Sinn und Unsinn von Desktop-Firewalls

Wilhelm Dolle, Director Information Technology
interActive Systems GmbH

5. und 6. März 2005

Chemnitzer Linux-Tage

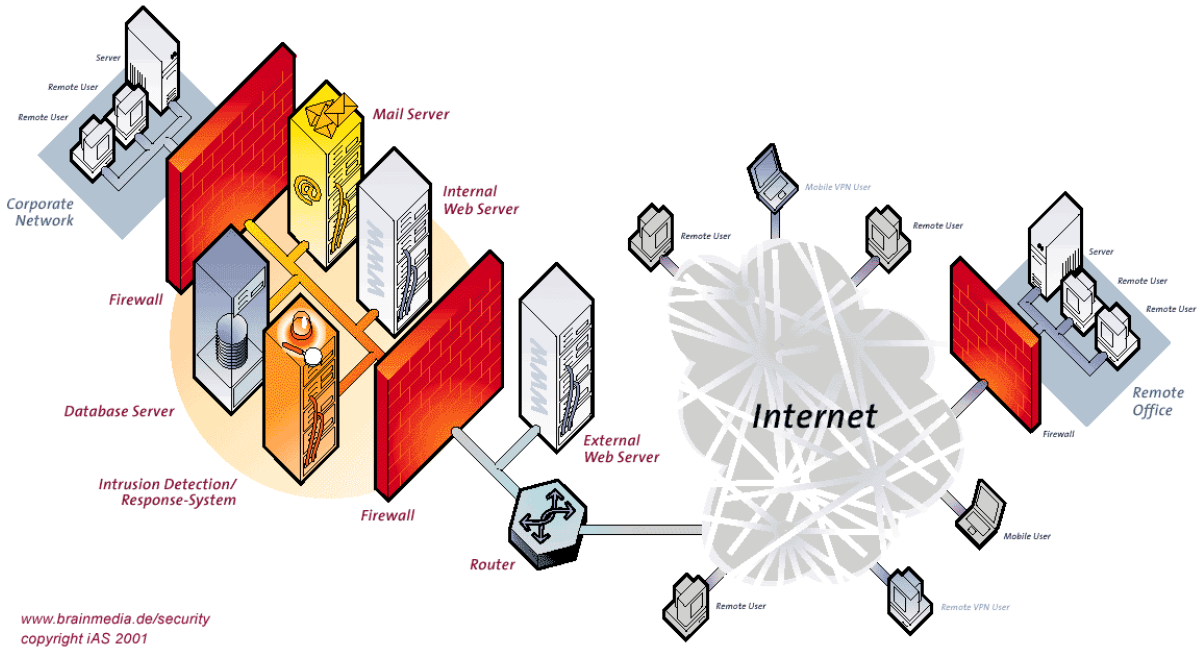
Agenda

- Was ist eine (Desktop-)Firewall?
- Netzwerk Grundlagen
- Versprechen von Desktop-Firewalls
- Beispiele unter Linux
- Angriffsvektoren
- Probleme
- Leistung in verschiedenen Szenarien / Fazit

Firewall

- Organisatorisches und technisches Konzept zur Trennung von Netzbereichen, dessen korrekte Umsetzung und dauerhafte Pflege

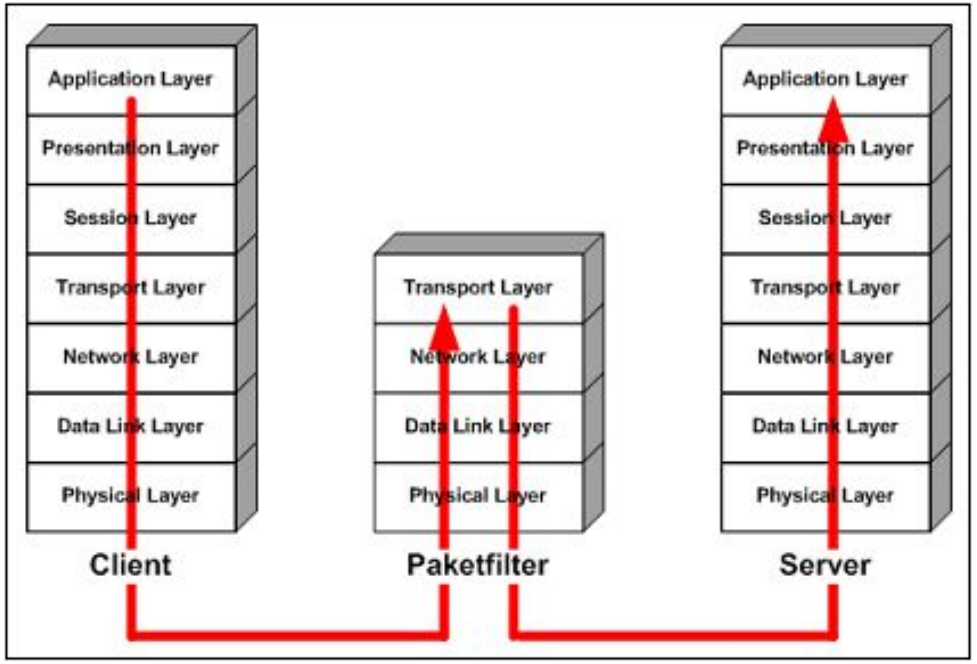
- Typische Umsetzung
  - Zwei Paketfilter
  - Grenznetz (DMZ)
  - Direkter Verkehr verboten
  - Proxys?



- Desktop-Firewall?

