



cesae
digital

Centro para o Desenvolvimento
de Competências Digitais

Trabalho de avaliação de CiberSegurança Ativa

Desenvolvido por

Ana Teixeira

Simão Oliveira

18 de setembro de 2023

Índice

- Observações
- Processo de instalação do Wazuh e clientes
- Correção dos erros de logs do Windows 10
- Correção dos erros de logs do Ubuntu
- Conclusão

Observações

O IP foi sendo alterado devido à utilização de diferentes ovas.

Processo de instalação do wazuh e Clientes

Durante o processo de instalação do Wazuh, deparamo-nos com um desafio inicial que exigiu a instalação manual de um pacote. Procedemos da seguinte forma:

```
root@anaserver:~# apt install apt-transport-https
```

```
root@anaserver:~# curl -s0 https://packages.wazuh.com/4.5/wazuh-install.sh && bash ./wazuh-install.sh -a
14/09/2023 10:29:28 INFO: Starting Wazuh installation assistant. Wazuh version: 4.5.2
14/09/2023 10:29:28 INFO: Verbose logging redirected to /var/log/wazuh-install.log
14/09/2023 10:29:31 INFO: Wazuh web interface port will be 443.
14/09/2023 10:29:33 INFO: Wazuh repository added.
14/09/2023 10:29:33 INFO: --- Configuration files ---
14/09/2023 10:29:33 INFO: Generating configuration files.
14/09/2023 10:29:34 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
14/09/2023 10:29:34 INFO: --- Wazuh indexer ---
14/09/2023 10:29:34 INFO: Starting Wazuh indexer installation.
14/09/2023 10:30:34 INFO: Wazuh indexer installation finished.
14/09/2023 10:30:34 INFO: Wazuh indexer post-install configuration finished.
14/09/2023 10:30:34 INFO: Starting service wazuh-indexer.
14/09/2023 10:30:43 INFO: wazuh-indexer service started.
14/09/2023 10:30:43 INFO: Initializing Wazuh indexer cluster security settings.
14/09/2023 10:30:54 INFO: Wazuh indexer cluster initialized.
14/09/2023 10:30:54 INFO: --- Wazuh server ---
14/09/2023 10:30:54 INFO: Starting the Wazuh manager installation.
```

```
14/09/2023 10:32:03 INFO: Wazuh manager installation finished.
14/09/2023 10:32:03 INFO: Starting service wazuh-manager.
14/09/2023 10:32:17 INFO: wazuh-manager service started.
14/09/2023 10:32:17 INFO: Starting Filebeat installation.
14/09/2023 10:32:22 INFO: Filebeat installation finished.
14/09/2023 10:32:25 INFO: Filebeat post-install configuration finished.
14/09/2023 10:32:25 INFO: Starting service filebeat.
14/09/2023 10:32:26 INFO: filebeat service started.
14/09/2023 10:32:26 INFO: --- Wazuh dashboard ---
14/09/2023 10:32:26 INFO: Starting Wazuh dashboard installation.
14/09/2023 10:33:25 INFO: Wazuh dashboard installation finished.
14/09/2023 10:33:25 INFO: Wazuh dashboard post-install configuration finished.
14/09/2023 10:33:25 INFO: Starting service wazuh-dashboard.
14/09/2023 10:33:26 INFO: wazuh-dashboard service started.
14/09/2023 10:33:40 INFO: Initializing Wazuh dashboard web application.
14/09/2023 10:33:41 INFO: Wazuh dashboard web application initialized.
14/09/2023 10:33:41 INFO: --- Summary ---
14/09/2023 10:33:41 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: PPTsvR56fwBD1IPm1woEPZ*d+79yKiZX
14/09/2023 10:33:41 INFO: Installation finished.
```

```
root@anaserver:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f8:04:85 brd ff:ff:ff:ff:ff:ff
        inet 192.168.107.196/16 metric 100 brd 192.168.255.255 scope global dynamic enp0s3
            valid_lft 691077sec preferred_lft 691077sec
        inet6 fe80::a00:27ff:fe8:485/64 scope link
            valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:7b:d2:db brd ff:ff:ff:ff:ff:ff
```

Verificamos o IP de modo a inserir o url correto no browser e, enquanto estudantes de cibersegurança, decidimos que o primeiro passo evidente seria alterar a password default.

The screenshot shows a password reset interface for the 'admin' user. It includes fields for 'Current password', 'New password', and 'Re-enter new password'. A red error message at the bottom states: 'Failed to reset password. {"status": "FORBIDDEN", "message": "Resource 'admin' is read-only."}'.

Reset password for "admin"

Current password

New password

Re-enter new password

Failed to reset password. {"status": "FORBIDDEN", "message": "Resource 'admin' is read-only."}

Cancel Reset

Não sendo possível fazer a alteração no dashboard, procuramos no google e fizemos a alteração diretamente na máquina virtual servidor:

```
root@anaserver:~# curl -so wazuh-passwords-tool.sh https://packages.wazuh.com/4.4/wazuh-passwords-tool.sh
root@anaserver:~# bash wazuh-passwords-tool.sh -u admin -p cesae123
14/09/2023 10:58:22 ERROR: The password must have a length between 8 and 64 characters and contain at least one upper and lower case letter, a number and a symbol(.+?=-).
root@anaserver:~# bash wazuh-passwords-tool.sh -u admin -p Cesae123456789
14/09/2023 10:58:33 ERROR: The password must have a length between 8 and 64 characters and contain at least one upper and lower case letter, a number and a symbol(.+?=-).
root@anaserver:~# bash wazuh-passwords-tool.sh -u admin -p Cesae123456789!
14/09/2023 10:58:40 ERROR: The password must have a length between 8 and 64 characters and contain at least one upper and lower case letter, a number and a symbol(.+?=-).
root@anaserver:~# bash wazuh-passwords-tool.sh -u admin -p Cesae123456789?
14/09/2023 10:59:17 INFO: Generating password hash
14/09/2023 10:59:19 WARNING: Password changed. Remember to update the password in the Wazuh dashboard and Filebeat nodes if necessary, and restart the services.
root@anaserver:~# bash wazuh-passwords-tool.sh -u admin -p Cesae123456789?
14/09/2023 10:59:29 INFO: Generating password hash
14/09/2023 10:59:32 WARNING: Password changed. Remember to update the password in the Wazuh dashboard and Filebeat nodes if necessary, and restart the services.
root@anaserver:~#
```

De seguida, procedemos à inserção de máquinas clientes no sistema. Começamos pelo Ubuntu.

The screenshots show the Wazuh agent deployment process. The first screenshot captures steps 1 through 4: choosing the operating system (Ubuntu), version (Ubuntu 15+), architecture (x86_64), and the Wazuh server address (192.168.107.196). Step 5 (Optional settings) is partially visible. The second screenshot continues the process through steps 5, 6, and 7: assigning an agent name (UbuntuAnaSimao), selecting a group (default), and providing an install command. A yellow warning box in step 5 states: "The agent name must be unique. It can't be changed once the agent has been enrolled." The final step, starting the agent, is shown in the Systemd tab.

```

[+] Cliente Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

anaserver login: root
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-83-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 System information as of Thu Sep 14 10:13:20 AM UTC 2023

 System load: 0.0166015625 Processes: 120
 Usage of /: 23.0% of 20.99GB Users logged in: 0
 Memory usage: 9% IPv4 address for enp0s3: 192.168.107.218
 Swap usage: 0%

91 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Thu Sep 14 10:00:09 UTC 2023 on tty1
root@anaserver:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8c:59:24 brd ff:ff:ff:ff:ff:ff
        inet 192.168.107.218/16 metric 100 brd 192.168.255.255 scope global dynamic enp0s3
            valid_lft 782sec preferred_lft 782sec
        inet6 fe80::a00:27ff:fe8c:5924/64 scope link
            valid_lft forever preferred_lft forever
root@anaserver:~# _

root@anaserver:~# curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.5.2-1_amd64.deb && sudo WAZUH_MANAGER='192.168.107.196' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='UbuntuAnaSimao' dpkg -i ./wazuh-agent.deb
Selecting previously unselected package wazuh-agent.
(Reading database ... 74177 files and directories currently installed.)
Preparing to unpack ./wazuh-agent.deb ...
Unpacking wazuh-agent (4.5.2-1) ...
Setting up wazuh-agent (4.5.2-1) ...

root@anaserver:~# sudo systemctl daemon-reload
root@anaserver:~# sudo systemctl enable wazuh-agent
Synchronizing state of wazuh-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
root@anaserver:~# systemctl start wazuh-agent.service

```

Para o Win10, primeiro tentamos instalar usando a powershell.

```

Windows 10 - ciber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Writing web request
    Writing request stream... (Number of bytes written: 1664218)

nt-4.5.2-1.msi -OutFile ${env:tmp}\wazuh-agent.msi; msisexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.107.196' WAZUH_REGISTRATION_SERVER='192.168.107.196' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='WinAnaSimao'
Invoke-WebRequest : The remote name could not be resolved: 'packages.wazuh.com'
At line:1 char:1
+ Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-a ...
+ ~~~~~
+     CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
+     FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

