Recruiter Summary — IT Help Desk / Service Desk Portfolio

Candidate: Kingsley Otoo
Target Roles: IT Help Desk / IT Support / Service Desk Analyst
Environment: Windows 11, Windows Server 2022, Active Directory

Profile Overview

This portfolio demonstrates hands-on, job-ready IT Support capability through realistic Help Desk scenarios. All work was performed in a controlled Windows 11 and Active Directory lab designed to mirror real-world Service Desk operations. Each scenario follows a ticket-based workflow: issue reported, investigation, resolution, and validation.

Key Signals for Hiring Managers:
- Hands-on Windows 11 and Active Directory support experience
- Real-world incident troubleshooting using logs and policy tools
- Evidence-backed problem resolution with validation steps
- Documentation written to professional Service Desk standards

Core Capabilities Demonstrated

- Windows 11 troubleshooting and user support
- Active Directory user, group, and policy management
- Group Policy enforcement and validation (gpupdate, gpresult, RSOP)
- Account lockout, permissions, and UAC troubleshooting
- Scheduled task diagnostics and log analysis
- Network drive mapping and access control
- Professional documentation and evidence collection

Why This Candidate Is Job-Ready

- Thinks in tickets and incidents, not just technical tasks
- Demonstrates structured troubleshooting and root-cause analysis
- Produces documentation to professional IT standards
- Comfortable working in both standalone and domain environments
- Evidence-backed work suitable for interview deep dives

How to Review This Portfolio

1. Review the Help Desk Scenarios section to assess real-world support thinking.
2. Refer to the Evidence Appendix for screenshots and validation proof.
3. Use scenarios directly as interview discussion points.

Windows 11 Help Desk Scenarios – IT Support Portfolio

This portfolio presents practical Help Desk and IT Support scenarios based on a Windows 11 home lab environment. Each scenario is written in a ticket-style format to reflect real-world Service Desk workflows, including issue intake, investigation, resolution, and validation. Evidence is referenced throughout and supported by a full appendix of screenshots.

Environment Overview

- Client OS: Windows 11 Pro
- Server OS: Windows Server 2022 (Active Directory)
- Virtualisation Platform: VMware Workstation
- Domain: LAB.local
- Focus: First-line and second-line IT Support scenarios

Support Scenario 1 — User Unable to Log In (Account Lockout)

Reported Issue:
User unable to log in after multiple failed attempts.

Investigation:
Reviewed local security policy and Event Viewer logs.

Resolution:
Unlocked account and confirmed password policy settings.

Validation:
Successful login confirmed.

Evidence:
Figures 8–9

Support Scenario 2 — Administrative Task Blocked by UAC

Reported Issue:
User could not perform administrative task.

Investigation:
Confirmed standard user context and UAC behaviour.

Resolution:
Performed task with elevated credentials.

Validation:
Task completed successfully.

Evidence:
Figures 10–11

Support Scenario 3 — Scheduled Task Did Not Execute

Reported Issue:
Scheduled task failed to generate output.

Investigation:
Reviewed Task Scheduler logs and execution context.

Resolution:
Corrected execution settings.

Validation:
Task ran successfully.

Evidence:
Figures 12–20

Support Scenario 4 — Group Policy Not Applying

Reported Issue:
Expected policy not applied to user.

Investigation:
Used gpupdate, gpresult, and RSOP.

Resolution:
Corrected policy scope.

Validation:
Policy applied as expected.

Evidence:
Figures 21–37

Support Scenario 5 — Network Drive Missing

Reported Issue:
Mapped drive not visible.

Investigation:
Checked Group Policy Preferences and permissions.

Resolution:
Corrected access permissions.

Validation:
Drive visible and accessible.

Evidence:
Figures 38–40

Conclusion

This portfolio demonstrates the ability to handle realistic Help Desk incidents, apply structured troubleshooting, and validate outcomes using appropriate tools.

Evidence Appendix (Screenshots)

The following figures provide supporting evidence for the Help Desk scenarios documented in this portfolio. Figures are grouped by scenario to simplify review. Each figure includes the source filename.

