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

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:

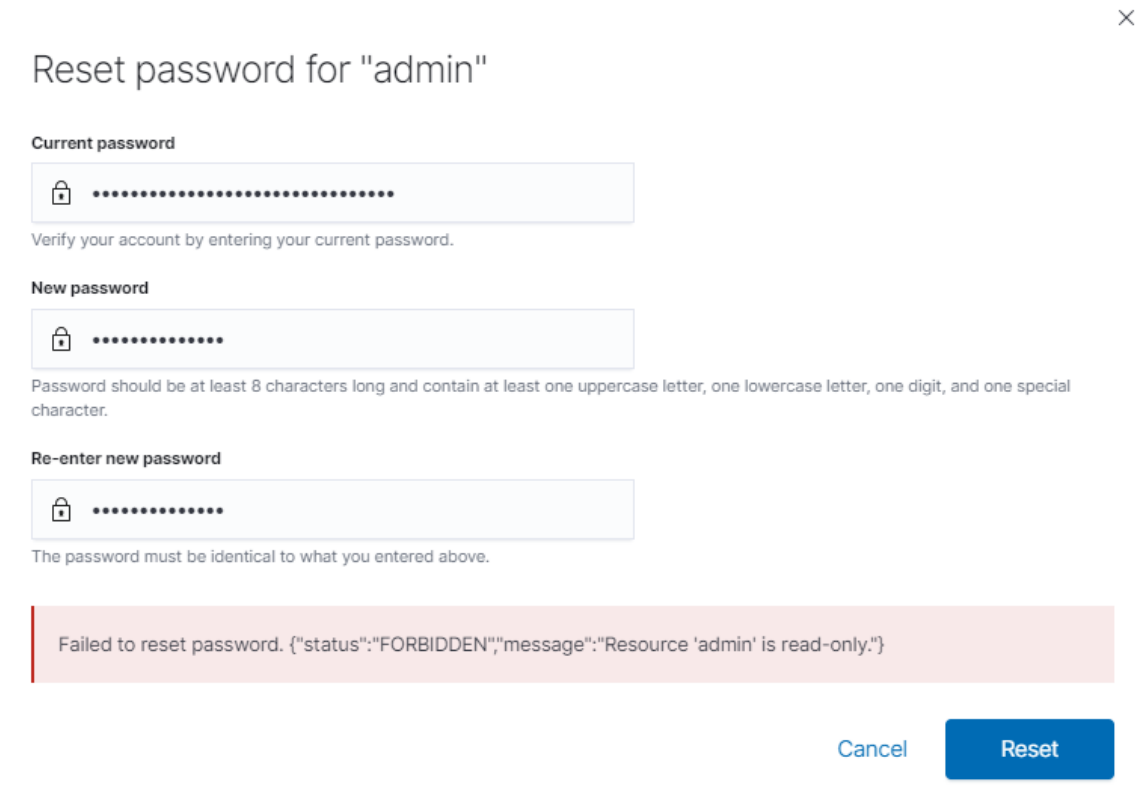
```
root@anaserver:~# apt install apt-transport-https
```

```
root@anaserver:~# curl -sO https://packages.wazuh.com/4.5/wazuh-install.sh && bash ./wazuh-install.s
h -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, certif
icates, 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 100
0
    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:fef8:485/64 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
```

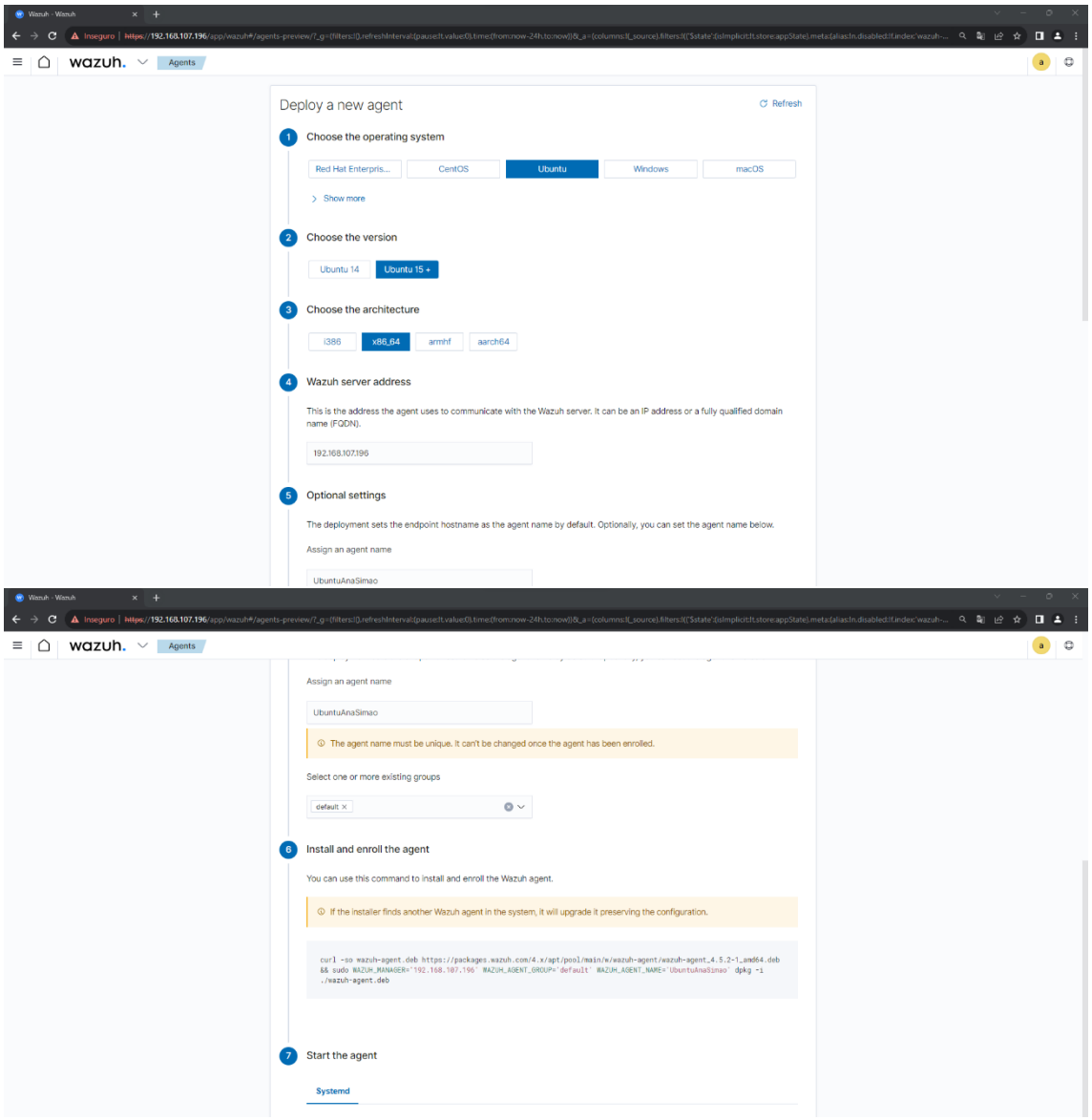
Verificamos o IP de modo a inserir o url correto no browser e, enquanto estudantes de cibersegurança, decidimos que o primeiro passo evidente seria alterar a password default.

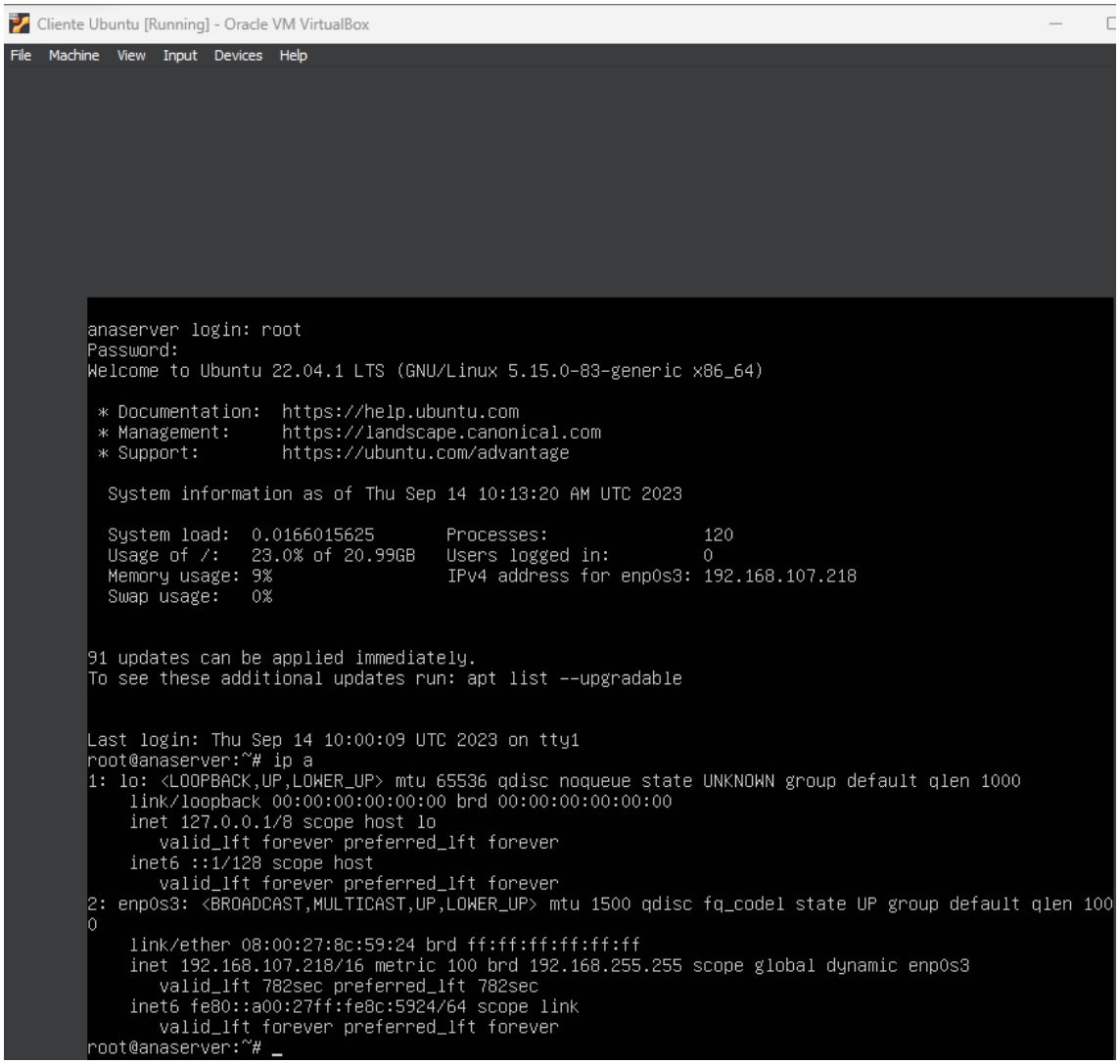


Não sendo possível fazer a alteração no dashboard, procuramos no google e fizemos a alteração diretamente na máquina virtual servidor:

```
root@anaserver:~# curl -so wazuh-passwords-tool.sh https://packages.wazuh.com/4.4/wazuh-passwords-to
ol.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 a
t 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 a
t 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 a
t 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 dashboar
d 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 dashboar
d and Filebeat nodes if necessary, and restart the services.
root@anaserver:~#
```

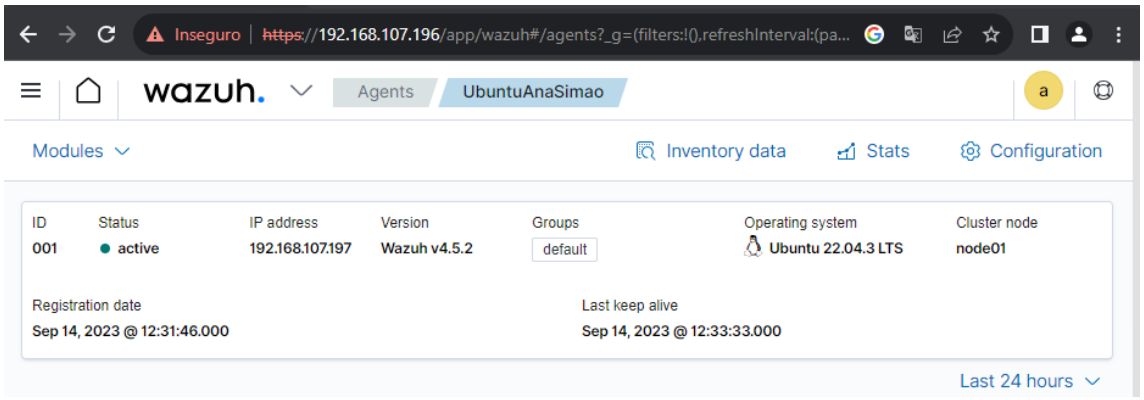
De seguida, procedemos à inserção de máquinas clientes no sistema. Começamos pelo Ubuntu.


wazuh.
Agents
Deploy a new agent
Refresh
1 Choose the operating system
Red Hat Enterpris...
CentOS
Ubuntu
Windows
macOS
Show more
2 Choose the version
Ubuntu 14
Ubuntu 15 +
3 Choose the architecture
i386
x86_64
armhf
aarch64
4 Wazuh server address
This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).
192.168.107.196
5 Optional settings
The deployment sets the endpoint hostname as the agent name by default. Optionally, you can set the agent name below.
Assign an agent name
UbuntuAnaSimao
wazuh.
Agents
Assign an agent name
UbuntuAnaSimao
The agent name must be unique. It can't be changed once the agent has been enrolled.
Select one or more existing groups
default
6 Install and enroll the agent
You can use this command to install and enroll the Wazuh agent.
If the installer finds another Wazuh agent in the system, it will upgrade it preserving the configuration.
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
7 Start the agent
Systemd

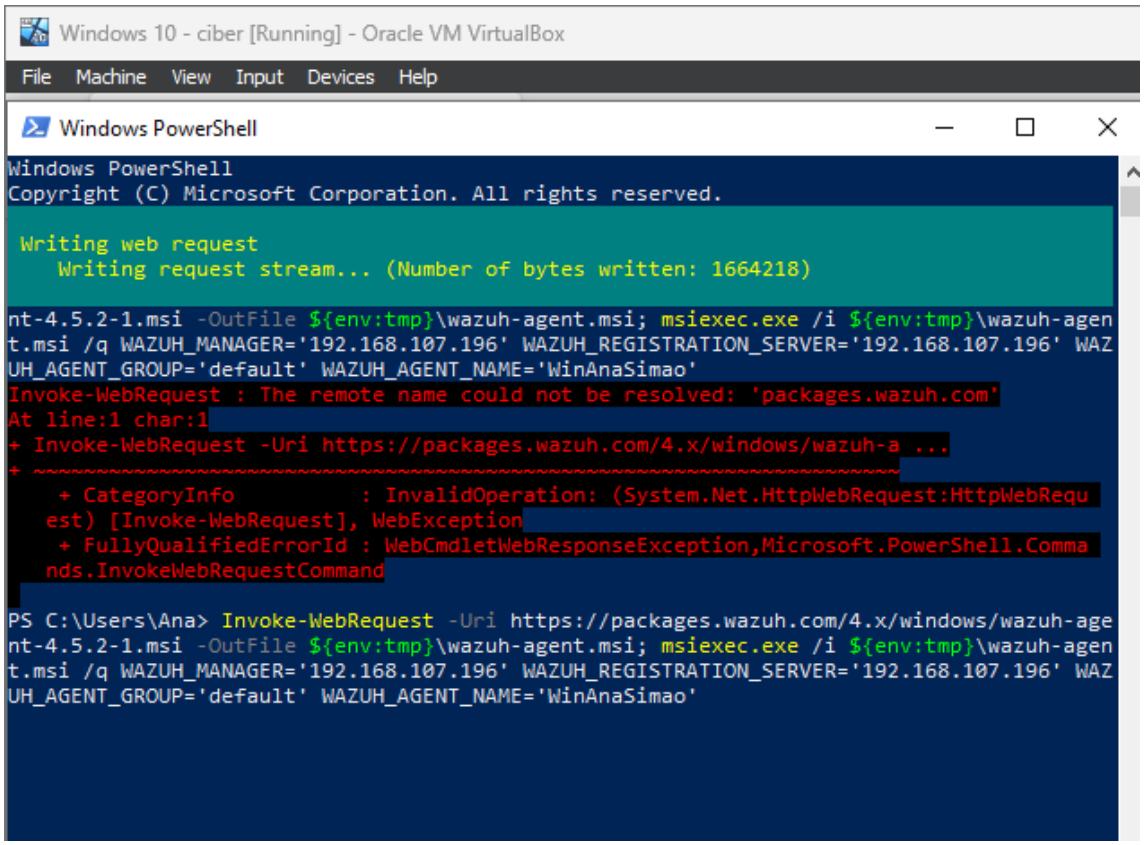



```
root@anaserver:~# curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agen
t/wazuh-agent_4.5.2-1_amd64.deb && sudo WAZUH_MANAGER='192.168.107.196' WAZUH_AGENT_GROUP='default'
WAZUH_AGENT_NAME='UbuntuAnaSimao' dpkg -i ./wazuh-agent.deb
Selecting previously unselected package 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-i
nstall.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/syste
m/wazuh-agent.service.
root@anaserver:~# systemctl start wazuh-agent.service
```

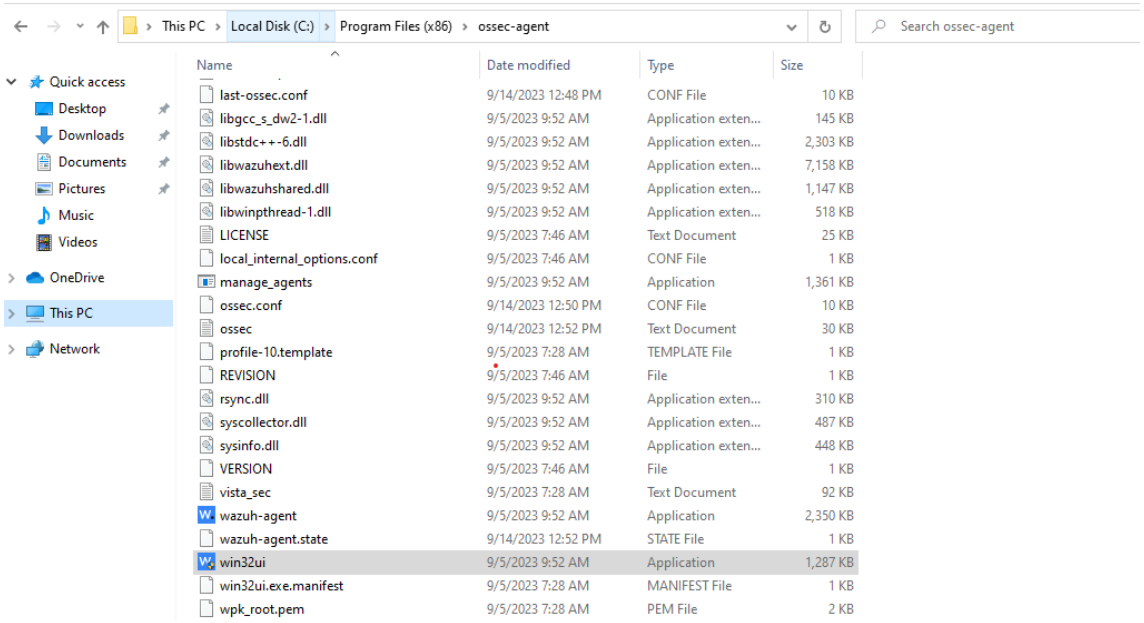


Para o Win10, primeiro tentamos instalar usando a powershell.

