



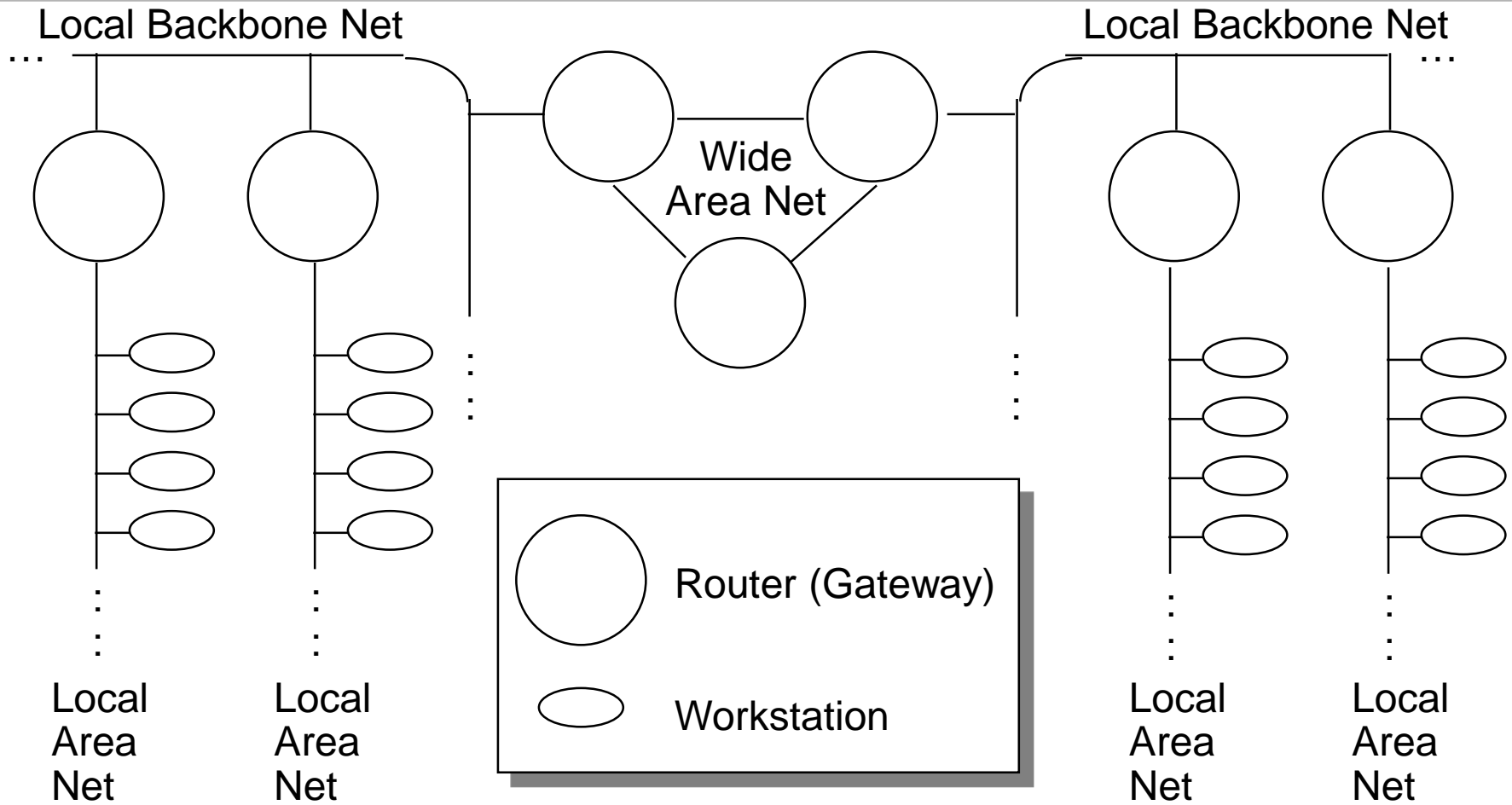
Resultate des 1. Assessments (10 min)

- Kurze Wiederholung der Aufgaben
- Typische Lösungen / Lösungselemente
- Gesamtauswertung der Ergebnisse
- Bekanntgabe der einzelnen Resultate

Lektion 7: Netzwerke und Informationssicherheit im Betriebssystem



- Grundlagen der Internet Protocol Suite
- Netzwerkschnittstellen im Betriebssystem
- Betrachtung und Konfiguration der Netzwerkschnittstelle



Leffer et al., The Design and Implementation of the 4.3BSD UNIX Operating System, Figure 11.5

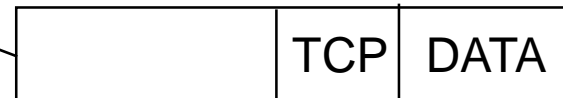
Schichtenarchitektur des Internet

Application Layer

socket

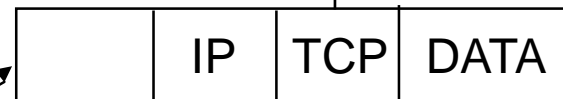


Transport Layer (TCP, UDP)



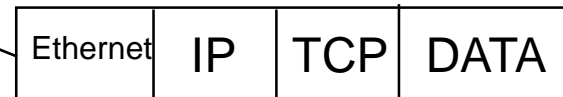
Network Layer (IP, ICMP, ARP)

protocol
input queue



software interrupt

Network Interface Layer



device
interrupt

Ethernet

Leffer et al., The Design and Implementation
of the 4.3BSD UNIX Operating System, Figure 11.1

- Name: *Identifikation* in einem Kontext, z.B "Zürich"
 - Adresse: *Ort* in einem Kontext, z.B "PLZ 8000"
 - Route: *Pfad* zum adressierten Objekt, z.B. Landkarte
-
- Name: DNS-Eintrag und "Resolving": www.fhnw.ch
 - Adresse: 32-Bit IP-Adresse, Subnetzmaske
 - Klasse A: 1 - 126
 - Klasse B: 128.1 bis 191.254
 - Klasse C: 192.1.1 bis 233.254.254
 - Route: Weiterleitungsinformation in Routern

Vergabeautorität und Subnetze

- Regional Internet Registries (RIRs)

- AfriNIC: Afrika
- APNIC: Asia/Pacific
- ARIN: Amerika
- LACNIC: Latin America / Caribbean
- RIPE NCC: Europa, naher Osten

0 1 2 3 4 8 16 24 31

Klasse B	10	NetID	HostID
----------	----	-------	--------

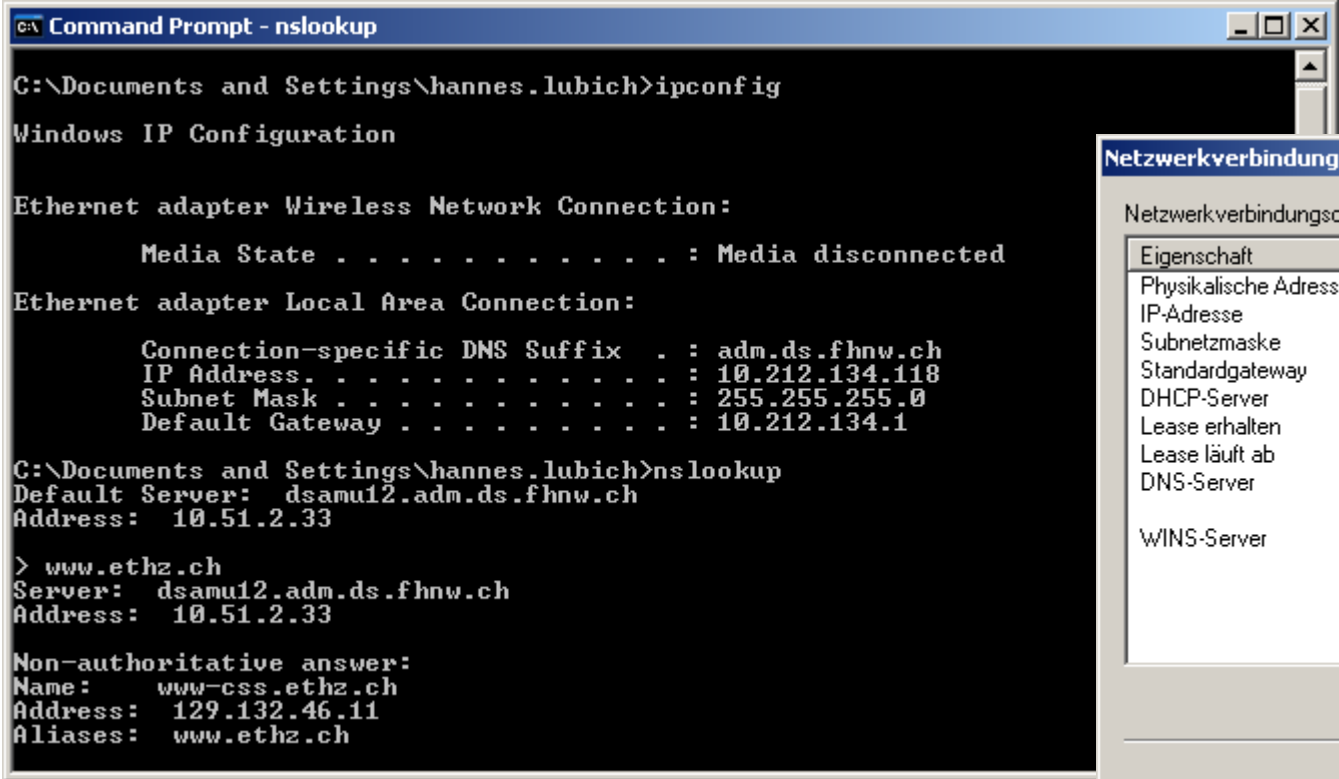
Subnetz	11	NetID	Subnet	HostID
---------	----	-------	--------	--------

16 bits n bits 16-n bits
 ← Subnet Maske →

Beispiel: Net 129.132.0.0, Mask 255.255.255.192 = 10 bit Subnet

Abbildung auf LAN-Adressen (Ethernet)

- Ethernet: standardisiertes LAN-Protokoll.
- Adressierung: 48 Bit, notiert in hexadezimaler Schreibweise, getrennt durch einen Doppelpunkt.
- Vordere Hälfte der Adresse kennzeichnet den Hersteller, z.B. 8:0:20:x:x:x = Sun Microsystems / Oracle.
- Hintere Hälfte wird vom Hersteller autonom verwaltet.
- Gemeinsam genutztes Übermittlungsmedium ohne Synchronisation, aber mit Detektion von Kollisionen beim Senden (CSMA/CD).
- Gesendete Datenpakete (Frames) werden von allen Stationen am LAN gesehen, die angesprochene Station nimmt den Frame vom Netz.
- Broadcast (Senden an alle Stationen im LAN) für Adressabbildung Ethernet/Internet (ARP-Protokoll).



```

C:\ Command Prompt - nslookup

C:\Documents and Settings\hannes.lubich>ipconfig

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected

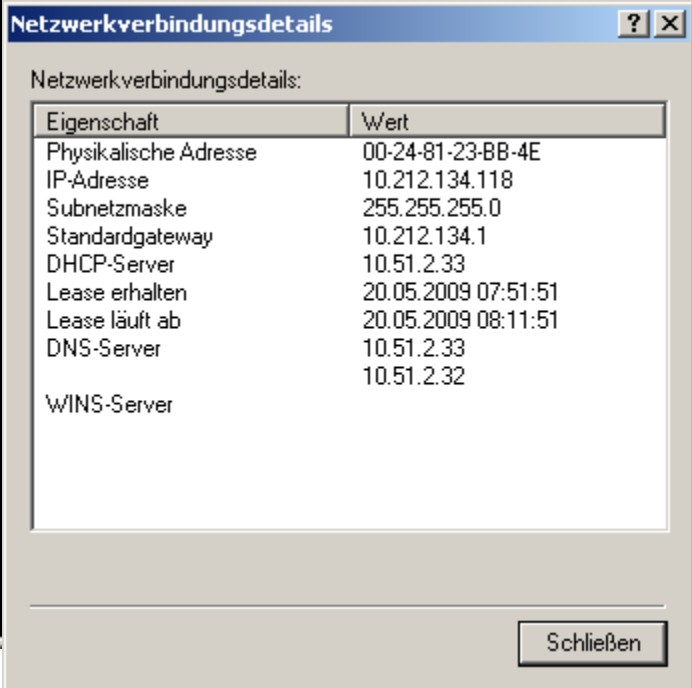
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : adm.ds.fhnw.ch
    IP Address. . . . . : 10.212.134.118
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.212.134.1

C:\Documents and Settings\hannes.lubich>nslookup
Default Server:  dsamu12.adm.ds.fhnw.ch
Address:  10.51.2.33

> www.ethz.ch
Server:  dsamu12.adm.ds.fhnw.ch
Address:  10.51.2.33

Non-authoritative answer:
Name:    www-css.ethz.ch
Address: 129.132.46.11
Aliases: www.ethz.ch
        
```



Netzwerkverbindungsdetails

Eigenschaft	Wert
Physikalische Adresse	00-24-81-23-BB-4E
IP-Adresse	10.212.134.118
Subnetzmaske	255.255.255.0
Standardgateway	10.212.134.1
DHCP-Server	10.51.2.33
Lease erhalten	20.05.2009 07:51:51
Lease läuft ab	20.05.2009 08:11:51
DNS-Server	10.51.2.33
WINS-Server	10.51.2.32

