Index

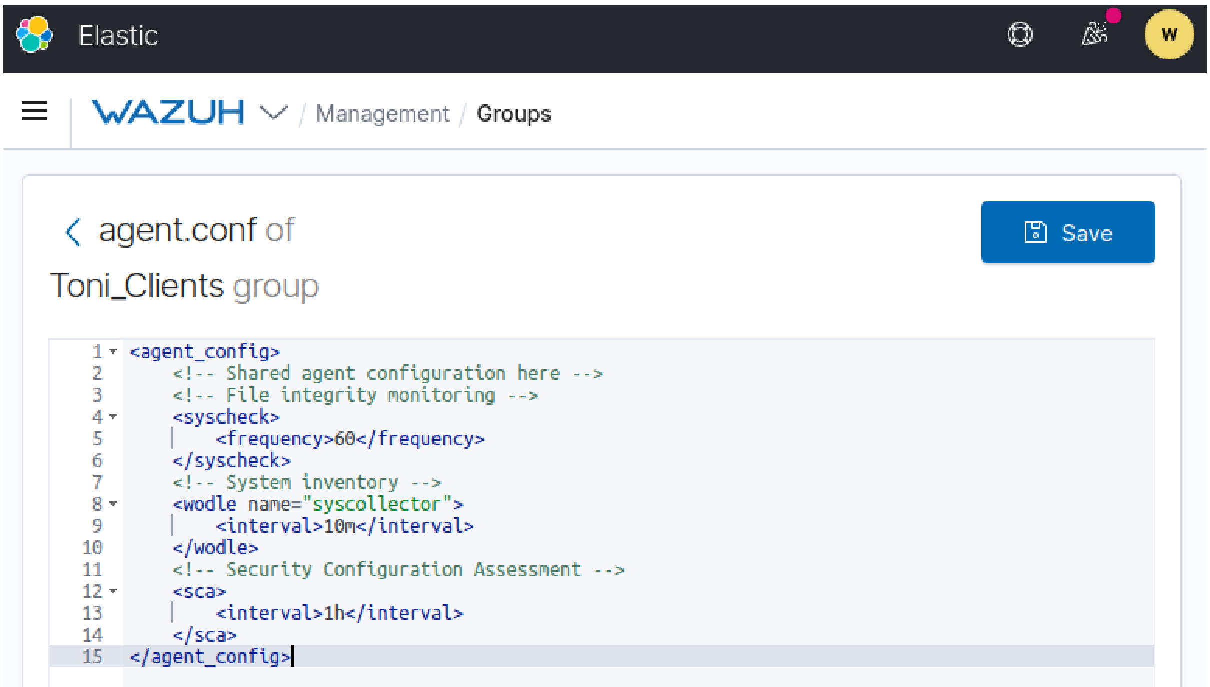
Wazuh FIM (File Integrity Monitoring)

This module runs periodic scans of the agent system, this action stores the checksums and atributes of the monitored elements and Windows registry in a local database.

In the next scan will comare the current checksums with the stored values.

When a change is detected, it is reported in our Wazuh manager.

Therefore, it is the appropriate module to identify possible intrusions that may have altered the integrity of our system.



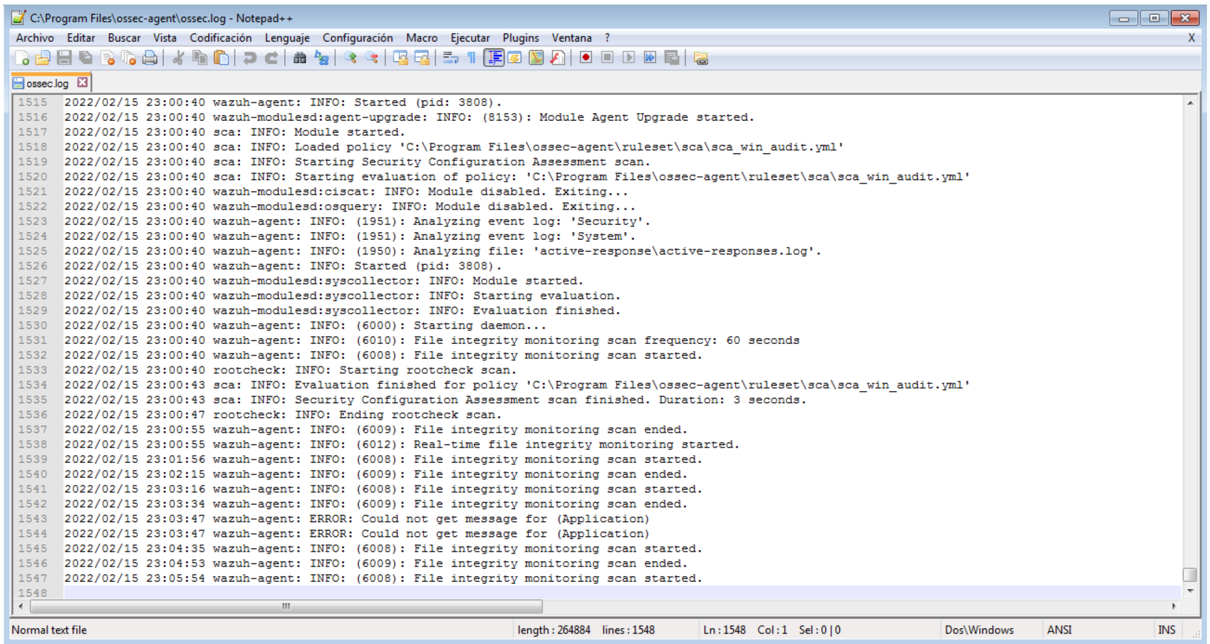
```
<agent_config>
    <!-- Shared agent configuration here -->
    <!-- File integrity monitoring -->
    <syscheck>
        <frequency>60</frequency>
    </syscheck>
    <!-- System inventory -->
    <wodle name="syscollector">
        <interval>10m</interval>
    </wodle>
    <!-- Security Configuration Assessment -->
    <sca>
        <interval>1h</interval>
    </sca>
</agent_config>
```

Figure 1: "Group config"

We change the file integrity monitoring frequency to make our tests. We set the frequency in 60 seconds.

```
<agent_config>
    <!-- Shared agent configuration here -->
    <!-- File integrity monitoring -->
    <syscheck>
        <frequency>60</frequency>
    </syscheck>
    <!-- System inventory -->
    <wodle name="syscollector">
        <interval>10m</interval>
    </wodle>
    <!-- Security Configuration Assessment -->
    <sca>
        <interval>1h</interval>
    </sca>
</agent_config>
```

In the agent logs we can see how the integrity check has been done every 60 seconds.


C:\Program Files\ossec-agent\ossec.log - Notepad++
Archivo Editar Buscar Vista Codificación Lenguaje Configuración Macro Ejecutar Plugins Ventana ?
ossec.log
Normal text file
length : 264884 lines : 1548
Ln : 1548 Col : 1 Sel : 0 | 0
Dos\Windows
ANSI
INS

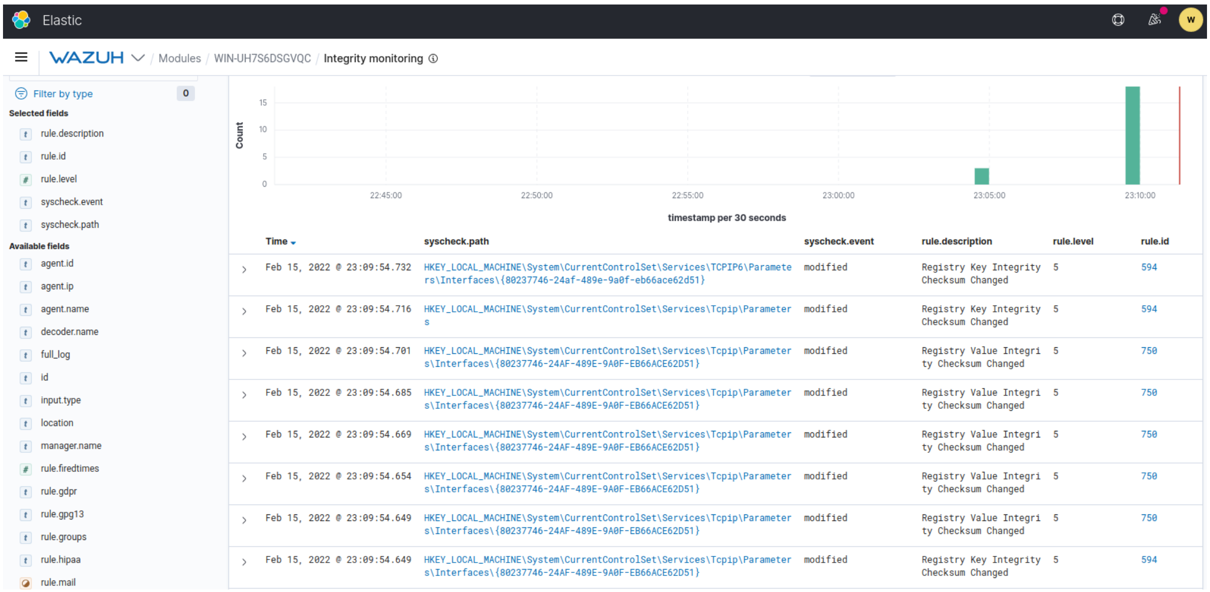
```
2022/02/15 23:00:40 wazuh-agent: INFO: Started (pid: 3808).
2022/02/15 23:00:40 wazuh-modulesd:agent-upgrade: INFO: (8153): Module Agent Upgrade started.
2022/02/15 23:00:40 sca: INFO: Module started.
2022/02/15 23:00:40 sca: INFO: Loaded policy 'C:\Program Files\ossec-agent\ruleset\sca\sca_win_audit.yml'
2022/02/15 23:00:40 sca: INFO: Starting Security Configuration Assessment scan.
2022/02/15 23:00:40 sca: INFO: Starting evaluation of policy: 'C:\Program Files\ossec-agent\ruleset\sca\sca_win_audit.yml'
2022/02/15 23:00:40 wazuh-modulesd:ciscat: INFO: Module disabled. Exiting...
2022/02/15 23:00:40 wazuh-modulesd:osquery: INFO: Module disabled. Exiting...
2022/02/15 23:00:40 wazuh-agent: INFO: (1951): Analyzing event log: 'Security'.
2022/02/15 23:00:40 wazuh-agent: INFO: (1951): Analyzing event log: 'System'.
2022/02/15 23:00:40 wazuh-agent: INFO: (1950): Analyzing file: 'active-response\active-responses.log'.
2022/02/15 23:00:40 wazuh-agent: INFO: Started (pid: 3808).
2022/02/15 23:00:40 wazuh-modulesd:syscollector: INFO: Module started.
2022/02/15 23:00:40 wazuh-modulesd:syscollector: INFO: Starting evaluation.
2022/02/15 23:00:40 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2022/02/15 23:00:40 wazuh-agent: INFO: (6000): Starting daemon...
2022/02/15 23:00:40 wazuh-agent: INFO: (6010): File integrity monitoring scan frequency: 60 seconds
2022/02/15 23:00:40 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2022/02/15 23:00:40 rootcheck: INFO: Starting rootcheck scan.
2022/02/15 23:00:43 sca: INFO: Evaluation finished for policy 'C:\Program Files\ossec-agent\ruleset\sca\sca_win_audit.yml'
2022/02/15 23:00:43 sca: INFO: Security Configuration Assessment scan finished. Duration: 3 seconds.
2022/02/15 23:00:47 rootcheck: INFO: Ending rootcheck scan.
2022/02/15 23:00:55 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
2022/02/15 23:00:55 wazuh-agent: INFO: (6012): Real-time file integrity monitoring started.
2022/02/15 23:01:56 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2022/02/15 23:02:15 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
2022/02/15 23:03:16 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2022/02/15 23:03:34 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
2022/02/15 23:03:47 wazuh-agent: ERROR: Could not get message for (Application)
2022/02/15 23:03:47 wazuh-agent: ERROR: Could not get message for (Application)
2022/02/15 23:04:35 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2022/02/15 23:04:53 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
2022/02/15 23:05:54 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
```

Figure 2: “Agent logs”

```
2022/02/15 23:00:40 wazuh-agent: INFO: (6010): File integrity monitoring scan frequency: 60 seconds
2022/02/15 23:00:40 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2022/02/15 23:00:40 rootcheck: INFO: Starting rootcheck scan.
2022/02/15 23:00:43 sca: INFO: Evaluation finished for policy 'C:\Program Files\ossec-agent\ruleset\sca\sca_win_audit.yml'
2022/02/15 23:00:43 sca: INFO: Security Configuration Assessment scan finished. Duration: 3 seconds.
2022/02/15 23:00:47 rootcheck: INFO: Ending rootcheck scan.
2022/02/15 23:00:55 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
2022/02/15 23:00:55 wazuh-agent: INFO: (6012): Real-time file integrity monitoring started.
2022/02/15 23:01:56 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2022/02/15 23:02:15 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
2022/02/15 23:03:16 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2022/02/15 23:03:34 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
2022/02/15 23:03:47 wazuh-agent: ERROR: Could not get message for (Application)
```

```
2022/02/15 23:03:47 wazuh-agent: ERROR: Could not get message for (Application)
2022/02/15 23:04:35 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2022/02/15 23:04:53 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
2022/02/15 23:05:54 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
```

We can see the events in our Wazuh agent Integrity Monitoring dashboard.



