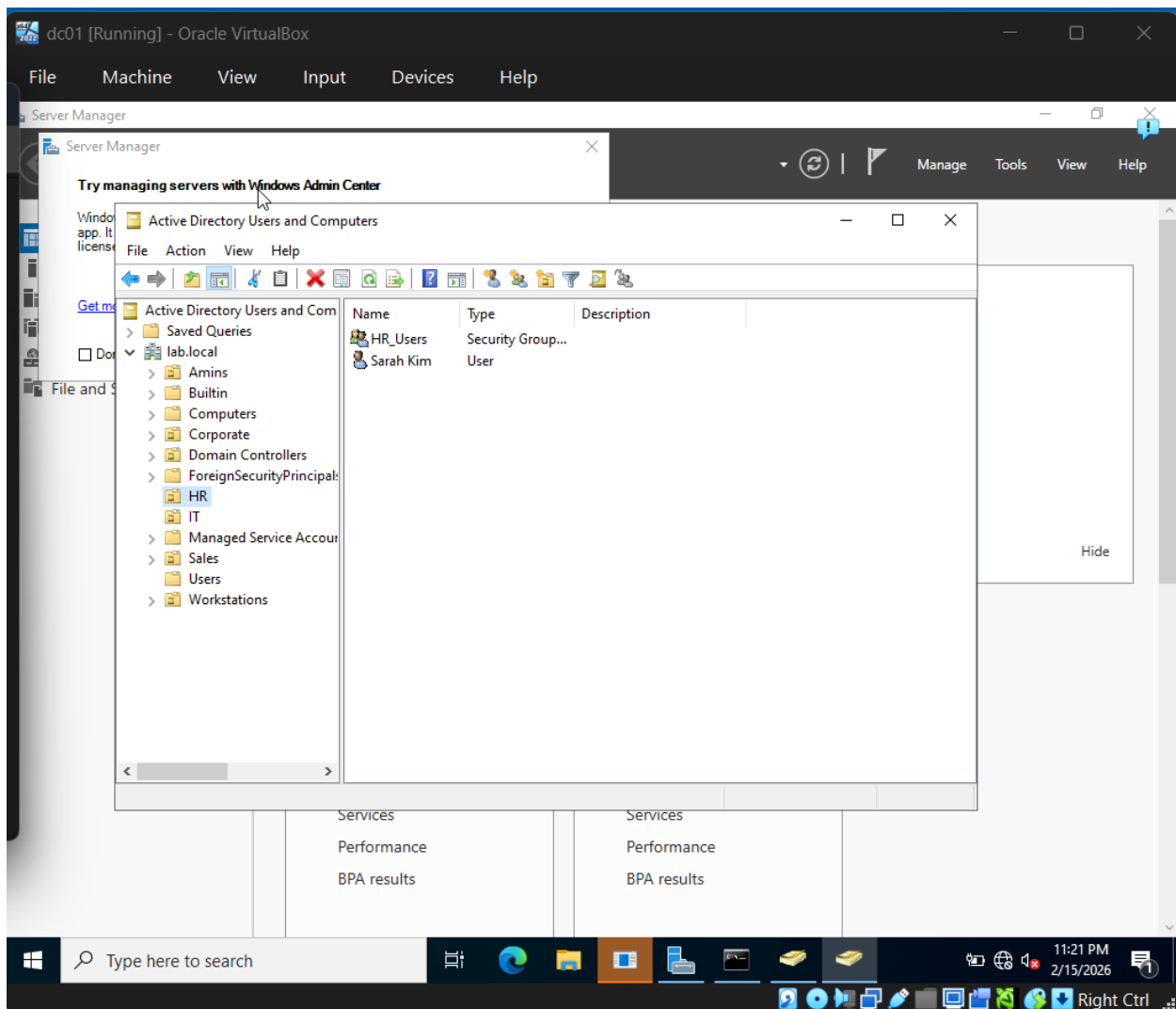
2–3. Identity & Access Structure

Created:

- Organizational Units (IT, HR)
- Department-specific user accounts
- Security groups (IT_Admins, HR_Users)

This demonstrates structured identity segmentation and adherence to least privilege principles.



