Implementing Privileged Access Workstation – part 4

michaelfirsov.wordpress.com/6301-2

June 16, 2021

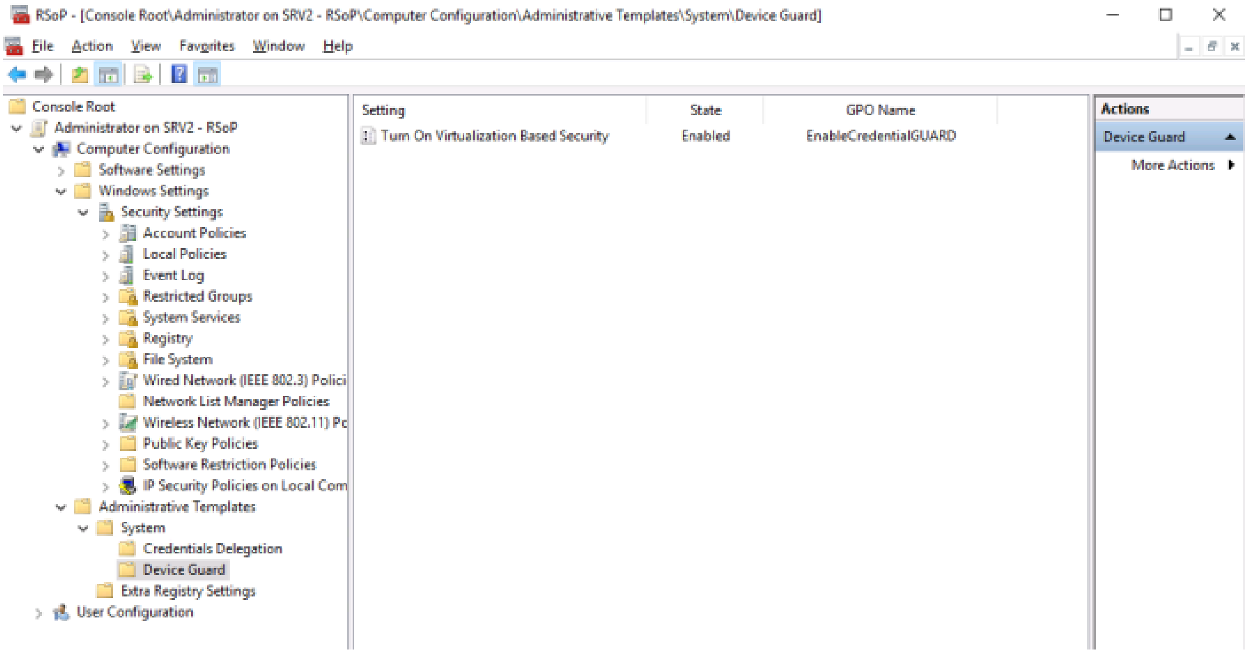
Working with Additional LSA protection

As you already may know the one more security feature – in addition to Credential Guard explained in part3 – exists in Windows 8.1/Windows 2012 R2 and later that can help protect account credentials – Additional LSA protection: you can read about it here. In this article I'd like to show how this feature works in my test environment.

Let's start from checking out what protection we would have with the Credential Guard alone followed with the Credential Guard coupled with the Additional LSA protection mode. For my tests I'll be using mimikatz.

1) Credential Guard alone

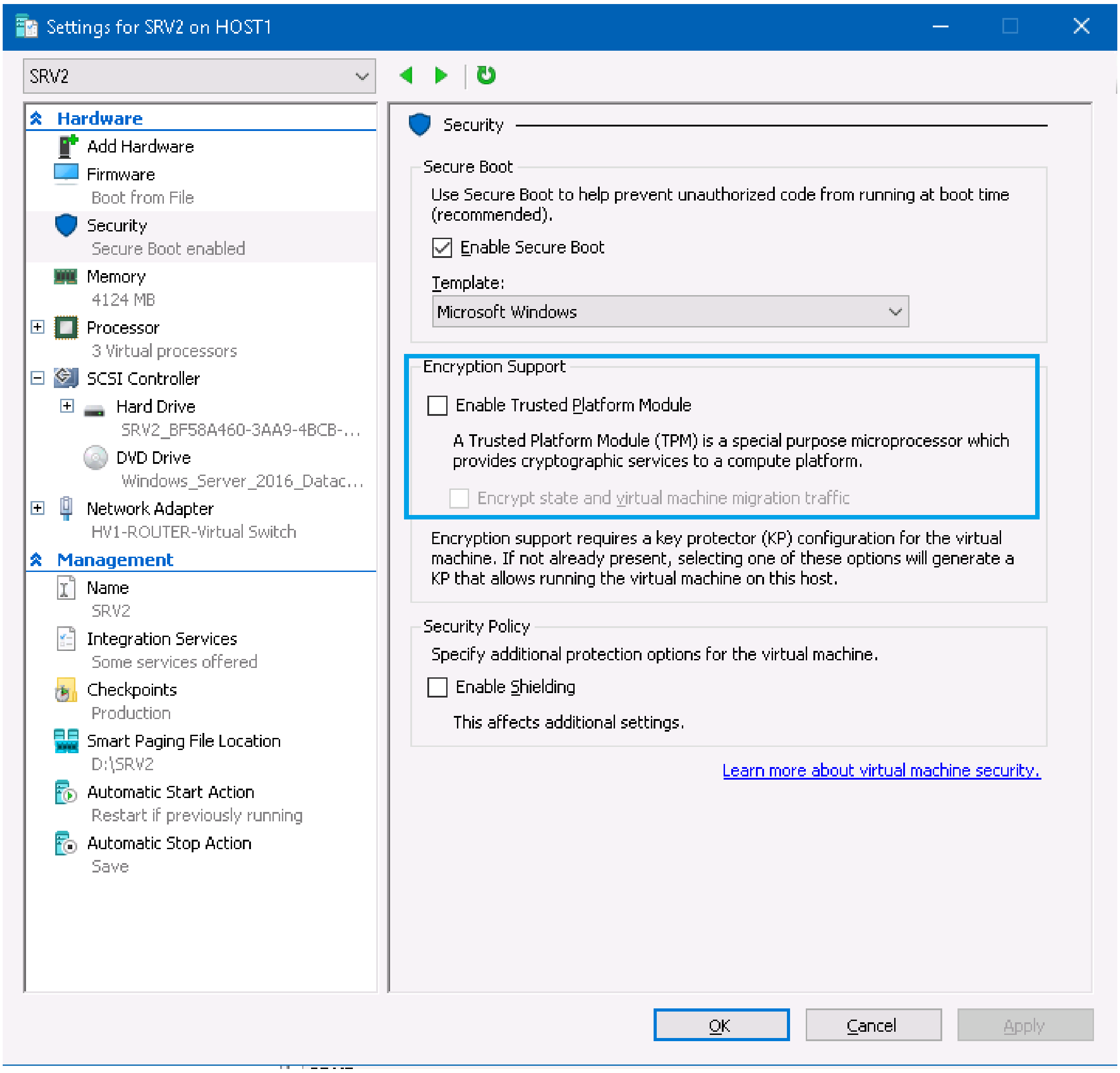
First of all I'll check whether the Credential Guard is enabled on the server (SRV2) :



RSoP - [Console Root\Administrator on SRV2 - RSoP\Computer Configuration\Administrative Templates\System\Device Guard]

Setting	State	GPO Name
Turn On Virtualization Based Security	Enabled	EnableCredentialGUARD

It's enabled in Windows but it' may be not enough for CG to function: it also requires Secure Boot and TPM which must be enabled either in the PC's BIOS or in the properties of the respective virtual machine. Since my SRV2 server is a VM I'll check the SRV2's properties:



Settings for SRV2 on HOST1

SRV2

Hardware

- Add Hardware
- Firmware — Boot from File
- Security — Secure Boot enabled
- Memory — 4124 MB
- Processor — 3 Virtual processors
- SCSI Controller
  - Hard Drive — SRV2_BF58A460-3AA9-4BCB-...
  - DVD Drive — Windows_Server_2016_Datac...
- Network Adapter — HV1-ROUTER-Virtual Switch

Management

- Name — SRV2
- Integration Services — Some services offered
- Checkpoints — Production
- Smart Paging File Location — D:\SRV2
- Automatic Start Action — Restart if previously running
- Automatic Stop Action — Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

☑ Enable Secure Boot

Template: Microsoft Windows

Encryption Support

☐ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

☐ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

Security Policy

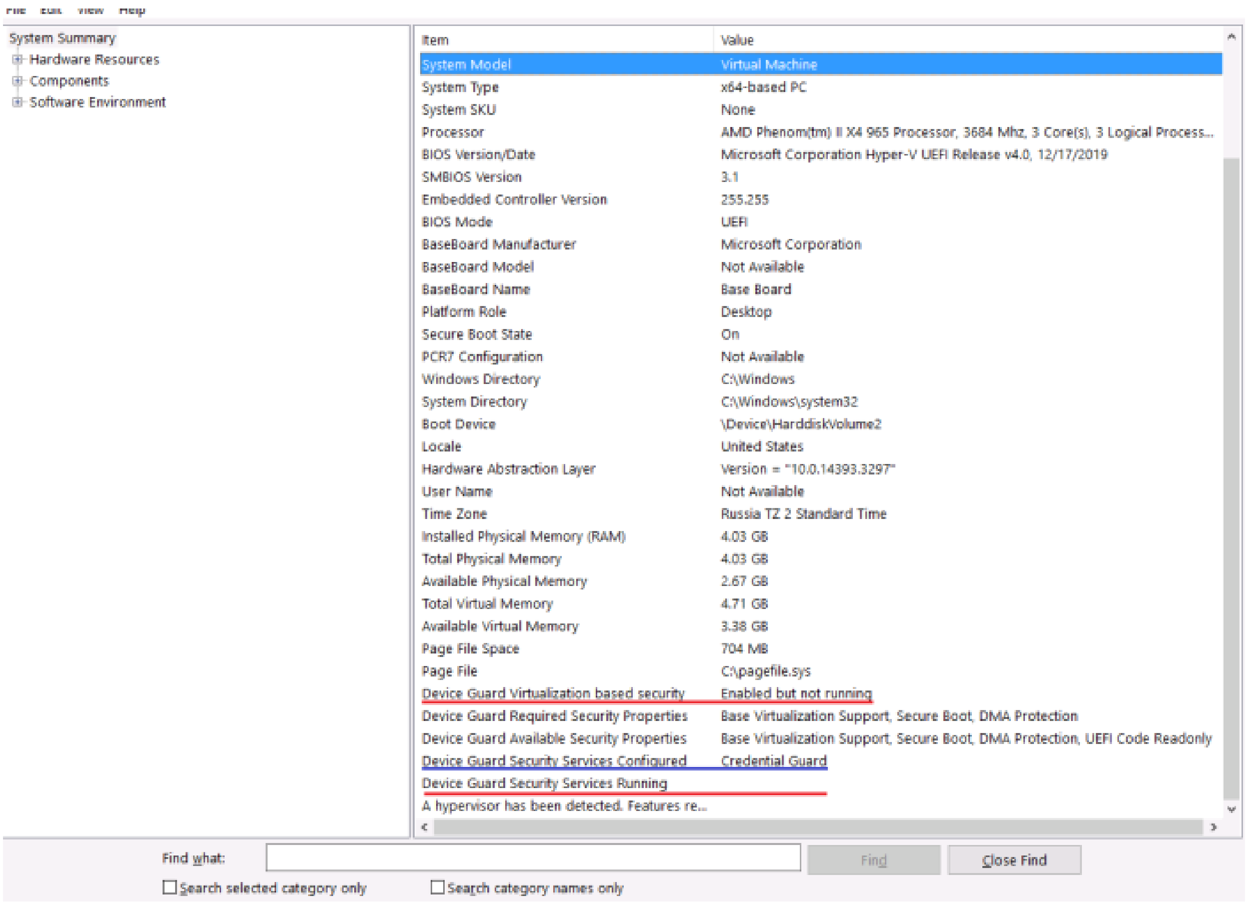
Specify additional protection options for the virtual machine.

☐ Enable Shielding

This affects additional settings.

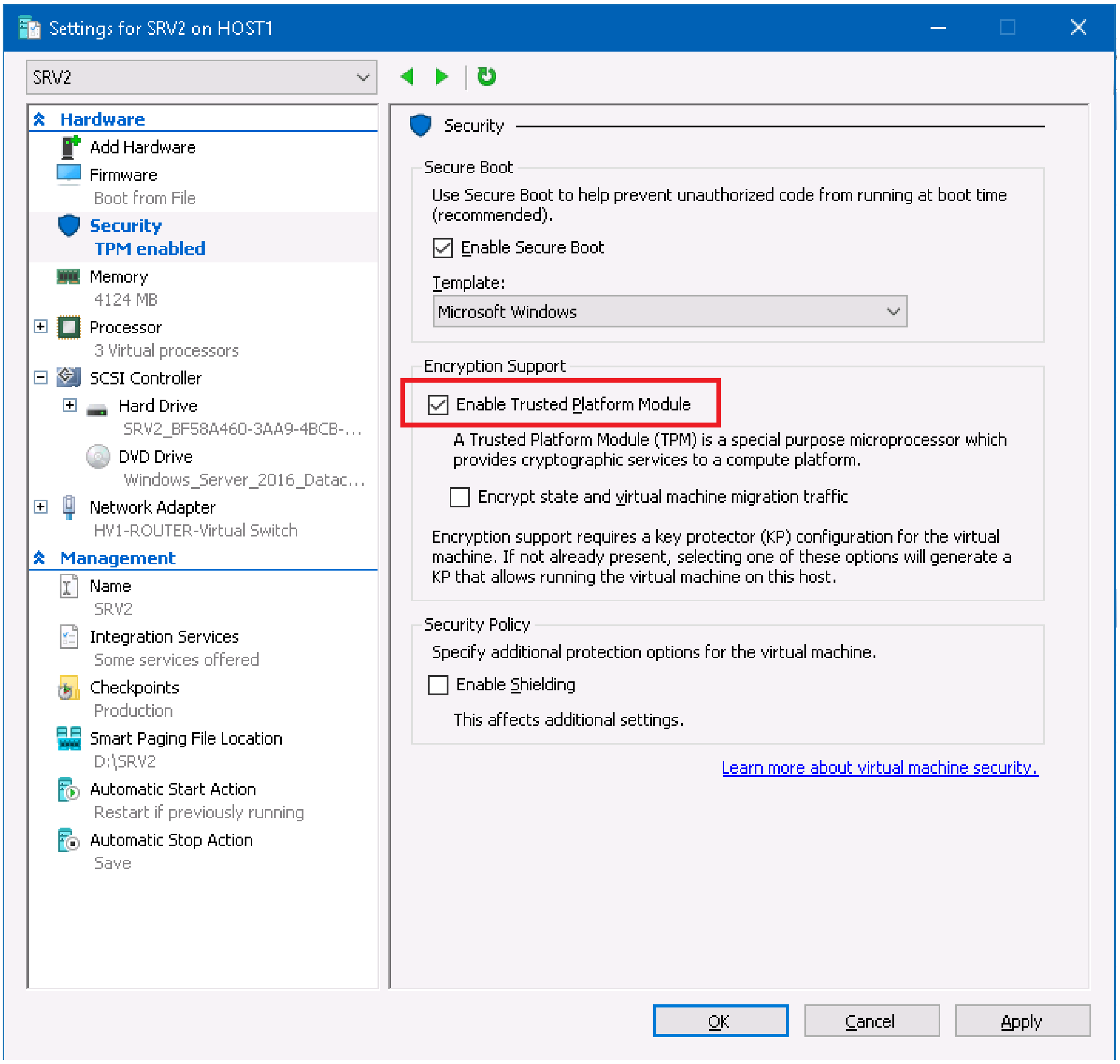
Learn more about virtual machine security.

In this configuration – SecureBoot is on by default but TPM is off so Credential Guard should not work – you can check it using msinfo32:



Item	Value
System Model	Virtual Machine
System Type	x64-based PC
System SKU	None
Processor	AMD Phenom(tm) II X4 965 Processor, 3684 Mhz, 3 Core(s), 3 Logical Process...
BIOS Version/Date	Microsoft Corporation Hyper-V UEFI Release v4.0, 12/17/2019
SMBIOS Version	3.1
Embedded Controller Version	255.255
BIOS Mode	UEFI
BaseBoard Manufacturer	Microsoft Corporation
BaseBoard Model	Not Available
BaseBoard Name	Base Board
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Not Available
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume2
Locale	United States
Hardware Abstraction Layer	Version = "10.0.14393.3297"
User Name	Not Available
Time Zone	Russia TZ 2 Standard Time
Installed Physical Memory (RAM)	4.03 GB
Total Physical Memory	4.03 GB
Available Physical Memory	2.67 GB
Total Virtual Memory	4.71 GB
Available Virtual Memory	3.38 GB
Page File Space	704 MB
Page File	C:\pagefile.sys
Device Guard Virtualization based security	Enabled but not running
Device Guard Required Security Properties	Base Virtualization Support, Secure Boot, DMA Protection
Device Guard Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonly
Device Guard Security Services Configured	Credential Guard
Device Guard Security Services Running	
A hypervisor has been detected. Features re...	