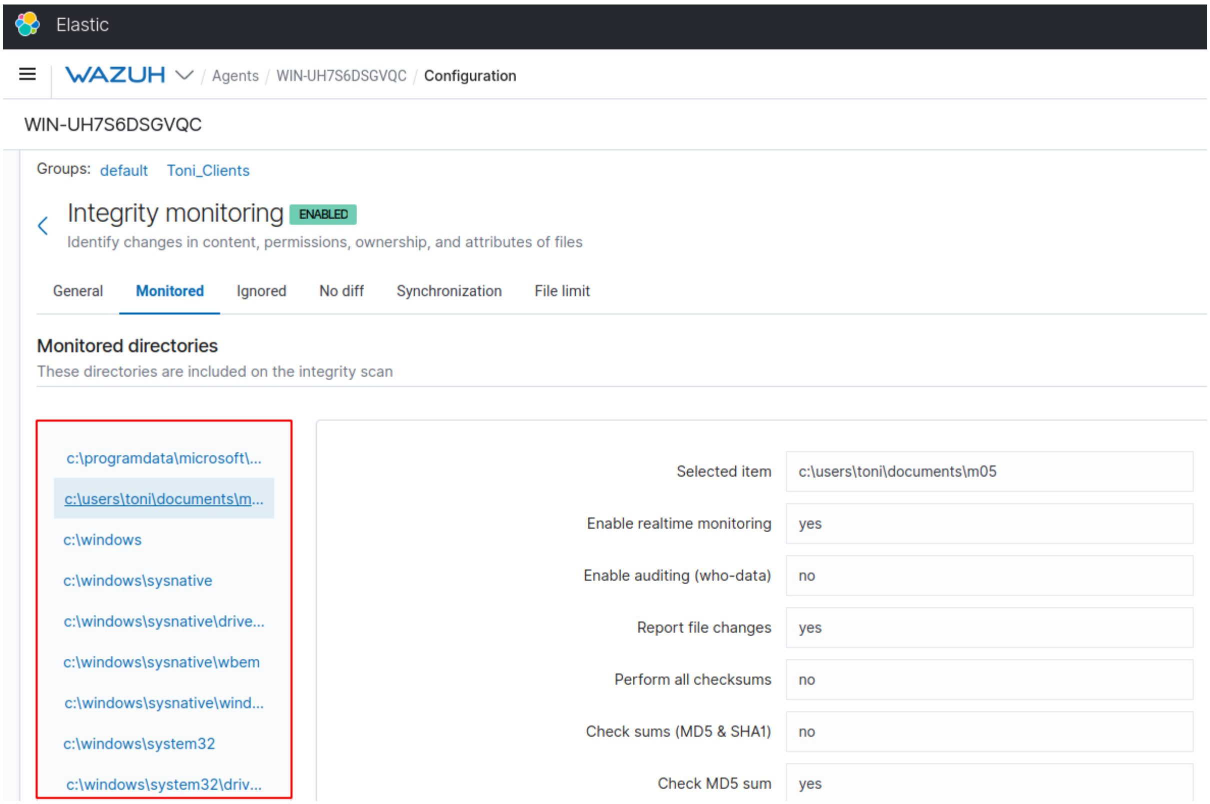
Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Feb 15, 2022 @ 23:09:54.732	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TCPIP6\Parameters\Interfaces\{80237746-24af-489e-9a0f-eb66ace62d51}	modified	Registry Key Integrity Checksum Changed	5	594
Feb 15, 2022 @ 23:09:54.716	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters	modified	Registry Key Integrity Checksum Changed	5	594
Feb 15, 2022 @ 23:09:54.701	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{80237746-24AF-489E-9A0F-EB66ACE62D51}	modified	Registry Value Integrity Checksum Changed	5	750
Feb 15, 2022 @ 23:09:54.685	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{80237746-24AF-489E-9A0F-EB66ACE62D51}	modified	Registry Value Integrity Checksum Changed	5	750
Feb 15, 2022 @ 23:09:54.669	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{80237746-24AF-489E-9A0F-EB66ACE62D51}	modified	Registry Value Integrity Checksum Changed	5	750
Feb 15, 2022 @ 23:09:54.654	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{80237746-24AF-489E-9A0F-EB66ACE62D51}	modified	Registry Value Integrity Checksum Changed	5	750
Feb 15, 2022 @ 23:09:54.649	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{80237746-24AF-489E-9A0F-EB66ACE62D51}	modified	Registry Value Integrity Checksum Changed	5	750
Feb 15, 2022 @ 23:09:54.649	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{80237746-24AF-489E-9A0F-EB66ACE62D51}	modified	Registry Key Integrity Checksum Changed	5	594

Figure 3: “Integrity monitoring notifications”

We can also check the integrity of a directory that we choose, changing the agent or group config. In our case we are going to check the integrity of the directory *C:/Users/Toni/Documents/m05*

```
<!-- File integrity monitoring -->
<syscheck>
    ...
    <directories check_all="yes" realtime="yes" report_changes="yes">
        C:/Users/Toni/Documents/m05
    </directories>
    ...
</syscheck>
```

The custom directory is added in the monitored directories section.



Elastic

WAZUH / Agents / WIN-UH7S6DSGVQC / Configuration

WIN-UH7S6DSGVQC

Groups: default Toni_Clients

Integrity monitoring ENABLED

Identify changes in content, permissions, ownership, and attributes of files

General Monitored Ignored No diff Synchronization File limit

Monitored directories

These directories are included on the integrity scan

- c:\programdata\microsoft\...
- c:\users\toni\documents\m...
- c:\windows
- c:\windows\sysnative
- c:\windows\sysnative\drive...
- c:\windows\sysnative\wbem
- c:\windows\sysnative\wind...
- c:\windows\system32
- c:\windows\system32\driv...

Selected item	c:\users\toni\documents\m05
Enable realtime monitoring	yes
Enable auditing (who-data)	no
Report file changes	yes
Perform all checksums	no
Check sums (MD5 & SHA1)	no
Check MD5 sum	yes

Figure 4: “Monitored directories”

Let’s check how well the integrity monitoring works. We will edit some files and directories that we know are included in the process.

- C:/Windows/win.ini

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
[MCI Extensions.BAK]
3g2=MPEGVideo
3gp=MPEGVideo
3gp2=MPEGVideo
3gpp=MPEGVideo
aac=MPEGVideo
adt=MPEGVideo
adts=MPEGVideo
m2t=MPEGVideo
m2ts=MPEGVideo
m2v=MPEGVideo
m4a=MPEGVideo
m4v=MPEGVideo
mod=MPEGVideo
mov=MPEGVideo
mp4=MPEGVideo
mp4v=MPEGVideo
```

```
mts=MPEGVideo
ts=MPEGVideo
tts=MPEGVideo
test=Test
```

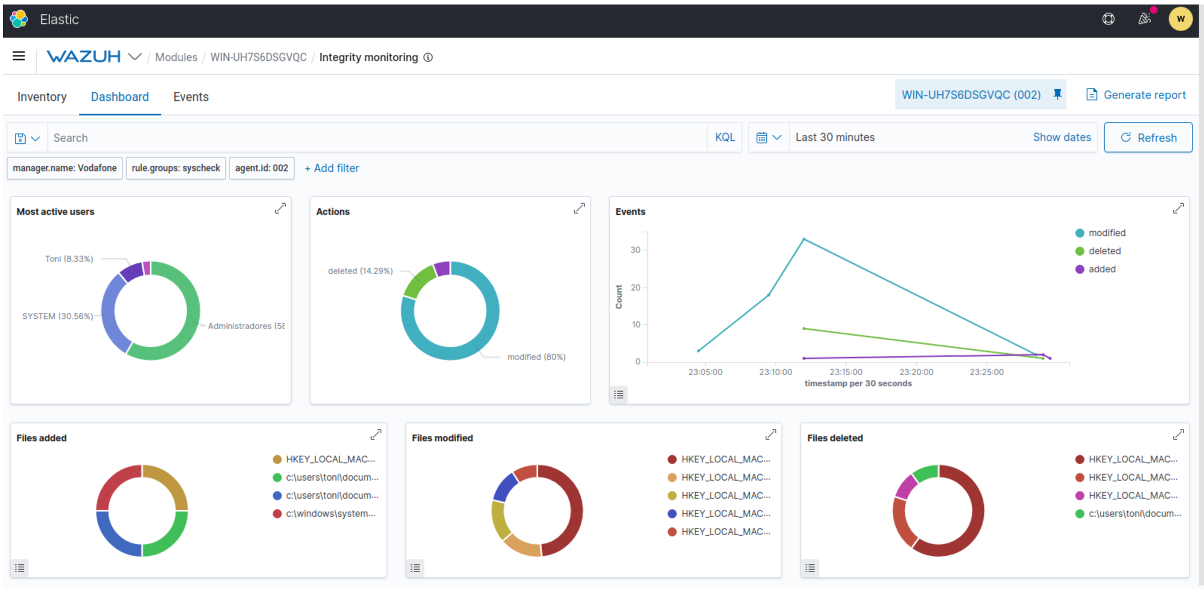
- C:/Windows/System32/drivers/etc/hosts

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
142.250.178.174 toni-pm.herokuapp.com
```

- Added C:/Windows/System32/drivers/etc/exploit
- Added C:/Users/Toni/Documents/m05/m05_exploit

These changes have generated alerts in the Integrity monitoring dashboard of the agent.



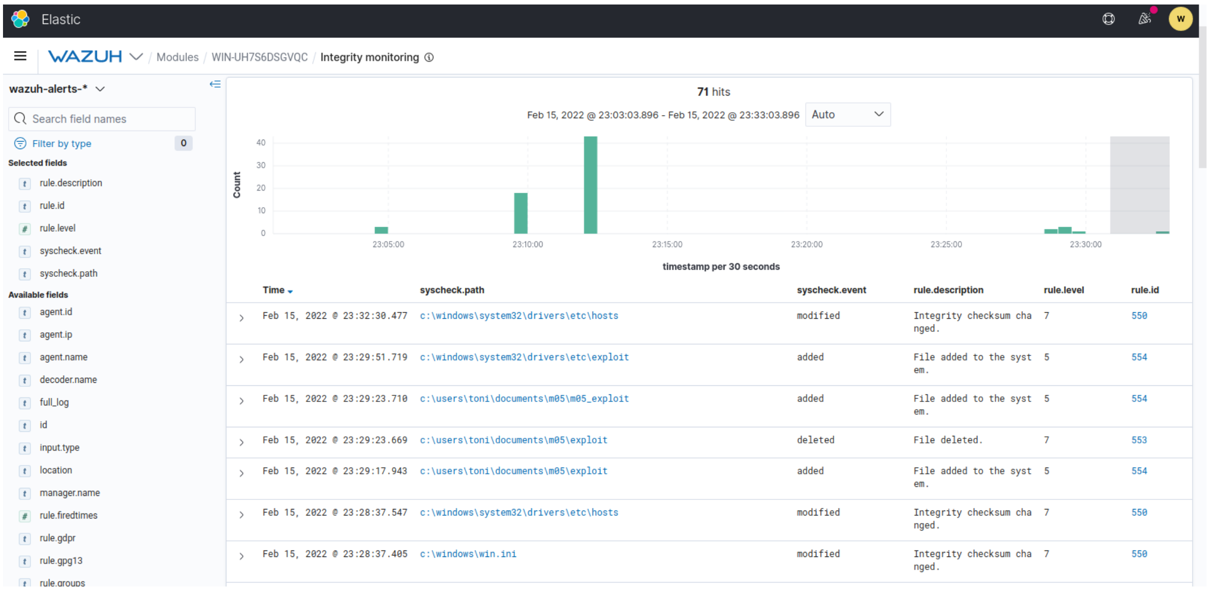
WAZUH / Modules / WIN-UH7S6DSGVQC / Integrity monitoring

WIN-UH7S6DSGVQC (002)

Search — KQL — Last 30 minutes

manager.name: Vodafone | rule.groups: syscheck | agent.id: 002

Figure 5: "Integrity monitoring dashboard"



Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Feb 15, 2022 @ 23:32:30.477	c:\windows\system32\drivers\etc\hosts	modified	Integrity checksum changed.	7	550
Feb 15, 2022 @ 23:29:51.719	c:\windows\system32\drivers\etc\exploit	added	File added to the system.	5	554
Feb 15, 2022 @ 23:29:23.710	c:\users\toni\documents\m05\m05_exploit	added	File added to the system.	5	554
Feb 15, 2022 @ 23:29:23.669	c:\users\toni\documents\m05\exploit	deleted	File deleted.	7	553
Feb 15, 2022 @ 23:29:17.943	c:\users\toni\documents\m05\exploit	added	File added to the system.	5	554
Feb 15, 2022 @ 23:28:37.547	c:\windows\system32\drivers\etc\hosts	modified	Integrity checksum changed.	7	550
Feb 15, 2022 @ 23:28:37.405	c:\windows\win.ini	modified	Integrity checksum changed.	7	550

Figure 6: “Integrity monitoring alerts”

Wazuh SCA (Security Configuration Assessment)

This module aims to provide the user with the best possible experience when performing scans about hardening and configuration policies.

