
# Rootserver absichern

Florian Lohoff, filoo GmbH

# Ihr Webinar-Team

filoo®
member of Thomas Krenn Group

- Referent: Florian Lohoff
  - Linux-Guru bei filoo GmbH
  - Debian Entwicker

- Moderation: Stefanie Jerchel
  - Marketing Thomas-Krenn.AG
  - Sammelt Fragen / Feedback

# filoo GmbH

member of Thomas Krenn Group

- Wir sind die Hosting-Tochter der Thomas-Krenn.AG
  - Sicheres, hochperformantes Hosting in Frankfurt
  - Mitarbeiter in Gütersloh und Freyung
- Primärer Rechenzentrumsstandort Frankfurt
  - Tier3, ISO 27001
  - Fläche in zwei Brandabschnitten
- Managed Services
  - Planung & Deployment
  - Security Services
  - Systemadministration

# Agenda

filoo®
member of Thomas Krenn Group

- Die ersten fünf Minuten auf einem Rootserver
  - Erstabsicherung
- Wie kommen sie rein – wie bleiben sie draußen?
  - Passwörter, SSH und Co.
- System aktuell halten
  - Automatische Updates unter Debian
- System Management Controller (IPMI)
  - Ausschalten ist auch ein Denial of Service (DoS)
- Zwei-Faktor-Authentifizierung
  - … Für SSH
- Wenn doch was passiert

# Neuer Rootserver

filoo®
member of Thomas Krenn Group

- Erster SSH-Login (als root oder sudo root):
  - apt-get update && apt-get upgrade
  - passwd – Rootpasswort ändern
    - Sicheres Passwort: apt-get install pwgen; pwgen –s 16 1

# User anlegen & sudo

filoo®
member of Thomas Krenn Group

- useradd admin
  mkdir /home/admin
  mkdir /home/admin/.ssh
  chmod 700 /home/admin/.ssh
- passwd admin
  - Vorher sicheres Passwort generieren
- visudo
  - Existierende Zeilen auskommentieren
  - root ALL=(ALL) ALL
    admin ALL=(ALL) ALL

# SSH Key Auth aktivieren

filoo®
member of Thomas Krenn Group

_ssh-keygen

_vim /home/admin/.ssh/authorized_keys

_chmod 400 /home/admin/.ssh/authorized_keys

_chown admin:admin /home/admin –R

# SSH-Server sichern

filoo®
member of Thomas Krenn Group

- vim /etc/ssh/sshd_config
- PermitRootLogin no
  PasswordAuthentication no

- Passwort-loses SSH ist sicherer (Bruteforcing wird ineffektiv)

# hosts.allow / hosts.deny

filoo®
member of Thomas Krenn Group

- Viele Anwendungen beachten hosts.allow/hosts.deny
  - ssh
  - snmp
  - mysql
- /etc/hosts.allow: Von hier Zugriff erlauben
- /etc/hosts.deny: Von hier Zugriff verbieten
- Sichere Konfiguration: Alles verbieten, selektiv erlauben

# Beispielkonfiguration

filoo®
member of Thomas Krenn Group

- /etc/hosts.deny
  ALL: ALL

- /etc/hosts.allow
  sshd: 1.2.3.4
  sshd: myhostname.dyndns.org
  mysqld: 127.0.0.1

- Konfiguration unbedingt mit neuer SSH-Session parallel testen, sonst u.U. direkt ausgesperrt

# Angreifer draußen halten

filoo®
member of Thomas Krenn Group

- apt-get install fail2ban
- Default-Configs für SSH aktiviert
  - Standardwerte passen meist
- Viele weitere Plugins
  - Mailserver (SMTP/POP/IMAP)
  - FTP
  - Wordpress
  - Etc.