After enabling TPM Credential Guard should be working:



Hardware
- Add Hardware
- Firmware
  Boot from File
- Security
  TPM enabled
- Memory
  4124 MB
- Processor
  3 Virtual processors
- SCSI Controller
  - Hard Drive
    SRV2_BF58A460-3AA9-4BCB-...
  - DVD Drive
    Windows_Server_2016_Datac...
- Network Adapter
  HV1-ROUTER-Virtual Switch

Management
- Name
  SRV2
- Integration Services
  Some services offered
- Checkpoints
  Production
- Smart Paging File Location
  D:\SRV2
- Automatic Start Action
  Restart if previously running
- Automatic Stop Action
  Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

☑ Enable Secure Boot

Template: Microsoft Windows

Encryption Support

☑ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

☐ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

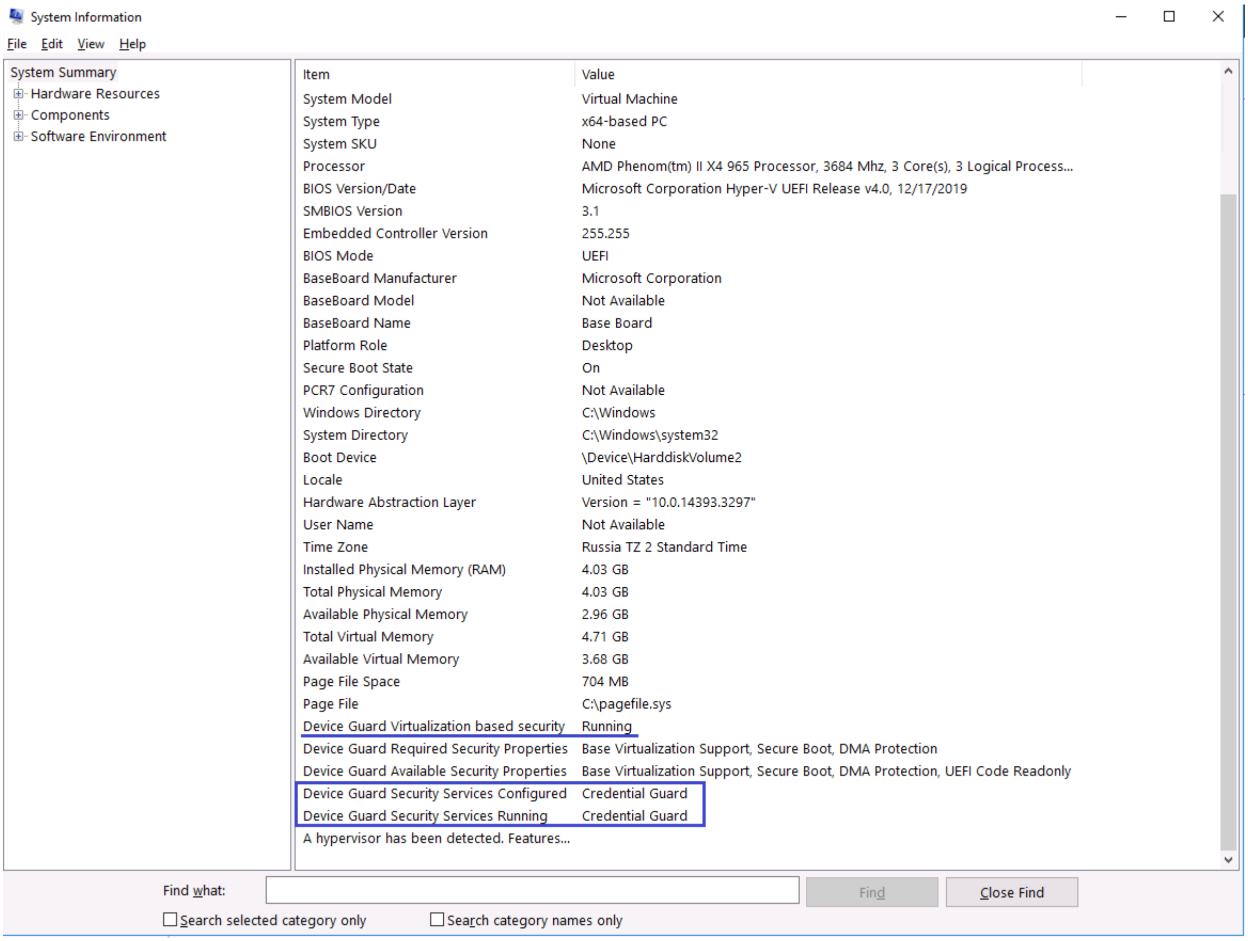
Security Policy

Specify additional protection options for the virtual machine.

☐ Enable Shielding

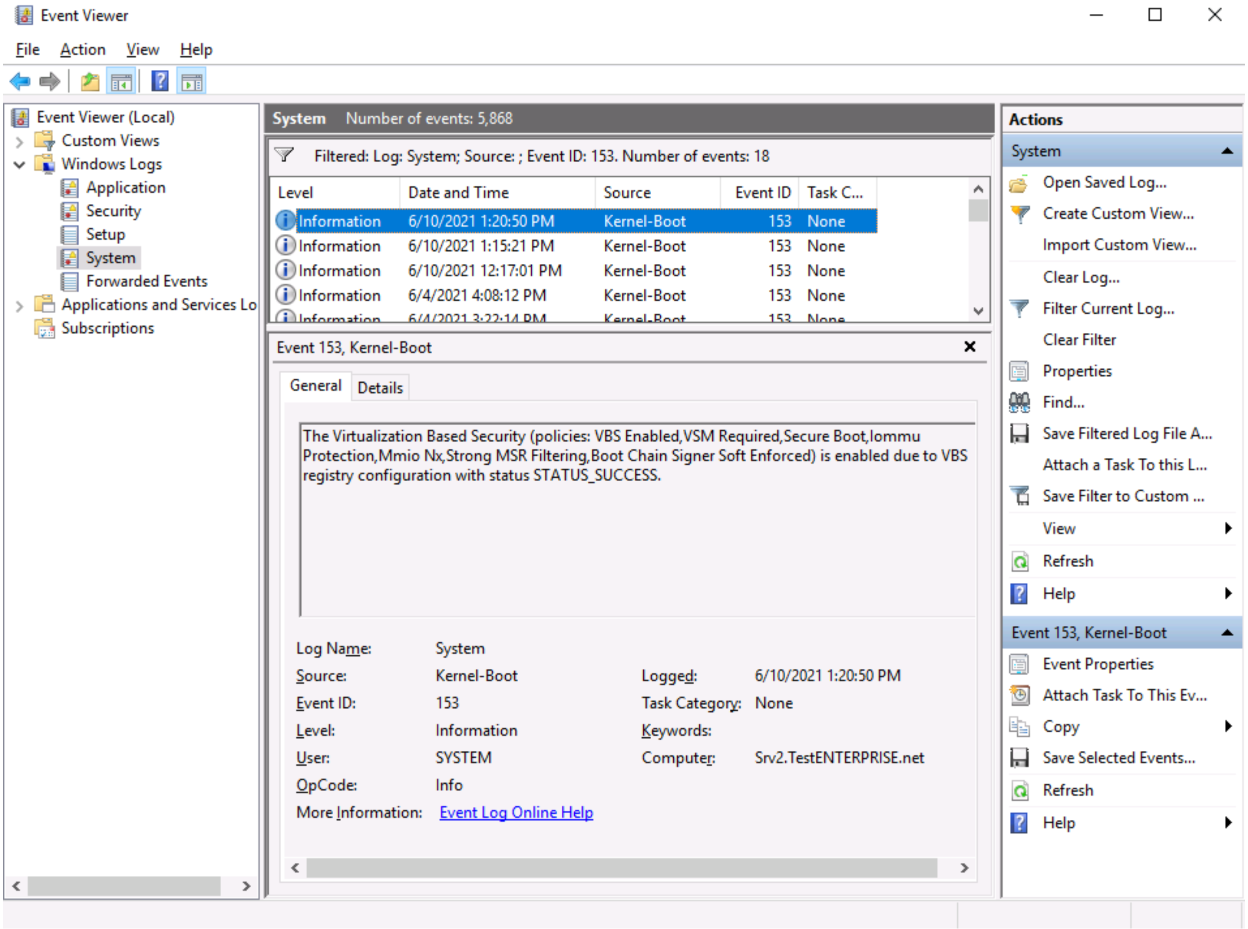
This affects additional settings.

Learn more about virtual machine security.



Item	Value
System Model	Virtual Machine
System Type	x64-based PC
System SKU	None
Processor	AMD Phenom(tm) II X4 965 Processor, 3684 Mhz, 3 Core(s), 3 Logical Process...
BIOS Version/Date	Microsoft Corporation Hyper-V UEFI Release v4.0, 12/17/2019
SMBIOS Version	3.1
Embedded Controller Version	255.255
BIOS Mode	UEFI
BaseBoard Manufacturer	Microsoft Corporation
BaseBoard Model	Not Available
BaseBoard Name	Base Board
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Not Available
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume2
Locale	United States
Hardware Abstraction Layer	Version = "10.0.14393.3297"
User Name	Not Available
Time Zone	Russia TZ 2 Standard Time
Installed Physical Memory (RAM)	4.03 GB
Total Physical Memory	4.03 GB
Available Physical Memory	2.96 GB
Total Virtual Memory	4.71 GB
Available Virtual Memory	3.68 GB
Page File Space	704 MB
Page File	C:\pagefile.sys
Device Guard Virtualization based security	Running
Device Guard Required Security Properties	Base Virtualization Support, Secure Boot, DMA Protection
Device Guard Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonly
Device Guard Security Services Configured	Credential Guard
Device Guard Security Services Running	Credential Guard
A hypervisor has been detected. Features...	

You can also check for the event ID 153 in the System log…



System Number of events: 5,868

Filtered: Log: System; Source: ; Event ID: 153. Number of events: 18

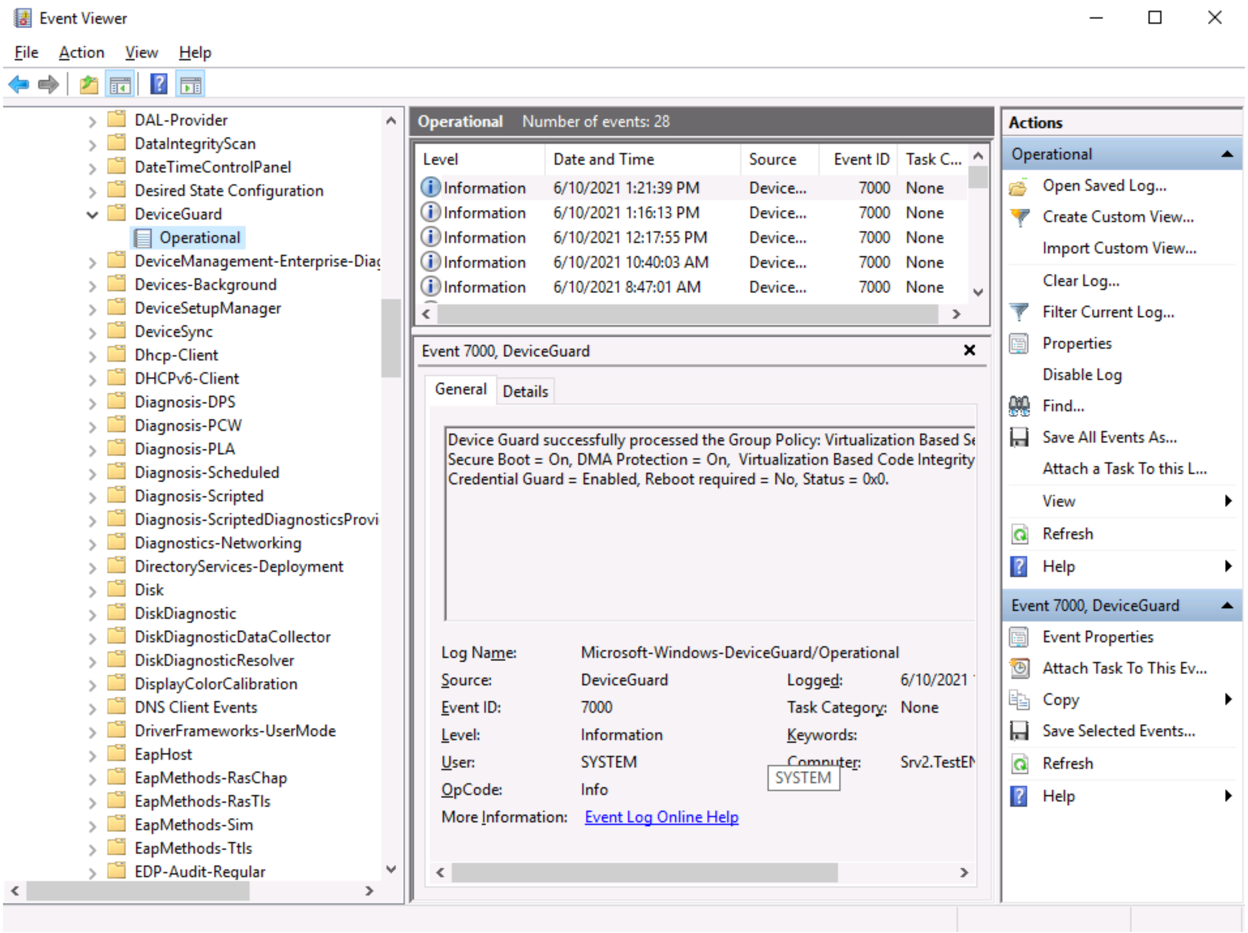
Level	Date and Time	Source	Event ID	Task C...
Information	6/10/2021 1:20:50 PM	Kernel-Boot	153	None
Information	6/10/2021 1:15:21 PM	Kernel-Boot	153	None
Information	6/10/2021 12:17:01 PM	Kernel-Boot	153	None
Information	6/4/2021 4:08:12 PM	Kernel-Boot	153	None
Information	6/4/2021 3:22:14 PM	Kernel-Boot	153	None

Event 153, Kernel-Boot

The Virtualization Based Security (policies: VBS Enabled,VSM Required,Secure Boot,Iommu Protection,Mmio Nx,Strong MSR Filtering,Boot Chain Signer Soft Enforced) is enabled due to VBS registry configuration with status STATUS_SUCCESS.

Log Name:	System		
Source:	Kernel-Boot	Logged:	6/10/2021 1:20:50 PM
Event ID:	153	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Srv2.TestENTERPRISE.net
OpCode:	Info		
More Information:	Event Log Online Help		

…and event ID 7000 in the DeviceGuard\Operational log:



Operational   Number of events: 28

Level	Date and Time	Source	Event ID	Task C...
Information	6/10/2021 1:21:39 PM	Device...	7000	None
Information	6/10/2021 1:16:13 PM	Device...	7000	None
Information	6/10/2021 12:17:55 PM	Device...	7000	None
Information	6/10/2021 10:40:03 AM	Device...	7000	None
Information	6/10/2021 8:47:01 AM	Device...	7000	None

Event 7000, DeviceGuard

General   Details

Device Guard successfully processed the Group Policy: Virtualization Based Se
Secure Boot = On, DMA Protection = On, Virtualization Based Code Integrity
Credential Guard = Enabled, Reboot required = No, Status = 0x0.

