jamk.fi

LAB 4 Configurations

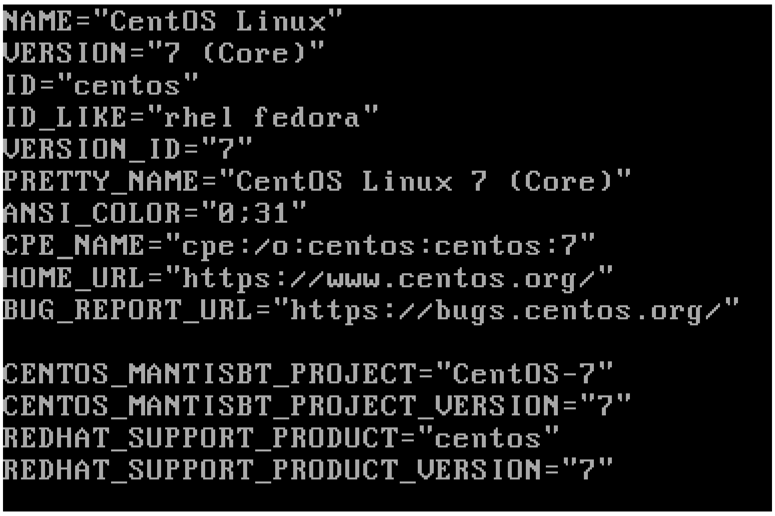
Data security testing

Jere Pesonen TTV18S1
m3227@student.jamk.fi

LAB-04-Configurations
Marraskuu-20
Tieto- ja viestintätekniikka
Tekniikan ja Liikenteen ala

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

1 CentOS

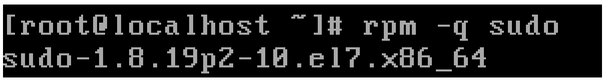


```
NAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="7"
PRETTY_NAME="CentOS Linux 7 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"

CENTOS_MANTISBT_PROJECT="CentOS-7"
CENTOS_MANTISBT_PROJECT_VERSION="7"
REDHAT_SUPPORT_PRODUCT="centos"
REDHAT_SUPPORT_PRODUCT_VERSION="7"
```

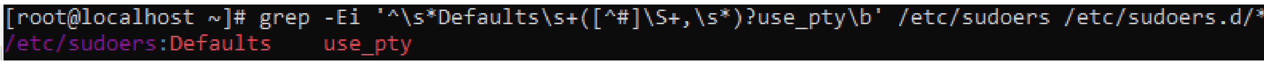
1.3 Configure sudo

verify that sudo is installed.



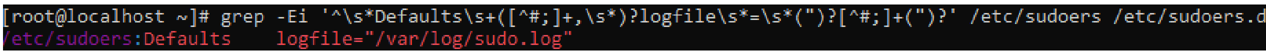
```
[root@localhost ~]# rpm -q sudo
sudo-1.8.19p2-10.el7.x86_64
```

Verify that sudo can only run other commands from a pseudo-pty



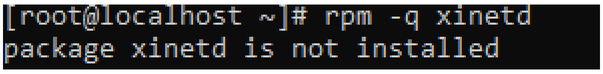
```
[root@localhost ~]# grep -Ei '^\s*Defaults\s+([^#]\S+,\s*)?use_pty\b' /etc/sudoers /etc/sudoers.d/*
/etc/sudoers:Defaults    use_pty
```

Ensure that sudo log file exists.



```
[root@localhost ~]# grep -Ei '^\s*Defaults\s+([^#;]+,\s*)?logfile\s*=\s*(")?[^#;]+(")?' /etc/sudoers /etc/sudoers.d
/etc/sudoers:Defaults    logfile="/var/log/sudo.log"
```

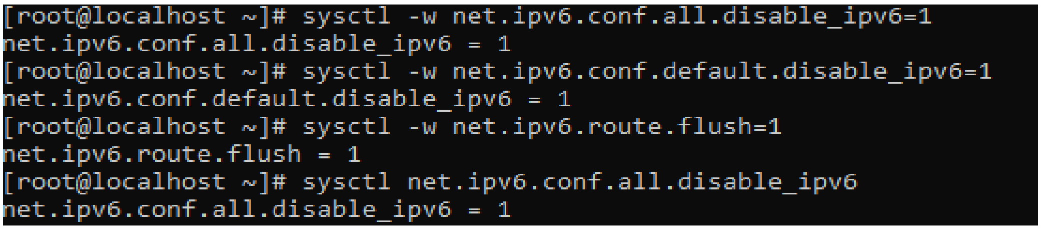
2.1 Ensure xinetd is not installed.



```
[root@localhost ~]# rpm -q xinetd
package xinetd is not installed
```

