



Agentúra

Ministerstva školstva, vedy, výskumu a športu SR
pre štrukturálne fondy EÚ



UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

PRÍPRAVA ŠTÚDIA MATEMATIKY A INFORMATIKY NA FMFI UK V
ANGLICKOM JAZYKU

ITMS: 26140230008

DOPYTOVO – ORIENTOVANÝ PROJEKT

Moderné vzdelávanie pre vedomostnú spoločnosť/Projekt je
spolufinancovaný zo zdrojov EÚ

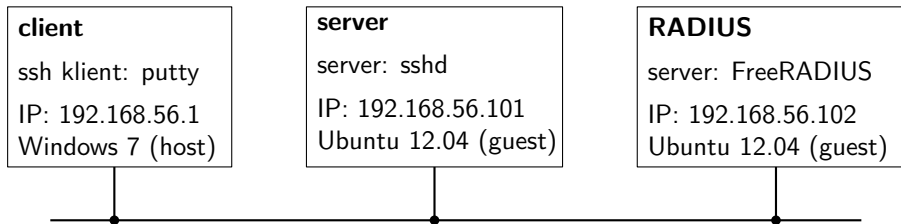
RADIUS – demo

Martin Stanek

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

Security of IT infrastructure (2014/15)

Setup



- ▶ server (fragment of shadows file):

```
root:!:15411:0:99999:7:::
```

```
daemon*:15259:0:99999:7:::
```

```
martin:$6$jKljYyA.....:15411:0:99999:7:::
```

```
sshd*:15411:0:99999:7:::
```

```
euler:!:15412:0:99999:7:::
```

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

RADIUS server

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

```
client test-sshd-server {  
    ipaddr = 192.168.56.101  
    secret = najtajniejsie  
}
```

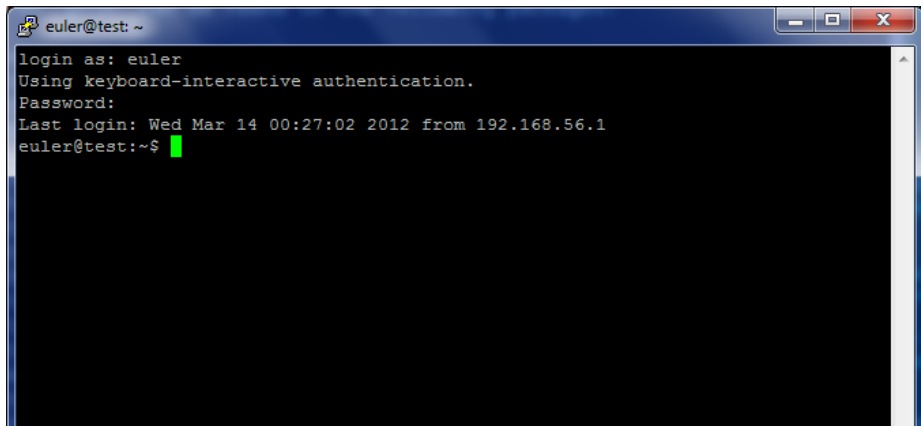
- ▶ user definition (plain text file), `users`:

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

SSH server

- ▶ PAM module for RADIUS required (`libpam_radius_auth`)
- ▶ add RADIUS server (`/etc/pam_radius_auth.conf`):
`192.168.56.102 najtajniejsie 1`
- ▶ modify PAM logic for `sshd` (`/etc/pam.d/sshd`):
`auth sufficient pam_radius_auth.so`
- ▶ modify `/etc/ssh/sshd_config`:
`ChallengeResponseAuthentication yes`

putty



The image shows a PuTTY terminal window with a blue title bar. The title bar contains a small icon on the left and three window control buttons (minimize, maximize, close) on the right. The text in the title bar is "euler@test: ~". The terminal area has a black background with white text. The text displayed is as follows:

```
login as: euler
Using keyboard-interactive authentication.
Password:
Last login: Wed Mar 14 00:27:02 2012 from 192.168.56.1
euler@test:~$
```

A green cursor is visible at the end of the prompt "euler@test:~\$".

Filter: **radius** Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
54	13.474325	127.0.0.1	127.0.0.1	RADIUS	133	Access-Request(1) (id=244, l=89)
55	13.474356	127.0.0.1	127.0.0.1	ICMP	161	Destination unreachable (Port unreachable)
58	14.480326	192.168.56.101	192.168.56.102	RADIUS	133	Access-Request(1) (id=9, l=89)
59	14.481806	192.168.56.102	192.168.56.101	RADIUS	64	Access-Accept(2) (id=9, l=20)

▶ Frame 58: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
 ▶ Linux cooked capture
 ▶ Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.102 (192.168.56.102)
 ▶ User Datagram Protocol, Src Port: mbg-ctrl (3569), Dst Port: radius (1812)
 ▼ Radius Protocol
 Code: Access-Request (1)
 Packet identifier: 0x9 (9)
 Length: 89
 Authenticator: c08de524a5a05ea3ffe0680e9e76fe28
 [\[The response to this request is in frame 59\]](#)
 ▼ Attribute Value Pairs
 ▶ AVP: l=7 t=User-Name(1): euler
 ▼ AVP: l=18 t=User-Password(2): Encrypted
 User-Password: {(\202\033m\034\hk\2309-D1
 ▶ AVP: l=6 t=NAS-IP-Address(4): 127.0.1.1
 ▶ AVP: l=6 t=NAS-Identifier(32): sshd
 ▶ AVP: l=6 t=NAS-Port(5): 2544
 ▶ AVP: l=6 t=NAS-Port-Type(61): Virtual(5)
 ▶ AVP: l=6 t=Service-Type(6): Authenticate-Only(8)
 ▶ AVP: l=14 t=Calling-Station-Id(31): 192.168.56.1

Filter:	radius			▼	Expression...	Clear	Apply
No.	Time	Source	Destination	Protocol	Length	Info	
54	13.474325	127.0.0.1	127.0.0.1	RADIUS	133	Access-Request(1) (id=244, l=89)	
55	13.474356	127.0.0.1	127.0.0.1	ICMP	161	Destination unreachable (Port unreachable)	
58	14.480326	192.168.56.101	192.168.56.102	RADIUS	133	Access-Request(1) (id=9, l=89)	
59	14.481806	192.168.56.102	192.168.56.101	RADIUS	64	Access-Accept(2) (id=9, l=20)	

- ▶ Frame 59: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
- ▶ Linux cooked capture
- ▶ Internet Protocol Version 4, Src: 192.168.56.102 (192.168.56.102), Dst: 192.168.56.101 (192.168.56.101)
- ▶ User Datagram Protocol, Src Port: radius (1812), Dst Port: mbg-ctrl (3569)
- ▼ Radius Protocol
 - Code: Access-Accept (2)
 - Packet identifier: 0x9 (9)
 - Length: 20
 - Authenticator: 35f64e74072b660298c631b78daebd1f
 - [\[This is a response to a request in frame 58\]](#)
 - [Time from request: 0.001480000 seconds]