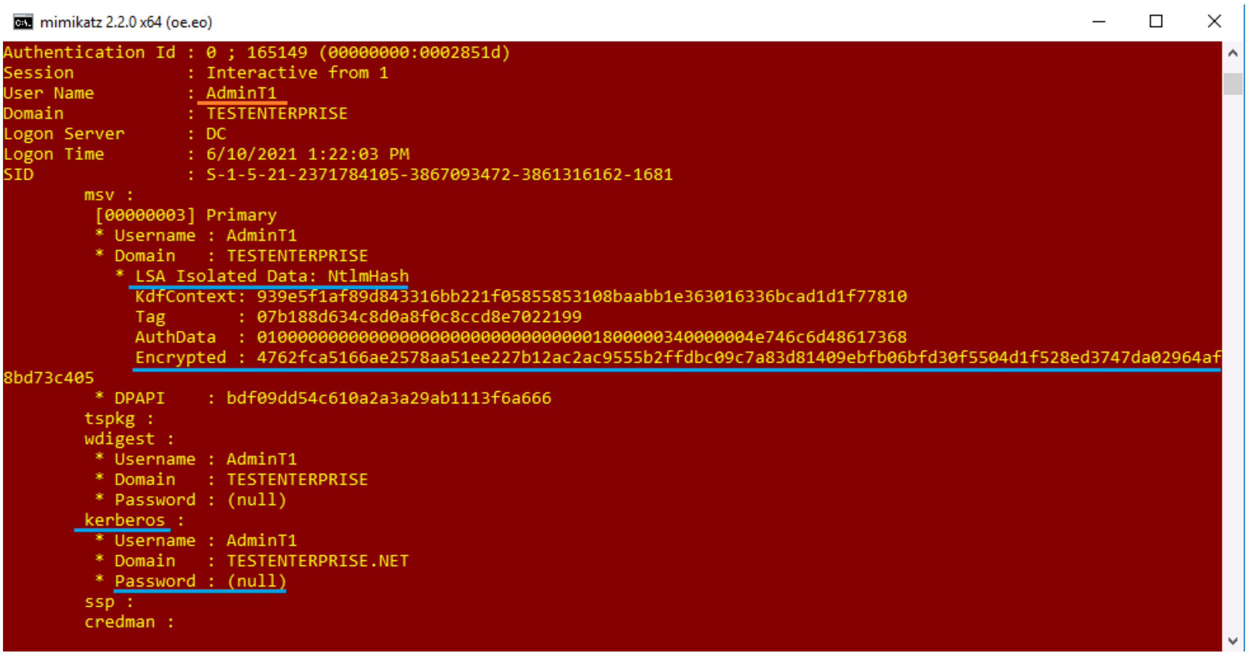
Log Name:	Microsoft-Windows-DeviceGuard/Operational		
Source:	DeviceGuard	Logged:	6/10/2021
Event ID:	7000	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Srv2.TestEN
OpCode:	Info		
More Information:	Event Log Online Help		

SYSTEM

Now I log on to SRV2 interactively as TestENTERPRISE\AdminT1, run mimikatz –

```
privilege::debug
sekurlsa::logonPasswords
```

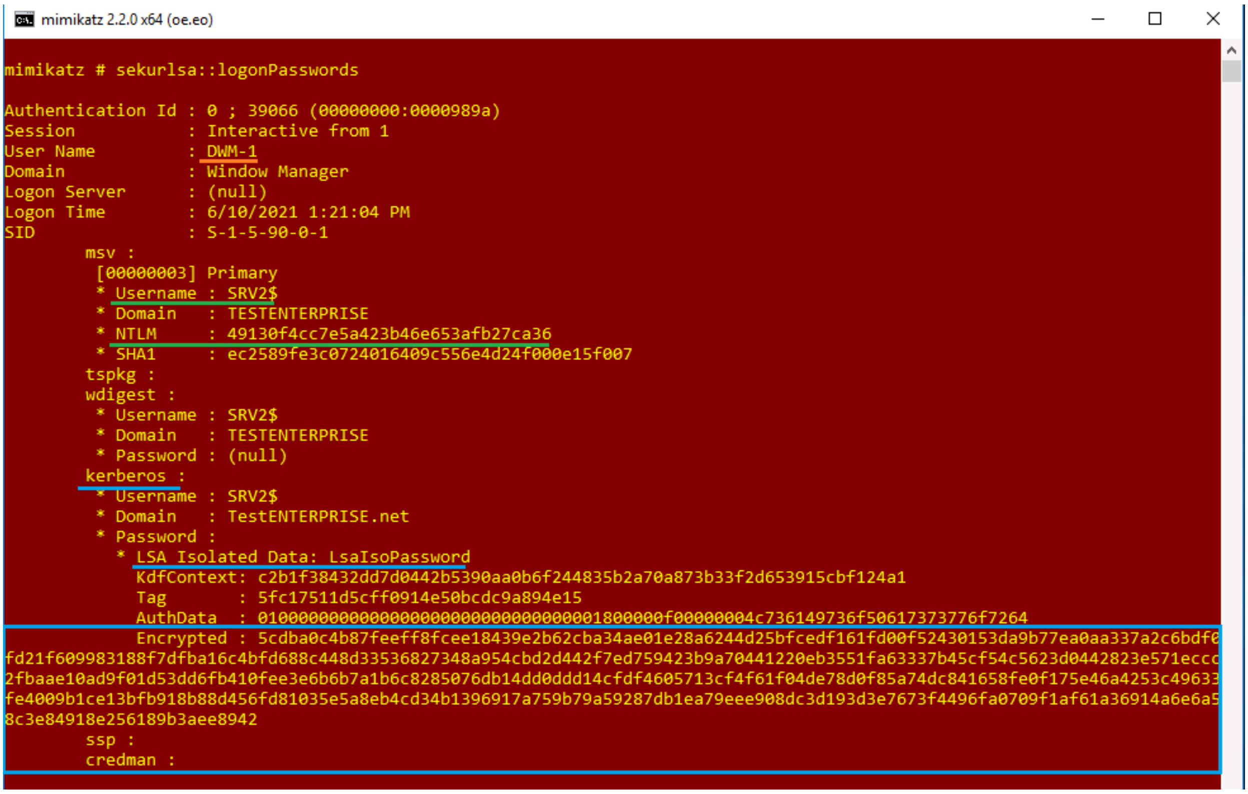
…and see information about logged on accounts:



```
Authentication Id : 0 ; 165149 (00000000:0002851d)
Session           : Interactive from 1
User Name         : AdminT1
Domain            : TESTENTERPRISE
Logon Server      : DC
Logon Time        : 6/10/2021 1:22:03 PM
SID               : S-1-5-21-2371784105-3867093472-3861316162-1681
        msv :
         [00000003] Primary
         * Username : AdminT1
         * Domain   : TESTENTERPRISE
           * LSA Isolated Data: NtlmHash
             KdfContext: 939e5f1af89d843316bb221f05855853108baabb1e363016336bcad1d1f77810
             Tag       : 07b188d634c8d0a8f0c8ccd8e7022199
             AuthData  : 0100000000000000000000000000000000180000034000000004e746c6d48617368
             Encrypted : 4762fca5166ae2578aa51ee227b12ac2ac9555b2ffdbc09c7a83d81409ebfb06bfd30f5504d1f528ed3747da02964af
8bd73c405
         * DPAPI    : bdf09dd54c610a2a3a29ab1113f6a666
        tspkg :
        wdigest :
         * Username : AdminT1
         * Domain   : TESTENTERPRISE
         * Password : (null)
        kerberos :
         * Username : AdminT1
         * Domain   : TESTENTERPRISE.NET
         * Password : (null)
        ssp :
        credman :
```

As you see there's the additional field that doesn't exist if CG is not enabled: **LSA Isolated Data**: NtlmHash. The NTLM hash is now encrypted and the Kerberos password is not displayed either (null) – so far so good.

Let's now examine the computer account – SRV2$:



```
mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 39066 (00000000:0000989a)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 6/10/2021 1:21:04 PM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : SRV2$
         * Domain   : TESTENTERPRISE
         * NTLM     : 49130f4cc7e5a423b46e653afb27ca36
         * SHA1     : ec2589fe3c0724016409c556e4d24f000e15f007
        tspkg :
        wdigest :
         * Username : SRV2$
         * Domain   : TESTENTERPRISE
         * Password : (null)
        kerberos :
         * Username : SRV2$
         * Domain   : TestENTERPRISE.net
         * Password :
           * LSA Isolated Data: LsaIsoPassword
             KdfContext: c2b1f38432dd7d0442b5390aa0b6f244835b2a70a873b33f2d653915cbf124a1
             Tag       : 5fc17511d5cff0914e50bcdc9a894e15
             AuthData  : 010000000000000000000000000000000001800000f00000004c736149736f50617373776f7264
             Encrypted : 5cdba0c4b87feeff8fcee18439e2b62cba34ae01e28a6244d25bfcedf161fd00f52430153da9b77ea0aa337a2c6bdf0
fd21f609983188f7dfba16c4bfd688c448d33536827348a954cbd2d442f7ed759423b9a70441220eb3551fa63337b45cf54c5623d0442823e571eccc
2fbaae10ad9f01d53dd6fb410fee3e6b6b7a1b6c8285076db14dd0ddd14cfdf4605713cf4f61f04de78d0f85a74dc841658fe0f175e46a4253c49633
fe4009b1ce13bfb918b88d456fd81035e5a8eb4cd34b1396917a759b79a59287db1ea79eee908dc3d193d3e7673f4496fa0709f1af61a36914a6e6a5
8c3e84918e256189b3aee8942
        ssp :
        credman :
```

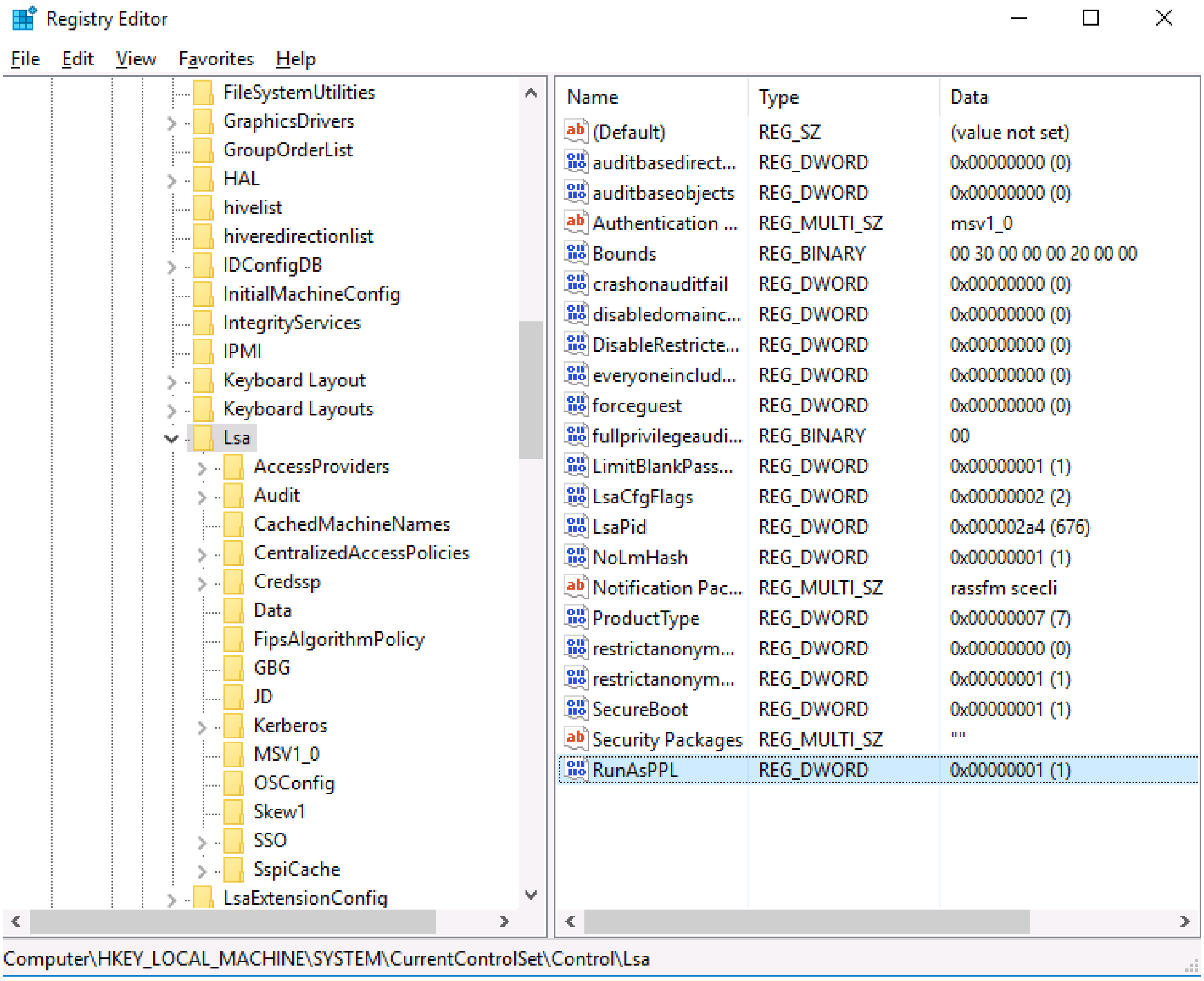
In spite of the enabled CG the NTLM hash for the SRV2$ computer account is still displayed unencrypted, although the Kerberos password field does contain the encrypted password instead of 'null' for the AdminT1 account.

As of this writing I don’t have any explanation to the difference in displaying user and computer accounts’ credentials but in any case we see that Credential Guard does work at least for user accounts.

What else can be done to further protect user credentials? Let’s enable Additional LSA protection and see!

2) Additional LSA protection

To enable the LSA protection you must add the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL – and set it to 0x0000000**1**:

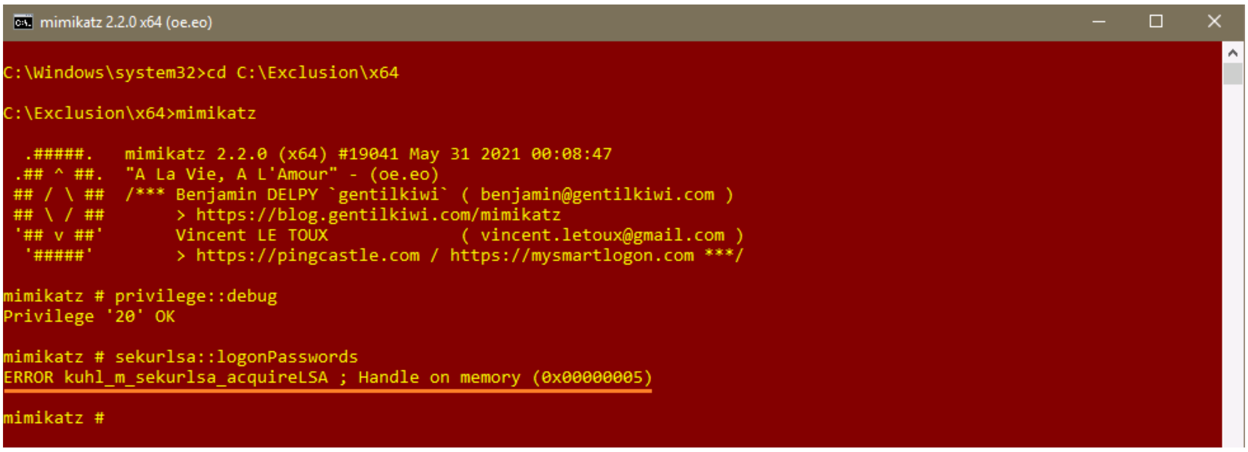


Name	Type	Data
ab (Default)	REG_SZ	(value not set)
auditbasedirect...	REG_DWORD	0x00000000 (0)
auditbaseobjects	REG_DWORD	0x00000000 (0)
ab Authentication ...	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomainc...	REG_DWORD	0x00000000 (0)
DisableRestricte...	REG_DWORD	0x00000000 (0)
everyoneinclud...	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
fullprivilegeaudi...	REG_BINARY	00
LimitBlankPass...	REG_DWORD	0x00000001 (1)
LsaCfgFlags	REG_DWORD	0x00000002 (2)
LsaPid	REG_DWORD	0x000002a4 (676)
NoLmHash	REG_DWORD	0x00000001 (1)
ab Notification Pac...	REG_MULTI_SZ	rassfm scecli
ProductType	REG_DWORD	0x00000007 (7)
restrictanonym...	REG_DWORD	0x00000000 (0)
restrictanonym...	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
ab Security Packages	REG_MULTI_SZ	""
RunAsPPL	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

It’s worth noting that prior to enabling LSA protection it’d be wise to first test this mode as described in the “*To enable the audit mode for Lsass.exe on a single computer by editing the Registry*” section of this article.