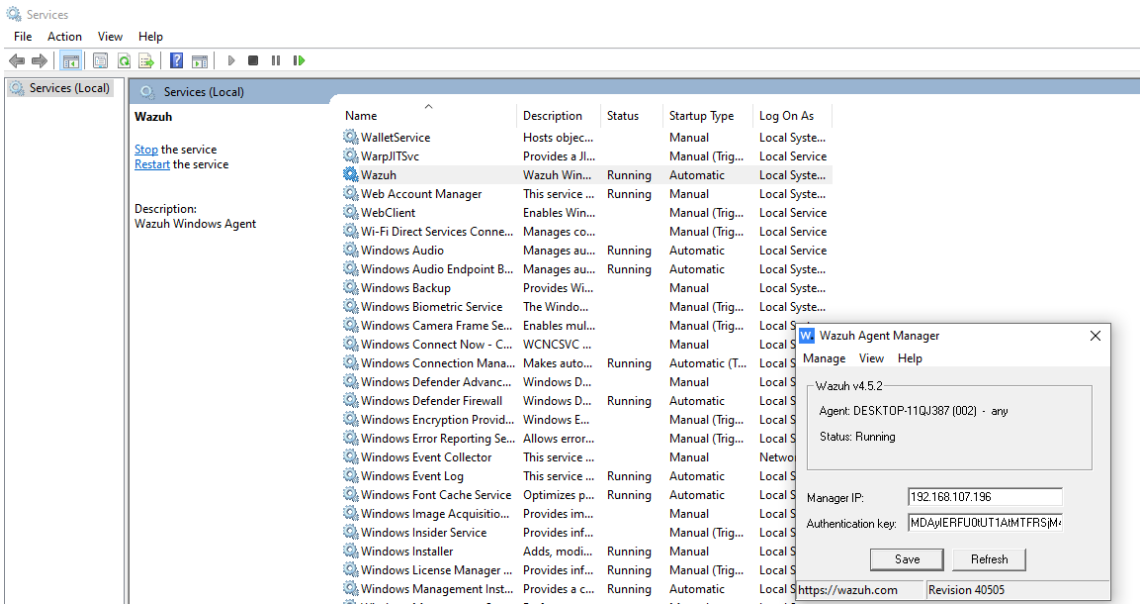


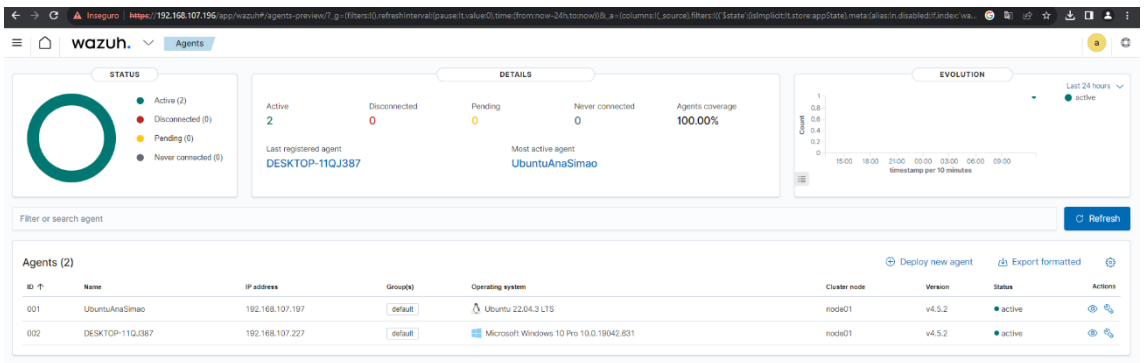
Não deu e fomos ver a documentação no site oficial do wazuh: https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html

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



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

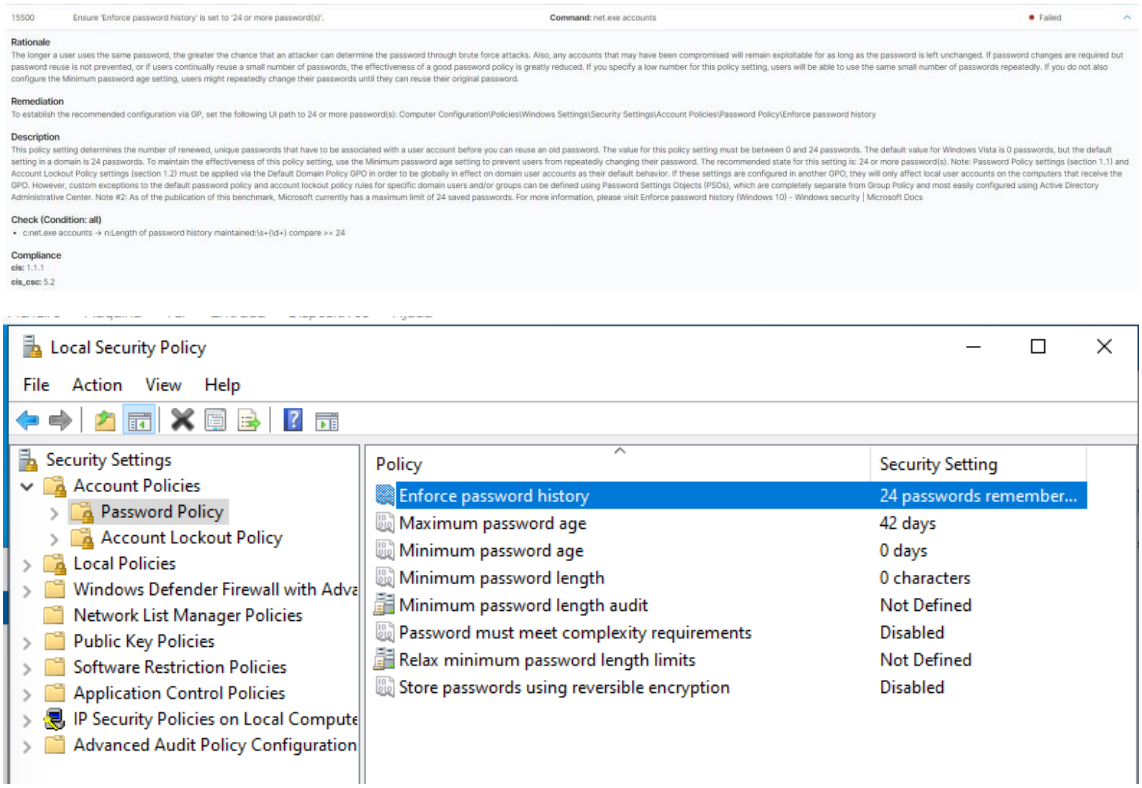




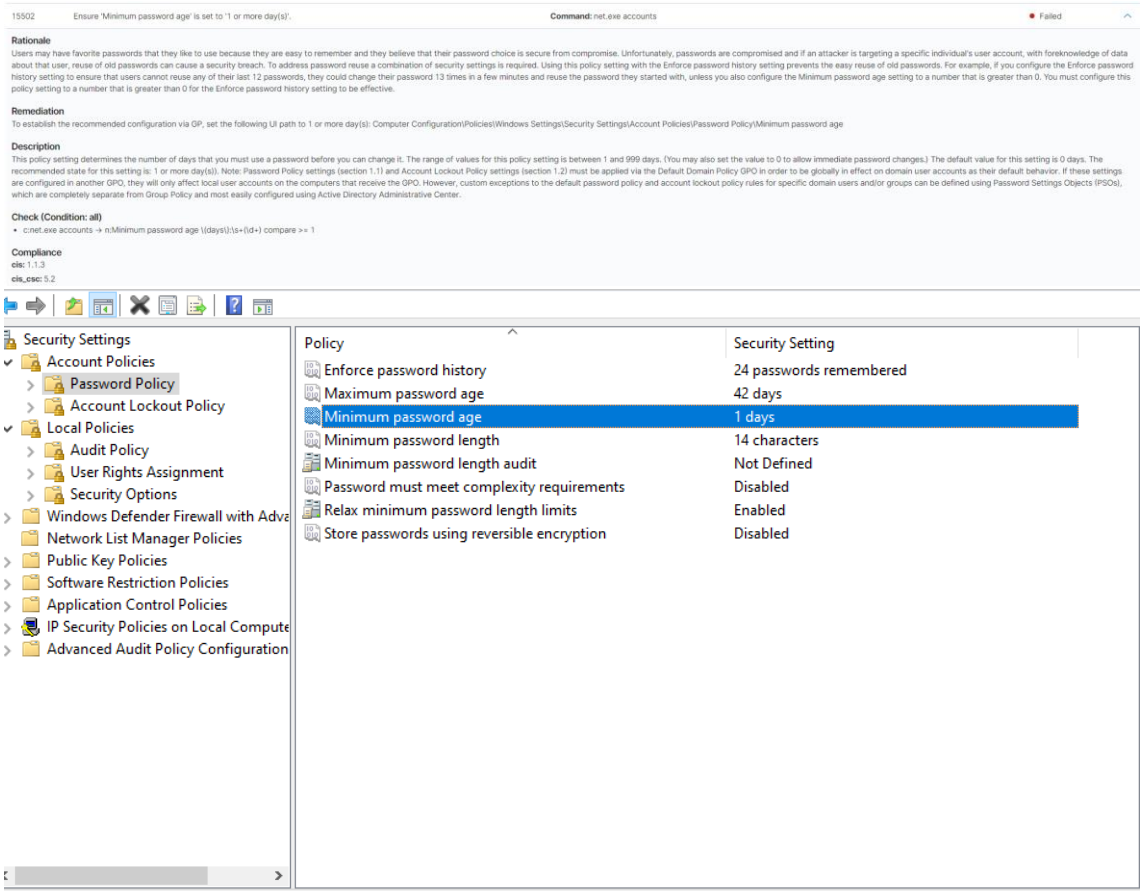
Correção dos erros de logs do Windows 10

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

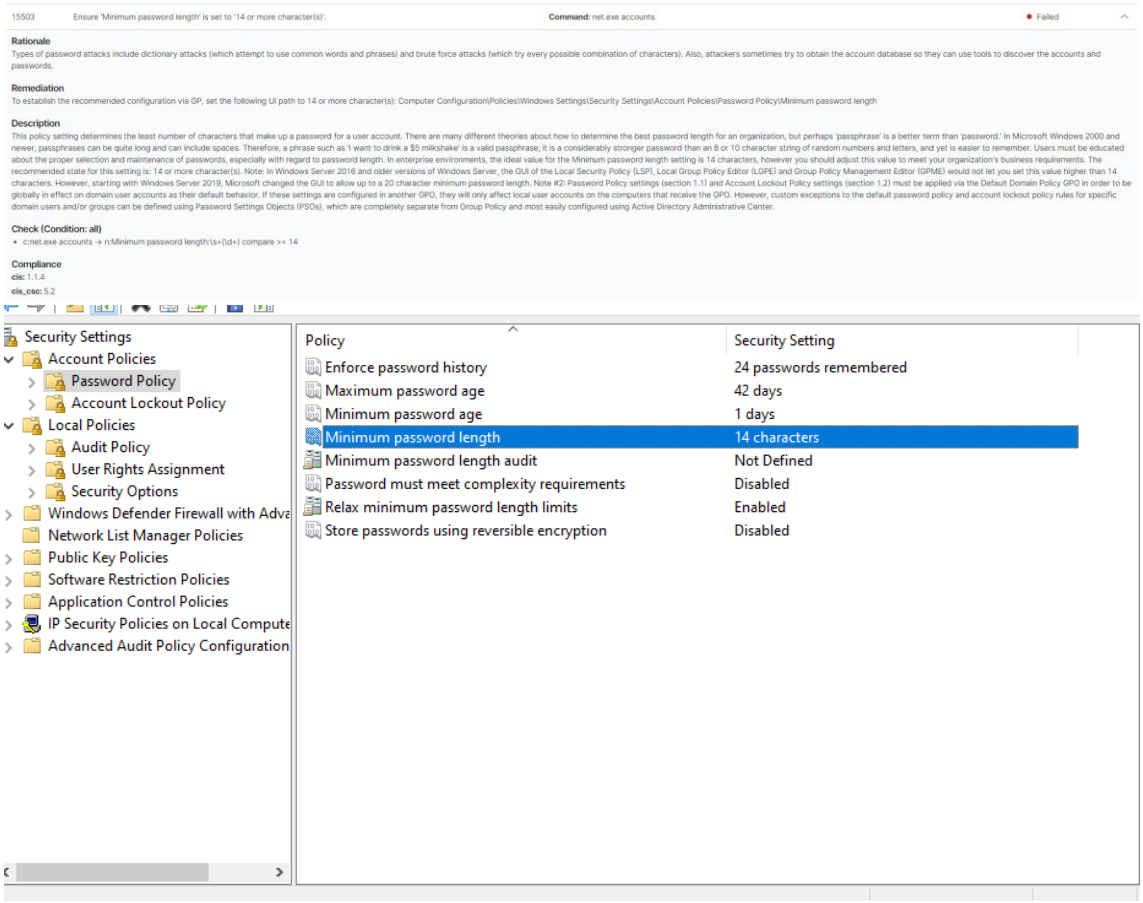
O primeiro erro corrigido foi garantir que um utilizador só pode utilizar a mesma password depois de 24 passwords únicas.



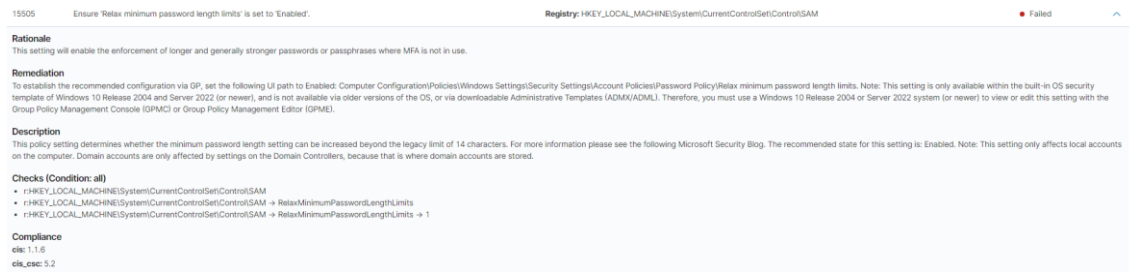
A próxima política implementada foi no âmbito da segurança da password. Estabeleceu-se o tempo mínimo de uso de uma password, garantindo que o número fosse superior a 0, neste caso 1.

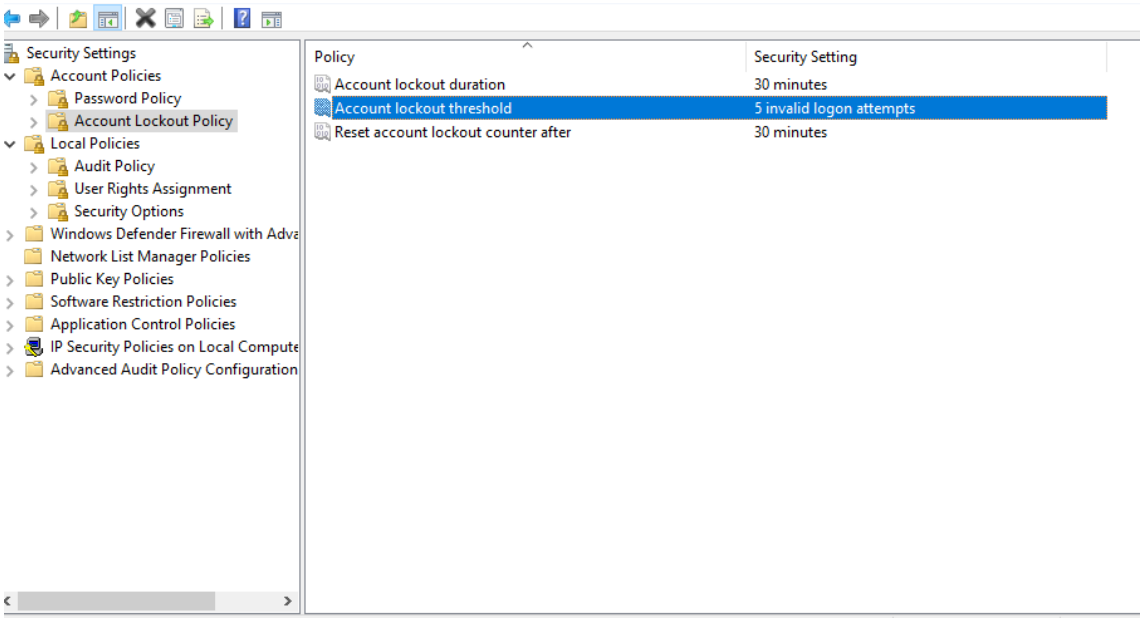


Estabeleceu-se o comprimento de uma password para 14 caracteres, como forma de garantir uma complexidade minima, dificultando ataques de força bruta.

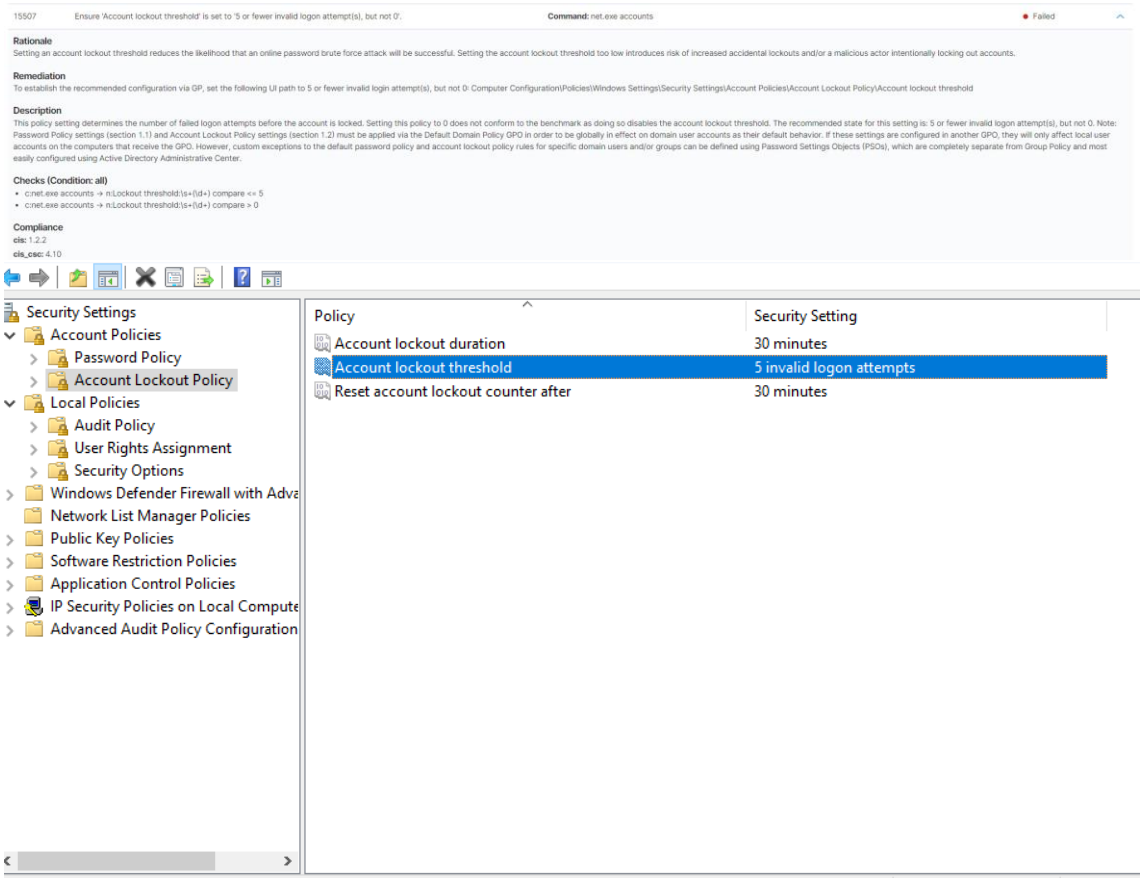


Ao ativar (enable) a seguinte “feature” reforçamos novamente a segurança da password, afetando apenas contas locais.