PS C:\Users\Ana> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.5.2-1.msi -OutFile ${env:tmp}\wazuh-agent.msi; msisexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.107.196' WAZUH_REGISTRATION_SERVER='192.168.107.196' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='WinAnaSimao'

```

Não deu e fomos ver a documentação no site oficial do wazuh: <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html>

Instalamos através <https://packages.wazuh.com/4.x/windows/wazuh-agent-4.5.2-1.msi>

File Explorer showing the contents of C:\Program Files (x86)\ossec-agent:

Name	Date modified	Type	Size
last-ossec.conf	9/14/2023 12:48 PM	CONF File	10 KB
libgcc_s_dw2-1.dll	9/5/2023 9:52 AM	Application exten...	145 KB
libstdc++-6.dll	9/5/2023 9:52 AM	Application exten...	2,303 KB
libwazuhext.dll	9/5/2023 9:52 AM	Application exten...	7,158 KB
libwazuhshared.dll	9/5/2023 9:52 AM	Application exten...	1,147 KB
libwinpthread-1.dll	9/5/2023 9:52 AM	Application exten...	518 KB
LICENSE	9/5/2023 7:46 AM	Text Document	25 KB
local_internal_options.conf	9/5/2023 7:46 AM	CONF File	1 KB
manage_agents	9/5/2023 9:52 AM	Application	1,361 KB
ossec.conf	9/14/2023 12:50 PM	CONF File	10 KB
ossec	9/14/2023 12:52 PM	Text Document	30 KB
profile-10.template	9/5/2023 7:28 AM	TEMPLATE File	1 KB
REVISION	9/5/2023 7:46 AM	File	1 KB
rsync.dll	9/5/2023 9:52 AM	Application exten...	310 KB
syscollector.dll	9/5/2023 9:52 AM	Application exten...	487 KB
sysinfo.dll	9/5/2023 9:52 AM	Application exten...	448 KB
VERSION	9/5/2023 7:46 AM	File	1 KB
vista_sec	9/5/2023 7:28 AM	Text Document	92 KB
wazuh-agent	9/5/2023 9:52 AM	Application	2,350 KB
wazuh-agent.state	9/14/2023 12:52 PM	STATE File	1 KB
win32ui	9/5/2023 9:52 AM	Application	1,287 KB
win32ui.exe.manifest	9/5/2023 7:28 AM	MANIFEST File	1 KB
wpk_root.pem	9/5/2023 7:28 AM	PEM File	2 KB

Só a meio nos apercebemos que o problema era a máquina estar em NAT. Alteramos para bridged adapter.

Services window showing the Wazuh service status:

Name	Description	Status	Startup Type	Log On As
Wazuh	Wazuh Windows Agent	Running	Automatic	Local System
WalletService	Hosts objec...	Manual	Local Syst...	
WarpITSvc	Provides a J...	Manual (Trig...	Local Service	
Wazuh	Wazuh Win...	Running	Automatic	Local Syst...
Web Account Manager	This service ...	Running	Manual	Local Syst...
WebClient	Enables Win...	Manual (Trig...	Local Service	
Wi-Fi Direct Services Conne...	Manages co...	Manual (Trig...	Local Service	
Windows Audio	Manages au...	Running	Automatic	Local Service
Windows Audio Endpoint B...	Manages au...	Running	Automatic	Local Syst...
Windows Backup	Provides Wi...	Running	Manual	Local Syst...
Windows Biometric Service	The Windo...	Manual (Trig...	Local Syst...	
Windows Camera Frame Se...	Enables mul...	Manual (Trig...	Local Syst...	
Windows Connect Now - C...	WCNCSV...	Manual	Local Syst...	
Windows Connection Mana...	Makes auto...	Running	Automatic (T...	Local Syst...
Windows Defender Advanc...	Windows D...	Running	Manual	Local Syst...
Windows Defender Firewall	Windows D...	Running	Automatic	Local Syst...
Windows Encryption Provid...	Windows E...	Manual (Trig...	Local Syst...	
Windows Error Reporting Se...	Allows error...	Manual (Trig...	Local Syst...	
Windows Event Collector	This service ...	Running	Manual	Netwo...
Windows Event Log	This service ...	Running	Automatic	Local Syst...
Windows Font Cache Service	Optimizes p...	Running	Automatic	Local Syst...
Windows Image Acquisitio...	Provides im...	Manual	Local Syst...	
Windows Insider Service	Provides inf...	Running	Manual (Trig...	Local Syst...
Windows Installer	Adds, modifi...	Running	Manual	Local Syst...
Windows License Manager ...	Provides inf...	Running	Manual (Trig...	Local Syst...
Windows Management Inst...	Provides a c...	Running	Automatic	Local Syst...

A modal window for the Wazuh service shows the configuration:

- Manager IP: 192.168.107.196
- Authentication key: MD5|ERFU0IUT1AI+MTFRSM:
- Status: Running

Wazuh Agents interface showing agent status and evolution:

STATUS

- Active (2)
- Disconnected (0)
- Pending (0)
- Never connected (0)

DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
2	0	0	0	100.00%

Last registered agent: DESKTOP-1IQJ387

Most active agent: UbuntuAnaSimao

EVOLUTION

Last 24 hours

Graph showing agent activity over time.

Agents (2)

ID	Name	IP address	Group(s)	Operating system	Cluster mode	Version	Status	Actions
001	UbuntuAnaSimao	192.168.107.197	default	Ubuntu 22.04.3 LTS	node01	v4.5.2	active	
002	DESKTOP-1IQJ387	192.168.107.227	default	Microsoft Windows 10 Pro 10.0.19042.631	node01	v4.5.2	active	

Correção dos erros de logs do Windows 10

Começamos por tratar dos erros do Windows 10. Como ilustrado, foram verificadas 261 falhas.



O primeiro erro corrigido foi garantir que um utilizador só pode utilizar a mesma password depois de 24 passwords únicas.

This screenshot shows the configuration details for the CIS rule 'Ensure 'Enforce password history' is set to '24 or more password(s)'. It includes sections for Rationale, Remediation, Description, Check (Condition: all), Compliance, and CIS score.

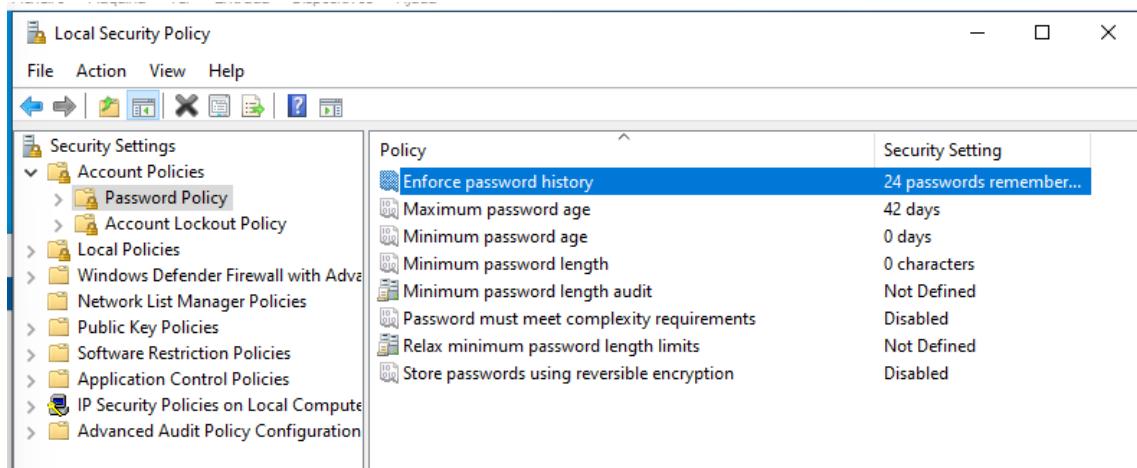
Rationale:
The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Remediation:
To establish the recommended configuration via GPO, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history

Description:
This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is 24 or more password(s). Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSO), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center. Note #2: As of the publication of this benchmark, Microsoft currently has a maximum limit of 24 saved passwords. For more information, please visit Enforce password history Windows 10 - Windows security | Microsoft Docs.

Check (Condition: all)
• c:\net.exe accounts > nLength of password history maintained:\s+(\d+)\ compare >= 24

Compliance
els: 1.1.1
cis_csc: 5.2



A próxima política implementada foi no âmbito da segurança da password. Estabeleceu-se o tempo mínimo de uso de uma password, garantindo que o número fosse superior a 0, neste caso 1.

15502 Ensure 'Minimum password age' is set to '1 or more day(s)'.

Command: net.exe accounts

• Failed

Rationale
Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual's user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

Remediation
To establish the recommended configuration via GPO, set the following UI path to 1 or more day(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age

Description
This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: 1 or more day(s). Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Check (Condition: all)

- c:\net.exe accounts > n\Minimum password age \((days)\)\s+\((d+)\) compare >> 1

Compliance

cis:1.1.3
cis_ecsc:5.2

Policy	Security Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	14 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Relax minimum password length limits	Enabled
Store passwords using reversible encryption	Disabled

Estabeleceu-se o comprimento de uma password para 14 caracteres, como forma de garantir uma complexidade minima, dificultando ataques de força bruta.

15503 Ensure 'Minimum password length' is set to '14 or more character(s)'.

Command: net.exe accounts

● Failed

Rationale
Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Remediation
To establish the recommended configuration via GP, set the following UI path to 14 or more character(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies>Password Policy\Minimum password length

Description
This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps 'passphrase' is a better term than 'password.' In Microsoft Windows 2000 and newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as 'I want to drink a \$5 milkshake' is a valid passphrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: 14 or more character(s). Note: In Windows Server 2016 and older versions of Windows Server, the GUI for the Local Security Policy (LSP), Local Group Policy Editor (LGPE) and Group Policy Management Editor (GPE) would not let you set this value higher than 14 characters. However, starting with Windows Server 2019, Microsoft changed the GUI to allow up to a 20 character minimum password length. Note #2: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Check (Condition: all)

- c:\net.exe accounts > n\Minimum password length\ls+(d+) compare >= 14

Compliance
cis: 1.1.6
cis_csc: 5.2

Policy	Security Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	14 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Relax minimum password length limits	Enabled
Store passwords using reversible encryption	Disabled

Ao ativar (enable) a seguinte “feature” reforçamos novamente a segurança da password, afetando apenas contas locais.

15505 Ensure 'Relax minimum password length limits' is set to 'Enabled'.

Registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SAM

● Failed

Rationale
This setting will enable the enforcement of longer and generally stronger passwords or passphrases where MFA is not in use.

Remediation
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies>Password Policy\Relax minimum password length limits. Note: This setting is only available within the built-in OS security template of Windows 10 Release 2004 and Server 2022 (or newer), and is not available via older versions of the OS, or via downloadable Administrative Templates (ADMX/ADML). Therefore, you must use a Windows 10 Release 2004 or Server 2022 system (or newer) to view or edit this setting with the Group Policy Management Console (GPMC) or Group Policy Management Editor (GPE).

Description
This policy setting determines whether the minimum password length setting can be increased beyond the legacy limit of 14 characters. For more information please see the following Microsoft Security Blog. The recommended state for this setting is: Enabled. Note: This setting only affects local accounts on the computer. Domain accounts are only affected by settings on the Domain Controllers, because that is where domain accounts are stored.

Checks (Condition: all)

- r\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SAM
- r\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SAM > RelaxMinimumPasswordLengthLimits
- t\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SAM > RelaxMinimumPasswordLengthLimits > 1

Compliance
cis: 1.1.6
cis_csc: 5.2

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Fixamos o número mínimo de vezes que o utilizador pode falhar o seu logon em cinco, que é o recomendado (substituindo o valor anterior que era zero).

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Acrescentamos uma política que previne que o utilizador acrescente uma nova conta da Microsoft ou fazer logon numa outra.

15510 Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'.

Rationale
Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used to log onto their computers will probably want to block Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

Remediation
To establish the recommended configuration via GP, set the following UI path to Users can't add or log on with Microsoft accounts: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts

Description
This policy setting prevents users from adding new Microsoft accounts on this computer. The recommended state for this setting is: Users can't add or log on with Microsoft accounts.

Checks (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\System -> NoConnectedUser
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> NoConnectedUser -> 3

Compliance
cis: 2.3.1.2
pol_dss: 8.1
tsc: CC6.1

Policy	Security Setting
Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d	Enabled

Policy	Security Setting
Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Users can't add or log o...
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined

Existem termos bastante utilizados em ataques por serem credenciais comuns, um dos quais é guest. Tendo isto em mente, decidimos renomear a conta convidado para simao, sendo desta forma mais difícil para pessoas não autorizadas acederem à máquina.

15514 Configure Accounts: Rename guest account.

Rationale
The Guest account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Remediation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Setting\Local Policies\Security Options\Accounts: Rename guest account

Description
The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security.

Check (Condition: all)
• cmd user guest >> r.The user name could not be found.

Compliance
cis 2.3.1.6
cis_esc: 4.7

Policy	Security Setting
Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Users can't add or log on
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled

File Action View Help

Accounts: Rename guest account Properties

Local Security Setting Explain

Accounts: Rename guest account

simao

OK Cancel Apply

Security Setting
Disabled
Users can't add or log on
Disabled
Enabled
Administrator
simao
Disabled
Disabled
Not Defined
Disabled
Not Defined
Not Defined
Enabled
Not Defined
Disabled
Not Defined
Enabled

Policy	Security Setting
Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Users can't add or log on