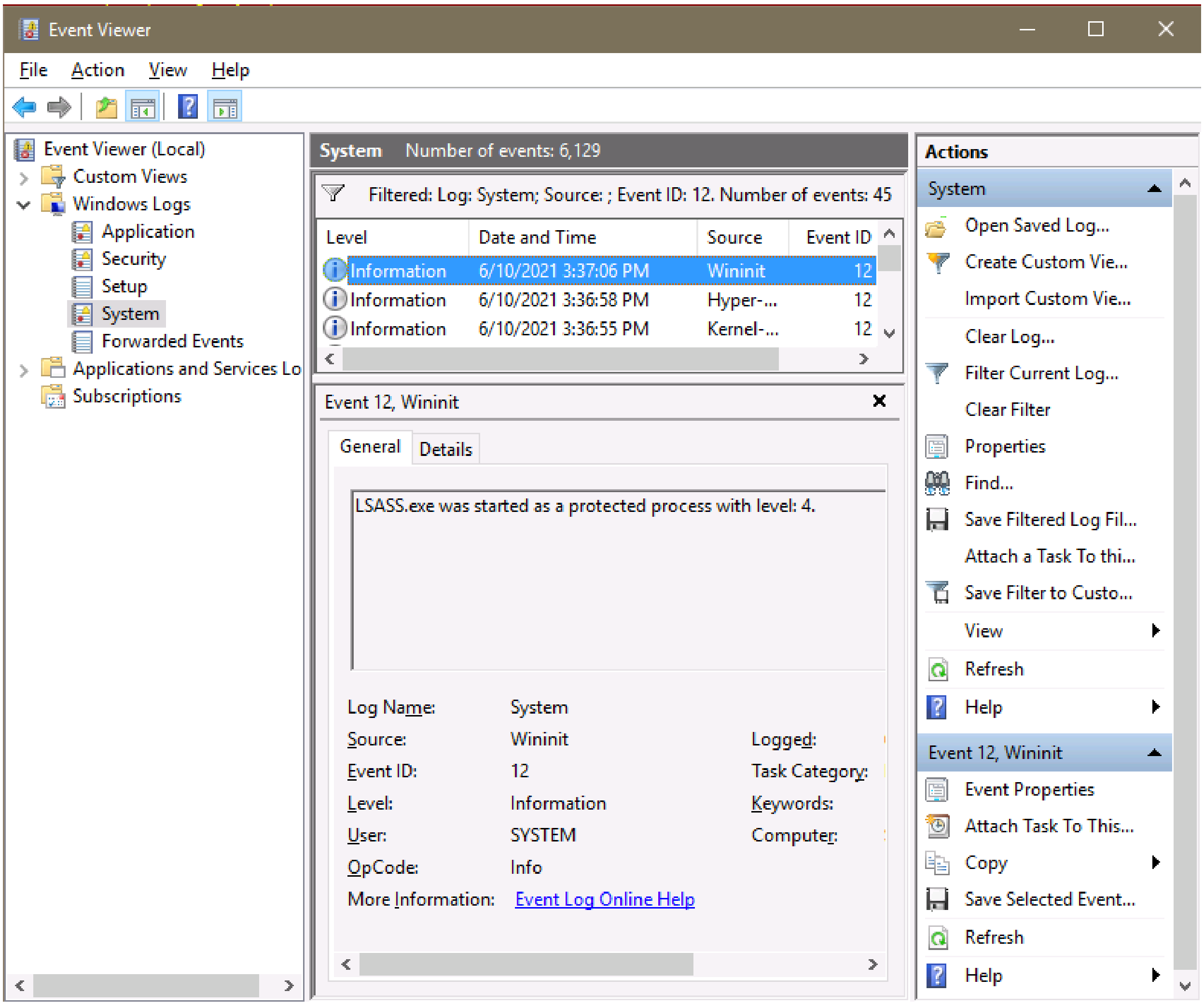
Once this mode is enabled programs like mimikatz should not be able to retrieve account credentials:



```
C:\Windows\system32>cd C:\Exclusion\x64

C:\Exclusion\x64>mimikatz

  .#####.   mimikatz 2.2.0 (x64) #19041 May 31 2021 00:08:47
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz #
```

As you see this time logonPasswords command raises the error.

Event ID 12 must be generated in the System log when the LSA process is started in protected mode:



System Number of events: 6,129

Filtered: Log: System; Source: ; Event ID: 12. Number of events: 45

Level	Date and Time	Source	Event ID
Information	6/10/2021 3:37:06 PM	Wininit	12
Information	6/10/2021 3:36:58 PM	Hyper-...	12
Information	6/10/2021 3:36:55 PM	Kernel-...	12

Event 12, Wininit

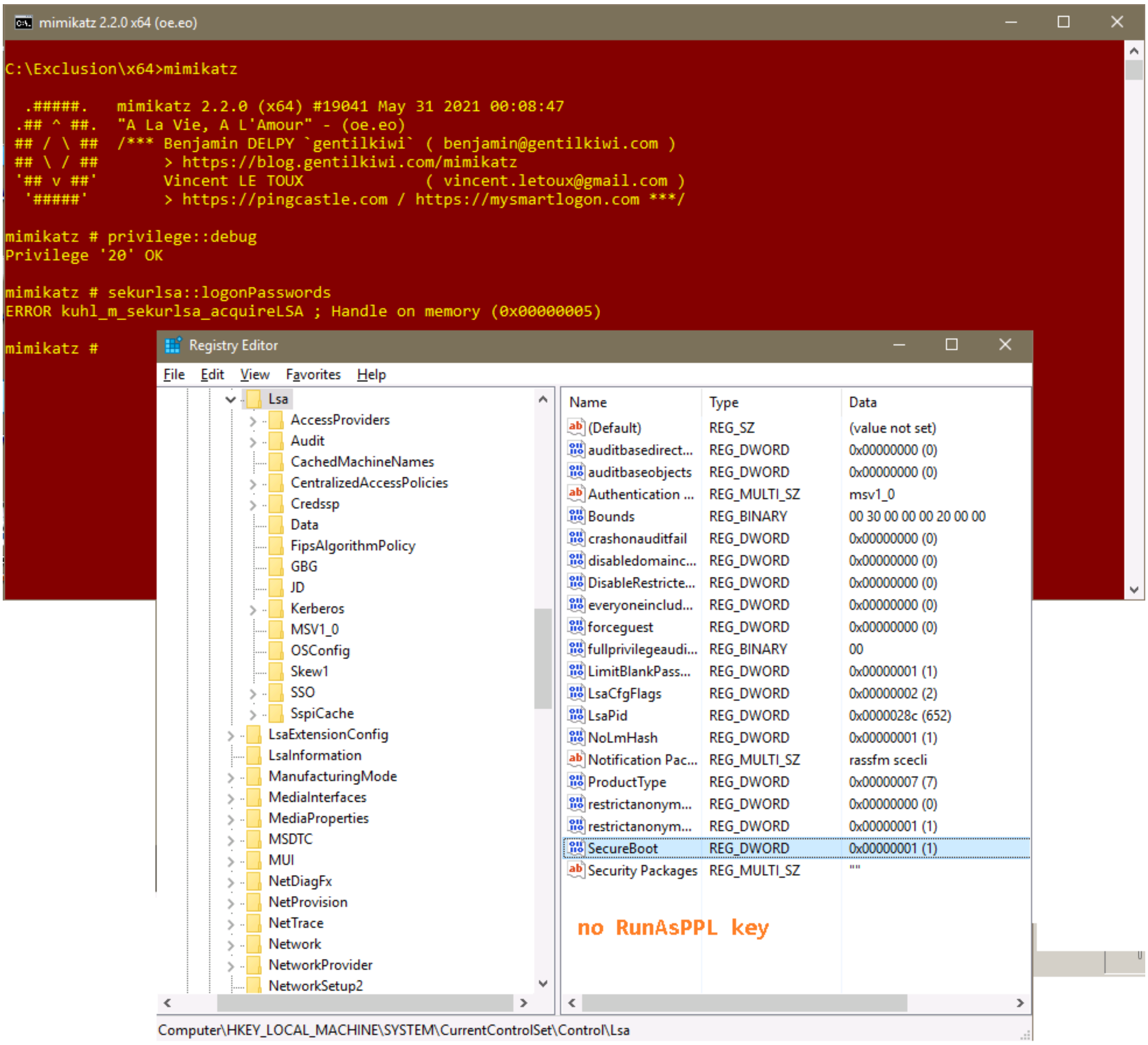
LSASS.exe was started as a protected process with level: 4.

Log Name: System
Source: Wininit
Logged:
Event ID: 12
Task Category:
Level: Information
Keywords:
User: SYSTEM
Computer:
OpCode: Info
More Information: Event Log Online Help

Now we have two Windows features that protect user accounts from stealing passwords/hashes and using them in PtH attacks. But what if, later on, an administrator would like to disable LSA protection? Please recall that the LSA protection was the second security option deployed – the first was the Credential Guard, and the CG required Secure Boot with TPM to work (more information here). But if the LSA protection is used together with Secure Boot, it's not possible to turn off LSA protection by simply deleting the RunAsPPL key from the registry:

"*When this setting is used in conjunction with Secure Boot, additional protection is achieved because disabling the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa registry key has no effect.*"

For example, if I delete the key and reboot, the LSA will keep starting in protected mode:



```
C:\Exclusion\x64>mimikatz

  .#####.   mimikatz 2.2.0 (x64) #19041 May 31 2021 00:08:47
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz #
```

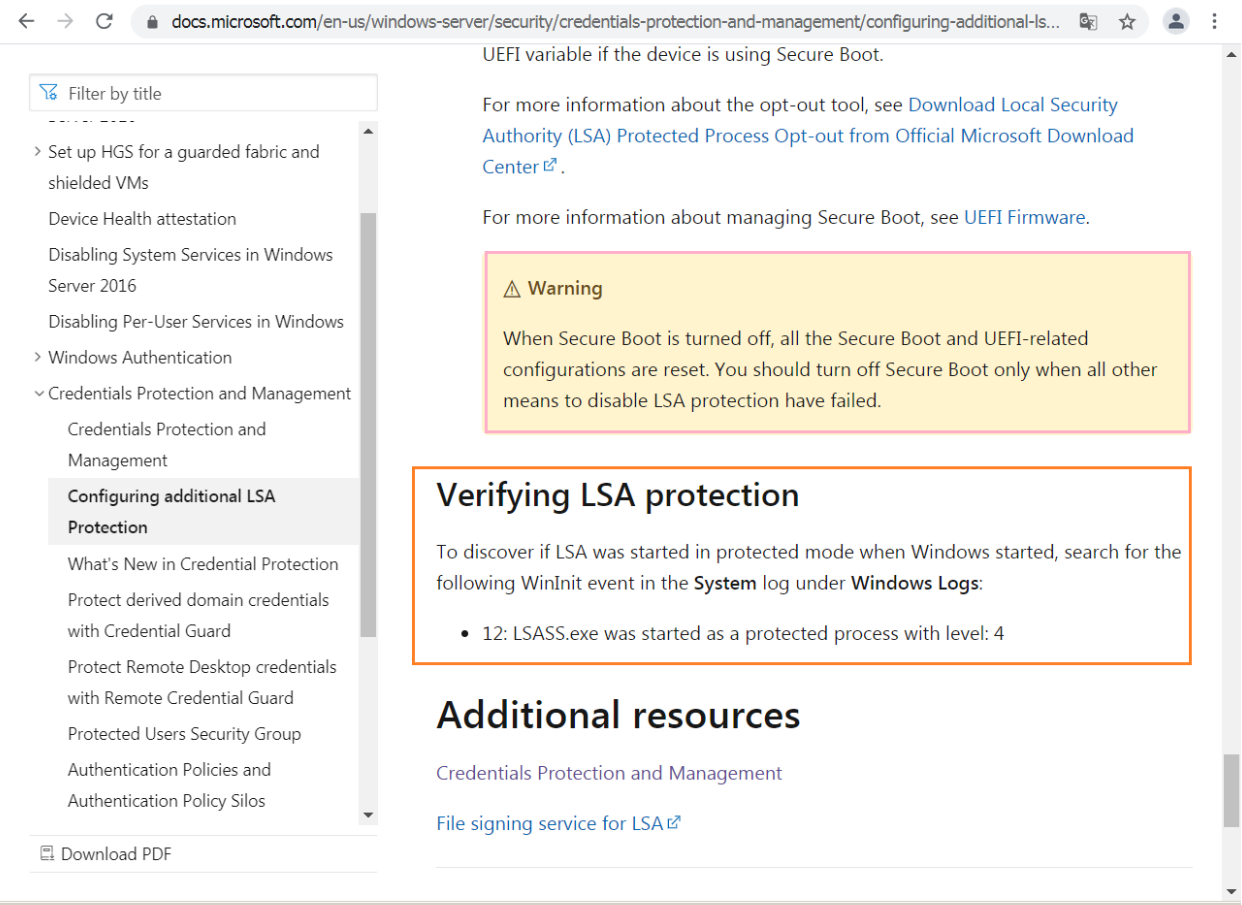
Name	Type	Data
(Default)	REG_SZ	(value not set)
auditbasedirect...	REG_DWORD	0x00000000 (0)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication ...	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomainc...	REG_DWORD	0x00000000 (0)
DisableRestricte...	REG_DWORD	0x00000000 (0)
everyoneinclud...	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
fullprivilegeaudi...	REG_BINARY	00
LimitBlankPass...	REG_DWORD	0x00000001 (1)
LsaCfgFlags	REG_DWORD	0x00000002 (2)
LsaPid	REG_DWORD	0x0000028c (652)
NoLmHash	REG_DWORD	0x00000001 (1)
Notification Pac...	REG_MULTI_SZ	rassfm scecli
ProductType	REG_DWORD	0x00000007 (7)
restrictanonym...	REG_DWORD	0x00000000 (0)
restrictanonym...	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	""

no RunAsPPL key

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

– and it's by design.

The MS article mentioned above does also say that as a last resort for disabling LSA protection you can turn off the Secure Boot (Credential Guard will be turned off either!) :



docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-ls...
Filter by title
Set up HGS for a guarded fabric and shielded VMs
Device Health attestation
Disabling System Services in Windows Server 2016
Disabling Per-User Services in Windows
Windows Authentication
Credentials Protection and Management
Credentials Protection and Management
Configuring additional LSA Protection
What's New in Credential Protection
Protect derived domain credentials with Credential Guard
Protect Remote Desktop credentials with Remote Credential Guard
Protected Users Security Group
Authentication Policies and Authentication Policy Silos
Download PDF

UEFI variable if the device is using Secure Boot.

For more information about the opt-out tool, see Download Local Security Authority (LSA) Protected Process Opt-out from Official Microsoft Download Center.

For more information about managing Secure Boot, see UEFI Firmware.

⚠ **Warning**

When Secure Boot is turned off, all the Secure Boot and UEFI-related configurations are reset. You should turn off Secure Boot only when all other means to disable LSA protection have failed.

Verifying LSA protection

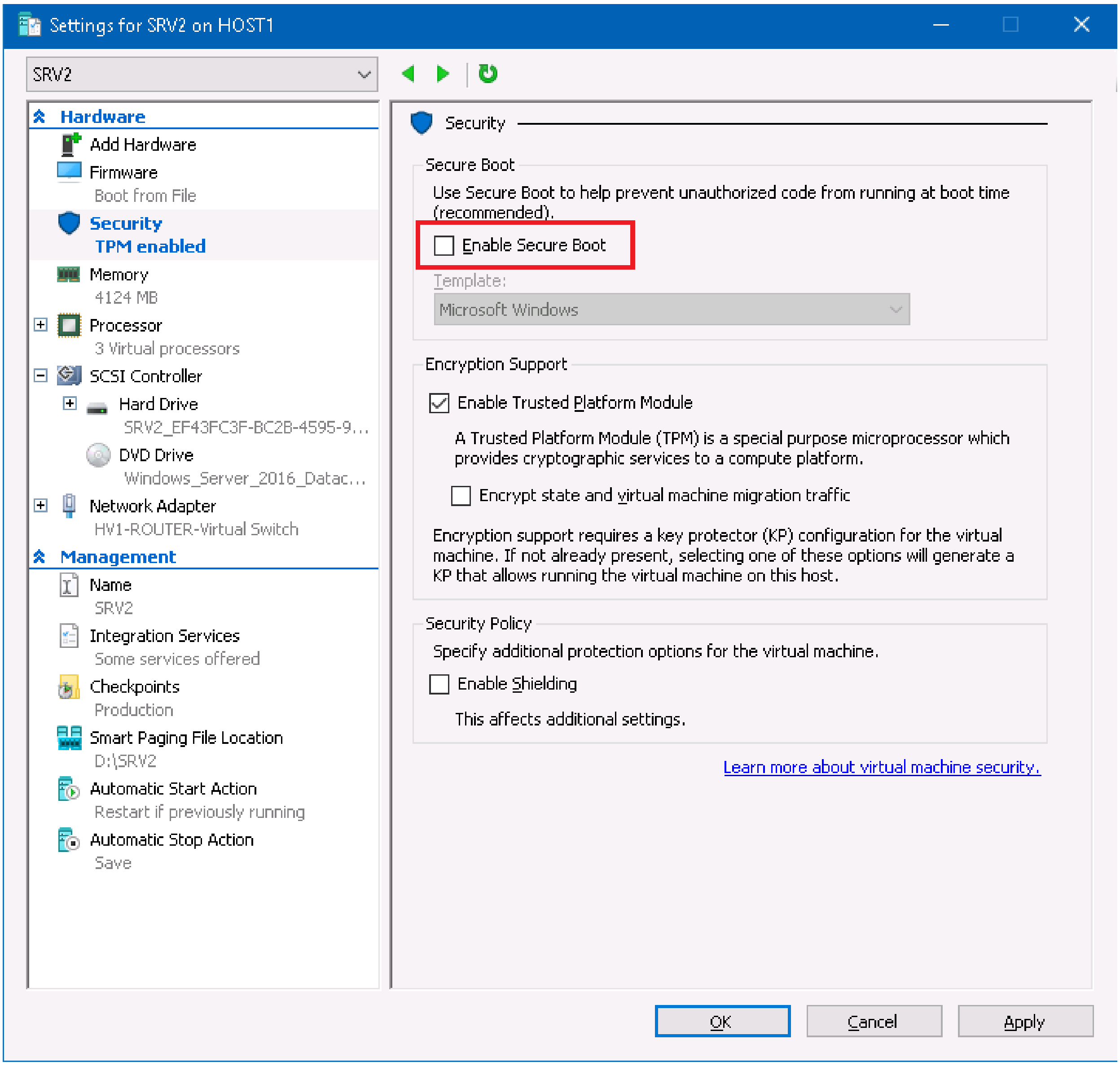
To discover if LSA was started in protected mode when Windows started, search for the following WinInit event in the **System** log under **Windows Logs**:

- 12: LSASS.exe was started as a protected process with level: 4

Additional resources

Credentials Protection and Management

File signing service for LSA



Settings for SRV2 on HOST1

SRV2

Hardware
- Add Hardware
- Firmware
  Boot from File
- Security
  TPM enabled
- Memory
  4124 MB
- Processor
  3 Virtual processors
- SCSI Controller
  - Hard Drive
    SRV2_EF43FC3F-BC2B-4595-9...
  - DVD Drive
    Windows_Server_2016_Datac...
- Network Adapter
  HV1-ROUTER-Virtual Switch

Management
- Name
  SRV2
- Integration Services
  Some services offered
- Checkpoints
  Production
- Smart Paging File Location
  D:\SRV2
- Automatic Start Action
  Restart if previously running
- Automatic Stop Action
  Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

□ Enable Secure Boot

Template:
Microsoft Windows

Encryption Support

☑ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

□ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

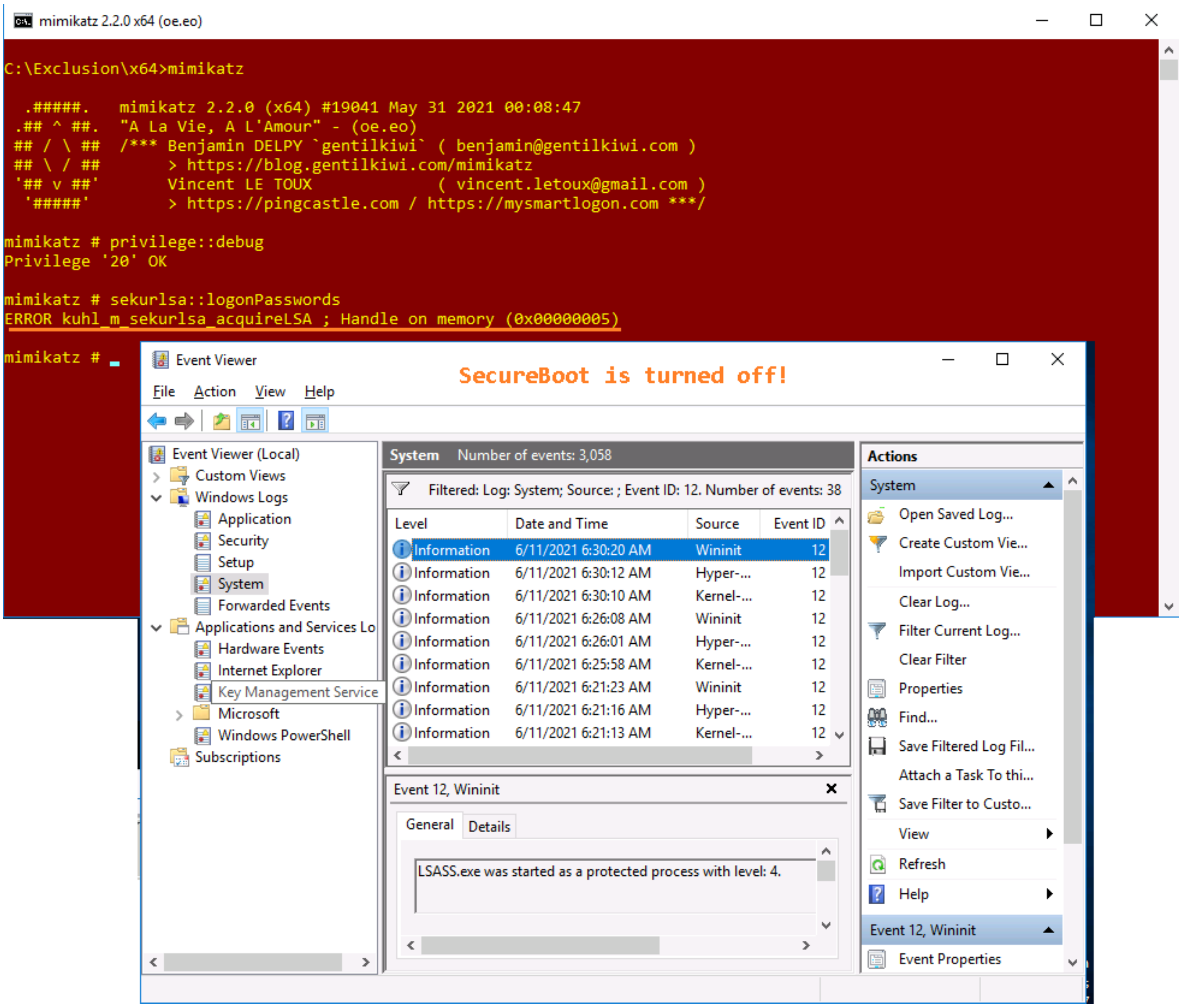
Security Policy

Specify additional protection options for the virtual machine.

□ Enable Shielding

This affects additional settings.

Learn more about virtual machine security.



```
C:\Exclusion\x64>mimikatz

  .#####.   mimikatz 2.2.0 (x64) #19041 May 31 2021 00:08:47
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz # _
```

SecureBoot is turned off!

System   Number of events: 3,058

Filtered: Log: System; Source: ; Event ID: 12. Number of events: 38

Level	Date and Time	Source	Event ID
Information	6/11/2021 6:30:20 AM	Wininit	12
Information	6/11/2021 6:30:12 AM	Hyper-...	12
Information	6/11/2021 6:30:10 AM	Kernel-...	12
Information	6/11/2021 6:26:08 AM	Wininit	12
Information	6/11/2021 6:26:01 AM	Hyper-...	12
Information	6/11/2021 6:25:58 AM	Kernel-...	12
Information	6/11/2021 6:21:23 AM	Wininit	12
Information	6/11/2021 6:21:16 AM	Hyper-...	12
Information	6/11/2021 6:21:13 AM	Kernel-...	12

Event 12, Wininit

LSASS.exe was started as a protected process with level: 4.

As far as I understand it's not by design and the Local Security Authority (LSA) Protected Process Opt-out tool will be the only way to disable LSA protection. Let's try out and see if it works!

Here's MS instructions for using the tool:

(The Local Security Authority (LSA) Protected Process Opt-out tool's Install instructions section contains the strange wording: ***Disable the registry key*** *(GP for the registry key, if applicable) and wait for the change to propagate to clients.* – you can't disable the key but should simply delete it instead: the MS's documentation clearly states "*Delete the following value from the registry key: "RunAsPPL"=dword:00000001.*")

1) Download the LSAPPLConfig files from the download center and store the efi tool that corresponds to your machines architecture on a local disk, for example at C: drive's root

2) Open a Command Prompt as an Administrator and run the following commands to bootstrap the tool.

mountvol X: /s

3) **copy C:\LSAPPLConfig.efi X:\EFI\Microsoft\Boot\LSAPPLConfig.efi /Y**

4) **bcdedit /create {0cb3b571-2f2e-4343-a879-d86a476d7215} /d “DebugTool” /application osloader**

5) **bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} path “\EFI\Microsoft\Boot\LSAPPLConfig.efi”**

6) **bcdedit /set {bootmgr} bootsequence {0cb3b571-2f2e-4343-a879-d86a476d7215}**

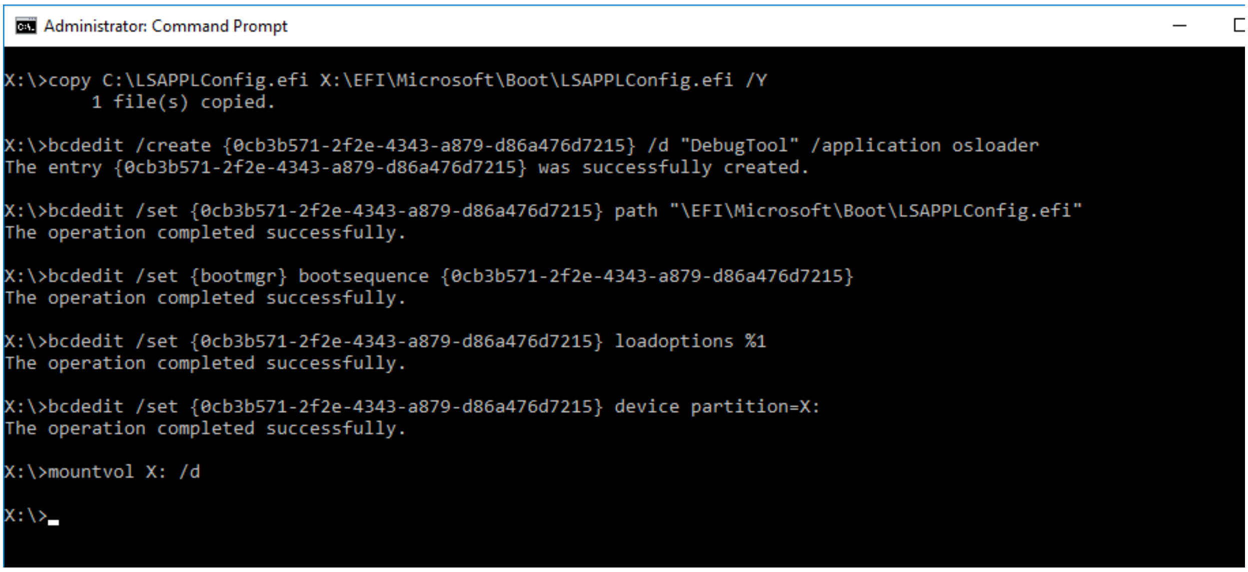
7) **bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} loadoptions %1**

8) **bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} device partition=X:**

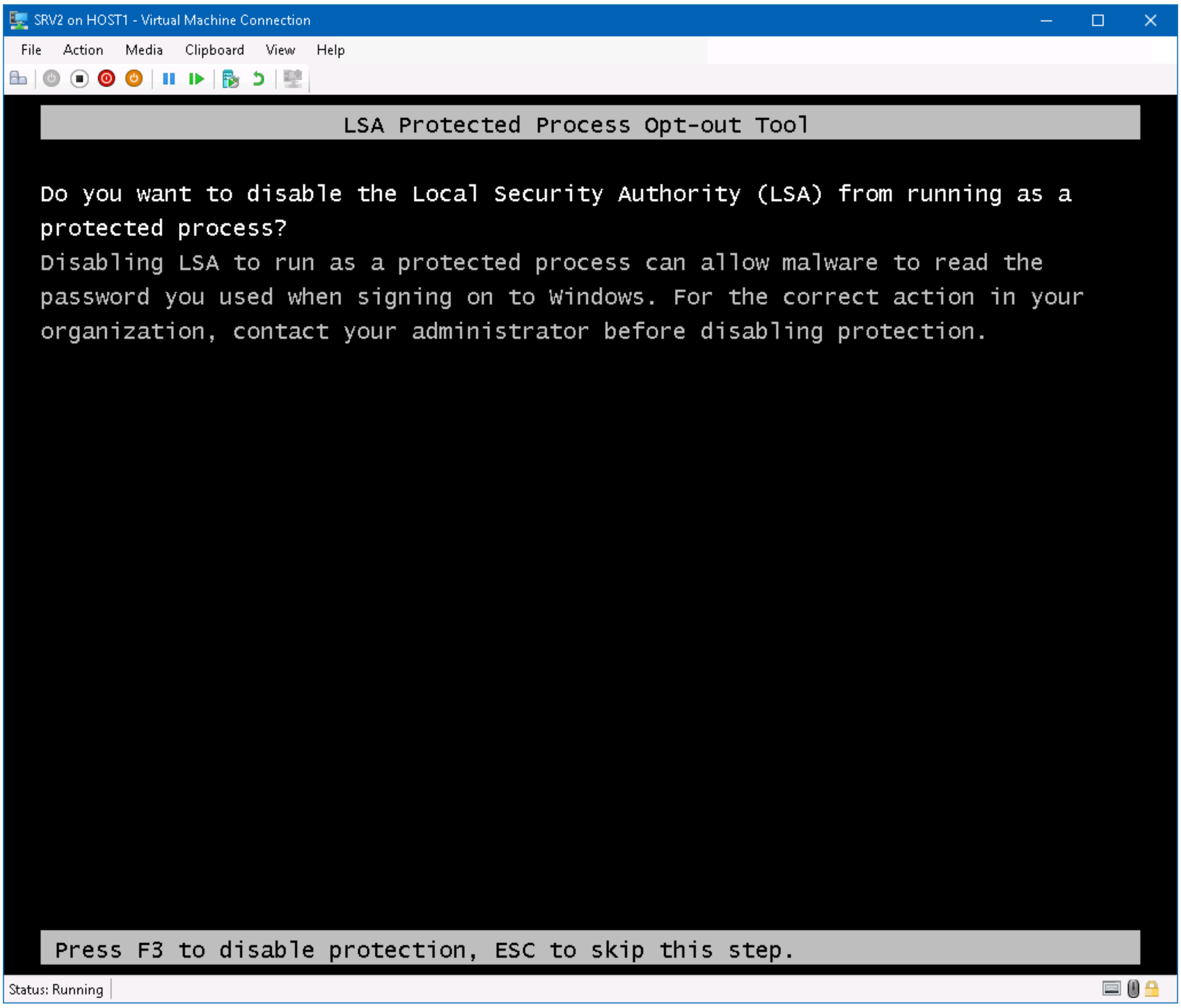
9) **mountvol X: /d**

10) Reboot the machine, the EFI application will start after the reboot. Accept the change to disable LSA’s protection. Windows will continue to launch and LSA protection will be disabled.

11) Verify LSA protection is disabled, search for the following WinInit event in the System log under Windows Logs, and ensure that it does not exist: 12: LSASS.exe was started as a protected process with level: 4

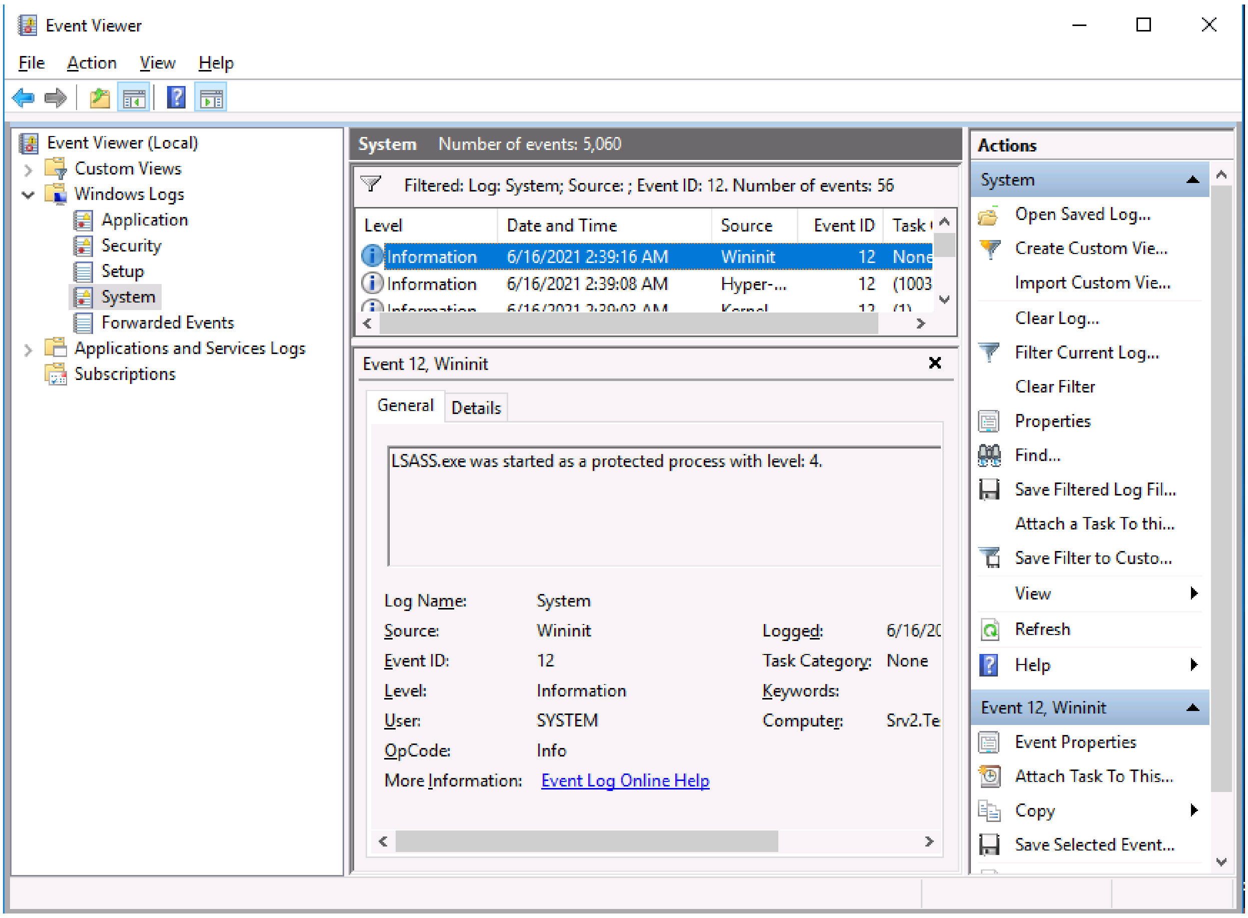


```
X:\>copy C:\LSAPPLConfig.efi X:\EFI\Microsoft\Boot\LSAPPLConfig.efi /Y
        1 file(s) copied.

X:\>bcdedit /create {0cb3b571-2f2e-4343-a879-d86a476d7215} /d "DebugTool" /application osloader
The entry {0cb3b571-2f2e-4343-a879-d86a476d7215} was successfully created.

X:\>bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} path "\EFI\Microsoft\Boot\LSAPPLConfig.efi"
The operation completed successfully.

X:\>bcdedit /set {bootmgr} bootsequence {0cb3b571-2f2e-4343-a879-d86a476d7215}
The operation completed successfully.

X:\>bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} loadoptions %1
The operation completed successfully.

X:\>bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} device partition=X:
The operation completed successfully.

X:\>mountvol X: /d

X:\>_
```