Schließen

DNS – mehr als IP-Adressen

Dns Reply

Query: Type: Class:

Result:

Field	Type	Name	Data
ans	CNAME	mail.ee.ethz.ch	tardis.ee.ethz.ch
ans	A	tardis.ee.ethz.ch	129.132.2.217
auth	NS	ethz.ch	ns2.ethz.ch
auth	NS	ethz.ch	scsnms.switch.ch
auth	NS	ethz.ch	ns1.ethz.ch
addt	A	ns1.ethz.ch	129.132.98.8
addt	A	ns2.ethz.ch	129.132.250.8
addt	A	scsnms.switch.ch	130.59.1.30
addt	A	scsnms.switch.ch	130.59.10.30
addt	Undef...	scsnms.switch.ch	

Close Print

Dns Reply

Query: Type: Class:

Result:

Field	Type	Name	Data
ans	CNAME	www.ethz.ch	www-css.ethz.ch

Dns Reply

Query: Type: Class:

Result:

Field	Type	Name	Data
auth	SOA	ch	domreg.nic.ch helpdesk.nic.ch 2009052008 3600 900 2592000 892

Close Print

Betrachtung und Konfiguration der Netzwerkschnittstelle I

- ifconfig
- netstat
- ping
- traceroute

```

Datei Bearbeiten Ansicht Terminal Hilfe
lubich@ubuntu:~$ ifconfig --help
Aufruf:
ifconfig [-a] [-v] [-s] <interface> [[<AF>] <adresse>]
[add <Adresse>[/<Präfixlänge>]]
[del <Adresse>[/<Präfixlänge>]]
[[-]broadcast [<Adresse>]] [[-]pointopoint [<Adresse>]]
[netmask <Adresse>] [dstaddr <Adresse>] [tunnel <Adresse>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <Adresse>] [metric <NN>] [mtu <NN>]
[[-]trailers] [[-]arp] [[-]allmulti]
[multicast] [[-]promisc]
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <Typ>]
[txqueuelen <Länge>]
[[-]dynamic]
[up|down] ...

<HW>=Hardwaretyp.
Liste möglicher Hardwaretypen:
loop (Lokale Schleife) slip (Serielle IP) cslip (Serielle VJ-IP)
slip6 (6-bit Serielle IP) cslip6 (VJ 6-bit Serielle IP) adaptive (Adaptive Serielle IP)
strip (Metricom Starmode IP) ash (Ash) ether (Ethernet)
tr (16/4 Mb/s Token-Ring) tr (16/4 Mb/s Token-Ring (neu)) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
ppp (Punkt-zu-Punkt-Verbindung) hdlc ((Cisco)-HDLC) lapb (LAPB)
arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
sit (IPv6-nach-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
irda (IrLAP) ec (Econet) x25 (Generisches X.25)
eui64 (Generisches EUI-64)
<AF>=Adressfamilie. Standardwert: inet
List der möglichen Adressfamilien:
unix (UNIX-Domain) inet (DARPA-Internet) inet6 (IPv6)
ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE)
ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet)
ash (Ash) x25 (CCITT X.25)
lubich@ubuntu:~$

```

```

Datei Bearbeiten Ansicht Terminal Hilfe

lubich@ubuntu:~$ ifconfig -a
eth0      Link encap:Ethernet  Hardware Adresse 00:24:81:23:bb:4e
          inet Adresse:10.212.134.118  Bcast:10.212.134.255  Maske:255.255.255.0
          inet6-Adresse: fe80::224:81ff:fe23:bb4e/64  Gültigkeitsbereich:Verbindung
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metrik:1
          RX packets:1889 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1481 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:100
          RX bytes:1983696 (1.9 MB)  TX bytes:127454 (127.4 KB)
          Speicher:d8400000-d8420000

lo        Link encap:Lokale Schleife
          inet Adresse:127.0.0.1  Maske:255.0.0.0
          inet6-Adresse: ::1/128  Gültigkeitsbereich:Maschine
          UP LOOPBACK RUNNING  MTU:16436  Metrik:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:0
          RX bytes:240 (240.0 B)  TX bytes:240 (240.0 B)

pan0      Link encap:Ethernet  Hardware Adresse 8a:8a:e2:1c:68:47
          BROADCAST MULTICAST  MTU:1500  Metrik:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet  Hardware Adresse 00:21:6a:10:d0:4c
          UP BROADCAST MULTICAST  MTU:1500  Metrik:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

wmaster0  Link encap:UNSPEC  Hardware Adresse 00-21-6A-10-D0-4C-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metrik:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lubich@ubuntu:~$
lubich@ubuntu:~$
lubich@ubuntu:~$
```

ifconfig

```

Datei Bearbeiten Ansicht Terminal Hilfe
lubich@ubuntu:~$ netstat --help
Benutzung: netstat [-veenNcCF] [<Af>] -r
               netstat {-V|--version|-h|--help}
               netstat [-vnNcaeol] [<Socket> ...]
               netstat { [-veenNac] -i | [-cnNe] -M | -s }

    -r, --route           Routentabelle anzeigen
    -i, --interfaces      Schnittstellentabelle auflisten
    -g, --groups          Mitgliedschaft in Multicastgruppen anzeigen
    -s, --statistics      Netzwerksstatistiken anzeigen (wie SNMP)
    -M, --masquerade      Maskierte Verbindungen auflisten

    -v, --verbose         Ausführliche Ausgaben
    -n, --numeric          Rechnernamen nicht auflösen
    --numeric-hosts       Host-Namen nicht auflösen
    --numeric-ports       Port-Namen nicht auflösen
    --numeric-users       Benutzer-Namen nicht auflösen
    -N, --symbolic        Hardwarenamen auflösen
    -e, --extend           Weitere/zusätzliche Informationen anzeigen
    -p, --programs        PID/Programmnamen für Sockets anzeigen
    -c, --continuous      Anzeige laufend aktualisieren

    -l, --listening       Empfangsbereite Serversockets auflisten
    -a, --all, --listening Alle Sockets anzeigen (normal: nur verbundene)
    -o, --timers           Timer auflisten
    -F, --fib             Forwarding Information Base anzeigen (Standard)
    -C, --cache            Routencache statt FIB anzeigen

<Socket>={-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --netrom
<AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
Liste möglicher Adressfamilien, die Routen unterstützen:
  inet (DARPA-Internet) inet6 (IPv6) ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
  x25 (CCITT X.25)
lubich@ubuntu:~$

```

```

Datei Bearbeiten Ansicht Terminal Hilfe
lubich@ubuntu:~$ netstat -v -a | more
Aktive Internetverbindungen (Server und stehende Verbindungen)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ipp            *:                       LISTEN
tcp        11320   0 ubuntu.adm.ds.fhn:57341 stream-2.ssatr.ch:www   VERBUNDEN
udp        0      0 *:bootpc                 *:                       *
udp        0      0 *:mdns                   *:                       *
udp        0      0 *:44924                  *:                       *

Aktive Sockets in der UNIX-Domäne (Server und stehende Verbindungen)
Proto RefCnt Flags       Type        State         I-Node   Pfad
unix    2      [ ACC ] STREAM     HöRT         6936     @/var/run/hald/dbus-jA0XhU4mZA
unix    2      [ ACC ] STREAM     HöRT         6691     /var/run/dbus/system_bus_socket
unix    2      [ ACC ] STREAM     HöRT         6914     @/var/run/hald/dbus-4W0IspDmTd
unix    2      [ ACC ] STREAM     HöRT         7731     /var/run/gdm_socket
unix    2      [ ]       DGRAM      HöRT         3103     @/com/ubuntu/upstart
unix    2      [ ACC ] STREAM     HöRT         7664     @/org/bluez/audio
unix    2      [ ACC ] STREAM     HöRT         8022     /var/run/cups/cups.sock
unix    2      [ ACC ] STREAM     HöRT         6486     /var/run/acpid.socket
unix    2      [ ACC ] STREAM     HöRT         7781     @/tmp/.X11-unix/X0
unix    2      [ ]       DGRAM      HöRT         3319     @/org/kernel/udev/udev
unix    2      [ ACC ] STREAM     HöRT         6903     /tmp/.winbindd/pipe
unix    2      [ ACC ] STREAM     HöRT         7782     /tmp/.X11-unix/X0
unix    2      [ ACC ] STREAM     HöRT         8901     /tmp/keyring-Tw4WNB/socket
unix    2      [ ACC ] STREAM     HöRT         9736     /tmp/ssh-bjyqWt3799/agent.3799
unix    2      [ ACC ] STREAM     HöRT         7821     /var/run/atievents.socket
unix    2      [ ]       DGRAM      HöRT         6958     @/org/freedesktop/hal/udev_event
unix    2      [ ACC ] STREAM     HöRT         9820     /tmp/orbit-lubich/linc-f75-0-3e69d3802ef3
1
unix    2      [ ACC ] STREAM     HöRT         10042    /tmp/orbit-lubich/linc-f73-0-407a12a42be7
unix    2      [ ACC ] STREAM     HöRT         10052    /tmp/.esd-1000/socket
unix    2      [ ACC ] STREAM     HöRT         10055    /home/lubich/.pulse/edabcc117c6bcb024b425
afc49eb151b:runtime/native
unix    2      [ ACC ] STREAM     HöRT         10095    /tmp/seahorse-HWBydg/S.gpg-agent
unix    2      [ ACC ] STREAM     HöRT         10126    /tmp/.ICE-unix/3799
unix    2      [ ACC ] STREAM     HöRT         10144    /tmp/orbit-lubich/linc-ed7-0-5c2328785667
e
unix    2      [ ACC ] STREAM     HöRT         10221    /tmp/orbit-lubich/linc-f85-0-4256e5056537
a
unix    2      [ ACC ] STREAM     HöRT         10276    /tmp/orbit-lubich/linc-eca-0-36e36ca27273
8
unix    2      [ ACC ] STREAM     HöRT         10280    /tmp/keyring-Tw4WNB/socket.ssh
unix    2      [ ACC ] STREAM     HöRT         10282    /tmp/keyring-Tw4WNB/socket.pkcs11
unix    2      [ ACC ] STREAM     HöRT         10641    /tmp/orbit-lubich/linc-f80-0-52c077be506e
9
--Mehr--
netstat: no support for `AF IPX' on this system.
netstat: no support for `AF AX25' on this system.
netstat: no support for `AF X25' on this system.
netstat: no support for `AF NETROM' on this system.
lubich@ubuntu:~$

```

netstat


```

Datei Bearbeiten Ansicht Terminal Hilfe
lubich@ubuntu:~$ netstat -r
Kernel-IP-Routentabelle
Ziel          Router      Genmask      Flags        MSS  Fenster  irtt  Iface
10.212.134.0  *          255.255.255.0 U            0 0        0 eth0
link-local    *          255.255.0.0  U            0 0        0 eth0
default       10.212.134.1 0.0.0.0      UG           0 0        0 eth0
lubich@ubuntu:~$

