چک‌لیست نهایی تحویل پروژه Hardening شبکه مایکروسافت و سرورها

این چک‌لیست می‌تواند به عنوان **Acceptance Checklist** یا **Closing Report** در انتهای پروژه Hardening به مشتری ارائه شود.

- آخرین Security Updates نصب شده است.
- SMBv1 غیرفعال شده است.
- LDAP Signing فعال شده است.
- LDAP Channel Binding فعال شده است.
- NTLMv1 غیرفعال شده است.
- Anonymous Enumeration غیرفعال شده است.
- Print Spooler روی Domain Controller غیرفعال شده است.
- دسترسی مستقیم کاربران به Domain Controller محدود شده است.
- سرویس‌های غیرضروری حذف یا غیرفعال شده‌اند.
- Secure Time Synchronization بررسی شده است.
- حساب Administrator پیش‌فرض Rename شده است.
- Guest Account غیرفعال شده است.
- Separate Admin Account پیاده‌سازی شده است.
- Privileged Accounts شناسایی و مستندسازی شده‌اند.
- گروه‌های Domain Admins بازبینی شده‌اند.
- گروه‌های Enterprise Admins بازبینی شده‌اند.
- گروه‌های Schema Admins بازبینی شده‌اند.
- اصل Least Privilege اعمال شده است.
- Delegationهای غیرضروری حذف شده‌اند.
- Password Complexity فعال است.
- Password History فعال است.
- Minimum Password Length تنظیم شده است.
- Maximum Password Age تنظیم شده است.
- Account Lockout Policy اعمال شده است.
- Kerberos Policy بررسی شده است.
- NTLM محدود شده است.
- MFA برای دسترسی‌های مدیریتی پیاده‌سازی شده است.
- Interactive Logon Banner فعال شده است.
- USB Storage Policy اعمال شده است.
- AutoRun غیرفعال شده است.
- PowerShell Logging فعال شده است.
- PowerShell Transcription فعال شده است.
- Command Prompt محدود شده است.
- LLMNR غیرفعال شده است.
- NetBIOS غیرفعال شده است.
- Windows Firewall توسط GPO مدیریت می‌شود.
- Audit Policies اعمال شده‌اند.
- آخرین Patch ها نصب شده‌اند.
- Windows Defender فعال است.
- Real-Time Protection فعال است.

- Tamper Protectionفعال است.
- SMB Signingفعال شده است.
- Windows Firewallفعال است.
- سرویس‌های غیرضروری حذف شده‌اند.
- Local Administrator Password Solution (LAPS)پیاده‌سازی شده است.
- UACفعال و تنظیم شده است.
- DNS Zone Transferمحدود شده است.
- Recursive Queryبررسی شده است.
- Dynamic Updateفقط برای سیستم‌های مجاز فعال است.
- DNS Loggingفعال شده است.
- DNS Cache Poisoning Protectionبررسی شده است.
- رکوردهای غیرضروری حذف شده‌اند.
- DHCP Authorized Serverبررسی شده است.
- Scopeها مستندسازی شده‌اند.
- Lease Configurationبازبینی شده است.
- DHCP Audit Loggingفعال شده است.
- Reservationهای غیرضروری حذف شده‌اند.
- Share Permissionها بازبینی شده‌اند.
- NTFS Permissionها بازبینی شده‌اند.
- Everyone Permissionحذف شده است.
- دسترسی‌های Excessive حذف شده‌اند.
- Sensitive Data Sharesشناسایی شده‌اند.
- File Access Auditingفعال شده است.
- Inheritanceهای غیرضروری اصلاح شده‌اند.
- RDPفقط برای کاربران مجاز فعال است.
- NLAفعال شده است.
- RDP Encryptionبررسی شده است.
- MFAبرای RDP فعال شده است.
- دسترسی RDP به Domain Controller محدود شده است.
- RDP Loggingفعال شده است.
- Advanced Audit Policyفعال شده است.
- Account Logon Auditingفعال شده است.
- Logon/Logoff Auditingفعال شده است.
- Object Access Auditingفعال شده است.
- Privilege Use Auditingفعال شده است.
- Event Forwardingتنظیم شده است.
- Vulnerability Scanقبل از Hardening انجام شده است.
- Vulnerability Scanپس از Hardening انجام شده است.
- تست عملکرد سرویس‌ها انجام شده است.
- تست احراز هویت کاربران انجام شده است.
- تست Group Policy انجام شده است.
- مستندات Hardening تحویل شده است.
- تأیید نهایی کارفرما اخذ شده است.