Environment & Infrastructure Evidence

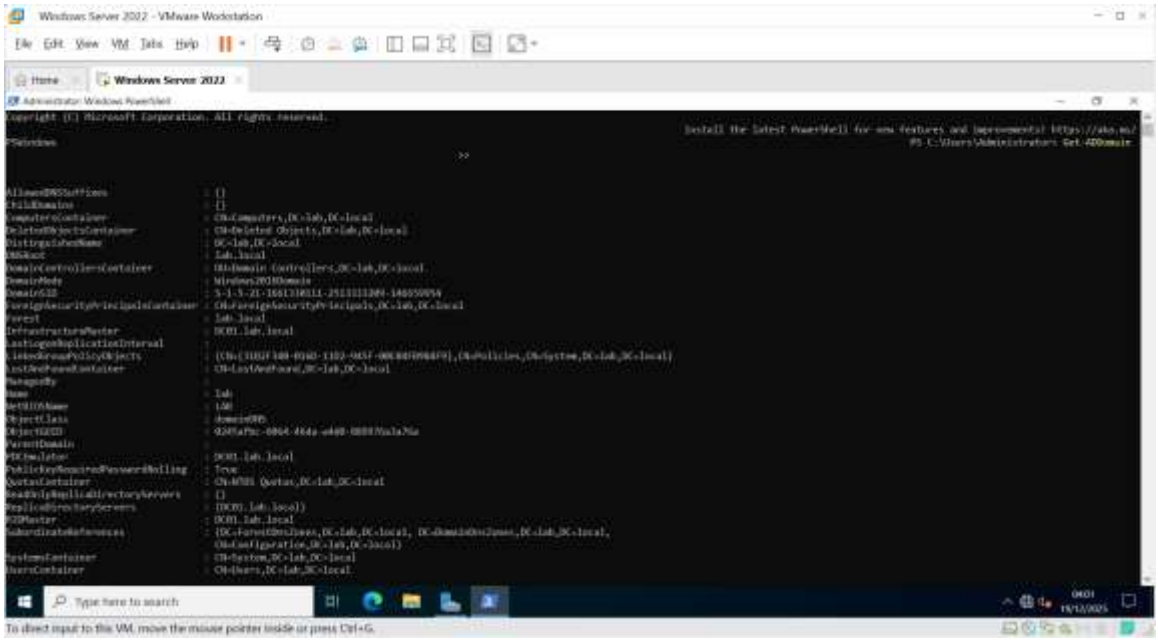

Figure 1: Screenshot evidence.
Source file: DomainControllerConfirmed.png

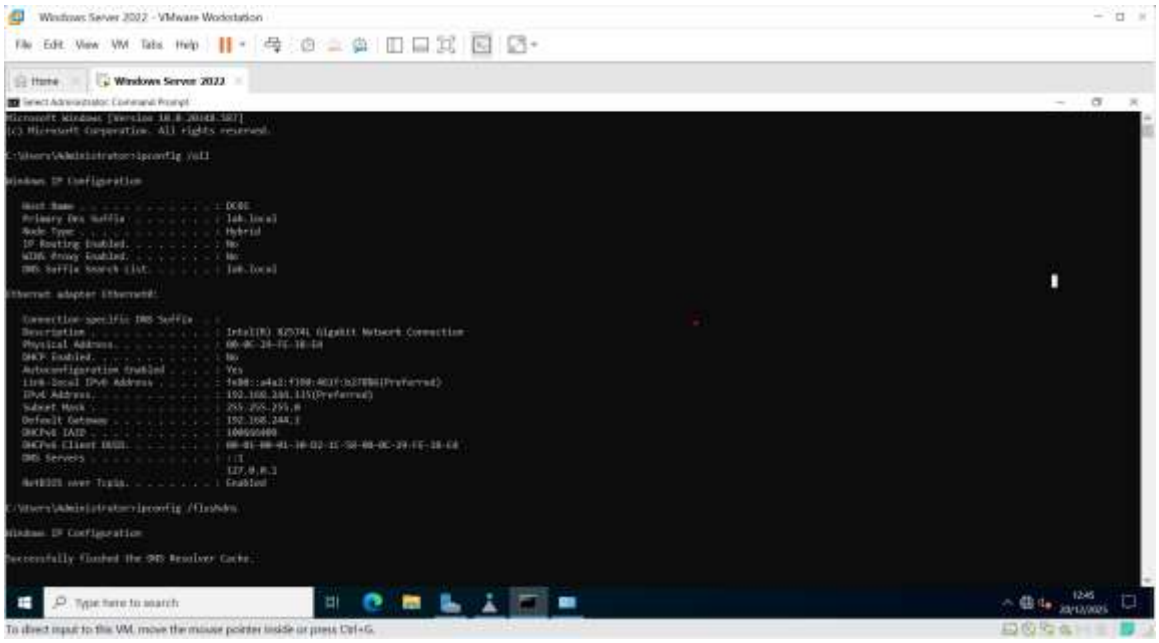

Figure 2: Screenshot evidence.
Source file: FixWindows11DNS.png

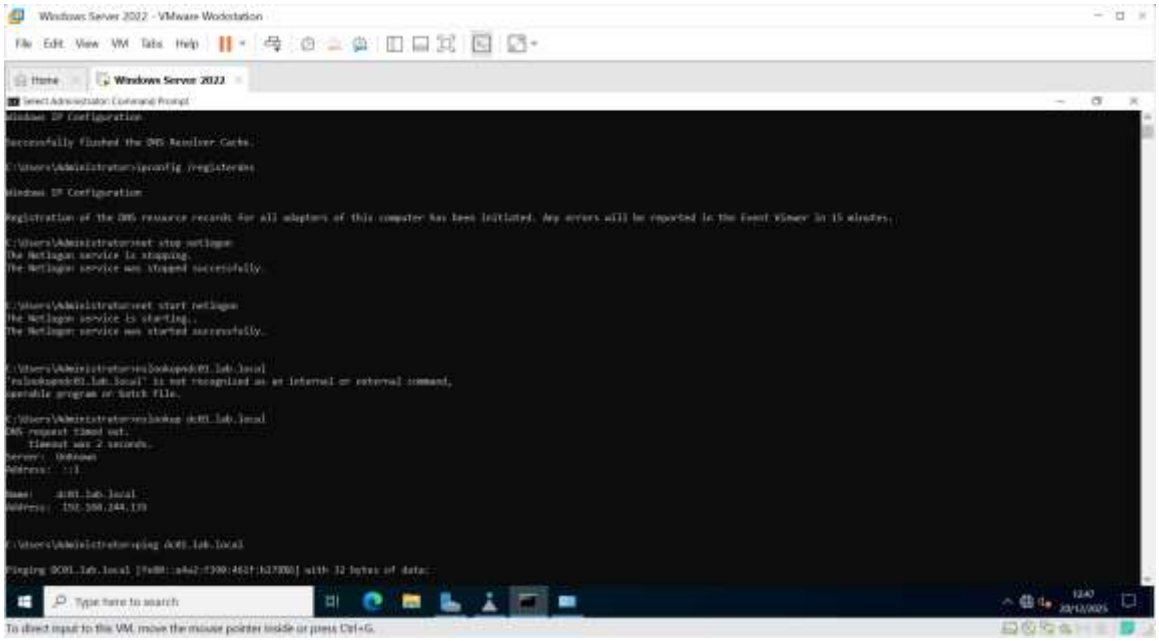

Figure 3: Screenshot evidence.
Source file: FixWindows11DNS1.png

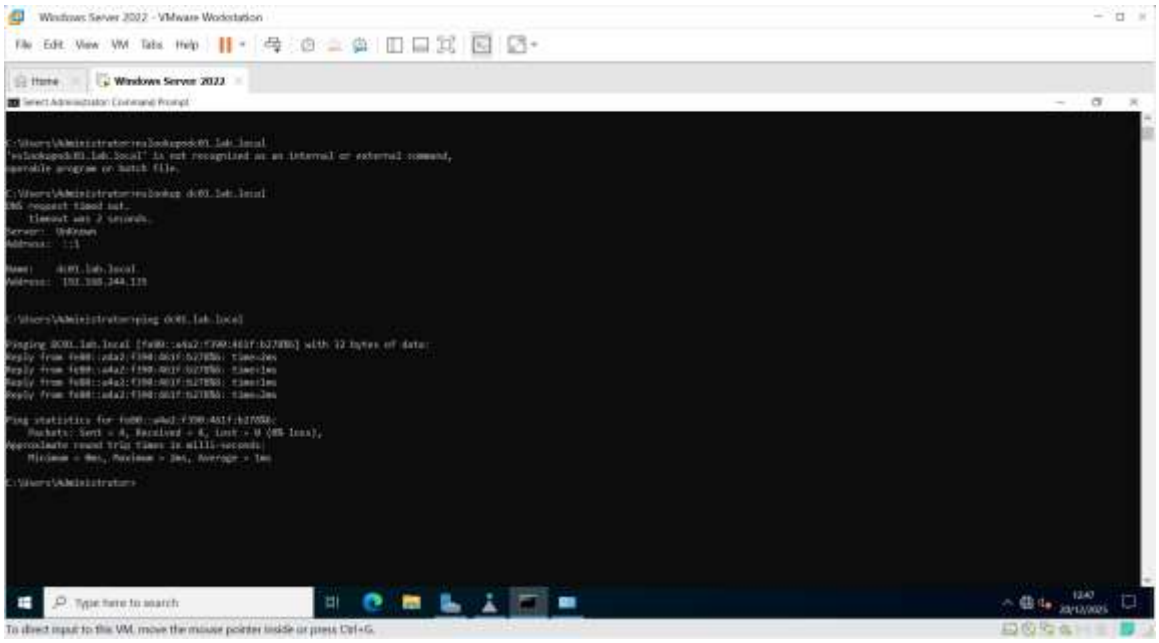

Figure 4: Screenshot evidence.
Source file: FixWindows11DNS2.png

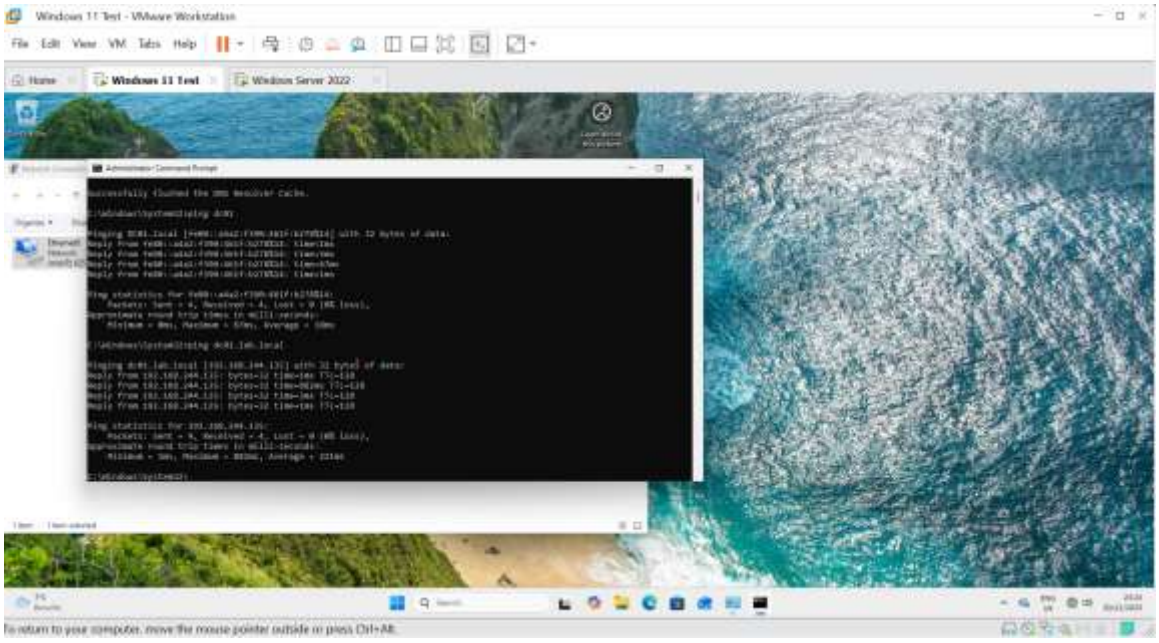

Figure 5: Screenshot evidence.
Source file: PingDC01.png

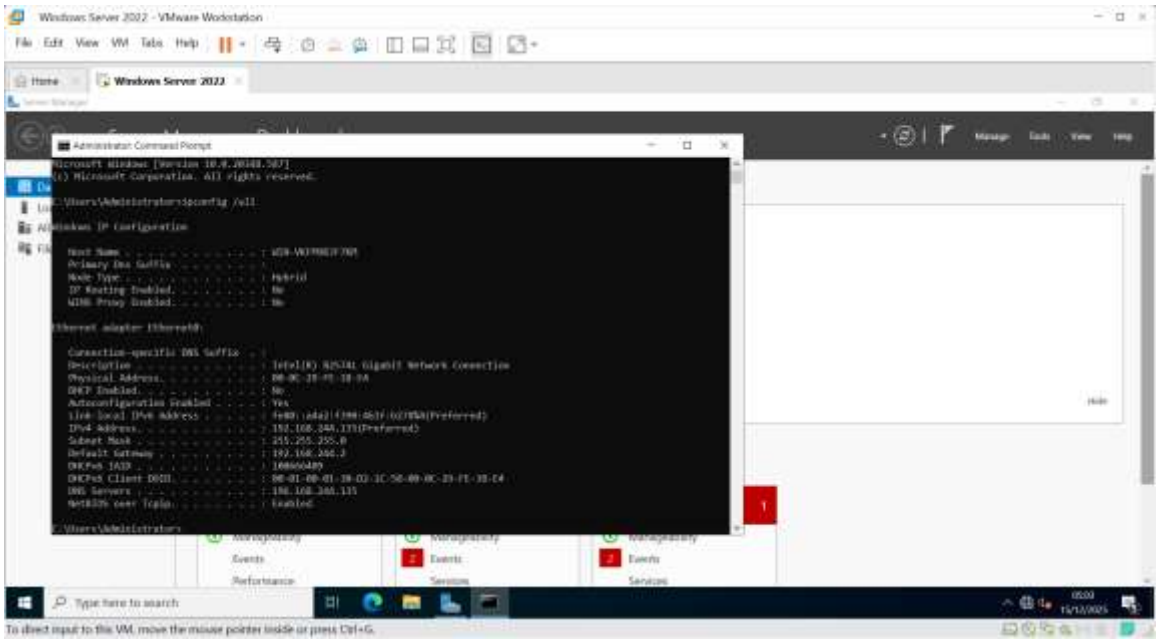

Figure 6: Screenshot evidence.
Source file: StaticIPConfig.png

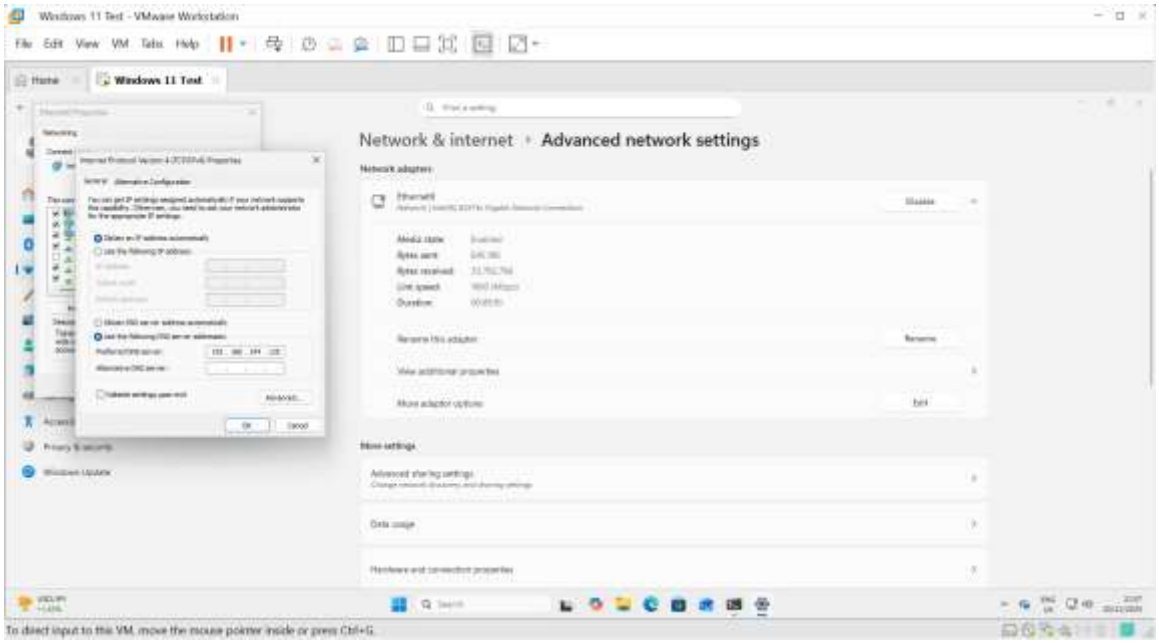

Figure 7: Screenshot evidence.
Source file: Win11DNSConfigured.png

Scenario 1 — Account Lockout / Logon

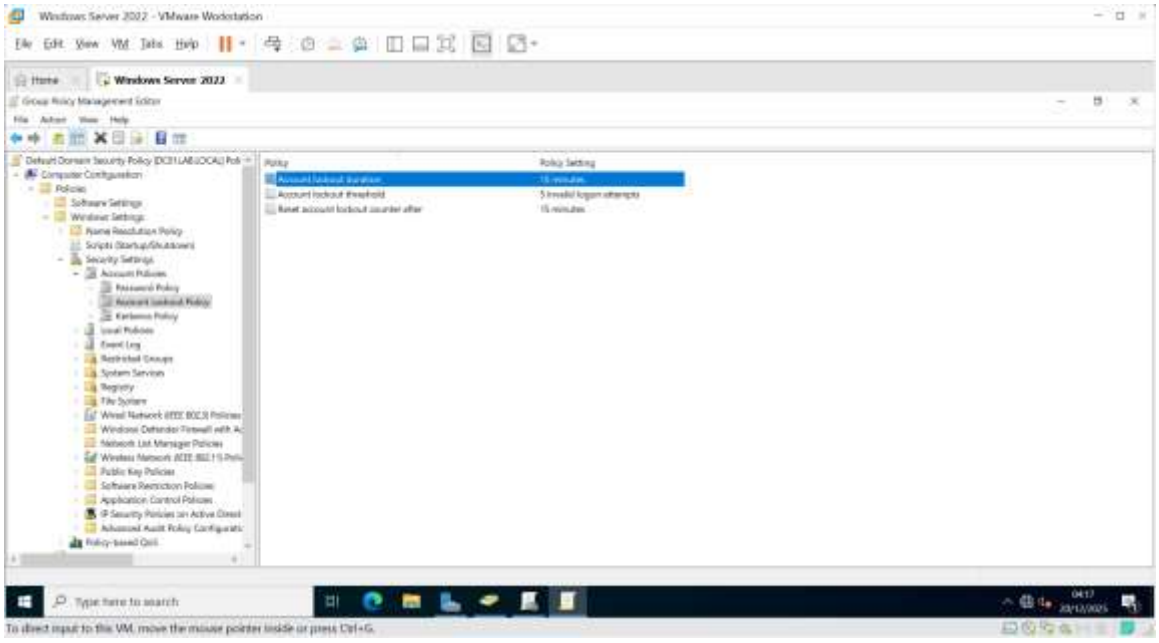

Figure 8: Account lockout policy configuration.

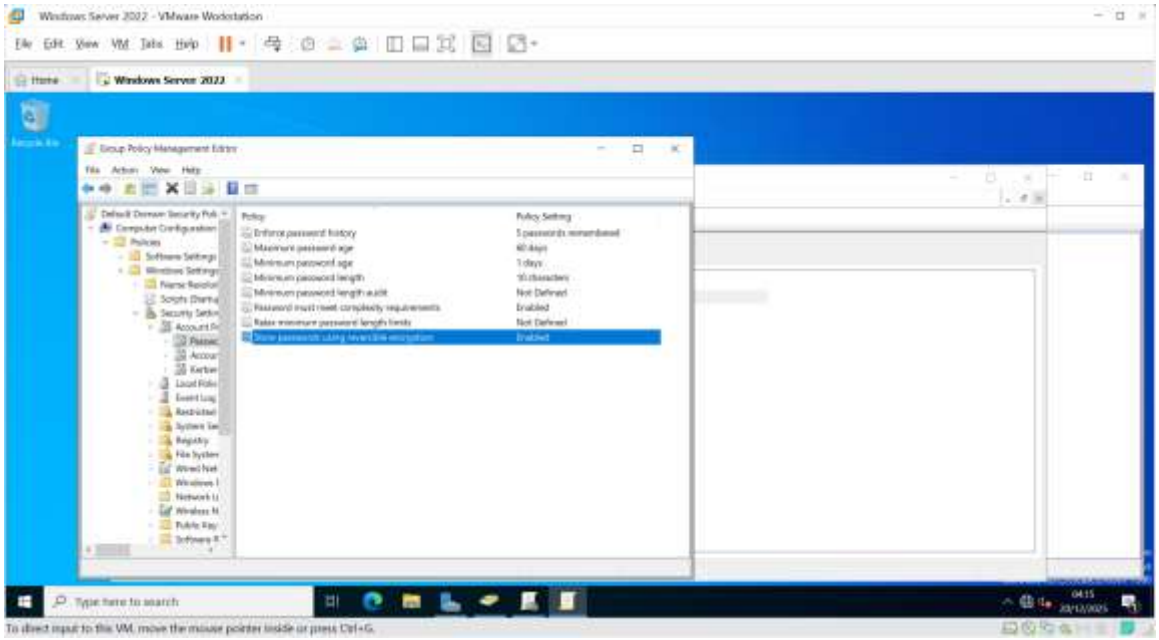

Figure 9: Screenshot evidence.
Source file: PasswordPolicyConfigured.png

Scenario 2 — UAC / Elevation

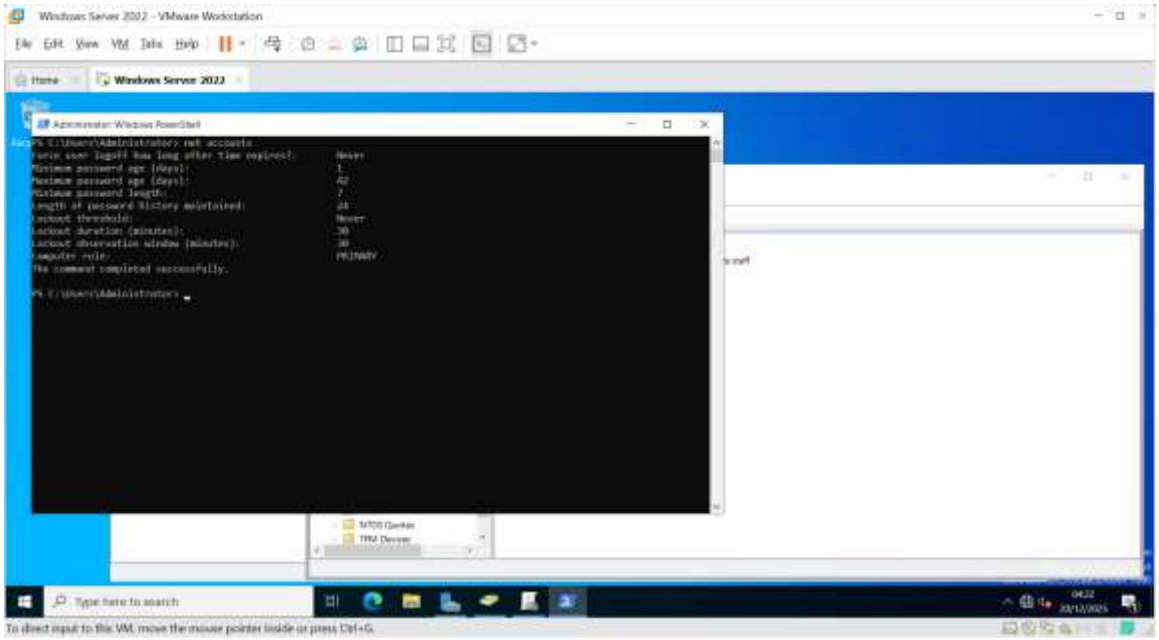

Figure 10: UAC-related policy verification.

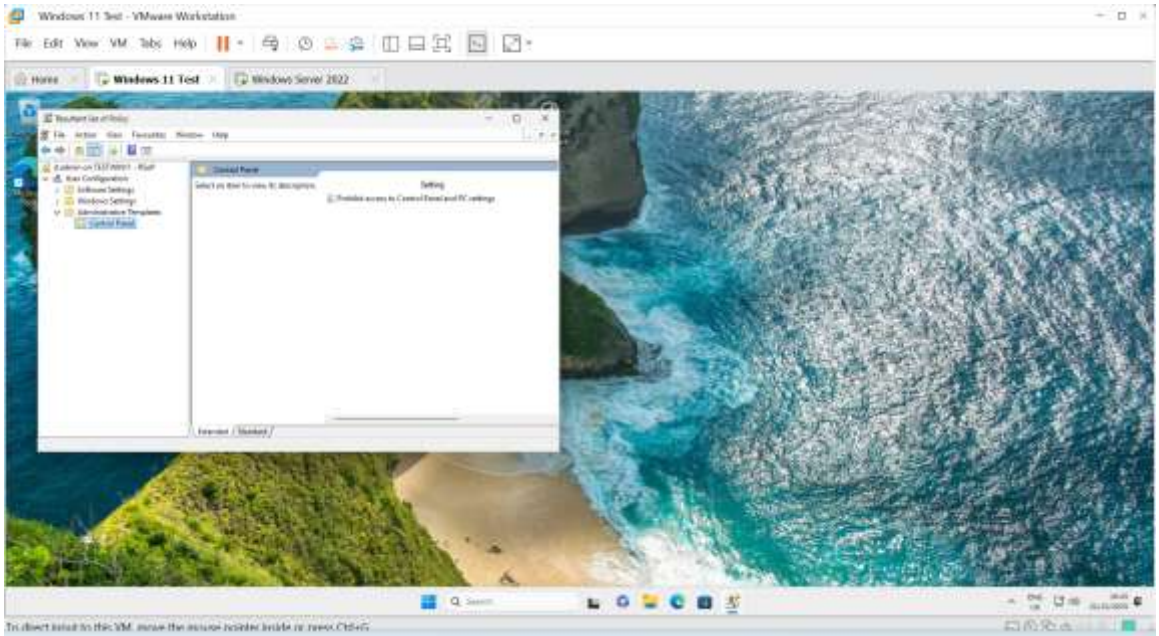

Figure 11: Screenshot evidence.
Source file: Week3_Task3_RSOP_ControlPanel.png

Scenario 3 — Scheduled Tasks / Logging

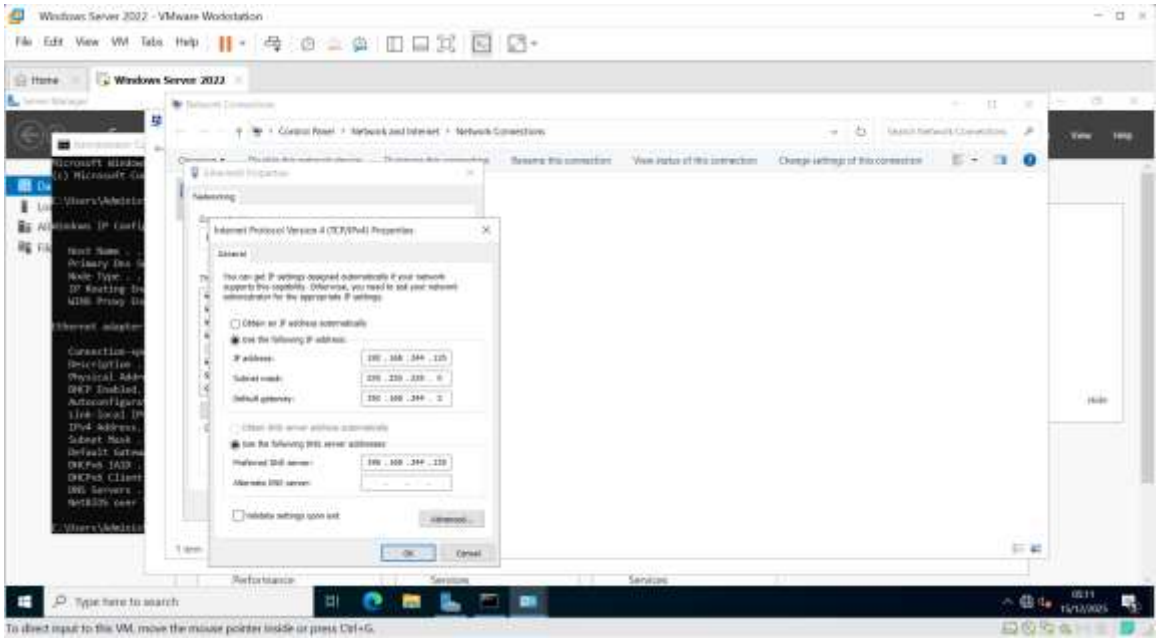

Figure 12: Task Scheduler configuration and execution context.