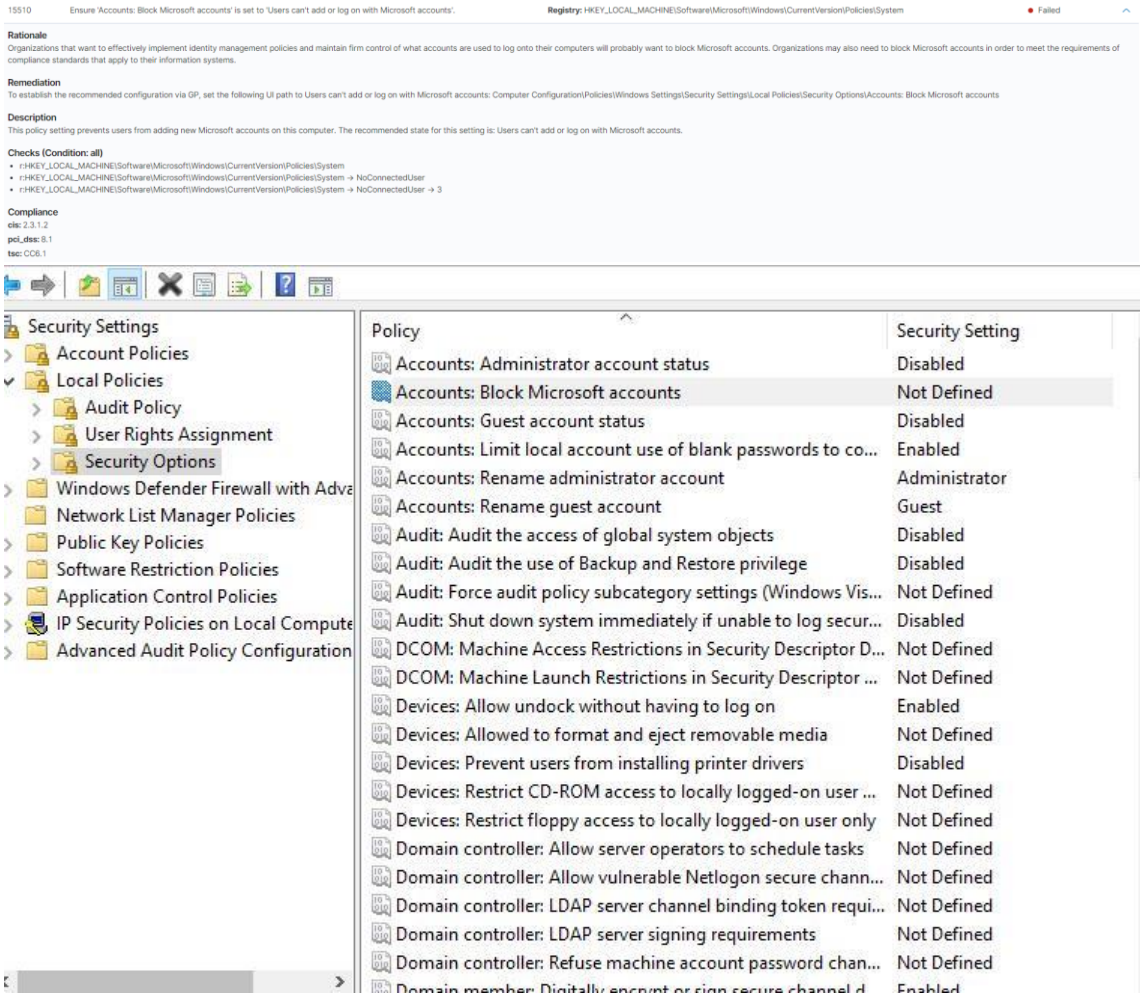


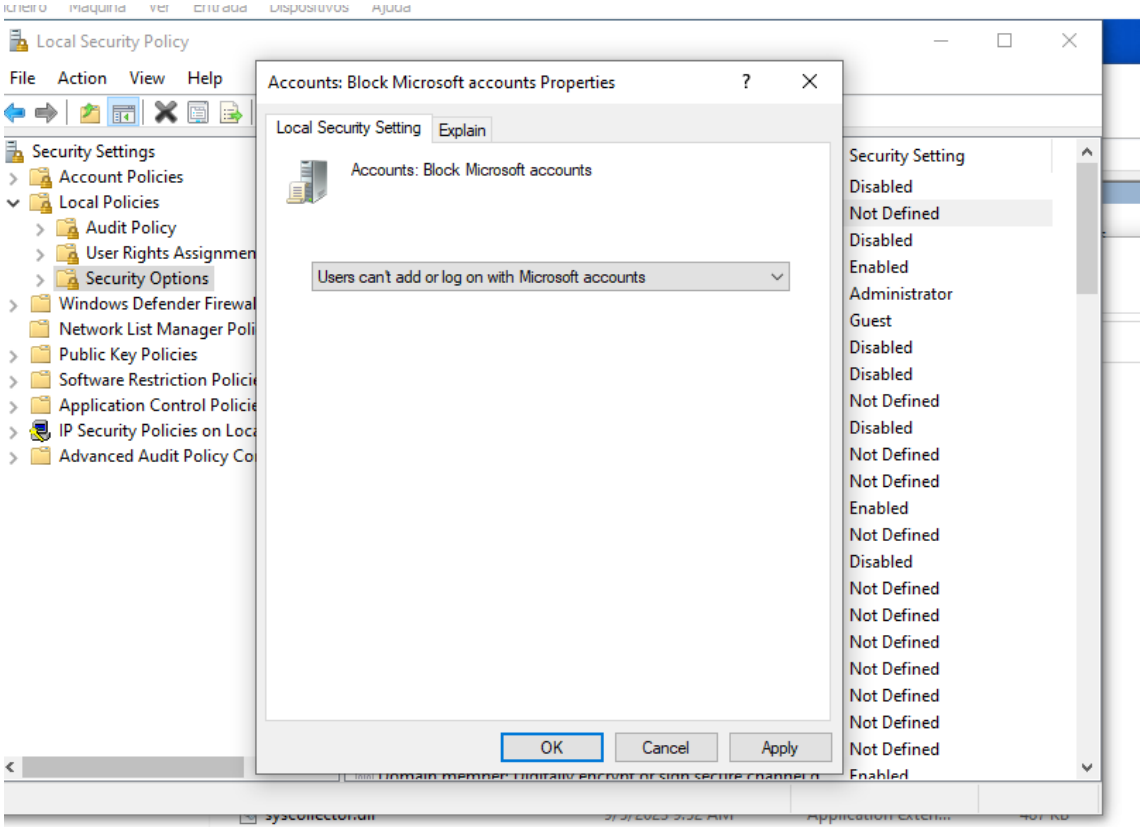


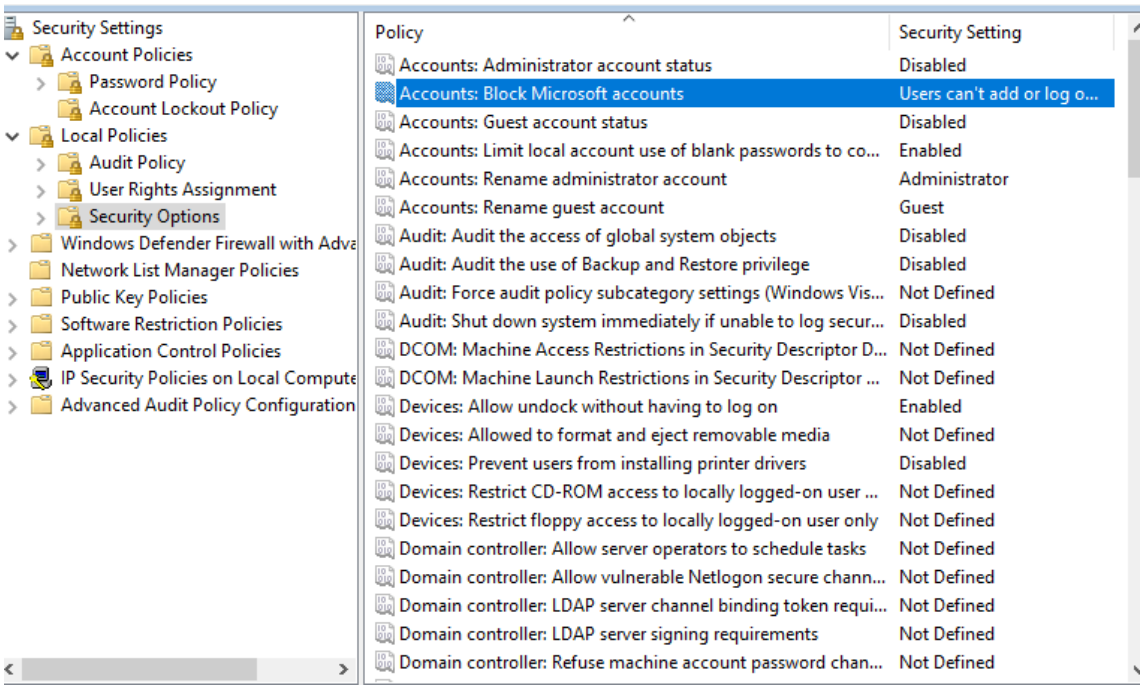
Fixamos o número mínimo de vezes que o utilizador pode falhar o seu logon em cinco, que é o recomendado (substituindo o valor anterior que era zero).



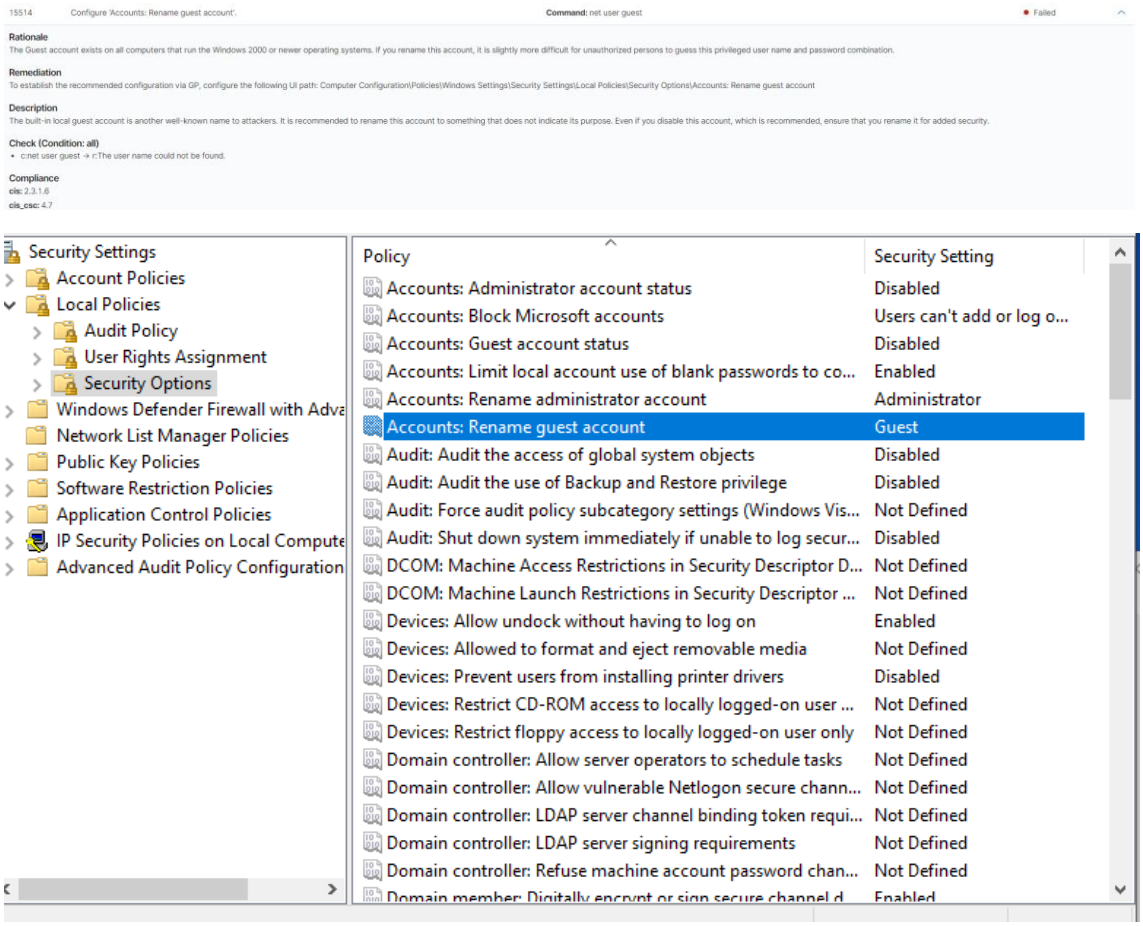
Acrescentamos uma política que previne que o utilizador acrescente uma nova conta da Microsoft ou fazer logon numa outra.

