# Securing a Samba-Fileserver inside an Active Directory

Stefan Kania

6. Juni 2018

# Distribution

## Which Distribution to choose

# Distribution

## Which Distribution to choose

- Select the distribution

# Distribution

## Which Distribution to choose

- Select the distribution
  - choose the same distribution for all systems

# Distribution

## Which Distribution to choose

- Select the distribution
  - choose the same distribution for all systems
  - LTS-versions

# Distribution

## Which Distribution to choose

- Select the distribution
  - choose the same distribution for all systems
  - LTS-versions
  - maintaining the Samba-Packages

# Distribution

## Which Distribution to choose

- Select the distribution
  - choose the same distribution for all systems
  - LTS-versions
  - maintaining the Samba-Packages
- same source for all packages

# Distribution

## Which Distribution to choose

- Select the distribution
  - choose the same distribution for all systems
  - LTS-versions
  - maintaining the Samba-Packages
- same source for all packages
  - build on your own

# Distribution

## Which Distribution to choose

- Select the distribution
  - choose the same distribution for all systems
  - LTS-versions
  - maintaining the Samba-Packages
- same source for all packages
  - build on your own
  - from distribution

# Distribution

## Which Distribution to choose

- Select the distribution
  - choose the same distribution for all systems
  - LTS-versions
  - maintaining the Samba-Packages
- same source for all packages
  - build on your own
  - from distribution
  - SerNet packages

# Systemsecurity

## System installation und configuration

# Systemsecurity

## System installation und configuration

- no gui

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages
- Partitioning

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages
- Partitioning
  - root-Partiton (rw)

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages
- Partitioning
  - root-Partiton (rw)
  - /boot (ro)

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages
- Partitioning
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages
- Partitioning
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages
- Partitioning
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)
  - /tmp (rw,noexec)

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages
- Partitioning
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)
  - /tmp (rw,noexec)
  - /daten (rw,noexec)

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages
- Partitioning
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)
  - /tmp (rw,noexec)
  - /daten (rw,noexec)
- Only needed protocols

# Systemsecurity

## System installation und configuration

- no gui
- only needed packages
- Partitioning
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)
  - /tmp (rw,noexec)
  - /daten (rw,noexec)
- Only needed protocols
- Only needed services (one server, one service)

# configuring Samba

## basic settings in smb.conf

# configuring Samba

## basic settings in smb.conf

- deactivate NetBIOS

# configuring Samba

## basic settings in smb.conf

- deactivate NetBIOS
- client ipc min protocol = smb2_10

# configuring Samba

## basic settings in smb.conf

- deactivate NetBIOS
- client ipc min protocol = smb2_10
- client min protocol = smb2_10

# configuring Samba

## basic settings in smb.conf

- deactivate NetBIOS
- client ipc min protocol = smb2_10
- client min protocol = smb2_10
- disable netbios = yes

# configuring Samba

## basic settings in smb.conf

- deactivate NetBIOS
- client ipc min protocol = smb2_10
- client min protocol = smb2_10
- disable netbios = yes
- smb ports = 445

# configuring an Admin-share

## Only for admins

# configuring an Admin-share

## Only for admins

- path = /data/admin-share

# configuring an Admin-share

## Only for admins

- path = /data/admin-share
- browsable = no

# configuring an Admin-share

## Only for admins

- path = /data/admin-share
- browsable = no
- read only = no

# configuring an Admin-share

## Only for admins

- path = /data/admin-share
- browsable = no
- read only = no
- administrative share = yes

# Creating a share for users

## with auditing

# Creating a share for users

## with auditing

- path = /data/admin-share/department

# Creating a share for users

## with auditing

- path = /data/admin-share/department
- browsable = no

# Creating a share for users

## with auditing

- path = /data/admin-share/department
- browsable = no
- read only = no

# Creating a share for users

## with auditing

- path = /data/admin-share/department
- browsable = no
- read only = no
- hide unreadable = yes

# Creating a share for users

## with auditing

- path = /data/admin-share/department
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit

# Creating a share for users

## with auditing

- path = /data/admin-share/department
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect

efan Kania
onsulting durch Training

# Creating a share for users

## with auditing

- path = /data/admin-share/department
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect
- full_audit:prefix = %u|%I|%m|%S

efan Kania
onsulting durch Training

# Creating a share for users

## with auditing

- path = /data/admin-share/department
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect
- full_audit:prefix = %u|%I|%m|%S
- full_audit:failure = none

efan Kania
onsulting durch Training

# Creating a share for users

## with auditing

- path = /data/admin-share/department
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect
- full_audit:prefix = %u|%I|%m|%S
- full_audit:failure = none
- full_audit:facility = local5

# Creating a share for users

## with auditing

- path = /data/admin-share/department
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect
- full_audit:prefix = %u|%I|%m|%S
- full_audit:failure = none
- full_audit:facility = local5
- full_audit:priority = notice

# Now the firewall

## Access control for all

# Now the firewall

## Access control for all

- Everyting is forbidden

# Now the firewall

## Access control for all

- Everyting is forbidden
- OUTPUT open for all ports

# Now the firewall

## Access control for all

- Everyting is forbidden
- OUTPUT open for all ports
- ssh open

# Now the firewall

## Access control for all

- Everyting is forbidden
- OUTPUT open for all ports
- ssh open
- Port 445 for smb open

# Now the firewall

## Access control for all

- Everyting is forbidden
- OUTPUT open for all ports
- ssh open
- Port 445 for smb open
- Protect against ssh-attackers

# Now the firewall

## Access control for all

- Everyting is forbidden
- OUTPUT open for all ports
- ssh open
- Port 445 for smb open
- Protect against ssh-attackers
- A simple portscanner protection

# test test test

## Checking security

# test test test

## Checking security

- test on a regular base

# test test test

## Checking security

- test on a regular base
- Test with Nmap

# test test test

## Checking security

- test on a regular base
- Test with Nmap
- Always test for updates

# test test test

## Checking security

- test on a regular base
- Test with Nmap
- Always test for updates
- Let some else test your systems