

<i>BAI4-RNP</i>	<i>Praktikum Rechnernetze</i> <small>SS 14/15</small>	<i>HBN/SLZ</i>
WS15/16	Aufgabe 4: Firewalling, Routing, Sniffing	Seite 1 von 3

1 Vorbemerkungen

- Die beteiligten Rechner müssen mit der Linux-Partition "[*BRV-Special*](#)" gestartet werden, da zur Durchführung dieser Aufgabe z.T. administrative Rechte erforderlich sind (vgl. Hinweise unten). Ausserdem muss der Netzwerkschrank im Raum 765 eingeschaltet sein.
- In Raum 765 gibt es neben dem Hochschulnetz (141.22.26.0/23) zwei laborinterne Netze: 192.168.17.0/24 bzw. 192.168.18.0/24 und 172.16.1.0/24, siehe [Netzwerkplan](#).
- Sie brauchen grundsätzlich zwei Rechner. Dazu gibt es eine [Gegenstellenzuordnung](#).
- Bei der Fehlersuche kann es nützlich sein, auf den beteiligten Rechnern den Netzwerkverkehr mit dem Sniffer (*wireshark*) aufzuzeichnen.
- Es wird erwartet, dass Sie sich **vor** dem Praktikum mit den hier verwendeten Werkzeugen vertraut gemacht haben. ([Public-Bereich: Kurzvorstellung der Werkzeuge](#), [Manual Pages](#), [iptables-Tutorial](#).)
- Zur Abnahme ist ein Protokoll vorzulegen, aus dem der Lösungsweg nachzuvollziehen ist.

2 Netzwerkanalysertools

Starten Sie Ihren Server aus Aufgabe 2/3 mit dem Port 9400 (alternativ: TCP-Server auf *socat*-Basis). Falls dies nicht funktioniert, soll die genaue Ursache (Prozess) zu ermittelt werden!

3 Paketfilterung (Firewalling)

Der Paketfilter wird mit dem Befehl *iptables* konfiguriert. Grundsätzlich kann eine Filterung zustandslos (*stateless*) oder zustandsorientiert (*stateful*) erfolgen.

Für die nachstehenden Szenarien ist jeweils ein Shellskript mit allen notwendigen Kommandos anzulegen, sodass die jeweilige Firewallkonfiguration jederzeit hergestellt werden kann.

Achten Sie auf Vollständigkeit Ihrer Regeln, auch bezüglich der Policies!

→ *In nachfolgenden Fällen sollen die nicht genannten Netze voll zugänglich bleiben!*

→ *Im Netz 172.16.1.0/24 gibt es keine Namensauflösung (DNS)!*

- a) Auf einem Ihrer beiden Rechner soll der Zugang vom und zum Netzwerk 172.16.1.0/24 vollständig gesperrt werden.
- b) Stellen Sie die Firewall des Rechners so ein, dass dort über das Netz 172.16.1.0/24 nur ein TCP-Server (z.B. aus Aufgabe 2/3) auf Port 51000 genutzt werden kann. Alle anderen Verbindungen über dieses Netz sollen gesperrt sein.
- c) Konfigurieren Sie den Rechner so, dass man keine TCP-Server auf diesem Rechner über

<i>BAI4-RNP</i>	<i>Praktikum Rechnernetze</i> <small>10.4.02/20</small>	<i>HBN/SLZ</i>
WS15/16	Aufgabe 4: Firewalling, Routing, Sniffing	Seite 2 von 3

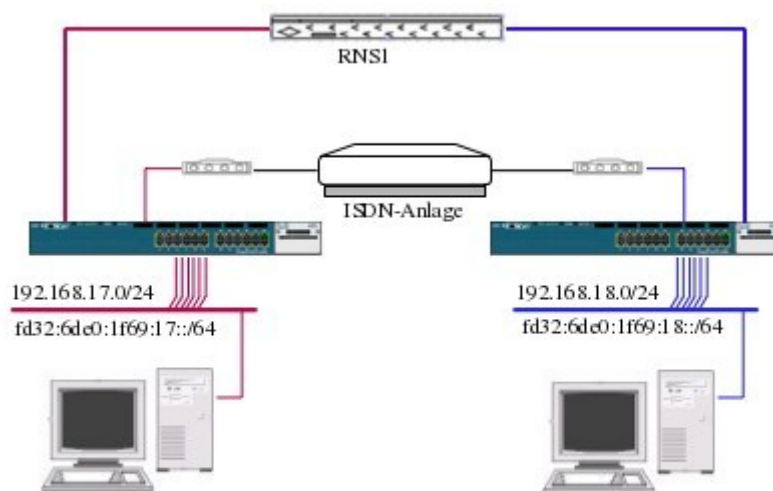
das Netz 172.16.1.0/24 ansprechen kann. Alle anderen Verbindungen über dieses Netz sollen dagegen möglich sein.