3.1 Disable unused network protocols and devices.

Disable IPv6



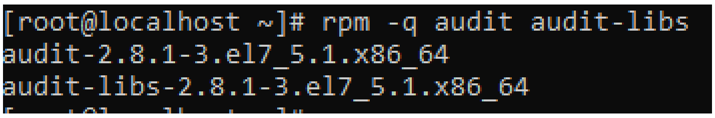
```
[root@localhost ~]# sysctl -w net.ipv6.conf.all.disable_ipv6=1
net.ipv6.conf.all.disable_ipv6 = 1
[root@localhost ~]# sysctl -w net.ipv6.conf.default.disable_ipv6=1
net.ipv6.conf.default.disable_ipv6 = 1
[root@localhost ~]# sysctl -w net.ipv6.route.flush=1
net.ipv6.route.flush = 1
[root@localhost ~]# sysctl net.ipv6.conf.all.disable_ipv6
net.ipv6.conf.all.disable_ipv6 = 1
```

Ensure wireless interfaces are disabled.

Im not going to disable any interfaces from the vm, put you can do it with command "ip link set <interface > down"

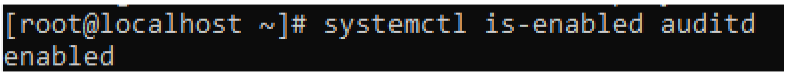
4.1 Configure system accounting.

Ensure auditing is installed.

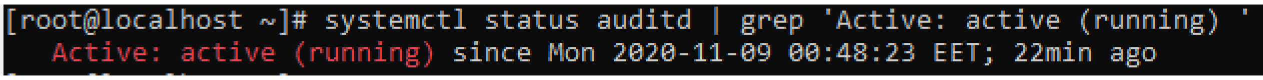


```
[root@localhost ~]# rpm -q audit audit-libs
audit-2.8.1-3.el7_5.1.x86_64
audit-libs-2.8.1-3.el7_5.1.x86_64
```

Ensure auditd service is enabled and running.

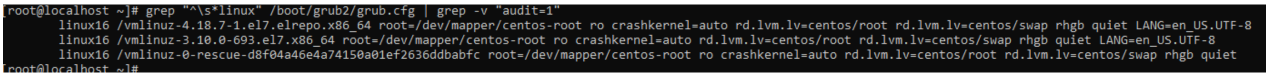


```
[root@localhost ~]# systemctl is-enabled auditd
enabled
```



```
[root@localhost ~]# systemctl status auditd | grep 'Active: active (running) '
   Active: active (running) since Mon 2020-11-09 00:48:23 EET; 22min ago
```

Ensure auditing for processes that start prior to auditd is enabled.

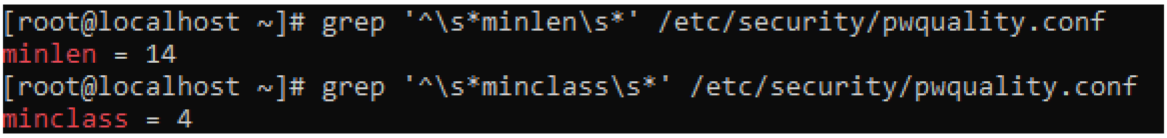


```
[root@localhost ~]# grep "^\s*linux" /boot/grub2/grub.cfg | grep -v "audit=1"
        linux16 /vmlinuz-4.18.7-1.el7.elrepo.x86_64 root=/dev/mapper/centos-root ro crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet LANG=en_US.UTF-8
        linux16 /vmlinuz-3.10.0-693.el7.x86_64 root=/dev/mapper/centos-root ro crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet LANG=en_US.UTF-8
        linux16 /vmlinuz-0-rescue-d8f04a46e4a74150a01ef2636ddbabfc root=/dev/mapper/centos-root ro crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet
[root@localhost ~]#
```

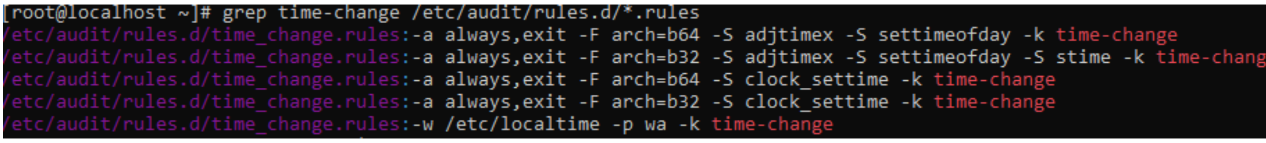
- I didn't get this to work. the command should not return anything. The noted fix didn't help.

5.3 Configure Pluggable Authentication Modules

Ensure password creation requirements are configured.