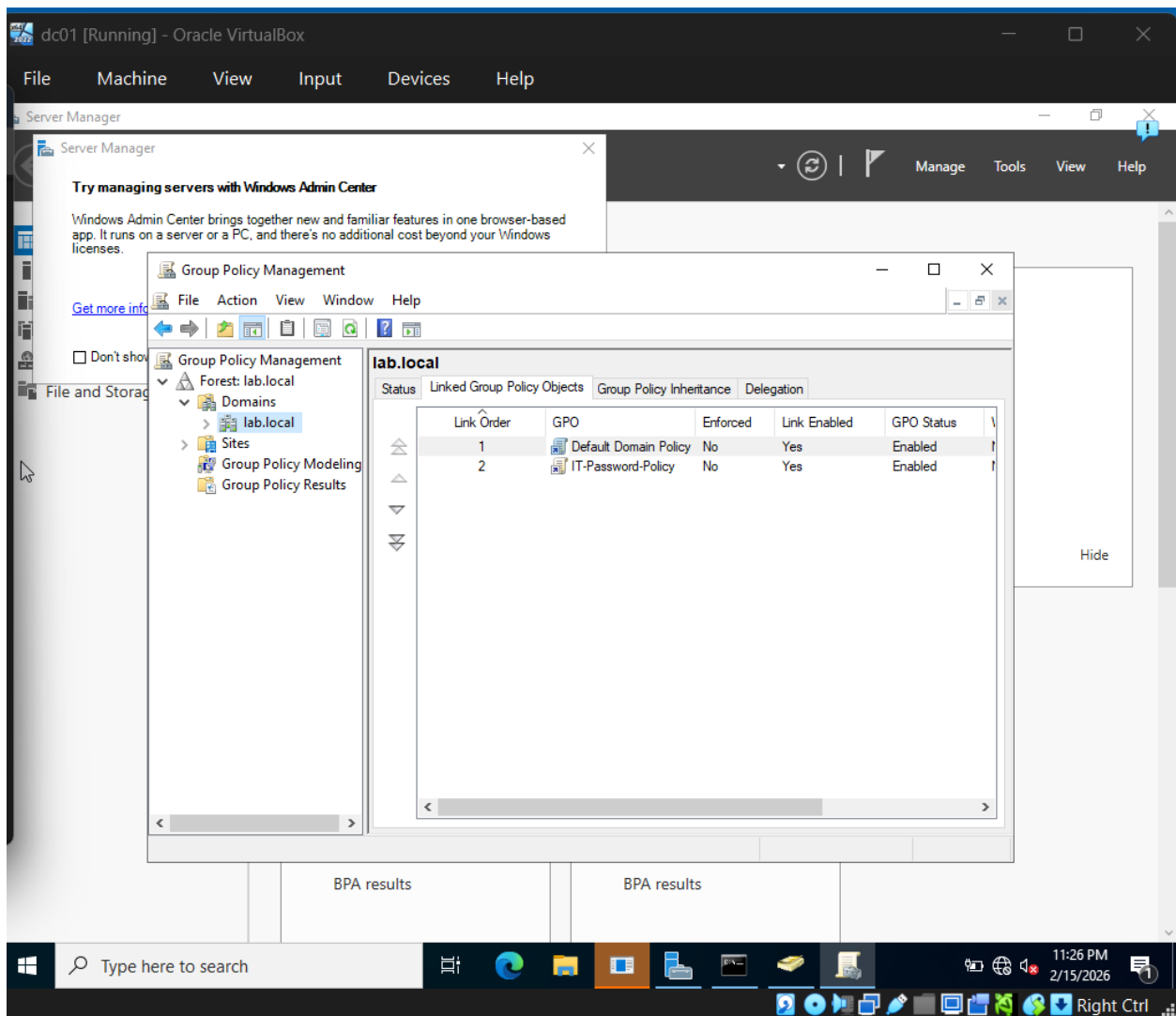


4. Group Policy Enforcement

Created and linked a custom GPO (IT-Password-Policy) to enforce:

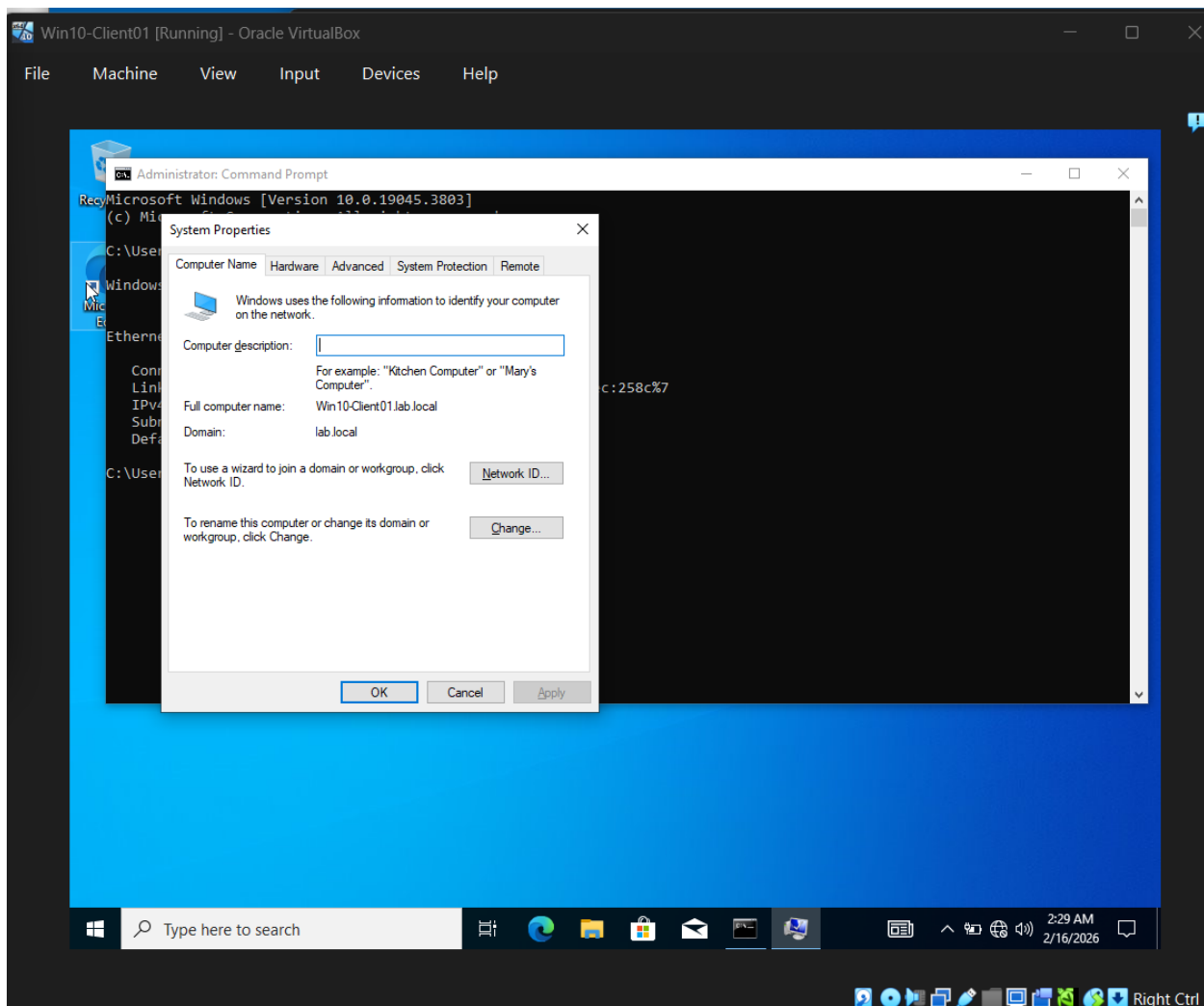
- Account lockout threshold
- Lockout duration
- Reset account lockout counter

