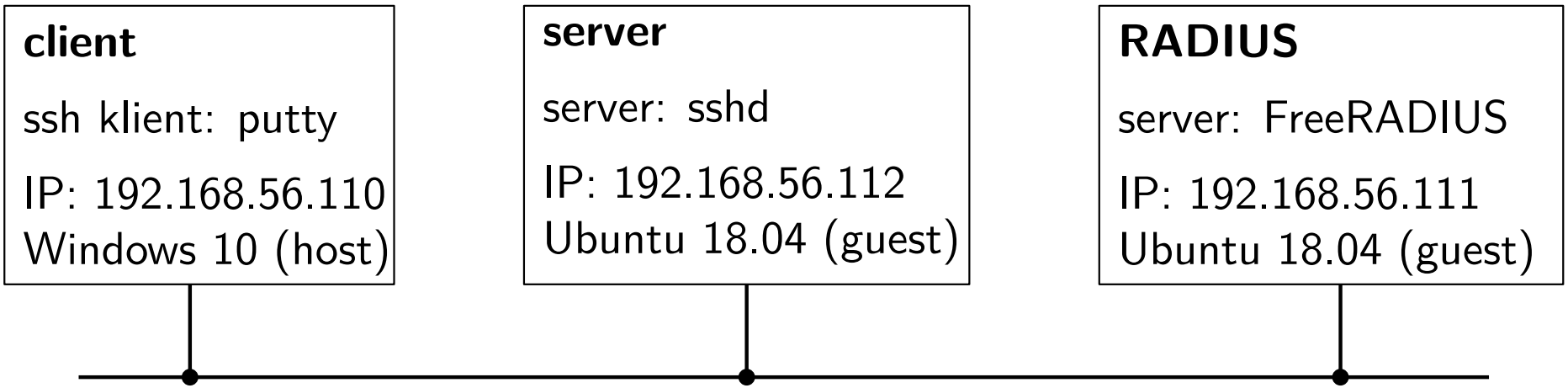
RADIUS – demo

Martin Stanek

Department of Computer Science
Comenius University
stanek@dcs.fmph.uniba.sk

Security of IT infrastructure (2018/19)

Setup



- server (fragment of the `shadow` file):

```
root:!:17991:0:99999:7:::
daemon:*:17937:0:99999:7:::
martin:$6$WjbLm3c.....................:17991:0:99999:7:::
sshd:*:17992:0:99999:7:::
euler:!:17992:0:99999:7:::
```

  ...user *euler* with locked password (account must exist locally!)

RADIUS server

- client definition (i.e. ssh server), `clients.conf`:

```
client 192.168.56.112 {
  secret = najtajnejsie
}
```

- user definition (plain text file), `users`:

```
euler Cleartext-Password := "testing"
```

SSH server

- PAM module for RADIUS required (`libpam_radius_auth`)
- add RADIUS server (`/etc/pam_radius_auth.conf`):

  ```
  192.168.56.111 najtajnejsie 2
  ```