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	simoao
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled

Através de uma política de grupo, prevenimos que os utilizadores possam instalar impressoras, deixando essa regalia para administradores. Assim, evita-se que dispositivos desconhecidos sejam conectados à rede.

15518 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

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.

Checks (Condition: all)

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers → AddPrinterDrivers
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers → AddPrinterDrivers → 1

Compliance

cis: 2.3.4
nist_800_53: CM.1
pci_dss: 2.2.4.2.2.5
tsc: C06.3,C05.2

The screenshot shows the Windows Local Security Policy Editor interface. The left pane displays a tree view of security settings, and the right pane shows a list of policies with their current values.

Left Pane (Tree View):

- Security Settings
 - Account Policies
 - Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options** (selected)
 - Windows Defender Firewall with Advanced Security
 - Network List Manager Policies
 - Public Key Policies
 - Software Restriction Policies
 - Application Control Policies
 - IP Security Policies on Local Computer
 - Advanced Audit Policy Configuration

Right Pane (List of Policies):

Policy	Security Setting
Audit: Force audit policy subcategory settings (Windows Vista and later)	Not Defined
Audit: Shut down system immediately if unable to log secure	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...)	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Disabled

Bottom Window (Properties for Devices: Prevent users from installing printer drivers):

Local Security Setting Explain

Devices: Prevent users from installing printer drivers

Enabled

Disabled

OK Cancel Apply

Security Setting

- Not Defined
- Disabled
- Not Defined
- Not Defined
- Enabled
- Not Defined
- Disabled
- Not Defined
- Enabled
- Enabled
- Enabled
- Disabled
- 30 days
- Enabled
- Not Defined
- Not Defined
- Disabled

Policy	Security Setting
Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Users can't add or log on with Microsoft accounts
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	simao
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled

Para prevenir ataques de força bruta, é recomendado estabelecer uma duração da password superior a 0 e inferior a 30 dias. Optamos por 10 dias.

15523 Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'. Command: net.exe accounts • Failed

Rationale
In Active Directory-based domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker will have more time to undertake a brute force attack to guess the password of one or more computer accounts.

Remediation
To establish the recommended configuration via GP, set the following UI path to 30 or fewer days, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age.

Description
This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days. If you increase this interval significantly so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts. The recommended state for this setting is: 30 or fewer days, but not 0. Note: A value of 0 does not conform to the benchmark as it disables maximum password age. Note #2: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Checks (Condition: all)

- c:\net.exe accounts -r:Maximum password age (days);(s+)(d+) compare <= 30
- c:\net.exe accounts -r:Maximum password age (days);(s+)(d+) compare > 0

Compliance
cis: 2.3.6.5

Policy	Security Setting
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Disabled

Screenshot showing the Local Security Settings dialog box and the Group Policy Management Editor.

Local Security Settings Dialog Box:

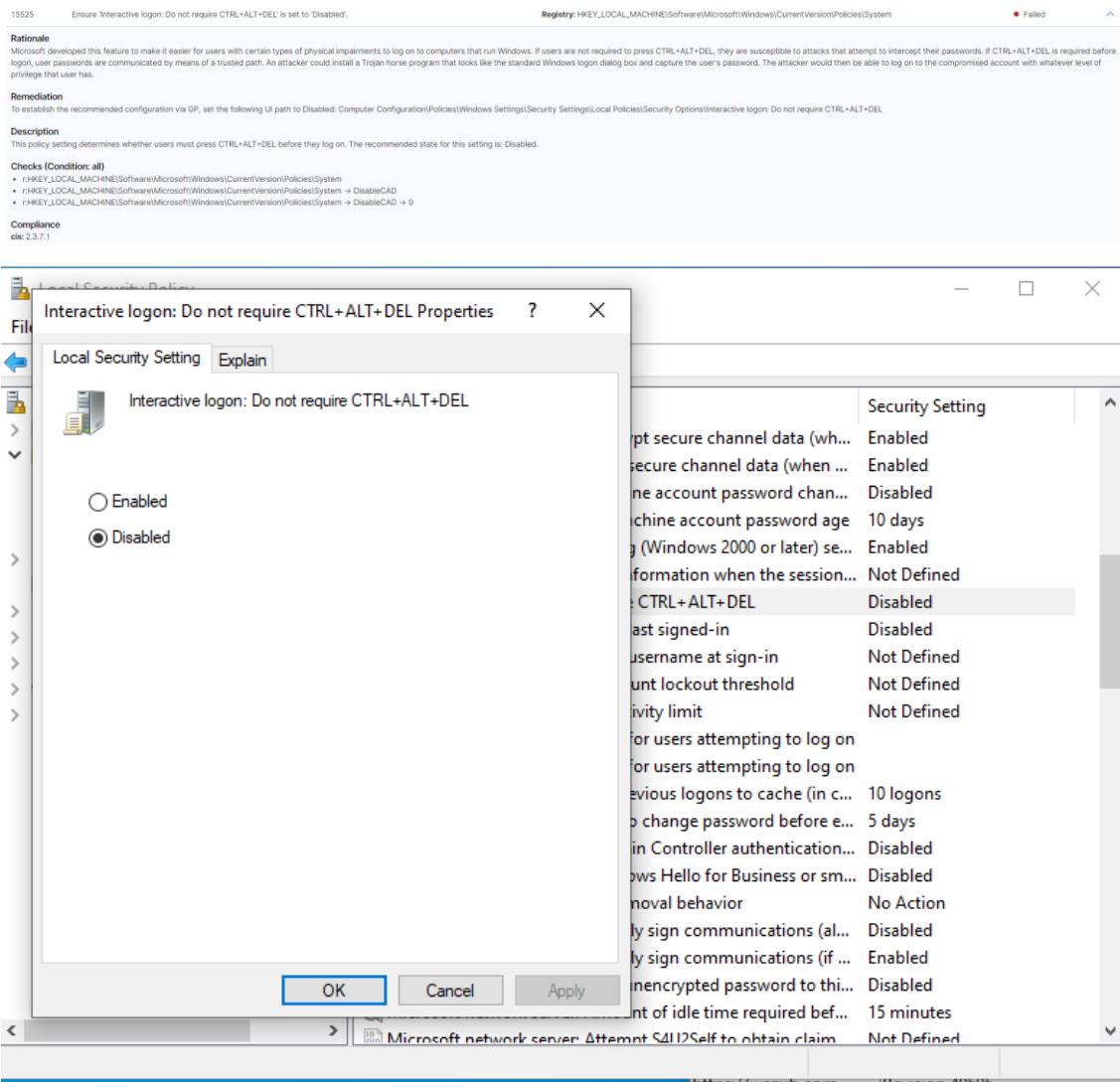
Setting	Value
Domain member: Maximum machine account password age	10 days

Group Policy Management Editor:

Policy	Security Setting
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...)	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	

A combinação Ctrl+Alt+Del é frequentemente usada como um atalho para funções de segurança, como o gerenciador de tarefas ou a tela de bloqueio. Desabilitá-la pode simplificar a experiência do utilizador, tornando o sistema mais amigável. Ao desabilitar a combinação Ctrl+Alt+Del, é

importante considerar a implementação de outras medidas de segurança para compensar. Isso pode incluir políticas de senha robustas, autenticação de dois fatores e controles de acesso apropriados. A política encontrava-se not defined.



Para impedir que um novo utilizador veja quem foi o último utilizador a fazer login definimos esta política para “don’t display last signed-in”, “enabled”.

15526 Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'. ● 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: Don't display last signed-in. Note: In older versions of Microsoft Windows, this setting was named interactive logon: Do not display last user name, but it was renamed starting with Windows 10 Release 1703.

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.

Checks (Condition: all)

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System → DontDisplayLastUserName
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System → DontDisplayLastUserName → 1

Compliance

clc:2.3.7.2
pdr:IV_35.7.d
gpp:19.4.3
hipax:164.312.b
nist:800_53-CM.1
pcd_dsc:2.2.3
tsc:CCS.2

Policy	Security Setting
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password change	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) session key exchange	Enabled
Interactive logon: Display user information when the session begins	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in case of a password change)	10 logons
Interactive logon: Prompt user to change password before every logon	5 days
Interactive logon: Require Domain Controller authentication	Disabled
Interactive logon: Require Windows Hello for Business or similar	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if possible)	Enabled
Microsoft network client: Send unencrypted password to third parties	Disabled
Microsoft network server: Amount of idle time required before disconnecting a session	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim	Not Defined

Interactive logon: Don't display last signed-in Properties

Local Security Setting Explain

Enabled
 Disabled

	Security Setting
Accept secure channel data (when ...)	Enabled
Accept secure channel data (when ...)	Enabled
Change account password chan...	Disabled
Machine account password age	10 days
Require strong (Windows 2000 or later) se...	Enabled
Information when the session...	Not Defined
Do not require CTRL+ALT+DEL	Disabled
Don't display last signed-in	Enabled
Display username at sign-in	Not Defined
Machine account lockout threshold	Not Defined
Machine inactivity limit	Not Defined
Message text for users attempting to log on	Not Defined
Number of previous logons to cache (in c...)	10 logons
Number of days before a user is prompted to change password before e...	5 days
Prevent logon to domain Controller authentication...	Disabled
Allow users to log on with Hello for Business or sm...	Disabled
Do not allow multiple logon behavior	No Action
Do not allow multiple logon communications (al...	Disabled
Do not allow multiple logon communications (if ...)	Enabled
Do not encrypt password to thi...	Disabled
Time limit for idle time required bef...	15 minutes
Message text for users attempting to log on	Not Defined

OK Cancel Apply

Microsoft network server Attempt S4112Self to obtain claim

Security Settings

- Account Policies
 - Password Policy
 - Account Lockout Policy
- Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options
- Windows Defender Firewall with Adv...
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Policy	Security Setting
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...)	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	Not Defined

Para impedir ataques contínuos de tentativa de adivinhar uma password é recomendado colocar um limite de tentativas, neste caso 10. Já tínhamos aplicado esta política relativamente a contas, neste caso incide sobre a máquina.

Screenshot showing the Group Policy Management Editor and Local Security Settings Manager for configuring the 'Interactive logon: Machine account lockout threshold' policy.

Group Policy Management Editor:

- Path: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\System`
- Description: Ensure 'Interactive logon: Machine account lockout threshold' is set to '10 or fewer invalid logon attempts, but not 0'.
- Remediation: To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid logon attempts, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine account lockout threshold.
- Checks (Condition: all):
 - not HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\System → MaxDevicePasswordFailedAttempts → 0
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\System → MaxDevicePasswordFailedAttempts → 10
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\System → MaxDevicePasswordFailedAttempts → n<(id) compare <=30
- Compliance:
 - cis: 2.3.7.3
 - cis_esc: 4.10

Local Security Settings Manager:

The 'Interactive logon: Machine account lockout threshold' setting is configured to 10 invalid logon attempts.

Setting	Value		
Interactive logon: Machine account lockout threshold	10 invalid logon attempts		
OK	Cancel	Apply	
Apply			

Group Policy Objects (GPO) Editor:

The 'Interactive logon: Machine account lockout threshold' policy is set to 10 invalid logon attempts.

Policy	Security Setting
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...)	10 logons
Interactive logon: Prompt user to change password before e...	5 days

Para bloquear uma sessão, porque o utilizador esqueceu-se de fazer log-out, alteramos esta política de forma a automaticamente o fazer dentro de 900 segundos.

15528 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer seconds', but not 0'. Registry: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System Failed

Rationale
If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

Remediation
To establish the recommended configuration via GP, set the following UI path to 900 or fewer seconds, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit.

Description
Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session. The recommended state for this setting is: 900 or fewer second(s), but not 0. Note: A value of 0 does not conform to the benchmark as it disables the machine inactivity limit.

Checks (Condition: all)

- not r:\KEY\LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> InactivityTimeoutSecs -> 0
- r:\KEY\LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> InactivityTimeoutSecs
- r:\KEY\LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> InactivityTimeoutSecs -> n:"(d+)" compare <= 900

Compliance
cie: 2.3.7.4
cia_esc: 4.3
pcl_dsc: 8.1.8
tsc: C06.1

Local Security Policy

File Action View Help

Security Settings

Policy	Security Setting
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password change	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session begins	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in case of failure)	10 logons
Interactive logon: Prompt user to change password before enabling	5 days
Interactive logon: Require Domain Controller authentication	Disabled
Interactive logon: Require Windows Hello for Business or similar	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if available)	Enabled
Microsoft network client: Send unencrypted password to third parties	Disabled
Microsoft network server: Amount of idle time required before disconnecting a session	15 minutes
Microsoft network server: Attempt S4LIDSelf to obtain claim	Not Defined

Interactive logon: Machine inactivity limit Properties

Local Security Setting Explain

Machine will be locked after **900** seconds

Policy	Security Setting
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before a...	5 days
Interactive logon: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Interactive logon: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before a...	5 days

Microsoft network server Attempt S4112Self to obtain claim

Security Settings

- Account Policies
 - Password Policy
 - Account Lockout Policy
- Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options**
- Windows Defender Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Numa tentativa de prevenir ataques, é possível mostrar um “banner” no início da sessão de modo a advertir a pessoa que está a tentar aceder das consequências de utilização imprópria.

Configure Interactive logon: Message text for users attempting to log on:

Command: reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v legalnoticetext

• Failed

Rationale
Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons—for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

Remediation
To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon.

Description
This policy setting specifies a text message that displays to users when they log on. Set the following group policy to a value that is consistent with the security and operational requirements of your organization.

Check (Condition: all)

