jamk.fi

Linux perusteet [TTC1040]

harjoitus 12

Maarit Salo

24.11.2021

1. **Change your user to another (for example from regular user to root) and input a wrong password. How and from what log file in /var/log path you can retrieve the information from this failed login attempt?**

```
user@P0033-Ubuntu:~$ su - mike
Password:
su: Authentication failure
user@P0033-Ubuntu:~$ cat /var/log/auth.log | grep mike
```

Loggaudutaan mikellä sisään, laitetaan salasanaksi lohikäärme. Ei onnistu. Grepataan auth.logista miken jutut

```
-Ubuntu su: pam_unix(su-l:auth): authentication failure; logname=user uid=1000 euid=0 tty=pts/0 ruser=user rhost=  user=mike
-Ubuntu su: FAILED SU (to mike) user on pts/0
```

Menee aika pieneksi, mutta toivottavasti saat zoomattua.

2. **How do you retrieve the logged information from journald from last 24 hours so that newest entries are displayed first (at the top)?**

```
user@P0033-Ubuntu:~$ journalctl --since "24 hours ago" --reverse
-- Logs begin at Tue 2021-10-19 19:51:22 EEST, end at Wed 2021-11-24 12:07:11 EET. --
Nov 24 12:07:11 P0033-Ubuntu su[1161]: FAILED SU (to mike) user on pts/0
Nov 24 12:07:08 P0033-Ubuntu su[1161]: pam_unix(su-l:auth): authentication failure; lo
Nov 24 12:07:08 P0033-Ubuntu su[1161]: pam_unix(su-l:auth): Couldn't open /etc/securet
Nov 24 12:06:59 P0033-Ubuntu su[1161]: pam_unix(su-l:auth): Couldn't open /etc/securet
Nov 24 11:59:16 P0033-Ubuntu systemd-logind[690]: Removed session 3.
Nov 24 11:59:16 P0033-Ubuntu systemd[1]: session-3.scope: Succeeded.
Nov 24 11:59:16 P0033-Ubuntu systemd-logind[690]: Session 3 logged out. Waiting for pr
Nov 24 11:59:16 P0033-Ubuntu sshd[1032]: pam_unix(sshd:session): session closed for us
Nov 24 11:58:17 P0033-Ubuntu systemd[1]: Failed to start Ubuntu Advantage APT and MOTD
Nov 24 11:58:17 P0033-Ubuntu systemd[1]: ua-messaging.service: Failed with result 'exi
```

3. **How much do stored journal files take up disk space?**

```
user@P0033-Ubuntu:~$ journalctl --disk-usage
Archived and active journals take up 1.5G in the file system.
user@P0033-Ubuntu:~$
```

Näköjään 1,5 gigaa.

4. **Open journald for real-time logging. Now open SSH connection to your Ubuntu (refer to Putty guide in here). Try to login by typing first the invalid and then the correct password. How are these entries logged?**

```
user@P0033-Ubuntu:~$ journalctl -f
-- Logs begin at Tue 2021-10-19 19:51:22 EEST. --
Nov 24 12:50:48 P0033-Ubuntu sudo[1386]: pam_unix(sudo:session): ses
Nov 24 12:50:48 P0033-Ubuntu sudo[1386]: pam_unix(sudo:session): ses
Nov 24 12:56:44 P0033-Ubuntu sshd[1392]: Accepted password for user
Nov 24 12:56:44 P0033-Ubuntu sshd[1392]: pam_unix(sshd:session): ses
Nov 24 12:56:44 P0033-Ubuntu systemd-logind[690]: New session 7 of u
Nov 24 12:56:44 P0033-Ubuntu systemd[1]: Started Session 7 of user u
Nov 24 12:56:51 P0033-Ubuntu sshd[1392]: pam_unix(sshd:session): ses
Nov 24 12:56:51 P0033-Ubuntu systemd-logind[690]: Session 7 logged o
Nov 24 12:56:51 P0033-Ubuntu systemd[1]: session-7.scope: Succeeded.
Nov 24 12:56:51 P0033-Ubuntu systemd-logind[690]: Removed session 7.
```