SRV2 on HOST1 - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

```
LSA Protected Process Opt-out Tool

Do you want to disable the Local Security Authority (LSA) from running as a
protected process?
Disabling LSA to run as a protected process can allow malware to read the
password you used when signing on to Windows. For the correct action in your
organization, contact your administrator before disabling protection.

Press F3 to disable protection, ESC to skip this step.
```

While I was taking the screenshot above the computer proceeded to boot as if ESC had been selected and LSA was running again:



System Number of events: 5,060

Filtered: Log: System; Source: ; Event ID: 12. Number of events: 56

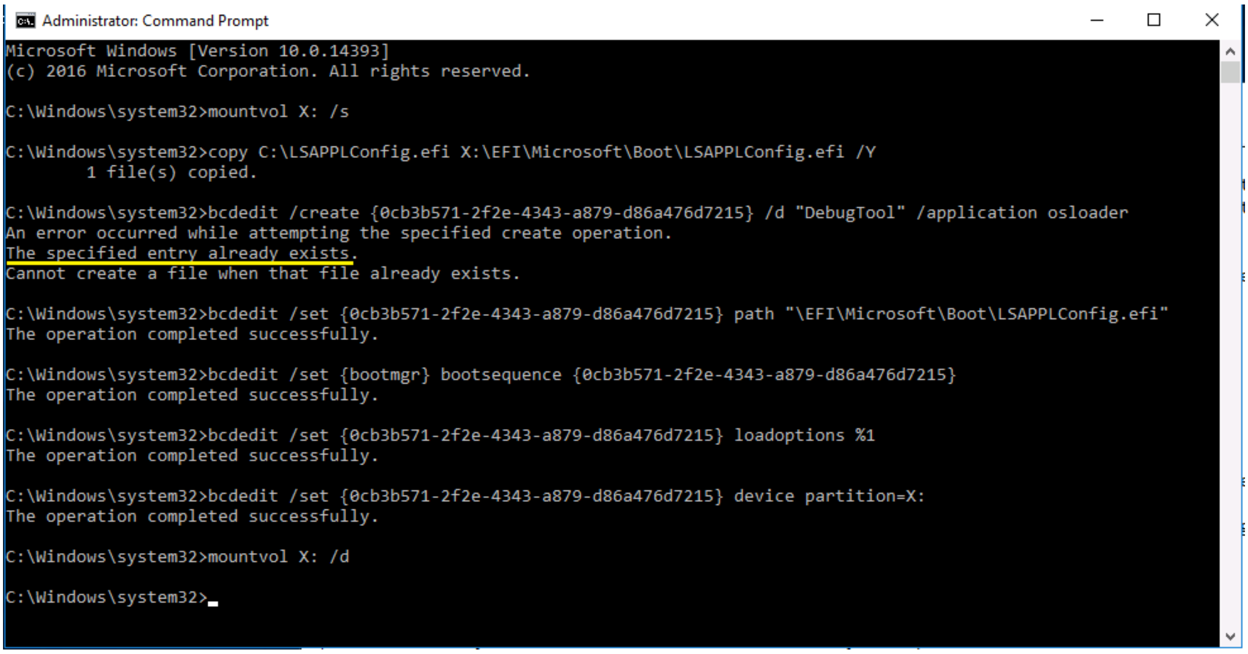
Level	Date and Time	Source	Event ID	Task (
Information	6/16/2021 2:39:16 AM	Wininit	12	None
Information	6/16/2021 2:39:08 AM	Hyper-...	12	(1003
Information	6/16/2021 2:39:03 AM	Kernel	12	(1)

Event 12, Wininit

LSASS.exe was started as a protected process with level: 4.

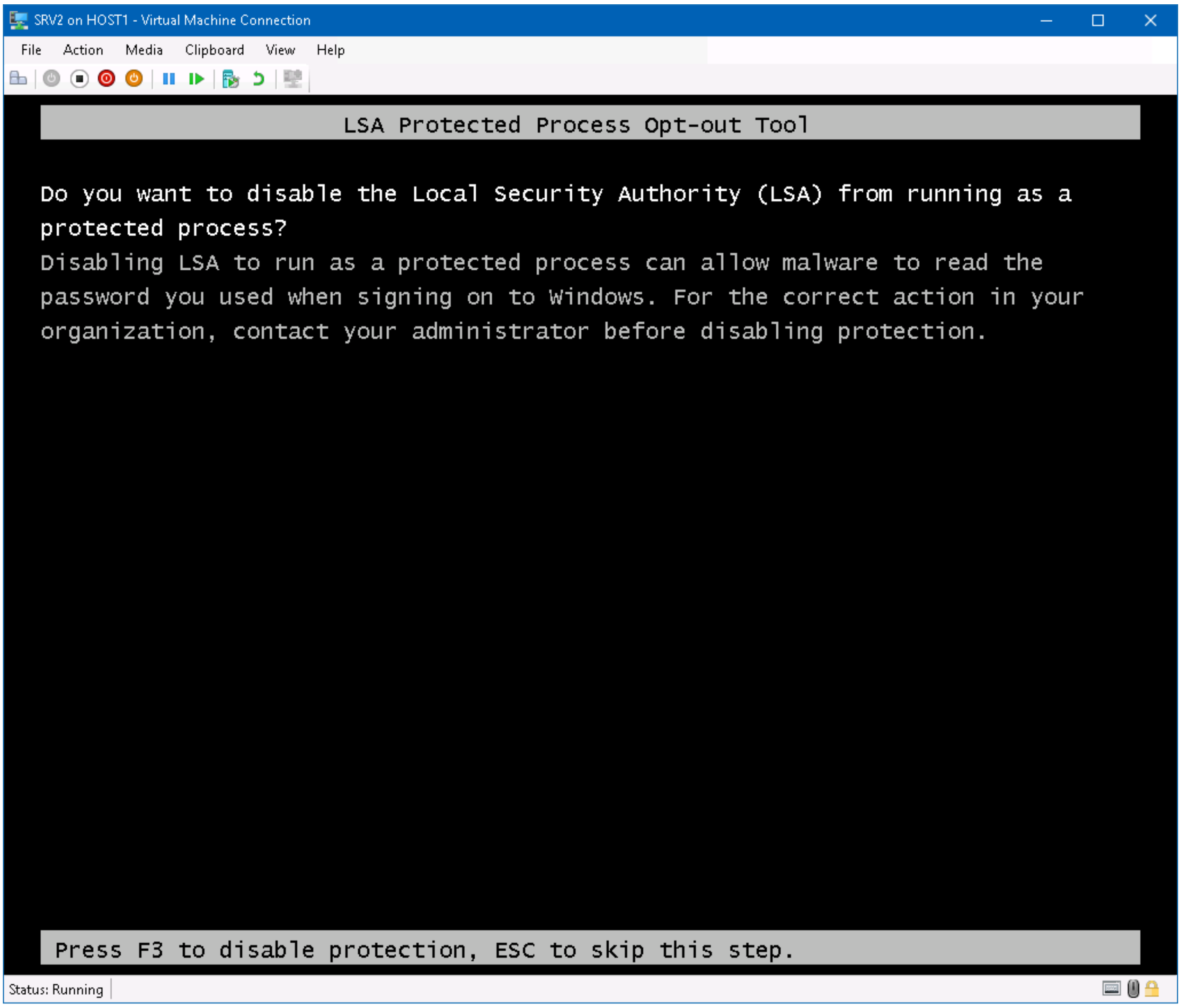
Log Name: System
Source: Wininit
Logged: 6/16/20
Event ID: 12
Task Category: None
Level: Information
Keywords:
User: SYSTEM
Computer: Srv2.Te
OpCode: Info
More Information: Event Log Online Help

It means the whole process must be started from scratch – (subsequent reboots will not invoke the tool once again!)



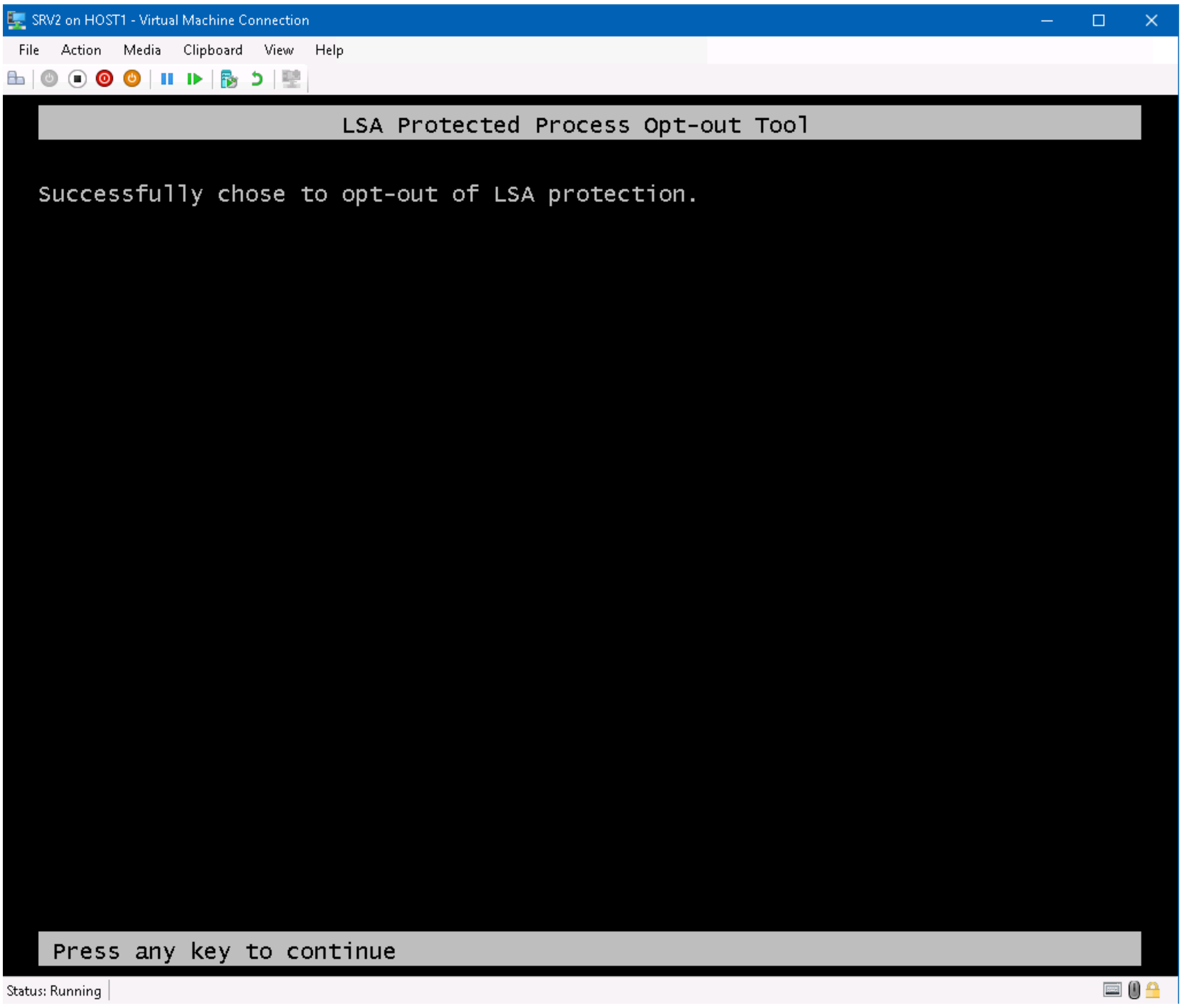
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>mountvol X: /s

C:\Windows\system32>copy C:\LSAPPLConfig.efi X:\EFI\Microsoft\Boot\LSAPPLConfig.efi /Y
        1 file(s) copied.

C:\Windows\system32>bcdedit /create {0cb3b571-2f2e-4343-a879-d86a476d7215} /d "DebugTool" /application osloader
An error occurred while attempting the specified create operation.
The specified entry already exists.
Cannot create a file when that file already exists.

C:\Windows\system32>bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} path "\EFI\Microsoft\Boot\LSAPPLConfig.efi"
The operation completed successfully.

C:\Windows\system32>bcdedit /set {bootmgr} bootsequence {0cb3b571-2f2e-4343-a879-d86a476d7215}
The operation completed successfully.

C:\Windows\system32>bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} loadoptions %1
The operation completed successfully.

C:\Windows\system32>bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} device partition=X:
The operation completed successfully.

C:\Windows\system32>mountvol X: /d

C:\Windows\system32>_
```

Please note that you should't issue the bcedit /create … command for the second time – this entry was created during the first run.



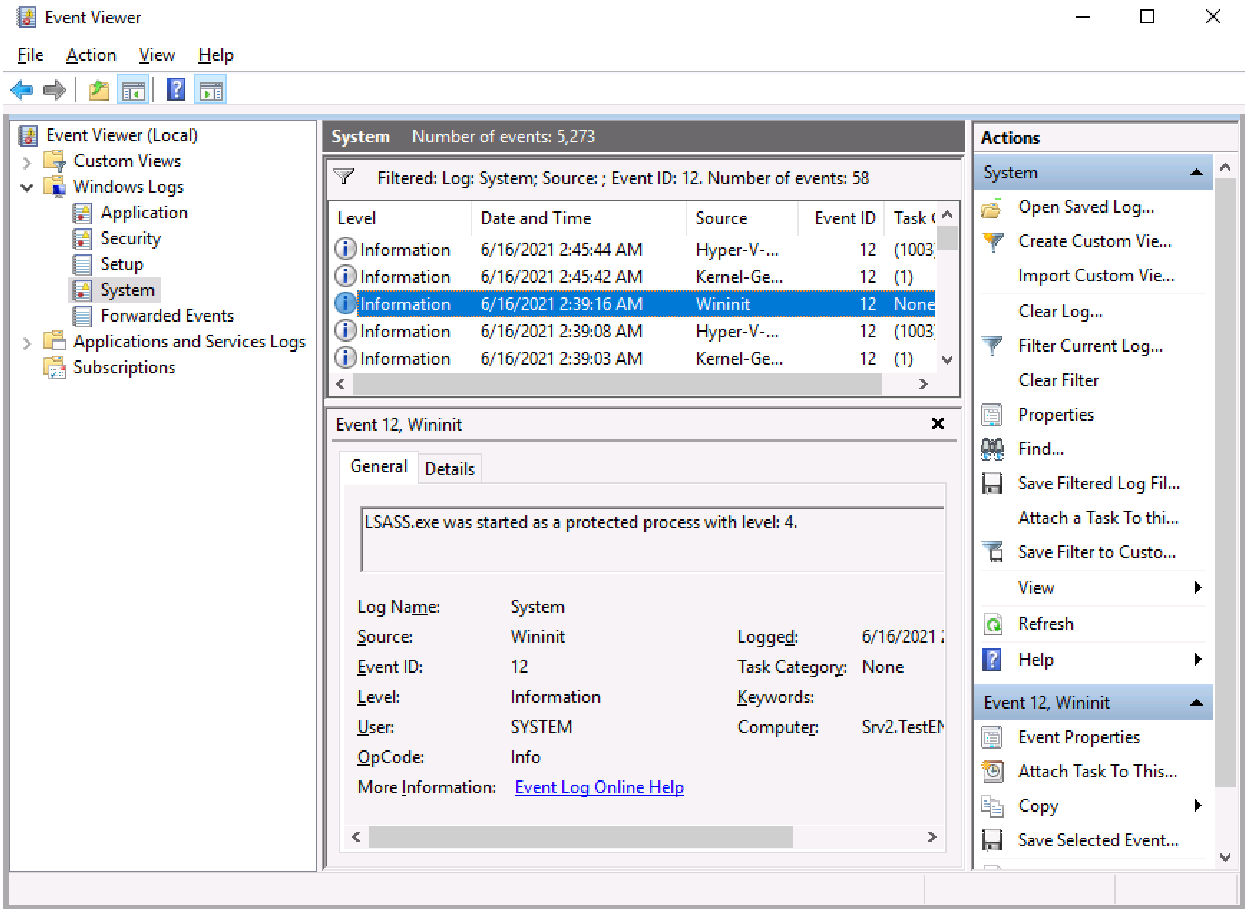
```
                    LSA Protected Process Opt-out Tool

Do you want to disable the Local Security Authority (LSA) from running as a
protected process?
Disabling LSA to run as a protected process can allow malware to read the
password you used when signing on to Windows. For the correct action in your
organization, contact your administrator before disabling protection.