# Firewalling / ferm

filoo®
member of Thomas Krenn Group

- Dienste die nicht gegen den tcpwrapper gelinkt sind.
- Unerwartete Dienste sind per definition erstmal unerreichbar.
- Integration von IPv4 und IPv6

# ferm Beispiel

member of Thomas Krenn Group

```
@def $RFC1918 = ( 192.168.0.0/16 172.16.0.0/12 10.0.0.0/8 );
@def $TRUSTHOST = ( 192.0.2.66 2001:db8:dead:beef::66 );

domain ( ip  ip6 ) {
table filter {
   chain  INPUT {
      policy  DROP;

      mod state state INVALID DROP;
      mod state state (ESTABLISHED RELATED) ACCEPT;

      interface lo ACCEPT;

      proto  icmp ACCEPT;
      saddr ( $TRUSTHOST ) proto tcp dport ssh ACCEPT;
      saddr ( $RFC1918 ) proto tcp dport ssh ACCEPT;
   }
}
```

# Automatisierte Updates

filoo®
member of Thomas Krenn Group

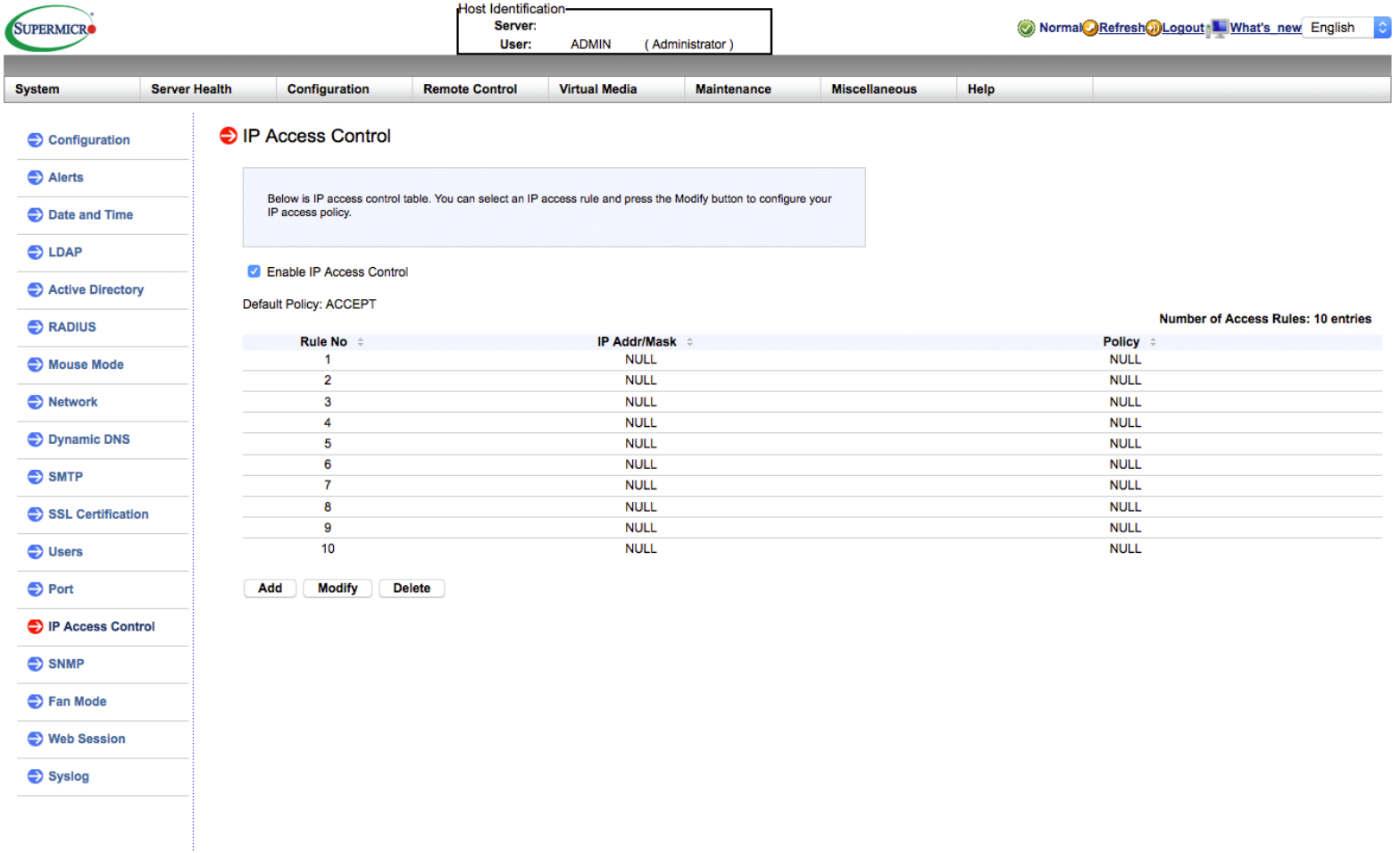
- Debian: unattended-upgrades / apticron
  - Auswahl von Paketen die nicht geupdated werden
  - Nur bestimmte repositories
- CentOS: yum-cron
  - Auswahl des yum updates, security-severity etc.