```

```

Datei Bearbeiten Ansicht Terminal Hilfe
lubich@ubuntu:~$ ping chalmers.se
PING chalmers.se (129.16.221.8) 56(84) bytes of data.
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=1 ttl=232 time=46.1 ms
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=2 ttl=232 time=49.1 ms
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=3 ttl=232 time=45.4 ms
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=4 ttl=232 time=45.3 ms
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=5 ttl=232 time=48.9 ms
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=6 ttl=232 time=45.5 ms
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=7 ttl=232 time=45.6 ms
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=8 ttl=232 time=49.0 ms
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=9 ttl=232 time=48.9 ms
64 bytes from www.chalmers.se (129.16.221.8): icmp_seq=10 ttl=232 time=45.3 ms
^C
--- chalmers.se ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 45.340/46.964/49.110/1.712 ms
lubich@ubuntu:~$ █

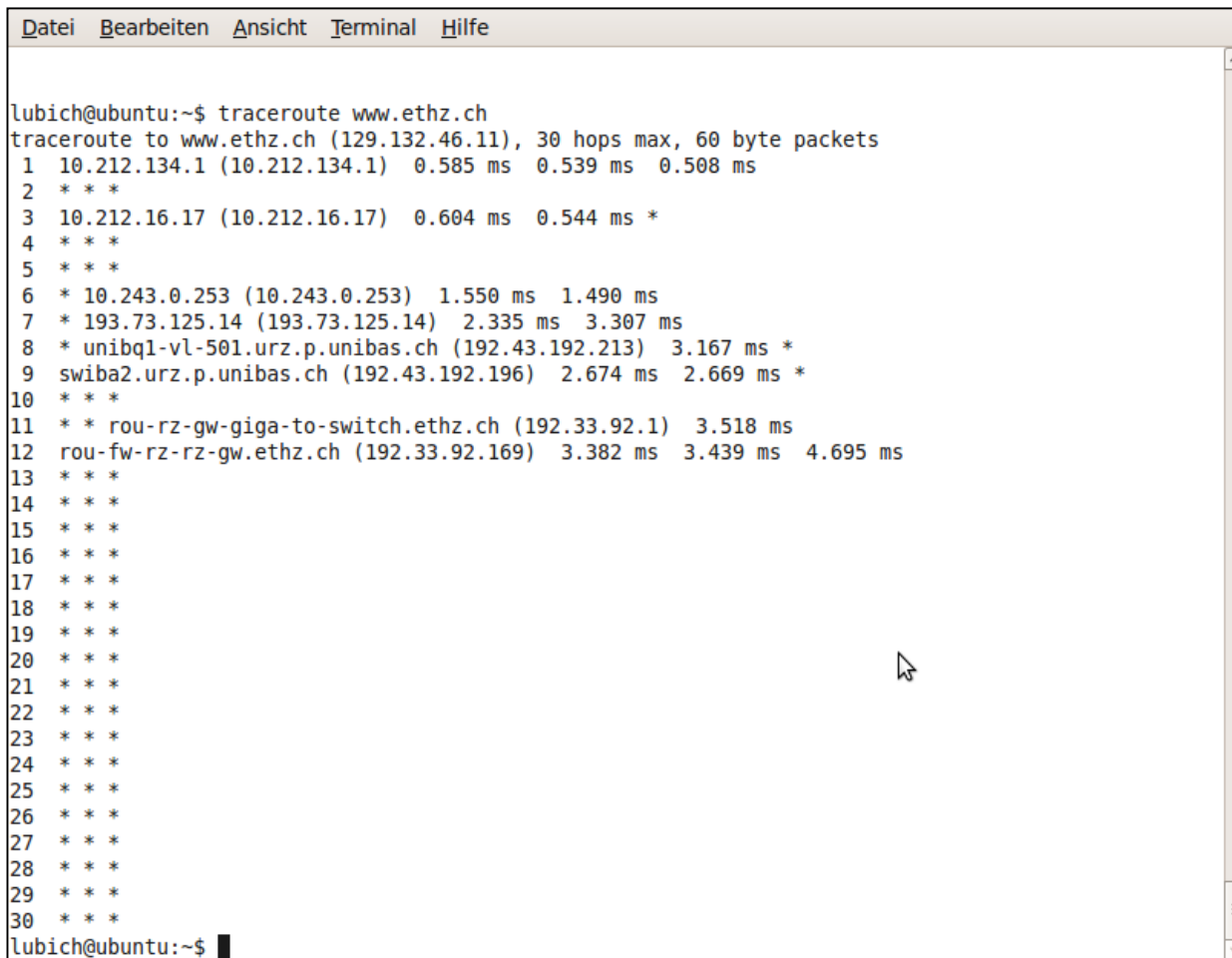
```

```

Datei Bearbeiten Ansicht Terminal Hilfe
lubich@ubuntu:~$ traceroute www.sun.com
Das Programm traceroute ist folgenden Paketen enthalten:
* traceroute
* traceroute-nanog
Versuchen Sie: sudo apt-get install <ausgewähltes Paket>
bash: traceroute: command not found
lubich@ubuntu:~$ sudo apt-get install traceroute
[sudo] password for lubich:
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut
Lese Status-Informationen ein... Fertig
Die folgenden NEUEN Pakete werden installiert:
  traceroute
0 aktualisiert, 1 neu installiert, 0 zu entfernen und 0 nicht aktualisiert.
Es müssen 56.0kB an Archiven heruntergeladen werden.
Nach dieser Operation werden 209kB Plattenplatz zusätzlich benutzt.
Hole:1 http://ch.archive.ubuntu.com jaunty/main traceroute 2.0.12-1 [56.0kB]
Es wurden 56.0kB in 0s geholt (137kB/s)
Wähle vormals abgewähltes Paket traceroute.
(Lese Datenbank ... 163440 Dateien und Verzeichnisse sind derzeit installiert.)
Entpacke traceroute (aus ../traceroute_2.0.12-1_amd64.deb) ...
Verarbeite Trigger für man-db ...
Richte traceroute ein (2.0.12-1) ...

lubich@ubuntu:~$ █

```



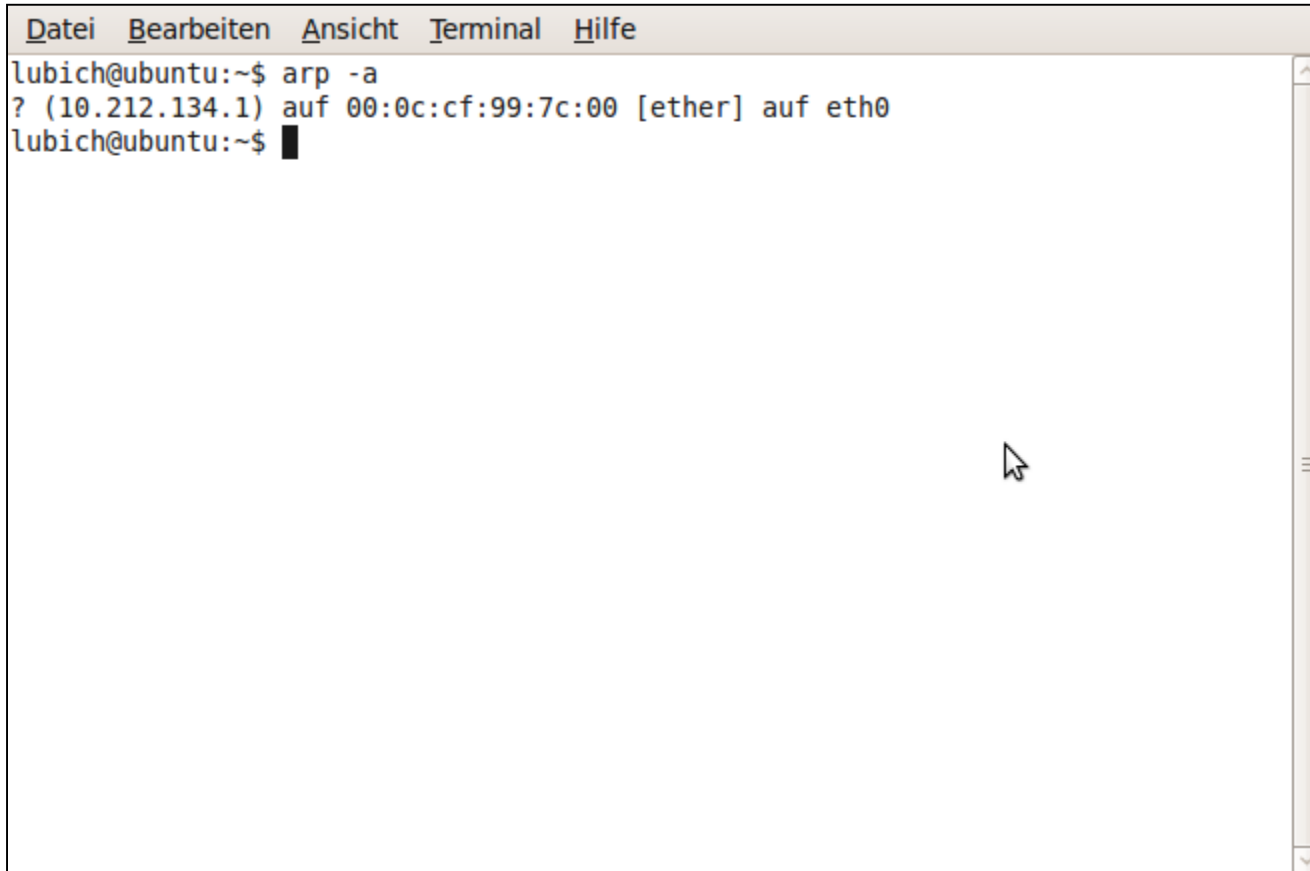
The screenshot shows a terminal window with a menu bar containing 'Datei', 'Bearbeiten', 'Ansicht', 'Terminal', and 'Hilfe'. The terminal content displays the execution of the 'traceroute' command from the user 'lubich' on an 'ubuntu' system. The command 'traceroute www.ethz.ch' is entered, followed by the output showing the path to 'www.ethz.ch' (129.132.46.11) with 30 hops max and 60 byte packets. The output lists hops 1 through 30, with some hops showing IP addresses and round-trip times, while others are marked with asterisks to indicate timeouts. The terminal ends with the prompt 'lubich@ubuntu:~\$'.

```
Datei Bearbeiten Ansicht Terminal Hilfe

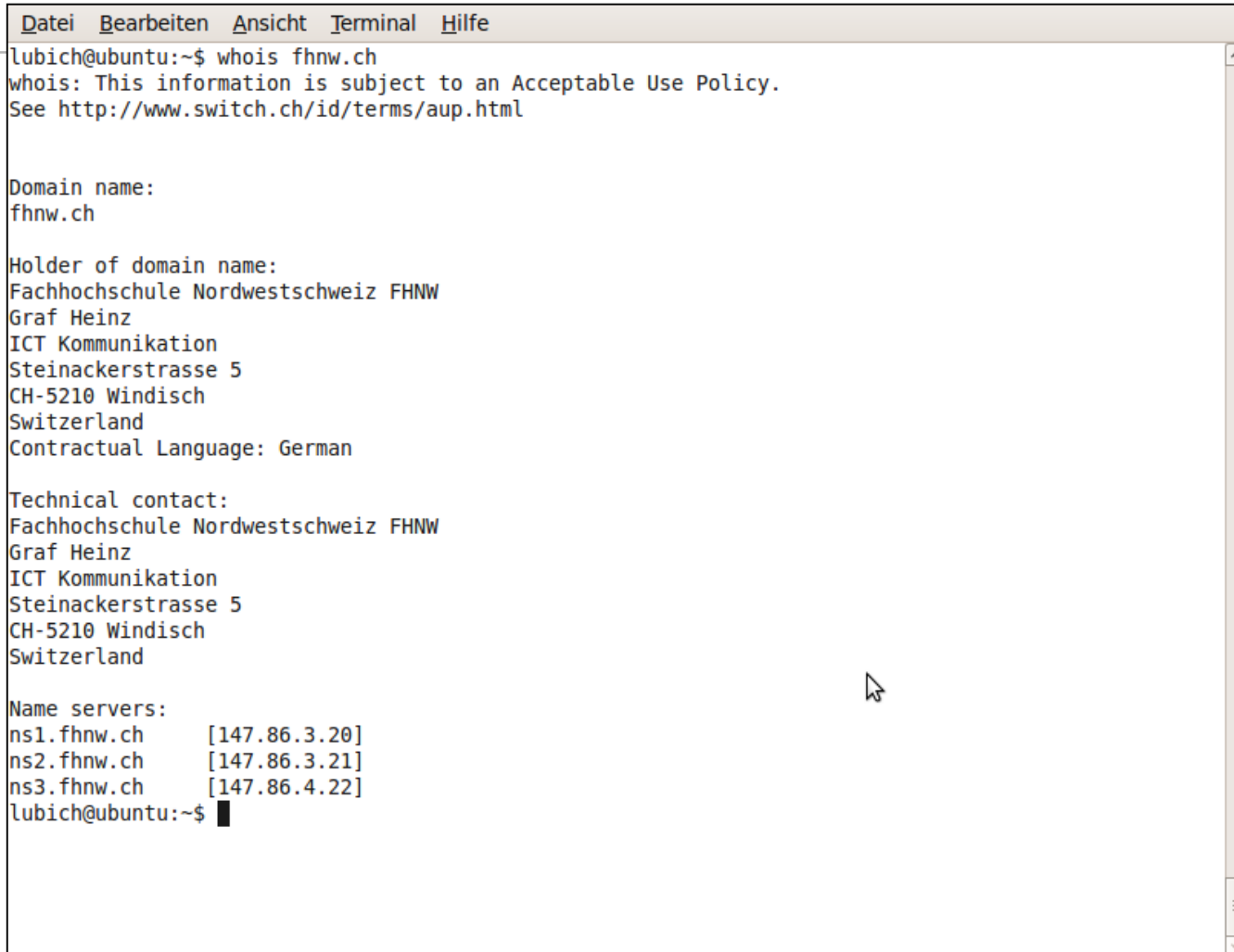
lubich@ubuntu:~$ traceroute www.ethz.ch
traceroute to www.ethz.ch (129.132.46.11), 30 hops max, 60 byte packets
 1  10.212.134.1 (10.212.134.1)  0.585 ms  0.539 ms  0.508 ms
 2  * * *
 3  10.212.16.17 (10.212.16.17)  0.604 ms  0.544 ms *
 4  * * *
 5  * * *
 6  * 10.243.0.253 (10.243.0.253)  1.550 ms  1.490 ms
 7  * 193.73.125.14 (193.73.125.14)  2.335 ms  3.307 ms
 8  * unibql-vl-501.urz.p.unibas.ch (192.43.192.213)  3.167 ms *
 9  swiba2.urz.p.unibas.ch (192.43.192.196)  2.674 ms  2.669 ms *
10  * * *
11  * * rou-rz-gw-giga-to-switch.ethz.ch (192.33.92.1)  3.518 ms
12  rou-fw-rz-rz-gw.ethz.ch (192.33.92.169)  3.382 ms  3.439 ms  4.695 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
lubich@ubuntu:~$
```

Betrachtung und Konfiguration der Netzwerkschnittstelle II

- arp
- whois
- nslookup
- Ubuntu GUI

A terminal window with a menu bar containing 'Datei', 'Bearbeiten', 'Ansicht', 'Terminal', and 'Hilfe'. The terminal text shows a user running 'arp -a' and receiving output for the interface eth0.

```
Datei Bearbeiten Ansicht Terminal Hilfe
lubich@ubuntu:~$ arp -a
? (10.212.134.1) auf 00:0c:cf:99:7c:00 [ether] auf eth0
lubich@ubuntu:~$
```

A terminal window with a menu bar (Datei, Bearbeiten, Ansicht, Terminal, Hilfe) and a title bar. The terminal shows a command prompt where the user has entered 'whois fhnw.ch'. The output displays domain information for fhnw.ch, including the holder's name (Graf Heinz), address (Steinackerstrasse 5, CH-5210 Windisch), and technical contact details. It also lists three name servers with their IP addresses. The prompt ends with a cursor.