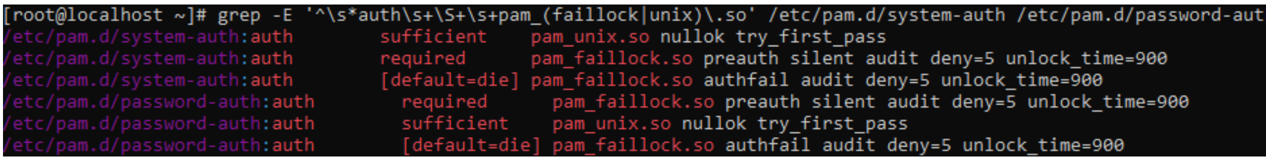


```
[root@localhost ~]# grep '^\s*minlen\s*' /etc/security/pwquality.conf
minlen = 14
[root@localhost ~]# grep '^\s*minclass\s*' /etc/security/pwquality.conf
minclass = 4
```



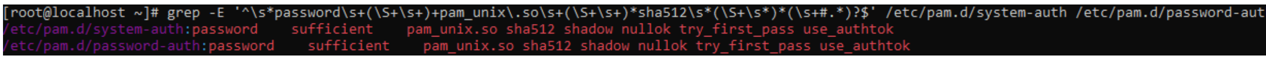
```
[root@localhost ~]# grep time-change /etc/audit/rules.d/*.rules
/etc/audit/rules.d/time_change.rules:-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
/etc/audit/rules.d/time_change.rules:-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-chang
/etc/audit/rules.d/time_change.rules:-a always,exit -F arch=b64 -S clock_settime -k time-change
/etc/audit/rules.d/time_change.rules:-a always,exit -F arch=b32 -S clock_settime -k time-change
/etc/audit/rules.d/time_change.rules:-w /etc/localtime -p wa -k time-change
```

Ensure lockout for failed password attempts is configured.



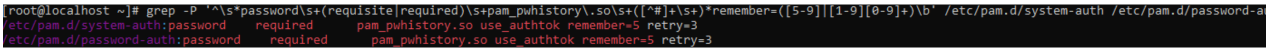
```
[root@localhost ~]# grep -E '^\s*auth\s+\S+\s+pam_(faillock|unix)\.so' /etc/pam.d/system-auth /etc/pam.d/password-aut
/etc/pam.d/system-auth:auth        sufficient    pam_unix.so nullok try_first_pass
/etc/pam.d/system-auth:auth        required      pam_faillock.so preauth silent audit deny=5 unlock_time=900
/etc/pam.d/system-auth:auth        [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
/etc/pam.d/password-auth:auth        required      pam_faillock.so preauth silent audit deny=5 unlock_time=900
/etc/pam.d/password-auth:auth        sufficient    pam_unix.so nullok try_first_pass
/etc/pam.d/password-auth:auth        [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
```

Ensure password hashing algorithm is SHA-512.



```
[root@localhost ~]# grep -E '^\s*password\s+(\S+\s+)+pam_unix\.so\s+(\S+\s+)*sha512\s*(\S+\s*)*(\s+#.*)?$' /etc/pam.d/system-auth /etc/pam.d/password-aut
/etc/pam.d/system-auth:password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
/etc/pam.d/password-auth:password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
```

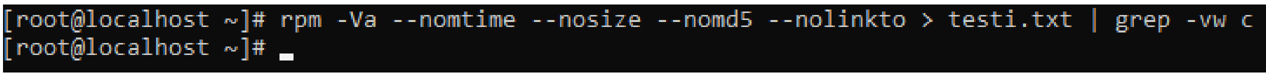
Ensure password reuse is limited.



```
[root@localhost ~]# grep -P '^\s*password\s+(requisite|required)\s+pam_pwhistory\.so\s+([^#]+\s+)*remember=([5-9]|[1-9][0-9]+)\b' /etc/pam.d/system-auth /etc/pam.d/password-a
/etc/pam.d/system-auth:password    required      pam_pwhistory.so use_authtok remember=5 retry=3
/etc/pam.d/password-auth:password    required      pam_pwhistory.so use_authtok remember=5 retry=3
```

6.1 System File Permissions

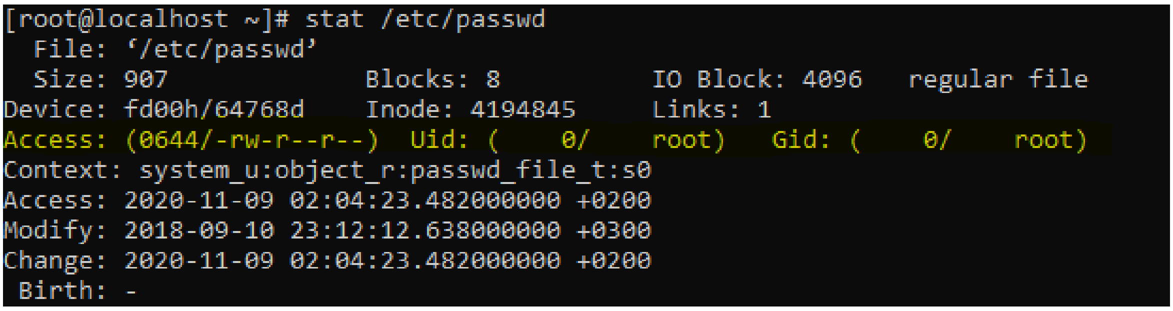
Audit system file permissions



```
[root@localhost ~]# rpm -Va --nomtime --nosize --nomd5 --nolinkto > testi.txt | grep -vw c
[root@localhost ~]# _
```