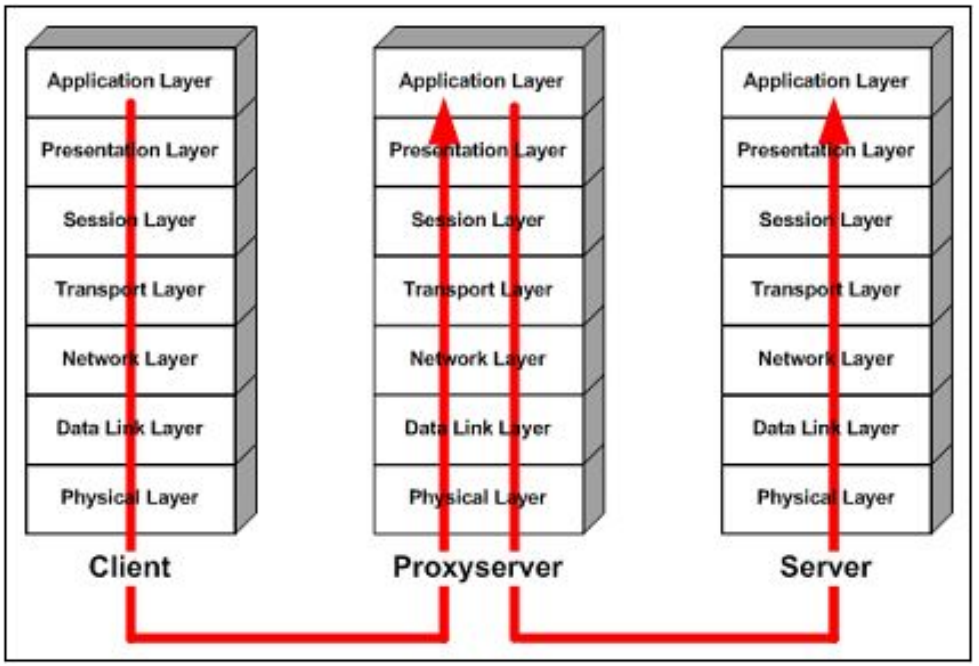
Paketfilter

- Reine Paketfilter arbeiten auf Layer 3 (Network) und 4 (Transport) des ISO/OSI Modells
- Sehen keine Applikationsdaten
- Pakete weiterleiten, verwerfen, zurückweisen, modifizieren oder mitloggen nach Kriterien wie
  - IP Quell- und Zieladresse
  - Protokoll
  - TCP/UDP Quell- und Zielport
  - ICMP-Typ
  - Fragmentierung
  - Zustand der Verbindung
  - ...

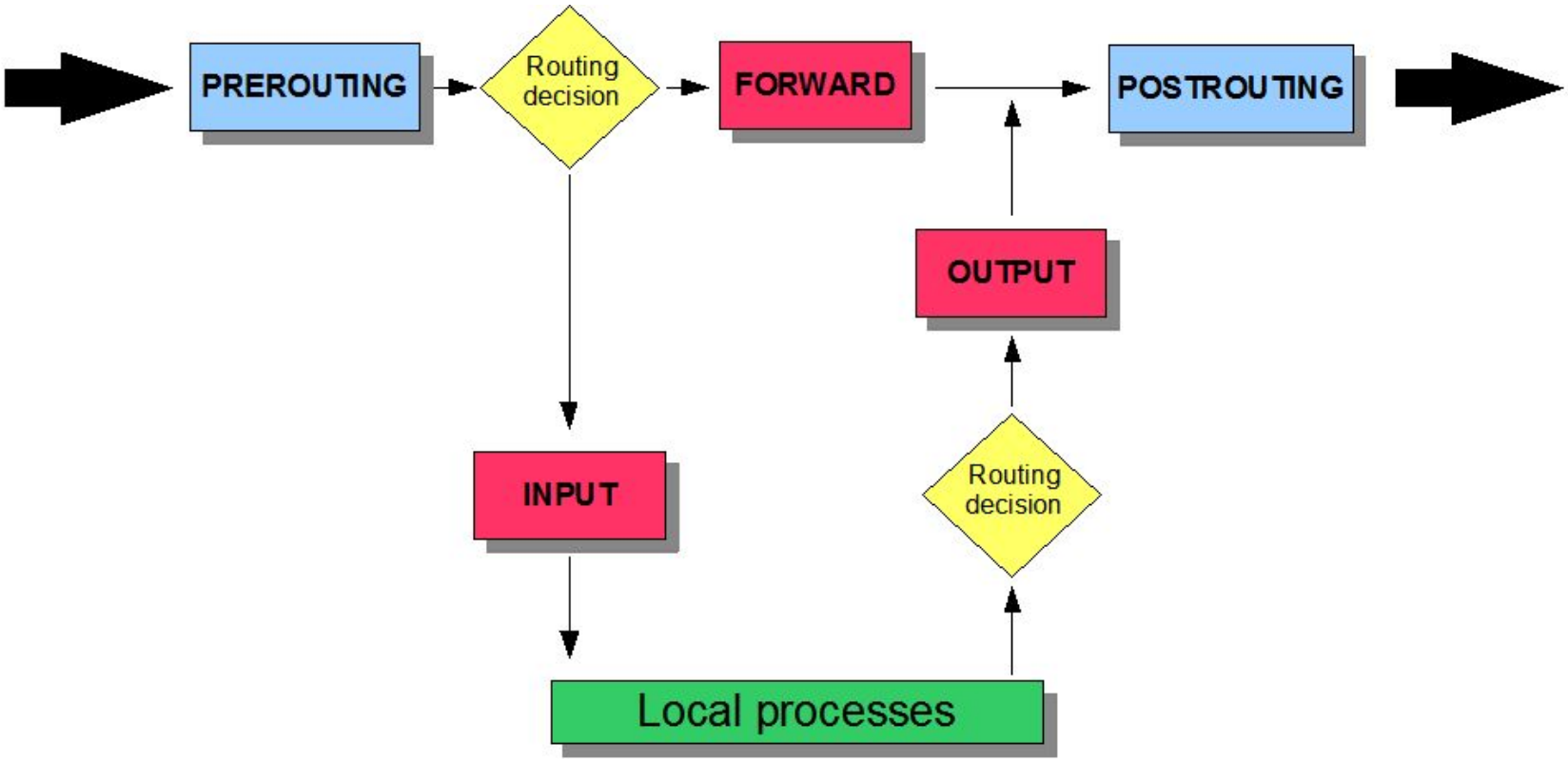


Proxys

- Proxys arbeiten auf Layer 5 bis 7 (Session, Presentation, Application) des ISO/OSI Modells
- Sehen Applikationsdaten
- Erweiterte Filtermöglichkeiten
- Logische Trennung der Netzbereiche (z.B. der Clients im LAN von den Servern im Internet)
- Einsatz auf Desktop-Firewalls?