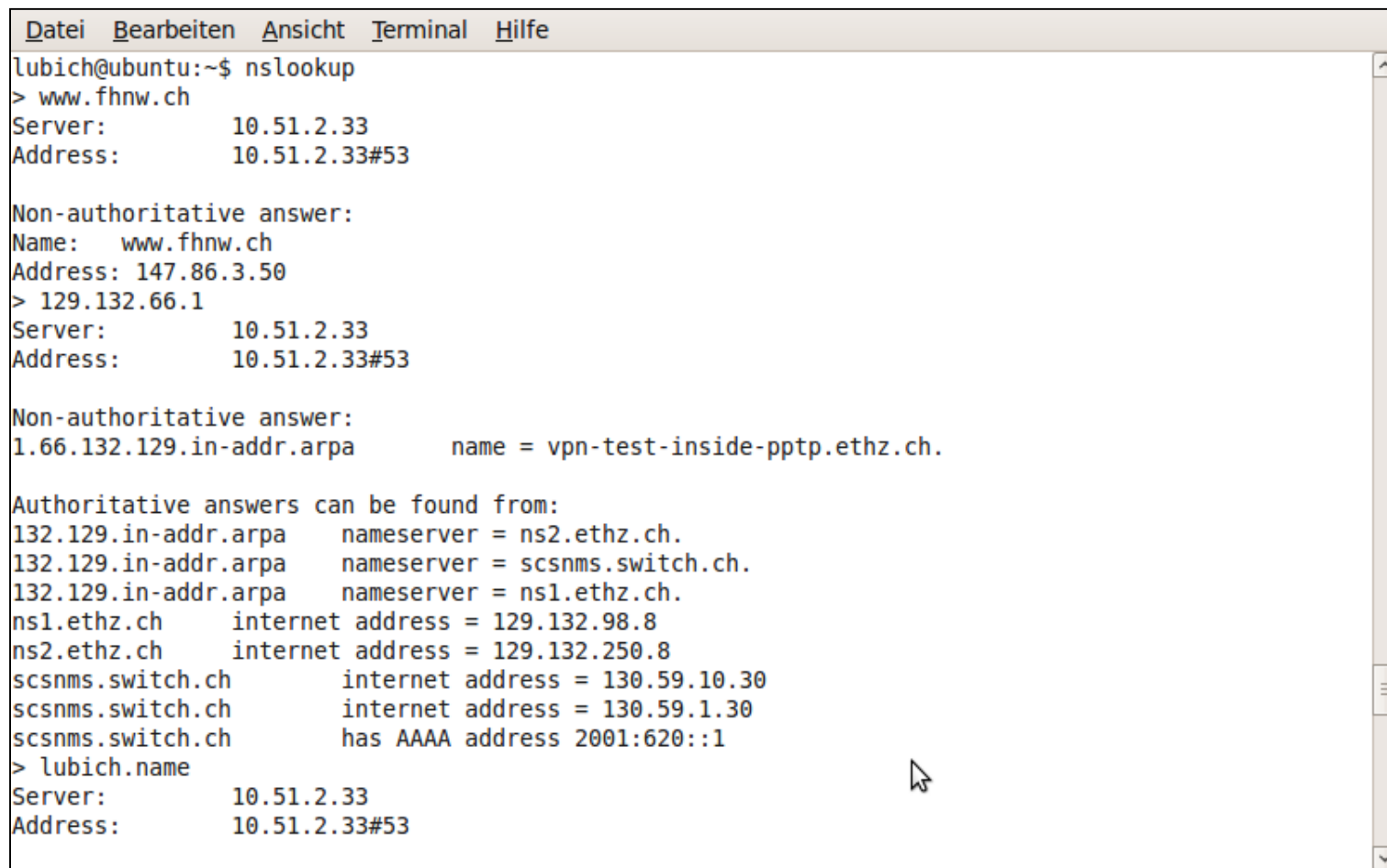
```
Datei Bearbeiten Ansicht Terminal Hilfe
lubich@ubuntu:~$ whois fhnw.ch
whois: This information is subject to an Acceptable Use Policy.
See http://www.switch.ch/id/terms/aup.html

Domain name:
fhnw.ch

Holder of domain name:
Fachhochschule Nordwestschweiz FHNW
Graf Heinz
ICT Kommunikation
Steinackerstrasse 5
CH-5210 Windisch
Switzerland
Contractual Language: German

Technical contact:
Fachhochschule Nordwestschweiz FHNW
Graf Heinz
ICT Kommunikation
Steinackerstrasse 5
CH-5210 Windisch
Switzerland

Name servers:
ns1.fhnw.ch      [147.86.3.20]
ns2.fhnw.ch      [147.86.3.21]
ns3.fhnw.ch      [147.86.4.22]
lubich@ubuntu:~$
```

