

SPOS 2016

Wednesday 17 February 2016

1.cviceni

Zakladni prikazy:

```
ps auxf
ls | ls -l | ls -al
mkdir | mkdir -p
touch
chmod | chown
man | info
cd | cd - | cd ~
pwd
netstat | netstat -tupln
w | who
id
find
grep | grep -R
cat
sort
mc
cut
nano | vim
for | while | if | read
sed | awk
```

SSH:

```
ssh-keygen
ssh-agent
ssh-add
ssh-copy
cat ~/.ssh/authorized_keys

command="./canrun",no-port-
forwarding,no-x11-forwarding,no-
agent-forwarding ssh-dss KEY
user@machine

ssh -i ~/.ssh/id_rsa.pub machine
ssh -l user machine.local
ssh user@machine.local
ssh user@machine "uname -a"

cat ~/.ssh/config

vim /etc/ssh/sshd_config
    PasswordAuthentication no
```

Zabezpeceni:

```
iptables -A INPUT -s 147.228.0.0/16 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j DROP
```

```
iptables-save > /etc/network/iptables
iptables-restore /etc/network/iptables
```

```
/etc/network/interfaces
    post-up /sbin/iptables-restore /etc/network/iptables
```

apt-get install fail2ban

ssh (/etc/ssh/sshd_config):

AllowUsers root

PasswordAuthentication no

PermitRootLogin without-password

* TcpWrappers (ldd /usr/sbin/sshd | grep libwrap):

/etc/hosts.allow

sshd : 147.228.0.0/255.255.0.0

/etc/hosts.deny

tcpdmatch sshd localhost

tcpdchk

Informace o serveru a nastavení:

Služby:

/etc/

/etc/resolv.conf

/etc/hostname

/etc/network/interfaces

/etc/fstab

/etc/hosts

/etc/passwd | /etc/group | /etc/shadow

/etc/debian_version | /etc/redhat-release

service fail2ban restart

/etc/init.d/fail2ban restart

systemctl restart fail2ban.service

start | stop | restart | status | ...

hostname

uname

iptables

ifconfig | route | ip

dpkg | aptitude

free

cat /proc/cpuinfo | cat /proc/meminfo

mount

netstat -tupln

crontab -l

top

htop