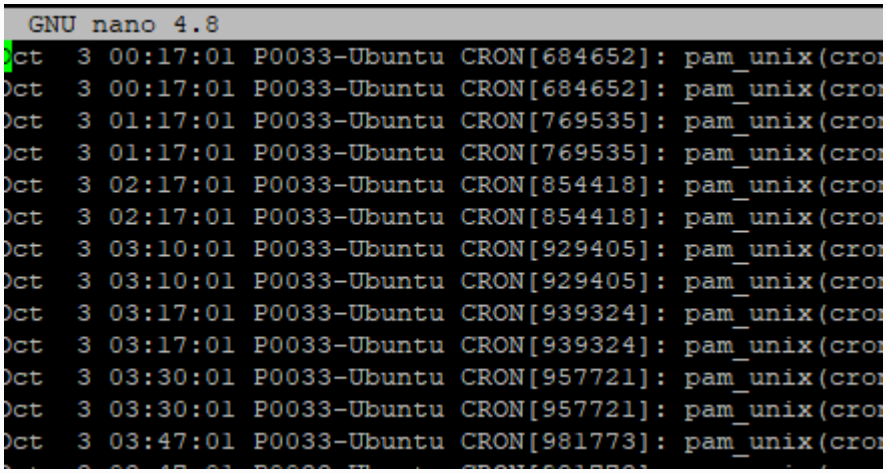
```
login as: user
user@172.21.1.51's password:
Access denied
user@172.21.1.51's password:
Last login: Wed Nov 24 12:56:44 2021 from 192.168.48.14
user@P0033-Ubuntu:~$
```

```
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser
Failed password for user from 192.168.48.14 port 54022 ssh2
Accepted password for user from 192.168.48.14 port 54022 ssh2
pam_unix(sshd:session): session opened for user user by (uid=0)
ind[690]: New session 8 of user user.
Started Session 8 of user user.
```

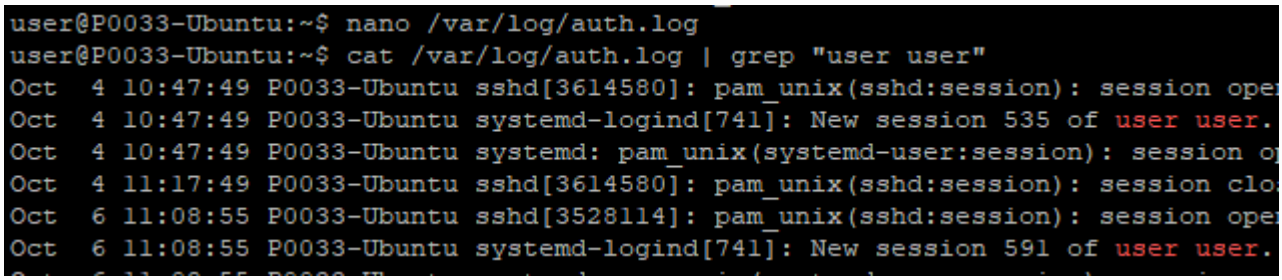
Ekaksi se sanoo että autentikaatio failure, ja että salasana meni mönkään.

Sitten hyväksytään salasana. Ja tulee tietoa uudesta sessiosta

5. **Open authentication log file (auth.log) and check the content. How can you print only lines from this log file to the CLI containing new sessions from your user (tip: use grep)?**

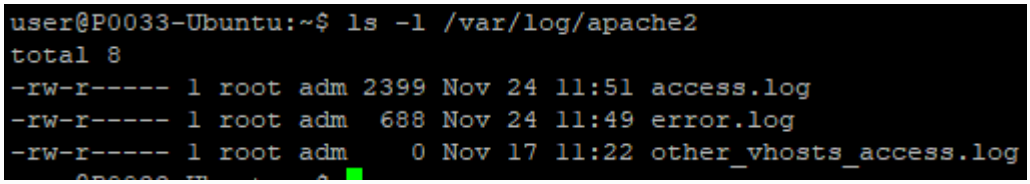


auth.logi näyttää tältä, paljon kamaa



Täältä tulee sitten pelkästään käyttäjä userin juttuja

6. **In previous exercise (EX-11) you installed Apache2 web server (if you haven't, install it with sudo apt install apache2). What log files does this service have (see /var/log directory)?**



Access.logissa on käyttöpyynnöt, error.logissa, noh, virheet, ja other_vhosts_access.logiin merkitään ne virtuaaliset hostit joilla ei ole omaa logi-tiedostoa.