```
+ not creg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v legalnoticetext > nul&& legalnoticetext<=REG_SZ<=$
```

Compliance

Interactive logon: Message text for users attempting to log on

Local Policy Setting Explain

AUTHORIZED ACCESS ONLY

	Security Setting
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCESS ONLY
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before e...	5 days

Esta mensagem semelhante à anterior serve para mostrar um título no login para evitar ou prevenir utilizadores de cometerem erros ou de usarem erroneamente máquinas da empresa.

15530 Configure 'Interactive logon: Message title for users attempting to log on'.

Command: reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v legalnoticecaption

Rationale
Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

Remediation
To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message title for users attempting to log on

Description
This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Check (Condition: all)
not creg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v legalnoticecaption > r\\$+legalnoticecaption\\$+RE0_SZ\\$+S

Compliance
cis:2.3.7.6

Interactive logon: Message title for users attempting to log on

	Security Setting
Message title for users attempting to log on	HELLO
Number of previous logons to cache (in case domain controller is not available)	4
Interactive logon: Prompt user to change password before log on	5 days

File Action View Help

Security Settings

- Account Policies
 - Password Policy
 - Account Lockout Policy
- Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options
- Windows Defender Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Policy	Security Setting
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure channel binding token requirements	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (when ...)	Enabled
Domain member: Digitally encrypt secure channel data (when ...)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) session security	Enabled
Interactive logon: Display user information when the session begins	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCESS ONLY
Interactive logon: Message title for users attempting to log on	HELLO
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons
Interactive logon: Prompt user to change password before log on	5 days

Esta política estabelece a quantidade de utilizadores que o sistema manterá em cache no evento de uma falha do controlador de domínio. Neste cenário específico, o valor foi ajustado para quatro utilizadores.

15531 Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer...' Registry: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon ● Failed

Rationale
The number that is assigned to this policy setting indicates the number of users whose logon information the computer will cache locally. If the number is set to 4, then the computer caches logon information for 4 users. When a 5th user logs on to the computer, the server overwrites the oldest cached logon session. Users who access the computer console will have their logon credentials cached on that computer. An attacker who is able to access the file system of the computer could locate this cached information and use a brute force attack to attempt to determine user passwords. To mitigate this type of attack, Windows encrypts the information and obscures its physical location.

Remediation
To establish the recommended configuration via GP, set the following UI path to 4 or fewer logon(s): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available)

Description
This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a Domain Controller cannot be contacted. This policy setting determines the number of unique users for whom logon information is cached locally. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords. The recommended state for this setting is: 4 or fewer logon(s).

Checks (Condition: all)

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\+CachedLogonsCount
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\+CachedLogonsCount → n=(d+) compare <= 4

Compliance
clc:2.3.7
pel_dss:8.2
tsc:CC6.1

Interactive logon: Number of previous logons to cache (in case domain controller is not available)

Policy	Security Setting
Domain controller: Allow vulnerable Netlogon secure channel connections	Not Defined
Domain controller: LDAP server channel binding token requirements	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCESS HELLO
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	4 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Requiere Windows Hello for Business or smart card	Disabled

Esta política define o uso de um smart card para ser possível fazer logon. Ao retirar o smart card, automaticamente termina a sessão.

15533 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher.

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.

Checks (Condition: all)

- r:\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
- r:\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon \ ScRemoveOption
- r:\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon \ ScRemoveOption \ r:"1\\$12\\$

Compliance

cis: 2.3.7.9
cis_esc: 4.3
pol_desc: 8.6
tsc: C08.1

Policy	Security Setting
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCESS
Interactive logon: Message title for users attempting to log on	HELLO
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	4 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled

Policy	Security Setting
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	10 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	10 invalid logon attempts
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCESS
Interactive logon: Message title for users attempting to log on	HELLO
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	4 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled

Esta política tem como objetivo garantir que o protocolo SMB (Server Message Block) usado pelo cliente se mantenha em sincronia com as configurações e requisitos de segurança definidos no servidor. Essa sincronização é fundamental para prevenir acessos não autorizados ao servidor da empresa por indivíduos mal-intencionados. Quando o protocolo SMB não está devidamente

sincronizado, podem surgir vulnerabilidades que permitiriam a um atacante explorar falhas de segurança e obter acesso não autorizado aos recursos do servidor.

19534 Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'. 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 intercept, edit, 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.

Checks (Condition: all)

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters \> RequireSecuritySignature
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters \> RequireSecuritySignature \> 1

Compliance
sts: 2.3.8.1
https://164.312.a.2/I4/164.312.a.1/164.312.a.2/I164.312.a.2/I
nist_800_53_SC.8
pd_dsc: 4.1
tscc: C06.1,C06.7,C07.2

Policy	Security Setting
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCE
Interactive logon: Message title for users attempting to log on	HELLO
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	4 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled

Policy	Security Setting
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCE
Interactive logon: Message title for users attempting to log on	HELLO
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	4 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled

Esta política, semelhante à anterior, tem como objetivo definir e controlar os pacotes que são utilizados no servidor SMB (Server Message Block) com o propósito de evitar que potenciais atacantes explorem a mesma rede. Em outras palavras, ela estabelece as regras e configurações relacionadas aos pacotes de dados que podem ser transmitidos pelo servidor SMB. Isso é feito

para evitar que invasores usem a rede SMB como um vetor de ataque para tentativas de acesso não autorizado ou exploração de vulnerabilidades.

Setting	Value
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCE
Interactive logon: Message title for users attempting to log on	HELLO
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	4 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled

Setting	Value
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCE
Interactive logon: Message title for users attempting to log on	HELLO
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	4 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled

A política determina como o servidor SMB (Server Message Block) responde aos pedidos dos clientes em relação aos pacotes SMB. É recomendado manter essa configuração como "enabled" (ativada) para permitir interações eficazes entre o servidor e os clientes, facilitando o acesso a recursos compartilhados. No entanto, é essencial configurar isso alinhado com

práticas de segurança adequadas para evitar vulnerabilidades de segurança. Essa política visa equilibrar a acessibilidade com a proteção contra possíveis ameaças cibernéticas.

15539 Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'. 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 intercept, edit, 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.

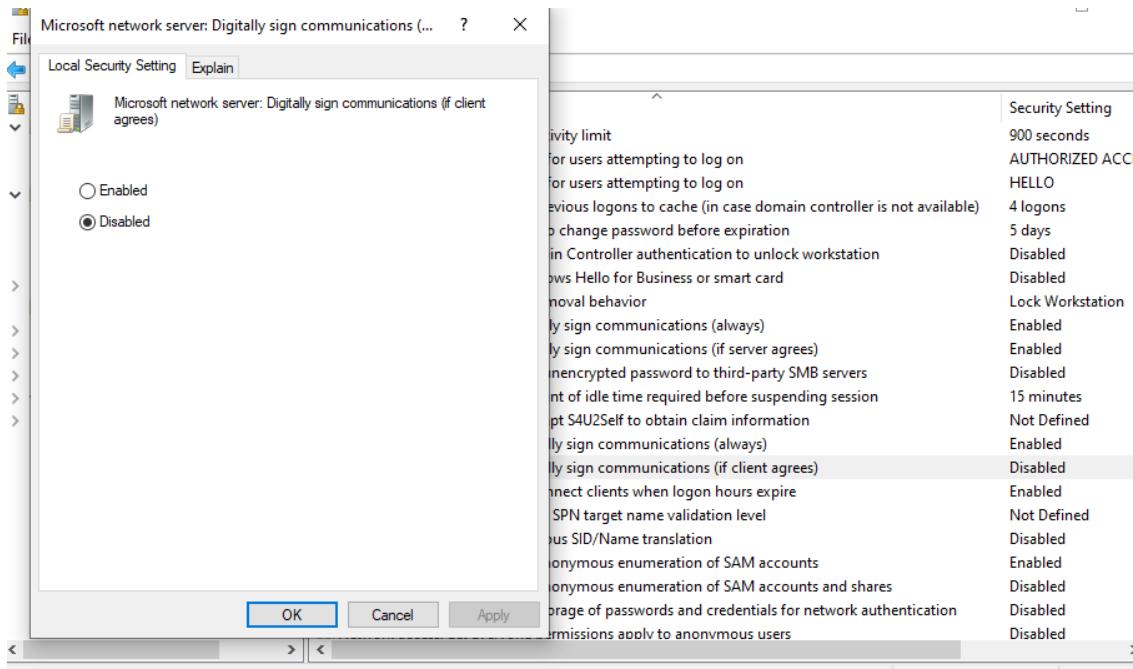
Remediation:
To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)

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.

Checks (Condition: all)

- r:\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters
- r:\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters \> EnableSecuritySignature
- r:\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters \> EnableSecuritySignature \> 1

Compliance:
es: 2.3.9.3
ipa: 164.312.a.2.IV,164.312.e.1,164.312.e.2.I,164.312.e.2.II
net_800_53: SC.B
pct_desc: 4.1
tsc: C08.1,C08.7,CC07.2



Setting	Value
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	AUTHORIZED ACCESS
Interactive logon: Message title for users attempting to log on	HELLO
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	4 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled



Conseguimos com sucesso resolver um total de 18 falhas de segurança do cliente Windows, de acordo com a plataforma Wazuh.

Correção dos erros de logs do cliente Ubuntu

Esta seção do relatório dedica-se à documentação das correções realizadas para abordar várias vulnerabilidades de segurança numa máquina virtual cliente com Ubuntu. O objetivo principal foi identificar e solucionar essas vulnerabilidades, resultando em um ambiente mais seguro.



Como pode ser observado na imagem, foram identificadas um total de 104 falhas de segurança inicialmente. Uma das primeiras ações tomadas foi atualizar o sistema operacional, pois ele não estava na sua versão mais recente, expondo a máquina a riscos conhecidos. Isso foi feito com os comandos apt upgrade e apt update.

A primeira correção significativa envolveu a remoção do serviço Telnet, que estava instalado na máquina. Isso foi considerado crítico para a segurança, uma vez que o Telnet é um protocolo de transmissão de dados não criptografados, suscetível a interceptação, com autenticação fraca e vulnerável a ataques de força bruta. A primeira imagem exibida no relatório representa a falha conforme documentada na plataforma de segurança Wazuh, enquanto a segunda imagem demonstra as ações tomadas na máquina cliente para corrigir a vulnerabilidade.

O resto das falhas serão organizadas de forma igual.

Rationale:
The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The ssh package provides an encrypted session and stronger security and is included in most Linux distributions.

Remediation:
Uninstall telnet: # apt purge telnet

Description:
The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol.

Checks (Condition: all)

- * cd /var/lib/dpkg/info/; dpkg-query -W -f \${binary:Package} | grep Status=install | grep telnet &> nro packages found matching telnet|deinstall|not-installed
- * cd /var/lib/dpkg/info/; dpkg-query -s telnet &> nro package 'telnet' is not installed

Compliance:

- cis: 2.3.4
- cis_esc_y7: 9.2
- cis_esc_y8: 4.8
- cmmc_v2.0: CM_L2-3.4.7,CM_L2-3.4.8,SC_L2-3.13.6
- mitre_mitigations: T1041,T1042
- mitre_tactics: TA0008,TA0009
- mitre_techniques: T1040,T1203,T1543,T1543.002
- pol_dss_3.2.1: 1.1.6,1.2.1,2.2.2,2.2.5
- pol_dss_4.0: 1.2.5,2.2.4,6.4.1
- soc_2: CC8.3,CC6.8

