Server Hardening

Wie sichern wir unseren Server (Host) ab, auf dem BFFH läuft und verhindern Angriffe? Auf dieser Seite finden sich Ansätze für ein stabiles, sicheres Setup in einer Linux-Umgebung.

Offene Ports prüfen

```
netstat -an | grep LISTEN | grep -v LISTENING
```

Unattended Upgrades

Automatische Updates per apt

```
sudo apt update
sudo apt upgrade -y
sudo apt install unattended-upgrades -y
sudo dpkg-reconfigure -plow unattended-upgrades
```

Fail2ban

Basiert auf https://www.digitalocean.com/community/tutorials/how-to-protect-an-nginx-server-with-fail2ban-on-ubuntu-20-04

```
sudo apt install fail2ban
sudo systemctl enable fail2ban.service
```

```
cd /etc/fail2ban/
sudo cp jail.conf jail.local
```

```
sudo vim /etc/fail2ban/jail.local
```

```
[DEFAULT]
. . .
findtime = 10m
maxretry = 5
```

```
. . .
```

```
sudo vim /etc/fail2ban/jail.d/defaults-debian.conf
```

```
[DEFAULT]
banaction = nftables
banaction_allports = nftables[type=allports]
backend = systemd

[sshd]
enabled = true
```

```
sudo systemctl restart fail2ban.service
```

Version #3
Erstellt: 2024-12-28 02:14:38 CET von Mario Voigt (Stadtfabrikanten e.V.)
Zuletzt aktualisiert: 2025-03-04 01:39:14 CET von Mario Voigt (Stadtfabrikanten e.V.)