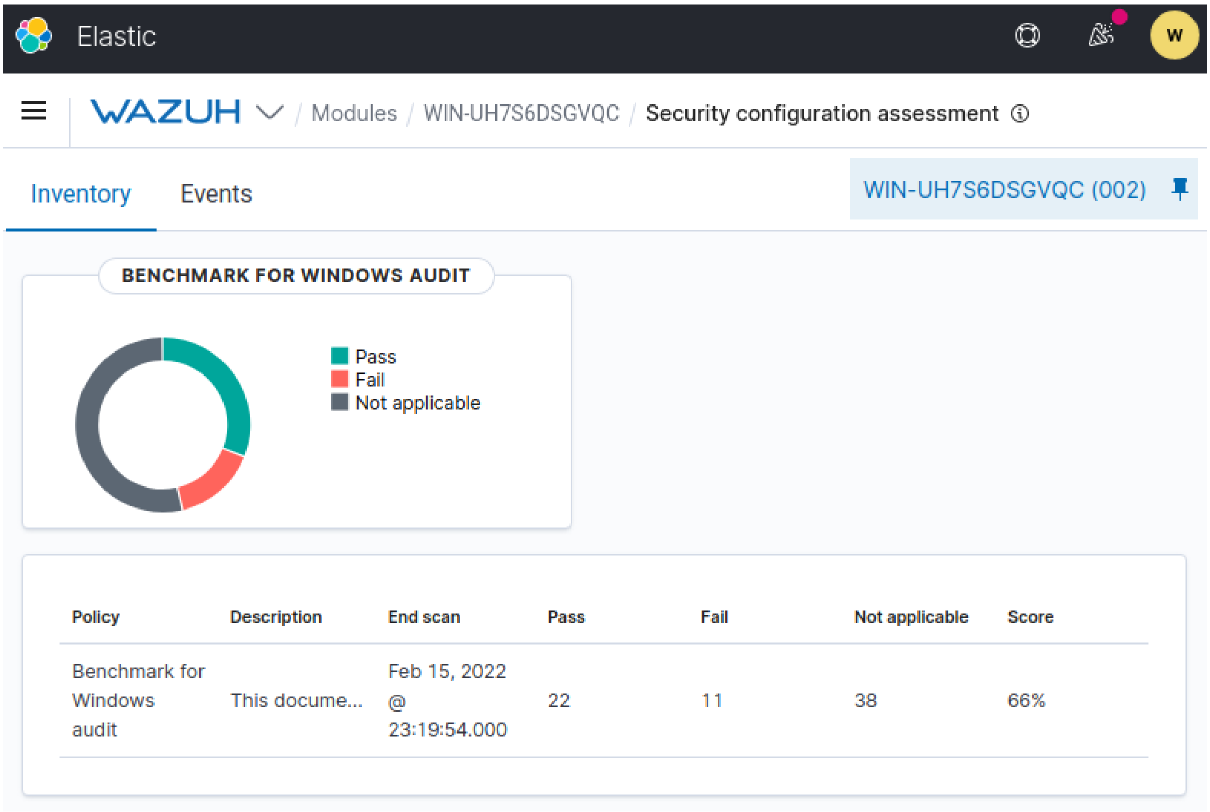
This allows us to improve some security elements of the system

The first thing is always to activate the functionality in the agent config.

```
<sca>
    <enabled>yes</enabled>
    <scan_on_start>yes</scan_on_start>
    <interval>12h</interval>
    <skip_nfs>yes</skip_nfs>
</sca>
```

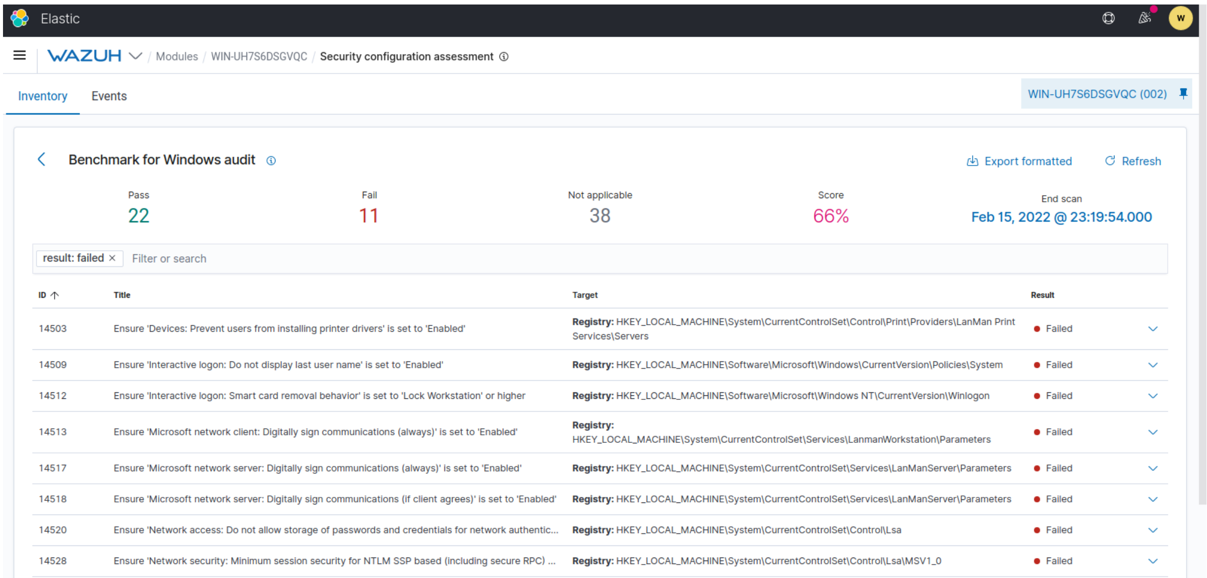
Once configured, we can refresh the SCA dashboard.

This action will provide us with information about those points that we can improve in the agent


Elastic
W
WAZUH
Modules / WIN-UH7S6DSGVQC / Security configuration assessment
Inventory
Events
WIN-UH7S6DSGVQC (002)
BENCHMARK FOR WINDOWS AUDIT
Pass
Fail
Not applicable

Policy	Description	End scan	Pass	Fail	Not applicable	Score
Benchmark for Windows audit	This docume...	Feb 15, 2022 @ 23:19:54.000	22	11	38	66%

Figure 7: “SCA Dashboard”



Pass 22 | Fail 11 | Not applicable 38 | Score 66% | End scan Feb 15, 2022 @ 23:19:54.000

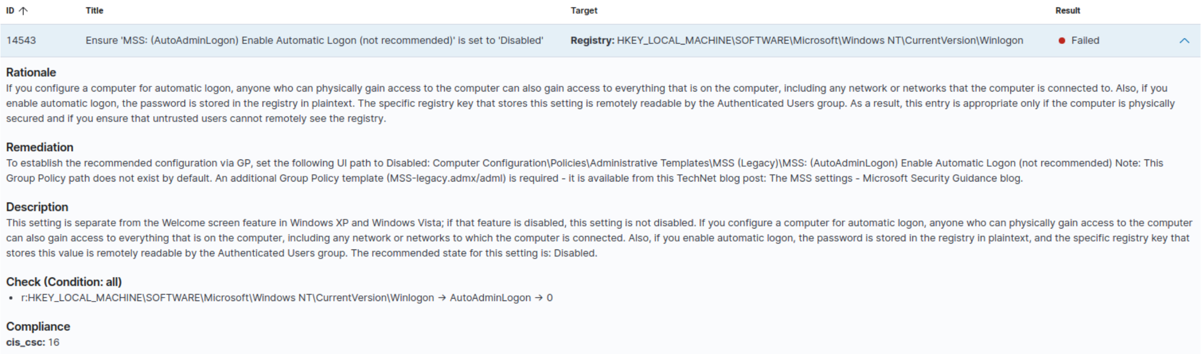
ID ↑	Title	Target	Result
14503	Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'	**Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers	● Failed
14509	Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'	**Registry:** HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	● Failed
14512	Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	**Registry:** HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	● Failed
14513	Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	**Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters	● Failed
14517	Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	**Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters	● Failed
14518	Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	**Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters	● Failed
14520	Ensure 'Network access: Do not allow storage of passwords and credentials for network authentic...	**Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa	● Failed
14528	Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) ...	**Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0	● Failed

Figure 8: “SCA Inventory”

I attach the failed points of my agent and how I have solved it based on the information received.

In total there are 11 points to correct.

14543 Ensure ‘MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)’ is set to ‘Disabled’



ID ↑	Title	Target	Result
14543	Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	**Registry:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	● Failed

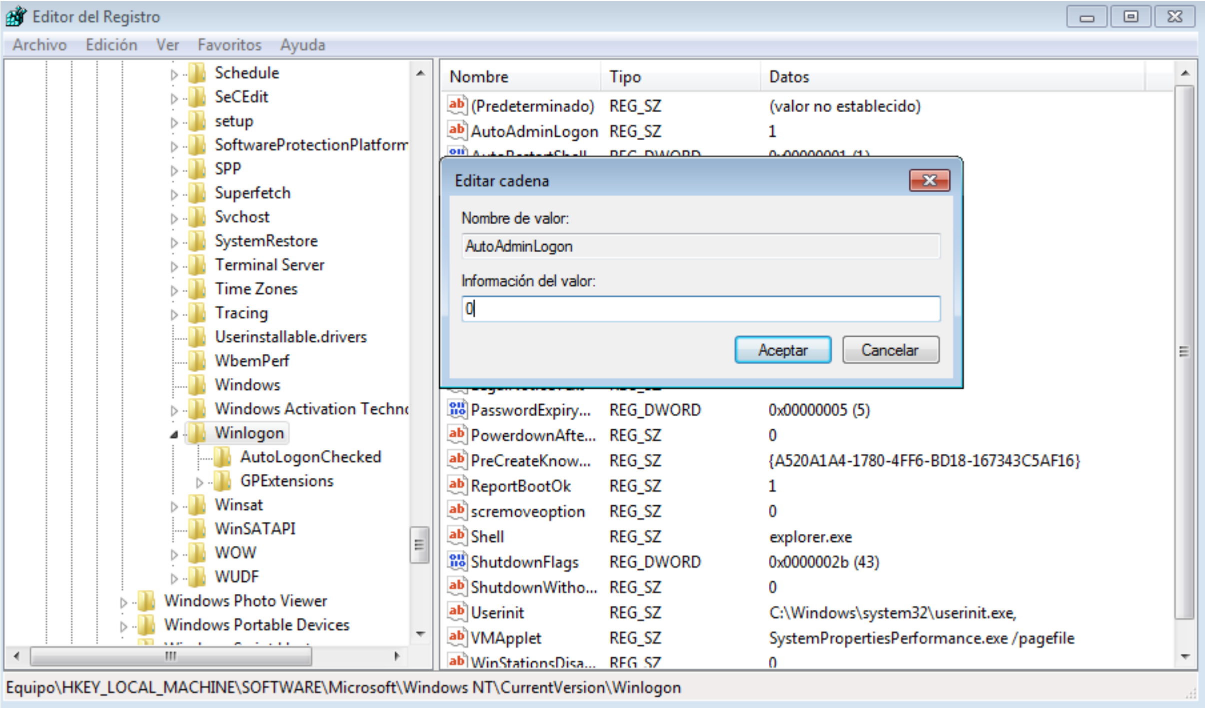
Rationale
If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

Remediation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is available from this TechNet blog post: The MSS settings - Microsoft Security Guidance blog.