```

root@ubuntu:~# apt purge telnet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
  telnet*
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 158 kB disk space will be freed.
Do you want to continue? [Y/n]
(Reading database ... 74550 files and directories currently installed.)
Removing telnet (0.17-44build1) ...
Processing triggers for man-db (2.10.2-1) ...
(Reading database ... 74541 files and directories currently installed.)
Purging configuration files for telnet (0.17-44build1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

```

Após a remoção do Telnet, a atenção foi direcionada para a correção das vulnerabilidades relacionadas ao SSH (Secure Shell), que é considerado um protocolo de rede mais seguro.

O primeiro passo foi alterar as permissões do ficheiro de configuração de modo a apenas o root conseguir modificar o ficheiro, o que garante a sua integridade.

28634	Ensure permissions on /etc/ssh/sshd_config...	Command: stat /etc/ssh/sshd_config	● Failed	▲
Rationale				
The /etc/ssh/sshd_config file needs to be protected from unauthorized changes by non-privileged users.				
Remediation				
Run the following commands to set ownership and permissions on /etc/ssh/sshd_config: # chown root:root /etc/ssh/sshd_config # chmod og-rwx /etc/ssh/sshd_config.				
Description				
The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root.				
Check (Condition: all)				
• c:stat /etc/ssh/sshd_config → r:Access:\s*\t*(0600/-rw-----)\s*\t*Uid:\s*\t*(\s*\t*0/\s*root)\s*\t*Gid:\s*\t*(\s*\t*0/\s*\t*root)				
Compliance				
cis: 5.2.1				
cis_csc_v7: 14.6				
cis_csc_v8: 3.3				
cmmc_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,AC.L2-3.1.5,AC.L2-3.1.3,MP.L2-3.8.2				
hipaa: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.312(a)(1)				
mitre_mitigations: M1022				
mitre_tactics: TA0005				
mitre_techniques: T1098,T1098.004,T1543,T1543.002				
nist_sp_800-53: AC-5,AC-6				
pci_dss_3.2.1: 7.1,7.1.1,7.1.2,7.1.3				
pci_dss_4.0: 1.3.1,7.1				
soc_2: CC5.2,CC6.1				

```

root@ubuntu:~# chown root:root /etc/ssh/sshd_config
root@ubuntu:~# chmod og-rwx /etc/ssh/sshd_config

```

Restringir o acesso SSH apenas para o gestor, pelo que não será possível entrar no sistema com outro utilizador.

28635 Ensure SSH access is limited. File: /etc/ssh/sshd_config ● Failed ^

Rationale
Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Remediation
Edit the /etc/ssh/sshd_config file or a included configuration file to set one or more of the parameter as follows: AllowUsers <userlist> OR AllowGroups <grouplist> OR DenyUsers <userlist> OR DenyGroups <grouplist>

Description
There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:
- AllowUsers: > The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.
- AllowGroups: > The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- DenyUsers: > The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.
- DenyGroups: > The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

Path
/etc/ssh/sshd_config.d

Checks (Condition: any)

- c: sshd -T → r:^s*t*Allowusers|s*t|w+|^s*t*Denyusers|s*t|w+|^s*t*Allowgroups|s*t|w+|^s*t*Denygroups|s*t|w+
- d:/etc/ssh/sshd_config.d → r:.*
r:^s*t*Allowusers|s*t|w+|^s*t*Denyusers|s*t|w+|^s*t*Allowgroups|s*t|w+|^s*t*Denygroups|s*t|w+
- f:/etc/ssh/sshd_config → r:^s*t*Allowusers|s*t|w+|^s*t*Denyusers|s*t|w+|^s*t*Allowgroups|s*t|w+|^s*t*Denygroups|s*t|w+

```
root@ubuntu:~# vi /etc/ssh/sshd_config
AllowUsers gestor
"/etc/ssh/sshd_config" 126L, 3301B written
root@ubuntu:~# _
```

Impede de se aceder com o root, pois o root tem privilégios ilimitados e qualquer erro ou acesso não autorizado pode causar danos significativos ao sistema. Portanto, os administradores devem fazer login como gestor e, em seguida, usar o comando sudo para obter privilégios de root quando necessário.

28638	Ensure SSH root login is disabled.	Command: sshd -T	● Failed	▲
Rationale				
Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root. This limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident.				
Remediation				
Edit the /etc/ssh/sshd_config file to set the parameter as follows: PermitRootLogin no				
Description				
The PermitRootLogin parameter specifies if the root user can log in using SSH. The default is prohibit-password.				
Checks (Condition: all)				
<ul style="list-style-type: none"> c:sshd -T → r:^permitrootlogin no f:/etc/ssh/sshd_config → r:^s*t*PermitRootLogin\s*t*no 				
Compliance				
cis: 5.2.7				
cis_csc_v7: 4.3				
cis_csc_v8: 5.4				
cmmc_v2.0: AC.L2-3.1.5,AC.L2-3.1.6,AC.L2-3.1.7,SC.L2-3.13.3				
mitre_mitigations: M1042				
mitre_tactics: TA0008				
mitre_techniques: T1021				
nist_sp_800-53: AC-6(2),AC-6(5)				
pci_dss_3.2.1: 7.1,7.1.1,7.1.2,7.1.3				
soc_2: CC6.1,CC6.3				
<pre># Authentication: #LoginGraceTime 2m PermitRootLogin no #StrictModes yes #MaxAuthTries 6 #MaxSessions 10 #PubkeyAuthentication yes # Expect .ssh/authorized_keys2 to be disregarded by default in future. #AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2 "/etc/ssh/sshd_config" 126L, 3285B written root@ubuntu:~#</pre>				

Desativei o encaminhamento gráfico durante as sessões SSH. O encaminhamento gráfico permite que aplicativos gráficos num servidor remoto sejam exibidos na máquina local. Ao desativar o encaminhamento X11 quando não é necessário, reduz-se a superfície de ataque, diminuindo as possíveis vias de ataque. No caso da nossa máquina, faz ainda mais sentido por ser um ambiente onde não é necessário.

28643	Ensure SSH X11 forwarding is disabled.	Command: sshd -T	● Failed	^
Rationale				
Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.				
Remediation				
Edit the /etc/ssh/sshd_config file to set the parameter as follows: X11Forwarding no				
Description				
The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.				
Checks (Condition: all)				
<ul style="list-style-type: none"> • c:sshd -T → r:^x11forwarding no • not f:/etc/ssh/sshd_config → r:^(\s*\t*x11forwarding\s*\t*yes 				
Compliance				
cis: 5.2.12				
cis_csc_v7: 9.2				
cis_csc_v8: 4.8				
cmmc_v2.0: CM.L2-3.4.7,CM.L2-3.4.8,SC.L2-3.13.6				
mitre_mitigations: M1042				
mitre_tactics: TA0008				
mitre_techniques: T1210				
pci_dss_3.2.1: 1.1.6,1.2.1,2.2.2,2.2.5				
pci_dss_4.0: 1.2.5,2.2.4,6.4.1				
soc_2: CC6.3,CC6.6				
<pre>#GatewayPorts no X11Forwarding no #X11DisplayOffset 10 #X11UseLocalhost yes #PermitTTY yes "/etc/ssh/sshd_config" 126L, 3284B written root@ubuntu:~# _</pre>				

Desativei o encaminhamento de portas TCP durante sessões SSH. O encaminhamento de portas TCP permite que as conexões de rede sejam encaminhadas do servidor SSH remoto para a máquina local e vice-versa. Pode ser uma funcionalidade útil. Deve-se avaliar caso a caso se se aplica esta medida.

28647	Ensure SSH AllowTcpForwarding is disabled.	Command: sshd -T	● Failed	▲
-------	--	------------------	----------	---

Rationale

Leaving port forwarding enabled can expose the organization to security risks and backdoors. SSH connections are protected with strong encryption. This makes their contents invisible to most deployed network monitoring and traffic filtering solutions. This invisibility carries considerable risk potential if it is used for malicious purposes such as data exfiltration. Cybercriminals or malware could exploit SSH to hide their unauthorized communications, or to exfiltrate stolen data from the target network.

Remediation

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows: `AllowTcpForwarding no`

Description

SSH port forwarding is a mechanism in SSH for tunneling application ports from the client to the server, or servers to clients. It can be used for adding encryption to legacy applications, going through firewalls, and some system administrators and IT professionals use it for opening backdoors into the internal network from their home machines.

Checks (Condition: all)

- c:sshd -T → r:^allowtcpforwarding && r:no\$
- not f:/etc/ssh/sshd_config → r:^s*\t*AllowTcpForwarding\s*\t*yes

Compliance

cis: 5.2.16

cis_cse_v7: 9.2

cis_csc_v8: 4.1

cmmc_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,CM.L2-3.4.1,CM.L2-3.4.6,CM.L2-3.4.2,CM.L2-3.4.7

mitre_mitigations: M1042

mitre_tactics: TA0008

mitre_techniques: T1048,T1048.002,T1572

nist_sp_800-53: CM-7(1),CM-9,SA-10

pci_dss_3.2.1: 2.2,11.5

pci_dss_4.0: 1.1.1,1.2.1,1.2.6,1.5.1,1.2.7,2.1.1,2.2.1

soc_2: CC7.1,CC8.1

```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#      X11Forwarding no
AllowTcpForwarding no
#      PermitTTY no
#      ForceCommand cvs server
PasswordAuthentication yes

AllowUsers gestor
"/etc/ssh/sshd_config" 126L, 3282B written
root@ubuntu:~#
```

Alterei o ficheiro de configuração do SSH para apresentar um banner ("HELLO!") no terminal SSH quando um utilizador se conectar ao sistema. Pode ser implementado para notificar os utilizadores sobre a política de uso do sistema, os termos de acesso ou qualquer aviso legal relevante.

28648	Ensure SSH warning banner is configured.	Command: sshd -T	● Failed	^
Rationale				
Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.				
Remediation				
Edit the /etc/ssh/sshd_config file to set the parameter as follows: Banner /etc/issue.net				
Description				
The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.				
Check (Condition: all)				
<ul style="list-style-type: none"> • c:sshd -T → r:^banner && r:/etc/issue.net\$ 				
Compliance				
cis: 5.2.17				
cis_esc_v7: 5.1				
cis_csc_v8: 4.1				
cmmc_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,CM.L2-3.4.1,CM.L2-3.4.6,CM.L2-3.4.2,CM.L2-3.4.7				
mitre_mitigations: M1035				
mitre_tactics: TA0001,TA0007				
nist_sp_800-53: CM-7(1),CM-9,SA-10				
pci_dss_3.2.1: 2.2,11.5				
pci_dss_4.0: 1.1.1,1.2.1,1.2.6,1.5.1,1.2.7,2.1.1,2.2.1				
soc_2: CC7.1,CC8.1				

```
# no default banner path
Banner /etc/issue.net

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
AllowTcpForwarding no
#    PermitTTY no
"/etc/ssh/sshd_config" 126L, 3291B written
root@ubuntu:~# vi /etc/issue.net
```