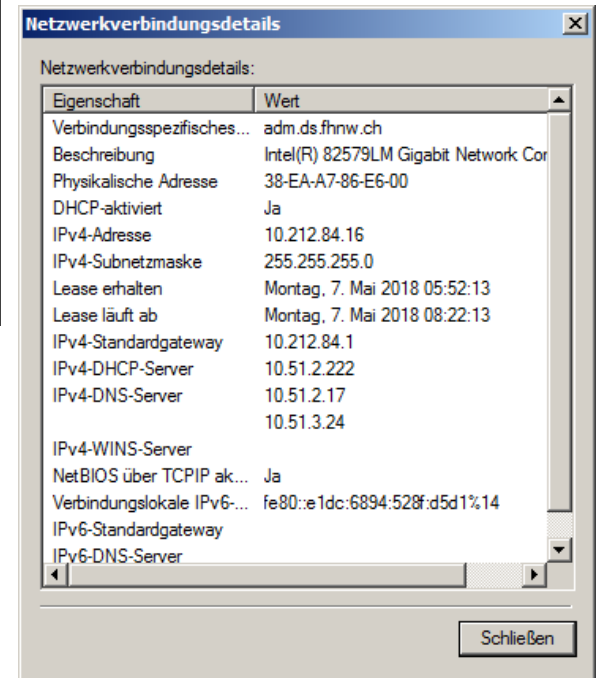
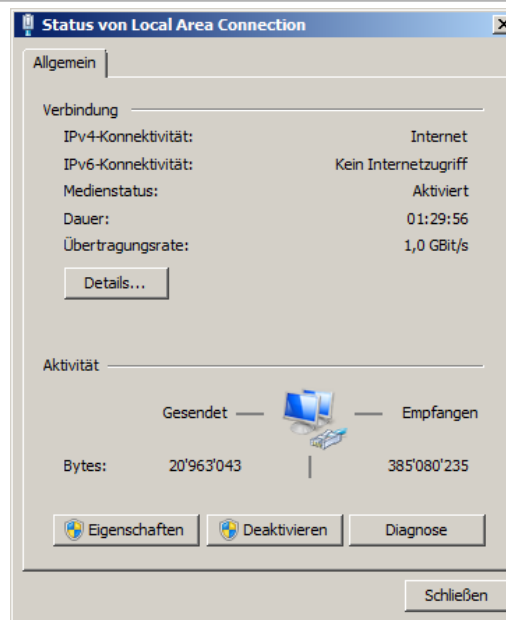
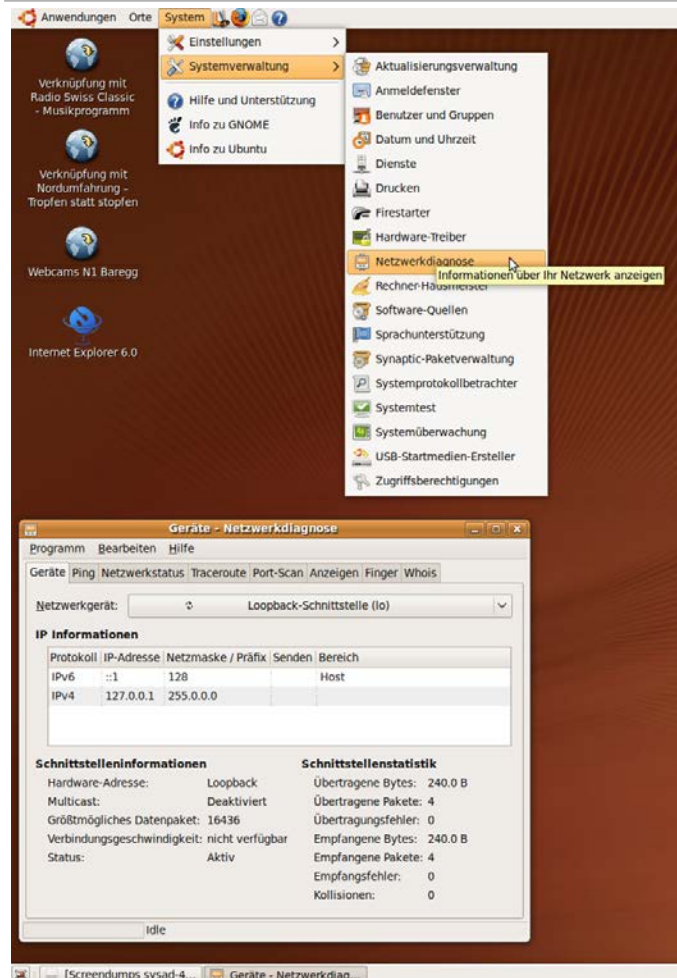


```
Datei Bearbeiten Ansicht Terminal Hilfe
lubich@ubuntu:~$ nslookup
> www.fhnw.ch
Server:      10.51.2.33
Address:     10.51.2.33#53

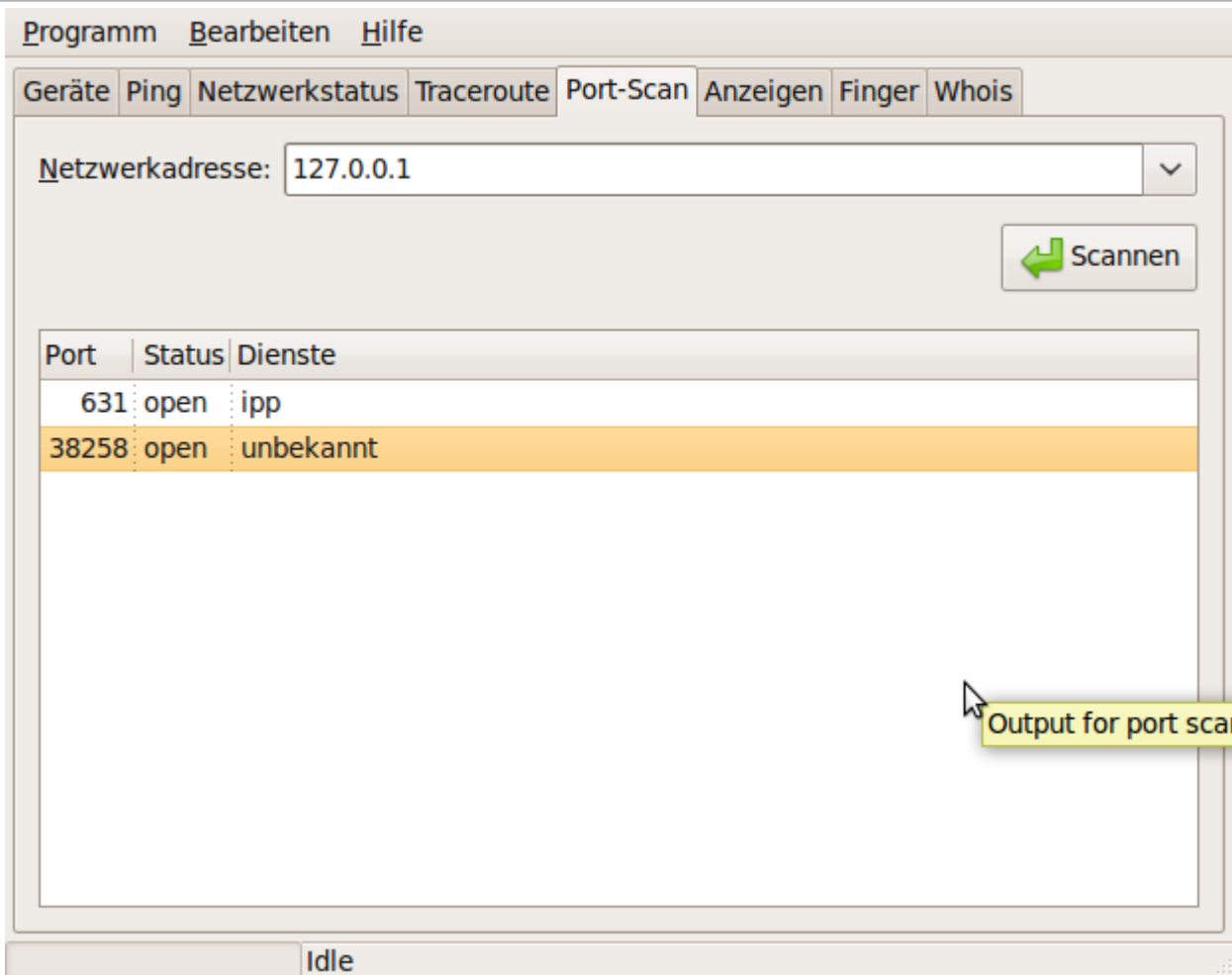
Non-authoritative answer:
Name:   www.fhnw.ch
Address: 147.86.3.50
> 129.132.66.1
Server:      10.51.2.33
Address:     10.51.2.33#53

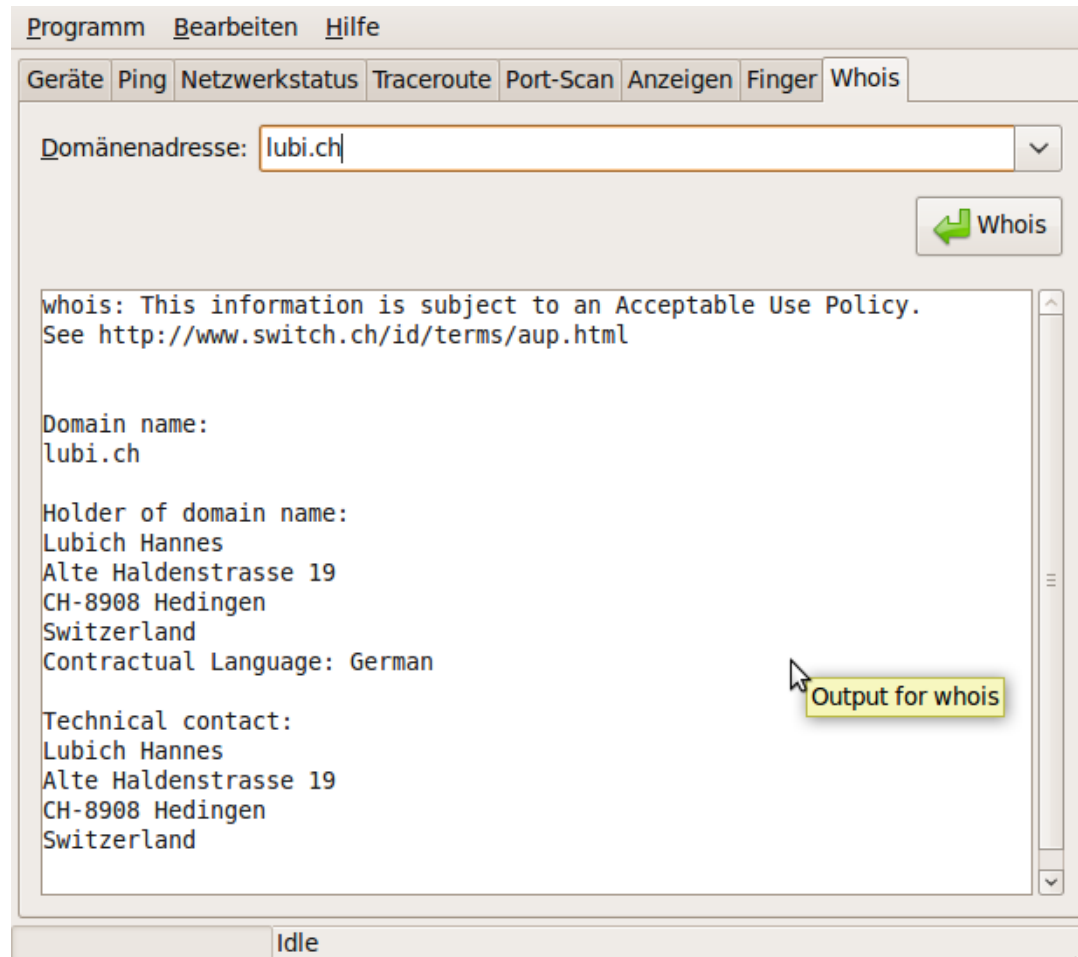
Non-authoritative answer:
1.66.132.129.in-addr.arpa      name = vpn-test-inside-pptp.ethz.ch.

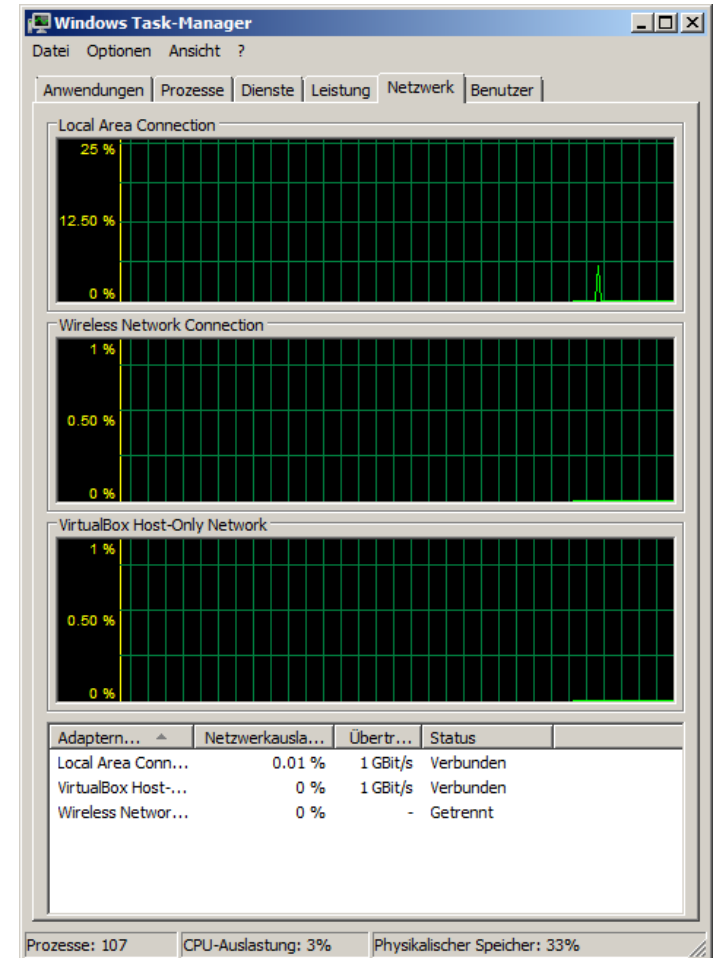
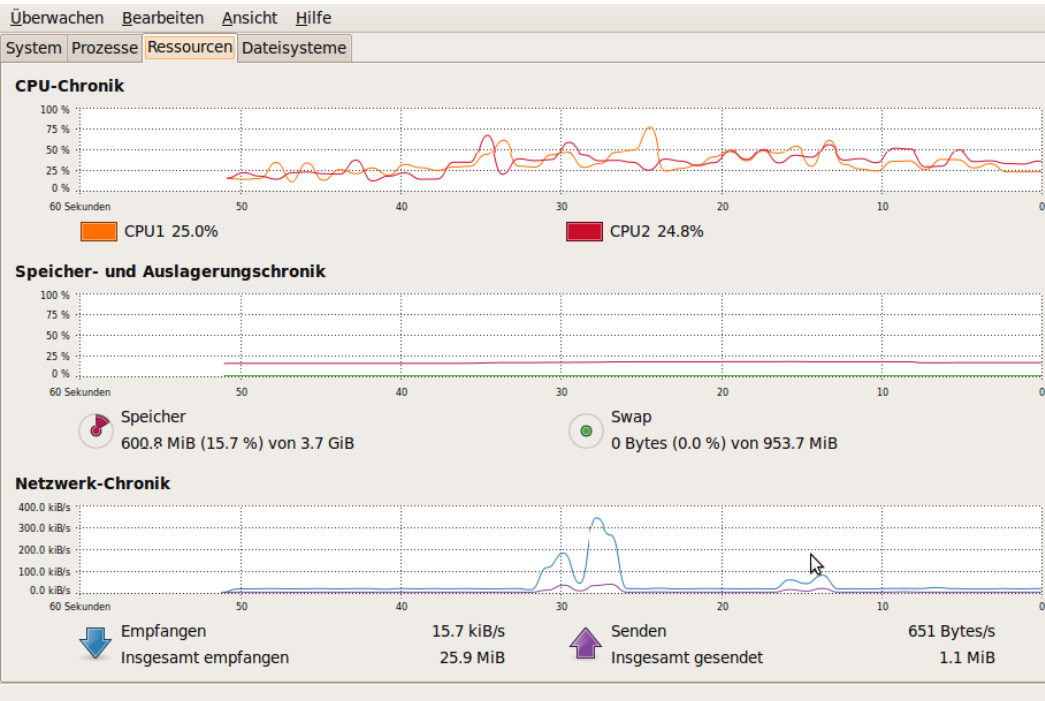
Authoritative answers can be found from:
132.129.in-addr.arpa  nameserver = ns2.ethz.ch.
132.129.in-addr.arpa  nameserver = scsnms.switch.ch.
132.129.in-addr.arpa  nameserver = ns1.ethz.ch.
ns1.ethz.ch           internet address = 129.132.98.8
ns2.ethz.ch           internet address = 129.132.250.8
scsnms.switch.ch      internet address = 130.59.10.30
scsnms.switch.ch      internet address = 130.59.1.30
scsnms.switch.ch      has AAAA address 2001:620::1
> lubich.name
Server:      10.51.2.33
Address:     10.51.2.33#53
```











Übung (ca. 30 min.)

- Aufgabe(n) gemäss separatem Aufgabenblatt
- Lösungsansatz: Einzelarbeit oder Gruppen von max. 3 Personen
- Hilfsmittel: beliebig
- Besprechung möglicher Lösungen in der Klasse (es gibt meist nicht die eine «Musterlösung»)

Übungsbesprechung (ca. 15 min.)

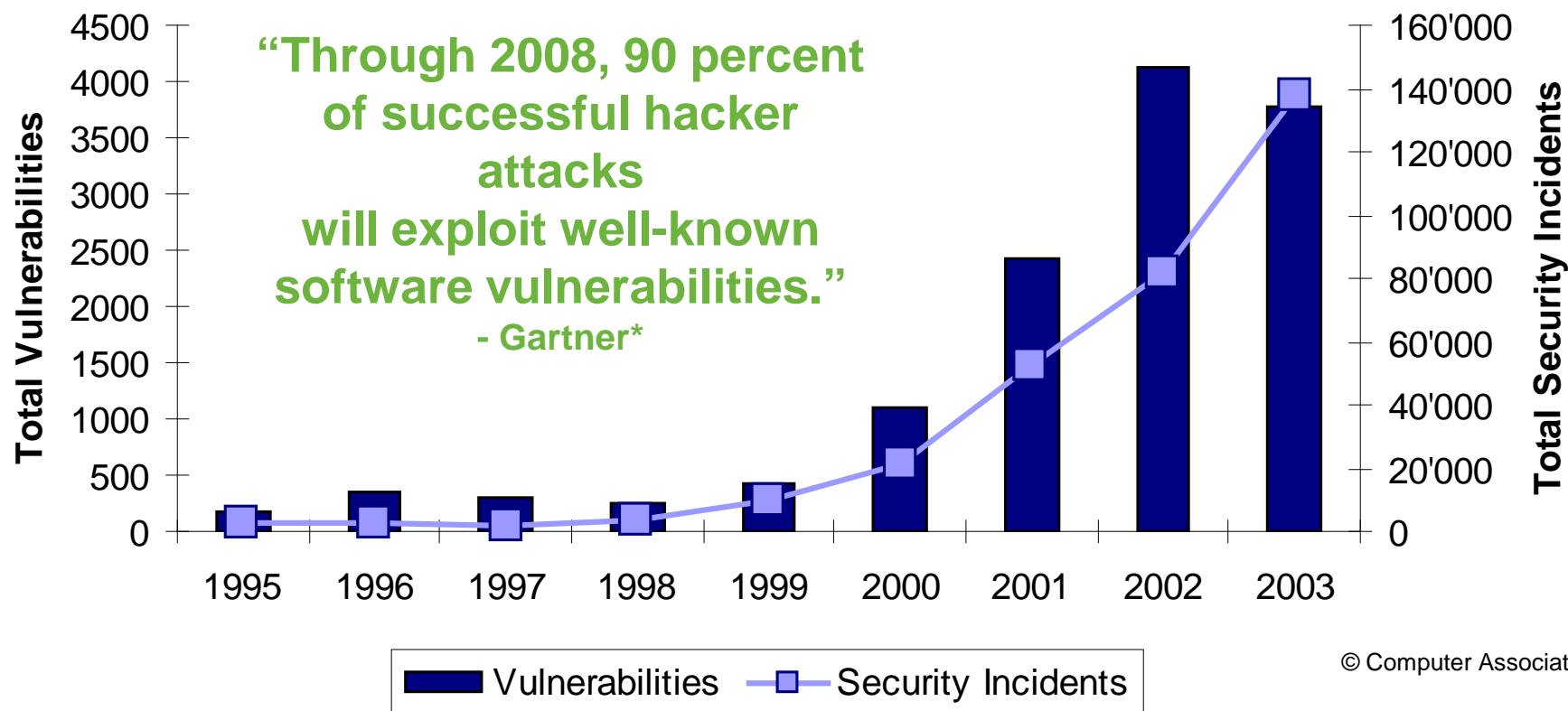
- Stellen Sie Ihre jeweilige Lösung der Klasse vor.
- Zeigen Sie auf, warum ihre Lösung korrekt, vollständig und effizient ist.
- Diskutieren Sie ggf. Design-Entscheide, Alternativen oder abweichende Lösungsansätze.
- Gibt es Unklarheiten? Stellen Sie Fragen.