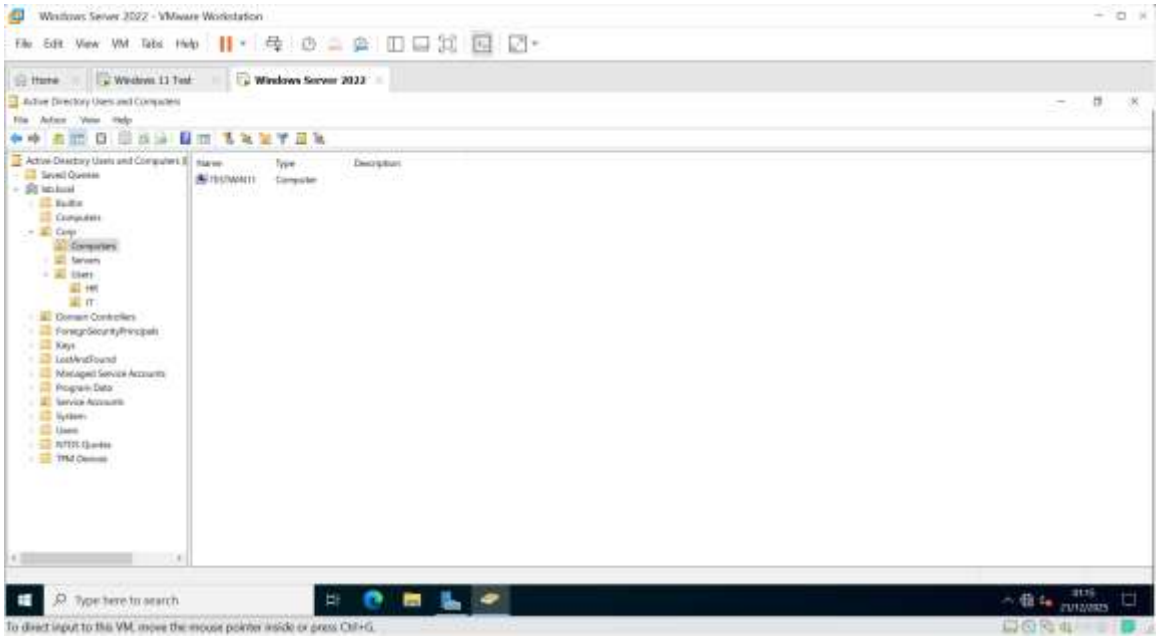

Figure 13: Screenshot evidence.
Source file: Week3_Task2_Computer_In_Correct_OU.png

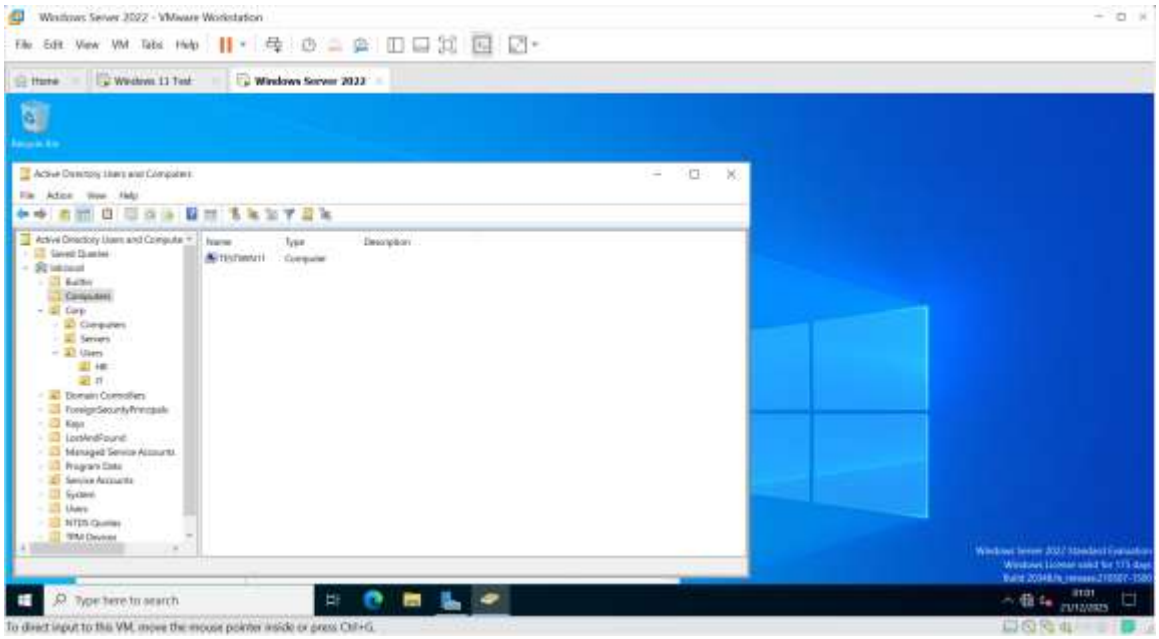

Figure 14: Screenshot evidence.
Source file: Week3_Task2_Computer_In_Default_Container.png

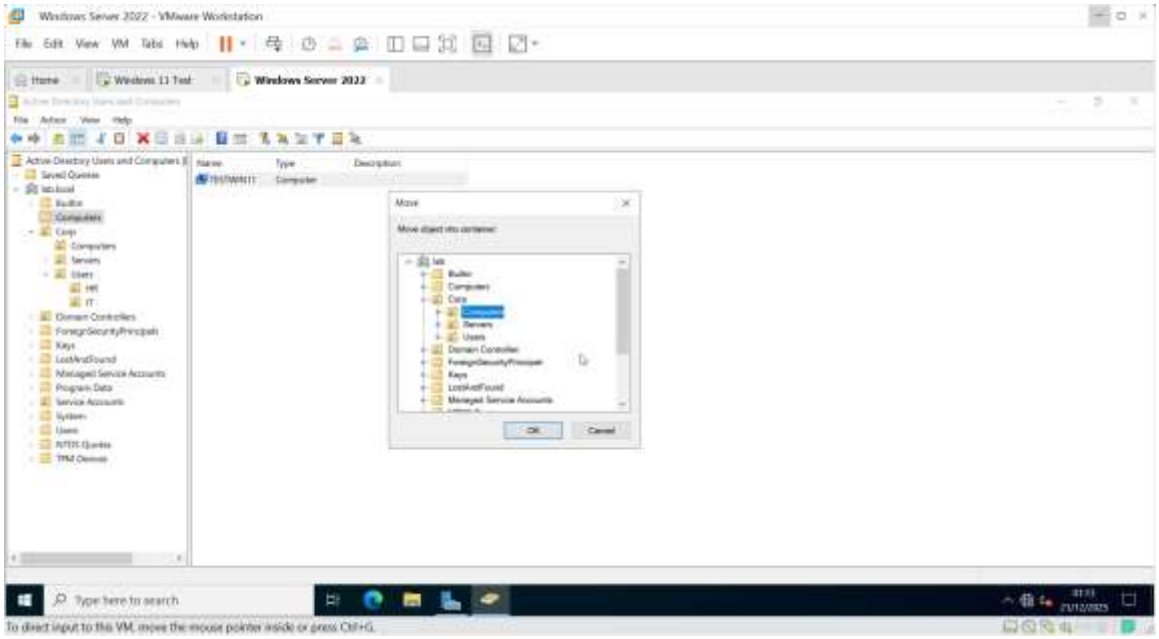

Figure 15: Screenshot evidence.
Source file: Week3_Task2_Computer_Moved_To_Corp_Computers.png

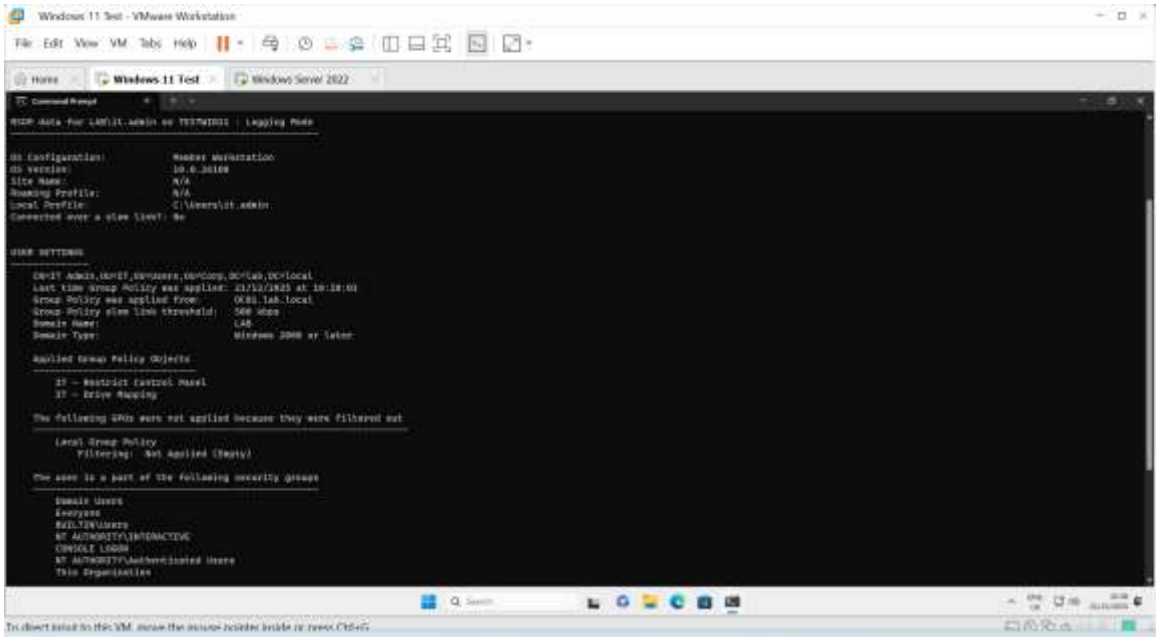

Figure 16: Screenshot evidence.
Source file: Week3_Task3_gpresult_r.png

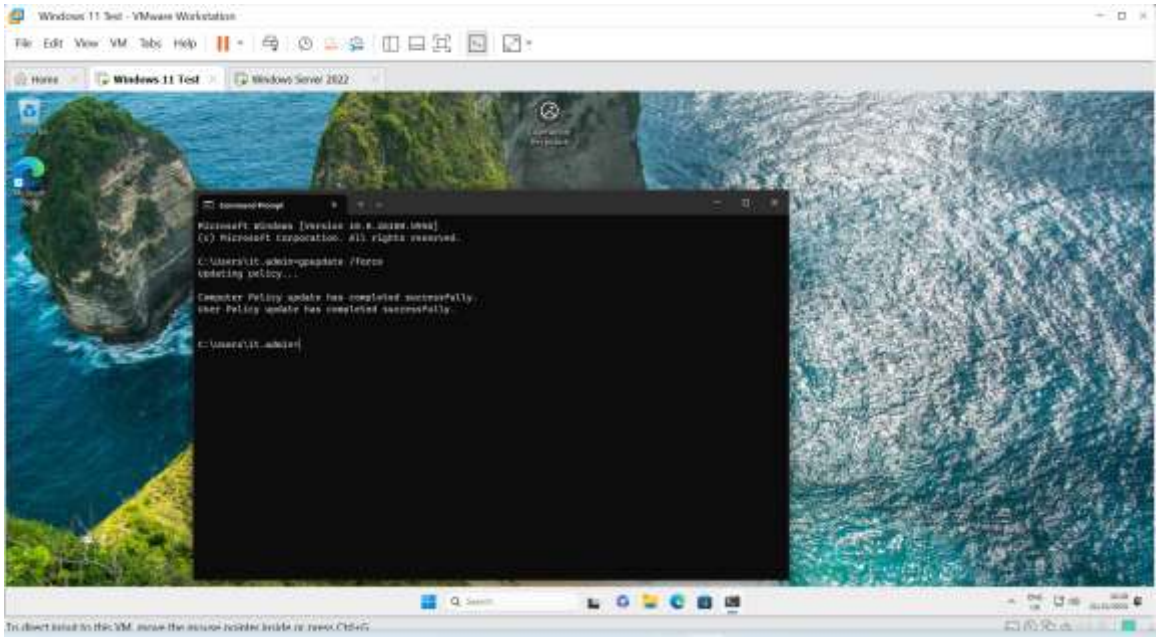

Figure 17: Screenshot evidence.
Source file: Week3_Task3_gpupdate_force.png

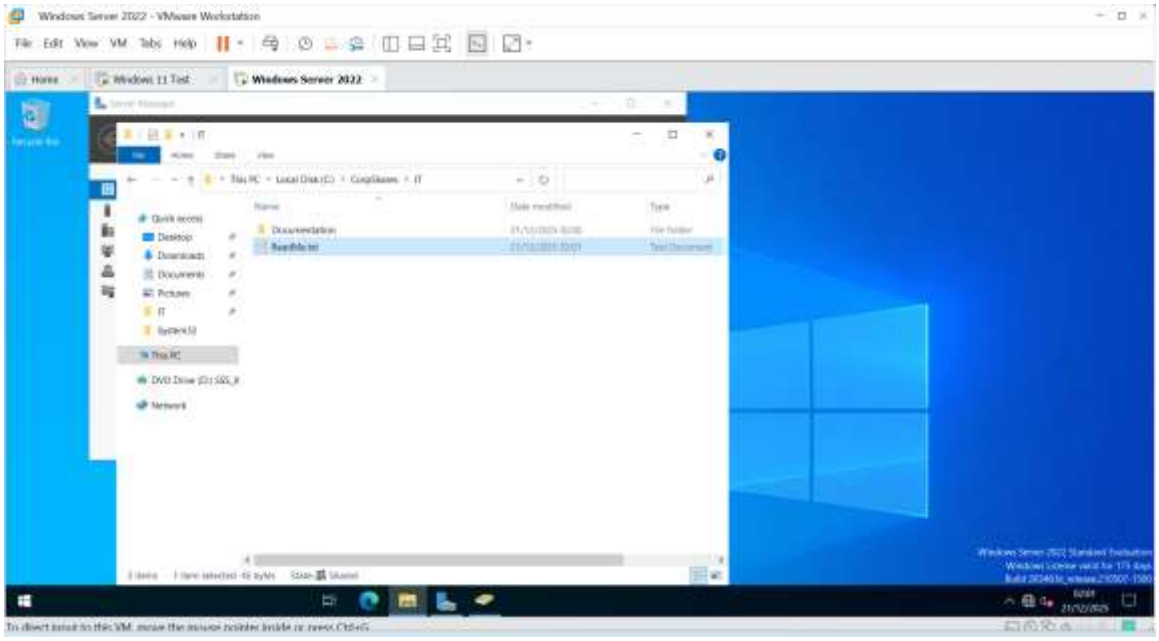

Figure 18: Screenshot evidence.
Source file: Week3_Task3_IT_Share_Content_Created.png

