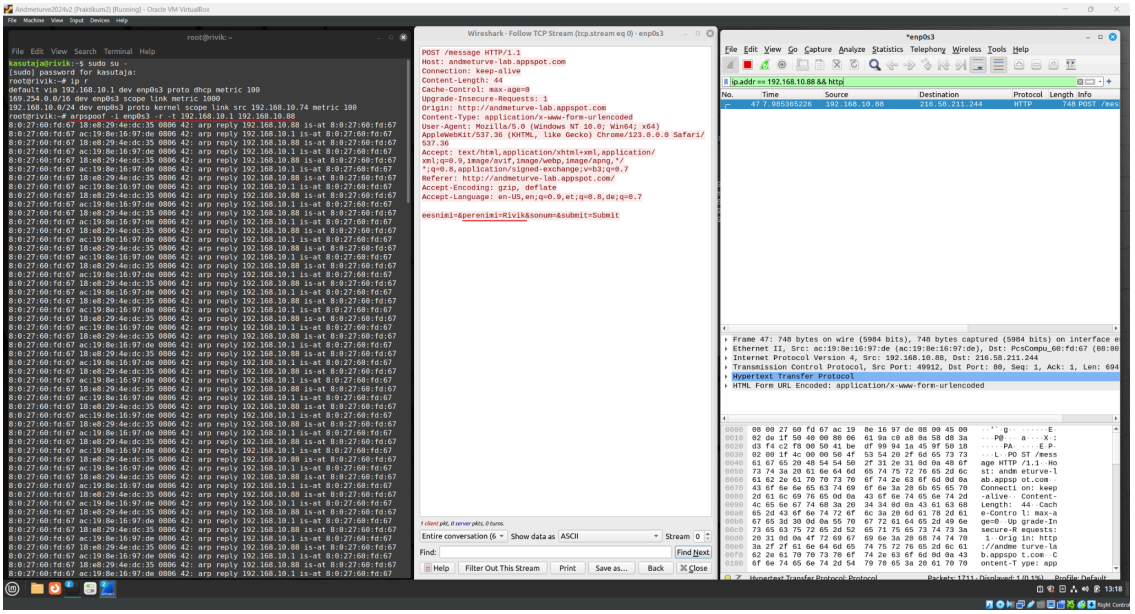
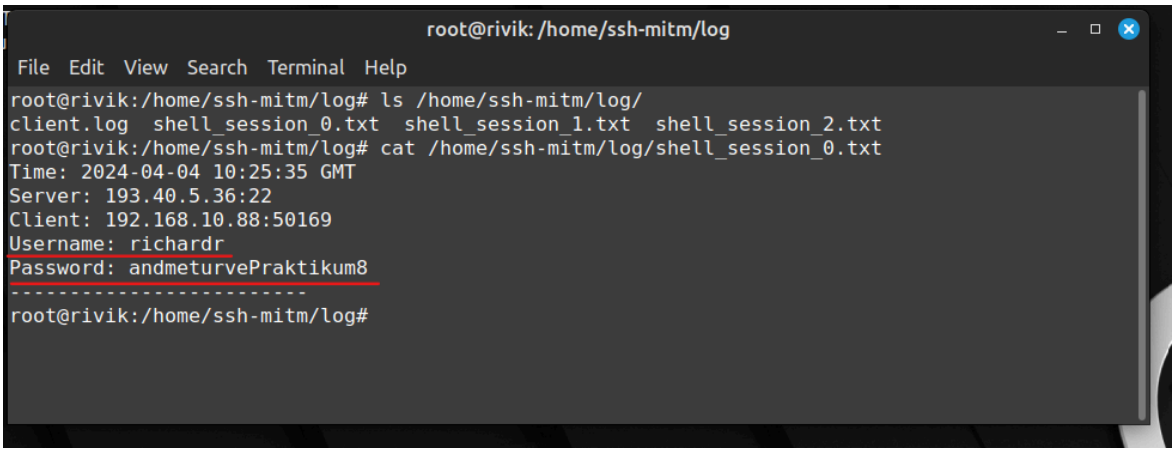
Praktikum 8