 Press F3 to disable protection, ESC to skip this step.
```

After pressing **F3**:



```
                          LSA Protected Process Opt-out Tool

Successfully chose to opt-out of LSA protection.

 Press any key to continue
```

Checking the LSASS process:



System Number of events: 5,273

Filtered: Log: System; Source: ; Event ID: 12. Number of events: 58

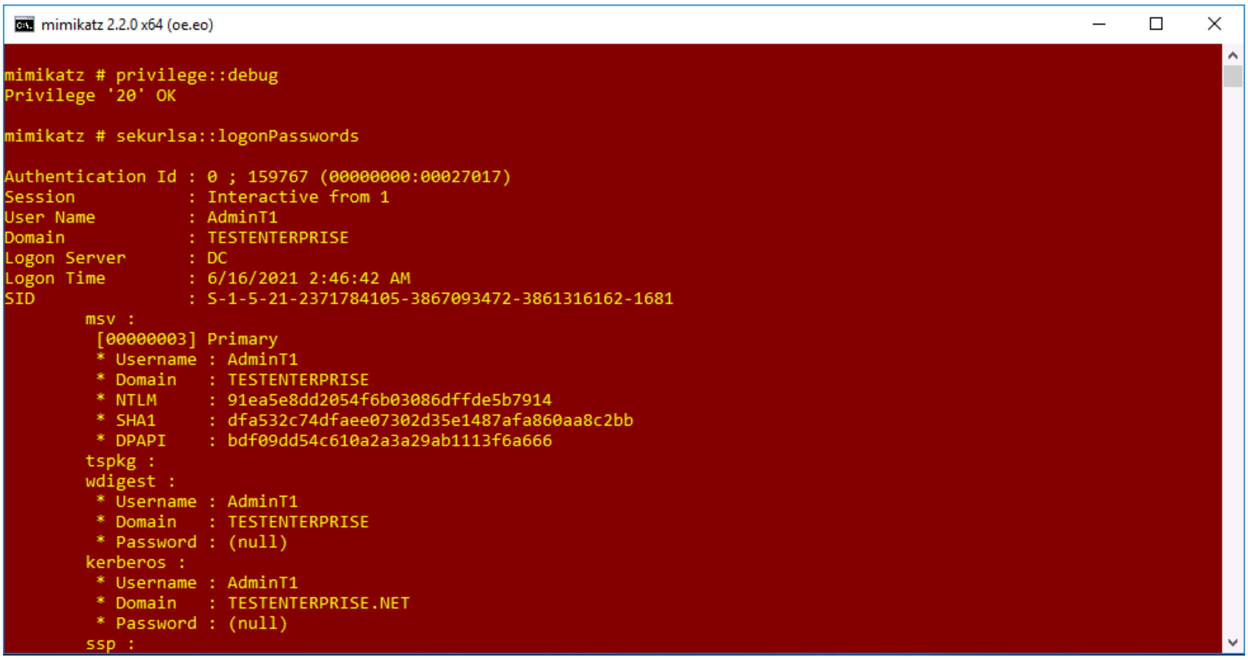
Level	Date and Time	Source	Event ID	Task (
Information	6/16/2021 2:45:44 AM	Hyper-V-...	12	(1003
Information	6/16/2021 2:45:42 AM	Kernel-Ge...	12	(1)
Information	6/16/2021 2:39:16 AM	Wininit	12	None
Information	6/16/2021 2:39:08 AM	Hyper-V-...	12	(1003
Information	6/16/2021 2:39:03 AM	Kernel-Ge...	12	(1)

Event 12, Wininit

LSASS.exe was started as a protected process with level: 4.

Log Name: System
Source: Wininit
Logged: 6/16/2021 2
Event ID: 12
Task Category: None
Level: Information
Keywords:
User: SYSTEM
Computer: Srv2.TestEN
OpCode: Info
More Information: Event Log Online Help

– there's no new event id 12 so now LSASS process must be running in non-protected mode:

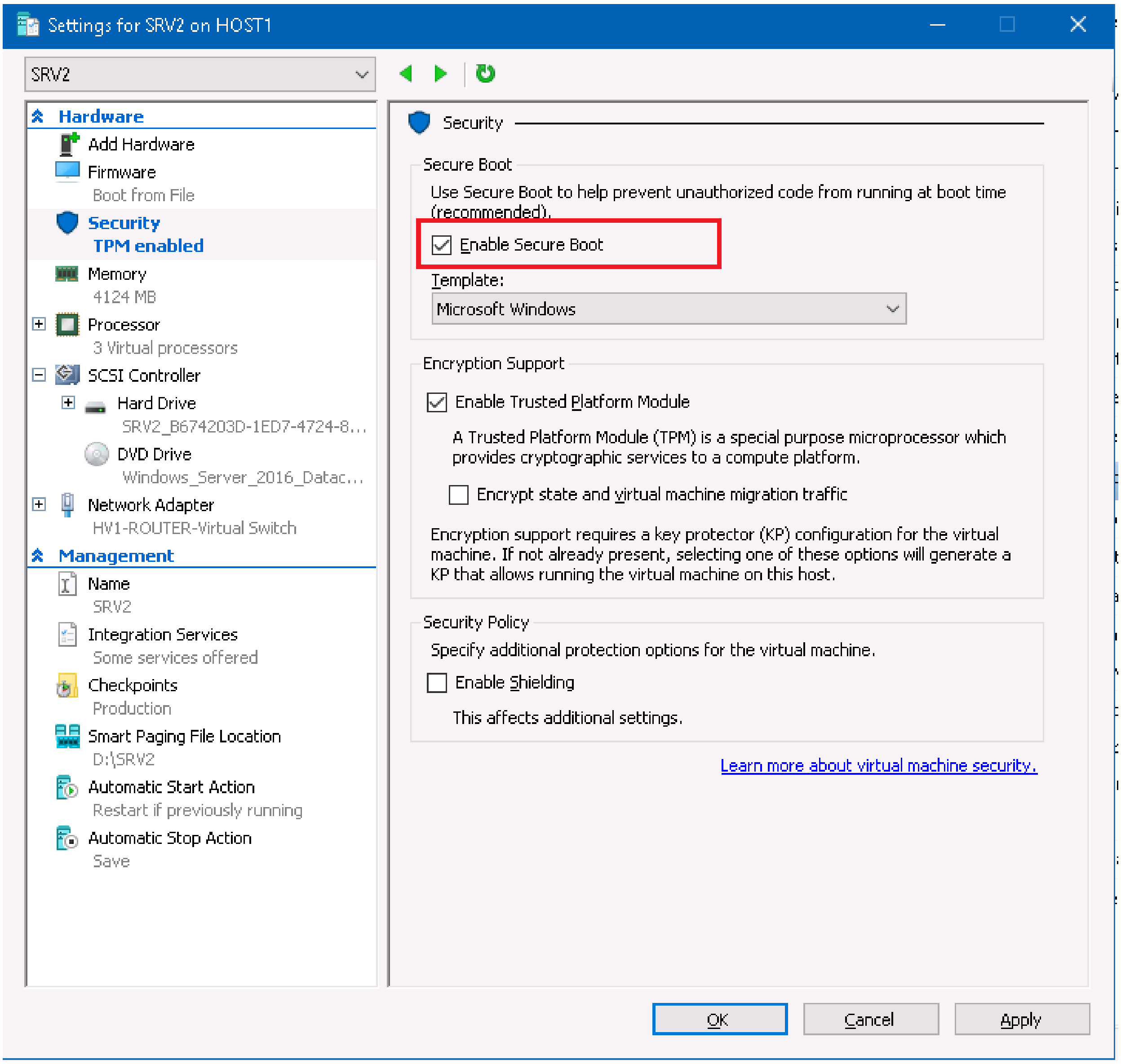