Iptables / Netfilter



- REJECT: aktives Ablehnen (ICMP oder TCP-Reset)
- DROP: kommentarloses Verwerfen

Chemnitzer Linux-Tage

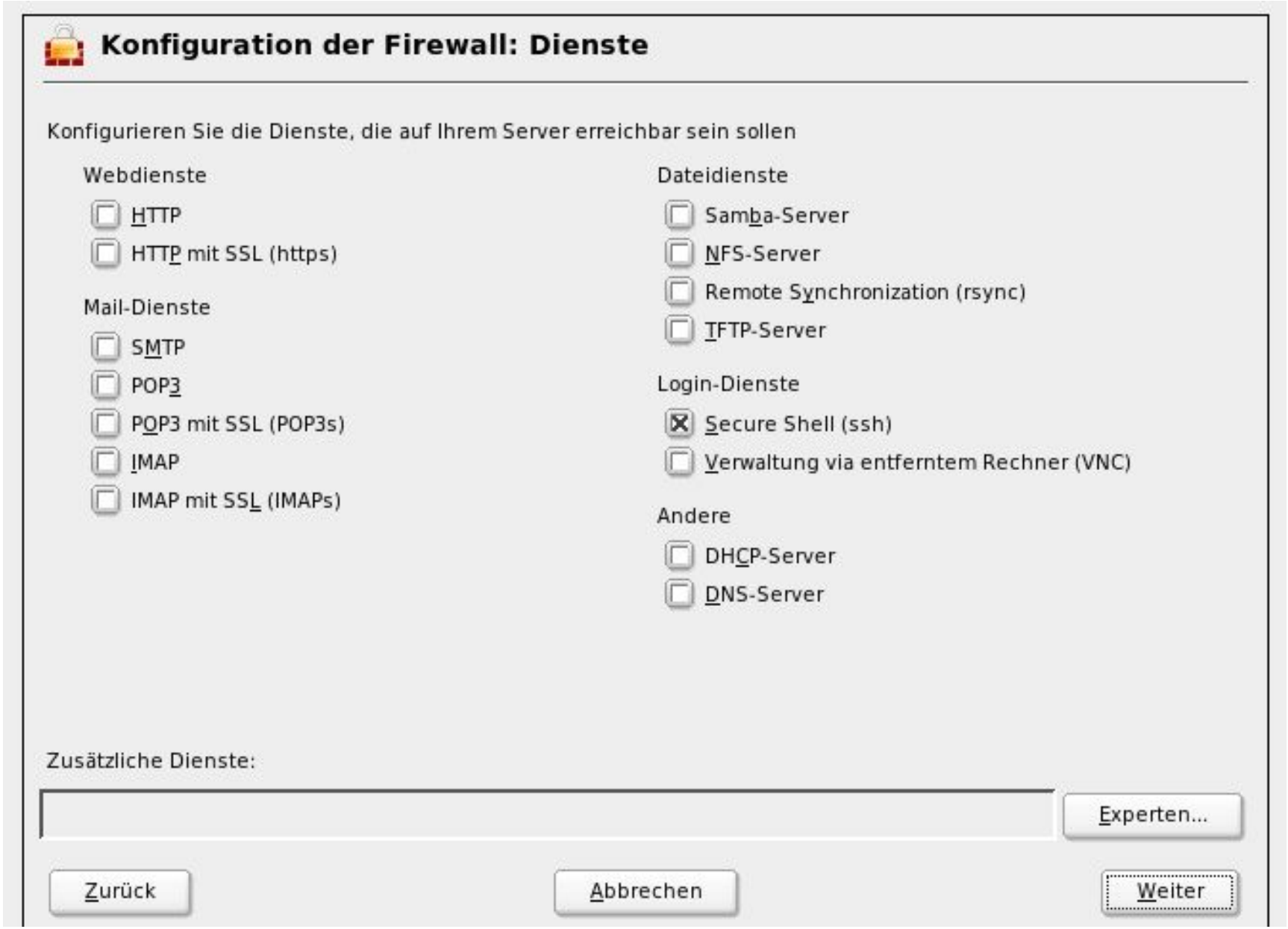
“Versprechen”

- Desktop-Firewall läuft (transparent) auf dem Rechner des Endanwenders
- Filtern von Netzverkehr auf Layer 3 und 4 (ein- und ausgehend) -> Paketfilter
- Filtern auf Anwendungsebene?
- “Verstecken” des Rechners?
- Datenschutz / Schutz der Privatsphäre?

Chemnitzer Linux-Tage

Fedora Core 3 Firewall

SuSE Firewall (SuSE 9.2)