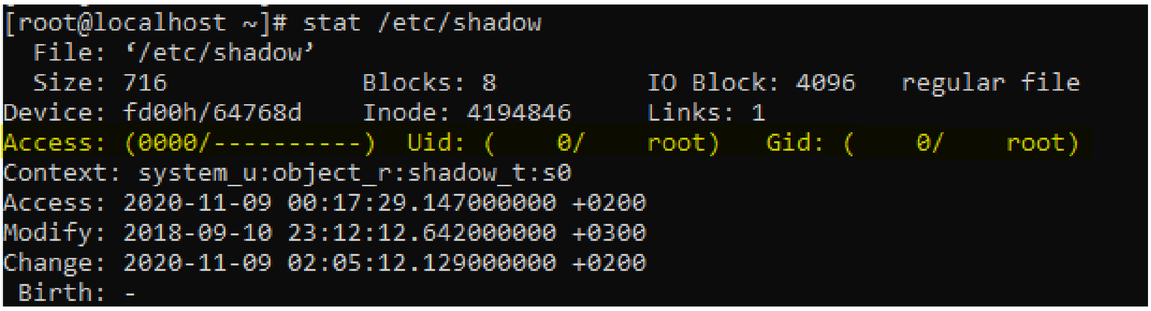
- with this command you can review all installed packages and their permissions

Ensure permissions on /etc/passwd are configured.



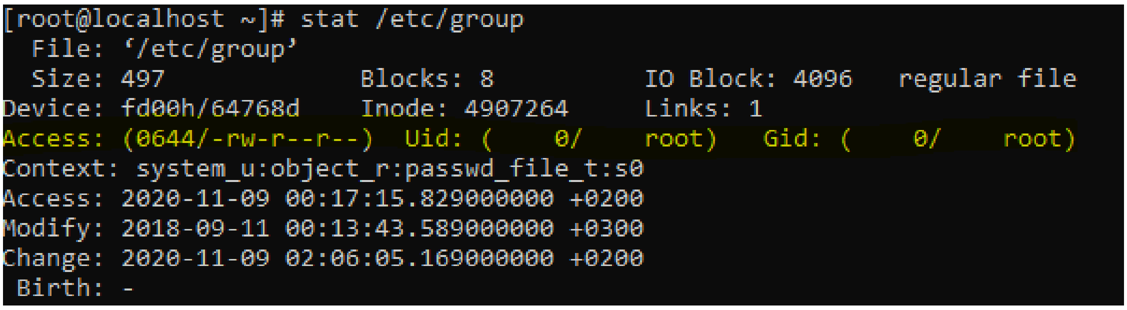
```
[root@localhost ~]# stat /etc/passwd
  File: ‘/etc/passwd’
  Size: 907             Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 4194845     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Context: system_u:object_r:passwd_file_t:s0
Access: 2020-11-09 02:04:23.482000000 +0200
Modify: 2018-09-10 23:12:12.638000000 +0300
Change: 2020-11-09 02:04:23.482000000 +0200
 Birth: -
```

Ensure permissions on /etc/shadow are configured.



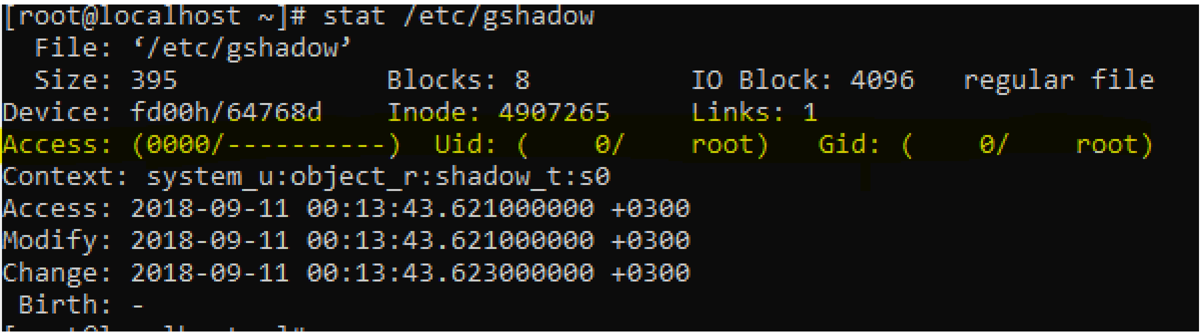
```
[root@localhost ~]# stat /etc/shadow
  File: ‘/etc/shadow’
  Size: 716             Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 4194846     Links: 1
Access: (0000/----------)  Uid: (    0/    root)   Gid: (    0/    root)
Context: system_u:object_r:shadow_t:s0
Access: 2020-11-09 00:17:29.147000000 +0200
Modify: 2018-09-10 23:12:12.642000000 +0300
Change: 2020-11-09 02:05:12.129000000 +0200
 Birth: -
```

Ensure permissions on /etc/group are configured.