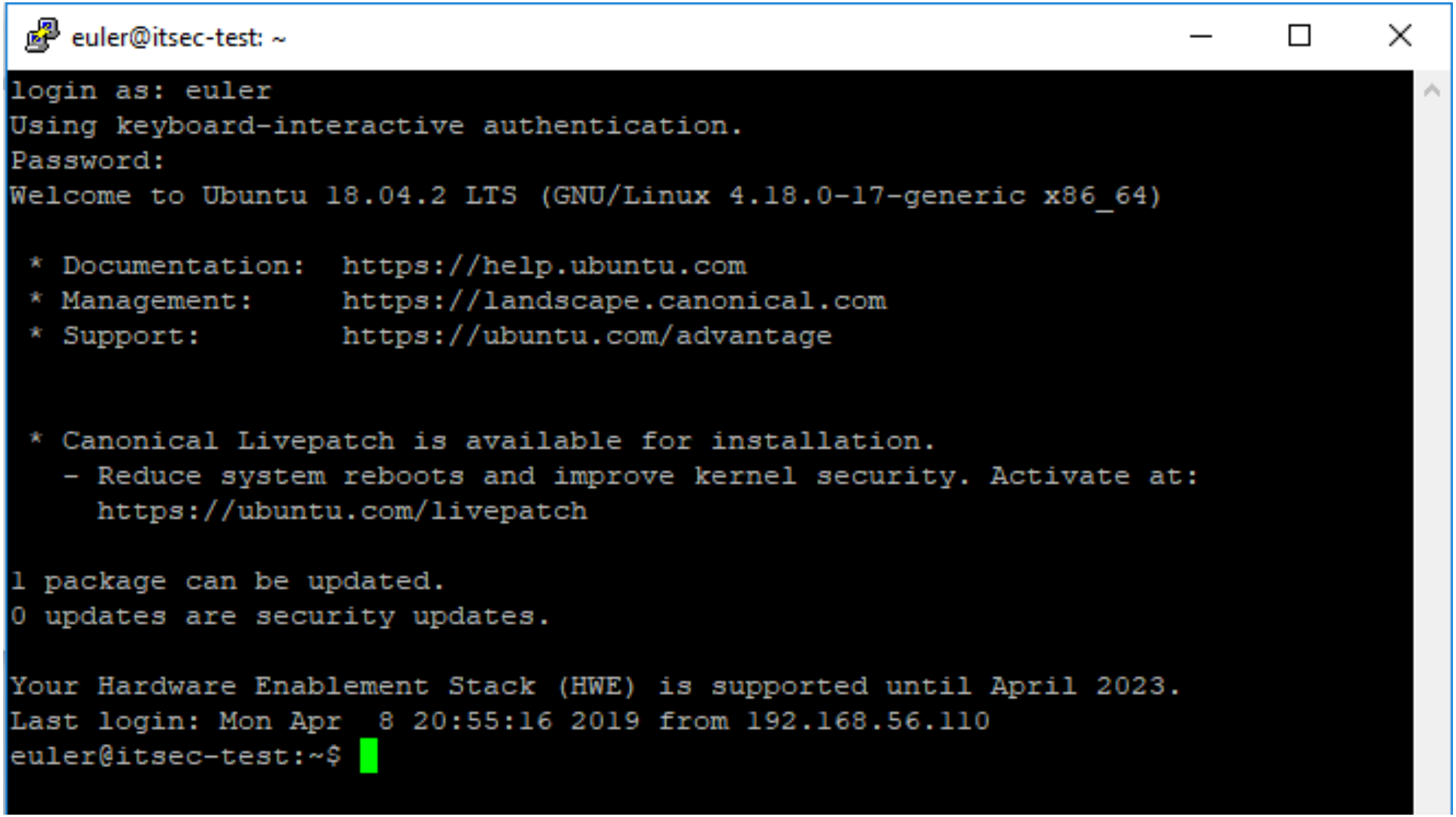
- modify PAM logic for sshd (`/etc/pam.d/sshd`):

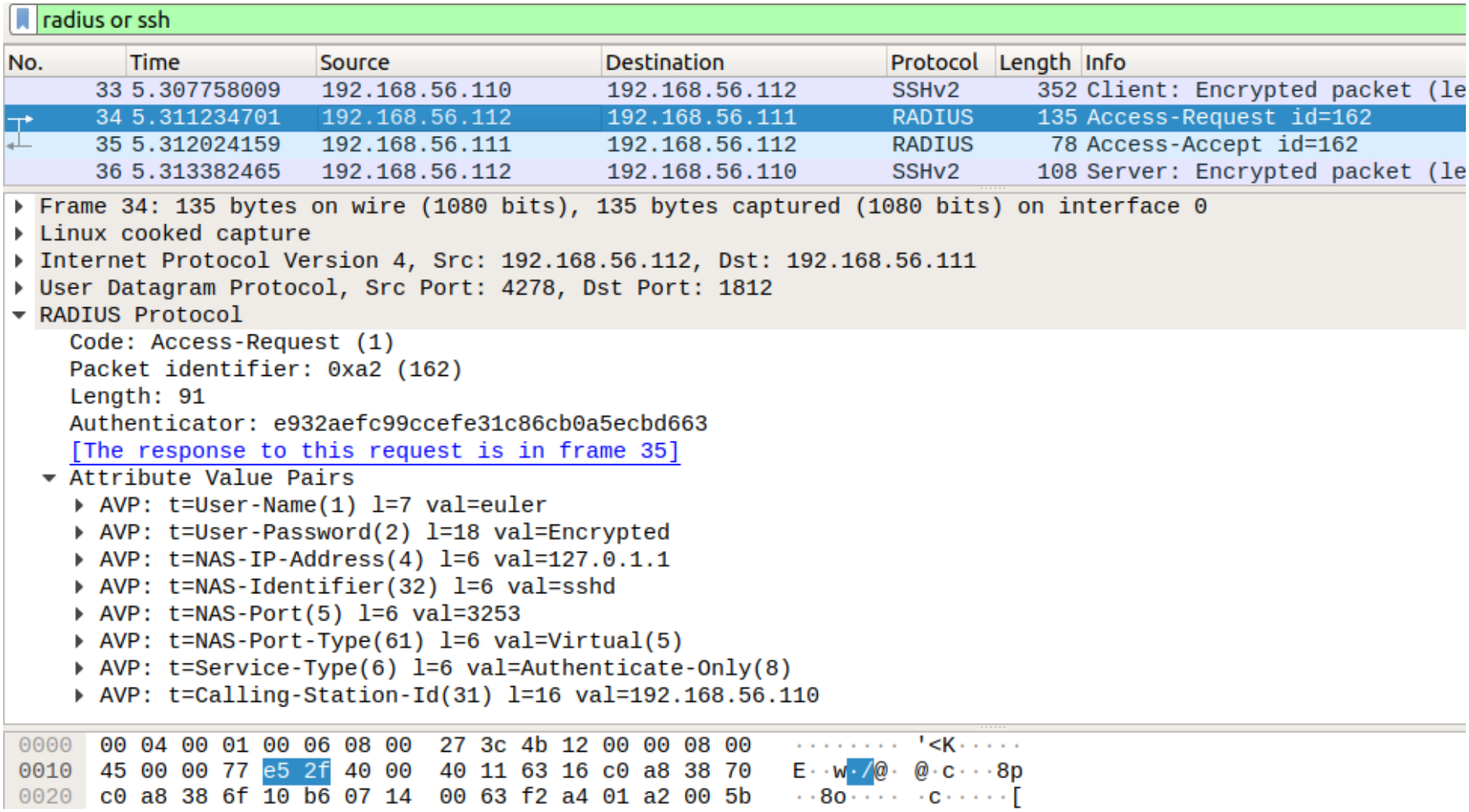
  ```
  auth sufficient pam_radius_auth.so
  ```

