BSA

147.228.67.154
Bs@-20*25

Users

Vytvoreni
adduser jakub
useradd jakub

Manipulace
usermod

Přidání do skupiny
usermod jakub -a -G customusers

Lock
usermod -L jakub

Změna hesla
passwd jakub

ACL

apt install acl -y

nastavení fs
nano /etc/fstab
UUID=xxxx / ext4 defaults,acl 0 1

sudo mount -o remount,acl /

výpis práv k souboru
getfacl test.txt

přidání práv
setfacl -m user:jakub:rw test.txt
setfacl -m group:bsa:r test.txt

odebrání práv
setfacl -x u:jakub test.txt

odebrání všech acl záznamů
setfacl -b test.txt

ugo práva mají přednost před acl - nutné odebrat
chmod 600 test.txt

LDAP

apt install slapd ldap-utils ldapscripts -y

první nastavení
dpkg-reconfigure -plow slapd
- Omit OpenLDAP server configuration? - No
- DNS domain name: jakub.bsa
- Organization name: jakub

vytvoření organizační jednotky
create_ou.ldiff:
dn: ou=users,dc=jakub,dc=bsa
objectClass: organizationalUnit
ou: users

ldapadd -f create_ou.ldif -D cn=admin,dc=jakub,dc=bsa -w test123

vytvoření usera
create_user.ldif:
dn: uid=pepa,ou=users,dc=jakub,dc=bsa
uid: pepa
cn: pepa
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: test123
shadowLastChange: 14846
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 10001
gidNumber: 10001
homeDirectory: /home/ldap/pepan

ldapadd -f create_user.ldif -D cn=admin,dc=jakub,dc=bsa -w test123

předávání hesla
-w ... heslo součástí skriptu
-W ... zeptá se na heslo

lokální výpis všech záznamů

slapcat

vyhledávání
ldapsearch -D cn=admin,dc=jakub,dc=bsa -w test123 -b "dc=jakub,dc=bsa" '(objectClass='account')' cn

Autentizace pomocí LDAP
apt install libnss-ldap libpam-ldap

ověření
getent passwd

Sudo

přidání uživatele do skupiny sudo
usermod -a -G sudo jakub

úprava souboru sudo
visudo

PAM moduly

apt-get install libpam-pwquality

soubor /etc/pam.d/common-password

Šifrování disků

apt install cryptsetup

založení volumu pomocí lvm
pvcreate /dev/sdb
vgcreate vgbsa /dev/sdb
lvcreate -L 1G -n test /dev/sdb/vgbsa

zašifrování volumu
cryptsetup -y -v luksFormat /dev/vgbsa/test

dešifrování volumu - otevře device /dev/mapper/decrypted
cryptsetup luksOpen /dev/vgbsa/test decrypted

zavření device
cryptsetup luksClose decrypted

tvorba filesystemu ext4
mkfs.ext4 /dev/mapper/decrypted

mount device
mount /dev/mapper/decrypted /mnt

Klíče
výpis klíčů
cryptsetup luksDump /dev/vgbsa/test

přidání klíče
cryptsetup luksAddKey /dev/vgbsa/test

přidání keyfile
cryptsetup luksAddKey /dev/vgbsa/test /some/key/file

otevření/přidání klíče pomocí keyfile
cryptsetup luksOpen /dev/vgbsa/test --key-file /some//key/file
cryptsetup luksAddKey /dev/vgbsa/test /some/key/file --key-file /some/existing/key/file

přidání klíče do konkrétního slotu
cryptsetup luksAddKey /dev/vgbsa/test -S 6

odstranění klíče
cryptsetup luksRemoveKey /dev/vgbsa/test

odstranění klíče z konkrétního slotu
cryptsetup luksKillSlot /dev/vgbsa/test 6

mount při startu
do /etc/crypttab přidat:
decrypted UUID=8063f862-4950-4632-a037-8925cb7b95a2 /root/keyfile luks
(UUID lze získat pomocí luksDump)

do /etc/fstab přidat:
/dev/mapper/decrypted /mnt/secure ext4 defaults 0 2

Certifikační autorita - EasyRSA
apt install easy-rsa -y
cp -r /usr/share/easy-rsa/ /etc/ca

nastavení
cp vars.example vars
vars:
set_var EASYRSA_REQ_COUNTRY "CZ"

```
set_var EASYRSA_REQ_PROVINCE    "Pilsen"
set_var EASYRSA_REQ_CITY        "Pilsen"
set_var EASYRSA_REQ_ORG         "Jakub BSA Corp."
set_var EASYRSA_REQ_EMAIL       "jakub@jakub.bsa"
set_var EASYRSA_REQ_OU          "Security"

set_var EASYRSA_KEY_SIZE        2048
...

./easyrsa init-pki
./easyrsa build-ca
```

tvorba a podpis server certifikátu

```
./easyrsa gen-req server.jakub.bsa
./easyrsa sign server server.jakub.bsa
```

revokace a tvorba revokačního listu

```
./easyrsa revoke server.jakub.bsa
./easyrsa gen-crl
```

výpis info o certifikátu

```
openssl x509 -in /etc/ca/pki/ca.crt -text
```

odstranění hesla z klíče pro použití ve webserveru

```
openssl rsa -in pki/private/server.jakub.bsa.key -out pki/private/
server.jakub.bsa.key.in
```