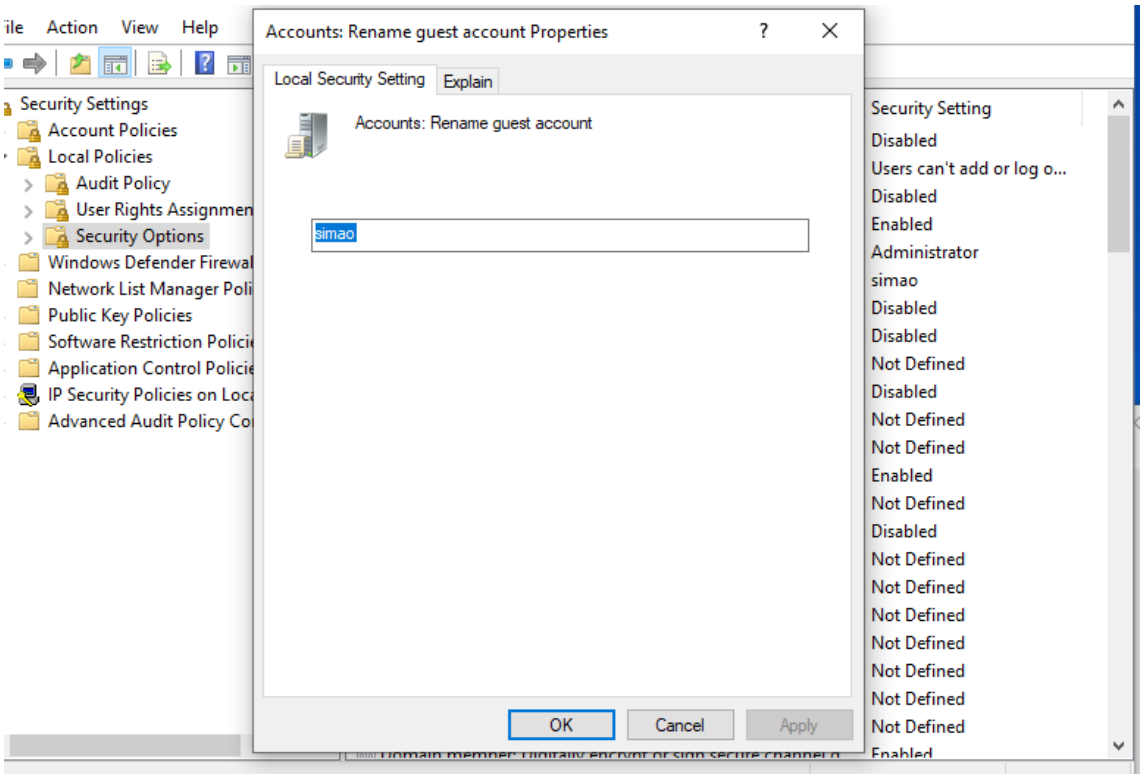


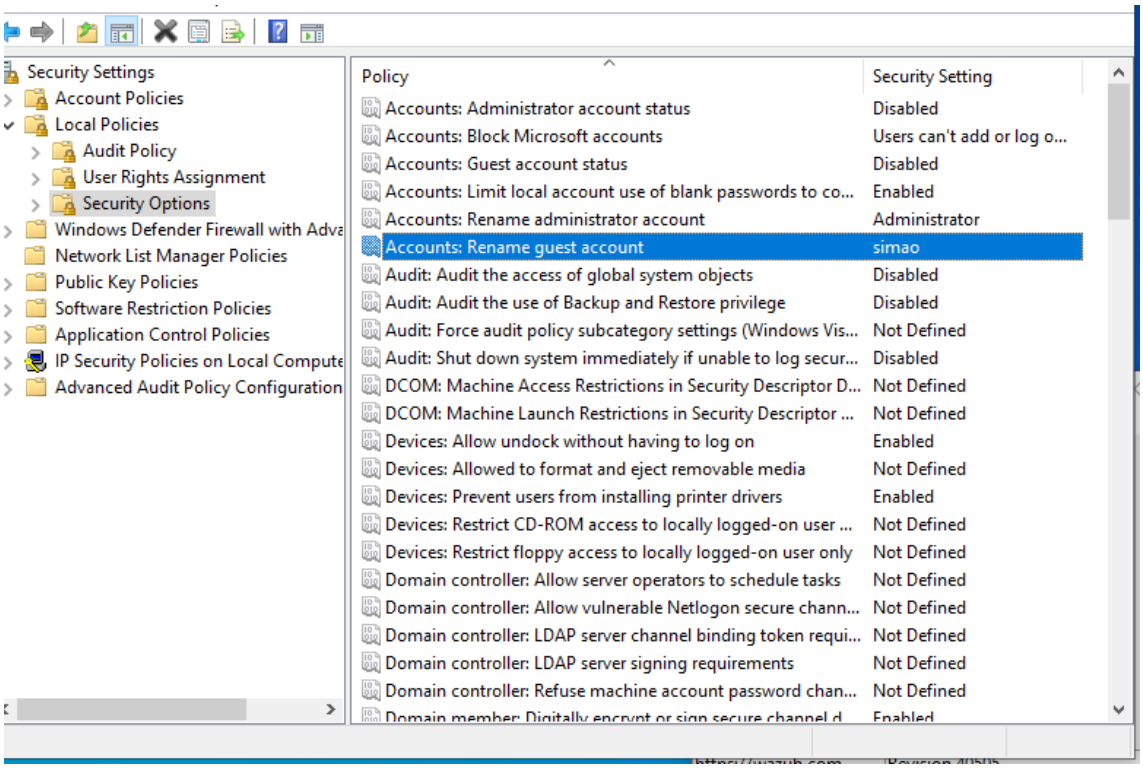




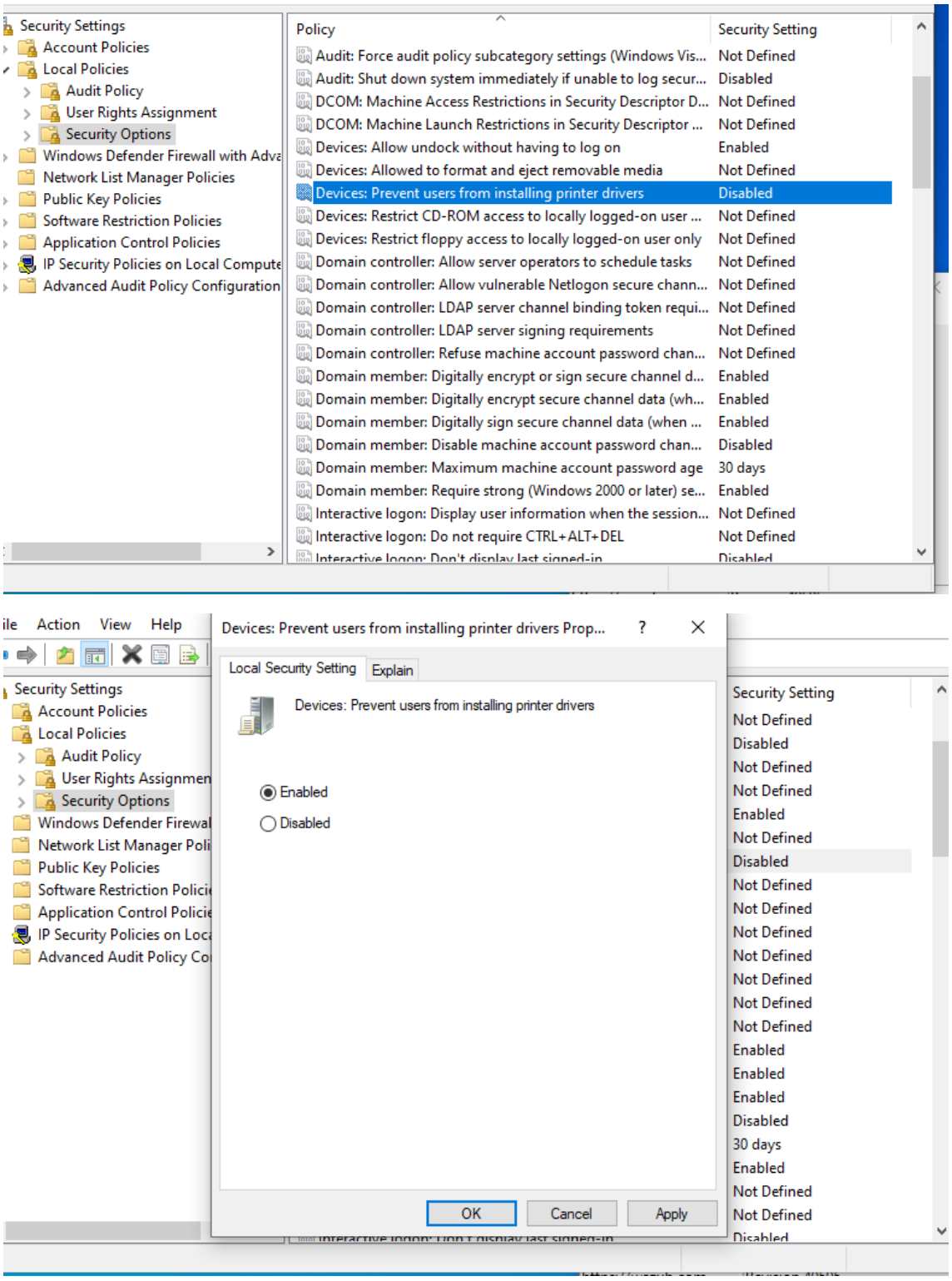
Existem termos bastante utilizados em ataques por serem credenciais comuns, um dos quais é guest. Tendo isto em mente, decidimos renomear a conta convidado para simao, sendo desta forma mais difícil para pessoas não autorizadas acederem à máquina.

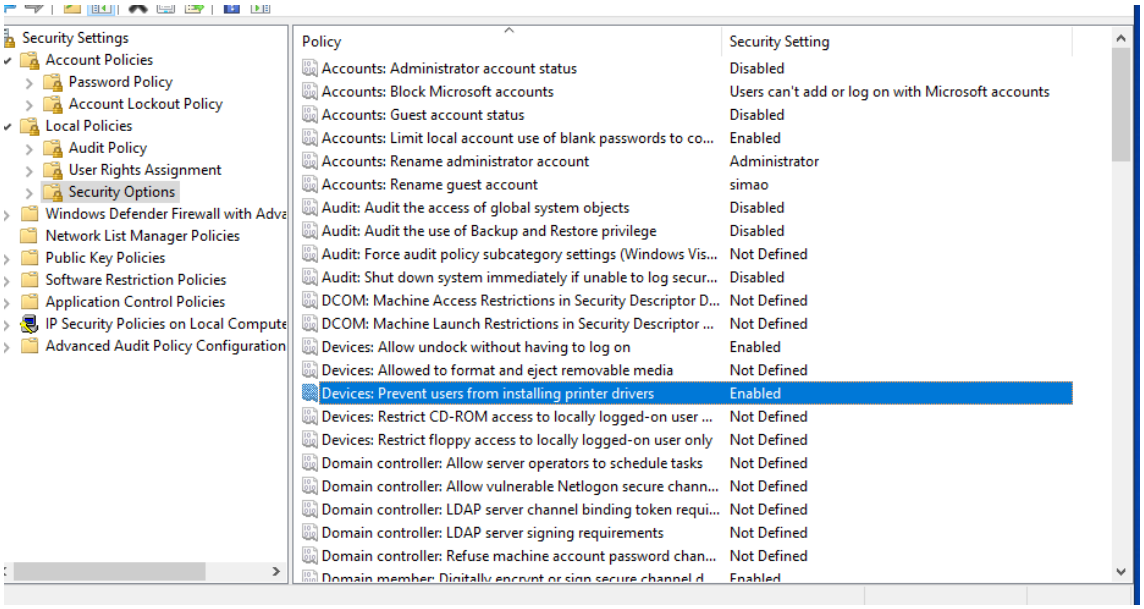

15514 Configure 'Accounts: Rename guest account'. Command: net user guest Failed
Rationale
The Guest account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.
Remediation
To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\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)
c:\net user guest -> r:The user name could not be found.
Compliance
cis: 2.3.1.6
cis_csc: 4.7
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Compute
Advanced Audit Policy Configuration
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


ile Action View Help
Accounts: Rename guest account Properties
Local Security Setting
Explain
Accounts: Rename guest account
simao
OK
Cancel
Apply
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignmen
Security Options
Windows Defender Firewal
Network List Manager Poli
Public Key Policies
Software Restriction Policie
Application Control Policie
IP Security Policies on Loca
Advanced Audit Policy Co
Security Setting
Disabled
Users can't add or log o...
Disabled
Enabled
Administrator
simao
Disabled
Disabled
Not Defined
Disabled
Not Defined
Not Defined
Enabled
Not Defined
Disabled
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined

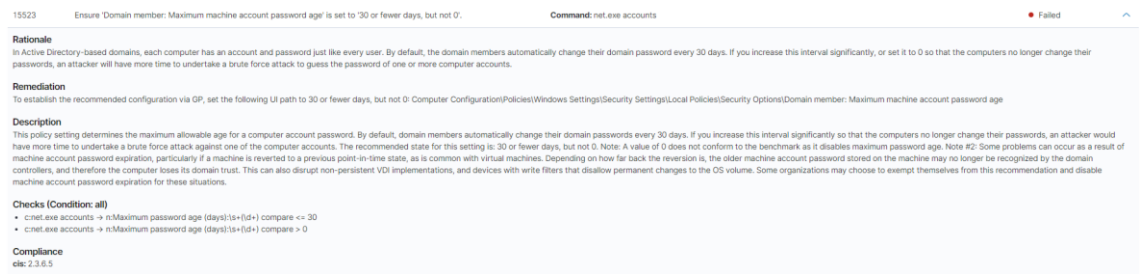


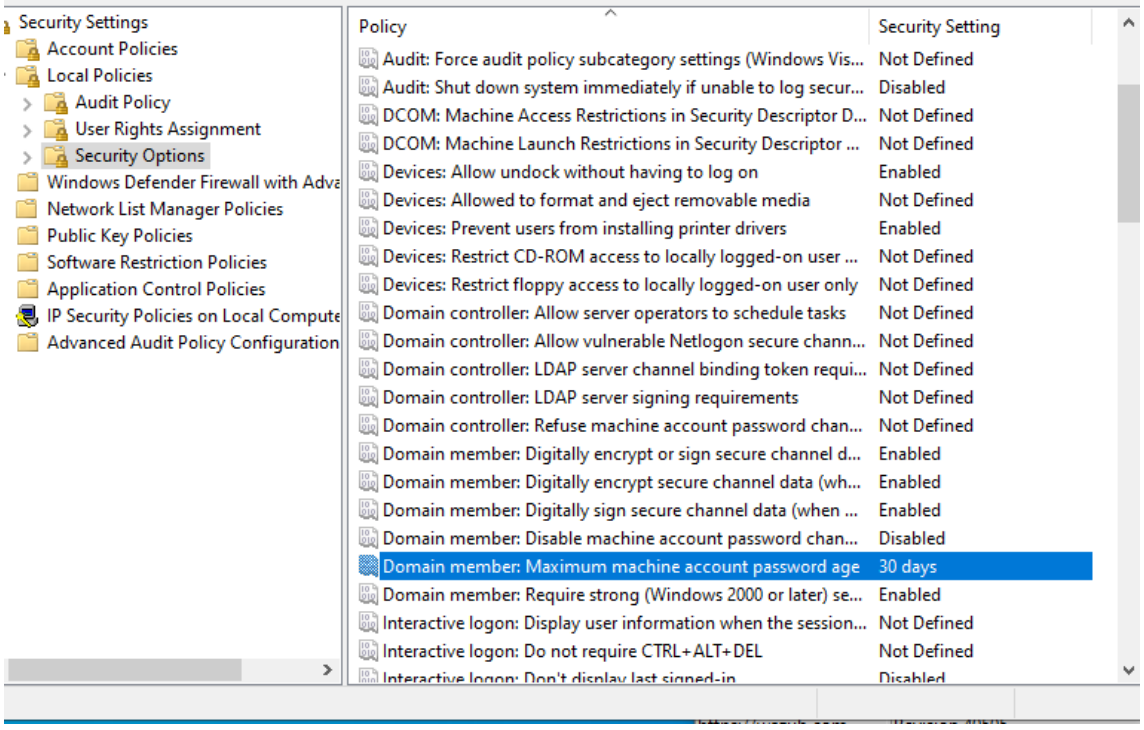
Através de uma política de grupo, prevenimos que os utilizadores possam instalar impressoras, deixando essa regalia para administradores. Assim, evita-se que dispositivos desconhecidos sejam conectados à rede.

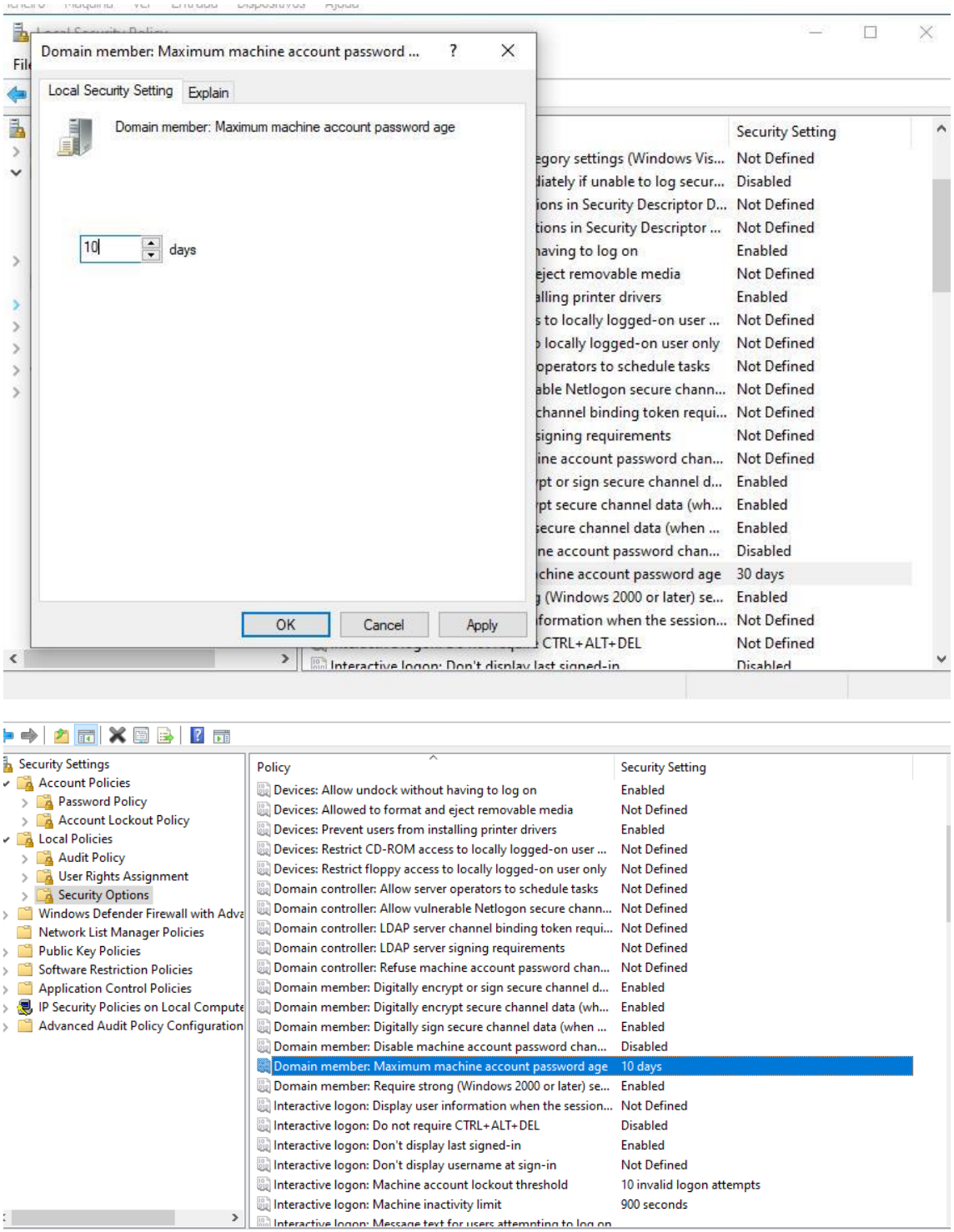

Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
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 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
Devices: Prevent users from installing printer drivers Prop...
Local Security Setting
Explain
Devices: Prevent users from installing printer drivers
Enabled
Disabled
OK
Cancel
Apply



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.

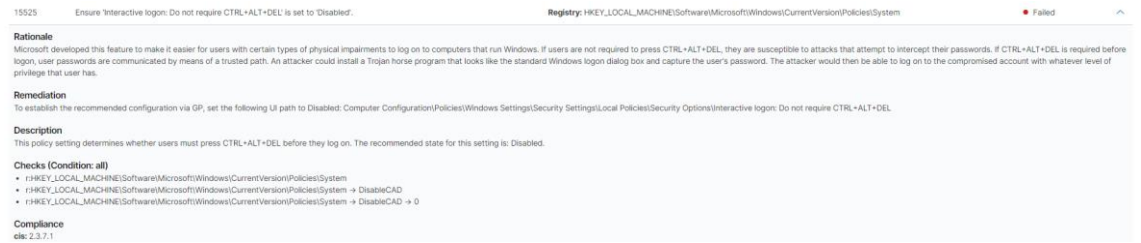


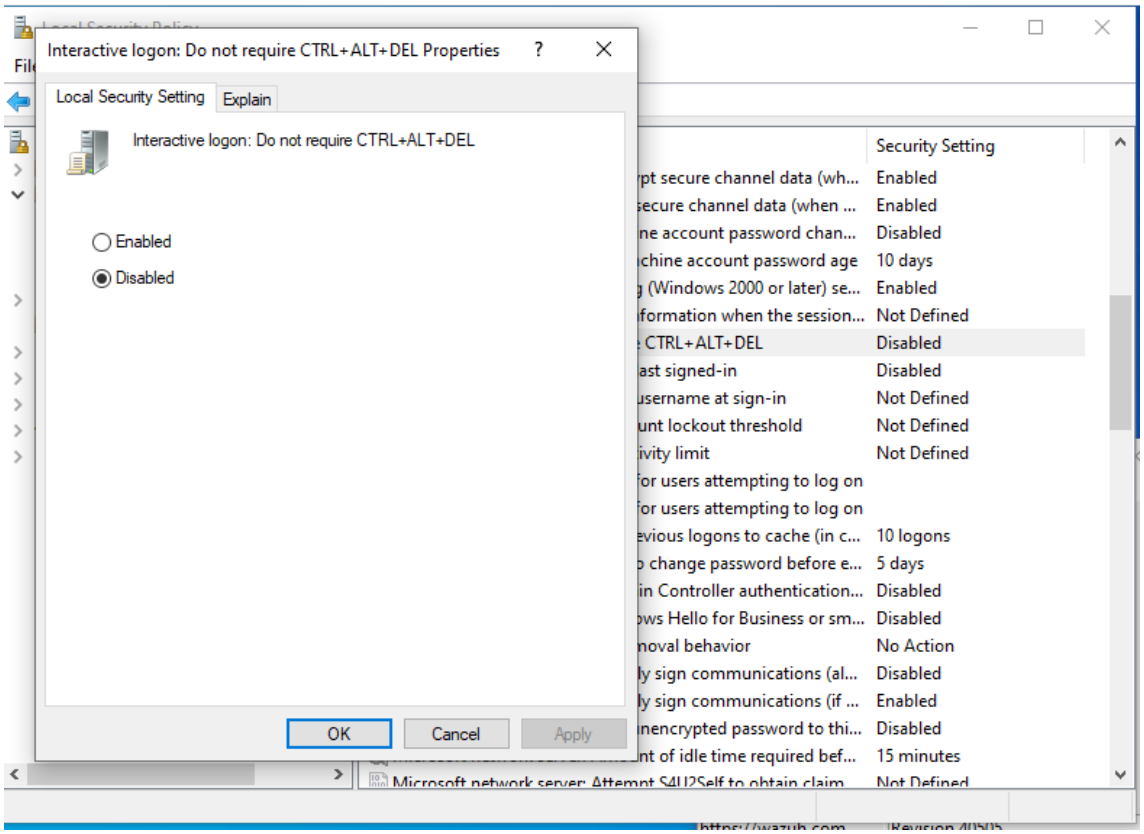




A combinação Ctrl+Alt+Del é frequentemente usada como um atalho para funções de segurança, como o gerenciador de tarefas ou a tela de bloqueio. Desabilitá-la pode simplificar a experiência do utilizador, tornando o sistema mais amigável. Ao desabilitar a combinação Ctrl+Alt+Del, é

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 definied.