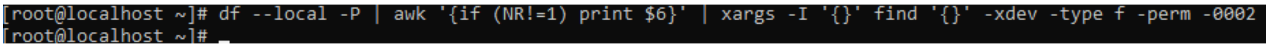
```
[root@localhost ~]# stat /etc/group
  File: ‘/etc/group’
  Size: 497             Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 4907264     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Context: system_u:object_r:passwd_file_t:s0
Access: 2020-11-09 00:17:15.829000000 +0200
Modify: 2018-09-11 00:13:43.589000000 +0300
Change: 2020-11-09 02:06:05.169000000 +0200
 Birth: -
```

Ensure permissions on /etc/gshadow are configured.



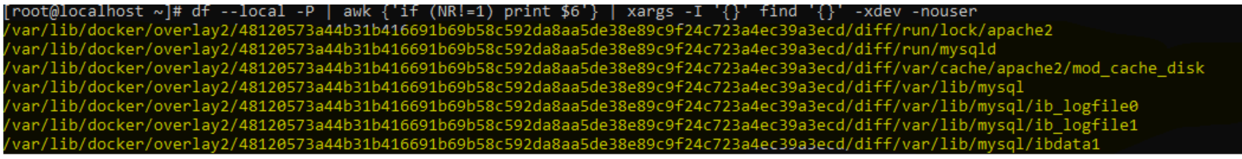
```
[root@localhost ~]# stat /etc/gshadow
  File: ‘/etc/gshadow’
  Size: 395             Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 4907265     Links: 1
Access: (0000/----------)  Uid: (    0/    root)   Gid: (    0/    root)
Context: system_u:object_r:shadow_t:s0
Access: 2018-09-11 00:13:43.621000000 +0300
Modify: 2018-09-11 00:13:43.621000000 +0300
Change: 2018-09-11 00:13:43.623000000 +0300
 Birth: -
```

Ensure no world writable files exist.



```
[root@localhost ~]# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -0002
[root@localhost ~]# _
```

Ensure no unowned or ungrouped files or directories exist.



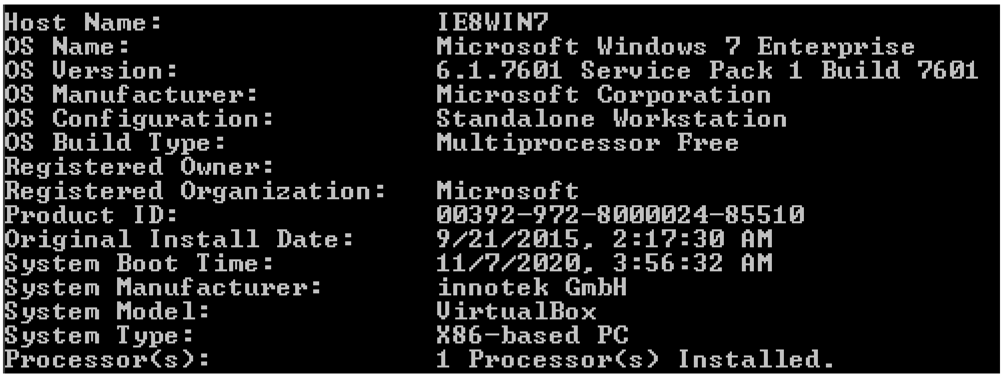
```
[root@localhost ~]# df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -nouser
/var/lib/docker/overlay2/48120573a44b31b416691b69b58c592da8aa5de38e89c9f24c723a4ec39a3ecd/diff/run/lock/apache2
/var/lib/docker/overlay2/48120573a44b31b416691b69b58c592da8aa5de38e89c9f24c723a4ec39a3ecd/diff/run/mysqld
/var/lib/docker/overlay2/48120573a44b31b416691b69b58c592da8aa5de38e89c9f24c723a4ec39a3ecd/diff/var/cache/apache2/mod_cache_disk
/var/lib/docker/overlay2/48120573a44b31b416691b69b58c592da8aa5de38e89c9f24c723a4ec39a3ecd/diff/var/lib/mysql
/var/lib/docker/overlay2/48120573a44b31b416691b69b58c592da8aa5de38e89c9f24c723a4ec39a3ecd/diff/var/lib/mysql/ib_logfile0
/var/lib/docker/overlay2/48120573a44b31b416691b69b58c592da8aa5de38e89c9f24c723a4ec39a3ecd/diff/var/lib/mysql/ib_logfile1
/var/lib/docker/overlay2/48120573a44b31b416691b69b58c592da8aa5de38e89c9f24c723a4ec39a3ecd/diff/var/lib/mysql/ibdata1
```

- this command printed loads of files, not sure what to do in this situation. Same thing when listing ungrouped files or directories

Audit SUID executables

Didnt get the remediation to this.