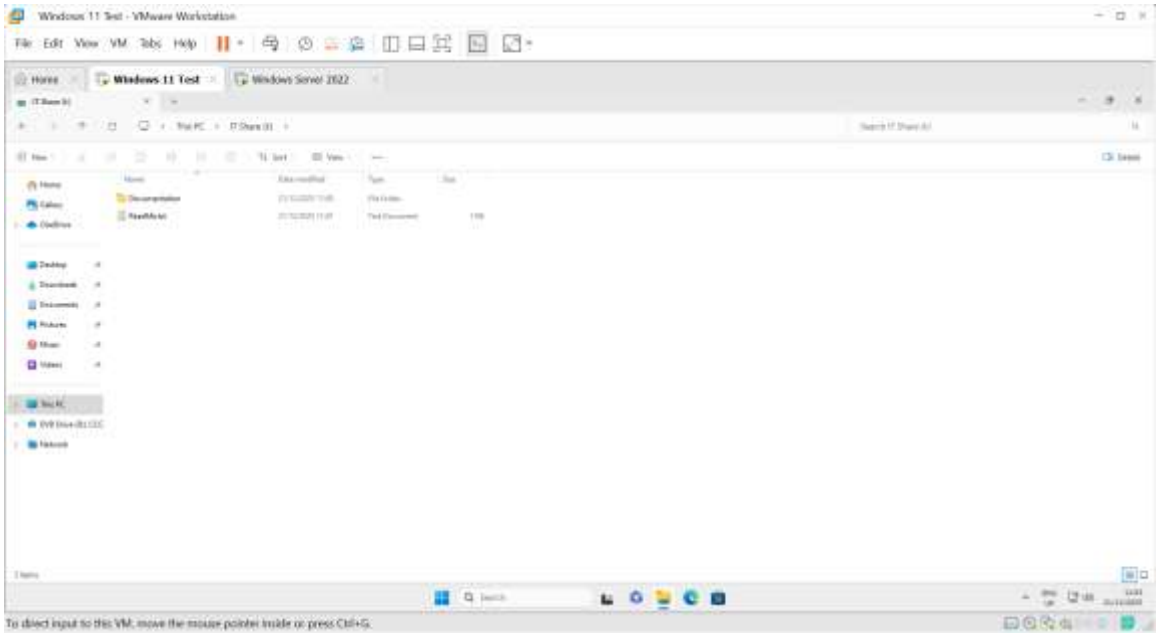

Figure 19: Screenshot evidence.
Source file: Week3_Task3_IT_Share_Content_Visible.png

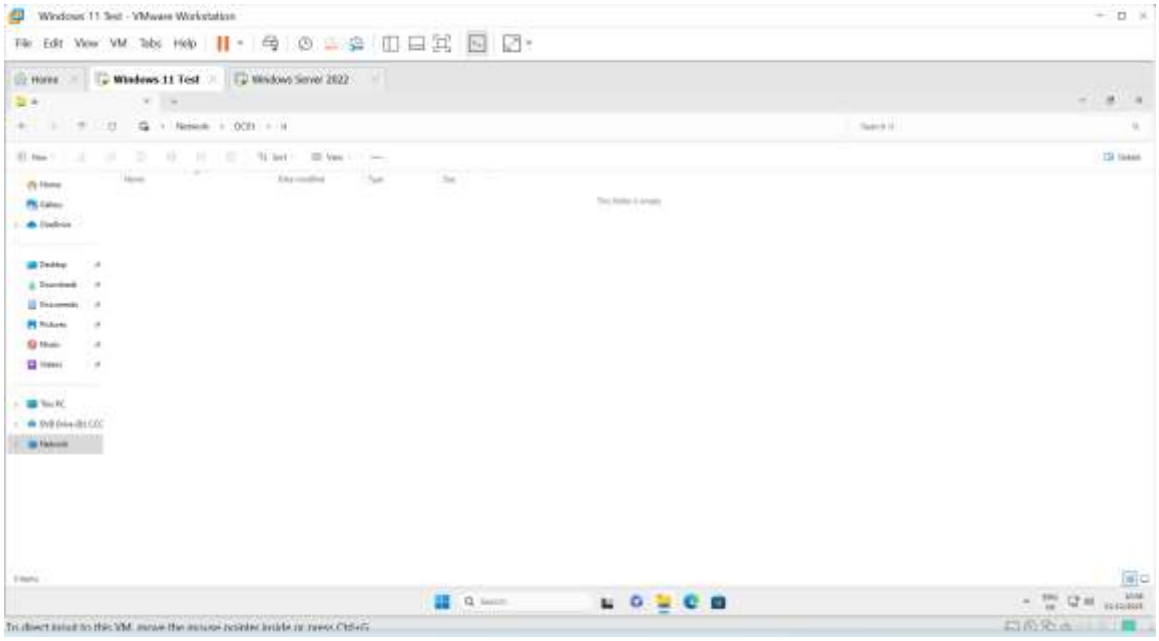

Figure 20: Screenshot evidence.
Source file: Week3_Task3_IT_Share_Empty_Confirmed.png

Scenario 4 — Group Policy / Active Directory

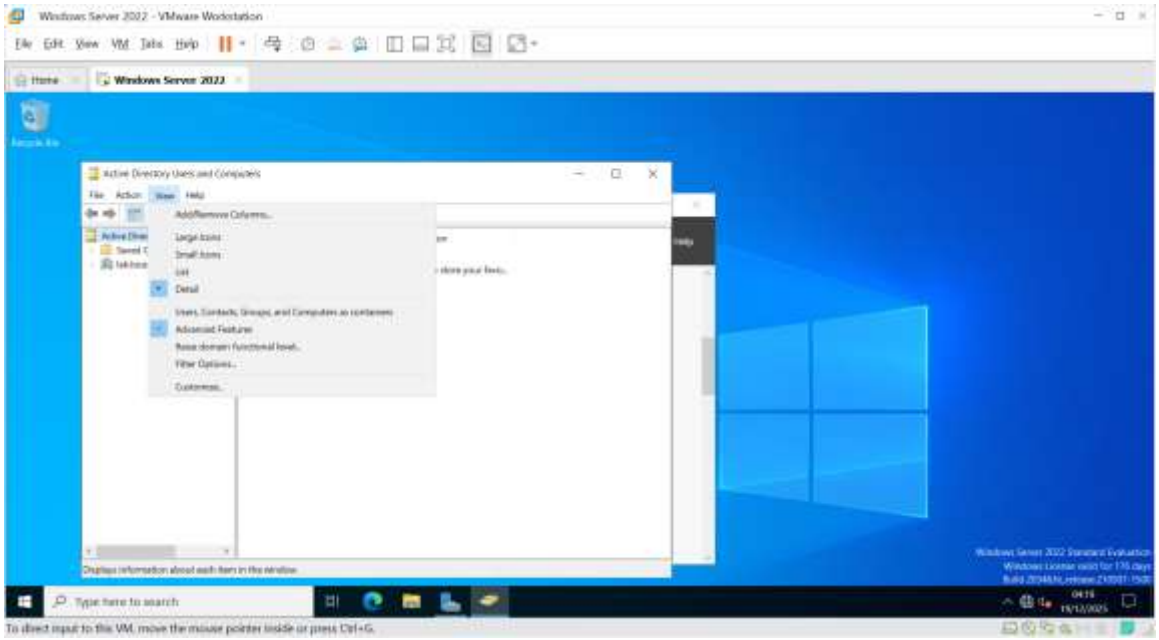

Figure 21: Active Directory Users and Computers with Advanced Features enabled.