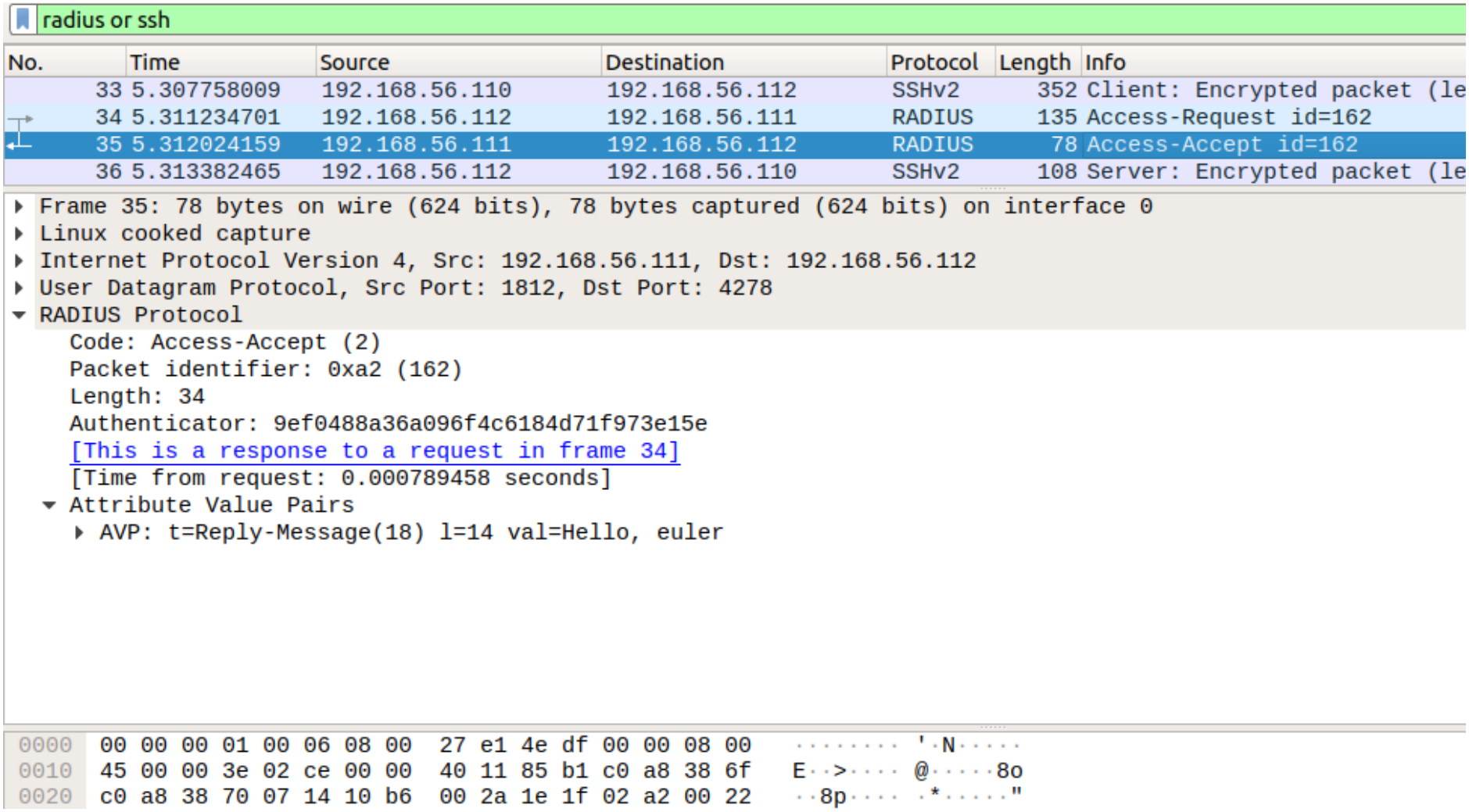
- modify `/etc/ssh/sshd_config`:

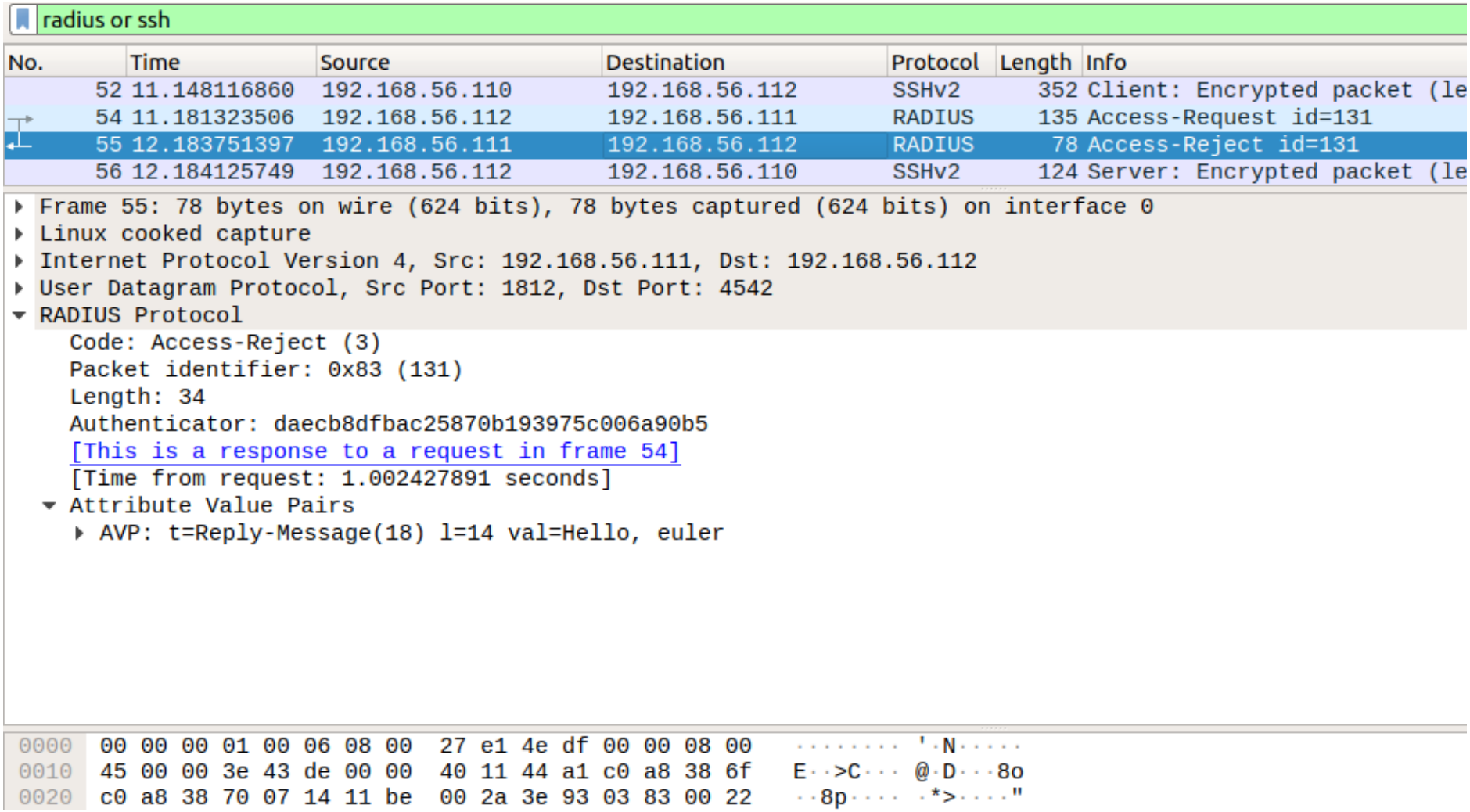
  ```
  ChallengeResponseAuthentication yes
  ```