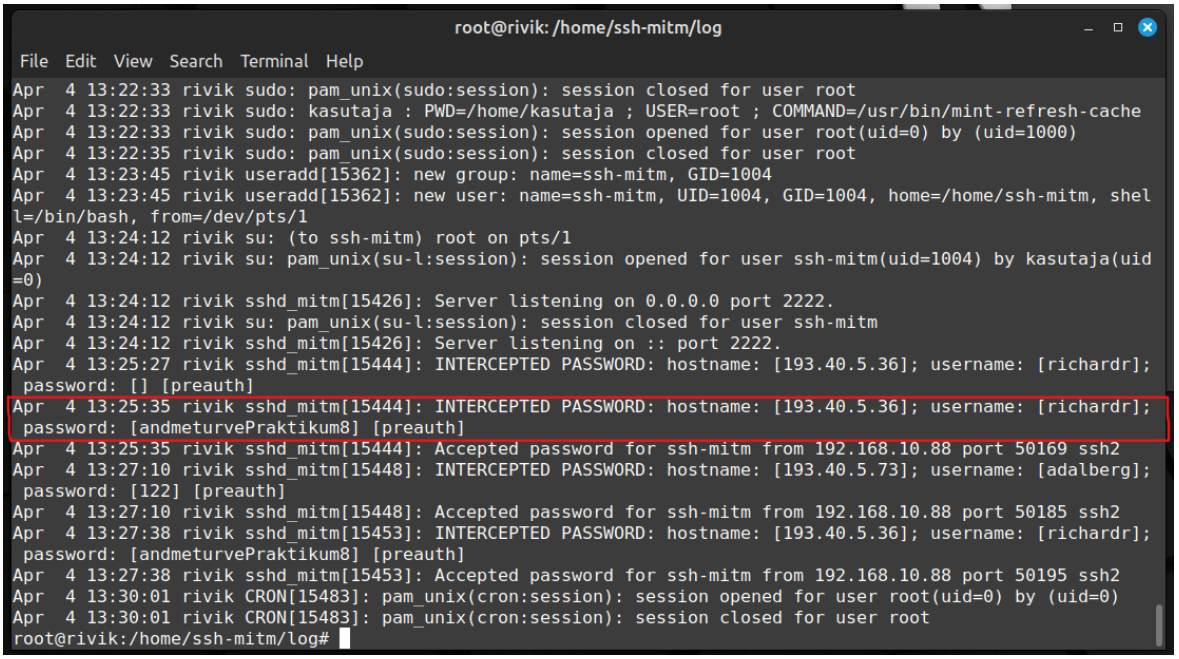
https://courses.cs.ut.ee/2024/turve/spring/Main/Praktikum8