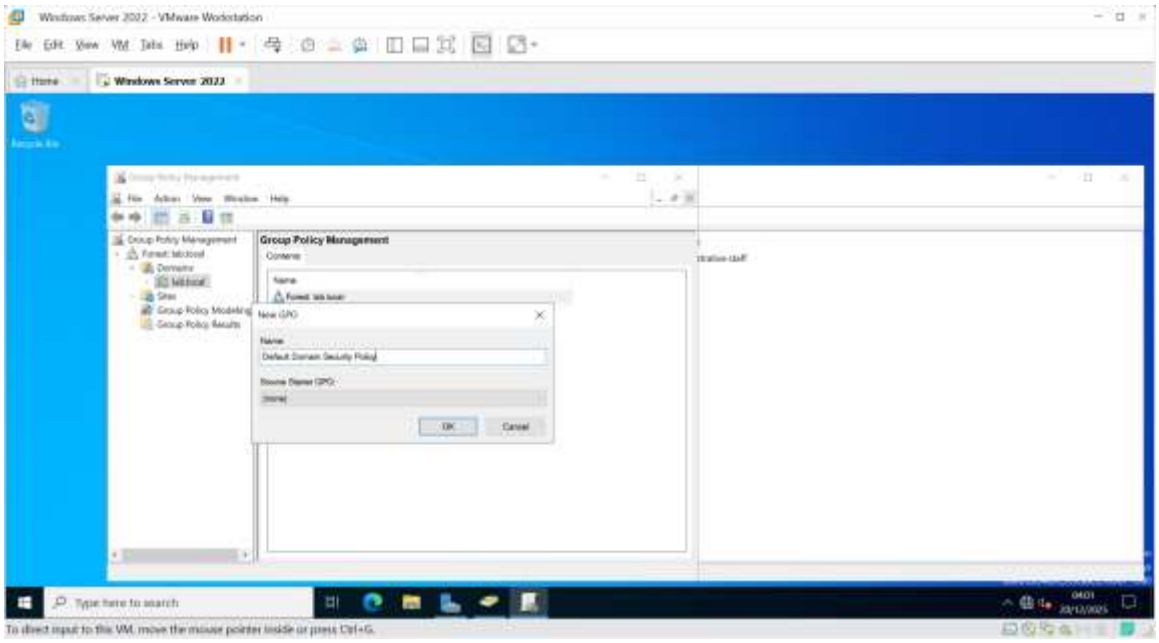

Figure 22: Screenshot evidence.
Source file: GPOCreated1.png

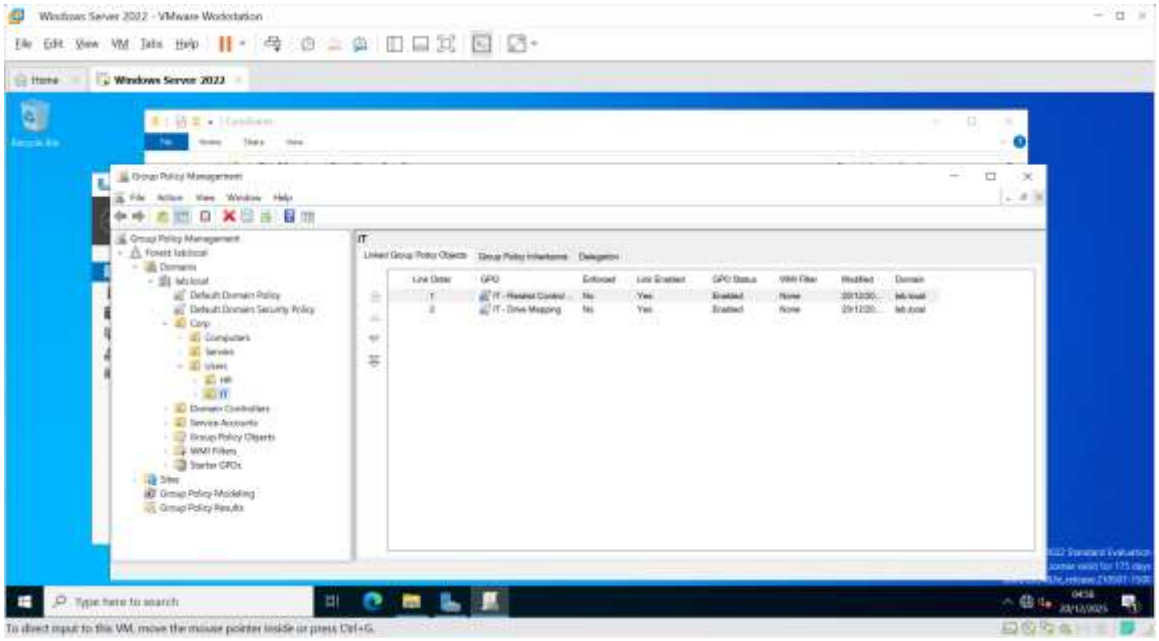

Figure 23: Screenshot evidence.
Source file: GPOCreatedDriveMapping.png

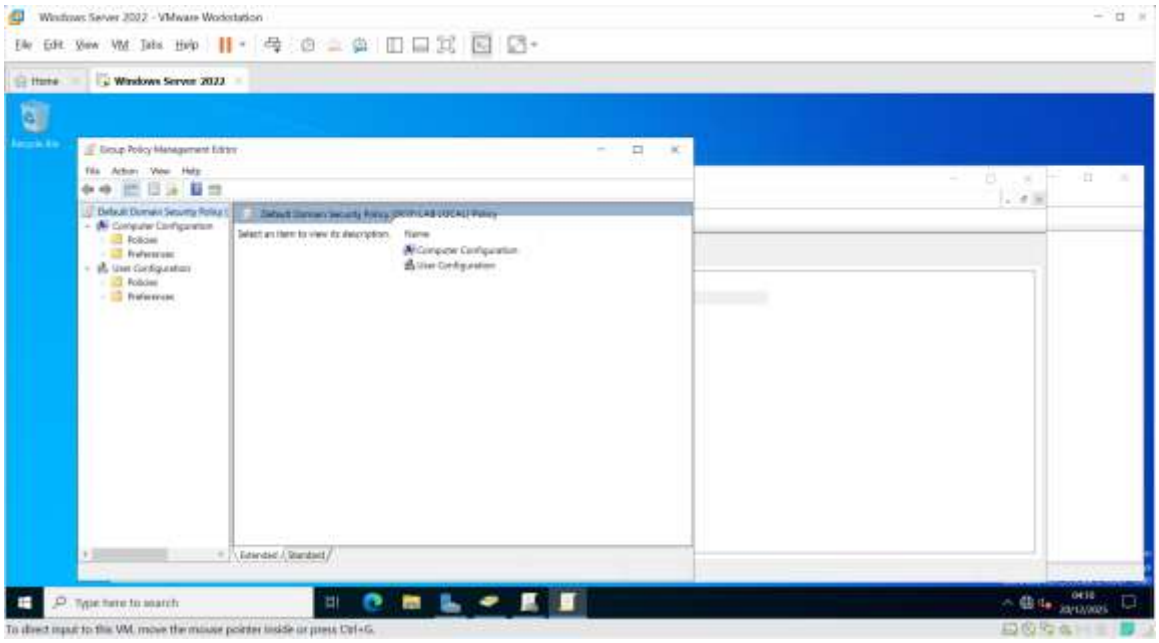

Figure 24: Screenshot evidence.
Source file: GPOEditorOpened.png

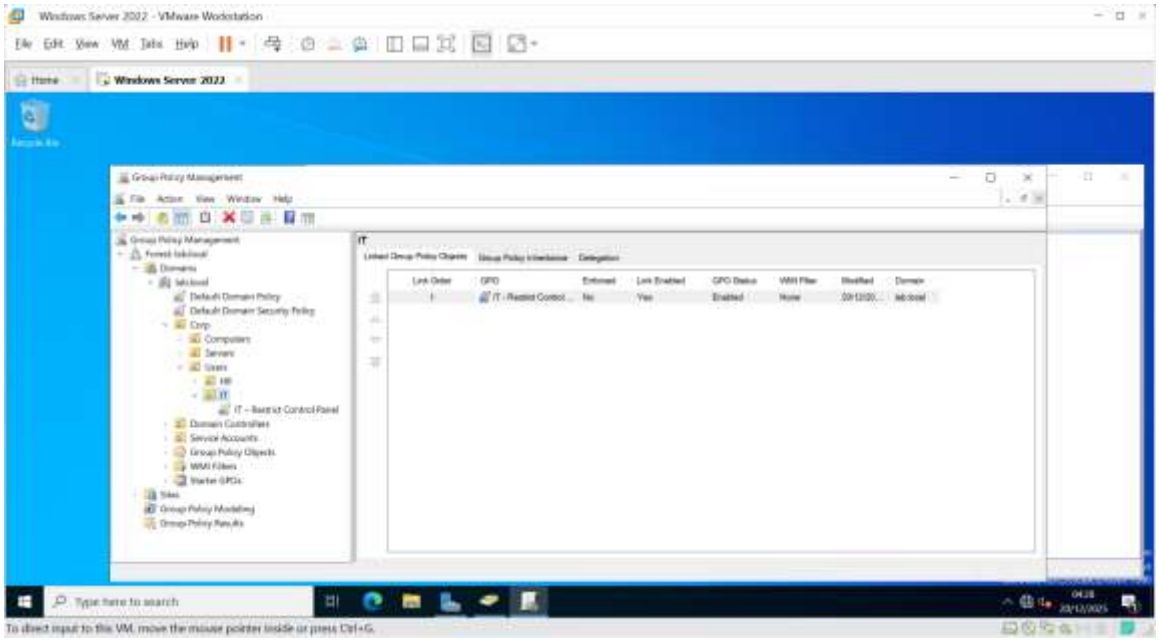

Figure 25: Screenshot evidence.
Source file: GPOLinkedITOU.png

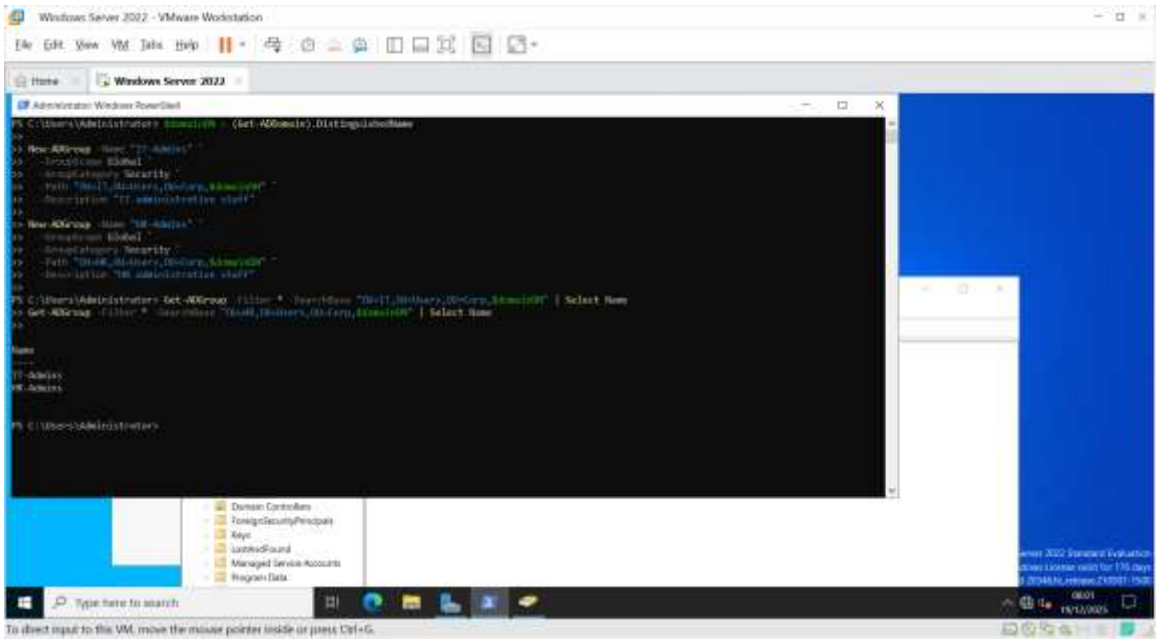

Figure 26: Screenshot evidence.
Source file: GroupsCreated.png

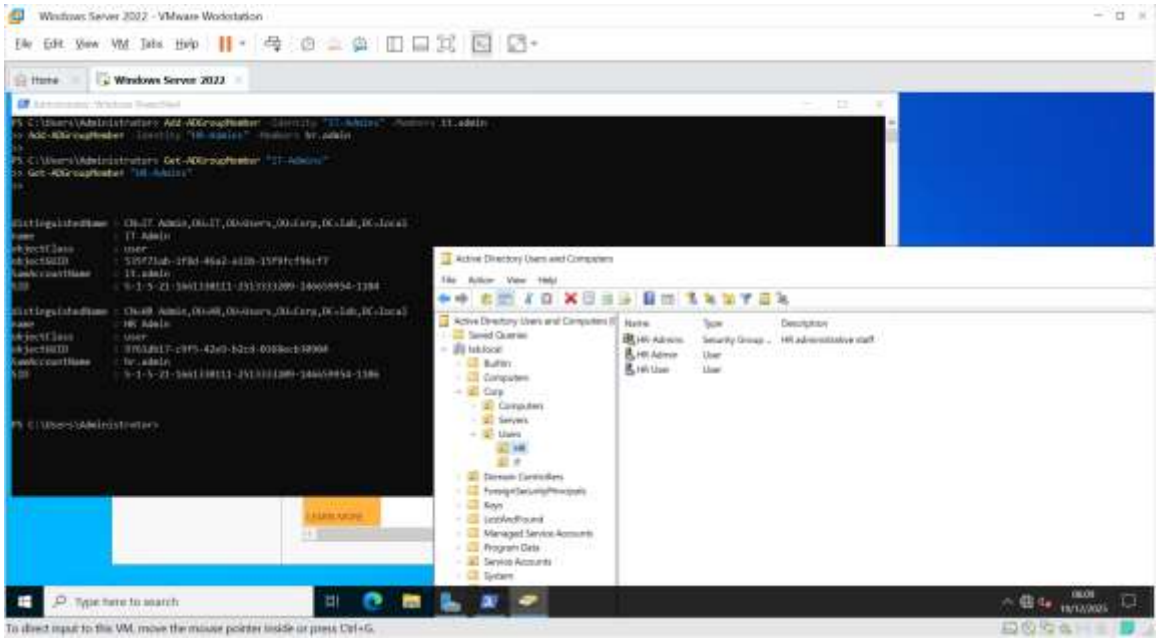

Figure 27: Screenshot evidence.
Source file: HRAdminsGroup.png

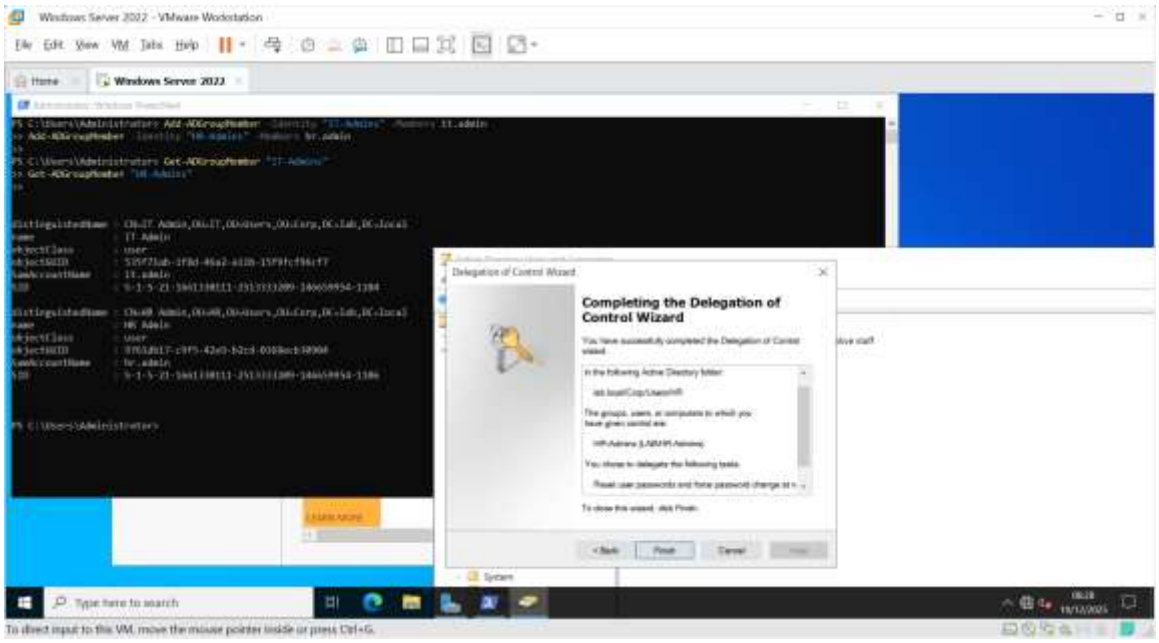

Figure 28: Screenshot evidence.
Source file: HRDelegation.png

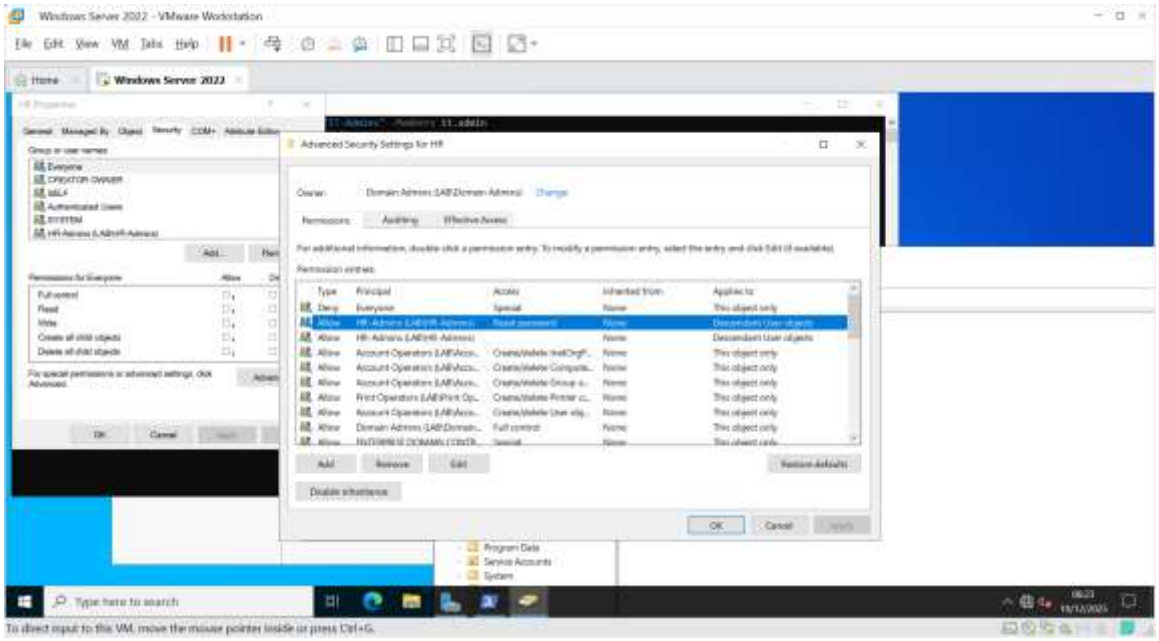

Figure 29: Screenshot evidence.
Source file: HRDelegationACL.png

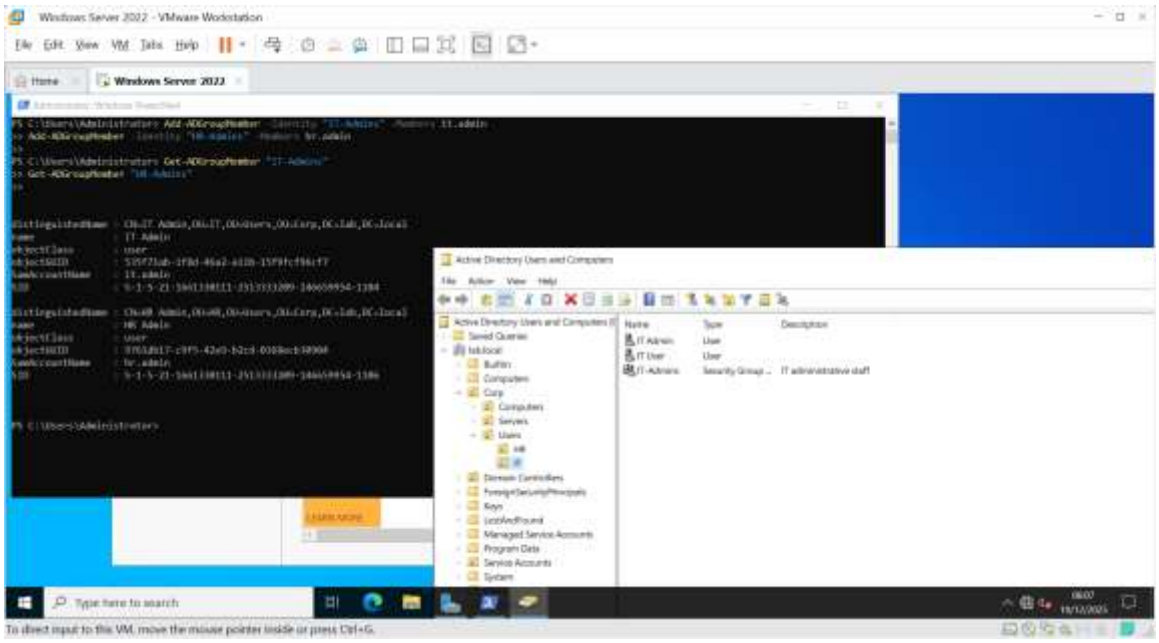

Figure 30: Screenshot evidence.