Použití certifikátů pro nginx https

```
apt install nginx -y
```

sites-available/default:

```
listen 443 ssl default_server;
listen [::]:443 ssl default_server;
ssl_certificate /etc/ca/pki/issued/server.jakub.bsa.crt;
ssl_certificate_key /etc/ca/pki/private/server.jakub.bsa.key.in;
```

reload

```
systemctl reload nginx
```

povolit 443 port na FW

```
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

stažení certifikátu na lokál

```
scp bsa:/etc/ca/pki/ca.crt ca.crt
```

kopie ca mezi servery
scp /etc/ca/pki/ca.crt bsa2:/usr/share/ca-certificates/ca-bsa.crt

trust self-signed ca na debian
cp /etc/ca/pki/ca.crt /usr/share/ca-certificates/ca-bsa.crt

/etc/ca-certificates.conf:
ca-bsa.crt

update-ca-certificates

Dehydrated

mkdir -p /var/www/dehydrated/.well-known/acme-challenge/
cp /usr/share/doc/dehydrated/examples/hook.sh .
chmod +x hook.sh

dehydrated --cron

OpenSSL

vygenerování private klíče
openssl genrsa -out key.pem 4096

vygenerování public klíče z private
openssl rsa -in key.pem -pubout > key.pub

podpis dat
openssl dgst -sign key.pem -keyform PEM -sha256 -out data.zip.sign -binary data.zip

verifikace podpisu
openssl dgst -verify key.pub -keyform PEM -sha256 -signature data.zip.sign data.zip

GPG
apt install gpg -y

vygenerování klíče
gpg --gen-key

export a import public klíče
gpg --export > pubkey.asc
gpg --import pubkey.asc

zašifrování a dešifrování souboru
gpg --encrypt test.txt
gpg --output test_dec.txt --decrypt test.txt.gpg

John the Ripper
apt install john

unshadow /etc/passwd /etc/shadow > output.db
john output.db

Stunnel
apt install stunnel

příprava certifikátu
cd /etc/ca
./easyrsa gen-req stunnel.jakub.bsa
./easyrsa sign server stunnel.jakub.bsa
openssl rsa -in pki/private/stunnel.jakub.bsa.key -out pki/private/
stunnel.jakub.bsa.key.in
cat pki/issued/stunnel.jakub.bsa.crt pki/ca.crt pki/private/stunnel.jakub.bsa.key.in
> /etc/stunnel/stunnel.jakub.bsa.pem

konfigurace - /etc/stunnel/stunnel.cnf
pid = /var/run/stunnel.pid
[https]
accept = 443
connect = 127.0.0.1:80
cert = /etc/stunnel/stunnel.jakub.bsa.pem

systemctl restart stunnel4

debug
openssl s_client -connect 147.228.67.151:443

OpenVPN
apt install openvpn

Server setup

setup certifikátů
cd /etc/ca
./easyrsa gen-req vpn.jakub.bsa nopass
./easyrsa sign server vpn.jakub.bsa

./easyrsa gen-crl
./easyrsa gen-dh

mkdir /etc/openvpn/certs
cp pki/ca.crt pki/dh.pem pki/crl.pem pki/issued/vpn.jakub.bsa.crt pki/private/vpn.jakub.bsa.key /etc/openvpn/certs

konfigurace
cd /etc/openvpn

wget https://raw.githubusercontent.com/jindrichskupa/kiv-bsa/master/cv05-vpn/bsa-server.conf
nastavit cesty k certifikátům
odebrat/zakomentovat řádku s script-security

mkdir bsa-clients
konfigurace pro každého clienta (filename podle common name z certifikátu klienta)
nano client-01
ifconfig-push 192.168.35.2 255.255.255.0

spuštění service
systemctl enable openvpn@bsa-server
systemctl start openvpn@bsa-server

firewall pravidlo
iptables -A INPUT -p udp --dport 1194 -j ACCEPT

Client setup

setup certifikátů (na serveru)
cd /etc/ca
./easyrsa gen-req client-01.vpn.jakub.bsa nopass
./easyrsa sign client client-01.vpn.jakub.bsa

scp /etc/ca/pki/ca.crt bsa2:/etc/openvpn/certs
scp /etc/ca/pki/issued/client-01.vpn.jakub.bsa.crt bsa2:/etc/openvpn/certs
scp /etc/ca/pki/private/client-01.vpn.jakub.bsa.key bsa2:/etc/openvpn/certs

konfigurace (client)
wget https://raw.githubusercontent.com/jindrichskupa/kiv-bsa/master/cv05-vpn/bsa-client-01.conf
nastavit cesty k certifikátům

validace server certifikátu - do bsa-client-01.conf doplnit:
remote-cert-tls server

konfigurace hosta:
sudo nano /etc/hosts
147.228.67.154 vpn.jakub.bsa

Ověření

výpis připojených klientů na serveru
cat /run/openvpn/bsa-server.status

výpis info v certifikátu
openssl x509 -in client-01.vpn.jakub.bsa.crt -text | less

Wireguard

Vygenerovat private key:
wg genkey > server.key

Public key:
cat server.key | wg pubkey > server.pub

zobrazení statistik
wg

DNS

Knot

apt install knot knot-dnsutils -y

reload konfigurace
knotc reload

nutné změnit owner zone souborů na knot
chown knot:knot jakub.bsa.zone

dig ns.jakub-secured.bsa +dnssec +trace @127.0.0.1

Bind + DNSSec
apt install bind9 dnsutils -y

konfigurace zóny
cd /etc/bind

named.conf.local:

```
zone "jakub.bsa." in {
    type master;
    file "/var/cache/bind/db.jakub.bsa";
    inline-signing yes;
    auto-dnssec maintain;
    key-directory "/etc/bind/keys";
};
```

zónový soubor
db.jakub.bsa:

```
$TTL    604800
@   IN  SOA jakub.bsa. root.localhost. (

        2025051701     ; Serial / YYYYMMDDXX
           604800     ; Refresh / seconds
            86400     ; Retry / seconds
          2419200 ; Expire / seconds
           604800 )   ; Negative Cache TTL / explicitni TTL

@         IN      NS              ns.jakub.bsa.
@         IN      A               147.228.173.147
bsa1      IN      A               147.228.173.147
mail      IN      A               147.228.173.147
pop3      IN      CNAME           mail
smtp      IN      CNAME           mail
imap      IN      CNAME           mail
@         IN      MX          10  mail
ns        IN      A               147.228.173.147
vpn       IN      A               147.228.173.147
bsa2      IN      A               147.228.173.37
```

kontrola zónového souboru:

```
named-checkzone jakub.bsa /var/cache/bind/db.jakub.bsa

chown bind:bind /var/cache/bind/db.jakub.bsa
```

klíče

```
mkdir /etc/bind/keys
cd /etc/bind/keys
dnssec-keygen -a ECDSAP256SHA256 -fK jakub.bsa
chmod g+r K*.private

systemctl restart bind9
rndc sign jakub.bsa
```

ověření

```
dig jakub.bsa +dnssec @localhost
```

(měl by zde být záznam RRSIG)

rndc signing -list jakub.bsa
(mělo by být něco jako Done signing with key 12732/ECDSAP256SHA256)

Signing pro zóny s view
rndc signing -list jakub.bsa IN localnetwork
named-compilezone -f raw -j -o - jakub.bsa /var/cache/bind/jakub.bsa

Maily

Postfix
apt install -y postfix
viz SPOS

Mutt
apt install mutt -y

soubor .muttrc
set folder = imap://jakub:test123@bsa1.jakub.bsa:143
set spoolfile = imap://jakub:test123@bsa1.jakub.bsa:143
set smtp_url = smtp://jakub:test123@bsa1.jakub.bsa:25

SPF

vygenerovat záznam pro DNS
https://www.spfwizard.com
něco jako:
@ IN TXT "v=spf1 mx a ip4:147.228.173.147/32 ~all"
přidat do dns a reload
rndc reload
rndc sign jakub.bsa

kontrola
dig jakub.bsa TXT

nastavení postfixu
apt-get install postfix-policyd-spf-python

/etc/postfix/master.cf - přidat
policyd-spf unix - n n - 0 spawn
user=policyd-spf argv=/usr/bin/policyd-spf

/etc/postfix/main.cf - upravit

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated reject_unauth_destination check_policy_service unix:private/policyd-spf

kontrola
poslat mail přes mutta / smtp přes nc
/var/mail/jakub - v mailech Received-SPF: Pass ...
/var/log/mail.log - policyd-spf[90247]: : prepend Received-SPF: Pass

DKIM

RSyslog
apt install rsyslog -y

Server setup
/etc/rsyslog.conf:
$template RemoteLogs,"/var/log/remote/%HOSTNAME%.log"
. ?RemoteLogs

odkomentit (pro udp)
module(load="imudp")
input(type="imudp" port="514")

nebo (pro tcp)
module(load="imtcp")
input(type="imtcp" port="514")

fw pravidlo
udp
iptables -A INPUT -p udp -s 147.228.0.0/16 --dport 514 -j ACCEPT
tpc
iptables -A INPUT -p tcp -s 147.228.0.0/16 --dport 514 -j ACCEPT

Client setup
/etc/rsyslog.conf:
. @@bsa1.jakub.bsa:514
(tcp, pokud máme dns)

. @bsa1.jakub.bsa:514
(udp, pokud máme dns)

. @@147.228.173.147:514
(tcp, pokud bez dns)

RSyslog do db

apt install postgresql rsyslog-pgsql -y
dpkg-reconfigure rsyslog-pgsql

- reinstall - yes
- connection method - unix socket
- authenticating administrator - ident
- authenticating user - password
- zbytek odklikat a nastavit heslo

ověření

su - postgres
psql
\c Syslog
select * from systemevents;