عنوان سند: چک لیست ممیزی امنیتی و مقاوم سازی VMware	کارفرما: واحد امنیت بانک	تاریخ تهیه سند: ۱۴۰۲/۲/۷
دسته بندی: کنترل های امنیتی جهت مقاوم سازی هایپروایزر ESXi	پیمانکار: شرکت فناوری	تهیه کننده : سیدحسام الدین حسینی

کنترل امنیتی	پاسخ			توضیحات	مقدار پیش فرض / مقدار پیشنهادی	نحوه ممیزی	اقدام اصلاحی
	بلی	خیر	نامربوط				
آیا اکانت کاربر در صورت لاگین ناموفق، برای مدت زمان مشخصی Lock Out خواهد شد؟				چنانچه کاربر چندین بار لاگین ناموفق داشته باشد نام کاربری در یک بازه زمانی مشخص که بر حسب ثانیه است Lockout میشود.	120 900	Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountUnlockTime	Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountUnlockTime | Set-AdvancedSetting -Value 900
آیا تعداد تلاش کاربر برای لاگین به سرور ESXi محدود شده است؟				جهت جلوگیری از حملاتی چون Brute Force بایستی تعداد دفعات تلاش کاربر برای لاگین به سرور محدود شود.	10 5	Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountLockFailures	Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountLockFailures | Set-AdvancedSetting -Value 5
آیا امکان استفاده از رمز عبورهای قبلی برای لاگین به سرور ESXi محدود شده است؟				توصیه میشود تاریخچه کلمات عبور کاربران نگهداری شود و به دلایل امنیتی کاربر امکان استفاده از رمز عبورهای اخیر خود را نداشته باشد.	0 5	Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordHistory	Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordHistory | Set-AdvancedSetting -Value 5
آیا پالیسی برای پیچیدگی رمز عبور کاربر تعیین شده است؟				استفاده از Password Policy از جمله استفاده از کلمات عبور با طول زیاد و استفاده از کاراکترهای ویژه جهت افزایش امنیت رمز عبور ضروری است .همچنین توصیه میشود از کلمه عبور root استفاده نشود.	"retry=3 min=disabled,disabled ,disabled,7,7"	Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordQualityControl	Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordQualityControl | Set-AdvancedSetting -Value "retry=3 min=disabled,15,15,15,15 max=64 similar=deny passphrase=3"
آیا احراز هویت کاربران اکتیودایرکتوری از طریق Authentication Proxy فعال شده است؟				چنانچه سرور ESXi به اکتیو دایرکتوری جوین شود، نام کاربری و رمز عبور کاربران در قسمت Host Profile سرور ESXi ذخیره می گردد. جهت جلوگیری از ذخیره سازی نام کاربری و رمز عبور می توان از قابلیت Authentication Proxy استفاده کرد.	Not Configured	Get-VMHost -Name $ESXi | Get-VMHostAuthentication | Select-Object VMHost,Domain,DomainMembershipStatus	N/A
آیا سرور ESXI به دامین جوین شده است ؟				با جوین کردن سرور ESXi به اکتیو دایرکتوری میتوان اطمینان داشت که یکسری پالیسی ها از جمله Password Policy از سمت اکتیودایرکتوری الزامی است. پیشنهاد میشود یک گروه به نام ESX Admins در اکتیودایرکتوری ایجاد و مجوز مدیریت ESXi به این گروه اعطا گردد.	Not Configured	Get-VMHost -Name $ESXi | Get-VMHostAuthentication | Select-Object VMHost,Domain,DomainMembershipStatus	N/A
آیا در صورت بیکار بودن ارتباط DCUI ، زمانی برای قطع ارتباط پیکربندی شده است؟ DCUI (Direct Console User Interface)				در صورتیکه ارتباط با سرور ESXi از طریق کنسول برقرار شده است و برای مدت مشخصی بیکار است باید این ارتباط قطع شود.	600 600	Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.DcuiTimeOut	Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.DcuiTimeOut | Set-AdvancedSetting -Value 600