Source file: ITAdminsGroup.png

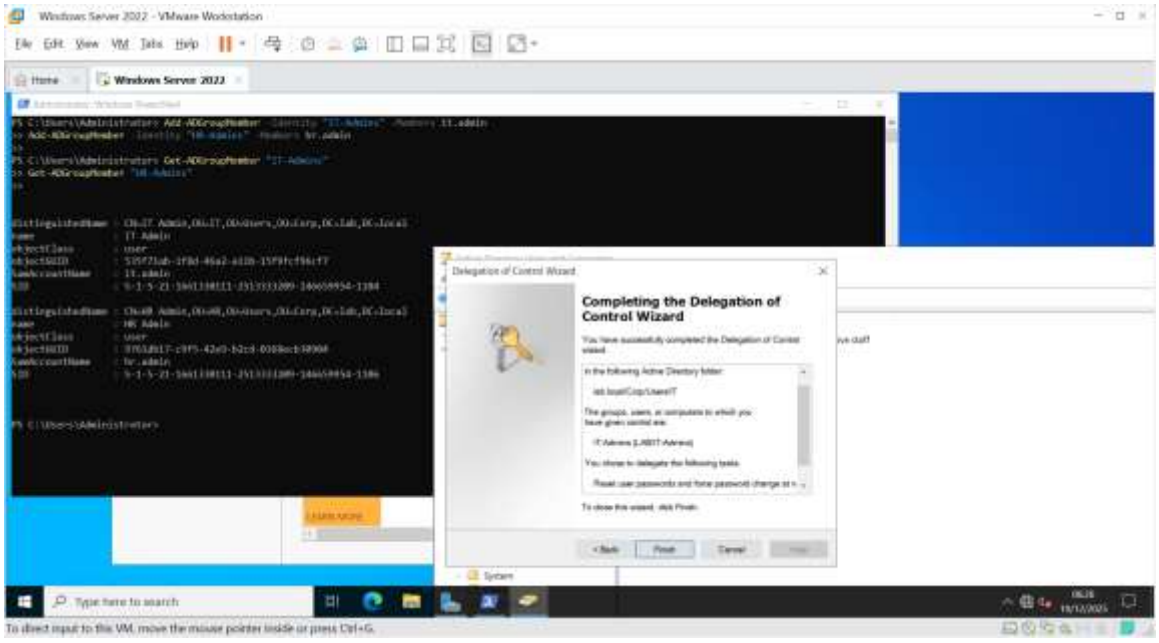

Figure 31: Screenshot evidence.
Source file: ITDelegation.png

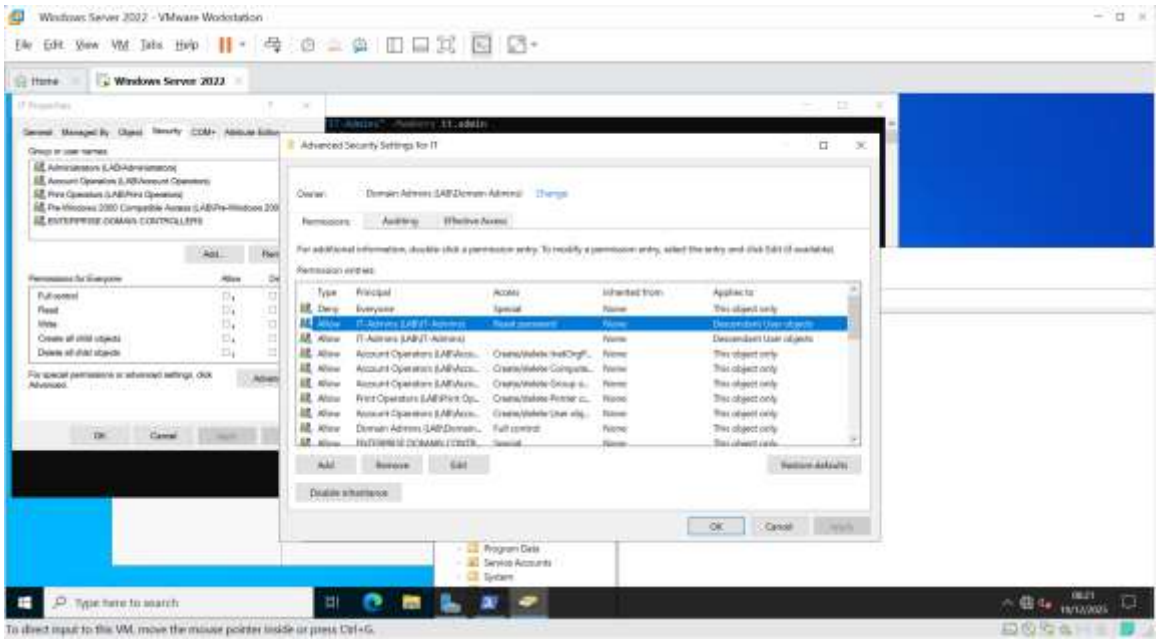

Figure 32: Screenshot evidence.
Source file: ITDelegationACL.png

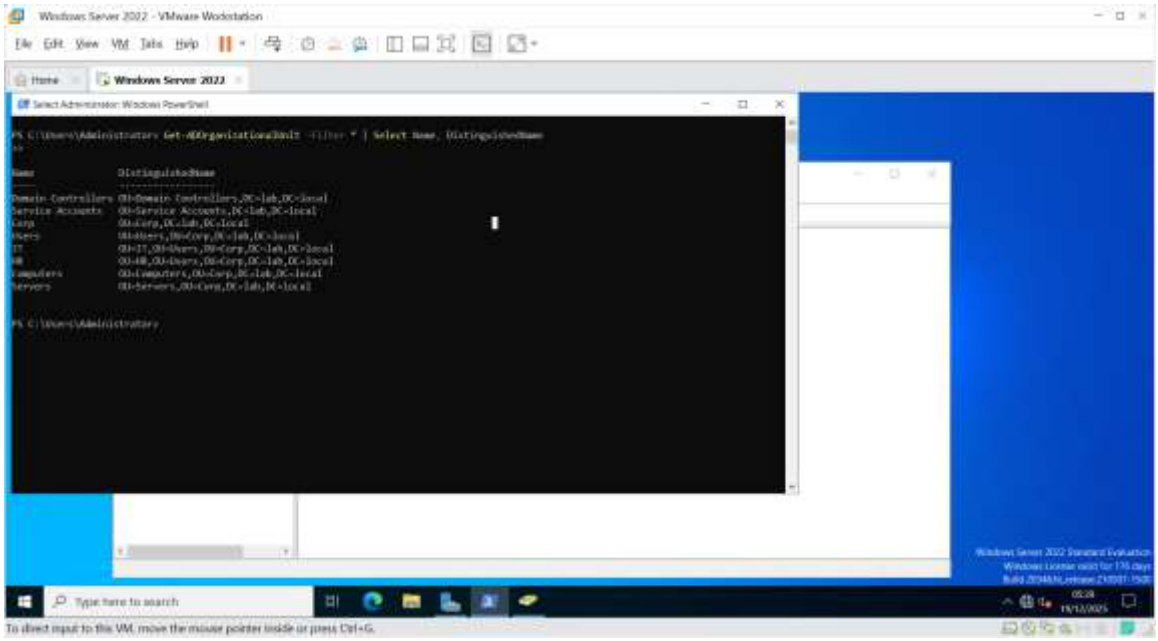

Figure 33: Screenshot evidence.
Source file: OUStructureConfirmed.png

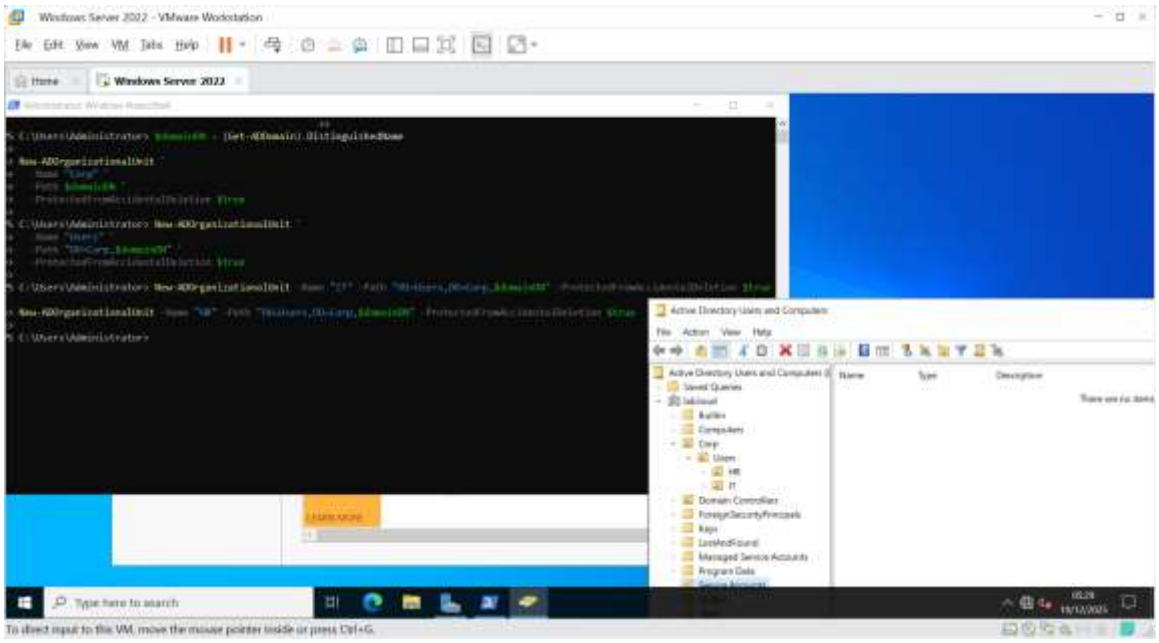

Figure 34: Screenshot evidence.
Source file: OUStructureCorrect.png

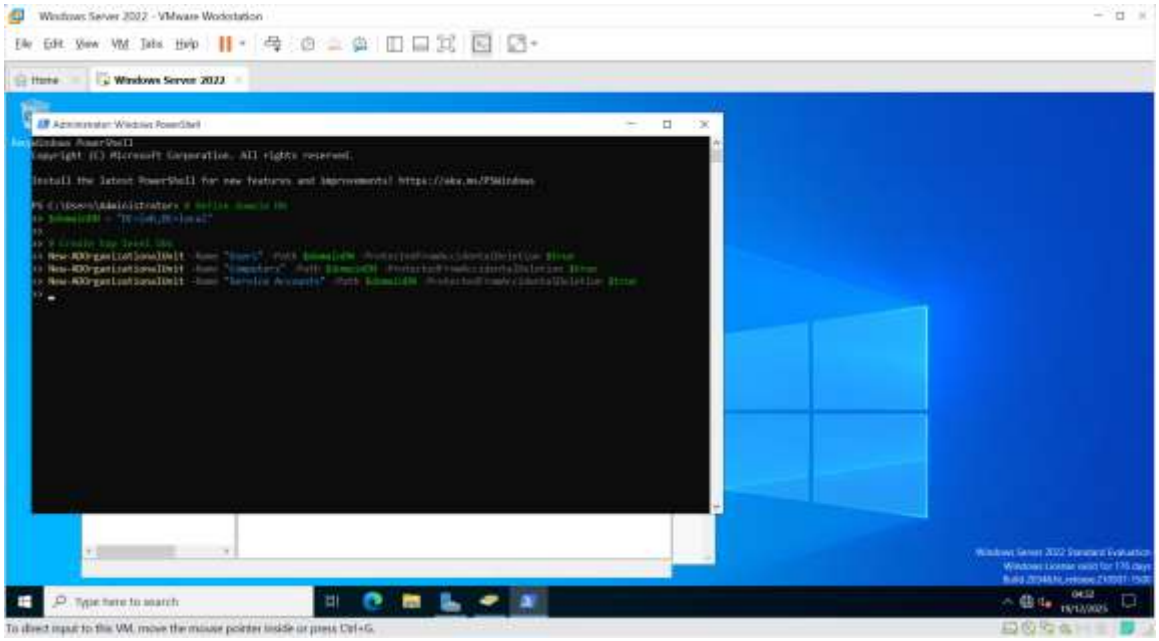

Figure 35: Screenshot evidence.
Source file: PowerShellScrpitCrreateTopLevelOUs.png

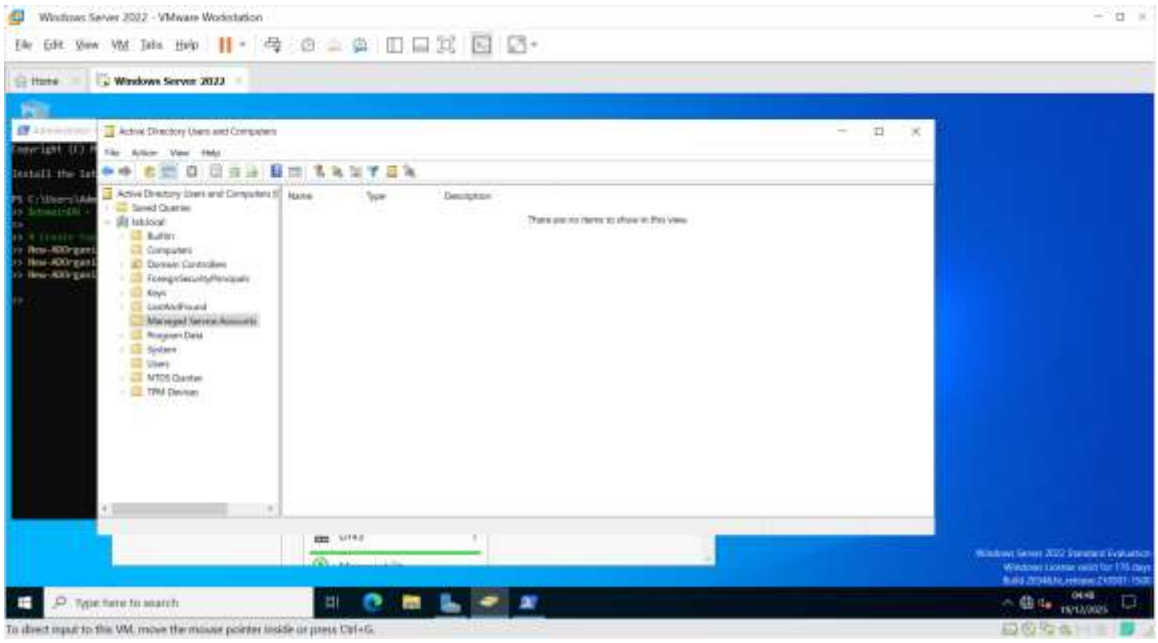

Figure 36: Screenshot evidence.
Source file: TopLevelOUs.png

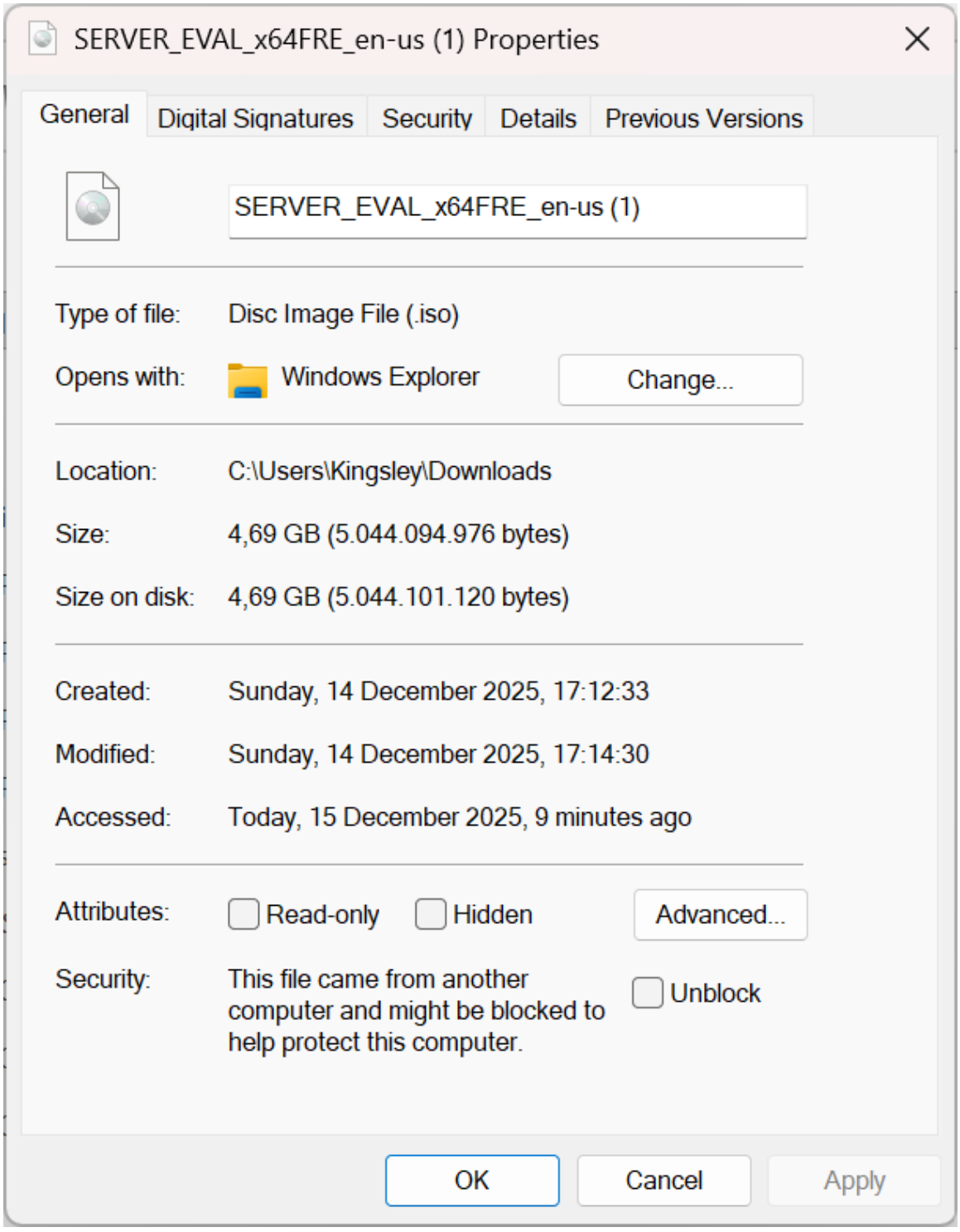

Figure 37: Screenshot evidence.
Source file: WindowsSeverisoUnblock.png

Scenario 5 — Drive Mapping / File Access

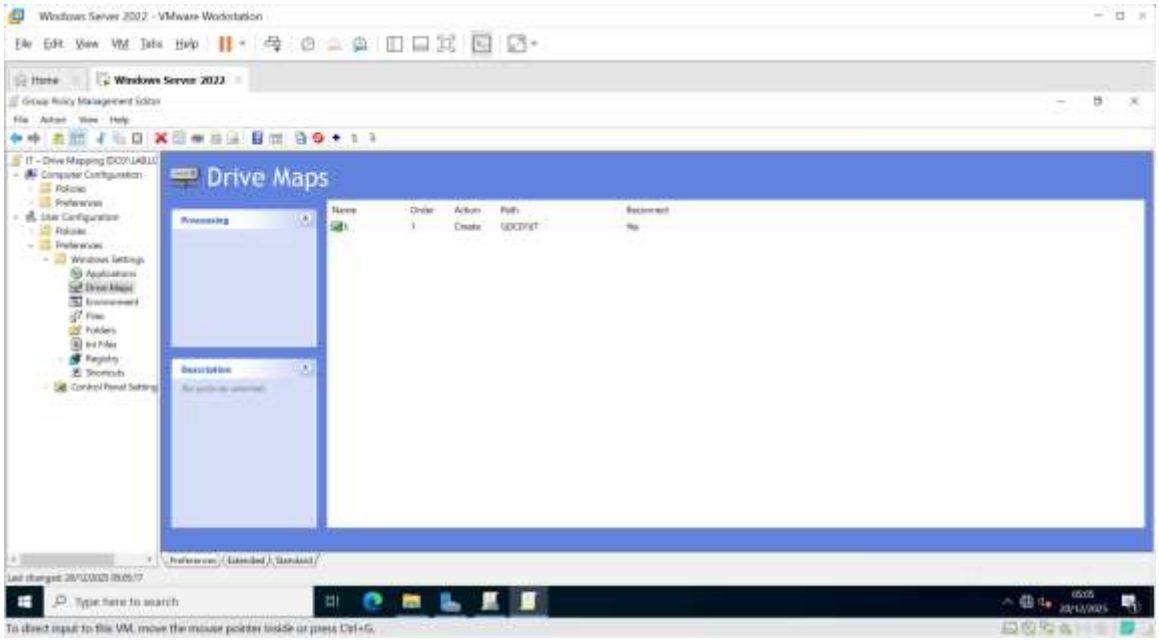

Figure 38: Group Policy drive mapping configuration.