```
HELLO!  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~/etc/issue.net" 3L, 27B written  
root@ubuntu:~#
```

Defini o número máximo de tentativas de autenticação permitidas. Assim, caso um utilizador insira mal as credenciais 4 vezes o servidor SSH encerrará a conexão. Não define um valor mais baixo, porque poderia causar bloqueios acidentais de utilizadores legítimos que cometem erros de digitação ao fazer login.

28649	Ensure SSH MaxAuthTries is set to 4 or less.	Command: sshd -T	● Failed	^
Rationale				
Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.				
Remediation				
Edit the /etc/ssh/sshd_config file to set the parameter as follows: MaxAuthTries 4				
Description				
The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.				
Checks (Condition: all)				
<ul style="list-style-type: none"> c:sshd -T → n:^maxauthtries)s+(\\d+) compare <= 4 not f:/etc/ssh/sshd_config → n:^\\s*\\t*maxauthtries)s+(\\d+) compare > 4 				
Compliance				
cis: 5.2.18				
cis_csc_v7: 16.13				
cis_csc_v8: 8.5				
cmme_v2.0: AU.L2-3.3.1				
mitre_mitigations: M1036				
mitre_tactics: TA0006				
mitre_techniques: T1110,T1110.001,T1110.003				
nist_sp_800-53: AU-3(1),AU-7				
pci_dss_3.2.1: 10.1,10.2.2,10.2.4,10.2.5,10.3				
pci_dss_4.0: 9.4.5,10.2,10.2.1,10.2.1.2,10.2.1.5				
soc_2: CC5.2,CC7.2				

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
MaxAuthTries 4
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

"/etc/ssh/sshd_config" 126L, 3290B written
root@ubuntu:~# -
```

Para controlar o tráfego de entrada no servidor SSH, evitando sobrecargas e impedindo ataques de negação de serviço (DoS) ou ataques de força bruta que podem tentar esgotar recursos do servidor, fiz a seguinte configuração:

- O servidor permitirá um mínimo de 10 conexões simultâneas.
- O servidor permitirá até 30 novas conexões por minuto.
- O número máximo total de conexões simultâneas permitidas é de 60.

28650	Ensure SSH MaxStartups is configured.	Command: sshd -T	● Failed	^
Rationale				
To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.				
Remediation				
Edit the /etc/ssh/sshd_config file to set the parameter as follows: MaxStartups 10:30:60				
Description				
The MaxStartups parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.				
Checks (Condition: all)				
<ul style="list-style-type: none"> c:sshd -T → n:^ s*maxstartups s+ (\d+): d+: d+ compare <= 10 && n:^maxstartups s+ (\d+): d+: d+ compare >= 1 c:sshd -T → n:^ s*maxstartups s+ d+: d+ compare <= 30 && n:^maxstartups s+ (\d+): d+: d+ compare >= 1 c:sshd -T → n:^ s*maxstartups s+ d+: d+:(\d+) compare <= 60 && n:^maxstartups s+ (\d+): d+: d+:(\d+) compare >= 1 not f:/etc/ssh/sshd_config → n:^ s* t*MaxStartups s* t*(\d+): d+: d+ compare == 0 not f:/etc/ssh/sshd_config → n:^ s* t*MaxStartups s* t*(\d+): d+: d+ compare > 10 not f:/etc/ssh/sshd_config → n:^ s* t*MaxStartups s* t* d+: (\d+): d+ compare == 0 not f:/etc/ssh/sshd_config → n:^ s* t*MaxStartups s* t* d+: (\d+): d+ compare > 30 not f:/etc/ssh/sshd_config → n:^ s* t*MaxStartups s* t* d+: d+:(\d+) compare == 0 not f:/etc/ssh/sshd_config → n:^ s* t*MaxStartups s* t* d+: d+:(\d+) compare > 60 				
Compliance				
cis: 5.2.19				
cis_csc_v7: 5.1				
cis_csc_v8: 4.1				
cmmc_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,CM.L2-3.4.1,CM.L2-3.4.6,CM.L2-3.4.2,CM.L2-3.4.7				
mitre_tactics: TA0040				
mitre_techniques: T1499,T1499.002				
<pre>#ClientAliveInterval 0 #ClientAliveCountMax 3 #UseDNS no #PidFile /run/sshd.pid MaxStartups 10:30:60 #PermitTunnel no #ChrootDirectory none #VersionAddendum none # no default banner path Banner /etc/issue.net # Allow client to pass locale environment variables "/etc/ssh/sshd_config" 126L, 3288B written root@ubuntu:~# _</pre>				

Alterei a configuração LoginGraceTime (tempo que um cliente tem para autenticar com sucesso antes que a conexão seja encerrada) para 60 segundos. Tal medida não só dificulta ataques, como também melhora a eficiência do servidor, libertando recursos.

28652	Ensure SSH LoginGraceTime is set to one m...	Command: sshd -T	● Failed	^
Rationale				
Setting the LoginGraceTime parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections. While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.				
Remediation				
Edit the /etc/ssh/sshd_config file to set the parameter as follows: LoginGraceTime 60				
Description				
The LoginGraceTime parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.				
Checks (Condition: all)				
<ul style="list-style-type: none"> • c:sshd -T → n:^ \s*logginggracetimel\s*(\d+) compare <= 60 && n:^ logginggracetimel\s*(\d+) compare >= 1 • not f:/etc/ssh/sshd_config → n:^ \s*t*LoginGraceTimel\s*\ t*(\d+) compare == 0 • not f:/etc/ssh/sshd_config → n:^ \s*t*LoginGraceTimel\s*\ t*(\d+) compare > 60 				
Compliance				
cis: 5.2.21				
cis_csc_v7: 5.1				
cis_csc_v8: 4.1				
cmmc_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,CM.L2-3.4.1,CM.L2-3.4.6,CM.L2-3.4.2,CM.L2-3.4.7				
mitre_mitigations: M1036				
mitre_tactics: TA0006				
mitre_techniques: T1110,T1110.001,T1110.003,T1110.004,T1499,T1499.002				
nist_sp_800-53: CM-7(1),CM-9,SA-10				
pci_dss_3.2.1: 2.2,11.5				
pci_dss_4.0: 1.1.1,1.2.1,1.2.6,1.5.1,1.2.7,2.1.1,2.2.1				
soc_2: CC7.1,CC8.1				
<pre># Authentication: LoginGraceTime 60 PermitRootLogin no #StrictModes yes MaxAuthTries 4 #MaxSessions 10 #PubkeyAuthentication yes "/etc/ssh/sshd_config" 126L, 3287B written root@ubuntu:~#</pre>				

Mudei as regras de manutenção de sessões SSH ativas e, consequente, desconexão automática de sessões inativas. Após 45 segundos de inatividade, uma sessão é desconectada.

28653 Ensure SSH Idle Timeout Interval is configur... **Command:** sshd -T ● Failed

Rationale
In order to prevent resource exhaustion, appropriate values should be set for both ClientAliveInterval and ClientAliveCountMax. Specifically, looking at the source code, ClientAliveCountMax must be greater than zero in order to utilize the ability of SSH to drop idle connections. If connections are allowed to stay open indefinitely, this can potentially be used as a DDOS attack or simple resource exhaustion could occur over unreliable networks. The example set here is a 45 second timeout. Consult your site policy for network timeouts and apply as appropriate.

Remediation
Edit the /etc/ssh/sshd_config file to set the parameters according to site policy. Example: ClientAliveInterval 15 ClientAliveCountMax 3

Description
NOTE: To clarify, the two settings described below is only meant for idle connections from a protocol perspective and not meant to check if the user is active or not. An idle user does not mean an idle connection. SSH does not and never had, intentionally, the capability to drop idle users. In SSH versions before 8.2p1 there was a bug that caused these values to behave in such a manner that they were abused to disconnect idle users. This bug has been resolved in 8.2p1 and thus it can no longer be abused disconnect idle users. The two options ClientAliveInterval and ClientAliveCountMax control the timeout of SSH sessions. Taken directly from man 5 sshd_config: - ClientAliveInterval Sets a timeout interval in seconds after which if no data has been received from the client, sshd(8) will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client. - ClientAliveCountMax Sets the number of client alive messages which may be sent without sshd(8) receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. It is important to note that the use of client alive messages is very different from TCPKeepAlive. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The TCP keepalive option enabled by TCPKeepAlive is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive. The default value is 3. If ClientAliveInterval is set to 15, and ClientAliveCountMax is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds. Setting a zero ClientAliveCountMax disables connection termination.

Checks (Condition: all)

- c:sshd -T → n:^clientalivecountmax\\$|t*(\d+) compare > 0
- c:sshd -T → n:^clientaliveinterval\\$|t*(\d+) compare > 0

Compliance
cis: 5.2.22
mitre_mitigations: M1026
mitre_tactics: TA0001
mitre_techniques: T1078,T1078.001,T1078.002,T1078.003

```
microsoft Environment no
#Compression delayed
ClientAliveInterval 15
ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
MaxStartups 10:30:60
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none
"/etc/ssh/sshd_config" 126L, 3286B written
root@ubuntu:~#
```

Estas foram todas as regras aplicadas quanto ao SSH.

Depois habilitei o UFW (Uncomplicated FireWall), que é uma ferramenta de firewall que simplifica a configuração e a gestão das regras de firewall no Ubuntu.

28575 Ensure ufw service is enabled. Command: systemctl is-enabled ufw.service,systemctl is-active ufw.ufw status Failed ^

Rationale
The ufw service must be enabled and running in order for ufw to protect the system.

Remediation
Run the following command to unmask the ufw daemon: # systemctl unmask ufw.service Run the following command to enable and start the ufw daemon: # systemctl --now enable ufw.service active Run the following command to enable ufw: # ufw enable

Description
UFW (Uncomplicated Firewall) is a frontend for iptables. ufw provides a framework for managing netfilter, as well as a command-line and available graphical user interface for manipulating the firewall. Notes: When running ufw enable or starting ufw via its script, ufw will flush its chains. This is required so ufw can maintain a consistent state, but it may drop existing connections (eg ssh). ufw does support adding rules before enabling the firewall. Run the following command before running ufw enable: # ufw allow proto tcp from any to any port 22 The rules will still be flushed, but the ssh port will be open after enabling the firewall. Please note that once ufw is 'enabled', ufw will not flush the chains when adding or removing rules (but will when modifying a rule or changing the default policy) By default, ufw will prompt when enabling the firewall while running under ssh. This can be disabled by using ufw --force enable.

Checks (Condition: all)

- cisystemctl is-active ufw -> r^active
- cisystemctl is-enabled ufw.service -> r^enabled
- cufw status -> rStatus:r+active

Compliance

cis: 3.5.1.3
cis_csc_v7: 4.4.5
cis_csc_v8: 4.4.5
cmmc_v2.0: AC.L1-3.1.20,CM.L2-3.4.7,SC.L1-3.13.1,SC.L2-3.13.6
mitre_tactics: TA0000
mitre_techniques: T1562,T1562.004
nist_ip_800-53: SC-719
pol_dss_3.2: 1.1.4,1.1.4
pol_dss_4.0: 1.2.1
soc_2: CC6.6

```
root@ubuntu:~# ufw enable
Firewall is active and enabled on system startup
```

Configurei a política em que a conta do utilizador é bloqueada automaticamente após 30 dias da expiração da senha.