- d) Stellen Sie die Firewall Ihres Rechners so ein, dass von dort ein *ping* auf andere Rechner/Geräte im Netz 172.16.1.0/24 möglich ist, nicht aber umgekehrt!

Wichtiger Hinweis: Nach kollektivem Löschen aller Regeln (Option *-F*), sind die Filesysteme hinter "My Home" und "Public" nicht mehr erreichbar. In diesem Fall müssen Sie – zusätzlich zu Ihren anderen Regeln – den Datenverkehr mit dem DNS-Server (141.22.192.100), dem Fileserver (*filercpt.informatik.haw-hamburg.de*) und auch Ihrem lokalen Rechner (*localhost*) explizit freigeben! (U.a. wird *localhost* von der Fensteroberfläche benutzt!)

4 Routing

Das interne **192er** Netz besteht aus zwei Subnetzen. Ihre beiden Rechner befinden sich in unterschiedlichen Subnetzen. Die beiden Subnetze sind physikalisch über zwei Wege verbunden: Über einen Router und über eine ISDN-Anlage.



Auszug Netzwerkplan

Konfigurieren Sie Ihre Rechner so, dass Sie den jeweils anderen Rechner im anderen Subnetz erreichen können. (Prüfung mit dem *ping*-Befehl). Dabei soll der Netzwerkverkehr zwischen diesen Rechnern entweder über den Router oder über die ISDN-Anlage laufen. Im Fall des Routers soll dies sowohl für IPv4 als auch für IPv6 eingestellt werden.

Was passiert, wenn Sie beim Weg über die ISDN-Anlage ein *ping* mit der Paketgröße 1000 Byte durchführen? (Beobachtung im Sniffer und/oder Standardausgabe von *ping*)

BAI4-RNP	Praktikum Rechnernetze <small>11.04.02/2016</small>	HBN/SLZ
WS15/16	Aufgabe 4: Firewalling, Routing, Sniffing	Seite 3 von 3

5 Erweitertes Netzwerk-Sniffing und Firewalling



- Starten Sie einen Browser und zeichnen Sie mit *Wireshark* den Netzwerkverkehr auf, während Sie die Homepage www.dmi.dk besuchen. (Achtung - währenddessen dürfen keine weiteren Internet-Sitzungen laufen!). Von welchen anderen Web-Servern werden bei dieser Sitzung automatisch ohne Zutun des Benutzers zusätzlich Seiten angefordert? (→ *Statistik* des Sniffers einsetzen!)
- Stellen Sie die Firewall so ein, dass über HTTP nur der Server www.dmi.dk erreicht werden kann, nicht aber die Web-Server der fremden Seiten!
Hinweise: Um Wartezeiten wegen Timeouts zu vermeiden, kann die *tcp-reset* - Option eingesetzt werden. Alle andere Protokolle, insbesondere zum Zugriff auf den DNS-Server und den Fileserver (Home-Verzeichnis!) sollen von der Filterung unberührt bleiben.
- Was ist zu beachten, wenn sich nach dem Einstellen von b) später die IP-Adresse des Servers www.dmi.dk ändert?

Hinweise

Sie benötigen u.a. die Programme ***ip***, ***iptables***, ***ping/ping6***, ***route*** und ***wireshark***, für die (ausser *ping/ping6*) in der Regel administrative Rechte notwendig sind. Dazu müssen diese mit dem ***sudo***-Kommando gestartet werden!

Beispiel : ***sudo*** /usr/sbin/iptables -F

Das *sudo*-Kommando ist nur für ausgewählte Programme zugelassen. Eigene Programme und Shellskripte können nicht mit *sudo* gestartet werden!

Informationen zu den o.g. Programmen finden Sie in [diesem Dokument](#) ( / ) im [Public-Bereich](#) sowie in den [Manual-Pages](#). Zu *Wireshark* gibt es auch einen [Short Guide](#).

Die Programme *iptables* und *route* führen defaultmässig eine Namensauflösung durch, die jedoch scheitert, wenn kein DNS-Server erreichbar ist. Dann erfolgt nach Ablauf des Timeouts eine Ausgabe mit Adressen statt Namen. Die Namensauflösung kann mit der Option *-n* ausgeschaltet werden.

Die Originaleinstellungen der Firewall können mit dem Kommando

```
sudo /sbin/rcSuSEfirewall12 restart
```

wiederhergestellt werden.