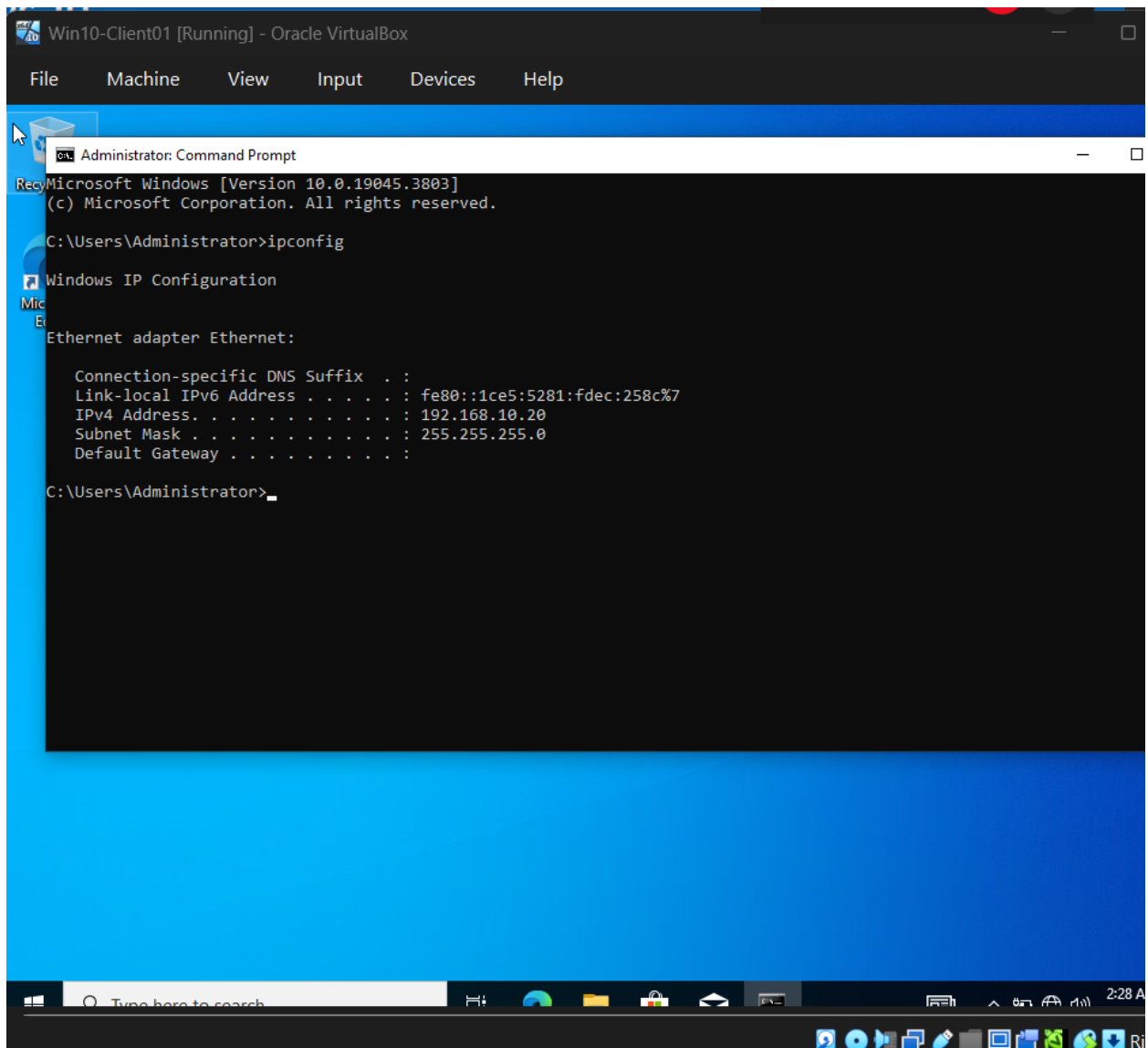
Validated link status and enforcement within Group Policy Management Console.