Windows



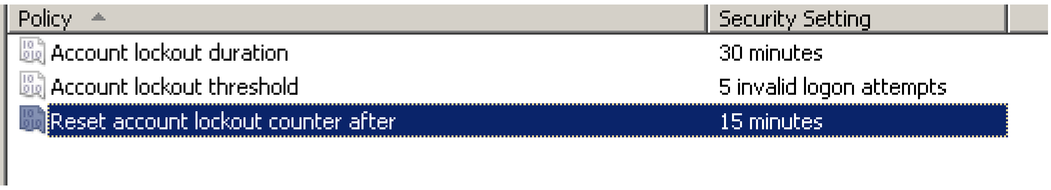
```
Host Name:                 IE8WIN7
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:
Registered Organization:   Microsoft
Product ID:                00392-972-8000024-85510
Original Install Date:     9/21/2015, 2:17:30 AM
System Boot Time:          11/7/2020, 3:56:32 AM
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
```

1.2 Account Lockout Policy

Ensure 'Account lockout duration' is set to '15 or more minute(s)'.

Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'.

Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'.



Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

2.3.1 Accounts

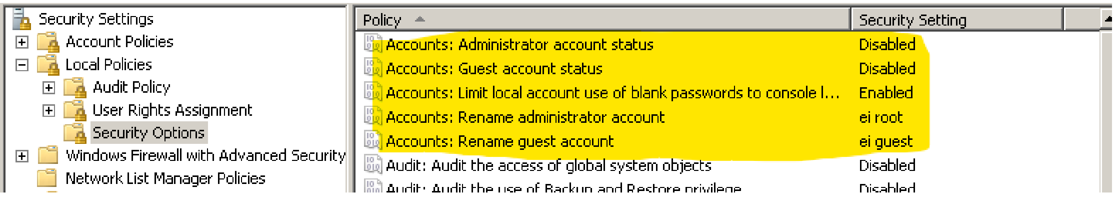
Ensure 'Accounts: Administrator account status' is set to 'Disabled'.

Ensure 'Accounts: Guest account status' is set to 'Disabled'.

Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'.

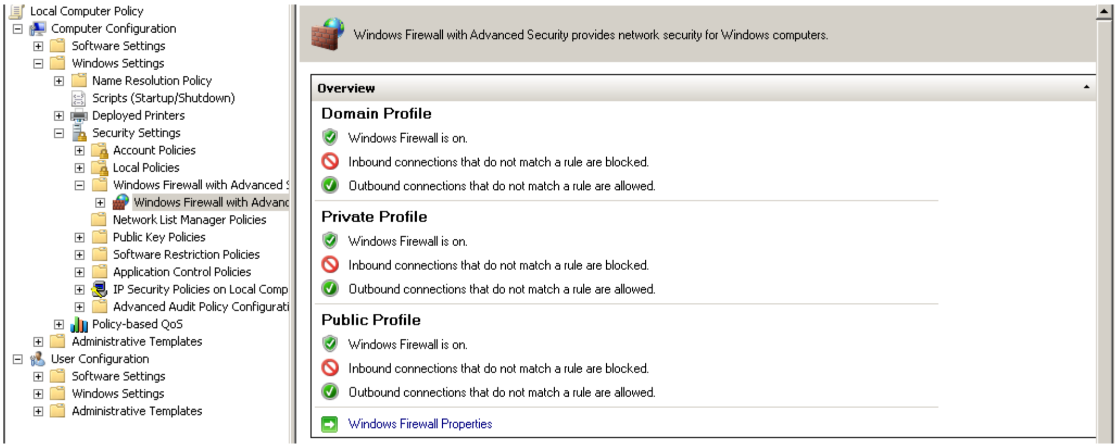
Configure 'Accounts: Rename administrator account'.

Configure 'Accounts: Rename guest account'.



Policy	Security Setting
Accounts: Administrator account status	Disabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console l...	Enabled
Accounts: Rename administrator account	ei root
Accounts: Rename guest account	ei guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled

9.1 Domain profile of windows firewall



Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- ✓ Windows Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Private Profile

- ✓ Windows Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

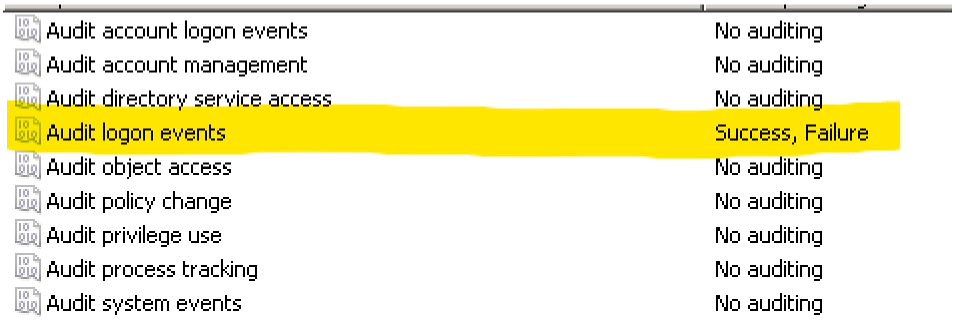
Public Profile

- ✓ Windows Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

17.1 Account Logon

Ensure 'Audit Credential Validation' is set to 'Success and Failure'.