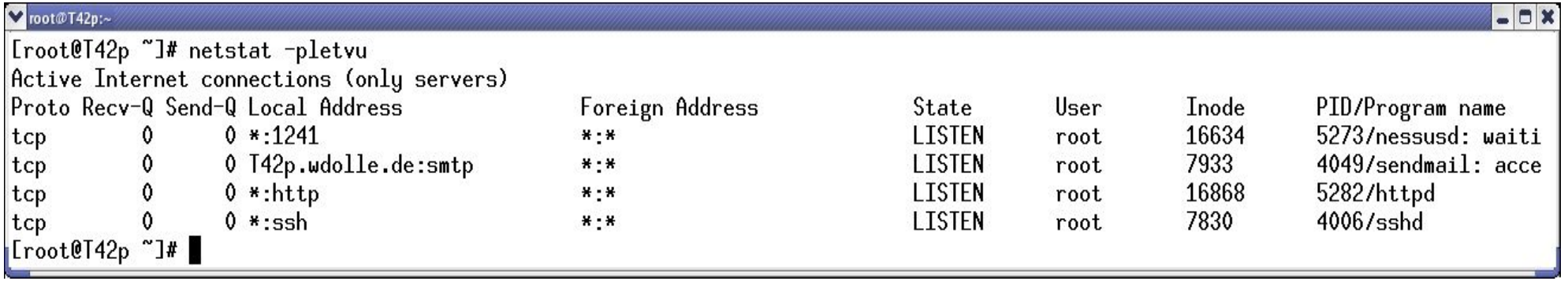


Angriffsvektoren

- Extern angebotene Dienste
  - Informationbeschaffung (Plattform, OS, Dienst, Version, ...)
  - Denial of Service
  - Einbruch ins System selber
- Ad-, Spy- oder Malware auf dem System selber
  - Gewünschte Programme mit “Zusatzfunktionen”
  - Viren, Würmer, trojanische Pferde
  - Rootkits
- Extern benutzte unsichere Protokolle
  - Informationsbeschaffung (vertrauliche Daten)
  - Übernehmen / Abbrechen der Verbindung
- **Der Benutzer selber!**

Extern angebotene Dienste

- Dienst durch Firewall nach extern blocken?
- Warum läuft der Dienst wenn ich ihn nicht anbieten möchte?
- Nur an benötigtes Interface binden



- Angriff, Portscan oder einfach Anfrage an einen Dienst?
  - False Positive (dynamische Adressen, ...)
  - False Negative
  - Automatische Reaktionen (kann zu DoS führen)?

Eingehender Verkehr (I)

- Firewall kann nicht verhindern das Sniffer, trojanische Pferde oder Rootkits Pakete von außen erhalten

```
root@T42p:~
[root@T42p ~]# iptables -L -v
Chain INPUT (policy ACCEPT 55 packets, 4620 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 53 packets, 4452 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@T42p ~]# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmnet1, link-type EN10MB (Ethernet), capture size 96 bytes
18:30:45.111229 IP 192.168.53.151 > 192.168.53.1: icmp 64: echo request seq 108
18:30:45.112793 IP 192.168.53.1 > 192.168.53.151: icmp 64: echo reply seq 108
18:30:47.441031 IP 192.168.53.151 > 192.168.53.1: icmp 64: echo request seq 109
18:30:47.441083 IP 192.168.53.1 > 192.168.53.151: icmp 64: echo reply seq 109

4 packets captured
4 packets received by filter
0 packets dropped by kernel
[root@T42p ~]#
```

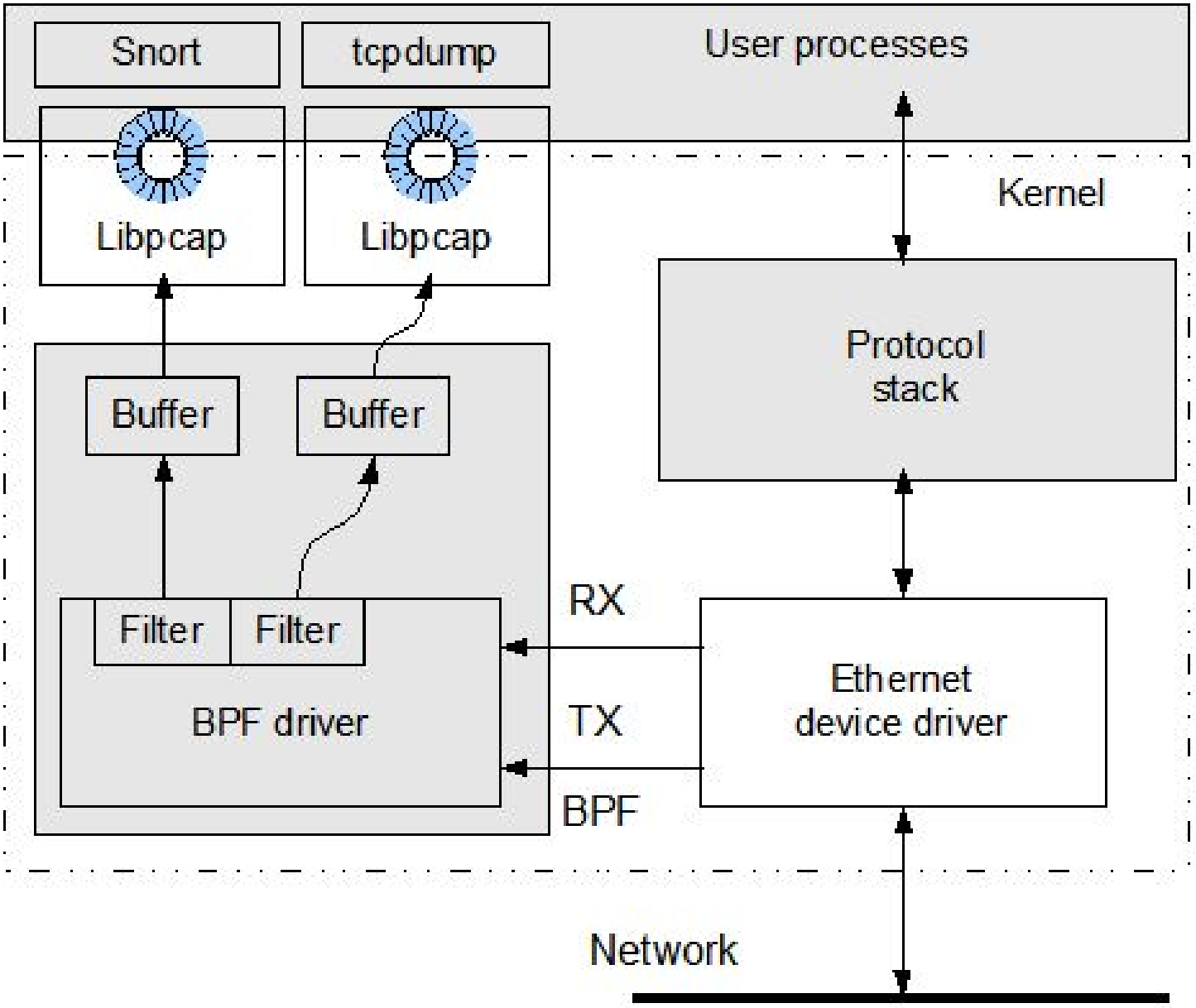
Eingehender Verkehr (II)