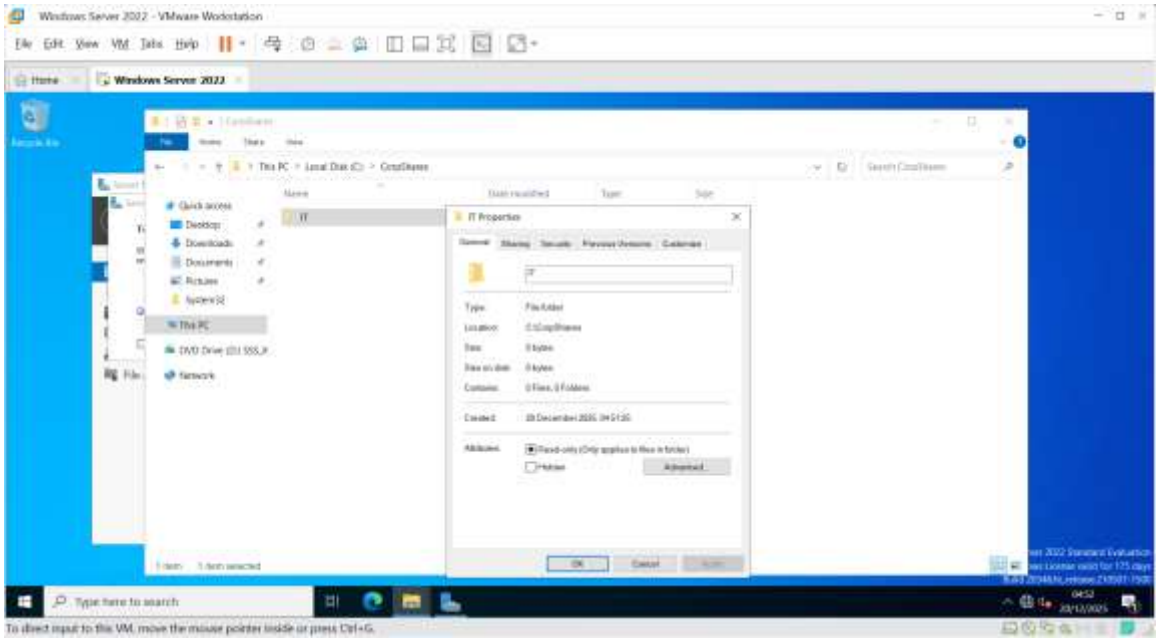

Figure 39: Screenshot evidence.
Source file: ShareFolderCreated.png

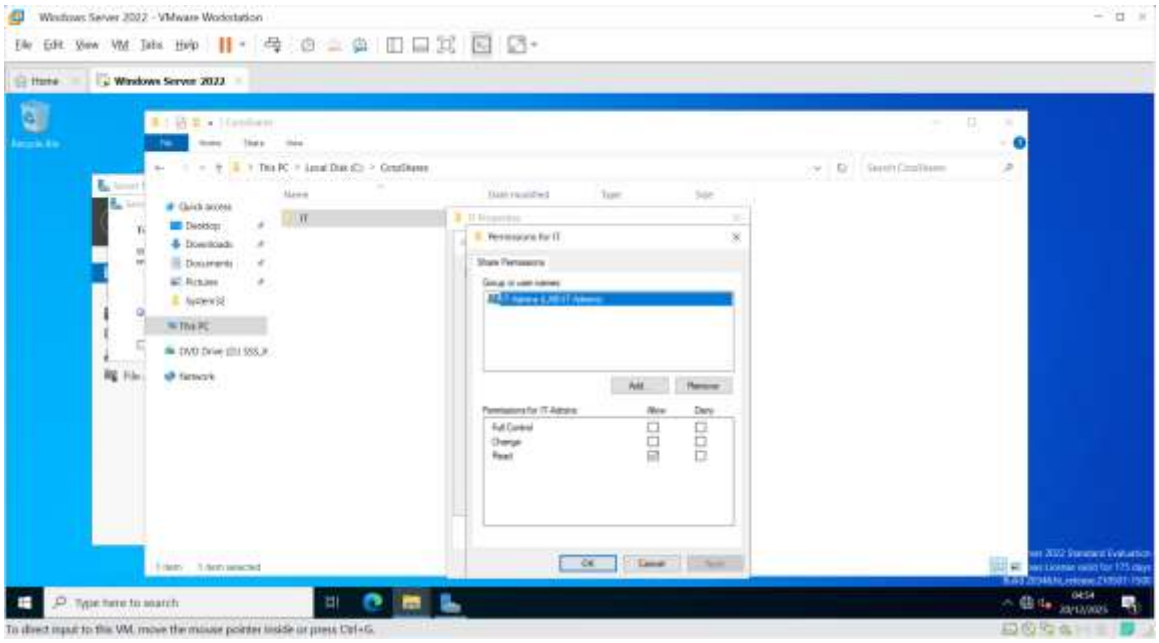

Figure 40: Screenshot evidence.
Source file: SharePermissions.png

Additional Supporting Evidence

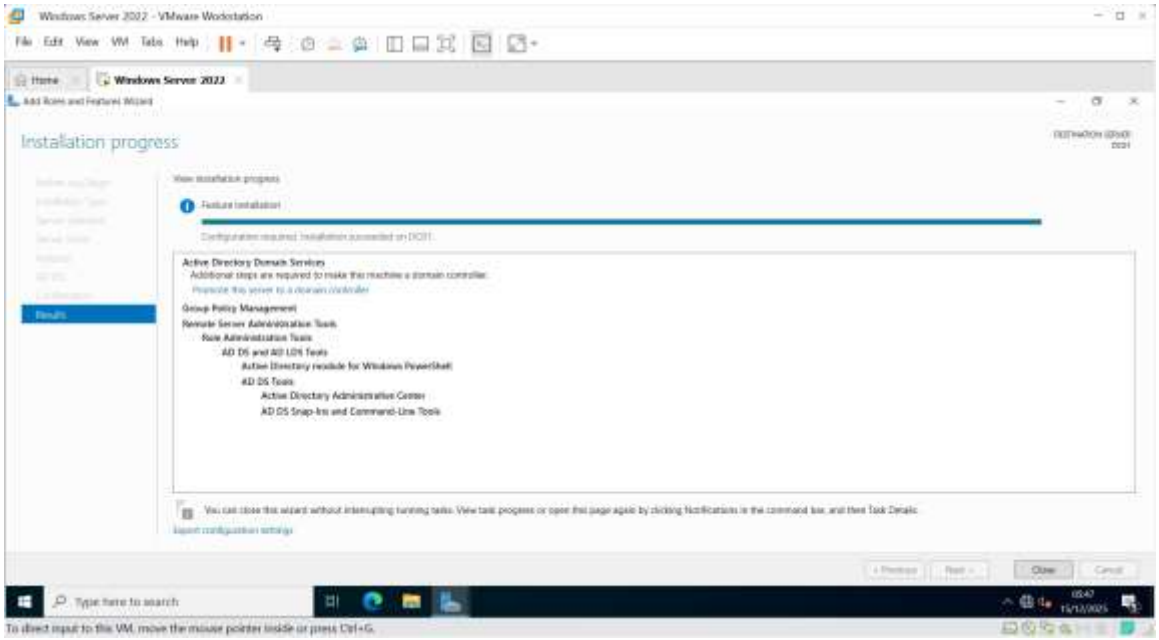

Figure 41: Screenshot evidence.
Source file: ADDSRoleInstalled.png

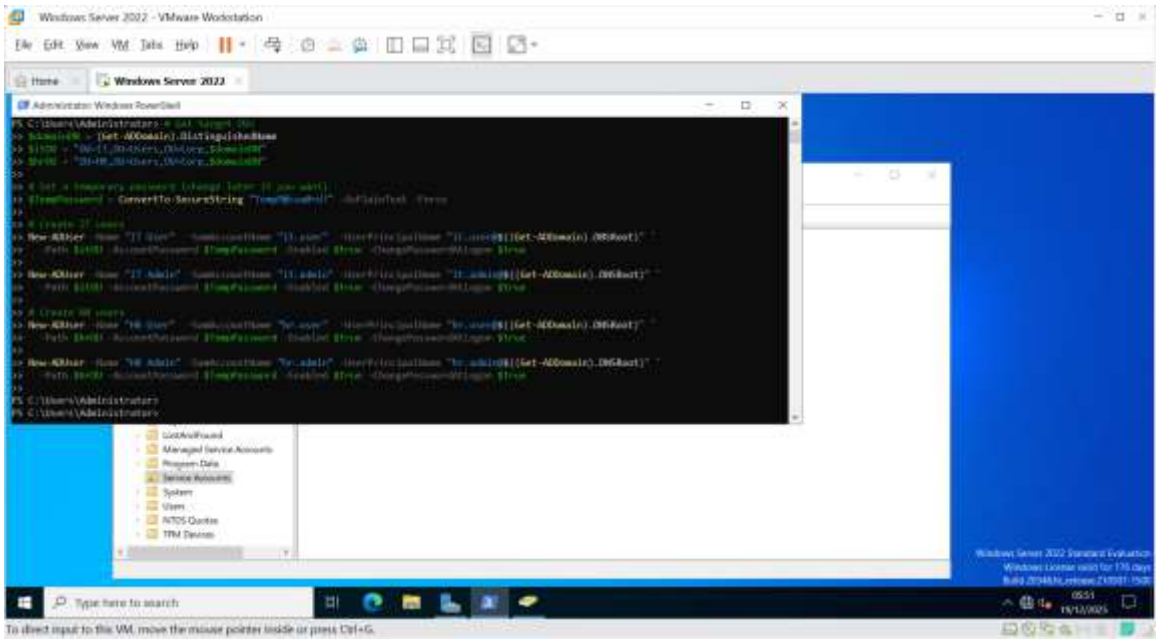

Figure 42: Screenshot evidence.
Source file: ADUsersCreatedPowerShell.png

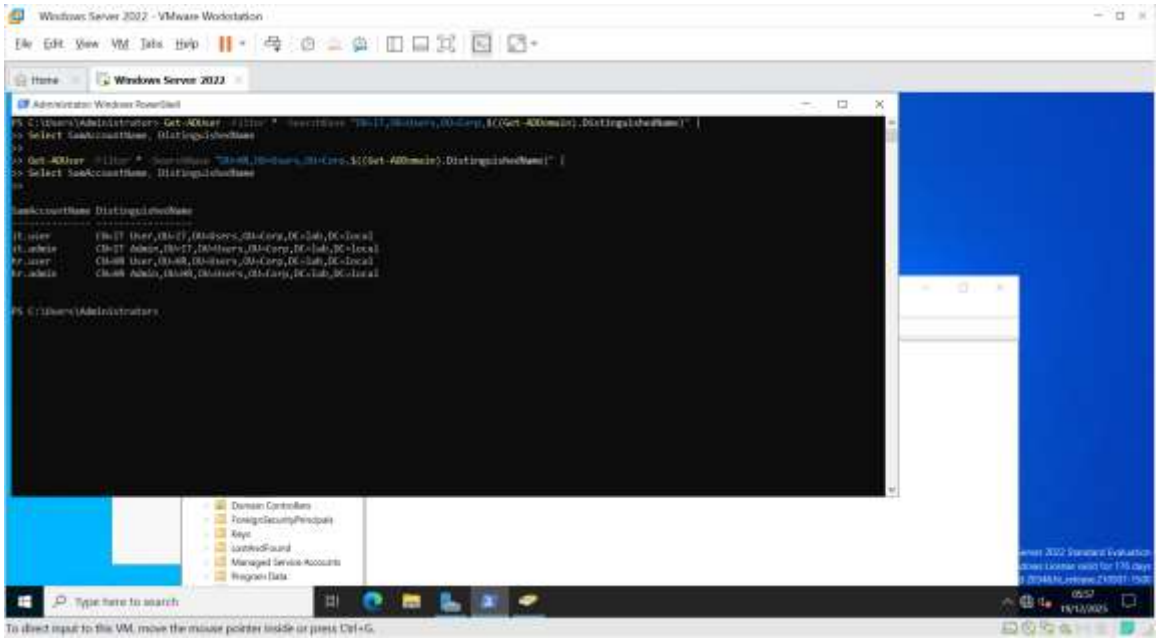

Figure 43: Screenshot evidence.
Source file: ADUsersVerifiedDN.png

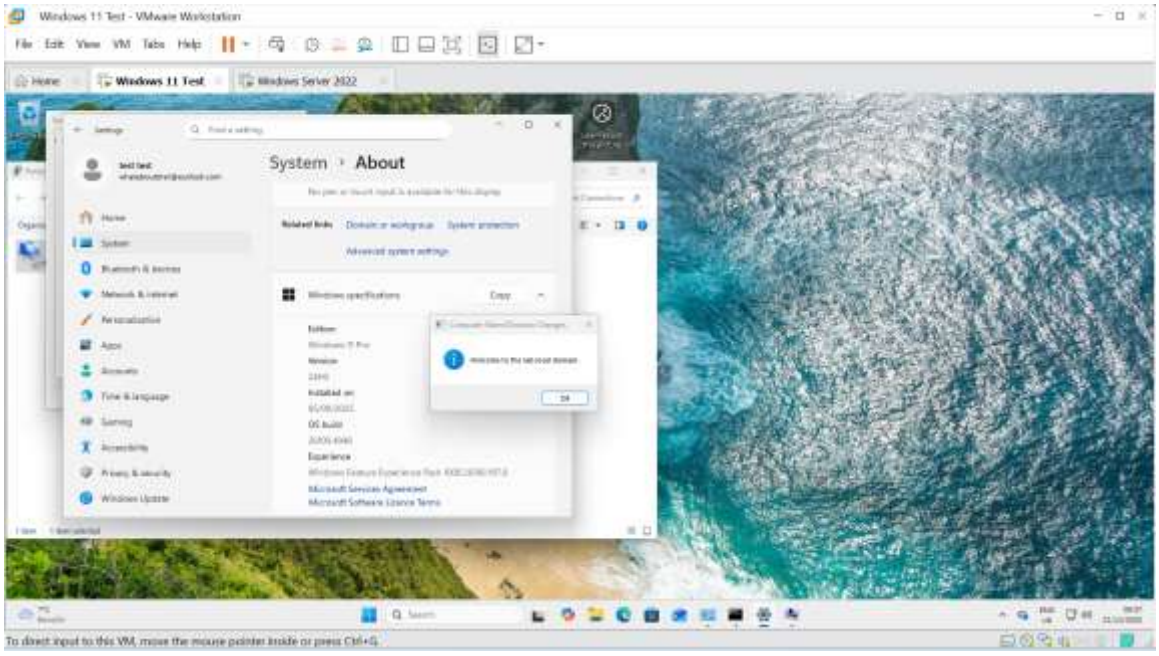

Figure 44: Screenshot evidence.
Source file: DomainJoinSuccess.png

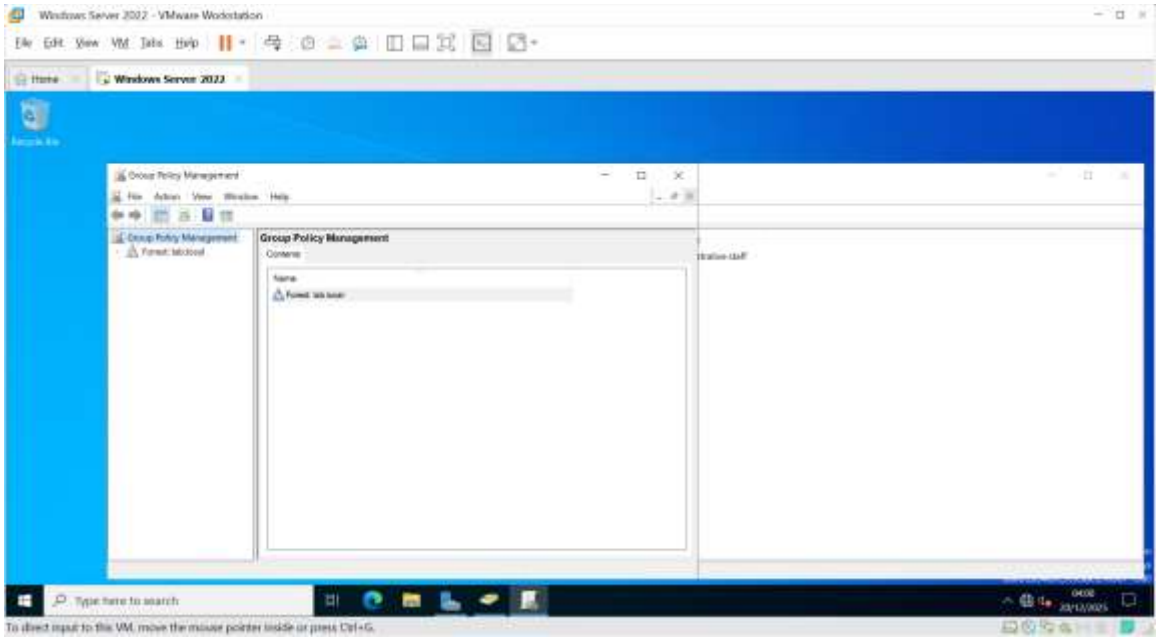

Figure 45: Screenshot evidence.