Inhalt – Sicherheit im Betriebssystem

- Analyse typischer Schwachstellen von Betriebssystemen am Beispiel Unix und Microsoft Windows.
- Diskussion typischer Angriffsarten und Angriffsmotivationen und deren Auswirkung
- Diskussion präventiver und reaktiver Schutzmassnahmen (Technik, Prozesse, Personen) und deren Auswirkung auf die Funktionalität und Leistungsfähigkeit des Betriebssystems
- Identifikation des weitergehenden Schutzbedarfs ausserhalb des Betriebssystems

Incidents and Vulnerabilities Reported to CERT/CC



* Gartner “CIO Alert: Follow Gartner’s Guidelines for Updating Security on Internet Servers, Reduce Risks.” J. Pescatore, February 2003

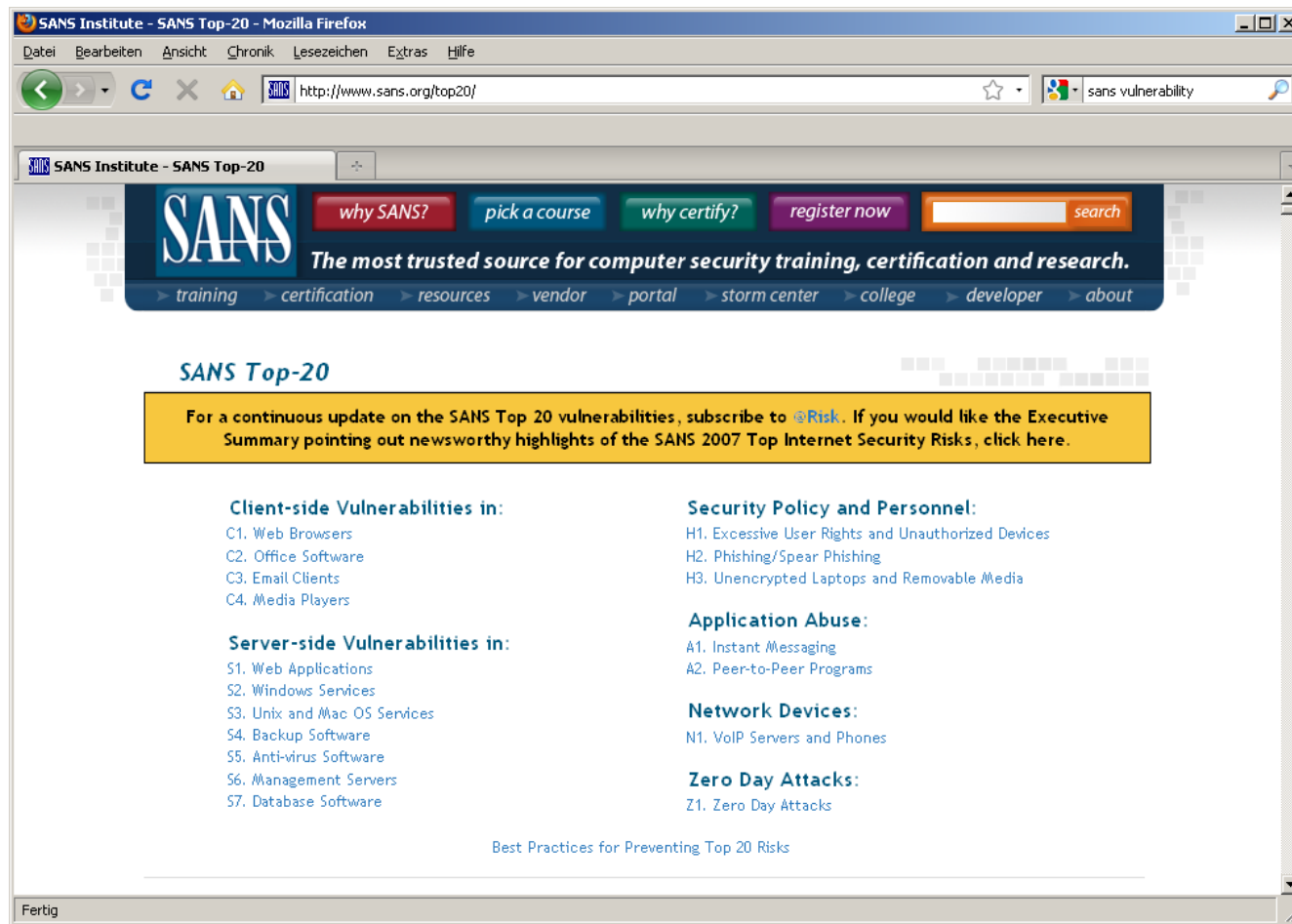
Typische Schwachstellen von ICT-Systemen

- Typische Schwachstellen
 - Lieferwege (physisch, aber vor allem elektronisch)
 - Software-Voreinstellungen (Defaults)
 - Funktionale Fehler der Software / Ausnutzbarkeit von Nebeneffekten
 - Nicht getestete oder nicht autorisierte Änderungen
 - Fremd-/Fernzugriffe oder Auslagerung aus dem Sicherheits-Kontext
 - Der Benutzer
 - Der Administrator
- Ursachen
 - Komplexes Zusammenwirken verschiedener Effekte
 - Ungerechtfertigtes Vertrauen („Es sah aber echt aus“)
 - Gutwilligkeit der Beteiligten („Wird schon stimmen“)
 - Fehlerhafte Ausführung und/oder Kontrolle (insbes. unter Zeitdruck)
 - Böswilligkeit / Vorsatz (Innen- oder Aussentäterschaft)

Analyse typischer Schwachstellen von Betriebssystemen

- Unix
 - Fehlerhafte Default-Konfigurationen
 - Unnötige (offene) Services / Ports
 - Zu wenig restriktive Zugriffsrechte
 - Technische Benutzer ohne Passworte
 - Brute Force Passwort-Angriffe auf Dienste wie telnet, ftp, ssh (Würmer, Botnets)
 - Ausnutzung von Software-Schwachstellen (meist Authentisierung, Speicherüberlauf, Escape-Shells)

- Microsoft Windows
 - Angriffe auf „Service Control“ Programme (SCP) unter Kontrolle des „Service Control Manager“ (SCM, „services.exe“)
 - Ausnutzung von Software-Schwachstellen („buffer overflow“) → aufgrund der schwachen BS-internen Abgrenzung des Speicher-Mgmt
 - Unbenötigte Services mit schwachem Schutz
 - Lokale Administratorenrechte



<http://www.sans.org/top20/>

Bedrohungen und Angreifer

- Outsiders:
 - Hackers / Crackers / Pranksters
 - Informationssammler / Presse
 - Kriminelle Individuen oder Organisationen
 - (Fremde) Aufklärungsdienste
 - Polizei / Strafverfolgungsbehörden
 - Geschäftspartner / Kunden
 - Wettbewerber / Neue Mitbewerber
 - Fanatiker / Terroristen
 - Information Warfare
- Insiders:
 - Unzufriedene Mitarbeitende
 - Lieferanten / (externes) Wartungspersonal
 - System Spezialisten
 - Kriminelle Mitarbeitende
 - Unvorsichtige Mitarbeitende
 - “Friends & Family”

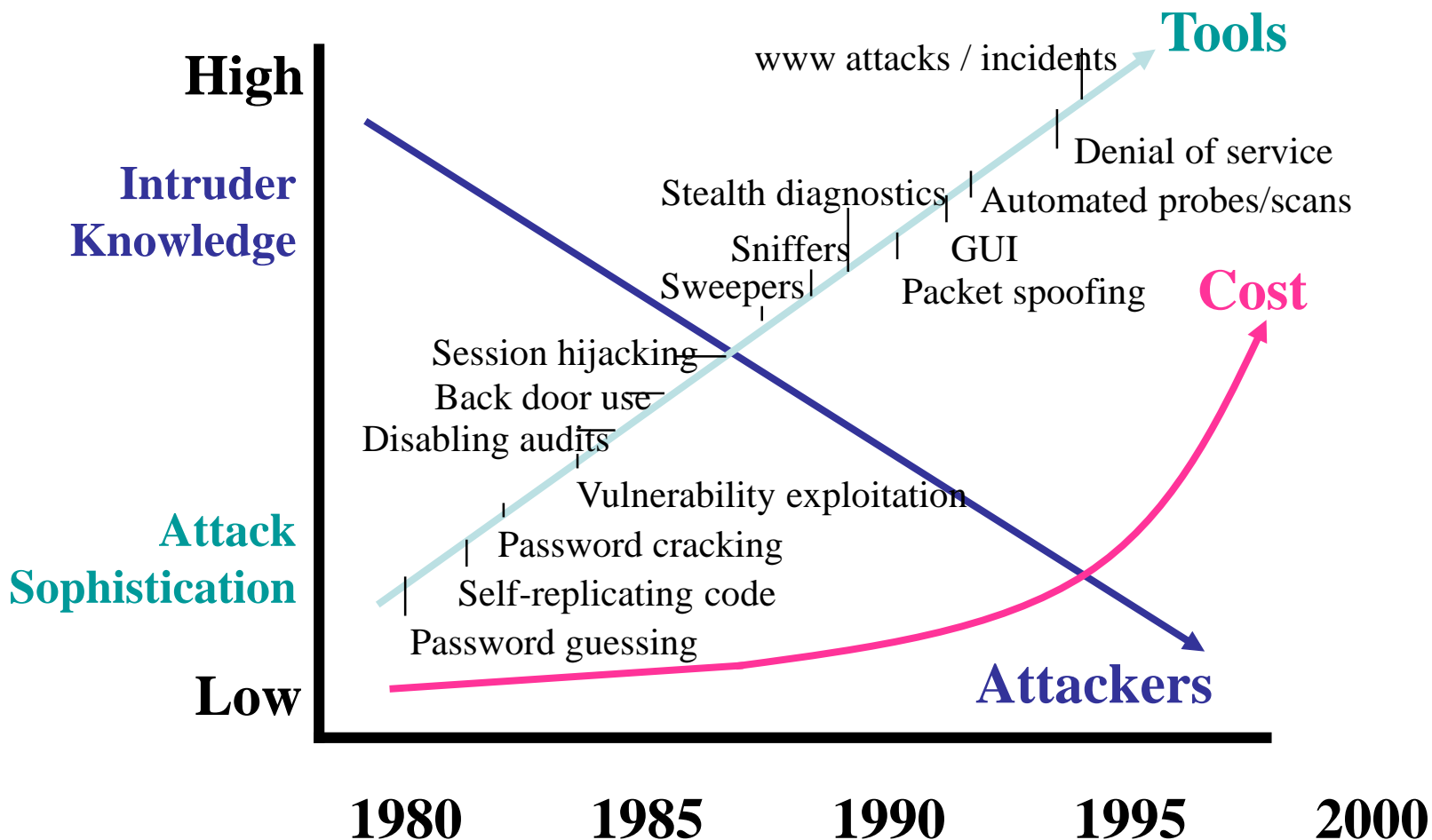
Classification:

- Script Kiddie
- Intermediate
- Professional
- Elite

- Reputation (Community, Freunde, Öffentlichkeit, ...)
- Langeweile (oft altersbedingt)
- Schaden / Rache (früherer Mitarbeiter, Ex-Partner, ...)
- Wettbewerb (Offerten, Kunden, Patente, ...)
- Direkter Vorteil (Software, Musik, ...)
- Indirekter Vorteil (Lizenzen, Information, Passworte, ...)
- Privater Auftrag (kommerzielle/industrielle Spionage)
- Regierungsauftrag (Terrorismusbekämpfung, Spionage, Gegenspionage, militärische Aufklärung, ...)

- Verfügbarkeit
- Vertraulichkeit
- Korrektheit
- Zeitliche Abfolge
- Bereitstellungstermin
- Identität / Autorisierung
- Handlungsfähigkeit
- Guter Ruf / Image

Aufwand für IT-Sicherheit



Präventive und reaktive Schutzmassnahmen

- Technik – Härten und Prüfen
 - Prozesse – Überwachung und automatische Reaktion
 - Personen – Awareness
- Auswirkung auf die Funktionalität
und Leistungsfähigkeit des Systems

- Identifikation relevanter Systeme oder Applikationen
- Technische Überprüfung (Security Scan, Penetration Testing, Application Security Audit, Ethical Hacking)
- Organisatorische Überprüfung (ICT Bedrohungs- und Risikoanalyse)
- Definition des Massnahmenkatalog zur Erhöhung des Sicherheitsniveaus:
 - Default-Installationen kritisch hinterfragen → ggf. eigener Default
 - Konfigurationsänderungen (Rechte, Rollen, Prozesse, ...)
 - Einspielen von Security-relevanten Updates
 - Entfernen nicht benötigter HW/SW-Komponenten oder Schnittstellen
 - Installation von sicherheitsspezifischer Zusatzsoftware
 - Zyklische Neuüberprüfung von aussen (Scan) oder innen (z.B. Secunia)
 - Veränderungen / Verbesserungen im Betriebsablauf oder Überwachung
 - Auswertung „echter“ Angriffsversuche oder Kollateralinformation

Prüfen: Fallbeispiel „Nessus“

The image shows the Nessus Setup window and the Session Properties dialog box for host 10.1.1.1.