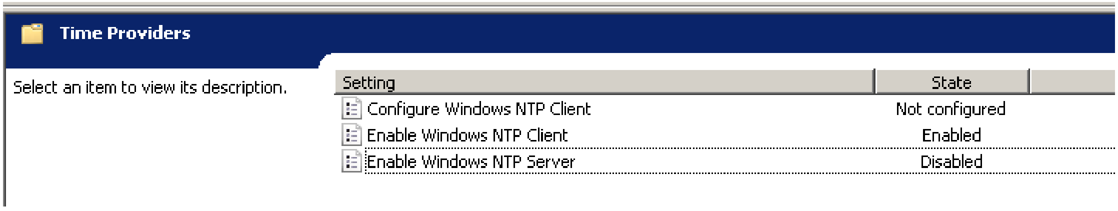


Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

18.8.52 Windows time service

Ensure 'Enable Windows NTP Client' is set to 'Enabled'.

Ensure 'Enable Windows NTP Server' is set to 'Disabled'

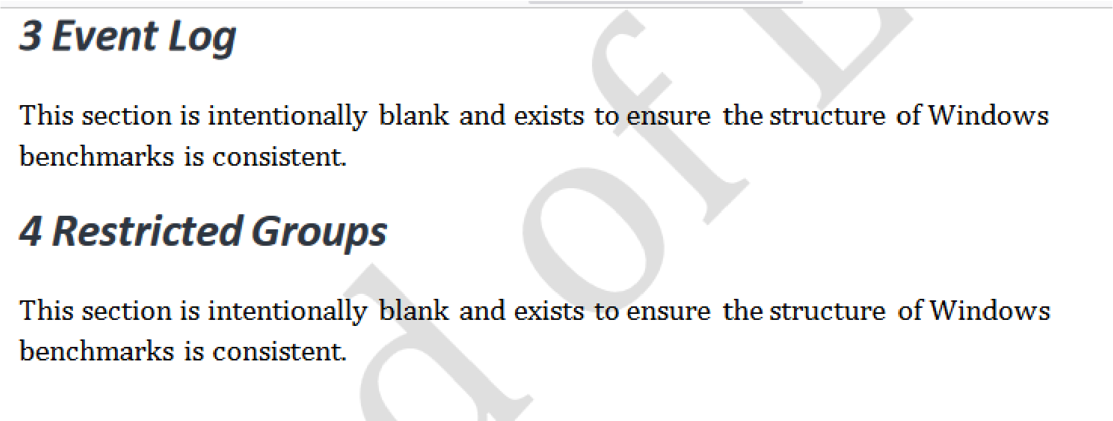


Time Providers

Select an item to view its description.

Setting	State
Configure Windows NTP Client	Not configured
Enable Windows NTP Client	Enabled
Enable Windows NTP Server	Disabled

Most of the section look like this.