Source file: GPMCOpened.png

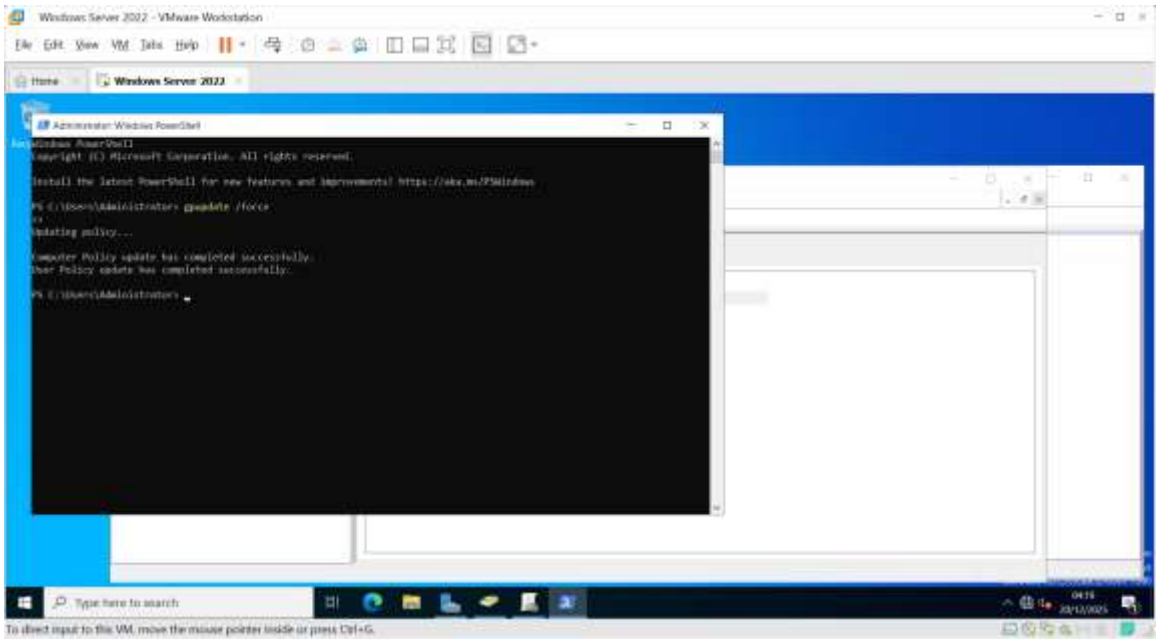

Figure 46: Screenshot evidence.
Source file: gpupdateforce.png

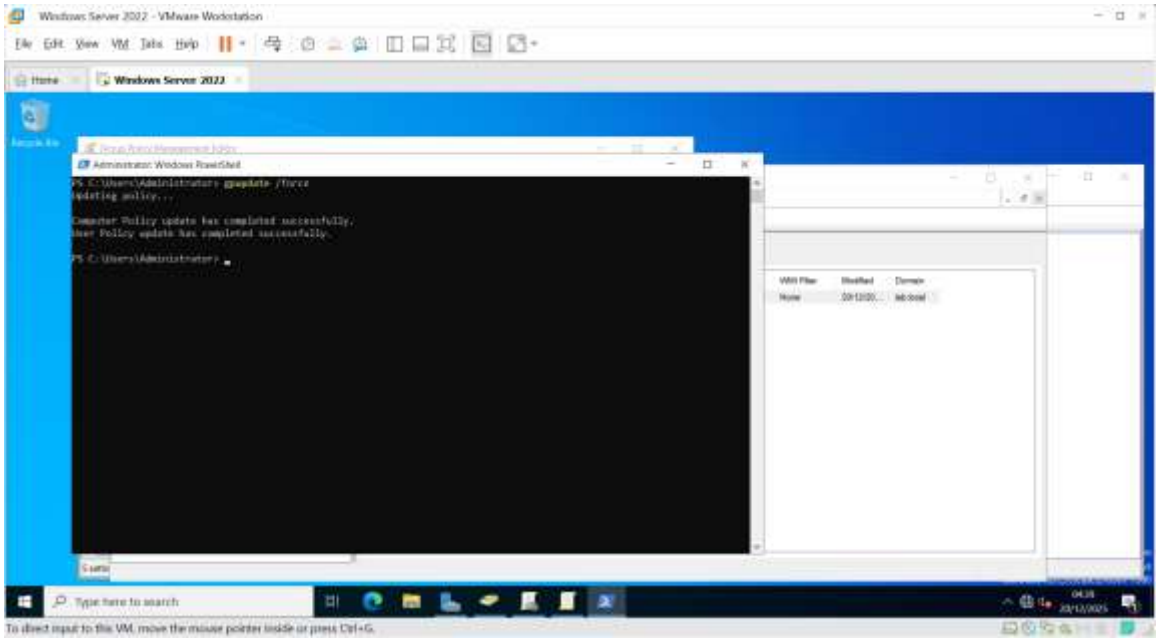

Figure 47: Screenshot evidence.
Source file: gpupdateforce1.png

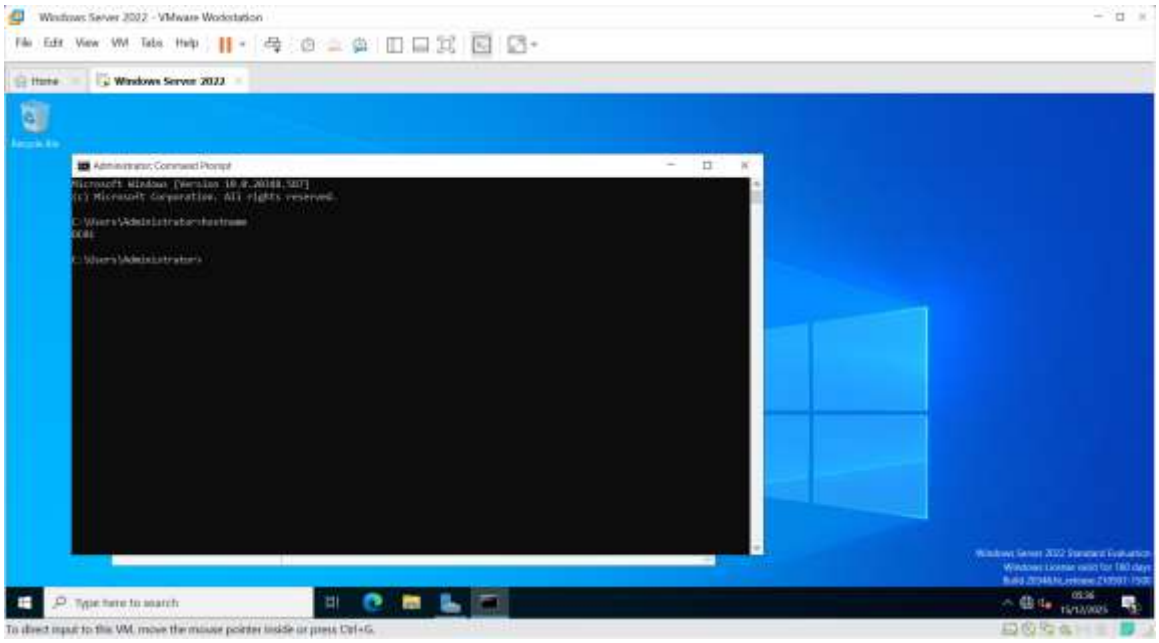

Figure 48: Screenshot evidence.
Source file: ServerRenamed.png

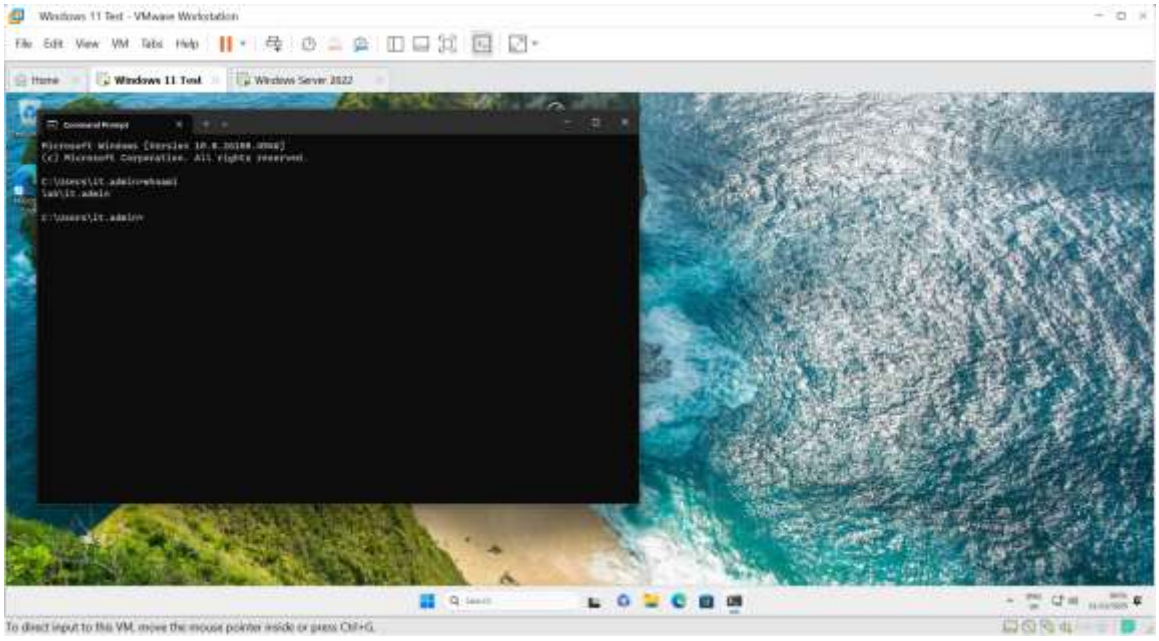

Figure 49: Screenshot evidence.
Source file: whoamiVerified.png

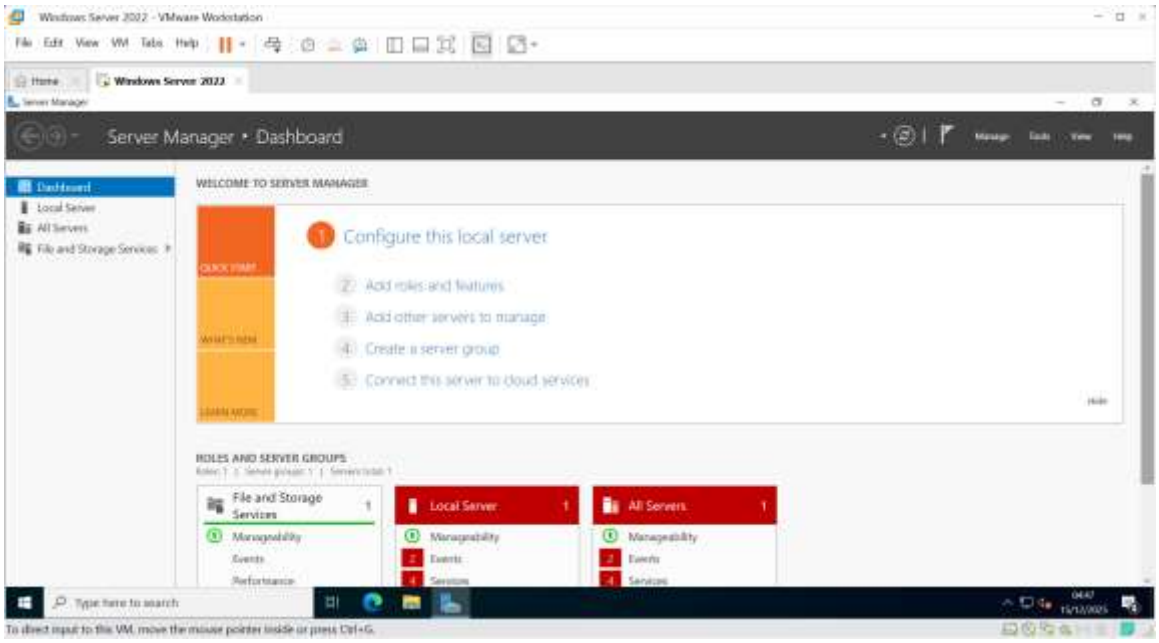

Figure 50: Screenshot evidence.
Source file: WindowsSever2022Installed.png

Tools Used:
- Event Viewer
- Task Scheduler
- Active Directory Users and Computers (ADUC)
- Group Policy Management Console (GPMC)
- gpupdate / gpresult / RSOP
- PowerShell (basic administration)
- VMware Workstation