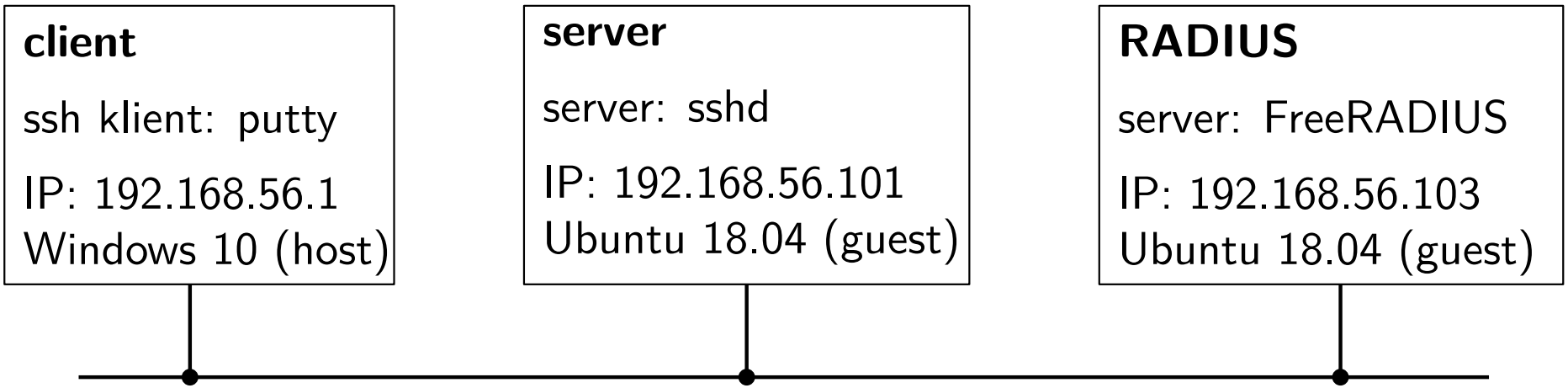
RADIUS – demo

Martin Stanek

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

Security of IT infrastructure (2019/20)

Setup



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

```
root:!:18314:0:99999:7:::
daemon:*:18113:0:99999:7:::
martin:$6$fcKNLOO.....................:18314:0:99999:7:::
sshd:*:18364:0:99999:7:::
euler:!:0:0:99999:7:::
```

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

RADIUS server

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

```
client ssh-server {
        ipaddr    = 192.168.56.101
        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`):