Description
This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group. The recommended state for this setting is: Disabled.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon → AutoAdminLogon → 0

Compliance
cis_csc: 16



Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
AutoAdminLogon	REG_SZ	1
AutoRestartShell	REG_DWORD	0x00000001 (1)
PasswordExpiry...	REG_DWORD	0x00000005 (5)
PowerdownAfte...	REG_SZ	0
PreCreateKnow...	REG_SZ	{A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
Shell	REG_SZ	explorer.exe
ShutdownFlags	REG_DWORD	0x0000002b (43)
ShutdownWitho...	REG_SZ	0
Userinit	REG_SZ	C:\Windows\system32\userinit.exe,
VMApplet	REG_SZ	SystemPropertiesPerformance.exe /pagefile
WinStationsDisa...	REG_SZ	0

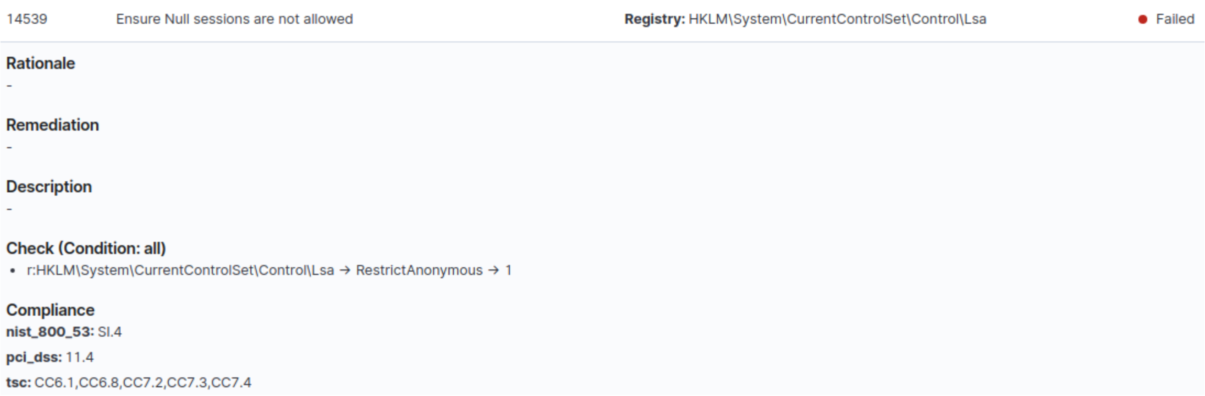
Nombre de valor: AutoAdminLogon

Información del valor: 0

Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

---

14539 Ensure Null sessions are not allowed



14539	Ensure Null sessions are not allowed	**Registry:** HKLM\System\CurrentControlSet\Control\Lsa	● Failed

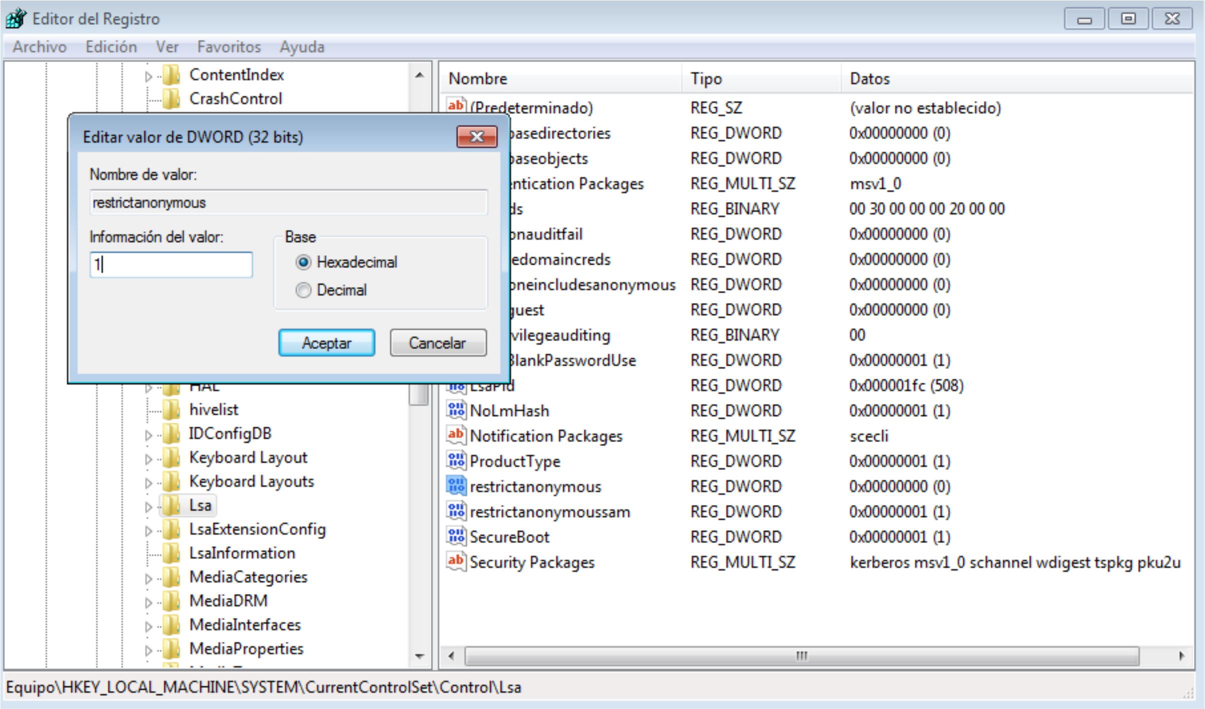
Rationale
-

Remediation
-

Description
-

Check (Condition: all)
- r:HKLM\System\CurrentControlSet\Control\Lsa → RestrictAnonymous → 1

Compliance
nist_800_53: SI.4
pci_dss: 11.4
tsc: CC6.1,CC6.8,CC7.2,CC7.3,CC7.4



Editar valor de DWORD (32 bits)

Nombre de valor: restrictanonymous

Información del valor: 1

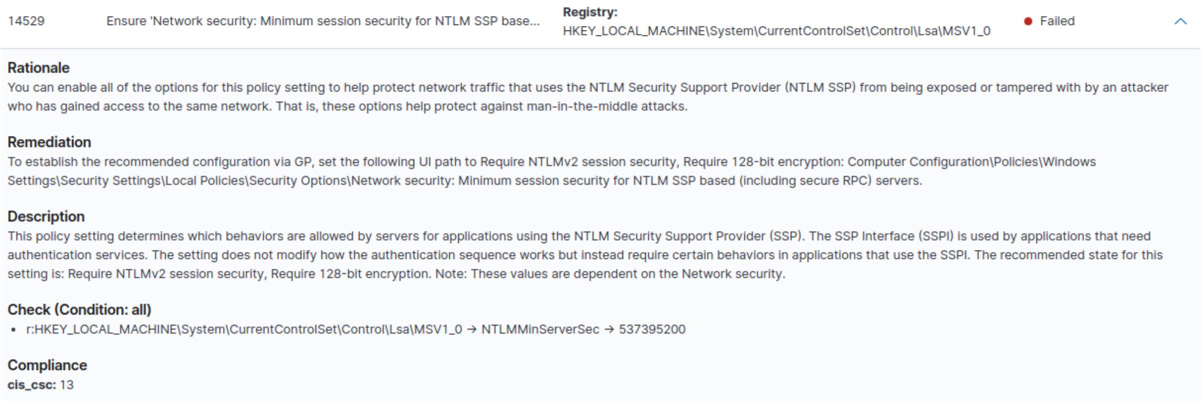
Base: ● Hexadecimal ○ Decimal

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
basedirectories	REG_DWORD	0x00000000 (0)
baseobjects	REG_DWORD	0x00000000 (0)
ntication Packages	REG_MULTI_SZ	msv1_0
ds	REG_BINARY	00 30 00 00 00 20 00 00
nauditfail	REG_DWORD	0x00000000 (0)
edomaincreds	REG_DWORD	0x00000000 (0)
neincludesanonymous	REG_DWORD	0x00000000 (0)
guest	REG_DWORD	0x00000000 (0)
vilegeauditing	REG_BINARY	00
BlankPasswordUse	REG_DWORD	0x00000001 (1)
LsaPid	REG_DWORD	0x000001fc (508)
NoLmHash	REG_DWORD	0x00000001 (1)
Notification Packages	REG_MULTI_SZ	scecli
ProductType	REG_DWORD	0x00000001 (1)
restrictanonymous	REG_DWORD	0x00000000 (0)
restrictanonymoussam	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	kerberos msv1_0 schannel wdigest tspkg pku2u

Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

---

14529 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'



14529 Ensure 'Network security: Minimum session security for NTLM SSP base... Registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0 ● Failed

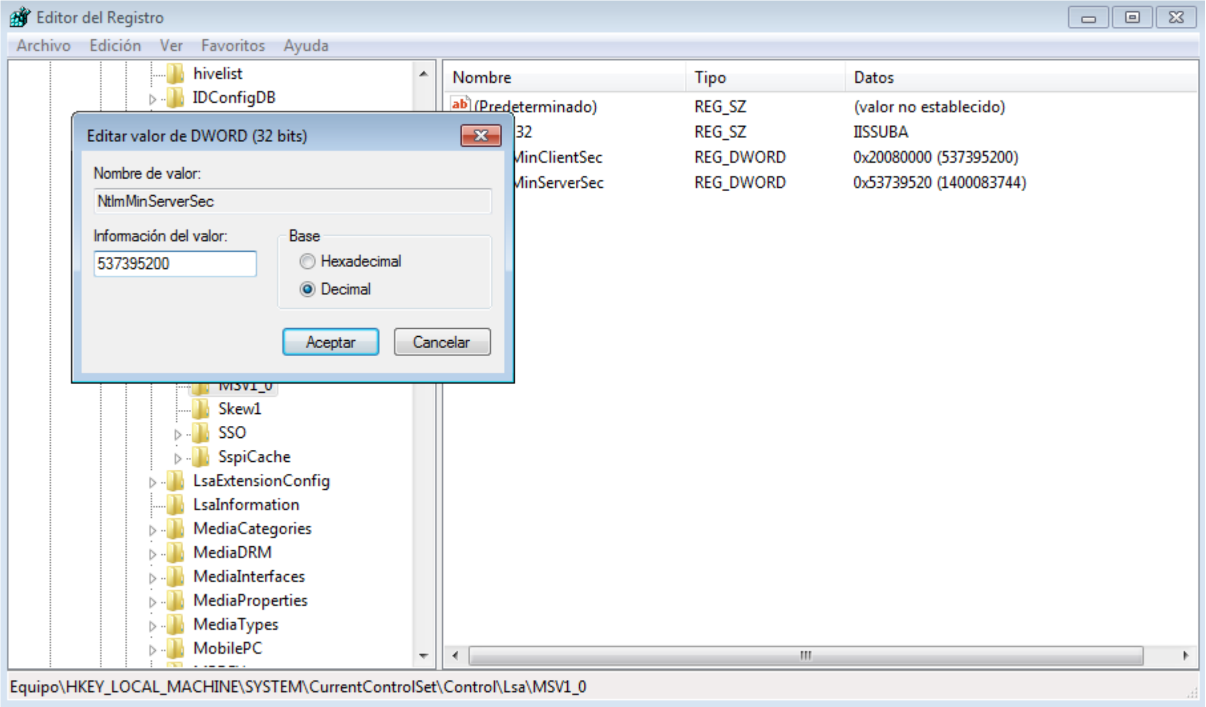
Rationale
You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

Remediation
To establish the recommended configuration via GP, set the following UI path to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers.

Description
This policy setting determines which behaviors are allowed by servers for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Note: These values are dependent on the Network security.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0 → NTLMMinServerSec → 537395200

Compliance
cis_csc: 13



Editar valor de DWORD (32 bits)

Nombre de valor:
NtlmMinServerSec

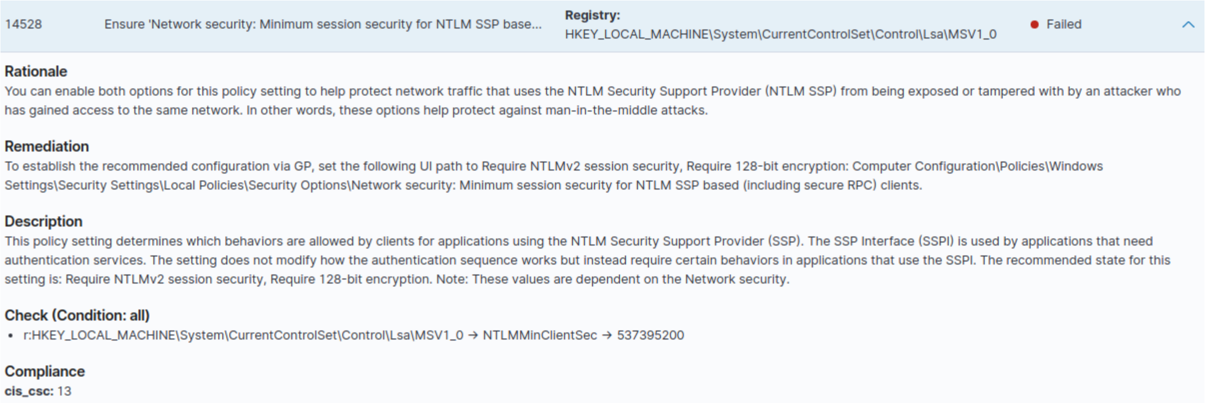
Información del valor:
537395200

Base
○ Hexadecimal
● Decimal

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
32	REG_SZ	IISSUBA
MinClientSec	REG_DWORD	0x20080000 (537395200)
MinServerSec	REG_DWORD	0x53739520 (1400083744)

Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0

14528 Ensure ‘Network security: Minimum session security for NTLM SSP based (including secure RPC) clients’ is set to ‘Require NTLMv2 session security, Require 128-bit encryption’


14528 Ensure 'Network security: Minimum session security for NTLM SSP base... **Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0 ● Failed

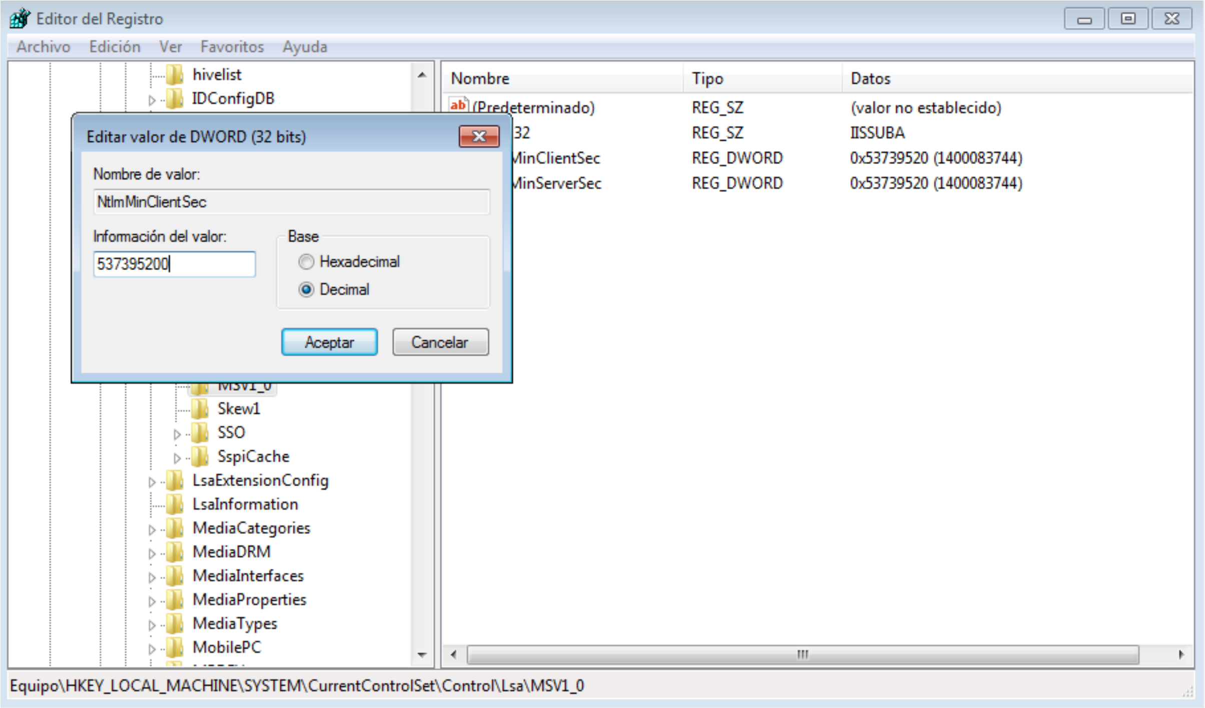
Rationale
You can enable both options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

Remediation
To establish the recommended configuration via GP, set the following UI path to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients.

Description
This policy setting determines which behaviors are allowed by clients for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Note: These values are dependent on the Network security.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0 → NTLMMinClientSec → 537395200

Compliance
cis_csc: 13



Editar valor de DWORD (32 bits)

Nombre de valor: NtlmMinClientSec

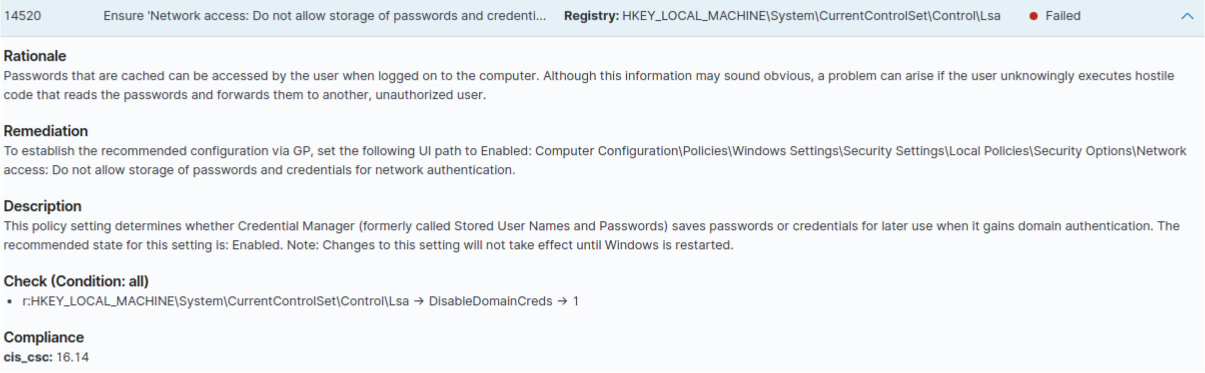
Información del valor: 537395200

Base: ○ Hexadecimal ● Decimal

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
32	REG_SZ	IISSUBA
MinClientSec	REG_DWORD	0x53739520 (1400083744)
MinServerSec	REG_DWORD	0x53739520 (1400083744)

Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0

14520 Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'


14520 Ensure 'Network access: Do not allow storage of passwords and credenti... **Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa ● Failed

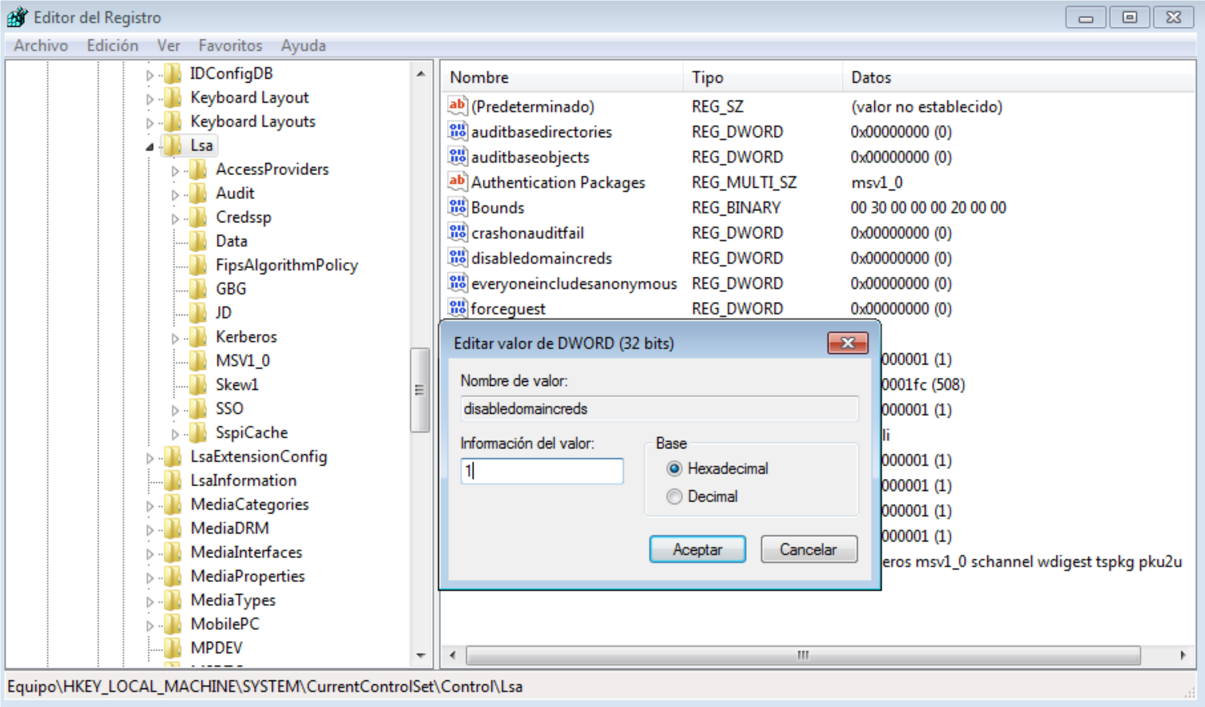
Rationale
Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

Remediation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication.

Description
This policy setting determines whether Credential Manager (formerly called Stored User Names and Passwords) saves passwords or credentials for later use when it gains domain authentication. The recommended state for this setting is: Enabled. Note: Changes to this setting will not take effect until Windows is restarted.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa → DisableDomainCreds → 1

Compliance
cis_csc: 16.14



- IDConfigDB
- Keyboard Layout
- Keyboard Layouts
- Lsa
  - AccessProviders
  - Audit
  - Credssp
  - Data
  - FipsAlgorithmPolicy
  - GBG
  - JD
  - Kerberos
  - MSV1_0
  - Skew1
  - SSO
  - SspiCache
- LsaExtensionConfig
- LsaInformation
- MediaCategories
- MediaDRM
- MediaInterfaces
- MediaProperties
- MediaTypes
- MobilePC
- MPDEV

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
auditbasedirectories	REG_DWORD	0x00000000 (0)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication Packages	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomaincreds	REG_DWORD	0x00000000 (0)
everyoneincludesanonymous	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
		000001 (1)
		0001fc (508)
		000001 (1)
		li
		000001 (1)
		000001 (1)
		000001 (1)
		000001 (1)
		eros msv1_0 schannel wdigest tspkg pku2u

Editar valor de DWORD (32 bits)

Nombre de valor: disabledomaincreds

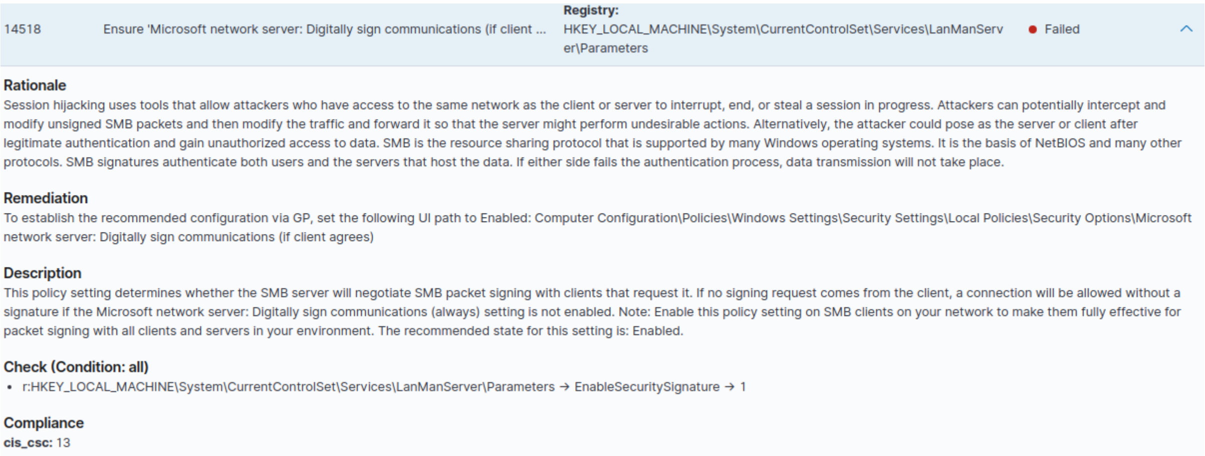
Información del valor: 1

Base: ● Hexadecimal ○ Decimal

Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

---

14518 Ensure ‘Microsoft network server: Digitally sign communications (if client agrees)’ is set to ‘Enabled’



14518 Ensure 'Microsoft network server: Digitally sign communications (if client ... **Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters ● Failed