28668 Ensure inactive password lock is 30 days or ... Command: useradd -D Failed ^

Rationale
Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Remediation
Run the following command to set the default password inactivity period to 30 days: # useradd -D -f 30 Modify user parameters for all users with a password set to match: # chage --inactive 30 <user>

Description
User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Checks (Condition: none)

- c:useradd -D → n:^INACTIVE=(\d+) compare == 0
- c:useradd -D → n:^INACTIVE=(\d+) compare >= 30
- c:useradd -D → r:^INACTIVE=-1
- f:/etc/shadow → lr:^w+:|p: && n:^|w+:|S*:|d*:|d*:|d+:|(\d+) compare > 30

Compliance

cis: 5.5.1.4
cis_csc_v7: 4.4
cis_csc_v8: 5.2
cmmc_v2.0: IA.L2-3.5.7
mitre_mitigations: M1027
mitre_tactics: TA0001
mitre_techniques: T1078,T1078.002,T1078.003
pci_dss_4.0: 2.2.2,8.3.5,8.3.6,8.6.3
soc_2: CC6.1

```
root@ubuntu:~# useradd -D -f 30
root@ubuntu:~# chage --inactive 30 gestor
```

Alterei as permissões e a propriedade das pastas relacionadas com o cron (serviço de agendamento de tarefas no sistema operativo). É importante impedir que um utilizador indevido tenha acesso ao sistema com privilégios ilimitados. Ele não pode facilmente manipular as tarefas cron ou adicionar comandos maliciosos à lista de agendamento. Assim, mantém-se a integridade do sistema e previne-se a exploração de falhas de segurança.

28631 Ensure permissions on /etc/cron.d are config... **Command:** stat /etc/cron.d/ ● Failed ^

Rationale

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Remediation

Run the following commands to set ownership and permissions on the /etc/cron.d directory: # chown root:root /etc/cron.d/ # chmod og-rwx /etc/cron.d/

Description

The /etc/cron.d directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from /etc/crontab, but require more granular control as to when they run. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy.

Check (Condition: all)

- c:stat /etc/cron.d/ → r:Access:`\s*\t*(0700/drwx-----)\s*\t*Uid:\s*\t*(\s*\t*0/\s*\t*root)\s*\t*Gid:\s*\t*(\s*\t*0/\s*\t*root)`

Compliance

cis: 5.1.7

cis_csc_v7: 14.6

cis_csc_v8: 3.3

cmme_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,AC.L2-3.1.5,AC.L2-3.1.3,MP.L2-3.8.2

hipaa: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.312(a)(1)

mitre_mitigations: M1018

mitre_tactics: TA0002,TA0007

mitre_techniques: T1053,T1053.003

nist_sp_800-53: AC-5,AC-6

pci_dss_3.2.1: 7.1,7.1.1,7.1.2,7.1.3

pci_dss_4.0: 1.3.1,7.1

soc_2: CC5.2,CC6.1

```
root@ubuntu:~# chown root:root /etc/cron.d
root@ubuntu:~# chmod og-rwx /etc/cron.d
```

28630	Ensure permissions on /etc/cron.monthly ar...	Command: stat /etc/cron.monthly/	● Failed	^
Rationale				
Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.				
Remediation				
Run the following commands to set ownership and permissions on the /etc/cron.monthly directory: # chown root:root /etc/cron.monthly/ # chmod og-rwx /etc/cron.monthly/				
Description				
The /etc/cron.monthly directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy.				
Check (Condition: all)				
• c:stat /etc/cron.monthly/ → r:Access: \s*\t*(0700/drwx-----)\s*\t*Uid:\s*\t*\(\s*\t*0/\s*\t*root\)\s*\t*Gid:\s*\t*\(\s*\t*0/\s*\t*root\)				
Compliance				
cis: 5.1.6				
cis_csc_v7: 14.6				
cis_csc_v8: 3.3				
cmmc_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,AC.L2-3.1.5,AC.L2-3.1.3,MP.L2-3.8.2				
hipaa: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.312(a)(1)				
mitre_mitigations: M1018				
mitre_tactics: TA0002,TA0007				
mitre_techniques: T1053,T1053.003				
nist_sp_800-53: AC-5,AC-6				
pci_dss_3.2.1: 7.1,7.1.1,7.1.2,7.1.3				
pci_dss_4.0: 1.3.1,7.1				
soc_2: CC5.2,CC6.1				

```
root@ubuntu:~# chown root:root /etc/cron.monthly/
root@ubuntu:~# chmod og-rwx /etc/cron.monthly/
```

28626

Ensure permissions on /etc/crontab are con...

Command: stat /etc/crontab

● Failed

^

Rationale

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Remediation

Run the following commands to set ownership and permissions on /etc/crontab : # chown root:root /etc/crontab # chmod og-rwx /etc/crontab

Description

The /etc/crontab file is used by cron to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file. Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy.

Check (Condition: all)

- c:stat /etc/crontab → r:Access:`\s*\t*(0600/-rw-----)\s*\t*Uid:\s*\t*\(\s*\t*0/\s*\t*root\)\s*\t*Gid:\s*\t*\(\s*\t*0/\s*\t*root\)`

Compliance**cis:** 5.1.2**cis_csc_v7:** 14.6**cis_csc_v8:** 3.3**cmmc_v2.0:** AC.L1-3.1.1,AC.L1-3.1.2,AC.L2-3.1.5,AC.L2-3.1.3,MP.L2-3.8.2**hipaa:** 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.312(a)(1)**mitre_mitigations:** M1018**mitre_tactics:** TA0002,TA0007**mitre_techniques:** T1053,T1053.003**nist_sp_800-53:** AC-5,AC-6**pci_dss_3.2.1:** 7.1,7.1.1,7.1.2,7.1.3**pci_dss_4.0:** 1.3.1,7.1**soc_2:** CC5.2,CC6.1

```
root@ubuntu:~# chown root:root /etc/crontab
root@ubuntu:~# chmod og-rwx /etc/crontab
```

28627	Ensure permissions on /etc/cron.hourly are ...	Command: stat /etc/cron.hourly/	● Failed	^
Rationale				
Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges.				
Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.				
Remediation				
Run the following commands to set ownership and permissions on the /etc/cron.hourly directory: # chown root:root /etc/cron.hourly/ # chmod og-rwx /etc/cron.hourly				
Description				
This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy.				
Check (Condition: all)				
• c:stat /etc/cron.hourly/ → r:Access: <code>\s*\t*(0700/drwx-----)\s*\t*Uid:\s*\t*((\s*\t*0/\s*\t*root))\s*\t*Gid:\s*\t*((\s*\t*0/\s*\t*root))</code>				
Compliance				
cis: 5.1.3				
cis_csc_v7: 14.6				
cis_csc_v8: 3.3				
cmmc_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,AC.L2-3.1.5,AC.L2-3.1.3,MP.L2-3.8.2				
hipaa: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.312(a)(1)				
mitre_mitigations: M1018				
mitre_tactics: TA0002,TA0007				
mitre_techniques: T1053,T1053.003				
nist_sp_800-53: AC-5,AC-6				
pci_dss_3.2.1: 7.1,7.1.1,7.1.2,7.1.3				
pci_dss_4.0: 1.3.1,7.1				
soc_2: CC5.2,CC6.1				

```
root@ubuntu:~# chown root:root /etc/cron.hourly/
root@ubuntu:~# chmod og-rwx /etc/cron.hourly/
```

28628	Ensure permissions on /etc/cron.daily are c...	Command: stat /etc/cron.daily/	● Failed	^
Rationale				
Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.				
Remediation				
Run the following commands to set ownership and permissions on the /etc/cron.daily directory: # chown root:root /etc/cron.daily/ # chmod og-rwx /etc/cron.daily/				
Description				
The /etc/cron.daily directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy.				
Check (Condition: all)				
• c:stat /etc/cron.daily/ → r:Access:\s*\t*(0700/drwx-----)\s*\t*Uid:\s*\t*(\s*\t*0/\s*\t*root)\s*\t*Gid:\s*\t*(\s*\t*0/\s*\t*root\)				
Compliance				
cis: 5.1.4				
cis_csc_v7: 14.6				
cis_csc_v8: 3.3				
cmmc_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,AC.L2-3.1.5,AC.L2-3.1.3,MP.L2-3.8.2				
hipaa: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.312(a)(1)				
mitre_mitigations: M1018				
mitre_tactics: TA0002,TA0007				
mitre_techniques: T1053,T1053.003				
nist_sp_800-53: AC-5,AC-6				
pci_dss_3.2.1: 7.1,7.1.1,7.1.2,7.1.3				
pci_dss_4.0: 1.3.1,7.1				
soc_2: CC5.2,CC6.1				

```
root@ubuntu:~# chown root:root /etc/cron.daily/
root@ubuntu:~# chmod og-rwx /etc/cron.daily/
```

28629	Ensure permissions on /etc/cron.weekly are...	Command: stat /etc/cron.weekly/	● Failed	^
Rationale				
Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges.				
Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.				
Remediation				
Run the following commands to set ownership and permissions on the /etc/cron.weekly directory: # chown root:root /etc/cron.weekly/ # chmod og-rwx /etc/cron.weekly/				
Description				
The /etc/cron.weekly directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy.				
Check (Condition: all)				
<ul style="list-style-type: none"> c:stat /etc/cron.weekly/ → r:Access:\s*\t*(0700/drwx-----)\s*\t*Uid:\s*\t*(\s*\t*0/\s*\t*root)\s*\t*Gid:\s*\t*(\s*\t*0/\s*\t*root) 				
Compliance				
cis: 5.1.5				
cis_csc_v7: 14.6				
cis_csc_v8: 3.3				
cmmc_v2.0: AC.L1-3.1.1,AC.L1-3.1.2,AC.L2-3.1.5,AC.L2-3.1.3,MP.L2-3.8.2				
hipaa: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.312(a)(1)				
mitre_mitigations: M1018				
mitre_tactics: TA0002,TA0007				
mitre_techniques: T1053,T1053.003				
nist_sp_800-53: AC-5,AC-6				
pci_dss_3.2.1: 7.1,7.1.1,7.1.2,7.1.3				
pci_dss_4.0: 1.3.1,7.1				
soc_2: CC5.2,CC6.1				
<pre>root@ubuntu:~# chown root:root /etc/cron.weekly/ root@ubuntu:~# chmod og-rwx /etc/cron.we chmod: cannot access '/etc/cron.we': No such file or directory root@ubuntu:~# chmod og-rwx /etc/cron.weekly/</pre>				

Instalei um serviço para coletar logs de sistemas remotos e centralizá-los para análise, o que facilita a deteção de ameaças e a resposta a incidentes. Deve-se configurar a autenticação e a criptografia apropriadas para proteger os registos em trânsito, bem como garantir que apenas sistemas confiáveis possam encaminhar logs para o servidor central.

28614	Ensure systemd-journal-remote is installed.	Command: dpkg-query -s systemd-journal-remote ● Failed	^
Rationale			
Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.			
Remediation			
Run the following command to install systemd-journal-remote: # apt install systemd-journal-remote			
Description			
Journald (via systemd-journal-remote) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.			
Check (Condition: all)			
<ul style="list-style-type: none"> • c:dpkg-query -s systemd-journal-remote → r:install ok installed 			
Compliance			
cis: 4.2.1.1.1			
cis_csc_v7: 6.2,6.3			
cis_csc_v8: 8.2			
cmmc_v2.0: AU.L2-3.3.1			
hipaa: 164.312(b)			
mitre_mitigations: M1029			
mitre_tactics: TA0040			
mitre_techniques: T1070,T1070.002,T1562,T1562.006			
nist_sp_800-53: AU-7			
pci_dss_3.2.1: 10.2,10.3			
pci_dss_4.0: 5.3.4,6.4.1,6.4.2,10.2.1,10.2.1.1,10.2.1.2,10.2.1.3,10.2.1.4,10.2.1.5,10.2.1.6,10.2.1.7,10.2.2			
<pre>root@ubuntu:~# apt install systemd-journal-remote Reading package lists... Done Building dependency tree... Done Reading state information... Done The following packages were automatically installed and are no longer required: libflashrom1 libftfdi1-2 Use 'apt autoremove' to remove them. The following additional packages will be installed: libmicrohttpd12 The following NEW packages will be installed: libmicrohttpd12 systemd-journal-remote 0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded. Need to get 146 kB of archives. After this operation, 599 kB of additional disk space will be used. Do you want to continue? [Y/n]</pre>			

Tentei instalar os plugins do auditd no sistema Linux. O auditd é um serviço de auditoria de segurança que regista eventos de auditoria em sistemas Linux. Os plugins do audisdp são extensões que podem ser usadas para processar eventos de auditoria e realizar ações específicas com base neles (melhorando a segurança e a visibilidade do sistema). Não me foi possível, mas no futuro cumprirei tal medida, pois ao estudar percebi a sua importância.

