http://spad.dy.fi
Teppo Rinne
8.11.2018

Quick survival guide

Käyttäjät

less /etc/passwd

who

su – tai su [käyttäjä] (huom. ympäristömuuttujat)

```
groupadd –g 700 [Group]

useradd YourService –c  ’desc’ –m –u 567 –G [Group] –s /bin/nologin
```

Levytila

Disk free (-human)

```
df –h
```

Disk used, human, vain alihakemistot nykyisessä sijainnissa

```
du –h –max-depth=1
```

Hakemistot

```
ll = ls –l
```

aikajärjestys vanhimmasta uusimpaan

```
ls –lart
```

Etsi tiedosto

```
find [mistä] –name [osa tiedostonimestä]
```

Pakkaa löydetyt tiedostot gzipillä

```
find [mistä] –name ’[osa tiedostonimestä]’ –exec gzip –v {} \;
```

Tiedostojärjestelmän oikeudet

antaa suoritusoikeudet käyttäjälle

```
chmod u+x [filu]
```

Lisää alihakemistoon uusien tiedostojen groupin asetus hakemiston ryhmän perusteella

```
chmod g+s [hakemisto]
```

Muuttaa käyttäjän root omistamat tiedostot toiselle

```
find . -user root -exec chown [user]:[group] {} \;
```

Logit

More or less?

shft + G → Loppuun

/[sana] → Etsi, n = next, N = previous

Huom. less osaa purkaa myös gzipit lennosta

```
less [tiedosto]
```

Etsi sanaa tiedostosta (-i = ignore case)

```
grep -i [sana] [tiedosto]
```

Ajastukset (huom. käyttäjäkohtaisia)

Listaa cron-jobit

```
crontab –l
```

Lue prosessit croniin tiedostosta

```
crontab [filu]
```

Palvelut ja prosessit

/etc/init.d

etc/rc.#/S## / K##

ps aux | grep [osa prosessin nimestä tai käyttäjä]

- a = all users
- u = show user

```
kill

kill -9
```

Verkkojutut

IP-osoitteet interfaceilla

```
ifconfig

ip addr
```

Hae nimipalvelusta

```
nslookup
```

Testaa yhteys kohteeseen (ICMP / haluamasi portti)

```
ping

telnet 8.8.8.8 25 (käytä vain jos nc ei käytössä)
```

Näytä käytössä olevat verkkoyhteydet

- -a = kuuntelussa

- -n = numeric format
- -p = show process
- -t = tcp

```
netstat –anlp –t
```

Testaa TCP-kättely haluttuun kohteeseen

```
nc locahost 443
```

Avaa portin kuunteluun

```
nc –l 443
```

Pakettikaappaukset

Tallentaa verkkoliikenteen tiedostoon

```
tcpdump –i [interface] –w [file] –s 0 host 8.8.8.8

tcpdump –i [interface] –w [file] –s 0 host 8.8.8.8 and port 443
```

Muuttaa IP-osoitteen (8.8.8.8 → 1.1.1.1) tai portin (8443→443) pakettikaappauksessa, laskien uuden tarkistussumman

```
tcprewrite --pnat=8.8.8.8:1.1.1.1 --portmap=8443:443--infile=in.pcap --
outfile=out.pcap --skipbroadcast
```

Tallentaa pakettien TCP-sekvenssinumeron ja –tarkistussumman tekstitiedostoon, josta niitä voi verrata toisiinsa → muuttuuko data matkalla verkon aktiivilaitteissa?

```
tshark –r side1.pcap –Y “ip.src == 8.8.8.8” –T fields –e tcp.seq –e tcp.checksum
>out_side1.txt

tshark –r side2.pcap –Y “ip.src == 8.8.8.8” –T fields –e tcp.seq –e tcp.checksum
>out_side2.txt

diff out_side1.txt out_side2.txt
```

Tiedostojen siirto

```
scp [tiedosto] [käyttäjä]@[palvelin]:/polku/

rsync
```

Sertit ja storet

Oletus keystoren sijainti <JAVA_HOME>/jre/lib/security/cacerts ja salasana on changeit

Kopioi oletus keystore uuteen sijaintiin ja resetoi salasana.

Luo uusi itse allekirjoitettu serti ja privaattiavain, sekä lisää se sertifikaatti-storeen

```
keytool –genkeypair –alias OmaSerti –keypass OmanAvaimenSalasana –keyalg RSA –keysize
2048 –dname ”CN=oma.domain.com” –keystore /1/2/mykeys.jks –storepass StorenSalasana
```

http://spad.dy.fi
Teppo Rinne
8.11.2018

Importtaa CA:n allekirjoittama serti storeen

```
keytool –importcert –file serti.pem –alias OmaSerti –keypass OmanAvaimenSalasana –
keystore /1/2/mykeys.jks –storepass StorenSalasana
```

Näytä storen sisältö

```
keytool –list –v –keystore /1/2/mykeys.jks –storepass StorenSalasana
```