Nessus Setup - Plugin selection:

- CGI abuses
- Denial of Service
- Gain root remotely
- Peer-To-Peer File Sharing
- Backdoors
- Firewalls
- RPC
- Useless services
- Windows
- Misc.
- FTP

Session Properties - 10.1.1.1:

- Targets:** Port range to scan: ☒ Well-known services, ☒ Privileged ports (1-1024), ☐ Specific range.
- Port scanners:**

Name	Status
SYN Scan	Enabled
Tcp connect() scan	Disabled

Hosts list:

Host	Status
192.168.1.16	Warning
192.168.1.17	Warning
192.168.1.33	Warning
192.168.1.51	Warning
192.168.1.54	Warning
192.168.1.62	Warning
192.168.1.65	Warning
192.168.1.147	Warning
192.168.1.164	Warning
192.168.1.166	Warning
192.168.1.178	Warning

Port and Severity details:

Port	Severity
netbios-rs (137/udp)	Security Warning

NetBIOS names gathered:

- WAX
- WING = Workgroup / Domain name
- WING = Workgroup / Domain name (Domain Controller)
- WAX
- WING = Workgroup / Domain name (part of the Browser election)
- WAX = This is the current logged in user or registered
- WING
- __MSBROWSE__

MAC address: 0x00 0x04 0x76 0x12 0x36 0xd1

Risk factor: Medium
CVE: CAN-1999-0621

Prüfen: Fallbeispiel „Secunia“ (leider eingestellt)

Fortschritt des Scanvorgangs: Schritt-für-Schritt

- Scanvorgang gestartet
- Suchregeln von Secunia werden heruntergeladen (https)
- Dateien auf lokalen Festplatten werden durchsucht
- Dateiinformatoren werden gesammelt
- Betriebssysteminformationen werden gesammelt
- Ermitteln von fehlenden Microsoft-Security-Patches
- Abgleich von Daten mit der Secunia-File-Signatures-Engine
- Scanvorgang beendet

Status des Scanvorgangs

Scanvorgang nicht gestartet.

Letzter & Nächster vollständiger System-Scan in [?]

Letzter vollständiger System-Scan:
25 Apr. 2009, 11:27

Nächster vollständiger System-Scan:
2 May. 2009, 11:27

Fehlerbericht

Keine Fehler entdeckt.

Secunia PSI

Secunia Personal Software Inspector

ANSICHT: [EINFACH](#) | [ERWEITERT](#)

Übersicht Unsicher Veraltet Aktualisiert Scan Einstellungen Secunia-Profil Forum

Guten Morgen, <unregistrierter Benutzer>

Programmübersicht (aktuell)

ind gefährden Ihren PC. Um Ihren PC gen in den Kategorien "Unsicher" und

90% Vor 2 Tagen

6 Unsicher
0 Veraltet
52 Aktualisiert
58 Insgesamt

Aktualisiert, 52

Veraltet, 0
Unsicher, 6

Secunia PSI

Secunia Personal Software Inspector

ANSICHT: [EINFACH](#) | [ERWEITERT](#)

Übersicht Unsicher Veraltet Aktualisiert Scan Einstellungen Secunia-Profil Forum

Unsichere Programme

Diese Seite zeigt Programme an, die durch den Secunia PSI erkannt wurden und für die Sicherheitsupdates verfügbar sind. Wir empfehlen, dass Sie alle hier aufgeführten Programme aktualisieren oder deinstallieren. Klicken Sie auf einen Eintrag für weitere Details.

Unsichere Programme [?]	Erkannte Version [?]	Gefahrenstufe [?]	Direktzugriff [?]
+ Cisco VPN Client 5.x	5.0.00.0340	<div><div></div><div></div><div></div><div></div><div></div></div>	
+ Microsoft Excel 2003	11.0.8231.0	<div><div></div><div></div><div></div><div></div><div></div></div>	
+ Microsoft Office PowerPoint Viewer 2003	11.0.6566.0	<div><div></div><div></div><div></div><div></div><div></div></div>	
+ Microsoft Word 2003	11.0.8227.0	<div><div></div><div></div><div></div><div></div><div></div></div>	
+ Sun Java JRE 1.5.x / 5.x	1.5.0.0	<div><div></div><div></div><div></div><div></div><div></div></div>	
+ Sun Java JRE 1.5.x / 5.x	1.5.0.0	<div><div></div><div></div><div></div><div></div><div></div></div>	

Helfen Sie uns, unseren Service zu verbessern:
[Fehlt ein Programm? Schlagen Sie es hier vor!](#)

wickelt. Es werden die Scores der letzten zehn Wochen im direkten Vergleich zum aktuellen

Wocher Privacy Statement. Secunia PSI v1.0.0.4

Security Monitoring Daten - Informationsfluss

Security Daten



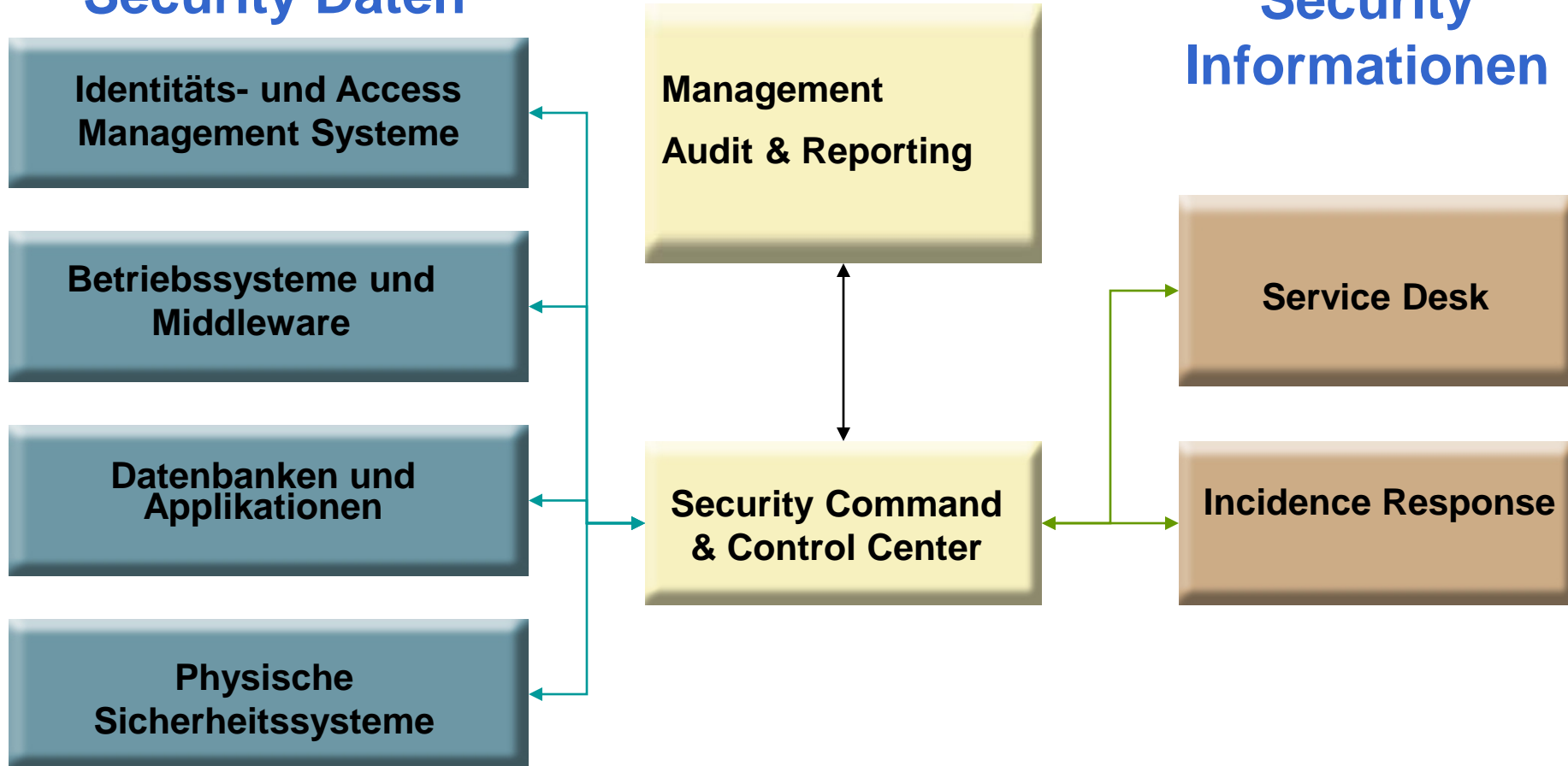
Management
Audit & Reporting

Security Command
& Control Center

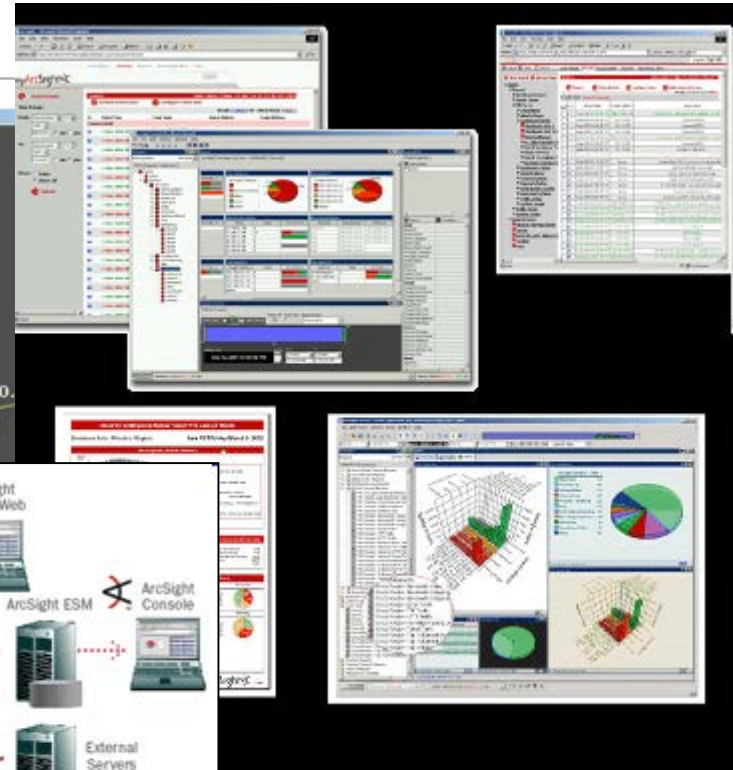
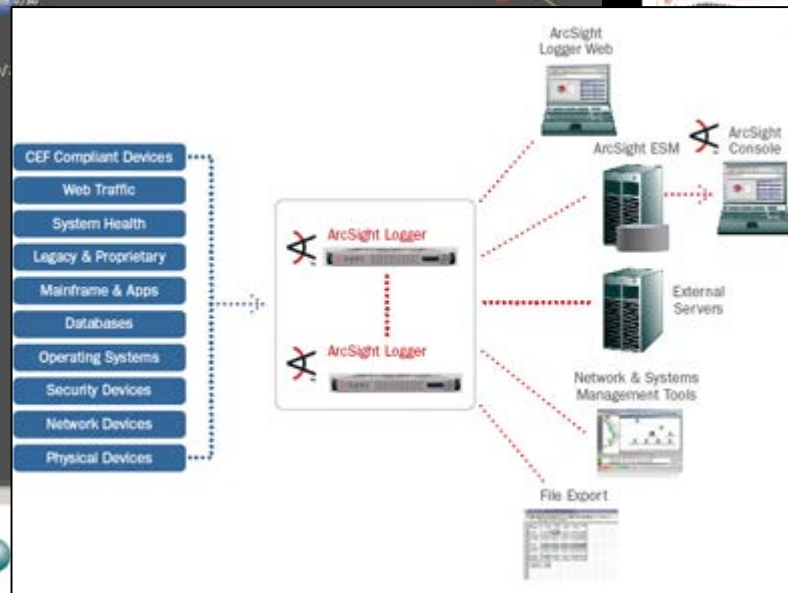
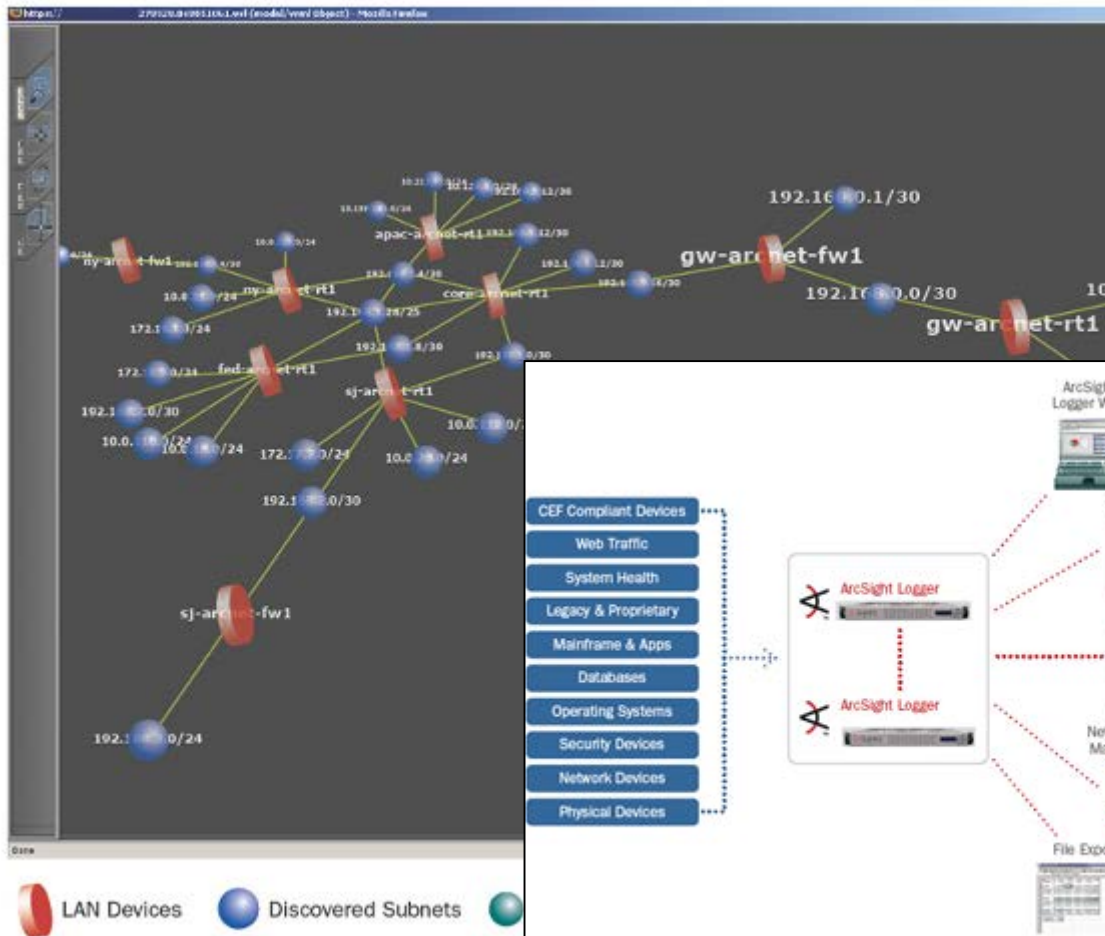
Security Informationen