- Trotz Default Policy DROP können Sniffer den eingehenden Verkehr sehen

root@T42p:~

```
[root@T42p ~]# iptables -L -v
Chain INPUT (policy DROP 18 packets, 1657 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@T42p ~]# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmnet1, link-type EN10MB (Ethernet), capture size 96 bytes
18:33:24.640641 IP 192.168.53.151 > 192.168.53.1: icmp 64: echo request seq 185
18:33:26.970774 IP 192.168.53.151 > 192.168.53.1: icmp 64: echo request seq 186
18:33:29.283527 IP 192.168.53.151 > 192.168.53.1: icmp 64: echo request seq 187
18:33:31.606128 IP 192.168.53.151 > 192.168.53.1: icmp 64: echo request seq 188

4 packets captured
4 packets received by filter
0 packets dropped by kernel
[root@T42p ~]#
```

Eingehender Verkehr (III)



Ausgehender Verkehr

- Typische (Desktop-)Firewalls filtern den Verkehr nach außen nicht (Bequemlichkeit vor Sicherheit)

FC 3 Firewall Regeln

root@fc3-server:~

```
[root@fc3-server ~]# uname -a
Linux fc3-server.wdolle.de 2.6.9-1.667 #1 Tue Nov 2 14:41:25 EST 2004 i686 i686 i386 GNU/Linux
[root@fc3-server ~]# iptables -v -L
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   18  1852 RH-Firewall-1-INPUT  all  --  any    any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 RH-Firewall-1-INPUT  all  --  any    any     anywhere             anywhere

Chain OUTPUT (policy ACCEPT 20 packets, 1512 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain RH-Firewall-1-INPUT (2 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
   18  1852 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp any
    0     0 ACCEPT     ipv6-crypt--  any    any     anywhere             anywhere
    0     0 ACCEPT     ipv6-auth--  any    any     anywhere             anywhere
    0     0 ACCEPT     udp  --  any    any     anywhere             224.0.0.251         udp dpt:5353
    0     0 ACCEPT     udp  --  any    any     anywhere             anywhere            udp dpt:ipp
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere            state NEW tcp dpt:ssh
    0     0 REJECT     all  --  any    any     anywhere             anywhere            reject-with icmp-host-prohibited
[root@fc3-server ~]#
```

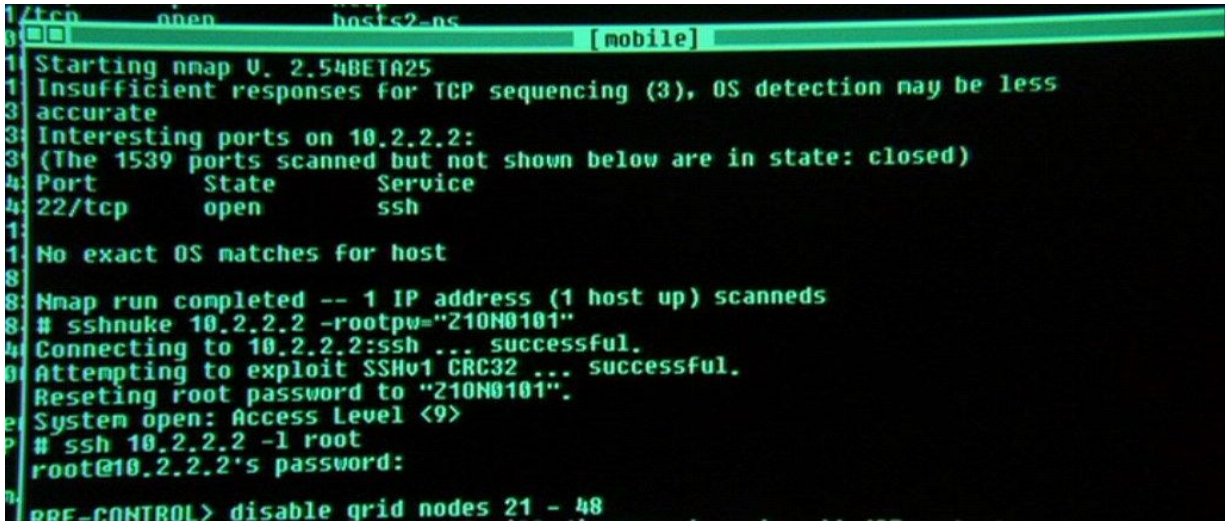
SuSE Firewall Regeln

wd@suse92:~ - Befehlsfenster - Konsole

```
suse92:~ # uname -a
Linux suse92 2.6.8-24-default #1 Wed Oct 6 09:16:23 UTC 2004 i686 i686 i386 GNU/Linux
suse92:~ # iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   40  2608 ACCEPT     all  --  lo     any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED
    1    88 input_ext  all  --  eth0   any     anywhere             anywhere
    0     0 LOG        all  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 LOG level w
arning tcp-options ip-options prefix `SFW2-IN-ILL-TARGET '
    0     0 DROP       all  --  any    any     anywhere             anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   40  2608 ACCEPT     all  --  any    lo      anywhere             anywhere
    0     0 LOG        icmp --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 icmp time-e
xceeded LOG level warning tcp-options ip-options prefix `SFW2-OUT-TRACERT-ATTEMPT '
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp time-exceeded
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp port-unreachable
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp fragmentation-needed
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp network-prohibited
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp host-prohibited
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp communication-prohibited
    0     0 DROP       icmp --  any    any     anywhere             anywhere            icmp destination-unreachable
    1    60 ACCEPT     all  --  any    any     anywhere             anywhere            state NEW,RELATED,ESTABLISHED
    0     0 LOG        all  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 LOG level w
arning tcp-options ip-options prefix `SFW2-OUT-ERROR '
```

Nmap

- Erstes Release: Phrack Magazine Volume 7, Issue 51 September 1997
- Autor: Fyodor
- Aktuell: 3.75
- Lizenz: GNU GPL 2



- Features um Netzwerke zu „mappen“:
  - Port Scanning (UDP und TCP)
  - Betriebssystemerkennung
  - Versionserkennung
  - Läuft auf Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, ...