ÜL 1

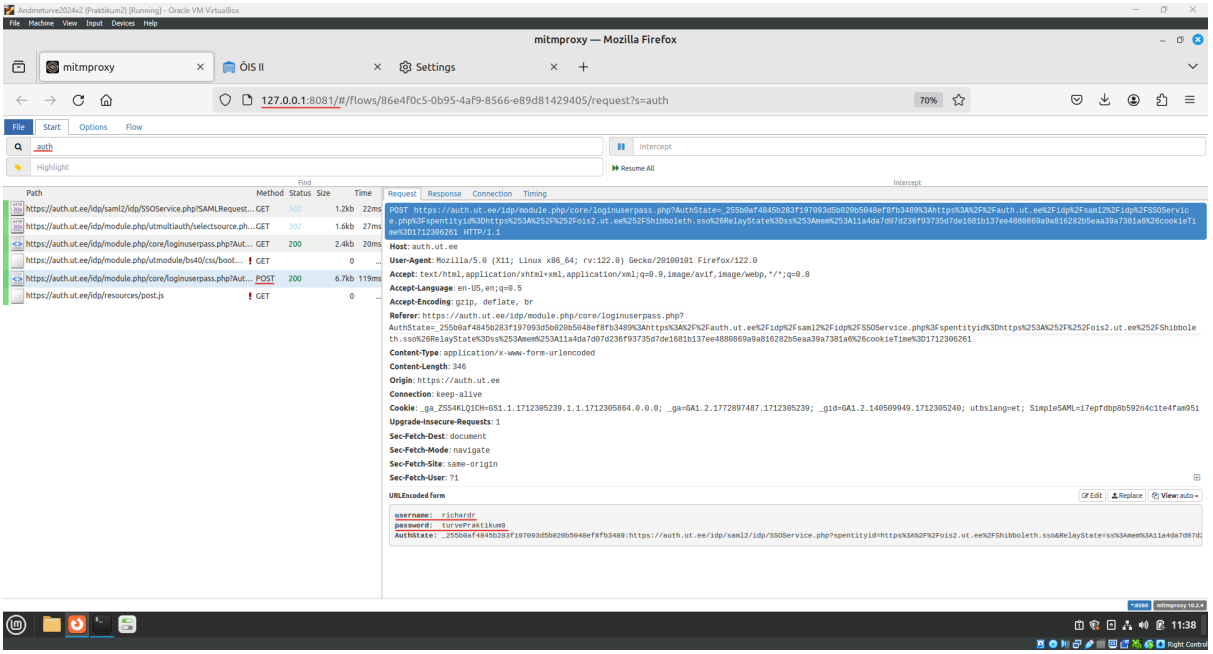


ÜL 2




root@rivik: /home/ssh-mitm/log
File Edit View Search Terminal Help
Apr 4 13:22:33 rivik sudo: pam_unix(sudo:session): session closed for user root
Apr 4 13:22:33 rivik sudo: kasutaja : PWD=/home/kasutaja ; USER=root ; COMMAND=/usr/bin/mint-refresh-cache
Apr 4 13:22:33 rivik sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Apr 4 13:22:35 rivik sudo: pam_unix(sudo:session): session closed for user root
Apr 4 13:23:45 rivik useradd[15362]: new group: name=ssh-mitm, GID=1004
Apr 4 13:23:45 rivik useradd[15362]: new user: name=ssh-mitm, UID=1004, GID=1004, home=/home/ssh-mitm, shel
l=/bin/bash, from=/dev/pts/1
Apr 4 13:24:12 rivik su: (to ssh-mitm) root on pts/1
Apr 4 13:24:12 rivik su: pam_unix(su-l:session): session opened for user ssh-mitm(uid=1004) by kasutaja(uid
=0)
Apr 4 13:24:12 rivik sshd_mitm[15426]: Server listening on 0.0.0.0 port 2222.
Apr 4 13:24:12 rivik su: pam_unix(su-l:session): session closed for user ssh-mitm
Apr 4 13:24:12 rivik sshd_mitm[15426]: Server listening on :: port 2222.
Apr 4 13:25:27 rivik sshd_mitm[15444]: INTERCEPTED PASSWORD: hostname: [193.40.5.36]; username: [richardr];
password: [] [preauth]
Apr 4 13:25:35 rivik sshd_mitm[15444]: INTERCEPTED PASSWORD: hostname: [193.40.5.36]; username: [richardr];
password: [andmeturvePraktikum8] [preauth]
Apr 4 13:25:35 rivik sshd_mitm[15444]: Accepted password for ssh-mitm from 192.168.10.88 port 50169 ssh2
Apr 4 13:27:10 rivik sshd_mitm[15448]: INTERCEPTED PASSWORD: hostname: [193.40.5.73]; username: [adalberg];
password: [122] [preauth]
Apr 4 13:27:10 rivik sshd_mitm[15448]: Accepted password for ssh-mitm from 192.168.10.88 port 50185 ssh2
Apr 4 13:27:38 rivik sshd_mitm[15453]: INTERCEPTED PASSWORD: hostname: [193.40.5.36]; username: [richardr];
password: [andmeturvePraktikum8] [preauth]
Apr 4 13:27:38 rivik sshd_mitm[15453]: Accepted password for ssh-mitm from 192.168.10.88 port 50195 ssh2
Apr 4 13:30:01 rivik CRON[15483]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Apr 4 13:30:01 rivik CRON[15483]: pam_unix(cron:session): session closed for user root
root@rivik:/home/ssh-mitm/log#

ÜL 3


mitmproxy — Mozilla Firefox
mitmproxy
ÕIS II
Settings
127.0.0.1:8081/#/flows/86e4f0c5-0b95-4af9-8566-e89d81429405/request?s=auth
File
Start
Options
Flow
Request
Response
Connection
Timing
Host: auth.ut.ee
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 346
Origin: https://auth.ut.ee
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
URLEncoded form
username: richardr
password: turvePraktikum8
11:38