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'. **Registry:** HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System Failed

Rationale

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

Remediation

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: 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

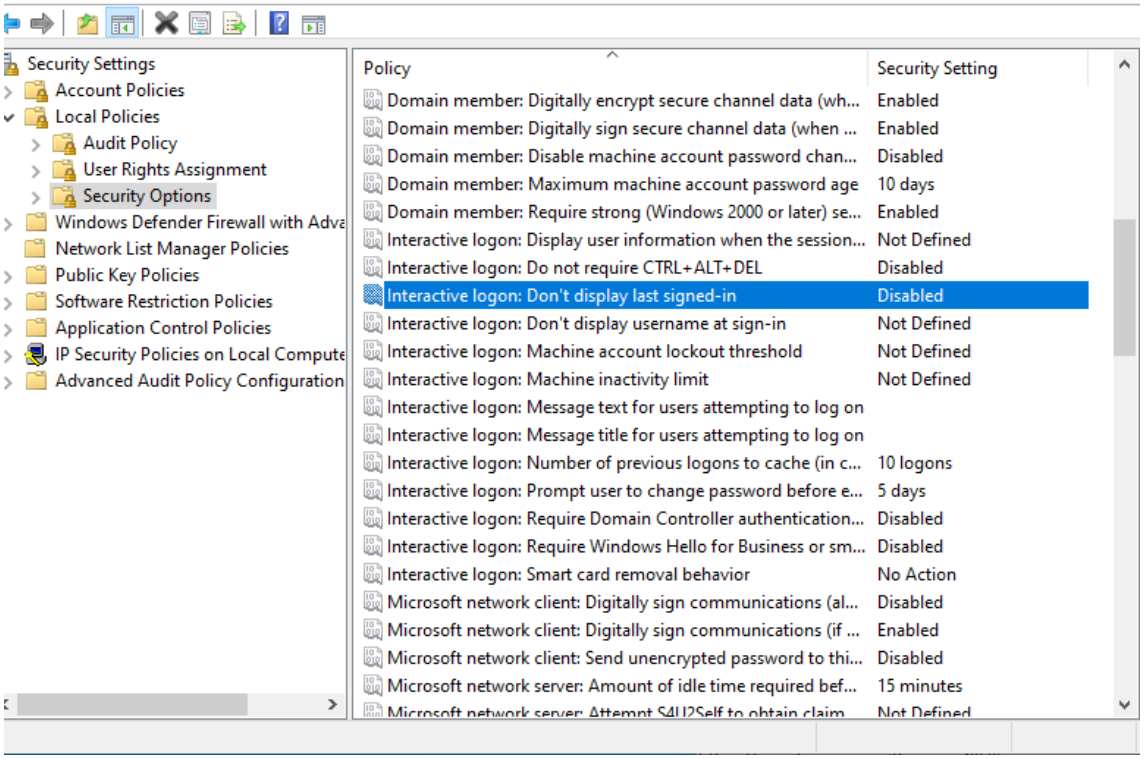
This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens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

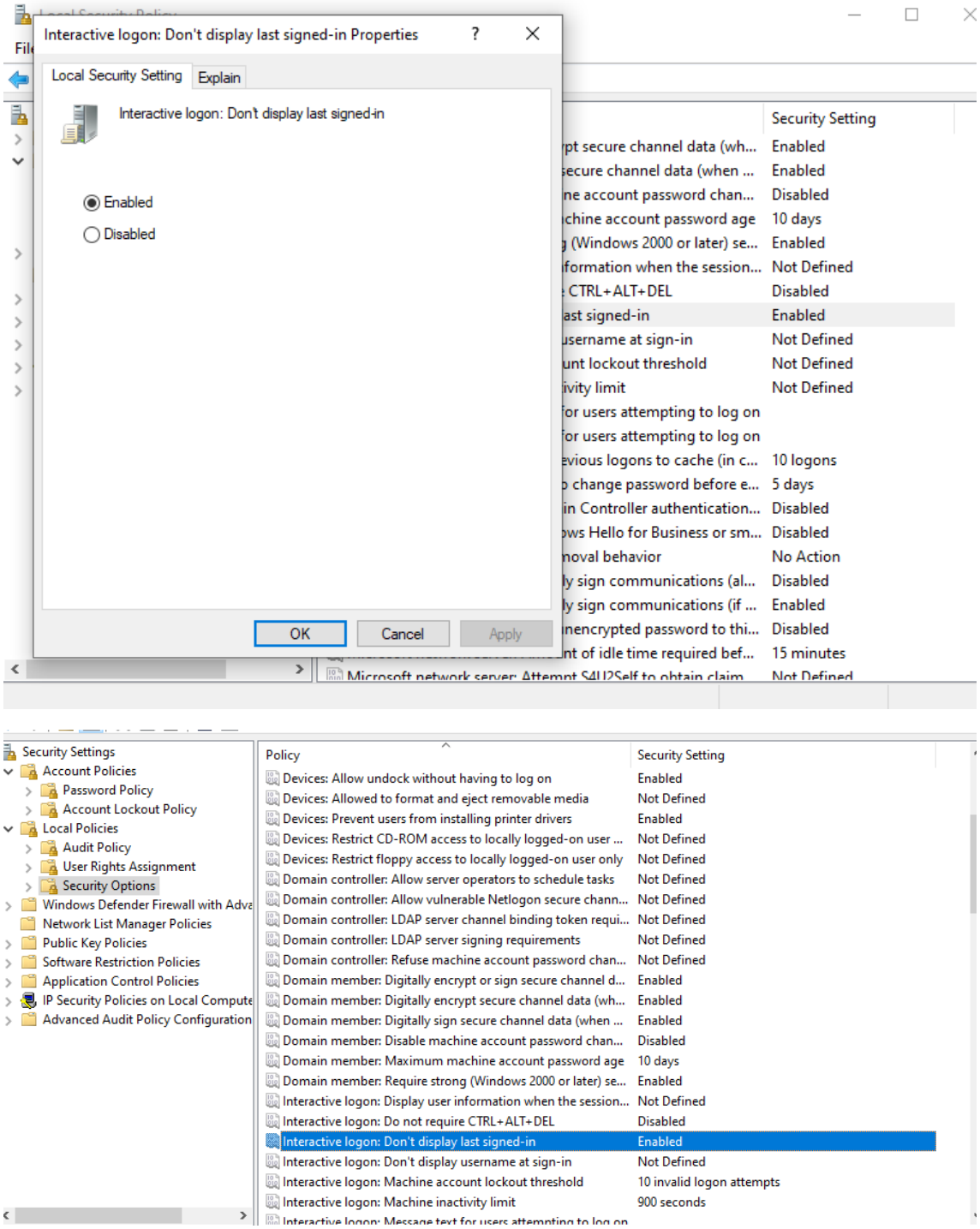
Checks (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> DontDisplayLastUserName
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> DontDisplayLastUserName -> 1

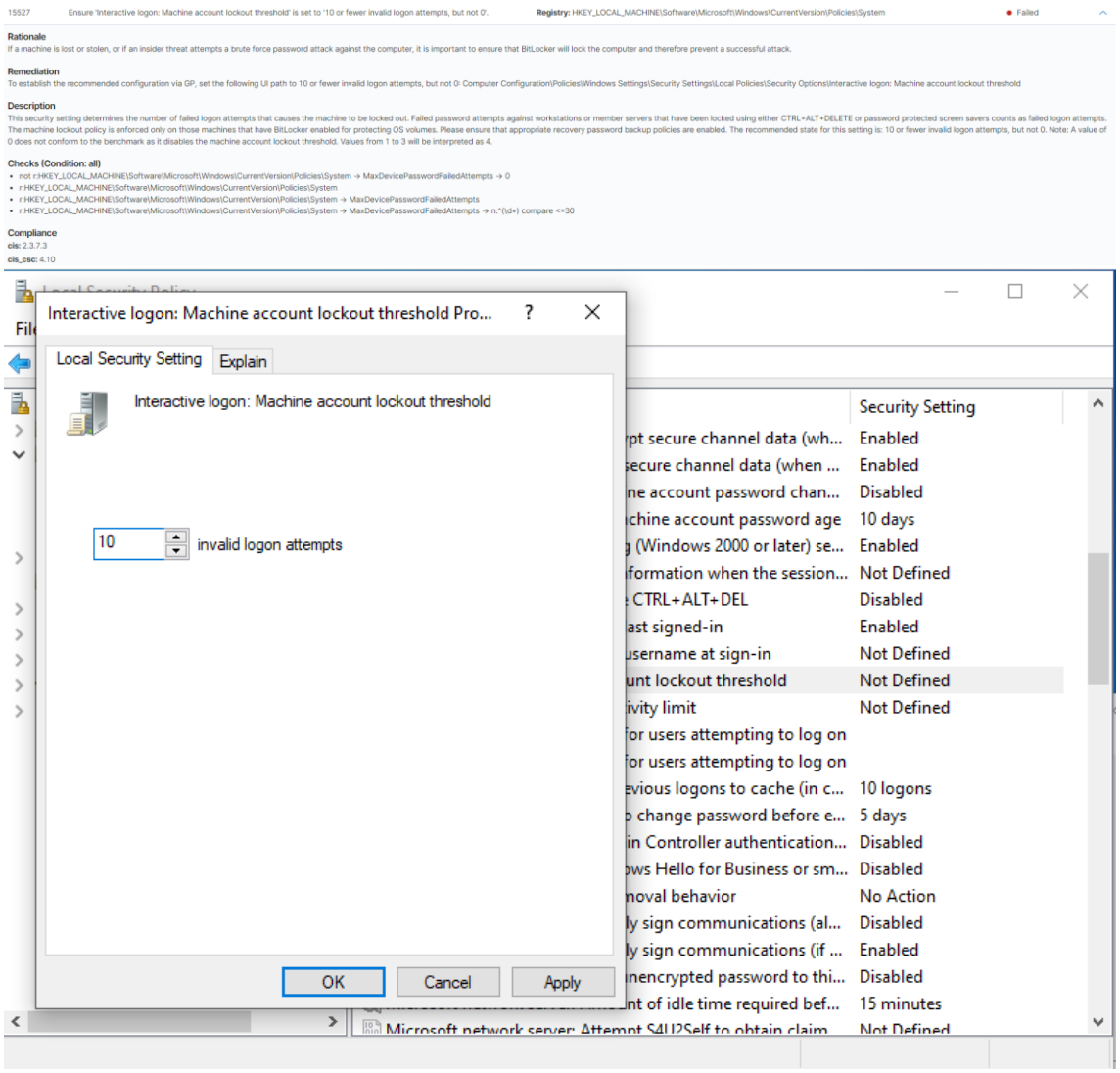
Compliance

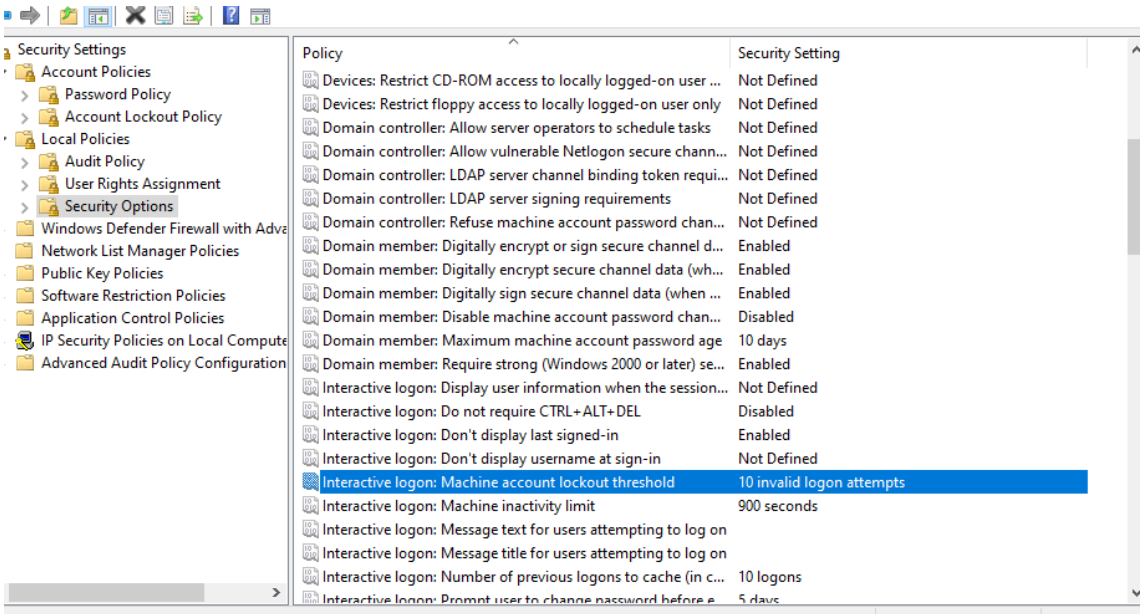
cis: 2.3.7.2
gdpr_IV: 35.7.d
gpg_13: 4.3
hipaa: 164.312.b
nist_800_53: CM.1
pci_dss: 2.2.3
tsc: CC5.2



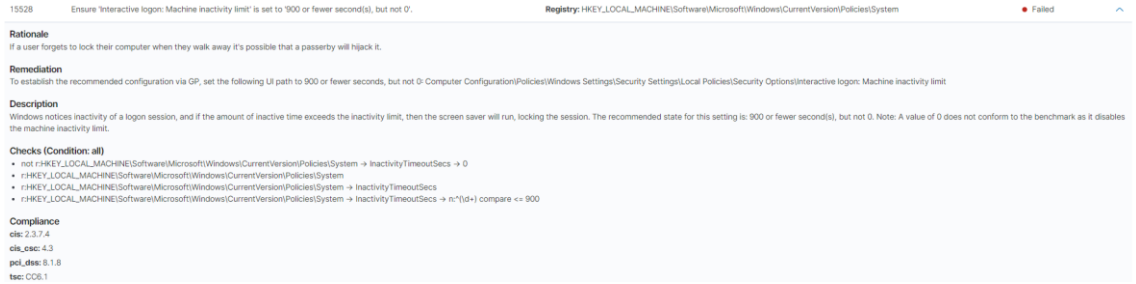

Interactive logon: Don't display last signed-in Properties
Local Security Setting
Explain
Interactive logon: Don't display last signed-in
Enabled
Disabled
OK
Cancel
Apply
Security Setting
Enabled
Enabled
Disabled
10 days
Enabled
Not Defined
Disabled
Enabled
Not Defined
Not Defined
Not Defined
10 logons
5 days
Disabled
Disabled
No Action
Disabled
Enabled
Disabled
15 minutes
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
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

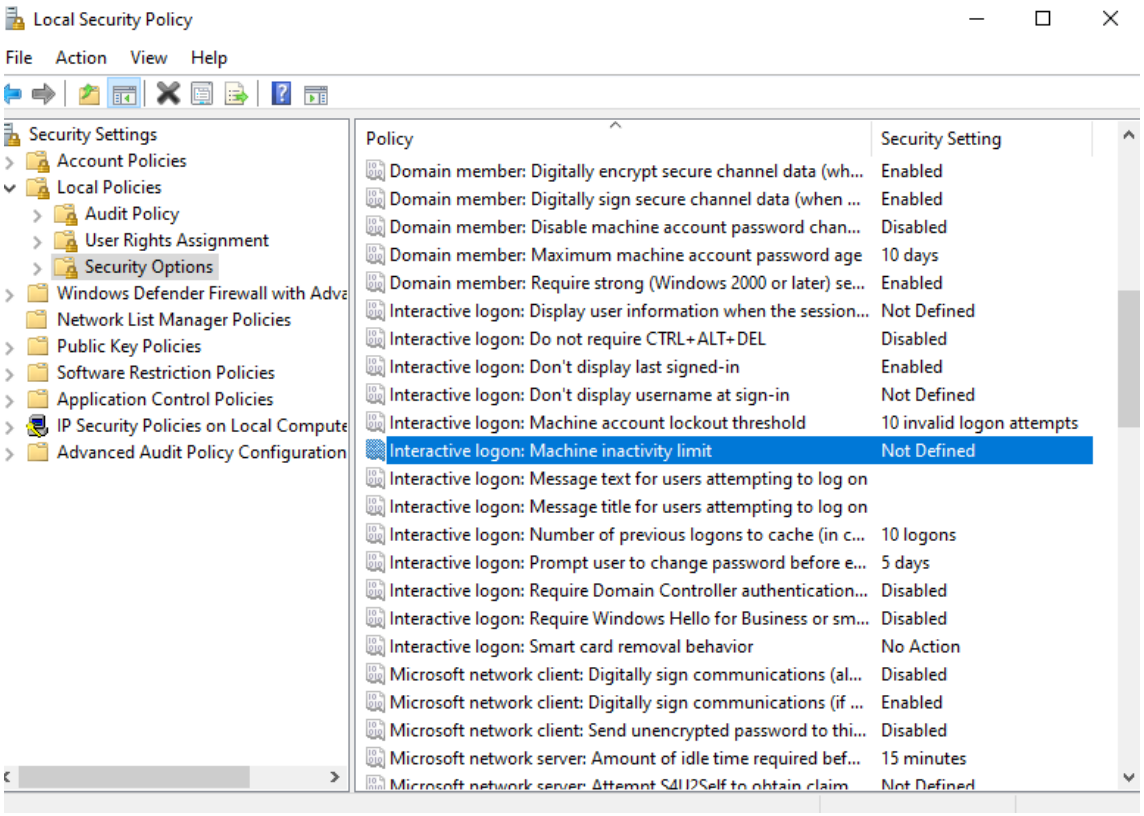
Para impedir ataques contínuos de tentativa de adivinhar uma password é recomendado colocar um limite de tentativas, neste caso 10. Já tínhamos aplicado esta política relativamente a contas, neste caso incide sobre a máquina.