Nmap Optionen

```
root@T42p:~
[root@T42p ~]# nmap
Nmap 3.75 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service & app names/versions
  -sR RPC scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: 1-1024,1080,6666,31337
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
[root@T42p ~]#
```

Chemnitzer Linux-Tage

TCP Connect Scan

- Versuch eines „normalen Verbindungsaufbaus“
  - Scanner: SYN senden
  - Ziel: SYN/ACK (Port offen) oder RST/ACK (Port geschlossen)
  - Scanner: ACK senden

- Paketfilter:
  - DROP/DENY: Timeout
  - ICMP Dest. Unrechable
  - RST: False Negativ

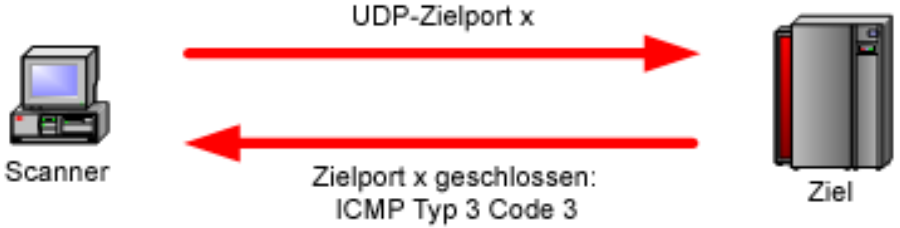
- Leicht zu implementieren durch Std. Calls (socket(), connect(), ...)
- Keine root-Rechte notwendig
- False Negative nur bei Paketfiltern, keine False Positives
- Sehr schnell

TCP SYN Scan (half open)

- Verbindung wird nicht vollständig aufgebaut
  - Scanner: SYN senden
  - Ziel: SYN/ACK (Port offen) oder RST/ACK (Port geschlossen)
  - Scanner: RST/ACK senden
- Zustand der Verbindung geht nicht über das halboffene Stadium hinaus
- Root-Rechte notwendig, da am TCP-Stack des Betriebssystems vorbei implementiert werden muss

UDP Scan

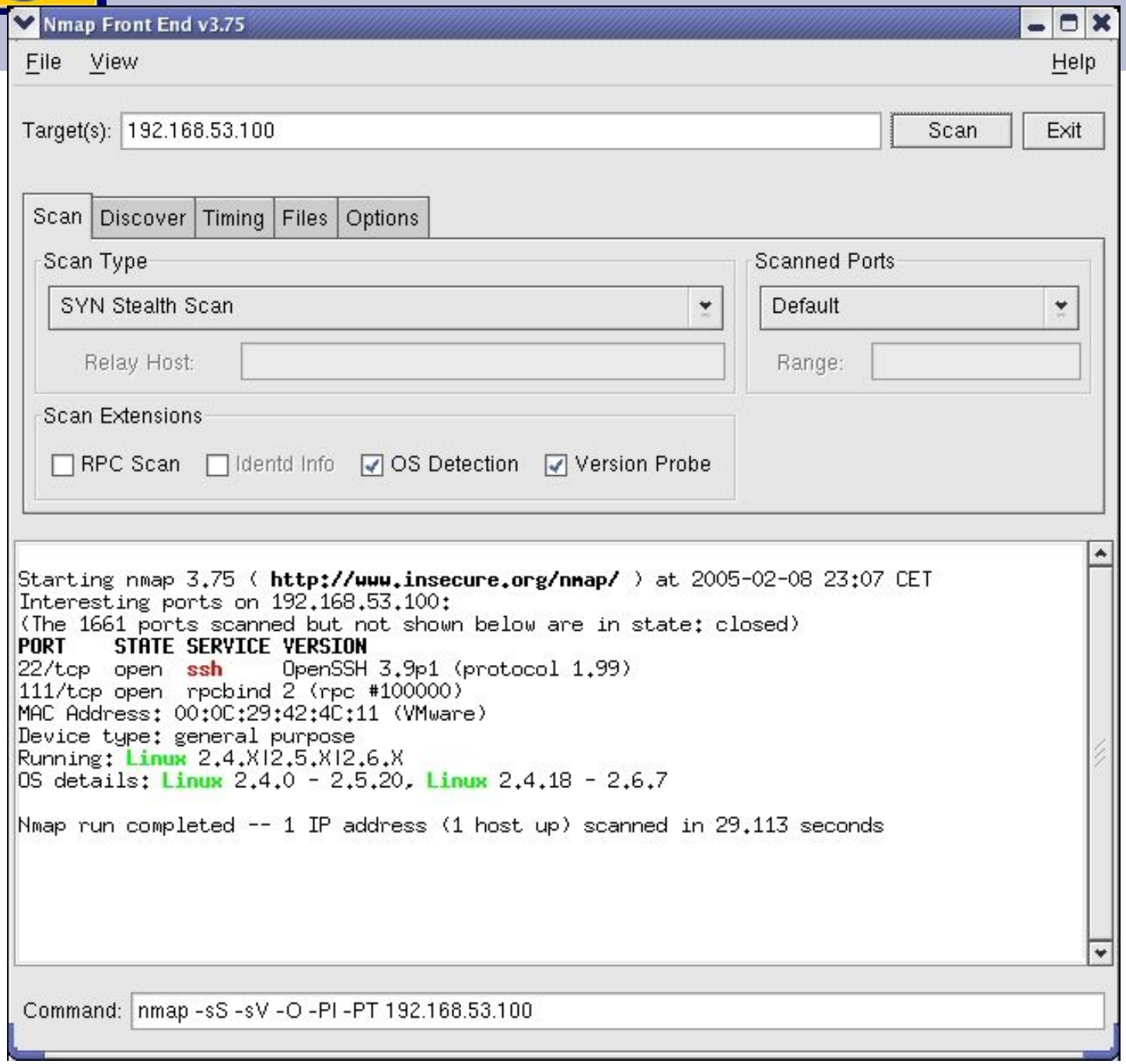
- Vorgehen:
  - Scanner: UDP-Paket an einen bestimmten Port
  - Ziel: ICMP Destination Unreachable, Port Unreachable (Type 3, Code 3) wenn Port geschlossen oder Paket wird verworfen wenn der Port offen ist