  ```
  192.168.56.103 najtajnejsie 2
  ```

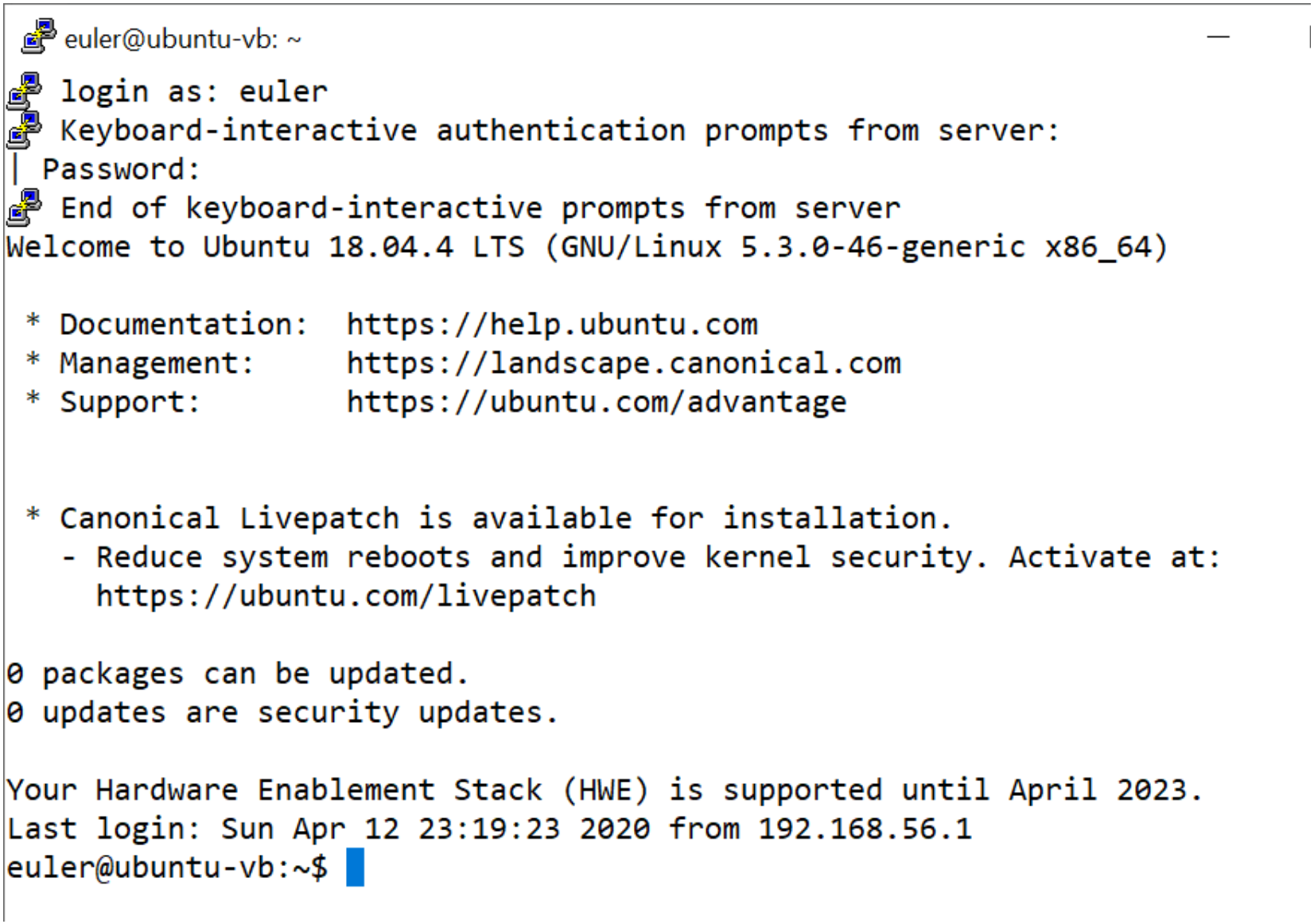
- modify PAM logic for sshd (`/etc/pam.d/sshd`):

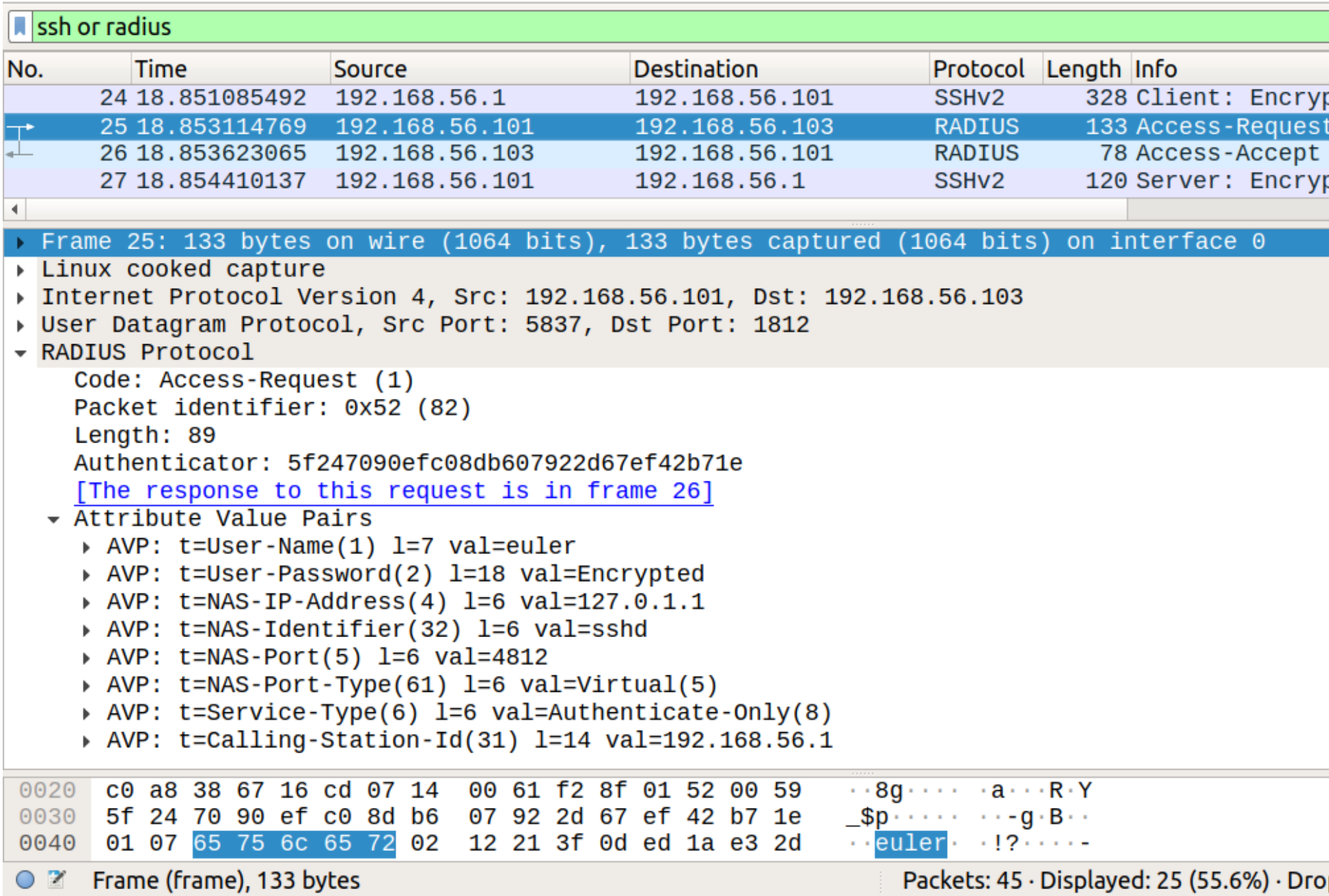
  ```
  auth sufficient pam_radius_auth.so
  ```

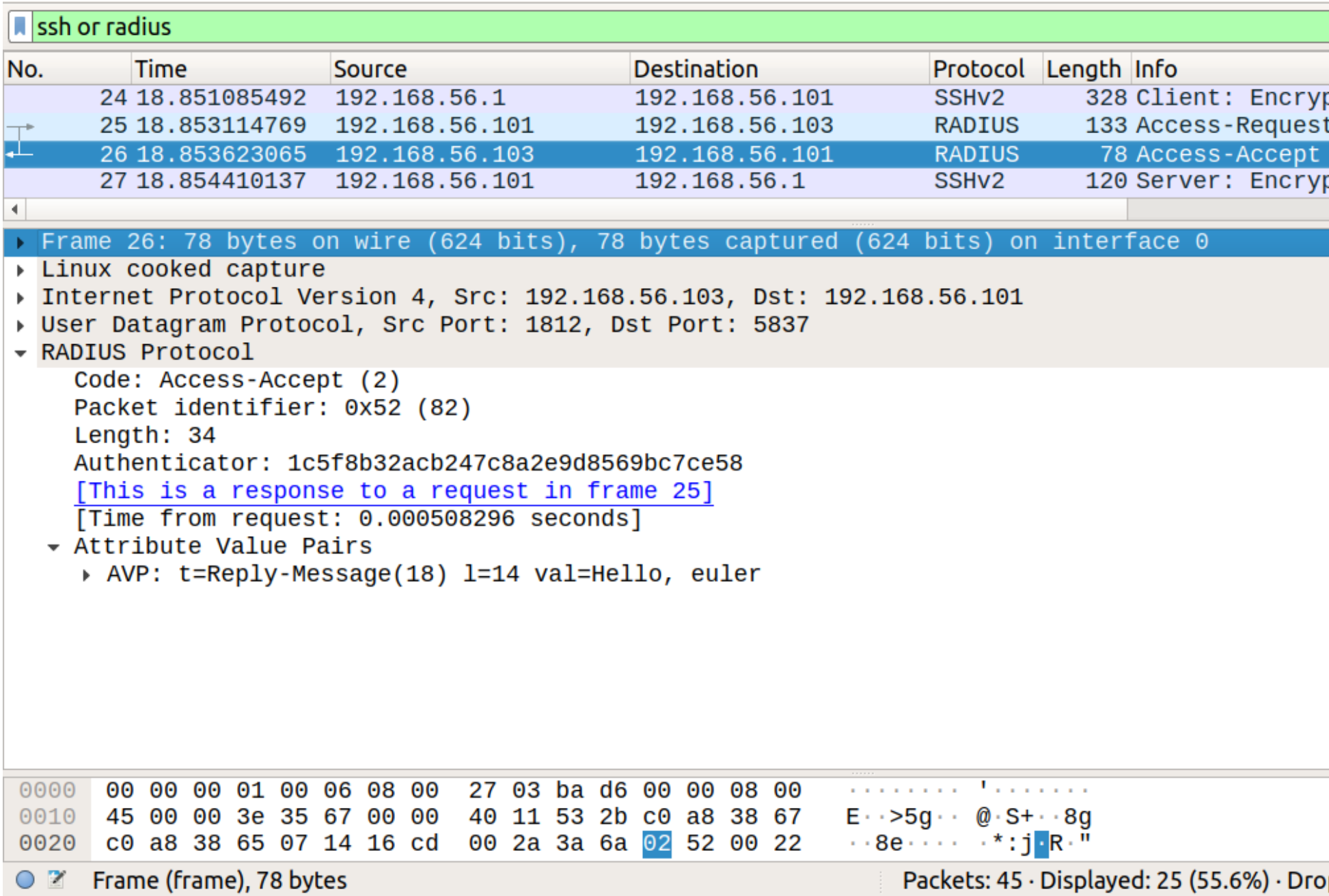
- modify `/etc/ssh/sshd_config`:

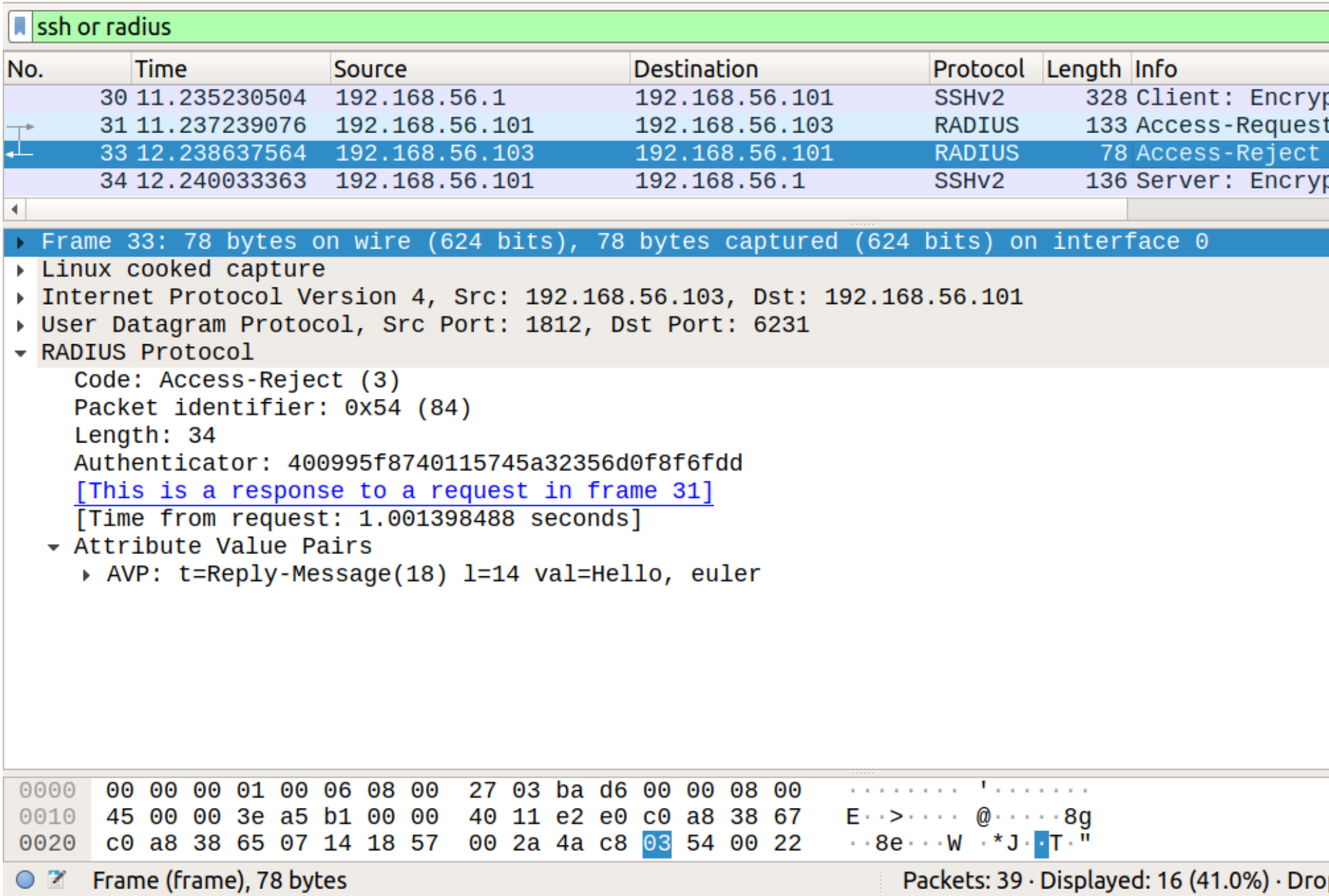
  ```
  ChallengeResponseAuthentication yes
  ```

putty


euler@ubuntu-vb: ~
login as: euler
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-46-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
0 packages can be updated.
0 updates are security updates.
Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Sun Apr 12 23:19:23 2020 from 192.168.56.1
euler@ubuntu-vb:~$


ssh or radius
No. Time Source Destination Protocol Length Info
24 18.851085492 192.168.56.1 192.168.56.101 SSHv2 328 Client: Encryp
25 18.853114769 192.168.56.101 192.168.56.103 RADIUS 133 Access-Request