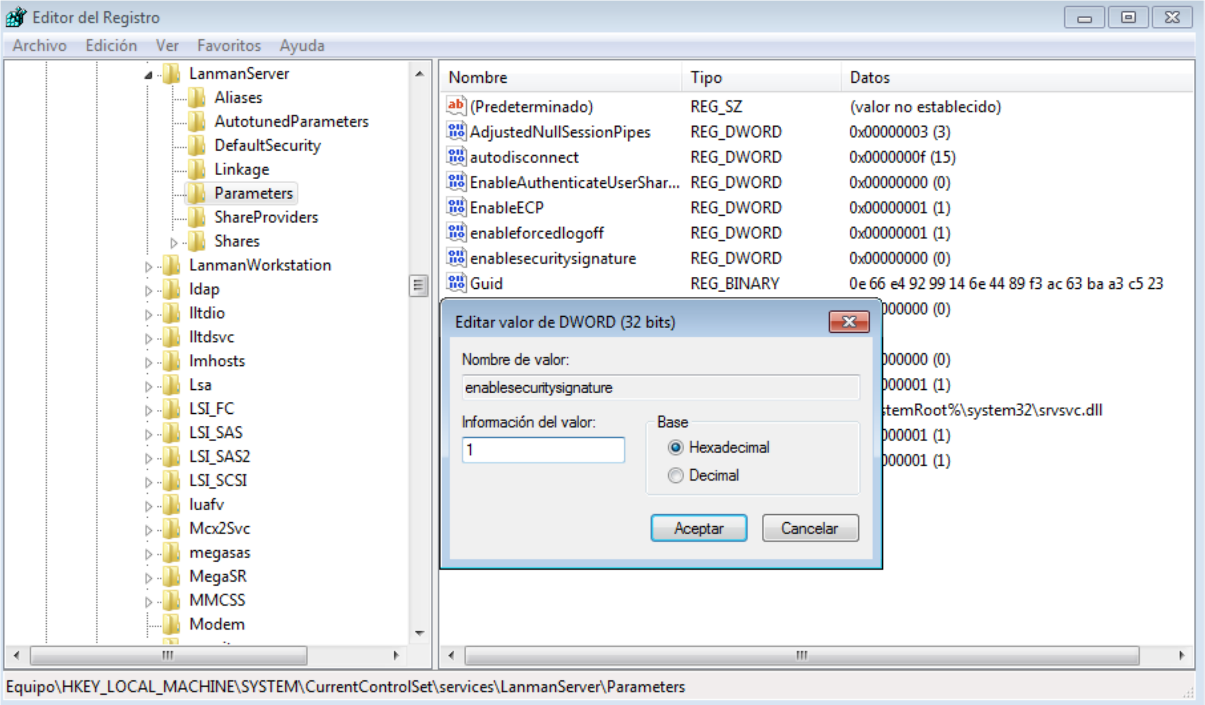
Rationale
Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Remediation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)

Description
This policy setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled. Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: Enabled.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters → EnableSecuritySignature → 1

Compliance
cis_csc: 13



- LanmanServer
  - Aliases
  - AutotunedParameters
  - DefaultSecurity
  - Linkage
  - Parameters
  - ShareProviders
  - Shares
- LanmanWorkstation
- ldap
- lltdio
- lltdsvc
- lmhosts
- Lsa
- LSI_FC
- LSI_SAS
- LSI_SAS2
- LSI_SCSI
- luafv
- Mcx2Svc
- megasas
- MegaSR
- MMCSS
- Modem

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
AdjustedNullSessionPipes	REG_DWORD	0x00000003 (3)
autodisconnect	REG_DWORD	0x0000000f (15)
EnableAuthenticateUserShar...	REG_DWORD	0x00000000 (0)
EnableECP	REG_DWORD	0x00000001 (1)
enableforcedlogoff	REG_DWORD	0x00000001 (1)
enablesecuritysignature	REG_DWORD	0x00000000 (0)
Guid	REG_BINARY	0e 66 e4 92 99 14 6e 44 89 f3 ac 63 ba a3 c5 23
		)00000 (0)
		)00000 (0)
		)00001 (1)
		stemRoot%\system32\srvsvc.dll
		)00001 (1)
		)00001 (1)

Editar valor de DWORD (32 bits)

Nombre de valor: enablesecuritysignature

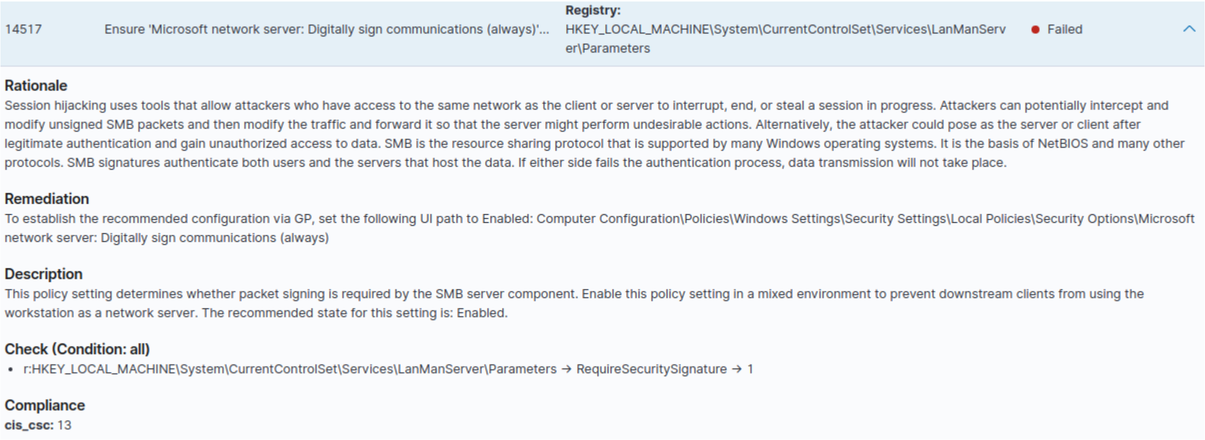
Información del valor: 1

Base: ◉ Hexadecimal ○ Decimal

Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters

---

14517 Ensure ‘Microsoft network server: Digitally sign communications (always)’ is set to ‘Enabled’



14517 Ensure 'Microsoft network server: Digitally sign communications (always)'... **Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters ● Failed

Rationale

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)

Description

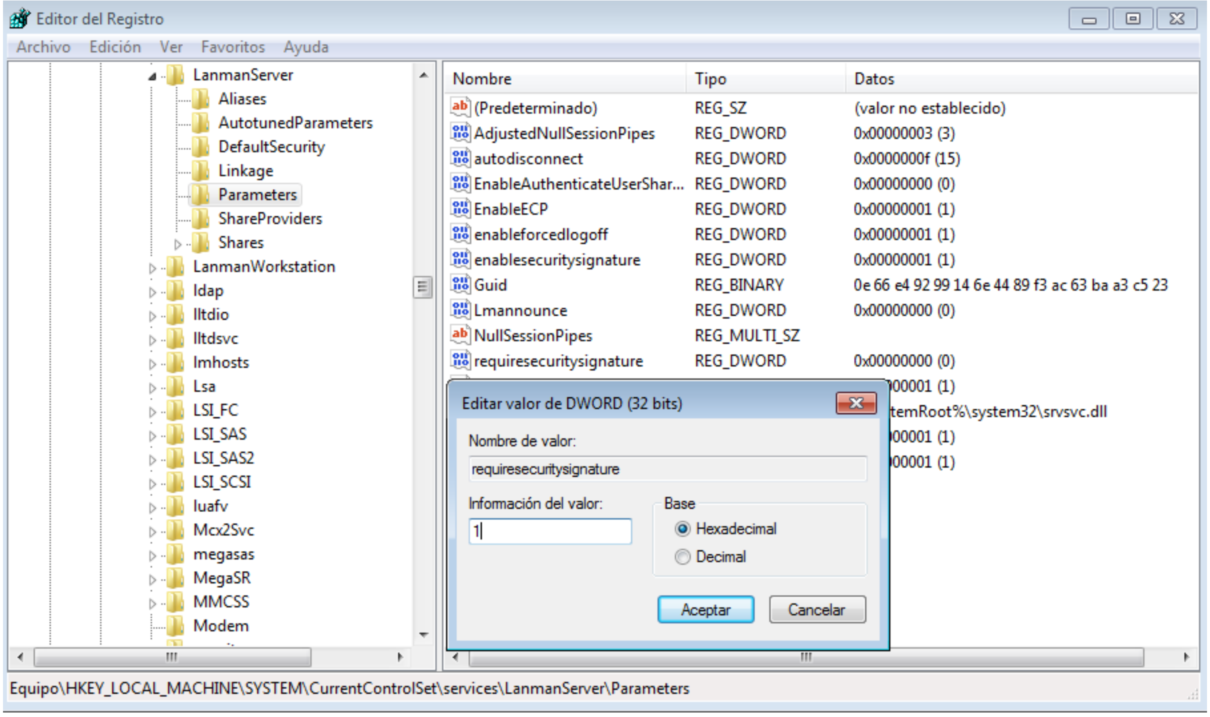
This policy setting determines whether packet signing is required by the SMB server component. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: Enabled.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters → RequireSecuritySignature → 1

Compliance

cis_csc: 13



Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
AdjustedNullSessionPipes	REG_DWORD	0x00000003 (3)
autodisconnect	REG_DWORD	0x0000000f (15)
EnableAuthenticateUserShar...	REG_DWORD	0x00000000 (0)
EnableECP	REG_DWORD	0x00000001 (1)
enableforcedlogoff	REG_DWORD	0x00000001 (1)
enablesecuritysignature	REG_DWORD	0x00000001 (1)
Guid	REG_BINARY	0e 66 e4 92 99 14 6e 44 89 f3 ac 63 ba a3 c5 23
Lmannounce	REG_DWORD	0x00000000 (0)
NullSessionPipes	REG_MULTI_SZ	
requiresecuritysignature	REG_DWORD	0x00000000 (0)
		)00001 (1)
		temRoot%\system32\srvsvc.dll
		)00001 (1)
		)00001 (1)

Editar valor de DWORD (32 bits)

Nombre de valor: requiresecuritysignature

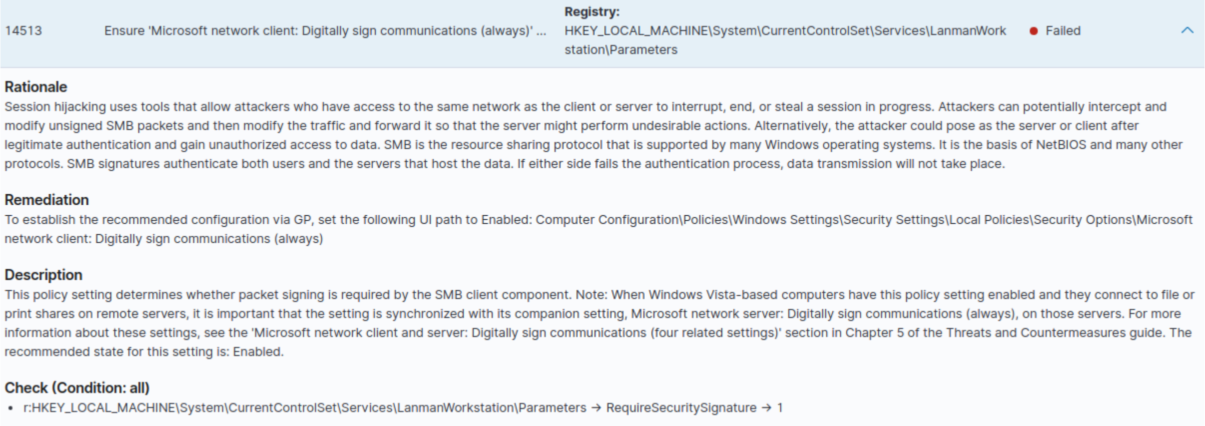
Información del valor: 1

Base: ● Hexadecimal ○ Decimal

Aceptar Cancelar

Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters

14513 Ensure ‘Microsoft network client: Digitally sign communications (always)’ is set to ‘Enabled’



14513 Ensure 'Microsoft network client: Digitally sign communications (always)' ... **Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters ● Failed

Rationale

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Remediation

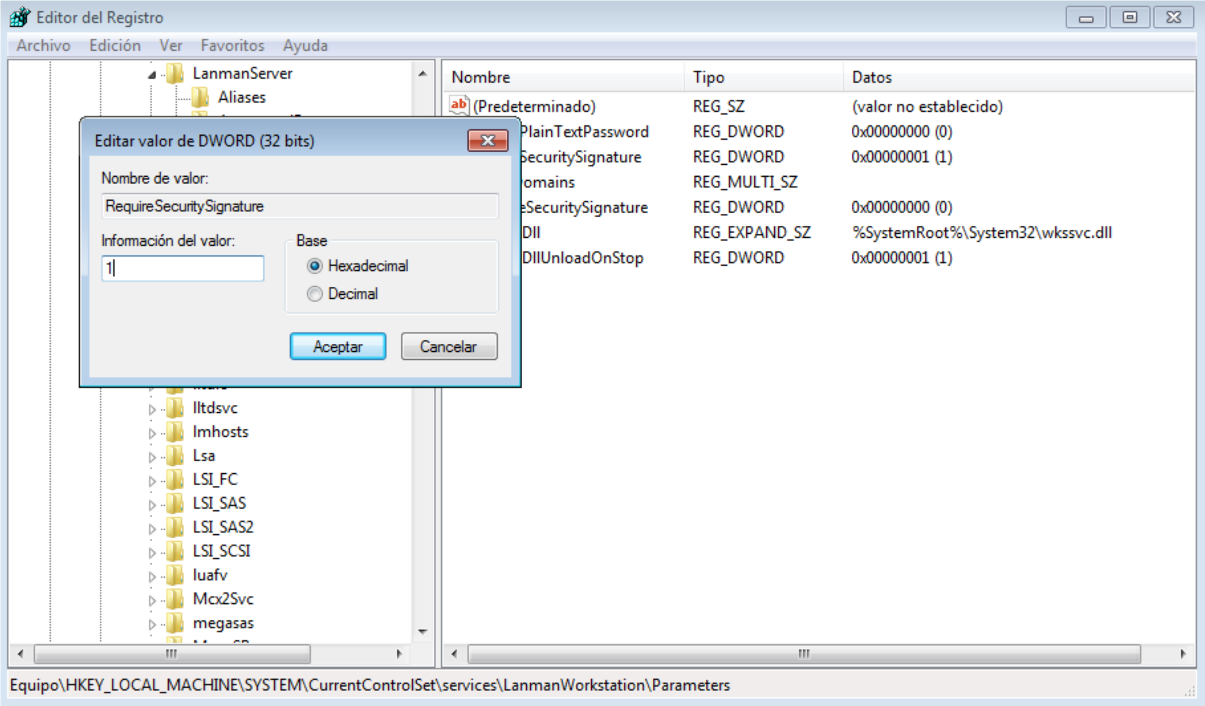
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)