5–6. Endpoint Integration

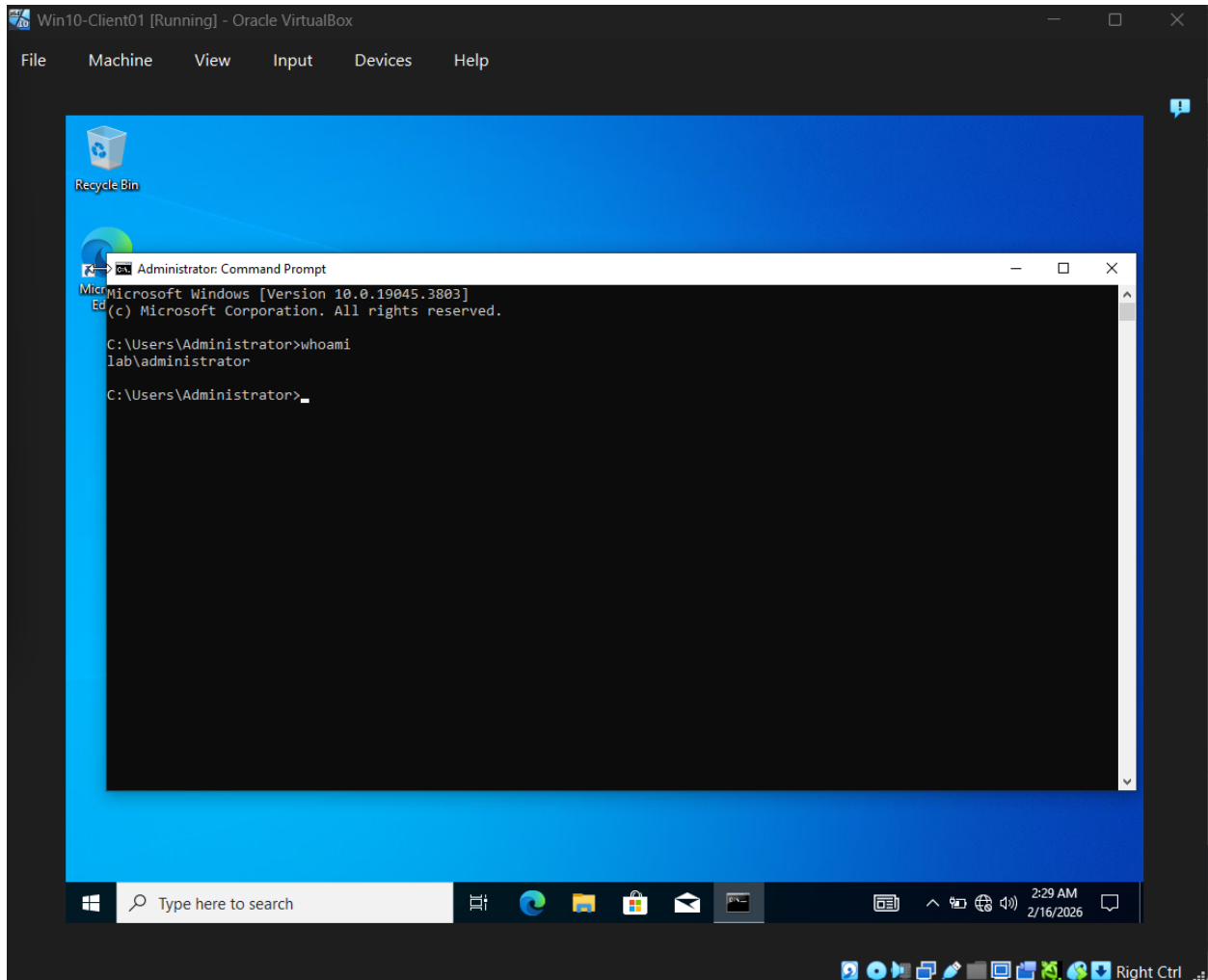
Successfully joined the Windows 10 endpoint to the lab.local domain and verified domain authentication.





7. Domain Authentication Validation

Executed `whoami` to confirm authentication under the lab domain context, validating centralized identity management.