26 18.853623065 192.168.56.103 192.168.56.101 RADIUS 78 Access-Accept
27 18.854410137 192.168.56.101 192.168.56.1 SSHv2 120 Server: Encryp
Frame 25: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.103
User Datagram Protocol, Src Port: 5837, Dst Port: 1812
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0x52 (82)
Length: 89
Authenticator: 5f247090efc08db607922d67ef42b71e
[The response to this request is in frame 26]
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=4812
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=14 val=192.168.56.1
0020 c0 a8 38 67 16 cd 07 14 00 61 f2 8f 01 52 00 59
0030 5f 24 70 90 ef c0 8d b6 07 92 2d 67 ef 42 b7 1e
0040 01 07 65 75 6c 65 72 02 12 21 3f 0d ed 1a e3 2d
Frame (frame), 133 bytes
Packets: 45 · Displayed: 25 (55.6%) · Dro


ssh or radius
No. Time Source Destination Protocol Length Info
24 18.851085492 192.168.56.1 192.168.56.101 SSHv2 328 Client: Encryp
25 18.853114769 192.168.56.101 192.168.56.103 RADIUS 133 Access-Request
26 18.853623065 192.168.56.103 192.168.56.101 RADIUS 78 Access-Accept
27 18.854410137 192.168.56.101 192.168.56.1 SSHv2 120 Server: Encryp
Frame 26: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.101
User Datagram Protocol, Src Port: 1812, Dst Port: 5837
RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0x52 (82)
Length: 34
Authenticator: 1c5f8b32acb247c8a2e9d8569bc7ce58
[This is a response to a request in frame 25]
[Time from request: 0.000508296 seconds]
Attribute Value Pairs
AVP: t=Reply-Message(18) l=14 val=Hello, euler
0000 00 00 00 01 00 06 08 00 27 03 ba d6 00 00 08 00
0010 45 00 00 3e 35 67 00 00 40 11 53 2b c0 a8 38 67
0020 c0 a8 38 65 07 14 16 cd 00 2a 3a 6a 02 52 00 22
Frame (frame), 78 bytes
Packets: 45 · Displayed: 25 (55.6%) · Dro


ssh or radius
No. Time Source Destination Protocol Length Info
30 11.235230504 192.168.56.1 192.168.56.101 SSHv2 328 Client: Encryp
31 11.237239076 192.168.56.101 192.168.56.103 RADIUS 133 Access-Request
33 12.238637564 192.168.56.103 192.168.56.101 RADIUS 78 Access-Reject
34 12.240033363 192.168.56.101 192.168.56.1 SSHv2 136 Server: Encryp
Frame 33: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.101
User Datagram Protocol, Src Port: 1812, Dst Port: 6231
RADIUS Protocol
Code: Access-Reject (3)
Packet identifier: 0x54 (84)
Length: 34
Authenticator: 400995f8740115745a32356d0f8f6fdd
[This is a response to a request in frame 31]
[Time from request: 1.001398488 seconds]
Attribute Value Pairs
AVP: t=Reply-Message(18) l=14 val=Hello, euler
0000 00 00 00 01 00 06 08 00 27 03 ba d6 00 00 08 00
0010 45 00 00 3e a5 b1 00 00 40 11 e2 e0 c0 a8 38 67
0020 c0 a8 38 65 07 14 18 57 00 2a 4a c8 03 54 00 22
Frame (frame), 78 bytes
Packets: 39 · Displayed: 16 (41.0%) · Dro