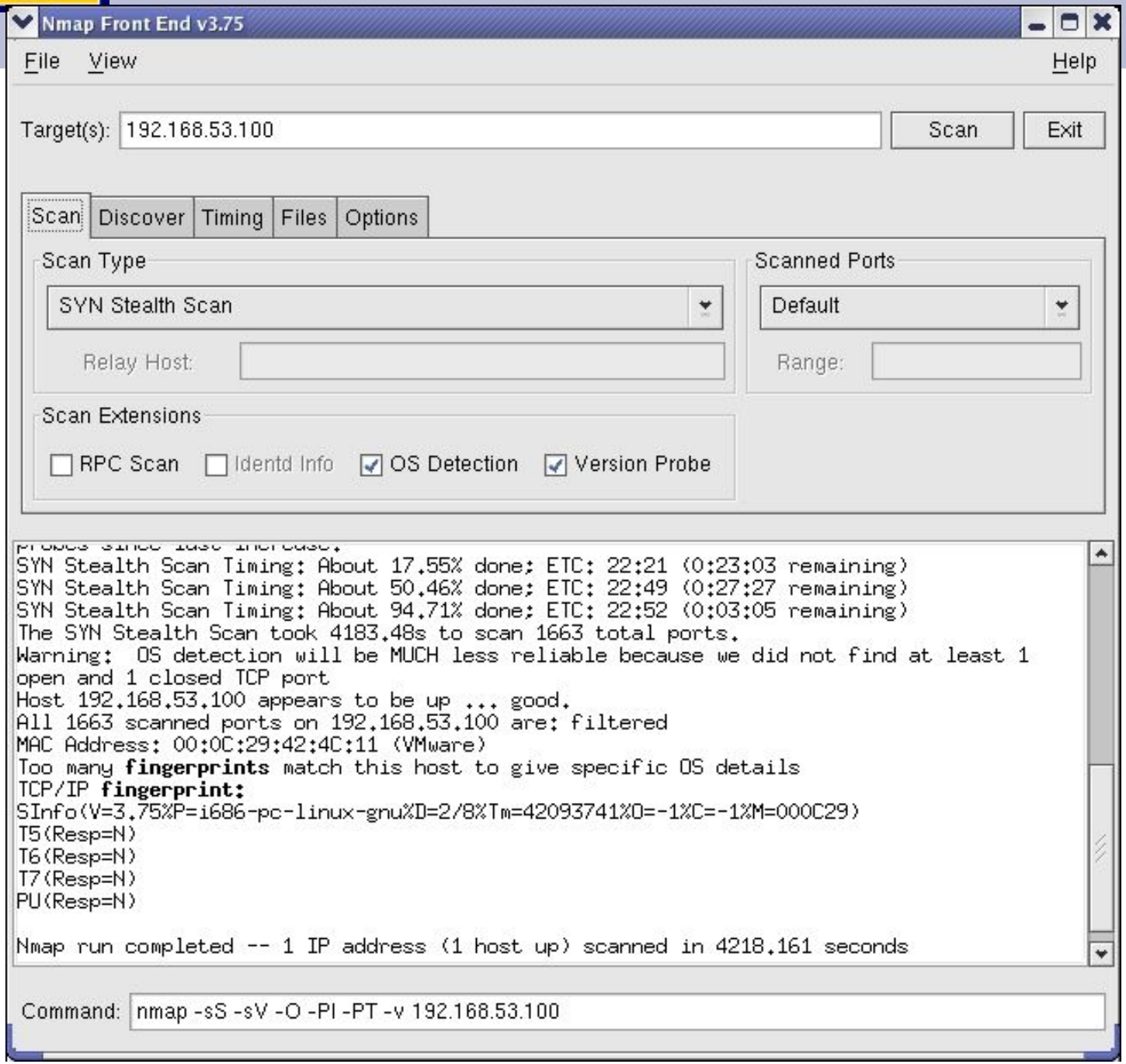
- Große Gefahr für False Positive durch Paketverlust oder DROP/DENY durch Paketfilter

- Vergleichsweise langsam (im Vergleich zu TCP Scans) wegen ICMP Rate Limits

NmapFE (FC3 ohne FW)



NmapFE (FC3 mit FW)