3 Event Log

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

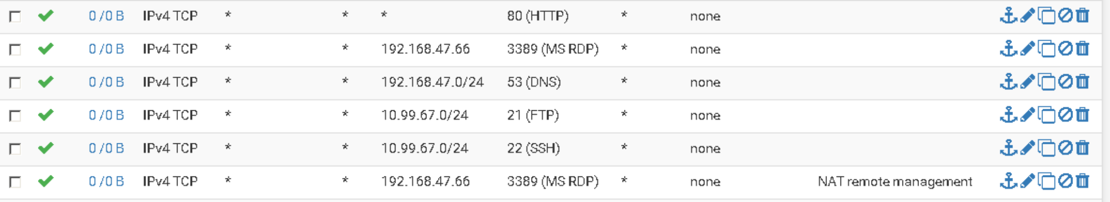
4 Restricted Groups

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

pfSense

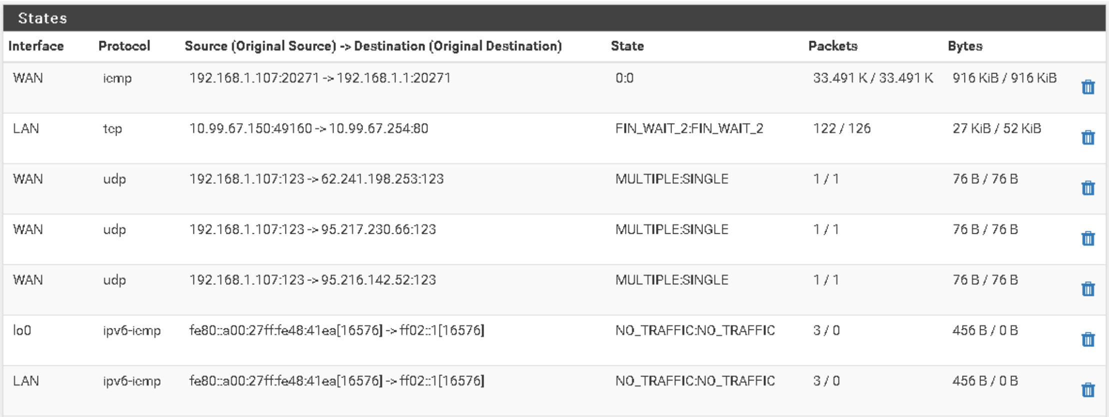
I implemented everything I cold, and got familiar with the rest

1 Review rulesets.



□	✓	0 / 0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none	
□	✓	0 / 0 B	IPv4 TCP	*	*	192.168.47.66	3389 (MS RDP)	*	none	
□	✓	0 / 0 B	IPv4 TCP	*	*	192.168.47.0/24	53 (DNS)	*	none	
□	✓	0 / 0 B	IPv4 TCP	*	*	10.99.67.0/24	21 (FTP)	*	none	
□	✓	0 / 0 B	IPv4 TCP	*	*	10.99.67.0/24	22 (SSH)	*	none	
□	✓	0 / 0 B	IPv4 TCP	*	*	192.168.47.66	3389 (MS RDP)	*	none	NAT remote management

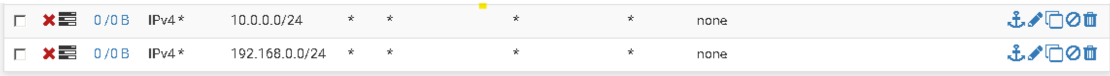
3. Review state tables



States

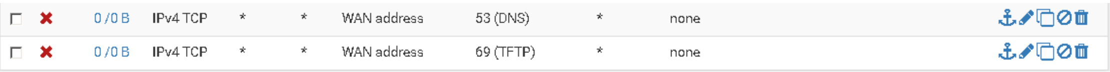
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	icmp	192.168.1.107:20271 -> 192.168.1.1:20271	0:0	33.491 K / 33.491 K	916 KiB / 916 KiB
LAN	tcp	10.99.67.150:49160 -> 10.99.67.254:80	FIN_WAIT_2:FIN_WAIT_2	122 / 126	27 KiB / 52 KiB
WAN	udp	192.168.1.107:123 -> 62.241.198.253:123	MULTIPLE:SINGLE	1 / 1	76 B / 76 B
WAN	udp	192.168.1.107:123 -> 95.217.230.66:123	MULTIPLE:SINGLE	1 / 1	76 B / 76 B
WAN	udp	192.168.1.107:123 -> 95.216.142.52:123	MULTIPLE:SINGLE	1 / 1	76 B / 76 B
lo0	ipv6-icmp	fe80::a00:27ff:fe48:41ea[16576] -> ff02::1[16576]	NO_TRAFFIC:NO_TRAFFIC	3 / 0	456 B / 0 B
LAN	ipv6-icmp	fe80::a00:27ff:fe48:41ea[16576] -> ff02::1[16576]	NO_TRAFFIC:NO_TRAFFIC	3 / 0	456 B / 0 B

9. Ensure that the following spoofed, private (RFC 1918) and illegal addresses are blocked.



□	✗	0 / 0 B	IPv4 *	10.0.0.0/24	*	*	*	*	none
□	✗	0 / 0 B	IPv4 *	192.168.0.0/24	*	*	*	*	none

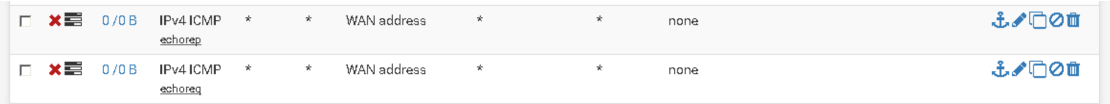
11. Port restrictions



□	✗	0 / 0 B	IPv4 TCP	*	*	WAN address	53 (DNS)	*	none
□	✗	0 / 0 B	IPv4 TCP	*	*	WAN address	69 (TFTP)	*	none

- I blocked couple one for test.

15. Ensure that there is a rule blocking ICMP echo requests and replies.



□	✗	0 / 0 B	IPv4 ICMP echorep	*	*	WAN address	*	*	none
□	✗	0 / 0 B	IPv4 ICMP echoreq	*	*	WAN address	*	*	none