Description

This policy setting determines whether packet signing is required by the SMB client component. Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the 'Microsoft network client and server: Digitally sign communications (four related settings)' section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: Enabled.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters → RequireSecuritySignature → 1



Editar valor de DWORD (32 bits)

Nombre de valor: RequireSecuritySignature

Información del valor: 1

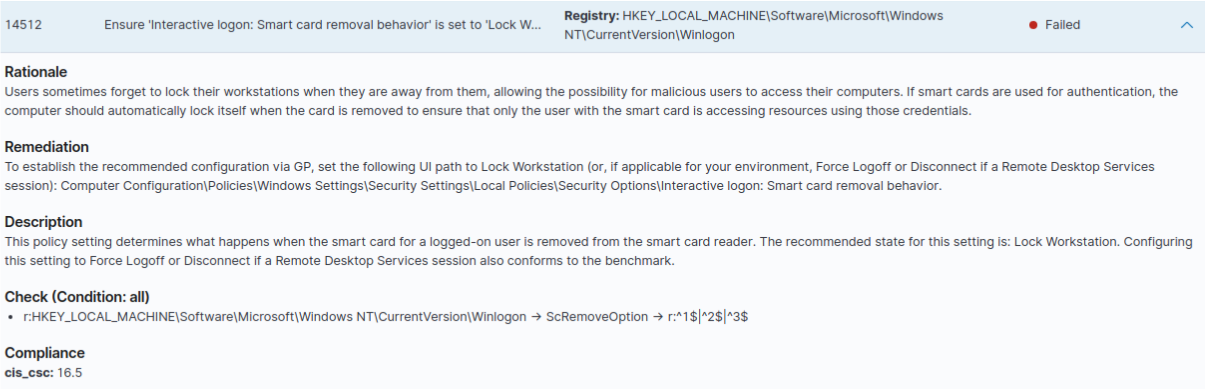
Base: ● Hexadecimal ○ Decimal

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
PlainTextPassword	REG_DWORD	0x00000000 (0)
ecuritySignature	REG_DWORD	0x00000001 (1)
omains	REG_MULTI_SZ	
eSecuritySignature	REG_DWORD	0x00000000 (0)
Dll	REG_EXPAND_SZ	%SystemRoot%\System32\wkssvc.dll
DllUnloadOnStop	REG_DWORD	0x00000001 (1)

Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanWorkstation\Parameters

---

14512 Ensure ‘Interactive logon: Smart card removal behavior’ is set to ‘Lock Workstation’ or higher



14512 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock W... **Registry:** HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon ● Failed

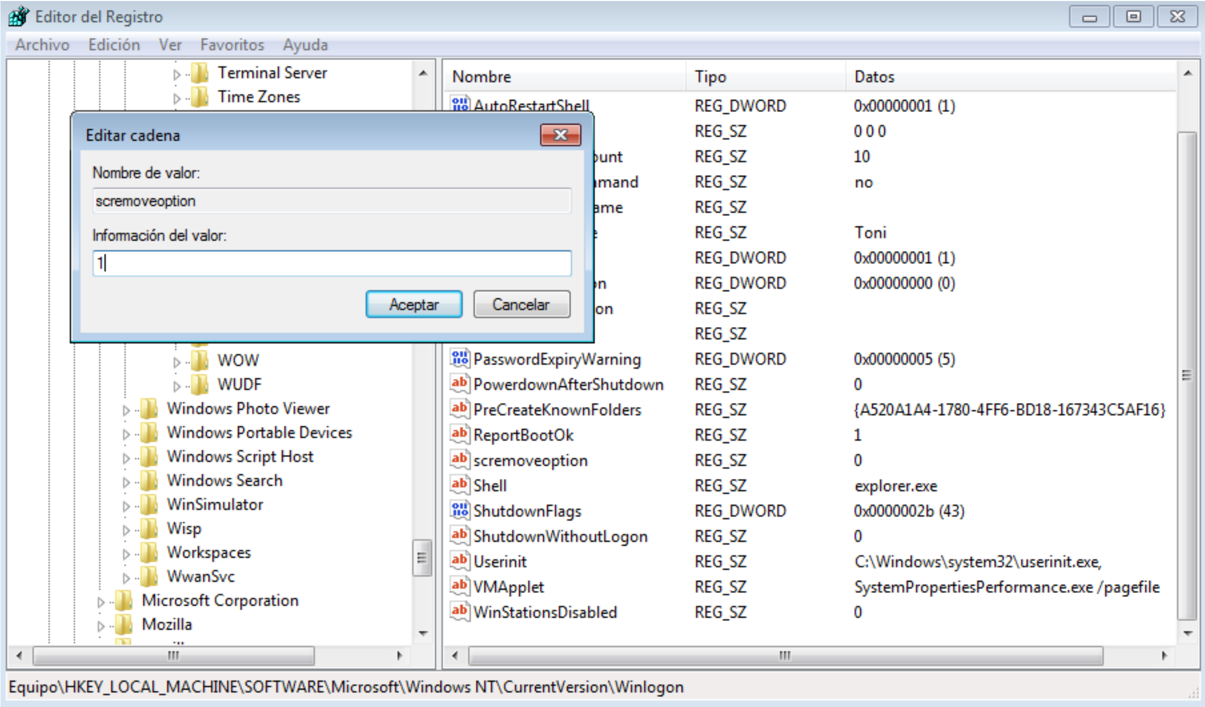
Rationale
Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

Remediation
To establish the recommended configuration via GP, set the following UI path to Lock Workstation (or, if applicable for your environment, Force Logoff or Disconnect if a Remote Desktop Services session): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior.

Description
This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: Lock Workstation. Configuring this setting to Force Logoff or Disconnect if a Remote Desktop Services session also conforms to the benchmark.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon → ScRemoveOption → r:^1$|^2$|^3$

Compliance
cis_csc: 16.5



Editar cadena

Nombre de valor: scremoveoption

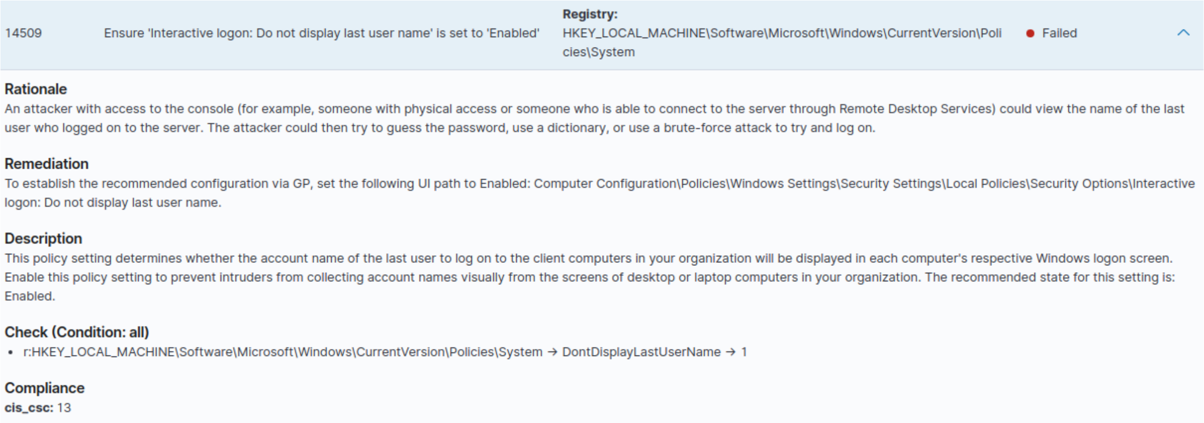
Información del valor: 1

Aceptar | Cancelar

Nombre	Tipo	Datos
AutoRestartShell	REG_DWORD	0x00000001 (1)
	REG_SZ	0 0 0
unt	REG_SZ	10
mand	REG_SZ	no
ame	REG_SZ	
	REG_SZ	Toni
	REG_DWORD	0x00000001 (1)
n	REG_DWORD	0x00000000 (0)
on	REG_SZ	
	REG_SZ	
PasswordExpiryWarning	REG_DWORD	0x00000005 (5)
PowerdownAfterShutdown	REG_SZ	0
PreCreateKnownFolders	REG_SZ	{A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
Shell	REG_SZ	explorer.exe
ShutdownFlags	REG_DWORD	0x0000002b (43)
ShutdownWithoutLogon	REG_SZ	0
Userinit	REG_SZ	C:\Windows\system32\userinit.exe,
VMApplet	REG_SZ	SystemPropertiesPerformance.exe /pagefile
WinStationsDisabled	REG_SZ	0

Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

14509 Ensure ‘Interactive logon: Do not display last user name’ is set to ‘Enabled’



14509 Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' **Registry:** HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System ● Failed

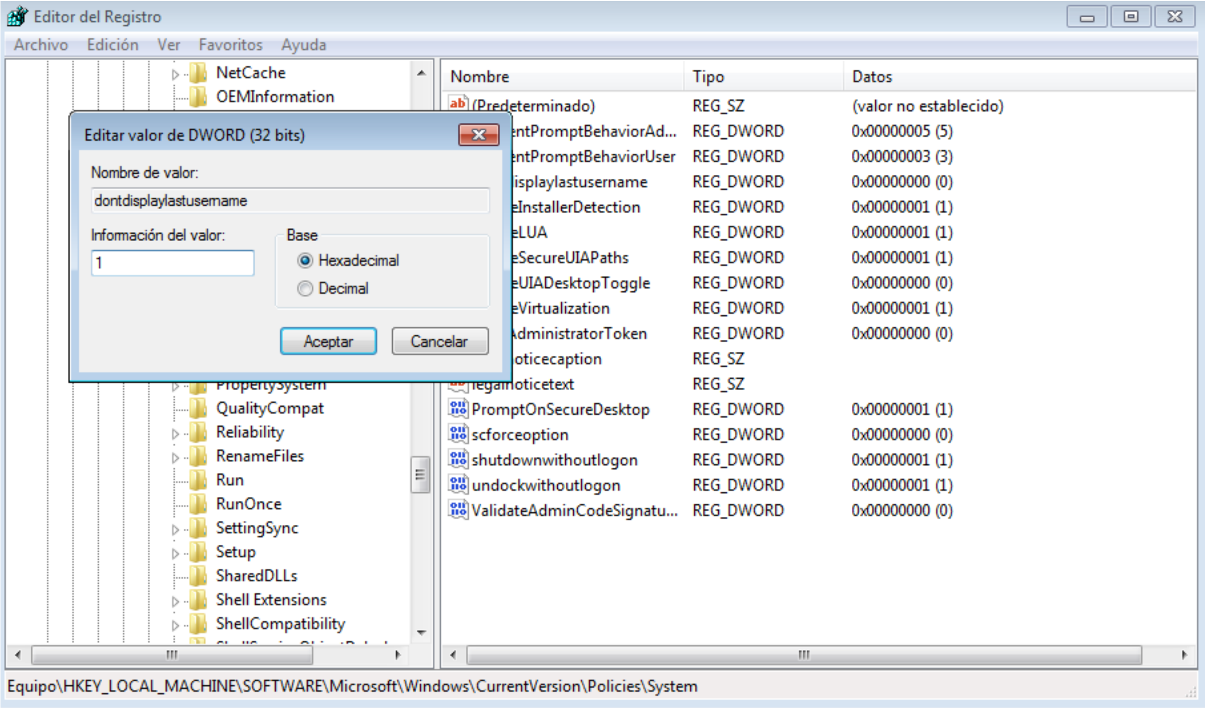
Rationale
An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Remote Desktop Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Remediation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name.