putty


euler@itsec-test: ~
login as: euler
Using keyboard-interactive authentication.
Password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.18.0-17-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch
1 package can be updated.
0 updates are security updates.
Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Mon Apr 8 20:55:16 2019 from 192.168.56.110
euler@itsec-test:~$


radius or ssh
No. Time Source Destination Protocol Length Info
33 5.307758009 192.168.56.110 192.168.56.112 SSHv2 352 Client: Encrypted packet (le
34 5.311234701 192.168.56.112 192.168.56.111 RADIUS 135 Access-Request id=162
35 5.312024159 192.168.56.111 192.168.56.112 RADIUS 78 Access-Accept id=162
36 5.313382465 192.168.56.112 192.168.56.110 SSHv2 108 Server: Encrypted packet (le
Frame 34: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.56.112, Dst: 192.168.56.111
User Datagram Protocol, Src Port: 4278, Dst Port: 1812
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0xa2 (162)
Length: 91
Authenticator: e932aefc99ccefe31c86cb0a5ecbd663
[The response to this request is in frame 35]
Attribute Value Pairs
AVP: t=User-Name(1) l=7 val=euler
AVP: t=User-Password(2) l=18 val=Encrypted
AVP: t=NAS-IP-Address(4) l=6 val=127.0.1.1
AVP: t=NAS-Identifier(32) l=6 val=sshd
AVP: t=NAS-Port(5) l=6 val=3253
AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)
AVP: t=Service-Type(6) l=6 val=Authenticate-Only(8)
AVP: t=Calling-Station-Id(31) l=16 val=192.168.56.110
0000 00 04 00 01 00 06 08 00 27 3c 4b 12 00 00 08 00
0010 45 00 00 77 e5 2f 40 00 40 11 63 16 c0 a8 38 70
0020 c0 a8 38 6f 10 b6 07 14 00 63 f2 a4 01 a2 00 5b


radius or ssh
No. Time Source Destination Protocol Length Info
33 5.307758009 192.168.56.110 192.168.56.112 SSHv2 352 Client: Encrypted packet (le
34 5.311234701 192.168.56.112 192.168.56.111 RADIUS 135 Access-Request id=162
35 5.312024159 192.168.56.111 192.168.56.112 RADIUS 78 Access-Accept id=162
36 5.313382465 192.168.56.112 192.168.56.110 SSHv2 108 Server: Encrypted packet (le
Frame 35: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.56.111, Dst: 192.168.56.112
User Datagram Protocol, Src Port: 1812, Dst Port: 4278
RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0xa2 (162)
Length: 34
Authenticator: 9ef0488a36a096f4c6184d71f973e15e
[This is a response to a request in frame 34]
[Time from request: 0.000789458 seconds]
Attribute Value Pairs
AVP: t=Reply-Message(18) l=14 val=Hello, euler
0000 00 00 00 01 00 06 08 00 27 e1 4e df 00 00 08 00
0010 45 00 00 3e 02 ce 00 00 40 11 85 b1 c0 a8 38 6f
0020 c0 a8 38 70 07 14 10 b6 00 2a 1e 1f 02 a2 00 22


radius or ssh
No. Time Source Destination Protocol Length Info
52 11.148116860 192.168.56.110 192.168.56.112 SSHv2 352 Client: Encrypted packet (le
54 11.181323506 192.168.56.112 192.168.56.111 RADIUS 135 Access-Request id=131
55 12.183751397 192.168.56.111 192.168.56.112 RADIUS 78 Access-Reject id=131
56 12.184125749 192.168.56.112 192.168.56.110 SSHv2 124 Server: Encrypted packet (le
Frame 55: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.56.111, Dst: 192.168.56.112
User Datagram Protocol, Src Port: 1812, Dst Port: 4542
RADIUS Protocol
Code: Access-Reject (3)
Packet identifier: 0x83 (131)
Length: 34
Authenticator: daecb8dfbac25870b193975c006a90b5
[This is a response to a request in frame 54]
[Time from request: 1.002427891 seconds]
Attribute Value Pairs
AVP: t=Reply-Message(18) l=14 val=Hello, euler
0000 00 00 00 01 00 06 08 00 27 e1 4e df 00 00 08 00
0010 45 00 00 3e 43 de 00 00 40 11 44 a1 c0 a8 38 6f
0020 c0 a8 38 70 07 14 11 be 00 2a 3e 93 03 83 00 22