```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 159767 (00000000:00027017)
Session           : Interactive from 1
User Name         : AdminT1
Domain            : TESTENTERPRISE
Logon Server      : DC
Logon Time        : 6/16/2021 2:46:42 AM
SID               : S-1-5-21-2371784105-3867093472-3861316162-1681
        msv :
         [00000003] Primary
         * Username : AdminT1
         * Domain   : TESTENTERPRISE
         * NTLM     : 91ea5e8dd2054f6b03086dffde5b7914
         * SHA1     : dfa532c74dfaee07302d35e1487afa860aa8c2bb
         * DPAPI    : bdf09dd54c610a2a3a29ab1113f6a666
        tspkg :
        wdigest :
         * Username : AdminT1
         * Domain   : TESTENTERPRISE
         * Password : (null)
        kerberos :
         * Username : AdminT1
         * Domain   : TESTENTERPRISE.NET
         * Password : (null)
        ssp :
```

Yes, the LSA protection is turned off (there's non-ecnrypted NTLM hash here because Secure Boot is turned off either)!

As all other security settings were deployed by means of GPO, the Additional LSA protection can also be enabled (but not disabled if used with Secure Boot – as we've just seen!!!) in the respective group policy object.

As I need Credental Guard working Secure Boot must be enabled before applying GPO (theoretically LSA protection can be turned off by deleting the RunAsPPL registry key if Secure Boot is NOT enabled!):



Add Hardware
Firmware
Boot from File
Security
TPM enabled
Memory
4124 MB
Processor
3 Virtual processors
SCSI Controller
Hard Drive
SRV2_B674203D-1ED7-4724-8...
DVD Drive
Windows_Server_2016_Datac...
Network Adapter
HV1-ROUTER-Virtual Switch
Name
SRV2
Integration Services
Some services offered
Checkpoints
Production
Smart Paging File Location
D:\SRV2
Automatic Start Action
Restart if previously running
Automatic Stop Action
Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

☑ Enable Secure Boot

Template:
Microsoft Windows

Encryption Support

☑ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

☐ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

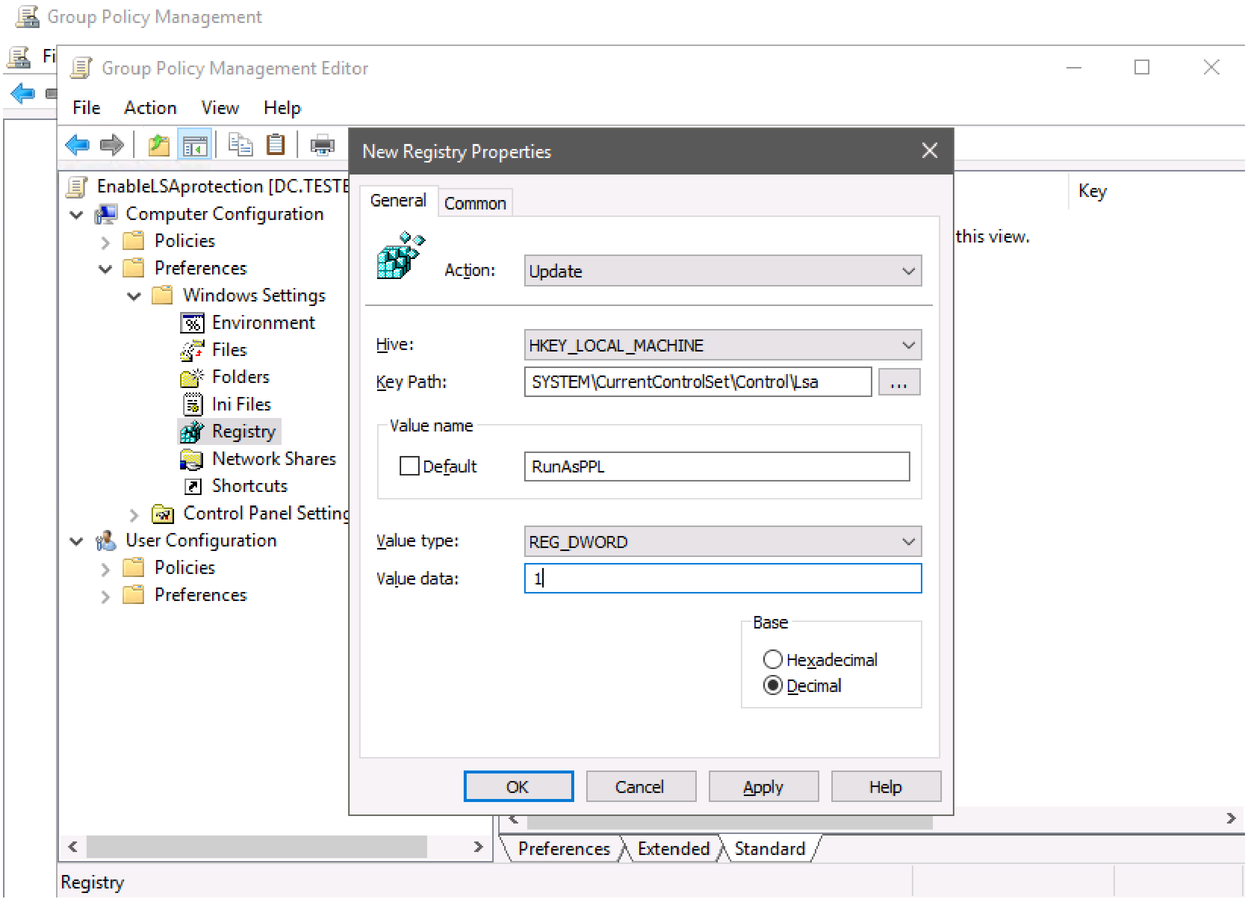
Security Policy

Specify additional protection options for the virtual machine.

☐ Enable Shielding

This affects additional settings.

Learn more about virtual machine security.



New Registry Properties

General | Common

Action: Update

Hive: HKEY_LOCAL_MACHINE

Key Path: SYSTEM\CurrentControlSet\Control\Lsa

Value name

□ Default RunAsPPL

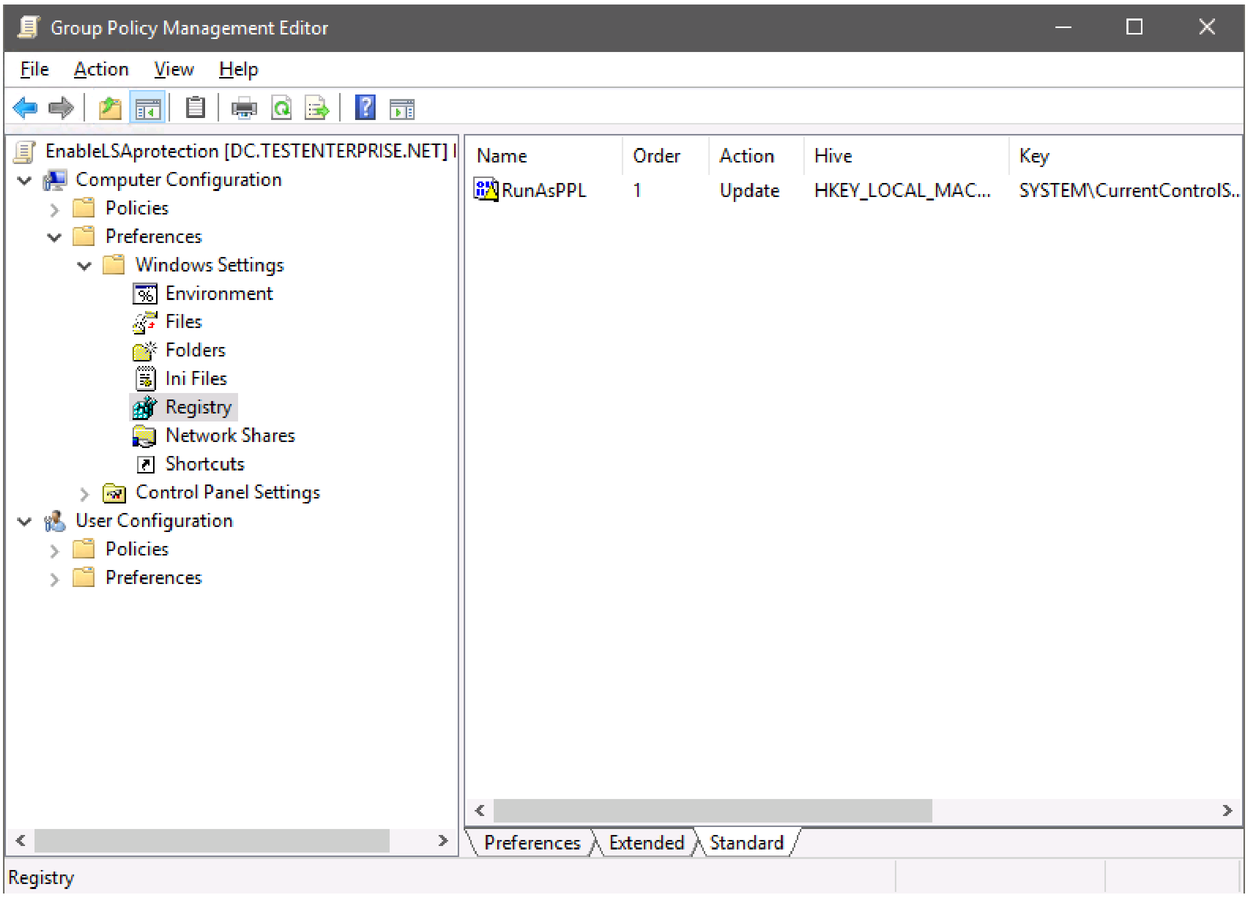
Value type: REG_DWORD

Value data: 1

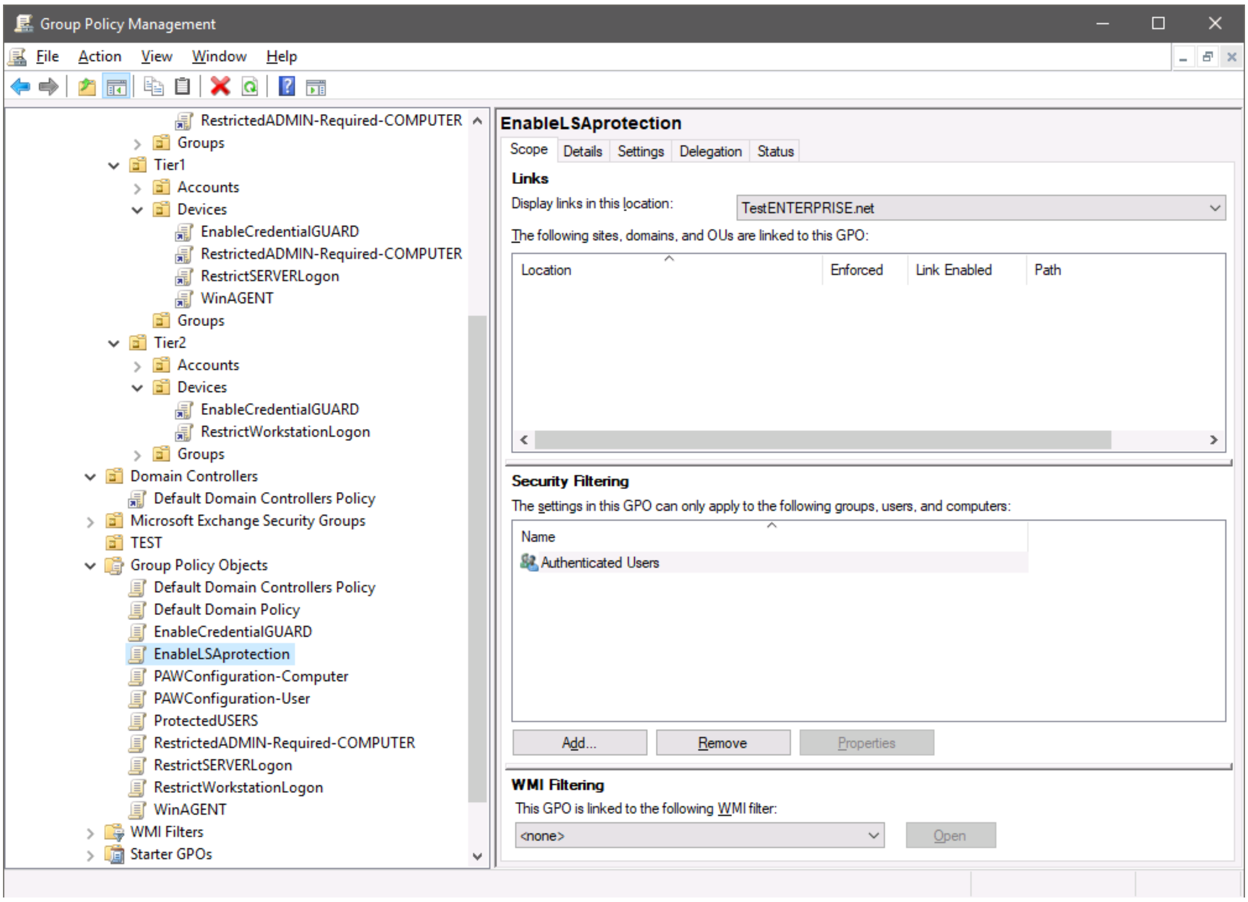
Base

○ Hexadecimal

● Decimal



Name	Order	Action	Hive	Key
RunAsPPL	1	Update	HKEY_LOCAL_MAC...	SYSTEM\CurrentControlS...



Group Policy Management

- RestrictedADMIN-Required-COMPUTER
- Groups
- Tier1
  - Accounts
  - Devices
    - EnableCredentialGUARD
    - RestrictedADMIN-Required-COMPUTER
    - RestrictSERVERLogon
    - WinAGENT
  - Groups
- Tier2
  - Accounts
  - Devices
    - EnableCredentialGUARD
    - RestrictWorkstationLogon
  - Groups
- Domain Controllers
  - Default Domain Controllers Policy
- Microsoft Exchange Security Groups
- TEST
- Group Policy Objects
  - Default Domain Controllers Policy
  - Default Domain Policy
  - EnableCredentialGUARD
  - EnableLSAprotection
  - PAWConfiguration-Computer
  - PAWConfiguration-User
  - ProtectedUSERS
  - RestrictedADMIN-Required-COMPUTER
  - RestrictSERVERLogon
  - RestrictWorkstationLogon
  - WinAGENT
- WMI Filters
- Starter GPOs

EnableLSAprotection

Links

Display links in this location: TestENTERPRISE.net

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

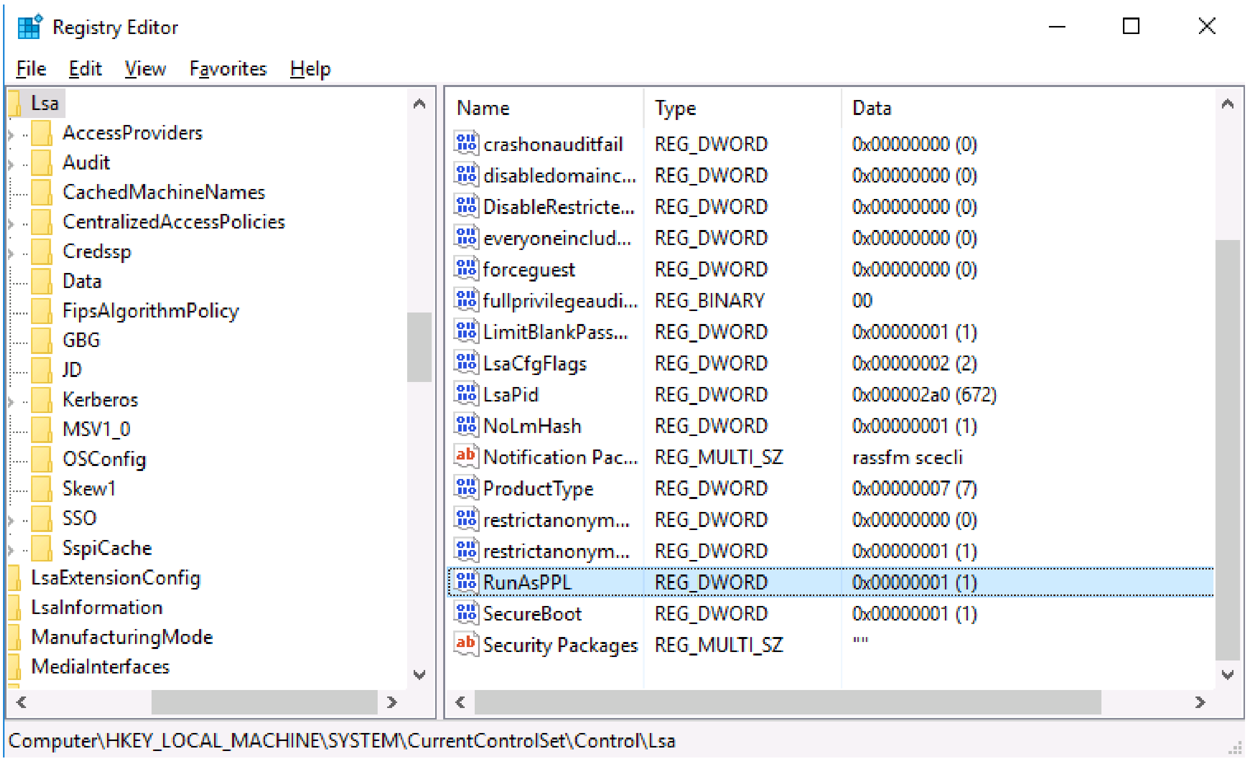
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

After applying EnableLSAprotection GPO to the Tier1\Devices OU:

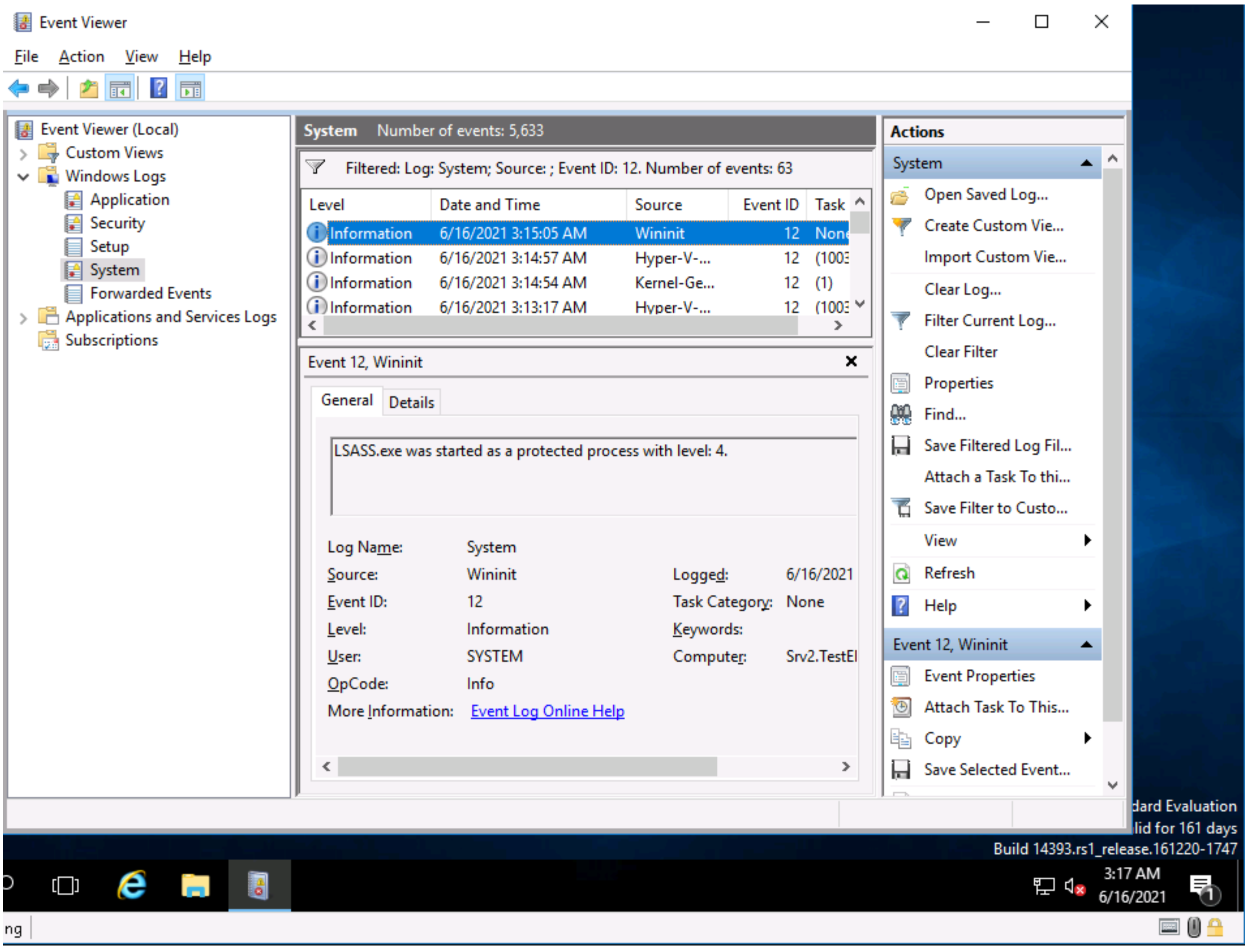


Registry Editor

- Lsa
  - AccessProviders
  - Audit
  - CachedMachineNames
  - CentralizedAccessPolicies
  - Credssp
  - Data
  - FipsAlgorithmPolicy
  - GBG
  - JD
  - Kerberos
  - MSV1_0
  - OSConfig
  - Skew1
  - SSO
  - SspiCache
- LsaExtensionConfig
- LsaInformation
- ManufacturingMode
- MediaInterfaces

Name	Type	Data
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomainc...	REG_DWORD	0x00000000 (0)
DisableRestricte...	REG_DWORD	0x00000000 (0)
everyoneinclud...	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
fullprivilegeaudi...	REG_BINARY	00
LimitBlankPass...	REG_DWORD	0x00000001 (1)
LsaCfgFlags	REG_DWORD	0x00000002 (2)
LsaPid	REG_DWORD	0x000002a0 (672)
NoLmHash	REG_DWORD	0x00000001 (1)
Notification Pac...	REG_MULTI_SZ	rassfm scecli
ProductType	REG_DWORD	0x00000007 (7)
restrictanonym...	REG_DWORD	0x00000000 (0)
restrictanonym...	REG_DWORD	0x00000001 (1)
RunAsPPL	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	""

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa



System Number of events: 5,633

Filtered: Log: System; Source: ; Event ID: 12. Number of events: 63

Level	Date and Time	Source	Event ID	Task
Information	6/16/2021 3:15:05 AM	Wininit	12	None
Information	6/16/2021 3:14:57 AM	Hyper-V-...	12	(1003
Information	6/16/2021 3:14:54 AM	Kernel-Ge...	12	(1)
Information	6/16/2021 3:13:17 AM	Hyper-V-...	12	(1003

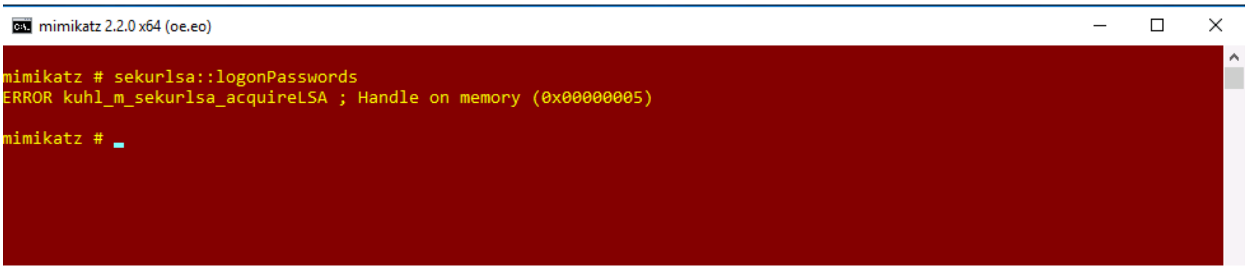
Event 12, Wininit

General Details

LSASS.exe was started as a protected process with level: 4.

Log Name: System
Source: Wininit Logged: 6/16/2021
Event ID: 12 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: Srv2.TestEI
OpCode: Info
More Information: Event Log Online Help

dard Evaluation
lid for 161 days
Build 14393.rs1_release.161220-1747
3:17 AM
6/16/2021


mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # sekurlsa::logonPasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz # _
```

Summary:

This blog post describes the process of enabling and disabling the Additional LSA protection. When LSA protection is used together with the Secure Boot the only way to disable the protection may be the Local Security Authority (LSA) Protected Process Opt-out tool – turning off the Secure Boot may not work as expected.

Part 5 – Mitigating Pass-The-Hash Attacks