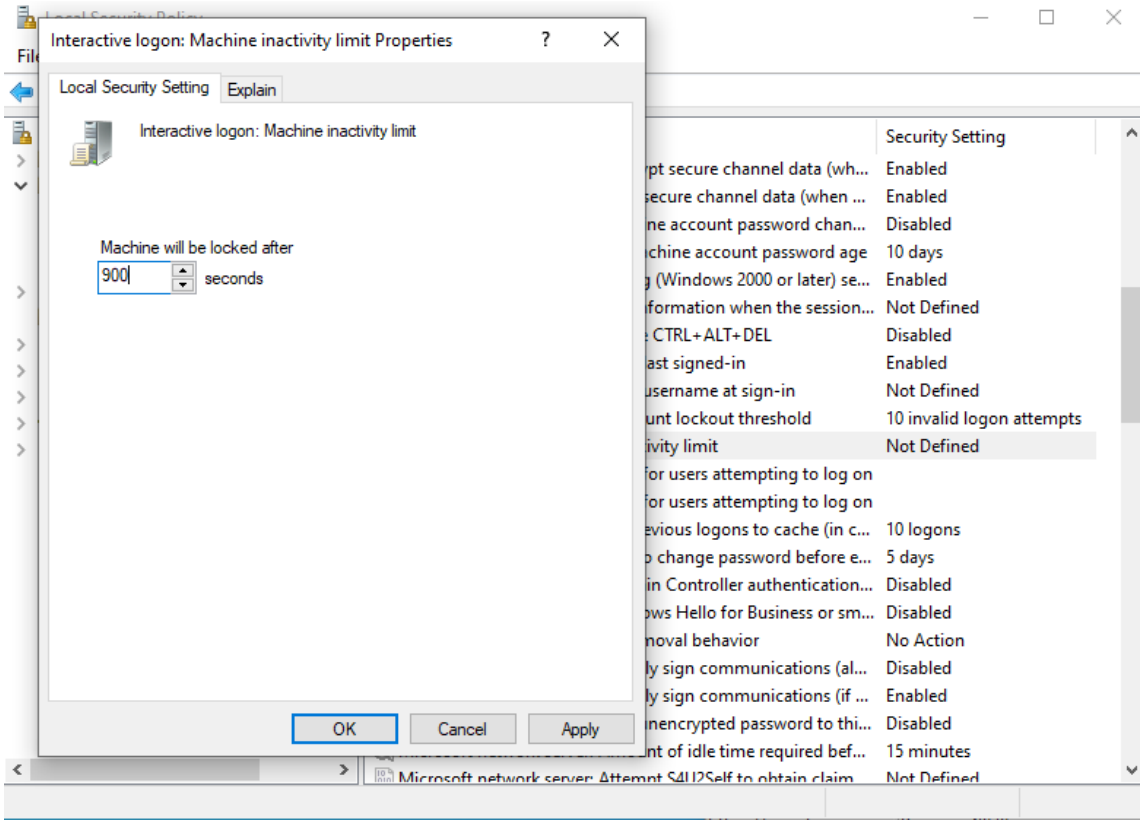


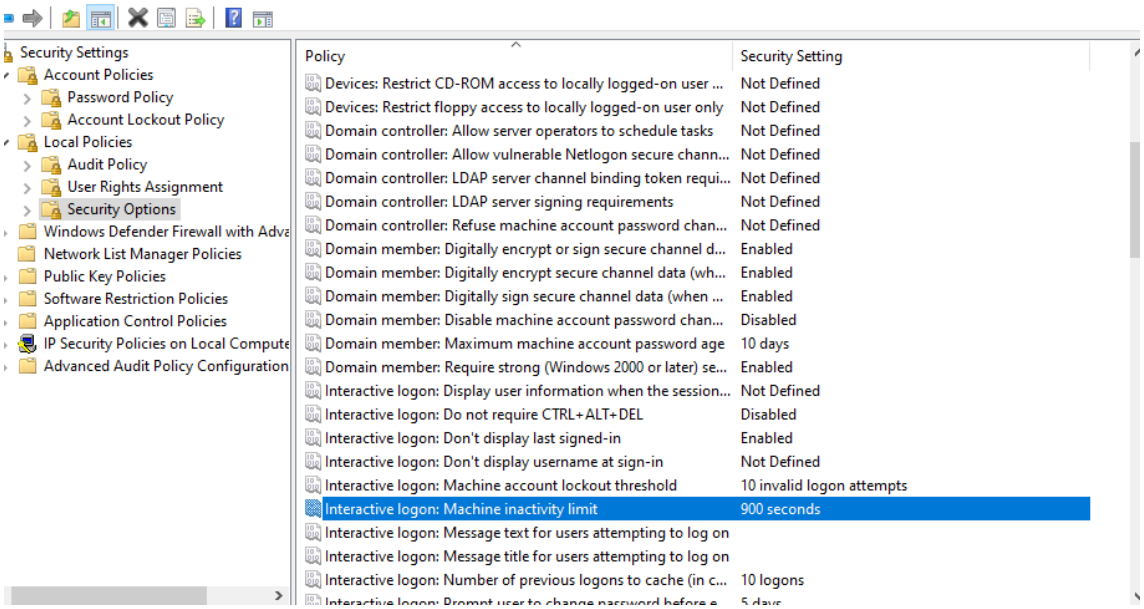


Para bloquear uma sessão, porque o utilizador esqueceu-se de fazer log-out, alteramos esta política de forma a automaticamente o fazer dentro de 900 segundos.

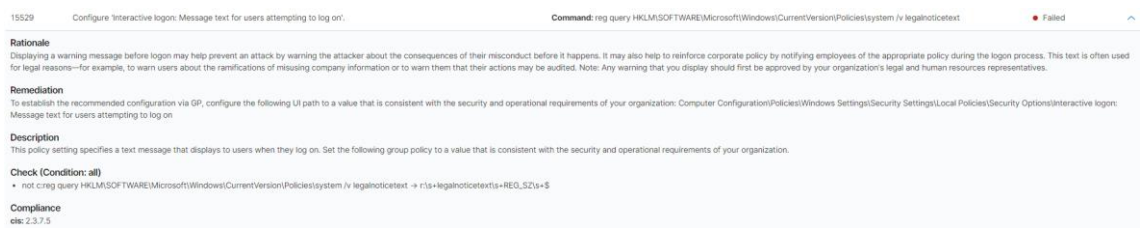


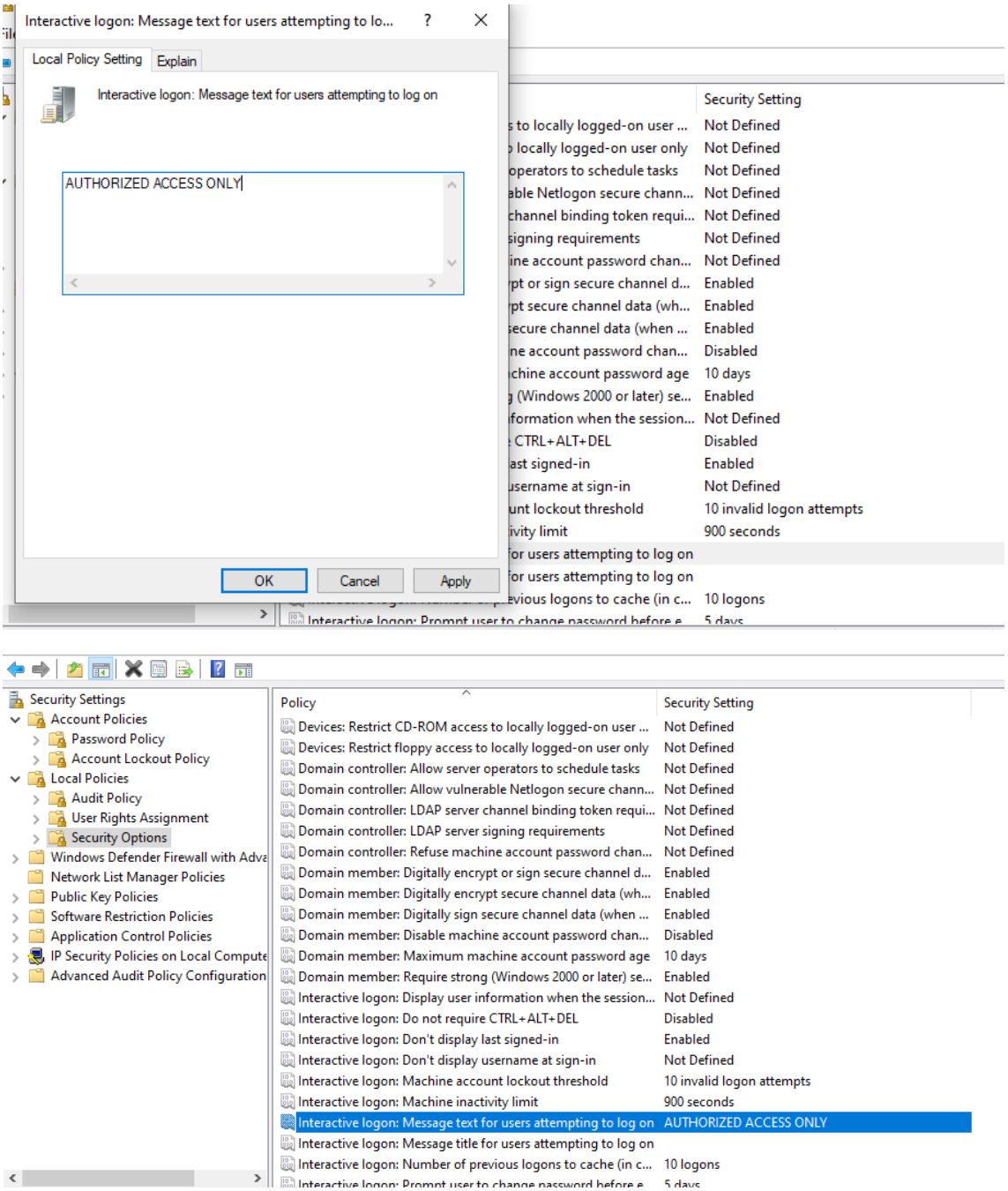




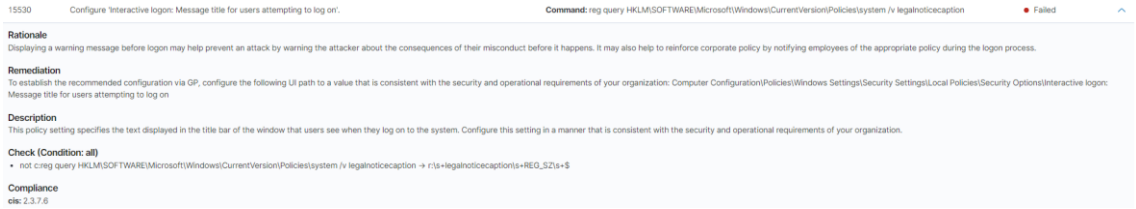


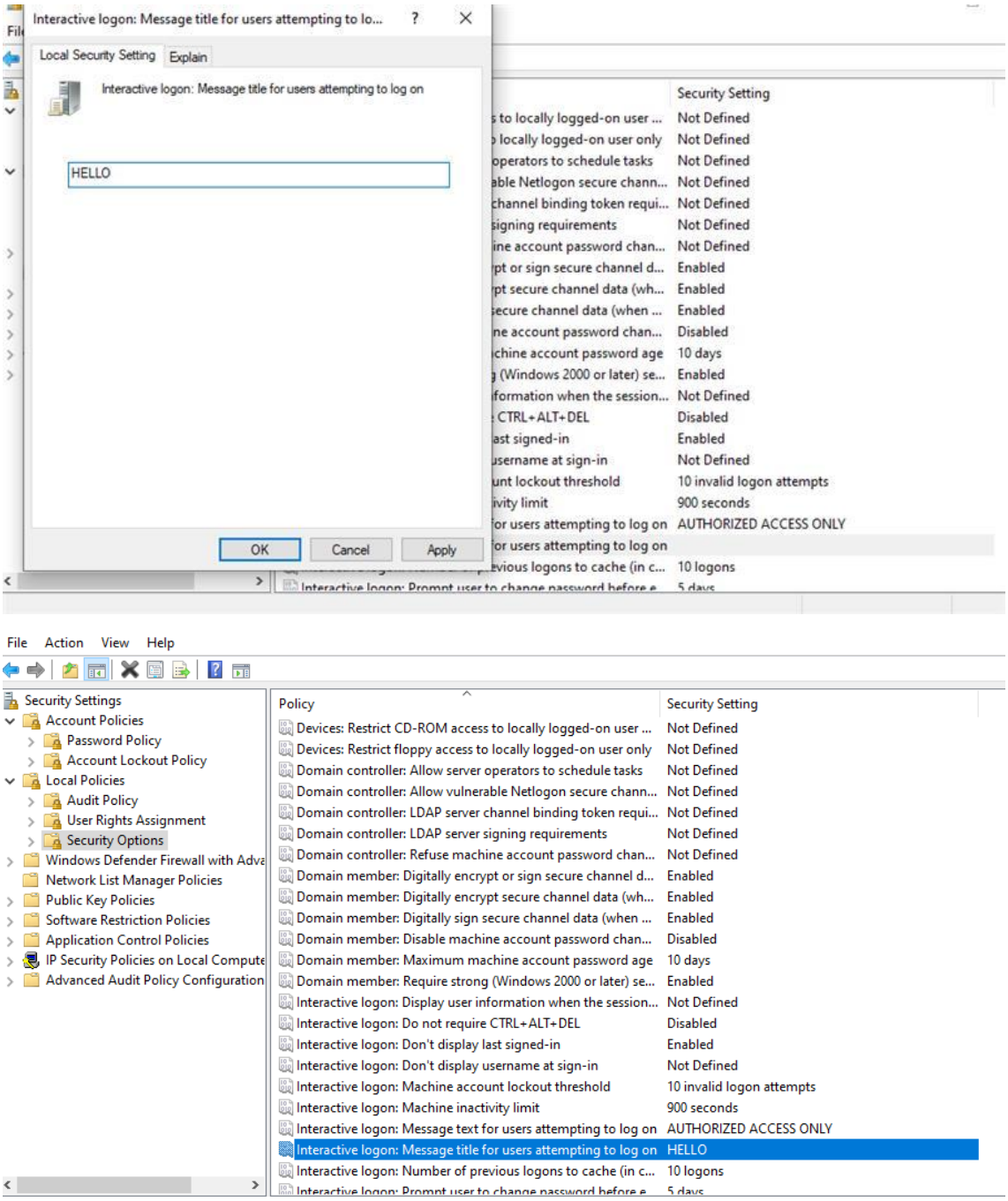
Numa tentativa de prevenir ataques, é possível mostrar um “banner” no início da sessão de modo a advertir a pessoa que está a tentar aceder das consequências de utilização imprópria.



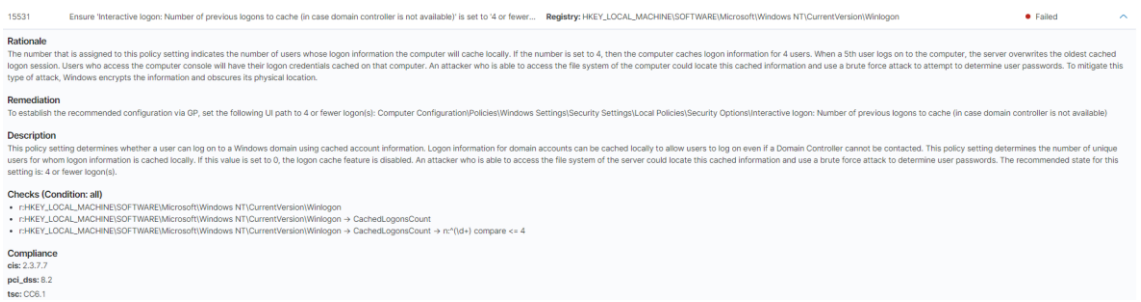


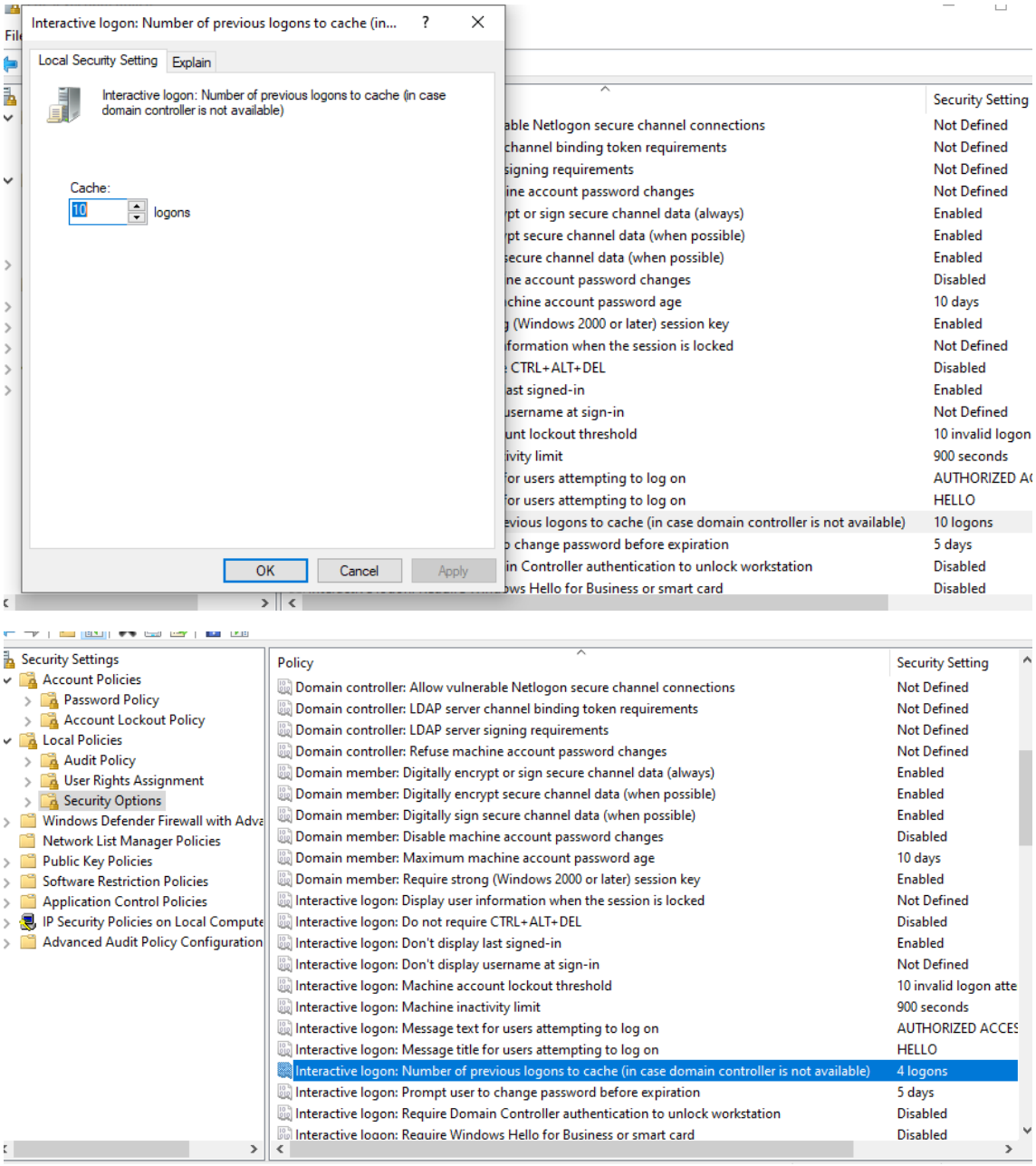
Esta mensagem semelhante à anterior serve para mostrar um título no login para evitar ou prevenir utilizadores de cometerem erros ou de usarem erroneamente máquinas da empresa.