Description
This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: Enabled.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System → DontDisplayLastUserName → 1

Compliance
cis_csc: 13



Editar valor de DWORD (32 bits)

Nombre de valor: dontdisplaylastusername

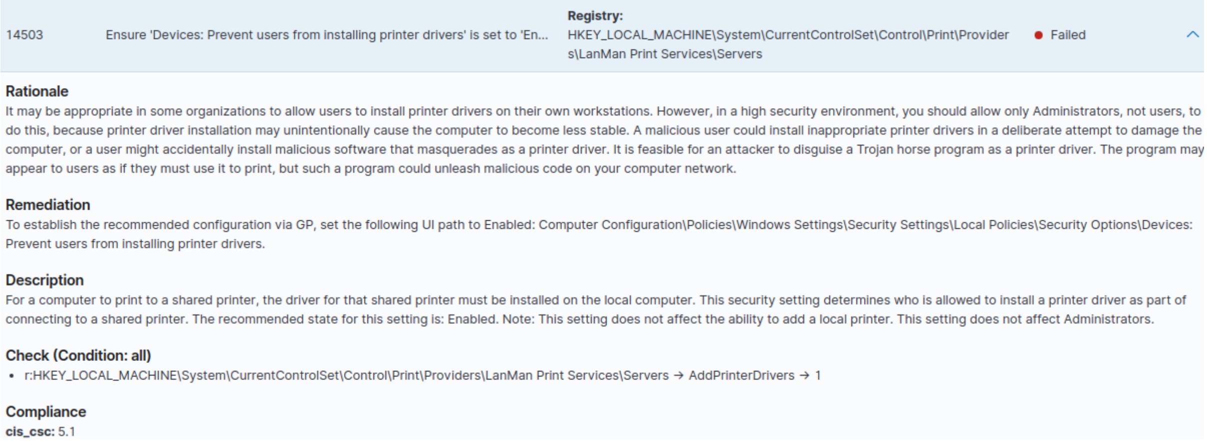
Información del valor: 1

Base: ● Hexadecimal ○ Decimal

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
ntPromptBehaviorAd...	REG_DWORD	0x00000005 (5)
ntPromptBehaviorUser	REG_DWORD	0x00000003 (3)
isplaylastusername	REG_DWORD	0x00000000 (0)
eInstallerDetection	REG_DWORD	0x00000001 (1)
eLUA	REG_DWORD	0x00000001 (1)
eSecureUIAPaths	REG_DWORD	0x00000001 (1)
eUIADesktopToggle	REG_DWORD	0x00000000 (0)
eVirtualization	REG_DWORD	0x00000001 (1)
dministratorToken	REG_DWORD	0x00000000 (0)
oticecaption	REG_SZ	
legalnoticetext	REG_SZ	
PromptOnSecureDesktop	REG_DWORD	0x00000001 (1)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwithoutlogon	REG_DWORD	0x00000001 (1)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatu...	REG_DWORD	0x00000000 (0)

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

14503 Ensure ‘Devices: Prevent users from installing printer drivers’ is set to ‘Enabled’



14503 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'En... **Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers ● Failed

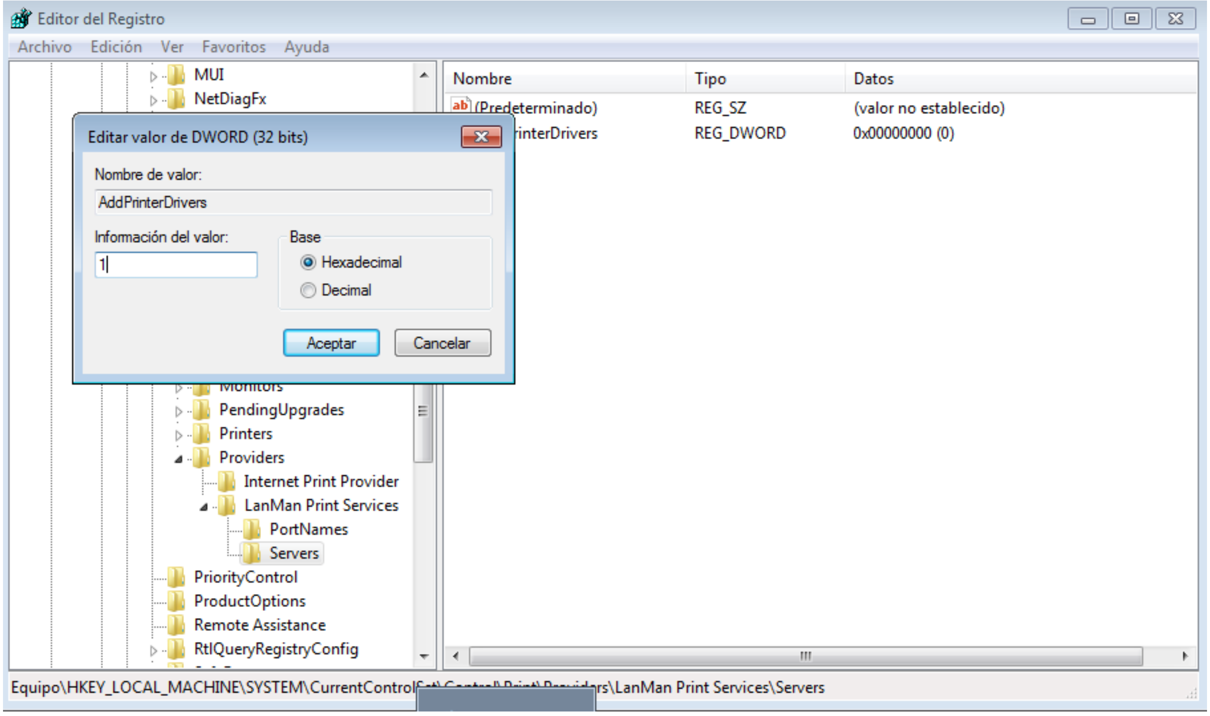
Rationale
It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, in a high security environment, you should allow only Administrators, not users, to do this, because printer driver installation may unintentionally cause the computer to become less stable. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious software that masquerades as a printer driver. It is feasible for an attacker to disguise a Trojan horse program as a printer driver. The program may appear to users as if they must use it to print, but such a program could unleash malicious code on your computer network.

Remediation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers.

Description
For a computer to print to a shared printer, the driver for that shared printer must be installed on the local computer. This security setting determines who is allowed to install a printer driver as part of connecting to a shared printer. The recommended state for this setting is: Enabled. Note: This setting does not affect the ability to add a local printer. This setting does not affect Administrators.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers → AddPrinterDrivers → 1

Compliance
cis_csc: 5.1



Editar valor de DWORD (32 bits)

Nombre de valor: AddPrinterDrivers

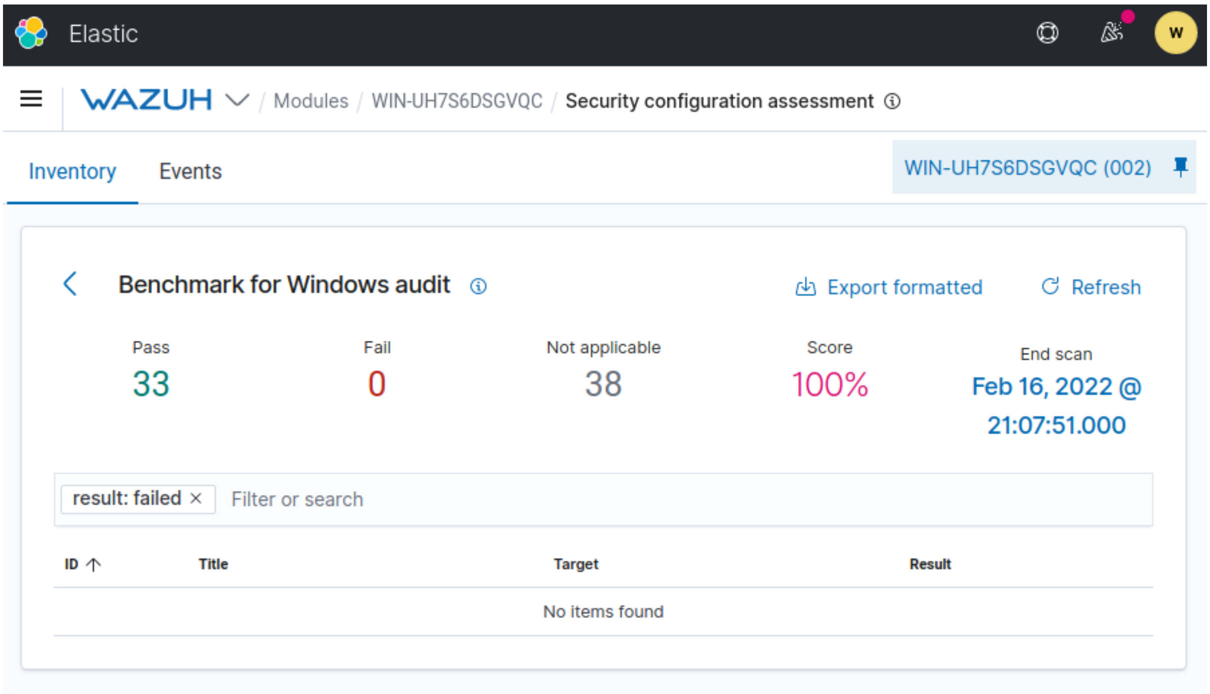
Información del valor: 1

Base: ● Hexadecimal ○ Decimal

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
rinterDrivers	REG_DWORD	0x00000000 (0)

Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl rs\LanMan Print Services\Servers

Once all the points have been corrected, we have the agent a little safer.



Elastic
W
WAZUH / Modules / WIN-UH7S6DSGVQC / Security configuration assessment
Inventory
Events
WIN-UH7S6DSGVQC (002)
Export formatted
Refresh

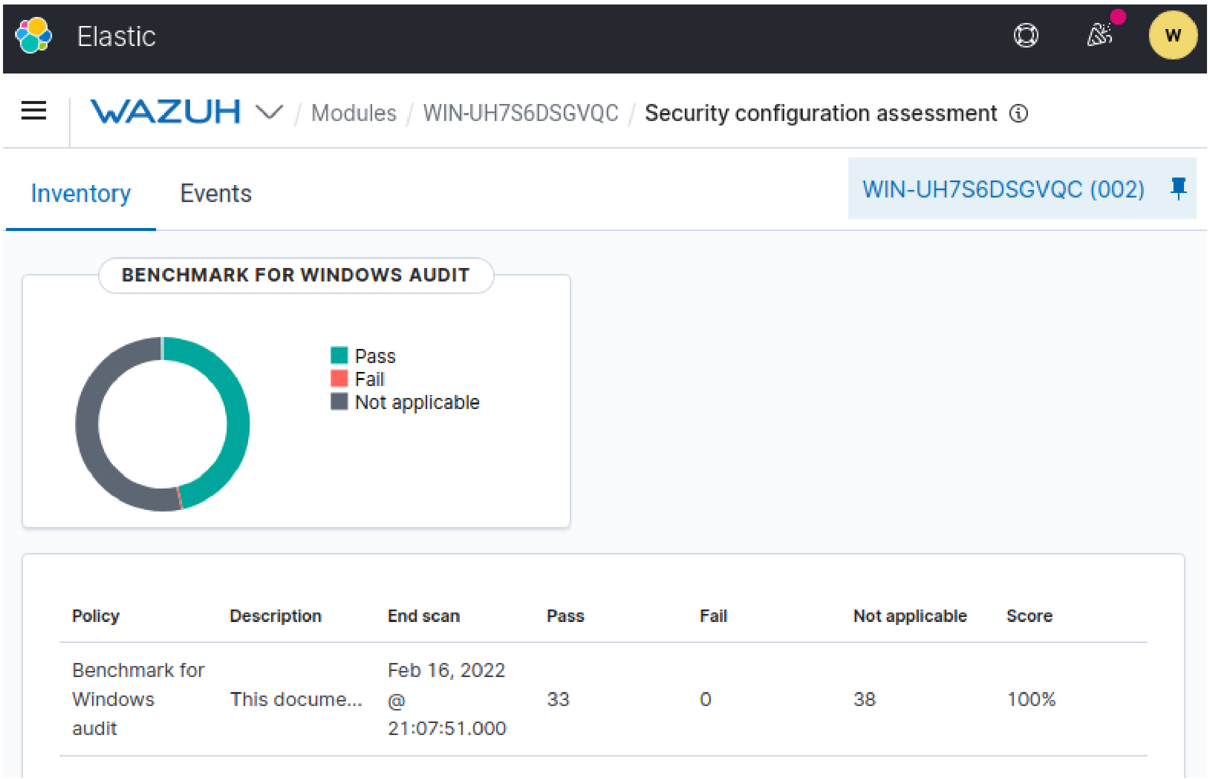
Benchmark for Windows audit

Pass	Fail	Not applicable	Score	End scan
33	0	38	100%	Feb 16, 2022 @ 21:07:51.000

result: failed × Filter or search

ID ↑	Title	Target	Result
No items found			

Figure 9: “SCA Inventory after corrections”


Elastic
WAZUH
Modules / WIN-UH7S6DSGVQC / Security configuration assessment
Inventory
Events
WIN-UH7S6DSGVQC (002)
BENCHMARK FOR WINDOWS AUDIT
🟩 Pass
🟥 Fail
⬛ Not applicable

Policy	Description	End scan	Pass	Fail	Not applicable	Score
Benchmark for Windows audit	This docume...	Feb 16, 2022 @ 21:07:51.000	33	0	38	100%

Figure 10: "SCA Dashboard after corrections"