28590	Ensure auditd is installed.	Command: dpkg-query -s auditd	● Failed	^
Rationale				
The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.				
Remediation				
Run the following command to install auditd # apt install auditd audisdp-plugins.				
Description				
auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk.				
Checks (Condition: all)				
<ul style="list-style-type: none"> • c:dpkg-query -s audisdp-plugins → r:install ok installed • c:dpkg-query -s auditd → r:install ok installed 				
Compliance				
cis: 4.1.1.1				
cis_csc_v7: 6.2				
cis_csc_v8: 8.5				
cmmc_v2.0: AU.L2-3.3.1				
mitre_tactics: TA0005				
mitre_techniques: T1562,T1562.001				
nist_sp_800-53: AU-3(1),AU-7				
pci_dss_3.2.1: 10.1,10.2.2,10.2.4,10.2.5,10.3				
pci_dss_4.0: 9.4.5,10.2,10.2.1,10.2.1.2,10.2.1.5				
soc_2: CC5.2,CC7.2				
<pre>root@ubuntu:~# apt install audit audisdp-plugins Reading package lists... Done Building dependency tree... Done Reading state information... Done E: Unable to locate package audit </pre>				

Removi o pacote “nftables” do sistema por questões de conflitos com outro serviço. Caso não tivesse “iptables”, poderia ser necessário. Não esquecer de verificar se há ou não dependências críticas para evitar consequências não intencionais.

28584	Ensure nftables is not installed with iptables.	Command: dpkg-query -s nftables	● Failed	^
Rationale				
Running both iptables and nftables may lead to conflict.				
Remediation				
Run the following command to remove nftables: # apt purge nftables				
Description				
nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.				
Checks (Condition: all)				
<ul style="list-style-type: none"> • c:dpkg-query -s iptables → r:install ok installed • not c:dpkg-query -s nftables → r:install ok installed 				
Compliance				
cis: 3.5.3.1.2				
cis_csc_v7: 9.4				
cis_csc_v8: 4.4,4.5				
cmmc_v2.0: AC.L1-3.1.20,CM.L2-3.4.7,SC.L1-3.13.1,SC.L2-3.13.6				
mitre_mitigations: M1031,M1037				
<pre>root@ubuntu:~# apt purge nftables Reading package lists... Done Building dependency tree... Done Reading state information... Done The following packages were automatically installed and are no longer required: libflashrom1 liblfd1-2 libnftables1 Use 'apt autoremove' to remove them. The following packages will be REMOVED: nftables* ubuntu-standard* 0 upgraded, 0 newly installed, 2 to remove and 0 not upgraded. After this operation, 236 KB disk space will be freed. Do you want to continue? [Y/n] (Reading database ... 74478 files and directories currently installed.) Removing ubuntu-standard (1.481.1) ... Removing nftables (1.0.2-1ubuntu3) ... Processing triggers for man-db (2.10.2-1) ... (Reading database ... 74440 files and directories currently installed.) Purging configuration files for nftables (1.0.2-1ubuntu3) ...</pre>				

Instalei o pacote “iptables” como ferramenta para gestão das regras de firewall.

28583	Ensure iptables packages are installed.	Command: dpkg -s iptables,dpkg -s iptables-persistent ● Failed	^
Rationale			
A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.			
Remediation			
Run the following command to install iptables and iptables-persistent # apt install iptables iptables-persistent			
Description			
iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.			
Checks (Condition: all)			
<ul style="list-style-type: none"> • c:dpkg -s iptables → r:Status: install ok installed • c:dpkg -s iptables-persistent → r:Status: install ok installed • c:dpkg -s nftables → r:package 'nftables' is not installed • c:dpkg -s ufw → r:package 'ufw' is not installed 			
Compliance			
cis: 3.5.3.1.1			
cis_csc_v7: 9.4			
cis_csc_v8: 4.4.4.5			
cmmc_v2.0: AC.L1-3.1.20,CM.L2-3.4.7,SC.L1-3.13.1,SC.L2-3.13.6			
mitre_mitigations: M1031,M1037			
mitre_tactics: TA0011			
mitre_techniques: T1562,T1562.004			
nist_sp_800-53: SC-7(5)			
pci_dss_3.2.1: 1.4,1.1.4			
pci_dss_4.0: 1.2.1			
soc_2: CC6.6			
<pre>Selecting previously unselected package netfilter-persistent. (Reading database ... 74439 files and directories currently installed.) Preparing to unpack .../netfilter-persistent_1.0.16_all.deb ... Unpacking netfilter-persistent (1.0.16) ... Selecting previously unselected package iptables-persistent. Preparing to unpack .../iptables-persistent_1.0.16_all.deb ... Unpacking iptables-persistent (1.0.16) ... Setting up netfilter-persistent (1.0.16) ... invoke-rc.d: policy-rc.d denied execution of restart. Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persistent.service → /lib/systemd/system/netfilter-persistent.service. /usr/sbin/policy-rc.d returned 101, not running 'restart netfilter-persistent.service' Setting up iptables-persistent (1.0.16) ... update-alternatives: using /lib/systemd/system/netfilter-persistent.service to provide /lib/systemd/system/iptables.service (iptables.service) in auto mode Processing triggers for man-db (2.10.2-1) ... Scanning processes... Scanning linux images... Running kernel seems to be up-to-date. No services need to be restarted. No containers need to be restarted. No user sessions are running outdated binaries. No VM guests are running outdated hypervisor (qemu) binaries on this host. root@ubuntu:~#</pre>			

Alterei a senha do utilizador root. Como se trata de uma conta com privilégios elevados, é boa prática exigir uma senha complexa. O acesso a esta conta deve ser devidamente controlado e a senha deve ser alterada com frequência.

28520 Ensure authentication required for single user mode.

Rationale
Requiring authentication in single user mode prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Remediation
Run the following command and follow the prompts to set a password for the root user: # passwd root.

Description
Single user mode is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.

Check (Condition: all)

- /etc/shadow → r::root:\$id+

Compliance

- cls: 1.4.3
- cls_csc_v7: 4.4
- cls_csc_v8: 5.2

cmmc_v2.0: IA.L2-3.5.7
mitre_mitigations: M1022
mitre_tactics: TA0005
mitre_techniques: T1548
pel_dss_v4.0: 0.2.2.2, 8.3.5, 8.3.6, 8.6.3
sec_2: C06.1

```
root@ubuntu:~# passwd root
New password:
Retype new password:
passwd: password updated successfully
```

Desativei o serviço rsync. O comando mask impede o serviço de ser iniciado, mesmo que alguém tente ativar manualmente. Deste modo, garante-se que apenas os serviços essenciais e seguros estão a ser executados no sistema, reduzindo a exposição a ameaças.

28566 Ensure rsync service is either not installed or masked.

Rationale
The rsync service presents a security risk as it uses unencrypted protocols for communication. The rsync package should be removed to reduce the attack area of the system.

Remediation
Run the following command to remove rsync: # apt purge rsync OR Run the following commands to stop and mask rsync: # systemctl stop rsync # systemctl mask rsync.

Description
The rsync service can be used to synchronize files between systems over network links.

Checks (Condition: all)

- dpkg-query -W -f '\${binary:Package} \${Status} \${db>Status>Status}'|grep rsync |grep -v installed
- systemctl is-active rsync → inactive
- systemctl is-enabled rsync → masked|disabled

Compliance

- cls: 2.2.16
- cls_csc_v7: 9.2
- cls_csc_v8: 4.8

cmmc_v2.0: CM.L2-3.4.7, SC.L2-3.13.6
mitre_mitigations: M1042
mitre_tactics: TA0008
mitre_techniques: T1105,T1203,T1210,T1543,T1543.002,1570
pel_dss_v3.2.1: 1.1.6, 1.2.1, 2.2.2, 2.2.5
pel_dss_v4.0: 1.2.5, 2.2.4, 8.4.1
sec_2: C06.3, C06.6

```
root@ubuntu:~# apt purge rsync
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2 libnftables1
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
  rsync*
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 813 kB disk space will be freed.
Do you want to continue? [Y/n]
(Reading database ... 74461 files and directories currently installed.)
Removing rsync (3.2.7-0ubuntu0.22.04.2) ...
/usr/sbin/policy-rc.d returned 101, not running 'stop rsync.service'
invoke-rc.d: policy-rc.d denied execution of stop.
Processing triggers for man-db (2.10.2-1) ...
(Reading database ... 74429 files and directories currently installed.)
Purging configuration files for rsync (3.2.7-0ubuntu0.22.04.2) ...
root@ubuntu:~# _
```

Centralizei os logs num sistema de log centralizado (rsyslog). Destarte, há melhor controlo e visibilidade das atividades do sistema, o que é essencial para monitorizar a segurança e detetar possíveis problemas.

28622 Ensure journald is configured to send logs to rsyslog. File: /etc/systemd/journald.conf Failed

Rationale
If RSyslog is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.

Remediation
Edit the /etc/systemd/journald.conf file and add the following line: ForwardToSyslog=yes Restart the service: # systemctl restart rsyslog.

Description
Data from journald may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of journald logs, however, use of the RSyslog service provides a consistent means of log collection and export.

Check (Condition: all)

- f/etc/systemd/journald.conf → r:::"s*(#ForwardToSyslog=yes\$

Compliance

cis: 4.2.3
cis_csc_7: 6.2.6.3.6.5
cis_csc_v8r: 8.2.8.0
nist_sp_800-53: AU-6(3)
pci_dss_3.2.1: 10.5.3,10.5.4
pci_dss_4.0: 10.3.3
sec_2: PL1.4

```
root@ubuntu:~# vi /etc/systemd/journald.conf

##MaxRetentionSec-
#MaxFileSec=1month
ForwardToSyslog=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
"/etc/systemd/journald.conf" 47L, 1281B written
root@ubuntu:~# systemctl restart rsyslog.service
```

No total, curiosamente tal como no cliente Windows, foram resolvidas durante essa revisão de segurança 18 vulnerabilidades no cliente Linux.



Conclusão

Na conclusão deste relatório, destacamos os esforços bem-sucedidos em identificar e corrigir um total de 36 falhas de segurança em dois sistemas operativos diferentes: Windows e Ubuntu. A implementação de políticas e configurações específicas fortaleceu a postura de segurança dos sistemas, reduzindo a exposição a ameaças e fortalecendo a defesa contra possíveis ataques.

Este relatório destaca a importância contínua da segurança cibernética e da adesão às melhores práticas em um ambiente em constante evolução. As ações tomadas demonstram um compromisso em manter a integridade, confidencialidade e disponibilidade dos sistemas de informação.

Reforçamos a necessidade de monitorar constantemente a segurança, atualizar políticas conforme necessário e continuar a adaptarmo-nos às ameaças emergentes. A cibersegurança é uma prática contínua e, com serviços como o Wazuh, estamos melhor preparados para enfrentar os desafios futuros.