Service Desk

Incidence Response



ArcSight (→ HP)

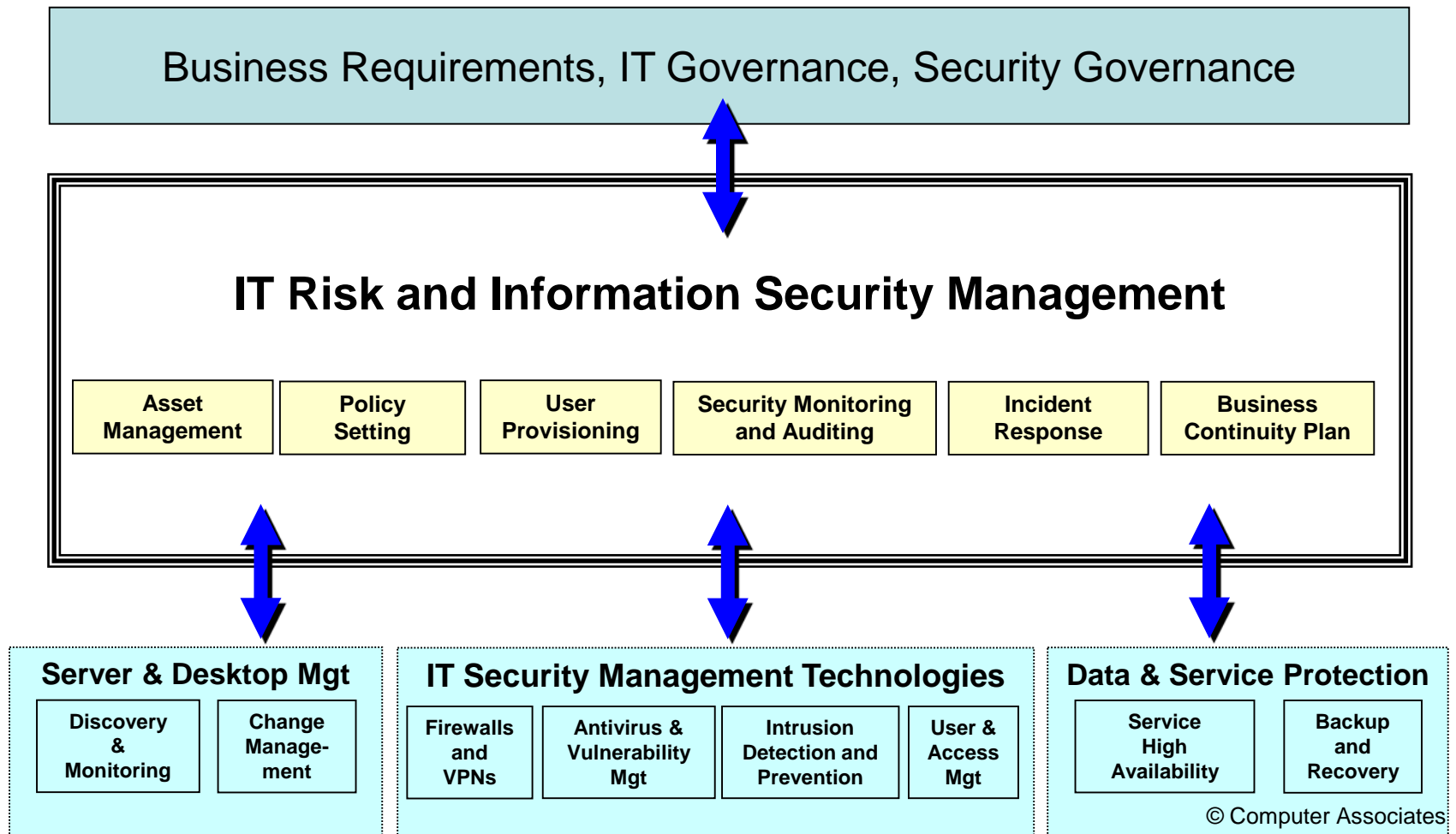


- Regelmässige Information über Bedrohungen und Gegenmassnahmen mit Bezug auf die Person / Firma / Situation
- Warnung vor akuten Problemen
- Übungen, Schulungen, Erfahrungsberichte
- Regelmässige Aktualisierung von Systemen und Applikationen aus zuverlässigen Quellen
- Bekannte Kontaktstelle bei Problemen

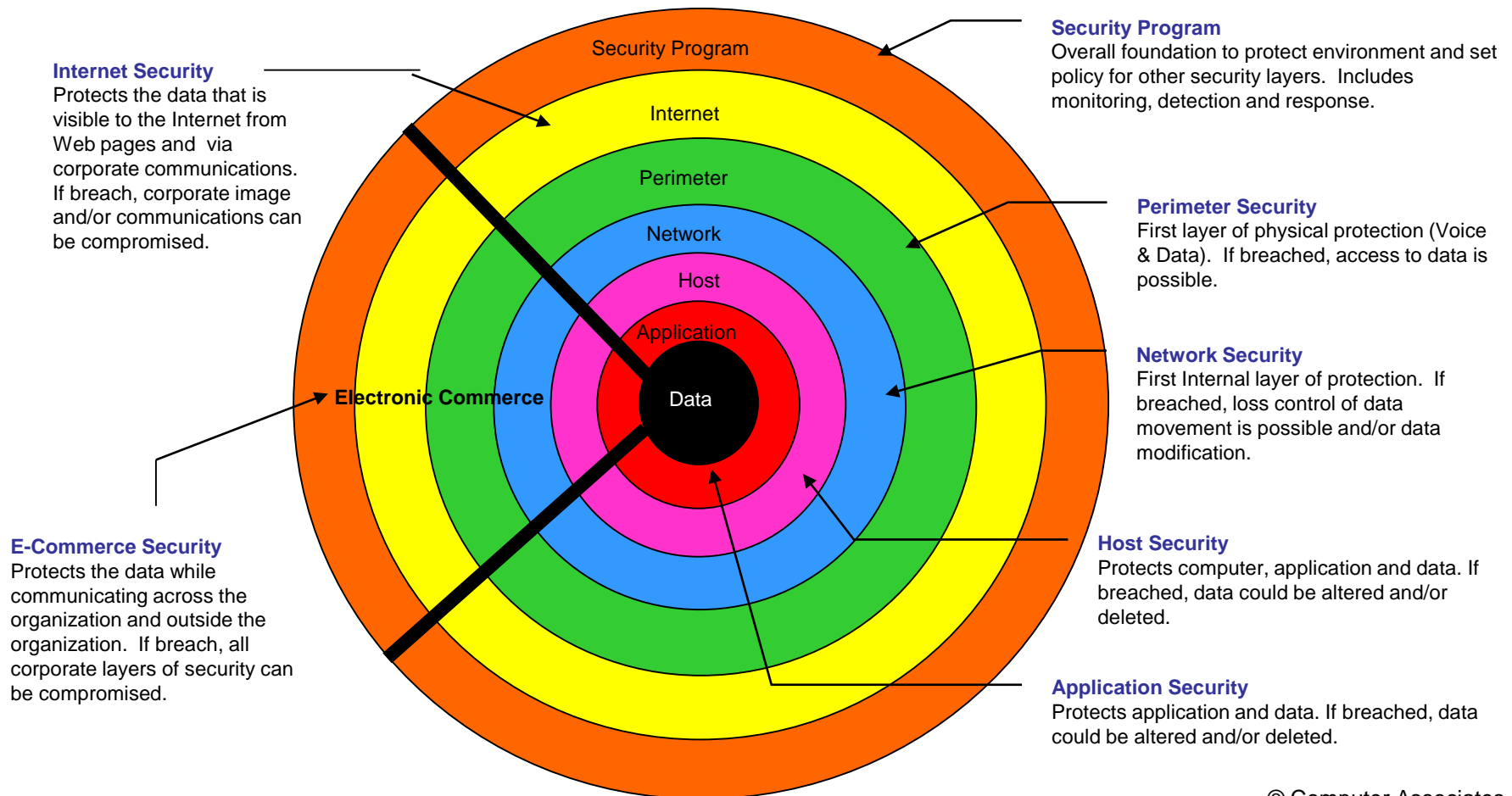
Weitergehender Schutzbedarfs ausserhalb des Betriebssystems

- IT Sicherheits-Architektur
- IT Sicherheits-Prozesse / Verfahren
- End-zu-End Sicherheit
- Einsatz von Baselines & Standards
- Systematische Risikoanalyse

Security-Architektur und -Prozesse



Firmenweite End-to-End Security



© Computer Associates

- Die wissentliche oder unwissentliche Akzeptanz einer Verlustwahrscheinlichkeit und möglichen Schadenhöhe.
- Risiko-Management durch:
 - Analyse
 - Vermeidung (nur bedingt möglich, ...)
 - Übertragung (Versicherung, Werkschutz, ...)
 - Begrenzung (präventive Massnahmen, ...)
 - Akzeptanz (formaler, dokumentierter Willensakt)
 - Ignoranz (wegschauen, ...)

Meist gibt es eine Mischung der Massnahmen, abhängig vom Risikotyp, der Risikokultur, den Kostenfolgen usw.

IT Sicherheit im Spannungsfeld

- “Die sicherste Bank hat keine Türen, aber auch keine Kunden” - IT-Sicherheit kann im Widerspruch zu Elementen der Geschäftstätigkeiten stehen.
- Auch bei einer funktionierenden Zusammenarbeit zwischen IT und Business kann es zu Zielkonflikten kommen, die systematisch gelöst werden müssen.
- Das Business trägt die abschliessende Verantwortung für Risiko-Entscheide.
- Die IT und die IT-Sicherheit müssen das Business wesentlich besser verstehen.

Zusammenfassung der Lektion 7

- Die Grundlagen der Vernetzung von Systemen über die Internet Protocol Suite /TCP/IP).
- Konkrete Konfiguration der Netzwerkschnittstelle.
- Zustand der Konfiguration der Netzwerkschnittstellen erkennen und Fehlersituationen erkennen / beheben.
- Typische Schwachstellen und Angriffsflächen eines Betriebssystems und seiner Umgebung.
- Typische Angriffsarten und deren Auswirkung auf das Gesamt-System.
- Mögliche technische, prozedurale und personelle Schutzmassnahmen und deren Wechselwirkung mit der Funktionalität und Leistungsfähigkeit des Betriebssystems.
- Hausaufgabe:
 - Repetieren Sie den Stoff dieser Lektion und erproben Sie die Kommandos zur Anzeige, Konfiguration und Überwachung der Netzwerkschnittstellen in ihrer Arbeits- und Heimnetzinfrastruktur.
 - Überprüfen Sie ihr eigenes Vorgehen bei der Sicherheitsüberprüfung, dem Einspielen von sicherheitsrelevanten Updates, der Nutzung von Anti-Malware-Software, dem Vorgehen bei Sicherheitsproblemen usw.