Compact Course in Networking and SSH
Content

Networking
IP address, DNS protocols, ports, ...

SSH
basic tools & usage, public keys, tunnels

"Introduction to SSH and Networking" | M. Ohlerich
Networking

IP Addresses and Domain Names

10.20.30.4
10.20.30.3
10.20.30.5
10.20.30.2
10.20.30.1
10.20.30.6
dc.mydomain.de
dns.mydomain.de
ping
nslookup
traceroute
<table>
<thead>
<tr>
<th>OSI Model, Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Application</strong></td>
</tr>
<tr>
<td><strong>Presentation</strong></td>
</tr>
<tr>
<td><strong>Session</strong></td>
</tr>
<tr>
<td><strong>Segments</strong></td>
</tr>
<tr>
<td><strong>Transport</strong></td>
</tr>
<tr>
<td><strong>Packets</strong></td>
</tr>
<tr>
<td><strong>Network</strong></td>
</tr>
<tr>
<td><strong>Frames</strong></td>
</tr>
<tr>
<td><strong>Data Link</strong></td>
</tr>
<tr>
<td><strong>Bits</strong></td>
</tr>
<tr>
<td><strong>Physical</strong></td>
</tr>
</tbody>
</table>

HTTP, HTTPS, FTP, SMTP, LDAP, DNS, SSH, TSL/SSL, NTP, ...
TCP, UDP, ...
IP, IPsec, ...
Ethernet, ...
1000 BASE-T, ...
Networking
Ports, Gateways, Firewalls

Ports

- **SSH Server**
  - 22 : SSH

- **Web-Server**
  - 80 : HTTP

- **VNC-Server**
  - 5901 : VNC

ports < 1024 privileged
ports >= 1024 user

```
netstat
```

10.20.30.3
10.20.30.1
129.187.30.254
129.187.30.2

"Introduction to SSH and Networking" | M. Ohlerich
## SSH Tools Overview

### SSH Tools
- `ssh`
- `scp`
- `ssh-keygen`
- `ssh-copy-id`
- `ssh-agent`
- `ssh-add`

### PuTTY Tools
- PuTTY (plink)
- `pscp`
- PuTTYgen
- `pageant`

---

https://www.ssh.com/ssh
https://www.ssh.com/ssh/putty/putty-manuals/0.68/index.html

"Introduction to SSH and Networking" | M. Ohlerich
SSH Session

SSH Client → SSH Server (Port 22)

- `ssh -l userB hostB`
- `ssh userB@hostB`
- `man ssh`
- `ssh -C ... (Compression)`
- `ssh -v ... (verbose; -vvv)`
SSH Session with Graphics

```
userA
hostA

SSH Client
X Server

SSH Server
X Client

userB
hostB

tunnel

ssh -X userB@hostB

ssh -Y userB@hostB
```
SSH Session via several Hosts

```
ssh userB@hostB -t ssh userC@hostC
ssh -J userB@hostB userC@hostC
ssh userB@hostB ls (remote command)
```
SSH
Data/File Exchange via SSH

scp file userB@hostB:
scp userB@hostB:file .
scp -r folder userB@hostB:

sshfs

https://portableapps.com/apps/internet/winscp_portable
https://portableapps.com/de/apps/internet/filezilla_portable
SSH

Public Key Authentication

**symmetric**

```
TXT
```

**asymmetric**

```
TXT
```

**public key**

**private key**

"Introduction to SSH and Networking" | M. Ohlerich
RSA - Asymmetric Encryption

Try to decompose into its prime factors: $176711573$

RSA by Example:

\[ n = 176711573, \quad k = 72097, \quad l = 45393253 \]

Encryption: Message $m < n$  
\[ m = 3213213 \]

\[ c = m^k \mod n \]
\[ c = 100332255 \]

Decryption:
\[ m = c^l \mod n \]
SSH

Public Key Authentication

Certification

Encryption
SSH
Public Key Authentication

```
.userA
hostA

.ssh/id_rsa
.ssh/id_rsa.pub
.ssh/known_hosts

ssh-keygen -t rsa
ssh-copy-id userB@hostB
eval "(ssh-agend -s)"
ssh-add
ssh-userB@hostB
```

```
.userB
hostB

.ssh/authorized_keys

https://www.lrz.de/services/compute/ssh/
```

Key Management:

```
ssh-add -l
ssh-add -d <key>
ssh-add -D
```
SSH Tunnel

**external network**  
**firewall**  
*(only port 22 open)*  
**internal network**

"Introduction to SSH and Networking" | M. Ohlerich
SSH Tunnel

http://localhost:8080

```
ssh -L 8080:localhost:80 userB@hostB
```
SSH Tunnel

ssh -L 8080:hostC:80 userB@hostB

http://localhost:8080
SSH

Convenience: ~/.ssh/config

```
ForwardX11Trusted no # no X forwarding
ForwardAgent yes # public key forwarding
User userB # default user name
Host hostB # alias
   HostName hostC.somewhere.com
   ProxyJump userB@hostB.somewhere.com
   User userC
Host hostB
   HostName hostB.somewhere.com
```
SSH

Further Reading ...

"Introduction to SSH and Networking" | M. Ohlerich
Course Evaluation

Please visit https://survey.lrz.de/index.php/791275 and rate this course.

Your feedback is highly appreciated!
Thank you!