# IPMI Security

filoo®
member of Thomas Krenn Group

- System Management Controller (IPMI) nicht ins Internet stellen
  - Nur per VPN / Tunnel / Gateway-Maschine
- Wenn es nicht anders geht: IP-ACL
  - Achtung, können nicht alle
- Vorsicht bei veralteten Firmwareständen
  - Jede Menge Sicherheitslücken
  - Regelmäßig updaten
  - Ggf. den Hoster fragen

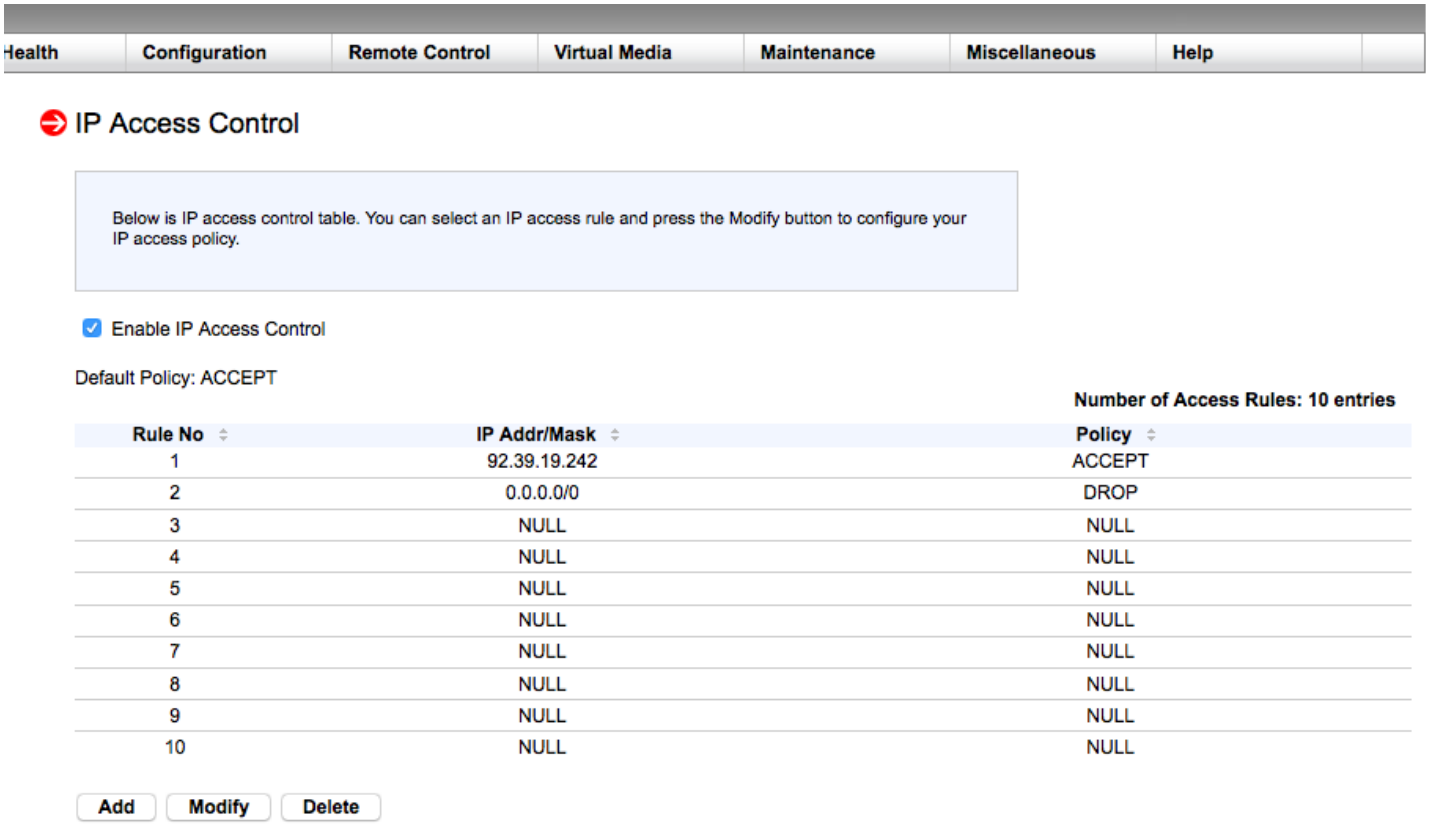
# IPMI ACL Settings



# IPMI Security: Regeln

filoo®
member of Thomas Krenn Group

# IPMI ACL Regelreihenfolge



# Zwei-Faktor-Auth

filoo®
member of Thomas Krenn Group

- Wichtig: Zwei verschiedene Faktoren
  - Zweimal derselbe reicht nicht
- Passwort + Smartcard
  - Etwas, das ich habe + etwas, das ich weiß
- SSH-Login mit verschlüsseltem Key
  - Etwas, das ich habe + etwas, das ich weiß
- One-Time-Code + Passwort
  - Etwas, das ich habe + etwas, das ich weiß

# PAM TFA

filoo®
member of Thomas Krenn Group

- apt-get install libpam-google-authenticator
  - Ab Debian 8 in apt
- Editiere /etc/pam.d/sshd