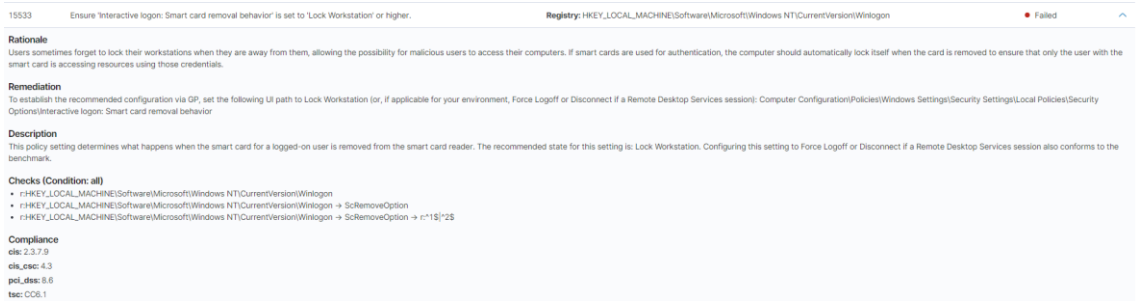


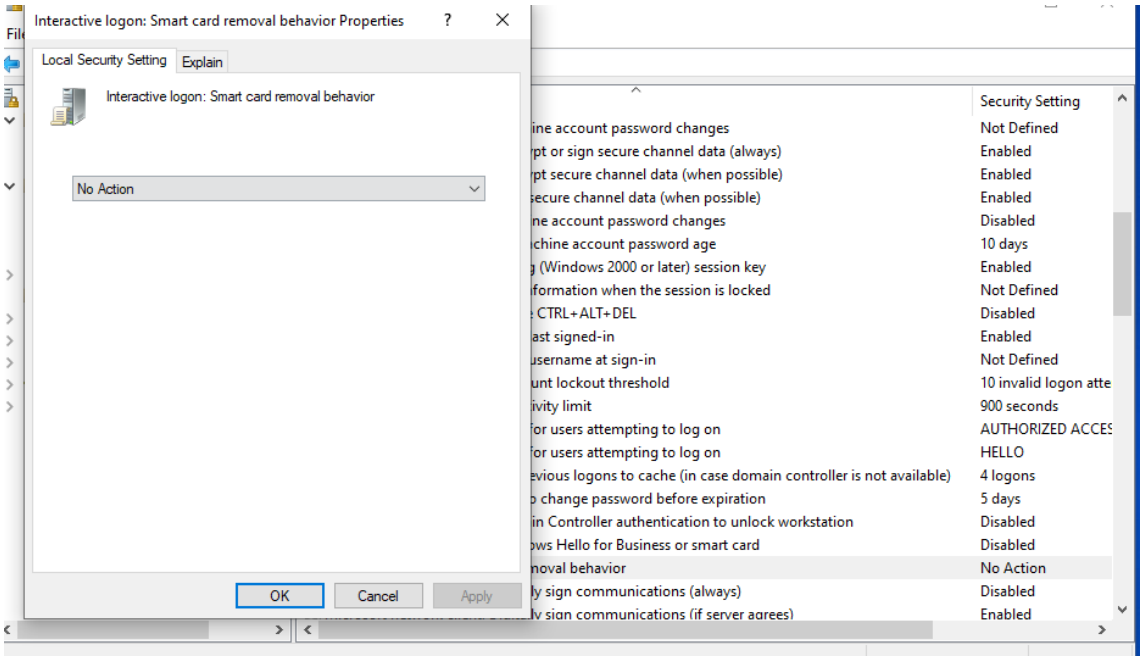
Esta política estabelece a quantidade de utilizadores que o sistema manterá em cache no evento de uma falha do controlador de domínio. Neste cenário específico, o valor foi ajustado para quatro utilizadores.

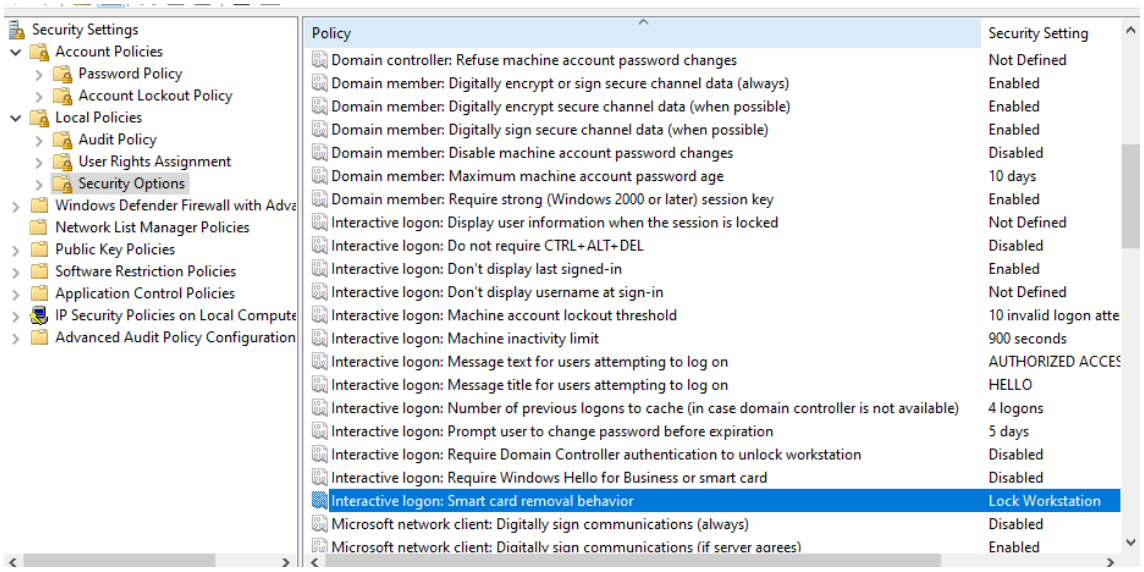




Esta política define o uso de um smart card para ser possível fazer logon. Ao retirar o smart card, automaticamente termina a sessão.

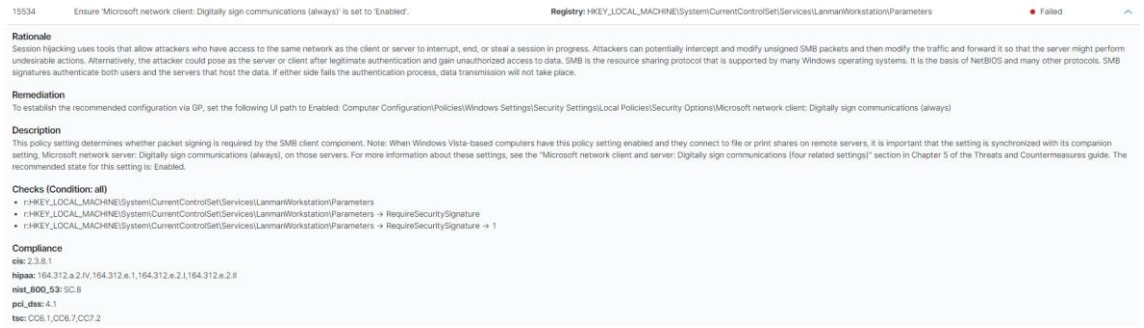


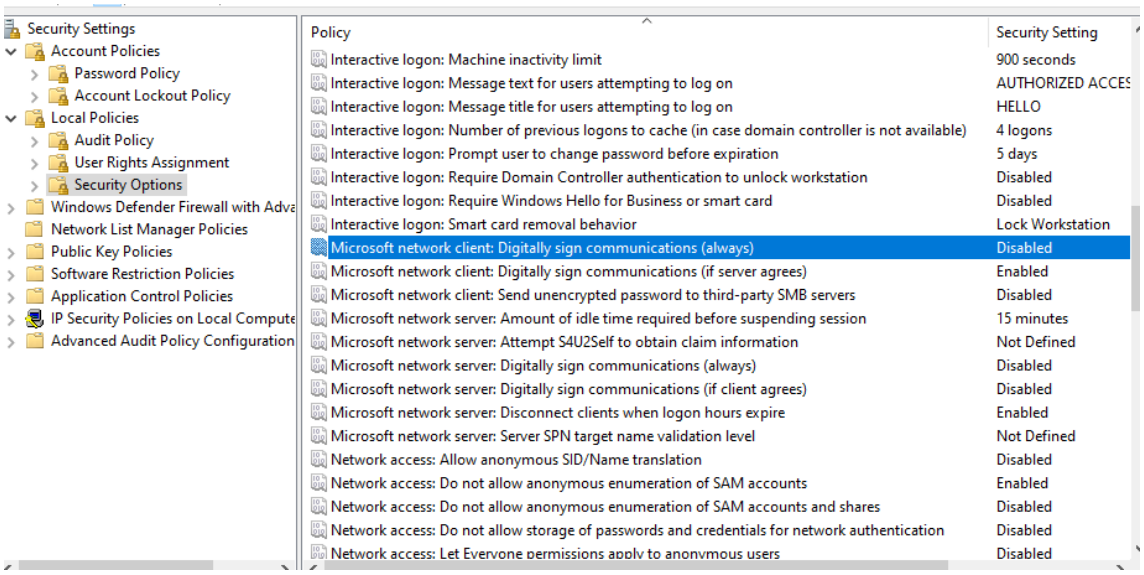


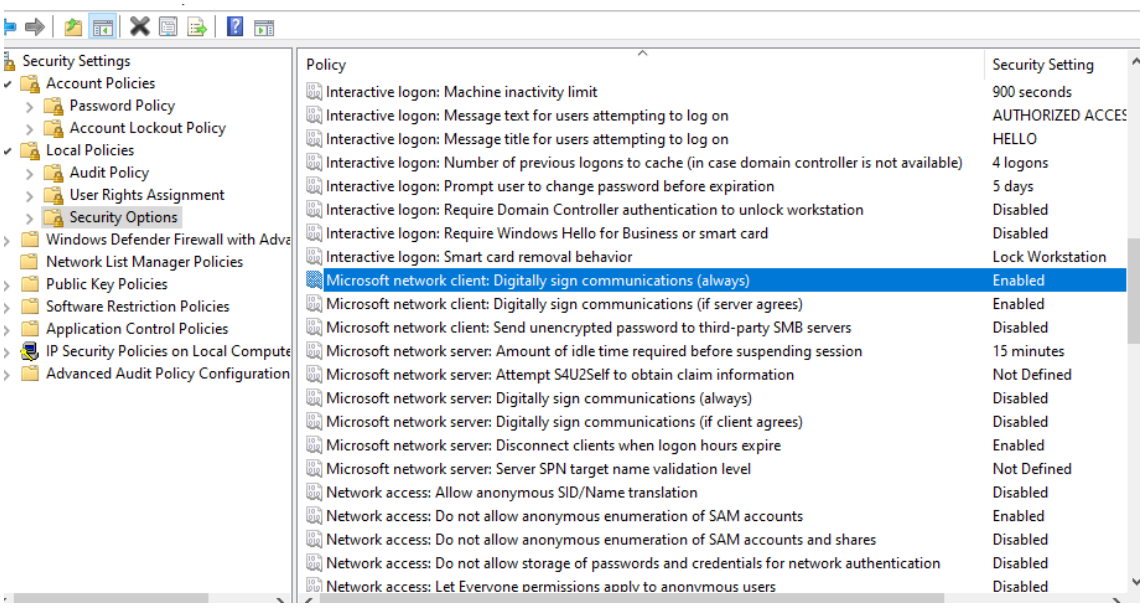


Esta política tem como objetivo garantir que o protocolo SMB (Server Message Block) usado pelo cliente se mantenha em sincronia com as configurações e requisitos de segurança definidos no servidor. Essa sincronização é fundamental para prevenir acessos não autorizados ao servidor da empresa por indivíduos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

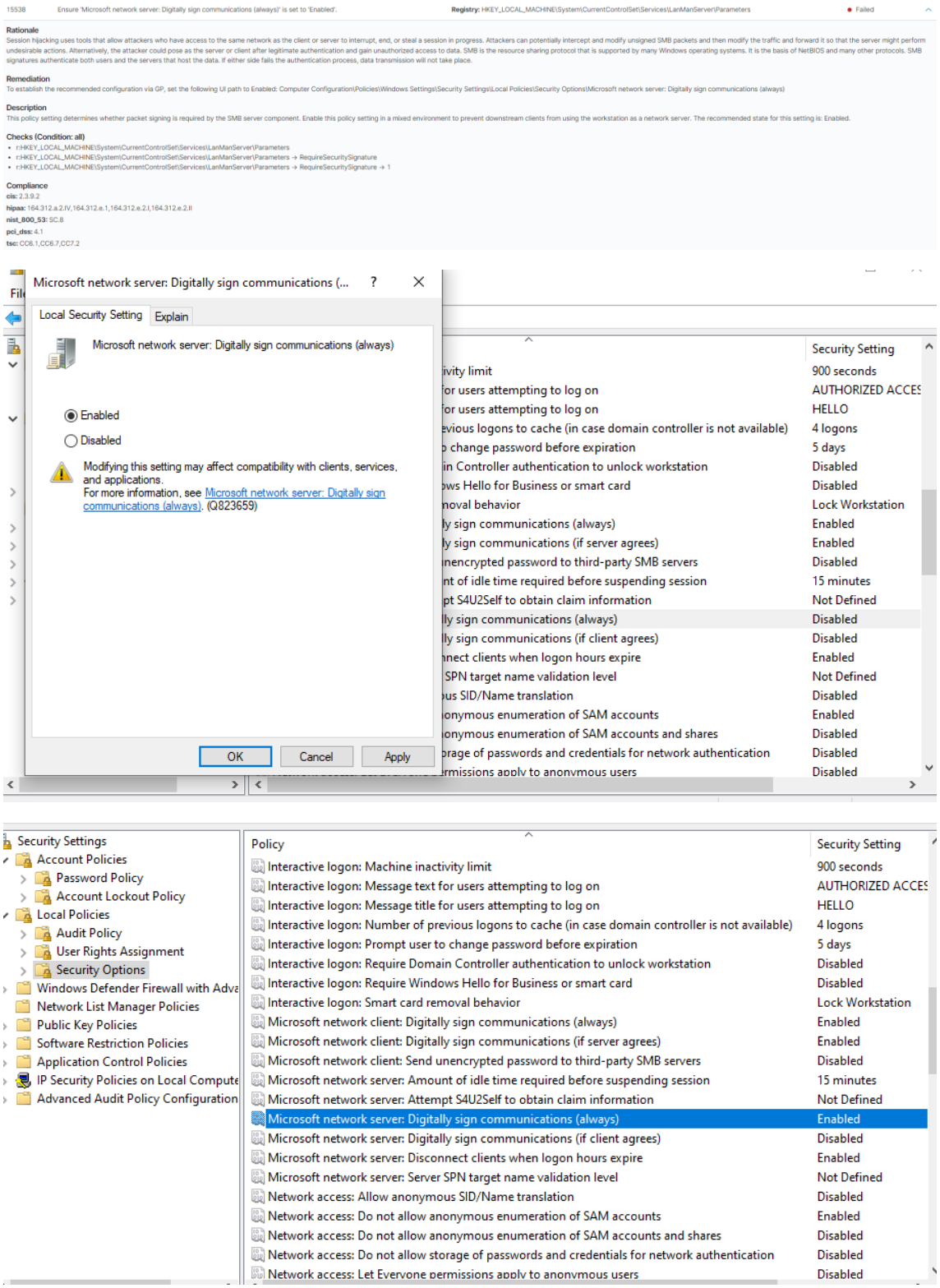






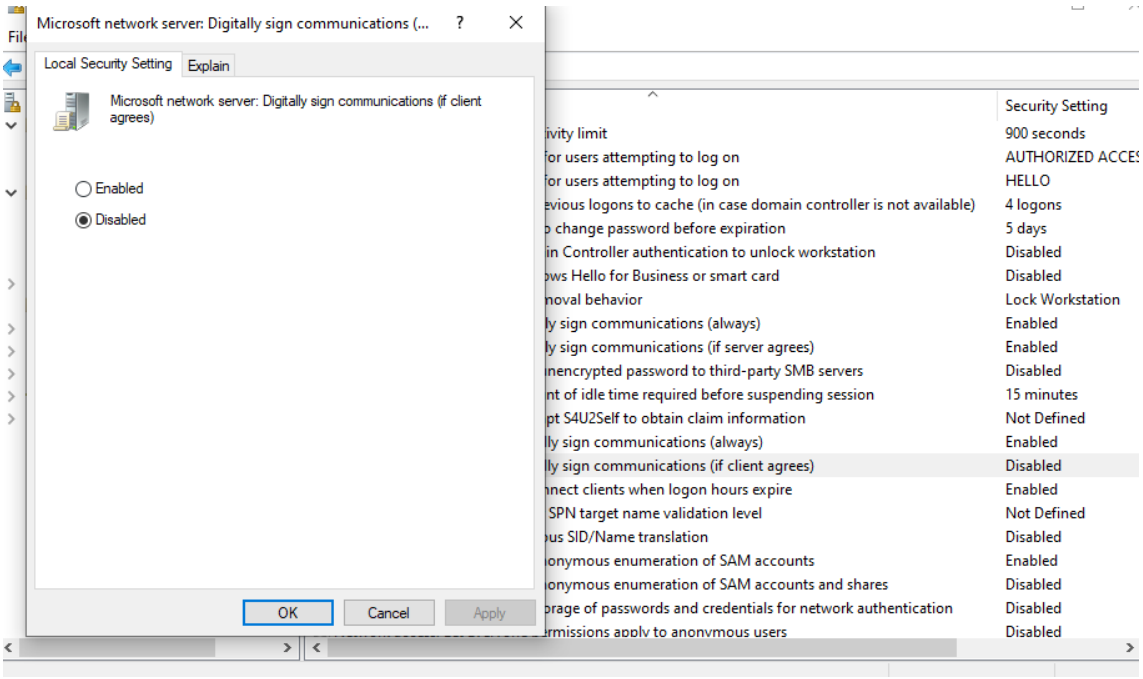
Esta política, semelhante à anterior, tem como objetivo definir e controlar os pacotes que são utilizados no servidor SMB (Server Message Block) com o propósito de evitar que potenciais atacantes explorem a mesma rede. Em outras palavras, ela estabelece as regras e configurações relacionadas aos pacotes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

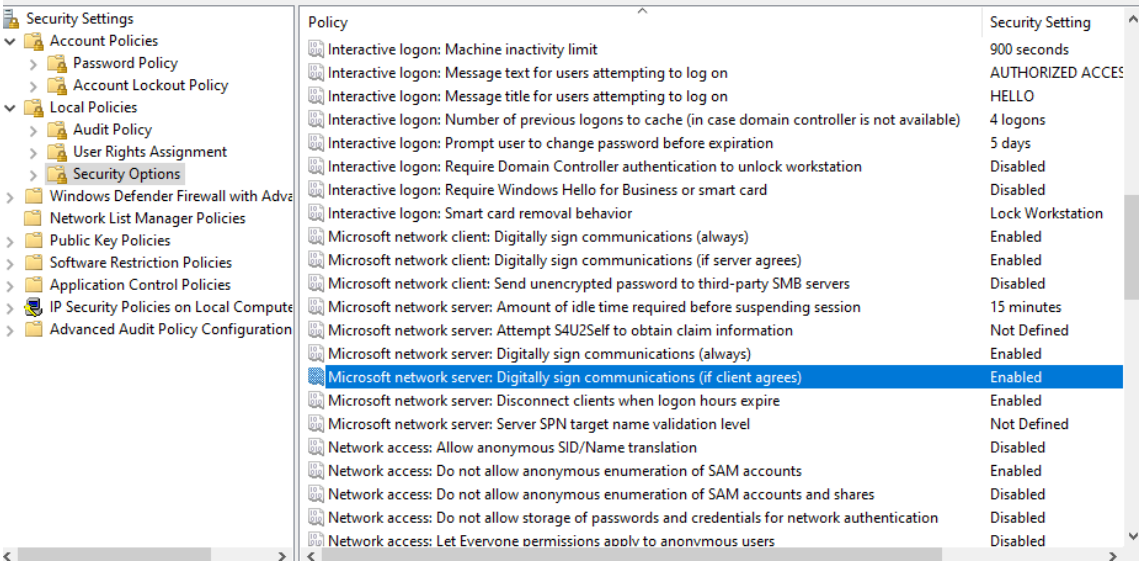
para evitar que invasores usem a rede SMB como um vetor de ataque para tentativas de acesso não autorizado ou exploração de vulnerabilidades.