Fedora Core 3 FW / ICMP

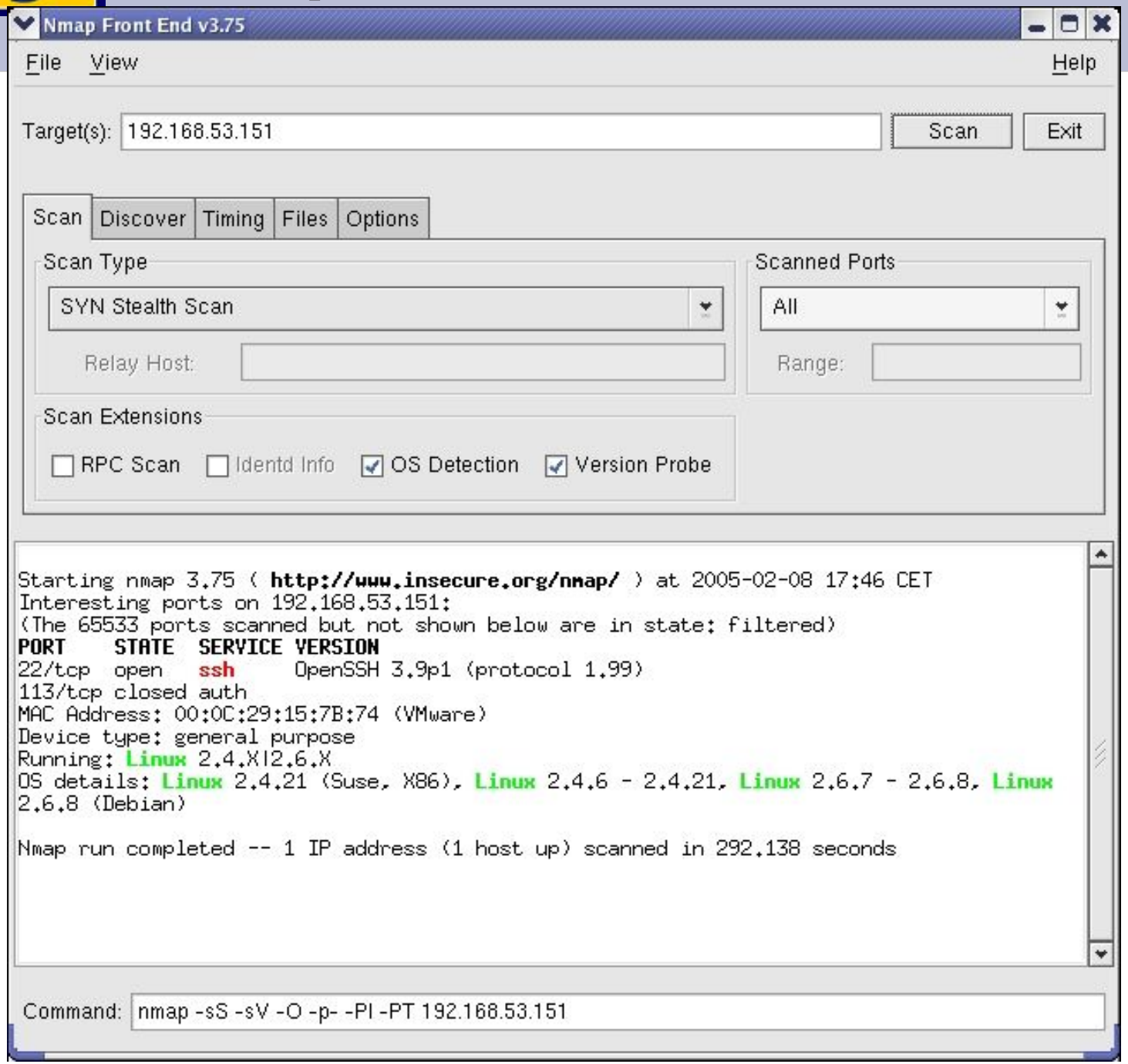
root@fc3-server:~

```
[root@fc3-server ~]# uname -a
Linux fc3-server.wdolle.de 2.6.9-1.667 #1 Tue Nov 2 14:41:25 EST 2004 i686 i686 i386 GNU/Linux
[root@fc3-server ~]# iptables -v -L
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   18  1852 RH-Firewall-1-INPUT  all  --  any    any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 RH-Firewall-1-INPUT  all  --  any    any     anywhere             anywhere

Chain OUTPUT (policy ACCEPT 20 packets, 1512 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain RH-Firewall-1-INPUT (2 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
   18  1852 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp any
    0     0 ACCEPT     ipv6-crypt--  any    any     anywhere             anywhere
    0     0 ACCEPT     ipv6-auth--  any    any     anywhere             anywhere
    0     0 ACCEPT     udp  --  any    any     anywhere             224.0.0.251         udp dpt:5353
    0     0 ACCEPT     udp  --  any    any     anywhere             anywhere            udp dpt:ipp
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere            state NEW tcp dpt:ssh
    0     0 REJECT     all  --  any    any     anywhere             anywhere            reject-with icmp-host-prohibited
[root@fc3-server ~]#
```

root@T42p:~

```
[root@T42p ~]# cat /proc/sys/net/ipv4/icmp_ratelimit
1000
[root@T42p ~]# cat /proc/sys/net/ipv4/icmp_ratemask
6168
[root@T42p ~]#
```

NmapFE (SuSE 9.2 mit FW)



SuSE 9.2 FW / TCP RST

wd@suse92:~ - Befehlsfenster - Konsole

```
Chain reject_func (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     tcp  --  any    any     anywhere             anywhere            reject-with tcp-reset
    0     0 REJECT     udp  --  any    any     anywhere             anywhere            reject-with icmp-port-unreachable
    0     0 REJECT     all  --  any    any     anywhere             anywhere            reject-with icmp-proto-unreachable
suse92:~ #
```

Sinnvolle Szenarien / Fazit

- Benutzer davon abhalten Ports nach außen zu öffnen
  - Durchsetzen von Sicherheits-Policies
  - Testen von neuer Software
  - Unbedarfte Benutzer
- Dienste auf notwendige Interfaces beschränken
- Für höhere Sicherheit auch ausgehenden Verkehr regeln
  - Erkennen von ungewünschter Kommunikation
  - Trotzdem Kommunikation via Standard-Ports möglich (80, 443, 25, 53, ...)
- “Schutz” vor Port- bzw. Verwundbarkeits-Scannern?
- Datenschutz und Schutz der Privatsphäre durch Krytographie

Chemnitzer Linux-Tage

Fragen?

Vielen Dank für die Aufmerksamkeit

Wilhelm Dolle, CISA, CISSP, BSI IT-Grundschutz-Auditor
Director Information Technology

iAS interActive Systems GmbH
Dieffenbachstrasse 33c
D-10967 Berlin

phone +49-(0)30-69004-100
fax +49-(0)30-69004-101
mail wilhelm.dolle@interActive-Systems.de
web http://www.interActive-Systems.de