  - auth [success=done new_authtok_reqd=done default=die] pam_google_authenticator.so nullok
- Editiere /etc/ssh/sshd_config
  - PermitRootLogin yes/no (without-password geht nicht!)
  - ChallengeResponseAuthentication yes
  - AuthenticationMethods publickey,keyboard-interactive:pam
  - UsePAM yes
- SSH neustarten: service ssh restart

# PAM TFA: User einrichten

filoo®
member of Thomas Krenn Group

# PAM TFA: Clients

filoo®
member of Thomas Krenn Group

- „Google Authenticator“ aus dem Appstore
  - Telefoniert nicht nach Hause
  - Funktioniert einfach
- Einrichten mit Barcode aus „google-authenticator“ Einrichtung
- Beliebig viele Codes möglich

# Wenn doch was passiert

filoo®
member of Thomas Krenn Group

- nmap
- debsums
- etckeeper
- tripwire
- rkhunter
- chkrootkit
- logcheck
- Und ein Backup ....

# Vielen Dank

filoo®
member of Thomas Krenn Group

_Ich freue mich auf Ihre Fragen!

_Kontaktdaten:
- _E-Mail: florian.lohoff@filoo.de
- _Telefon: 05241/86730-0

_Besuchen Sie filoo!
- _https://www.filoo.de/
- _http://twitter.com/filoogmbh