آیا ویژگی CIM غیرفعال شده است ؟ CIM (Common Information Model)				ویژگی CIM یکسری اطلاعات راجع به سلامت سخت افزارها ارایه می کند که اگر از این ویژگی استفاده نمی شود پیشنهاد میشود غیرفعال گردد. غیر فعال سازی این ویژگی بر روی عملکرد یکسری سنسورهای سخت افزاری که اطلاعاتی را گزارش می کنند تاثیر میگذارد.	Start and stop host → manually	Get-VMHostService -VMHost $ESXi \| Where-Object {$_.Key -eq 'sfcbd-watchdog' -and $_.Running -eq 'True'} Get-VMHostService -VMHost $ESXi \| Where-Object {$_.Key -eq 'sfcbd-watchdog' -and $_.Policy -eq 'On'}	Get-VMHostService -VMHost $ESXi \| where {$_.Key -eq 'sfcbd-watchdog'} | Set-VMHostService -Policy Off Get-VMHostService -VMHost $ESXi \| where {$_.Key -eq 'sfcbd-watchdog'} | Stop-VMHostService
آیا ویژگی MOB غیرفعال شده است ؟ MOB (Managed Object Browser)				MOB یک اپلیکیشن تحت وب است که از طریق ESXi و vcenter قابل دسترس است و یکسری اطلاعات اضافی و جزییات روی VM ها و Datastore و Resource Pool ها را ارایه می دهد.	False False	Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.plugins.solo.enableMob	Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.plugins.solo.enableMob | Set-AdvancedSetting -Value False
آیا سرویس SLP غیرفعال شده است ؟ SLP (Service Location Protocol)				سرویس SLP ترافیک ورودی شبکه را بدون احراز هویت و با دسترسی Root بررسی و مورد تجزیه و تحلیل قرار میدهد که باعث می شود هدف مناسبی برای سو استفاده و حمله باشد و بایستی غیرفعال گردد.	Start and stop host → manually	Get-VMHostService -VMHost $ESXi \| Where-Object {$_.Key -eq 'slpd' -and $_.Running -eq 'True'} Get-VMHostService -VMHost $ESXi \| Where-Object {$_.Key -eq 'slpd' -and $_.Policy -eq 'On'}	Get-VMHostService -VMHost $ESXi \| where {$_.Key -eq 'slpd'} | Set-VMHostService -Policy Off Get-VMHostService -VMHost $ESXi \| where {$_.Key -eq 'slpd'} | Stop-VMHostService
آیا پروتکل SNMP غیر فعال شده است ؟				پروتکل SNMP بمنظور مانیتورینگ منابع سرور ورد استفاده قرار میگیرد که اگر استفاده نمیشود بایستی غیرفعال گردد.	Start and stop host → manually	Get-VMHostService -VMHost $ESXi \| Where-Object {$_.Key -eq 'snmpd' -and $_.Running -eq 'True'} Get-VMHostService -VMHost $ESXi \| Where-Object {$_.Key -eq 'snmpd' -and $_.Policy -eq 'On'}	Get-VMHostService -VMHost $ESXi \| where {$_.Key -eq 'snmpd'} | Set-VMHostService -Policy Off Get-VMHostService -VMHost $ESXi \| where {$_.Key -eq 'snmpd'} | Stop-VMHostService
آیا پروتکل SSH غیرفعال شده است ؟				پروتکل SSH برای ارتباط و مدیریت سرور ESXi مورد استفاده قرار میگیرد که اگر استفاده نمی شود بایستی غیرفعال گردد.	Start and stop host → manually	Get-VMHostService -VMHost $ESXi \| Where-Object {$_.Key -eq 'TSM-SSH' -and $_.Running -eq 'True'} Get-VMHostService -VMHost $ESXi \| Where-Object {$_.Key -eq 'TSM-SSH' -and $_.Policy -eq 'On'}	Get-VMHostService -VMHost $ESXi \| where {$_.Key -eq 'TSM-SSH'} | Set-VMHostService -Policy Off Get-VMHostService -VMHost $ESXi \| where {$_.Key -eq 'TSM-SSH'} | Stop-VMHostService
آیا تنظیمات فایروال به درستی انجام شده است ؟				فایروال ESXi در عین سادگی، بسیار موثر عمل می کند و به عنوان یک لایه محافظ در استراتژی دفاع در عمق نقش مهمی دارد. فایروال باید به گونه ای پیکربندی شود که فقط از سیستم ها و سرورهای مورد تایید به ESXi دسترسی وجود داشته باشد.	allowed from any IP address → authorized infrastructure and administration workstations	$ESXcli = Get-EsxCli -VMHost $ESXi -V2 $ESXcli.network.firewall.ruleset.list.Invoke() $ESXcli.network.firewall.ruleset.allowedip.list.Invoke()	$ESXcli = Get-EsxCli -VMHost $ESXi -V2 # Disable firewall temporarily so we don't lose connectivity $arguments = $ESXcli.network.firewall.set.CreateArgs() $arguments.enabled = $false $ESXcli.network.firewall.set.Invoke($arguments) # Unset the "allow all" flag $arguments = $ESXcli.network.firewall.ruleset.set.CreateArgs() $arguments.allowedall = $false $arguments.rulesetid = "sshServer" $ESXcli.network.firewall.ruleset.set.Invoke($arguments) # Add an IP range $arguments =