8. Brute-Force Simulation & Log Analysis

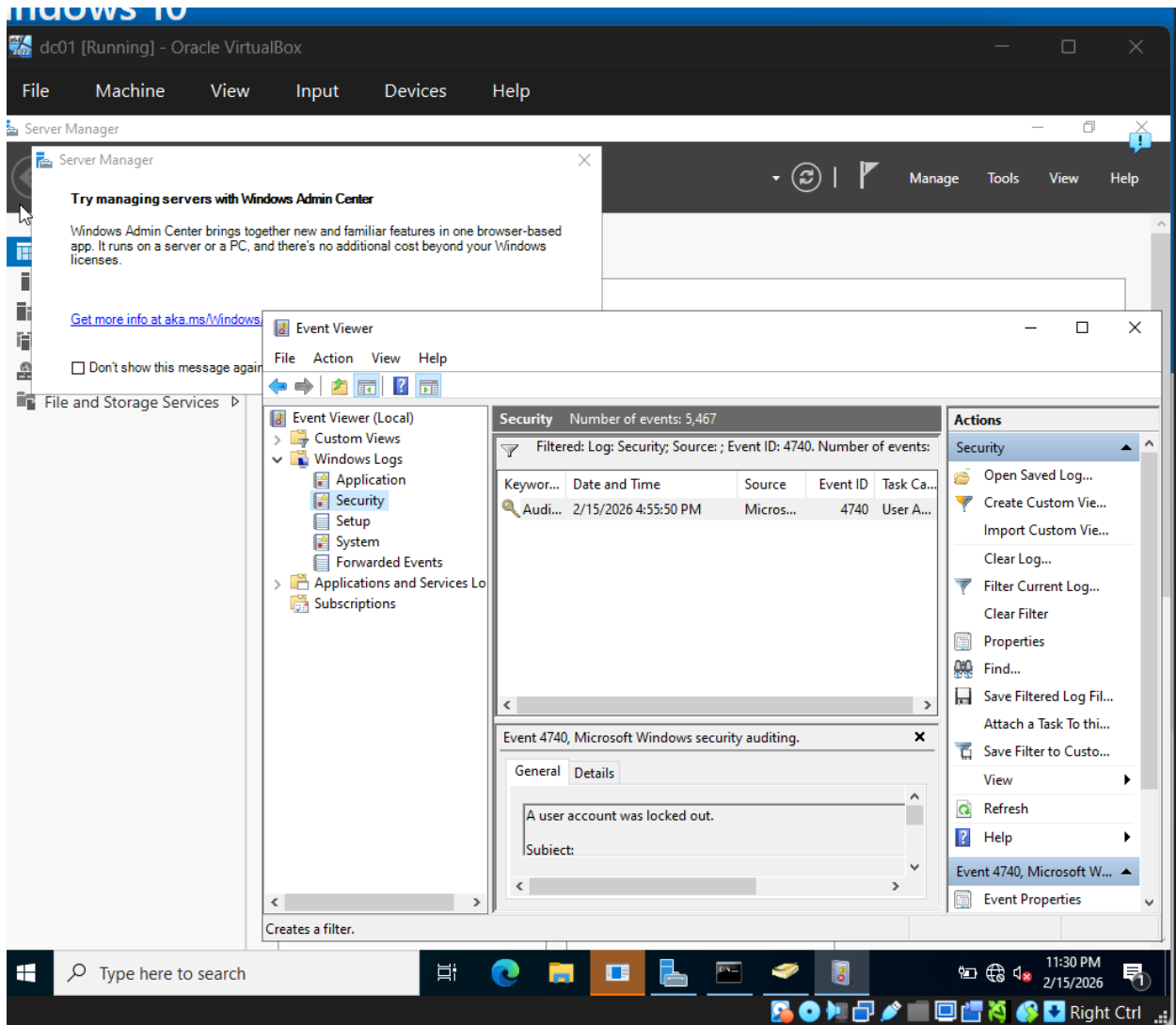
Simulated repeated failed login attempts on the Windows 10 endpoint.

Validated:

- Account lockout triggered as configured
- Event ID 4740 recorded in the Windows Security log

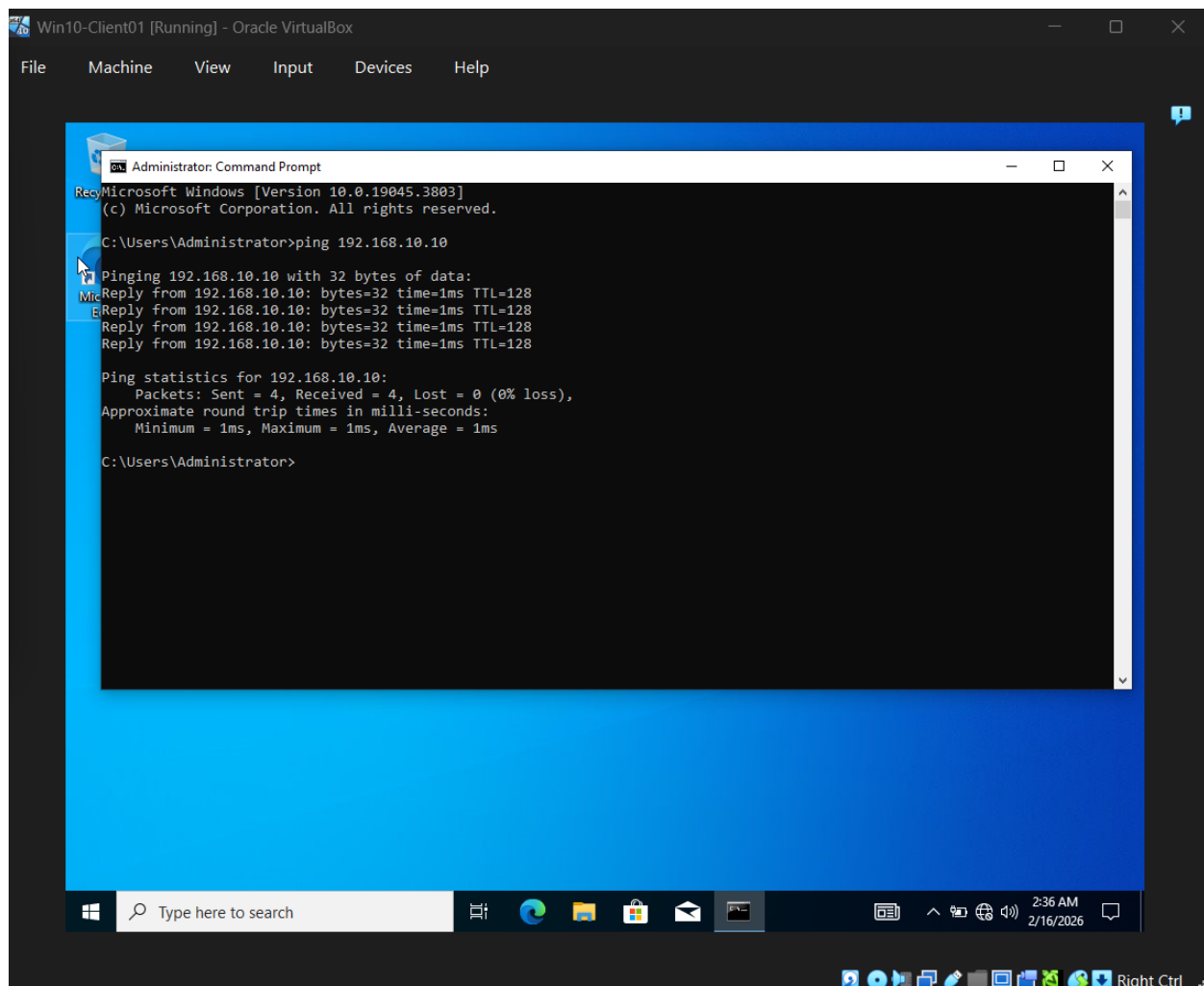
This demonstrates:

- Enforcement of defensive controls
- Log-based detection capability
- Practical blue team validation workflow



9. Network Communication Validation

Performed ICMP connectivity testing between endpoint and domain controller to confirm network-layer communication required for authentication and policy enforcement.



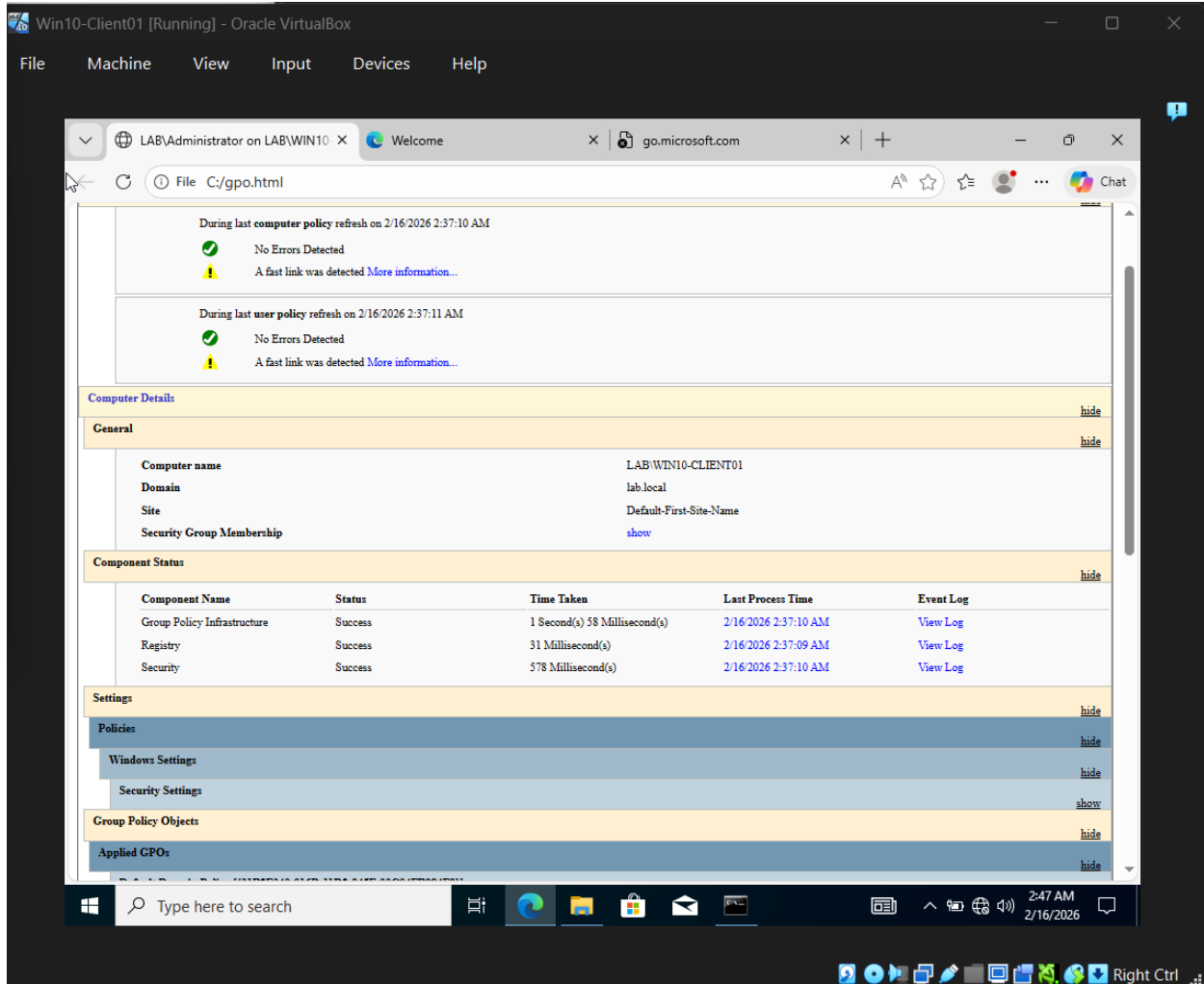
10–12. Policy Validation

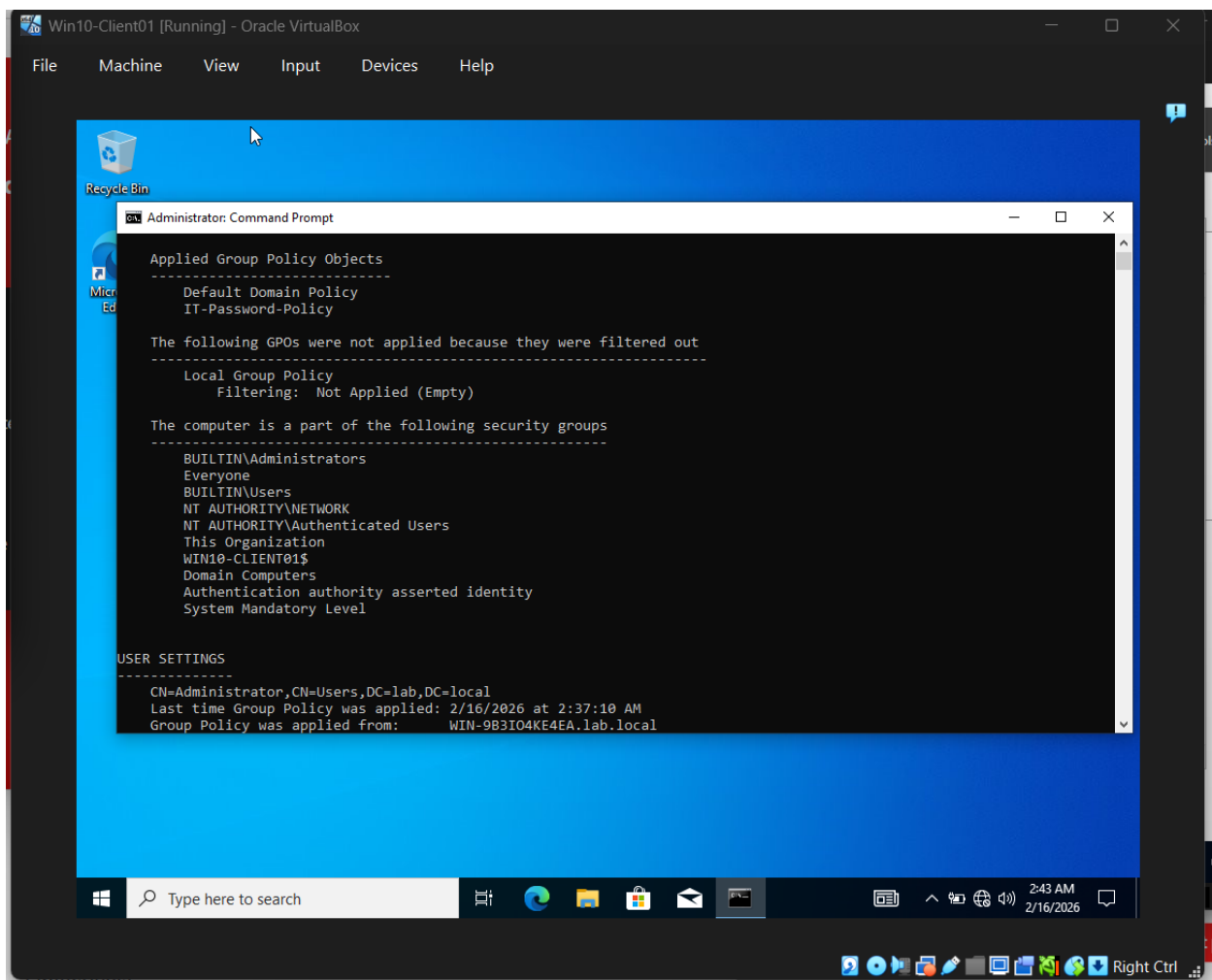
Executed:

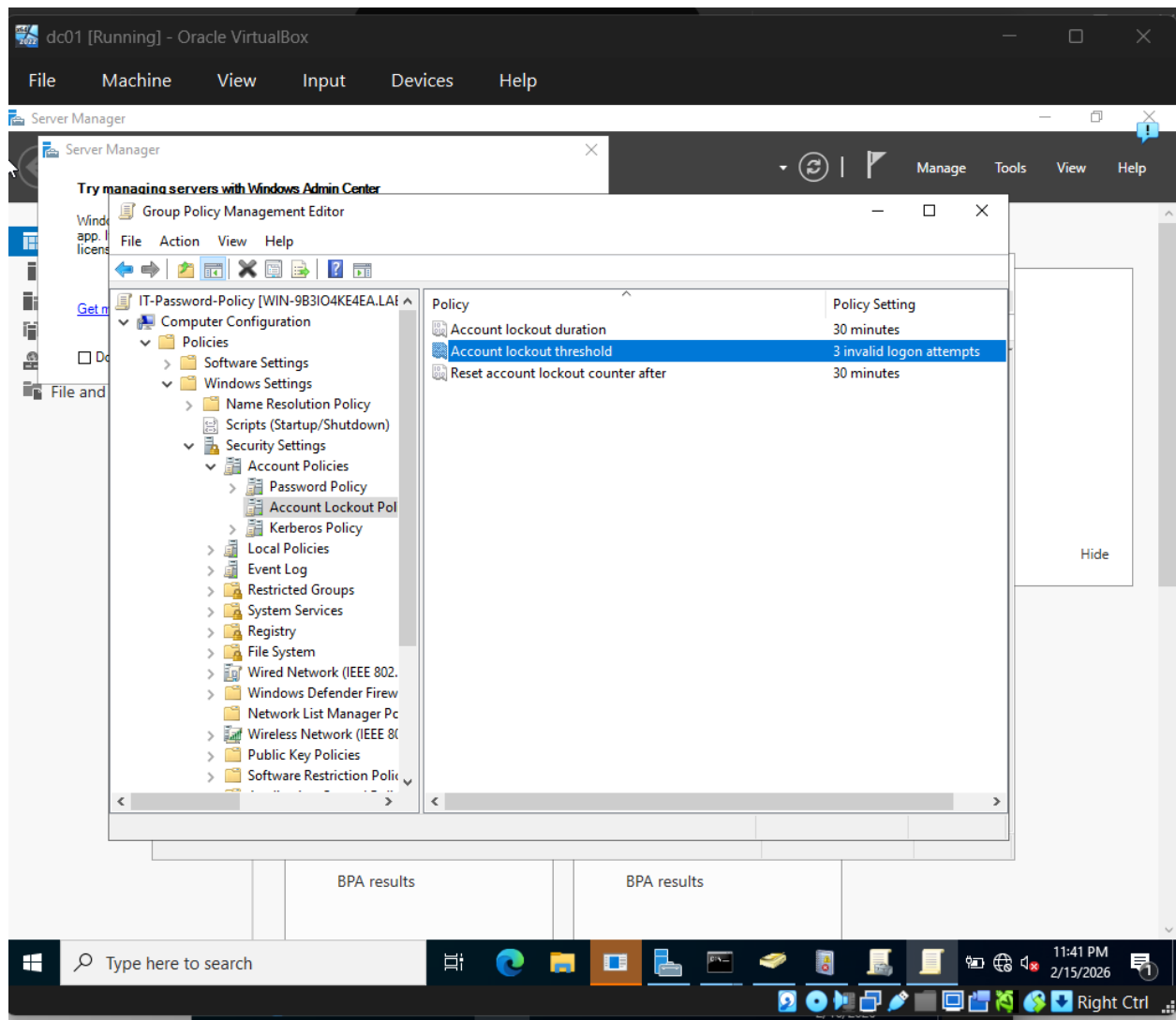
- gpupdate /force
- gpresult /r
- gpresult /h

Confirmed:

- Applied Group Policy Objects
- Proper policy enforcement on endpoint
- Operational security configuration







Challenges & Incident Troubleshooting

1. APIPA Address (169.254.x.x)

Issue:

The Windows 10 client received an APIPA address, preventing domain communication and authentication.

Investigation:

- Reviewed VirtualBox network adapter configuration
- Identified adapter mismatch between VMs
- Verified DNS server configuration

Resolution:

- Corrected internal network adapter configuration
- Revalidated IP assignment and subnet alignment

Lesson Learned:

Active Directory functionality is dependent on proper Layer 3 networking and DNS configuration. Identity infrastructure failures often originate from network misconfiguration.

2. GPO Displaying “Not Defined”

Issue:

Account Lockout Policy appeared as not configured despite being linked to the domain.

Investigation:

- Confirmed correct GPO editing scope
- Verified that policies were explicitly defined, not merely linked

Resolution:

- Defined account lockout threshold and duration settings
- Executed `gpupdate /force`
- Validated via `gpresult`

Lesson Learned:

Linking a policy does not guarantee enforcement. Configuration must be defined and validated.

3. DNS Dependency for Domain Join

Issue:

Initial domain join attempts failed due to DNS misconfiguration.

Resolution:

- Configured client DNS server to point to DC01 (192.168.10.10)
- Restarted services and reattempted domain join

Lesson Learned:

Active Directory is DNS-driven. Authentication failures frequently stem from incorrect DNS resolution.

Blue Team Skills Demonstrated

- Identity & Access Management (IAM)
 - Active Directory Hardening
 - Account Lockout Policy Enforcement
 - Brute-Force Mitigation Controls
 - Windows Security Log Analysis
 - Event ID 4740 Investigation
 - GPO Validation & Verification
 - Endpoint-to-Server Communication Testing
 - Infrastructure Troubleshooting
 - Structured Technical Documentation
-

Key Takeaways

This lab reinforced that effective security monitoring begins with properly configured infrastructure. Defensive controls such as account lockout policies are only effective when validated through controlled testing and log analysis.

The project strengthened my ability to:

1. Deploy and secure identity infrastructure.
2. Implement authentication hardening controls.
3. Simulate attack behavior in a controlled lab environment.
4. Validate detection through Windows Security logs.
5. Document technical implementation and troubleshooting processes clearly.