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.

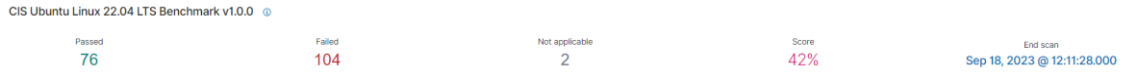




Conseguimos com sucesso resolver um total de 18 falhas de segurança do cliente Windows, de acordo com a plataforma Wazuh.

Correção dos erros de logs do cliente Ubuntu

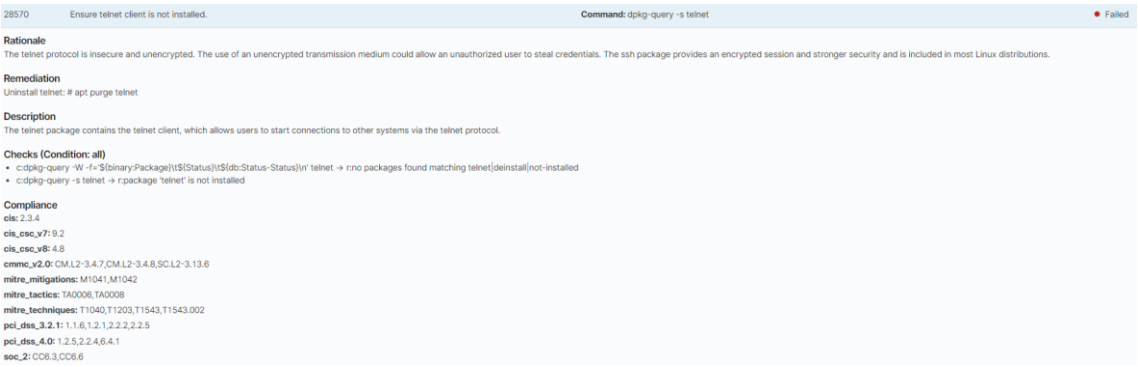
Esta seção do relatório dedica-se à documentação das correções realizadas para abordar várias vulnerabilidades de segurança numa máquina virtual cliente com Ubuntu. O objetivo principal foi identificar e solucionar essas vulnerabilidades, resultando em um ambiente mais seguro.



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 intercetação, 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.



```
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)

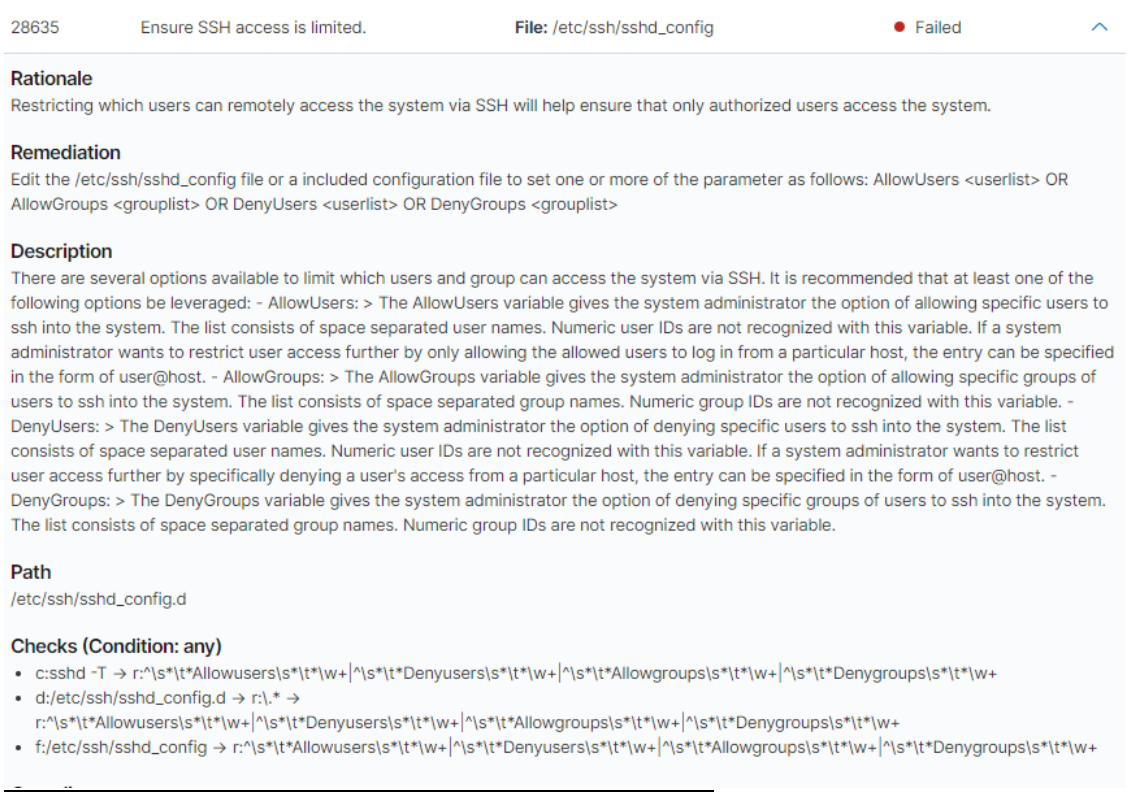
- c:stat /etc/ssh/sshd_config → r:Access:\s*\t*\(0600/-rw-------\)\s*\t*Uid:\s*\t*\(\s*\t*0/\s*root\)\s*Gid:\s*\t*\(\s*\t*0/\s*\t*root\)

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
```

Restringi 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:~# _
```

Impedi 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)

- 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

```
# 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:~#
```

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

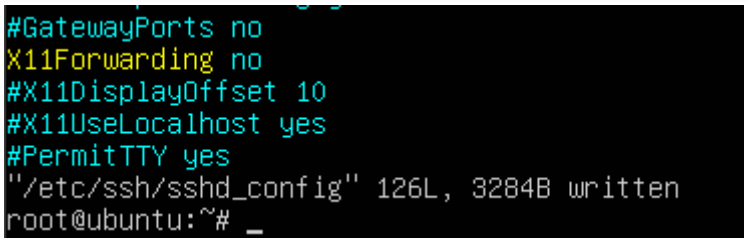
The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

Checks (Condition: all)

- 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



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_csc_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)

- c:sshd -T → r:^banner && r:/etc/issue.net$

Compliance

cis: 5.2.17

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: M1035

mitre_tactics: TA0001,TA0007

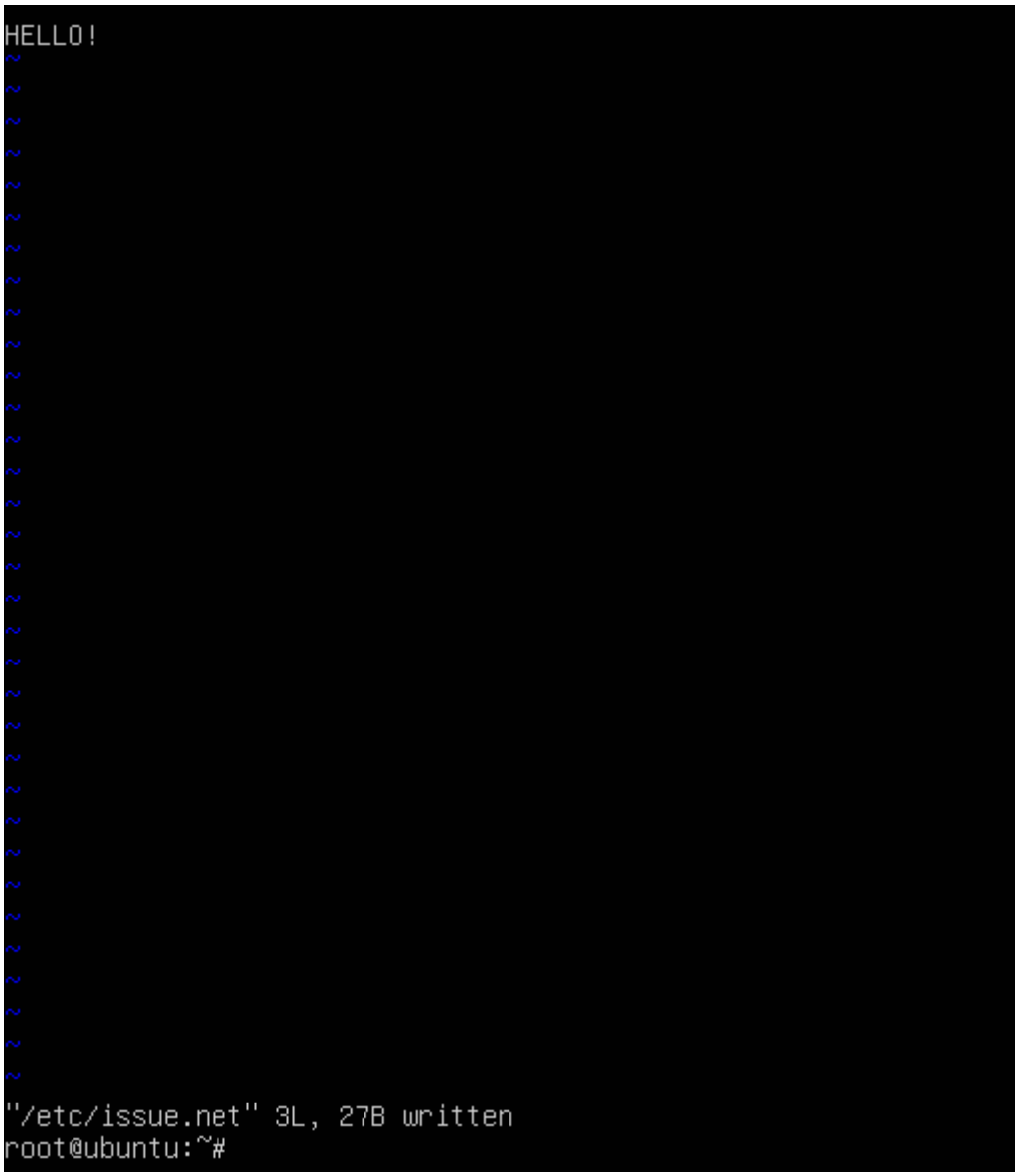
nist_sp_800-53: CM-7(1),CM-9,SA-10

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_
```



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)

- 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
cmmc_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)

- 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+):\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+ 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

```
#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:~# _
```

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)

- c:sshd -T -> n:^\s*logingracetime\s*(\d+) compare <= 60 && n:^logingracetime\s*(\d+) compare >= 1
- not f:/etc/ssh/sshd_config -> n:^\s*\t*LoginGraceTime\s*\t*(\d+) compare == 0
- not f:/etc/ssh/sshd_config -> n:^\s*\t*LoginGraceTime\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

```
# Authentication:

LoginGraceTime 60
PermitRootLogin no
#StrictModes yes
MaxAuthTries 4
#MaxSessions 10

#PubkeyAuthentication yes
"/etc/ssh/sshd_config" 126L, 3287B written
root@ubuntu:~#
```

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 indefinately, 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 where 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\s*\t*(\d+) compare > 0
- c:sshd -T -> -> n:^clientaliveinterval\s*\t*(\d+) compare > 0

Compliance

cis: 5.2.22

mitre_mitigations: M1026

mitre_tactics: TA0001

mitre_techniques: T1078,T1078.001,T1078.002,T1078.003

```
#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.


```
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 → !r:^\w+:\p: && n:^\w+:\S*:\d*:\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 confi...	**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

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.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:\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: 5.1.3

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)

- 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

```
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/
```

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)

- 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

```
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 libftdi1-2
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]
```

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 audispd 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 audispd-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)

- c:dpkg-query -s audispd-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

```
root@ubuntu:~# apt install audit audispd-plugins
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package audit
```

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)

- 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

```
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 libftdi1-2 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) ...
```

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)

- 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)

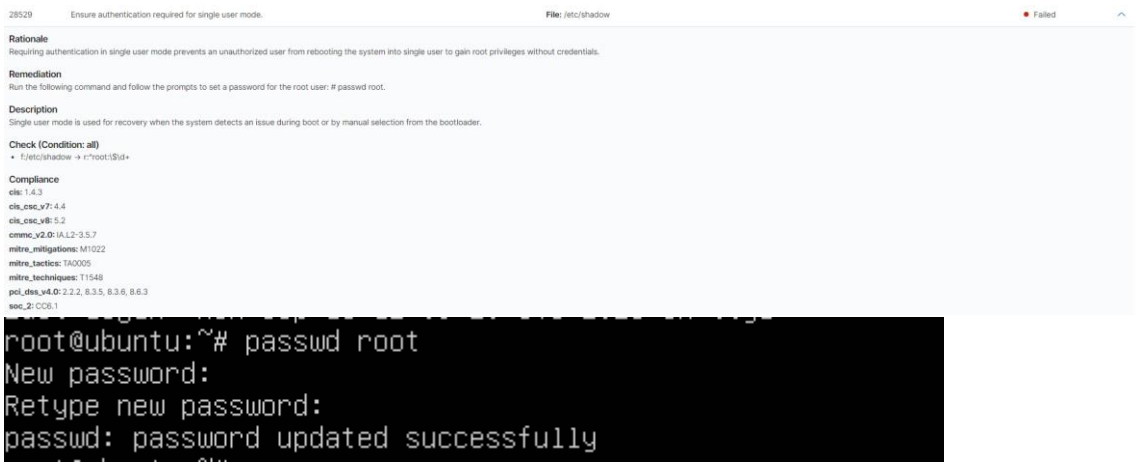
pci_dss_3.2.1: 1.4,1.1.4

pci_dss_4.0: 1.2.1

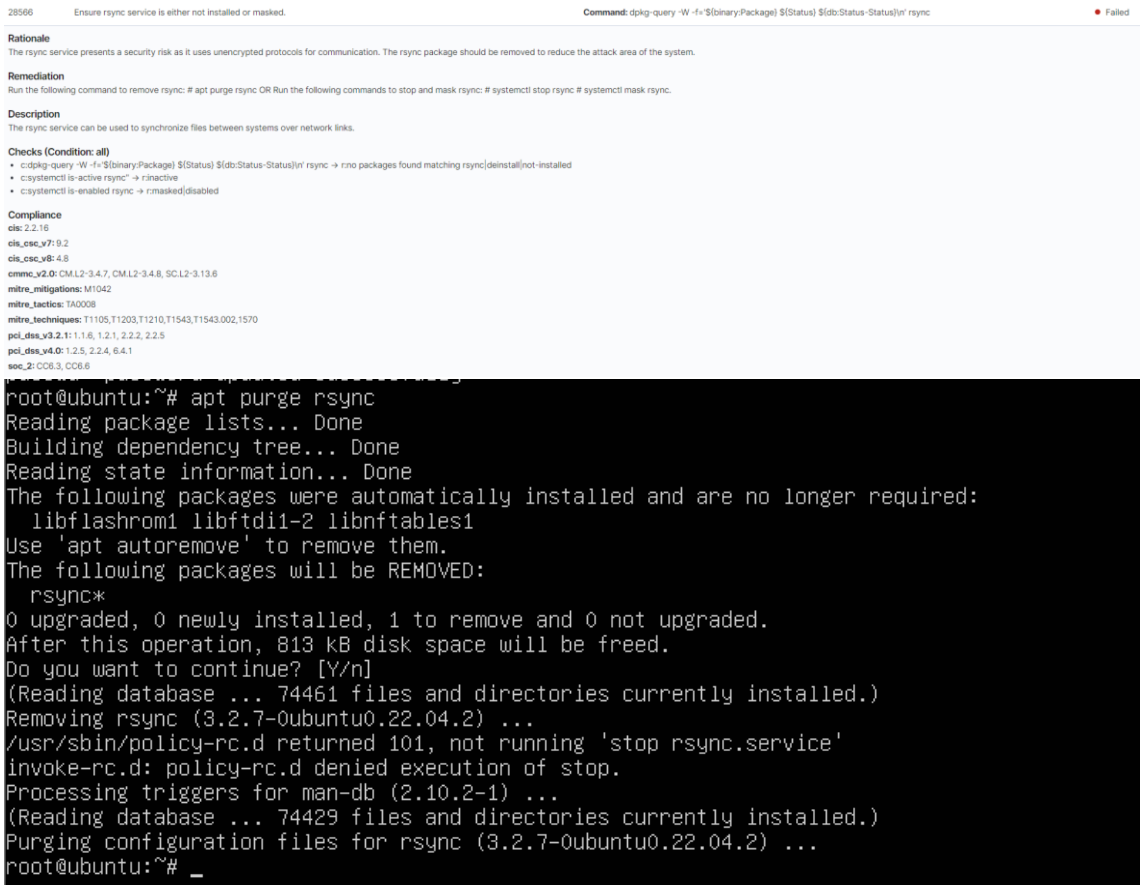
soc_2: CC6.6

```
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/syst
emd/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:~#
```

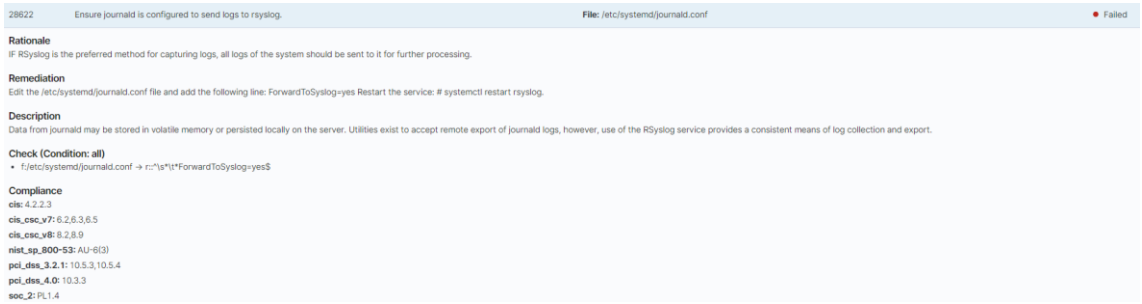
Alterei a senha do utilizador root. Como se trata de uma conta com privilégios elevados, é boa prática exigir uma senha complexa. O acesso a esta conta deve ser devidamente controlado e a senha deve ser alterada com frequência.



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.



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.




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

```
#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.