

## 6.5 Praktische Aufgaben

### 6.5.1 Topologie

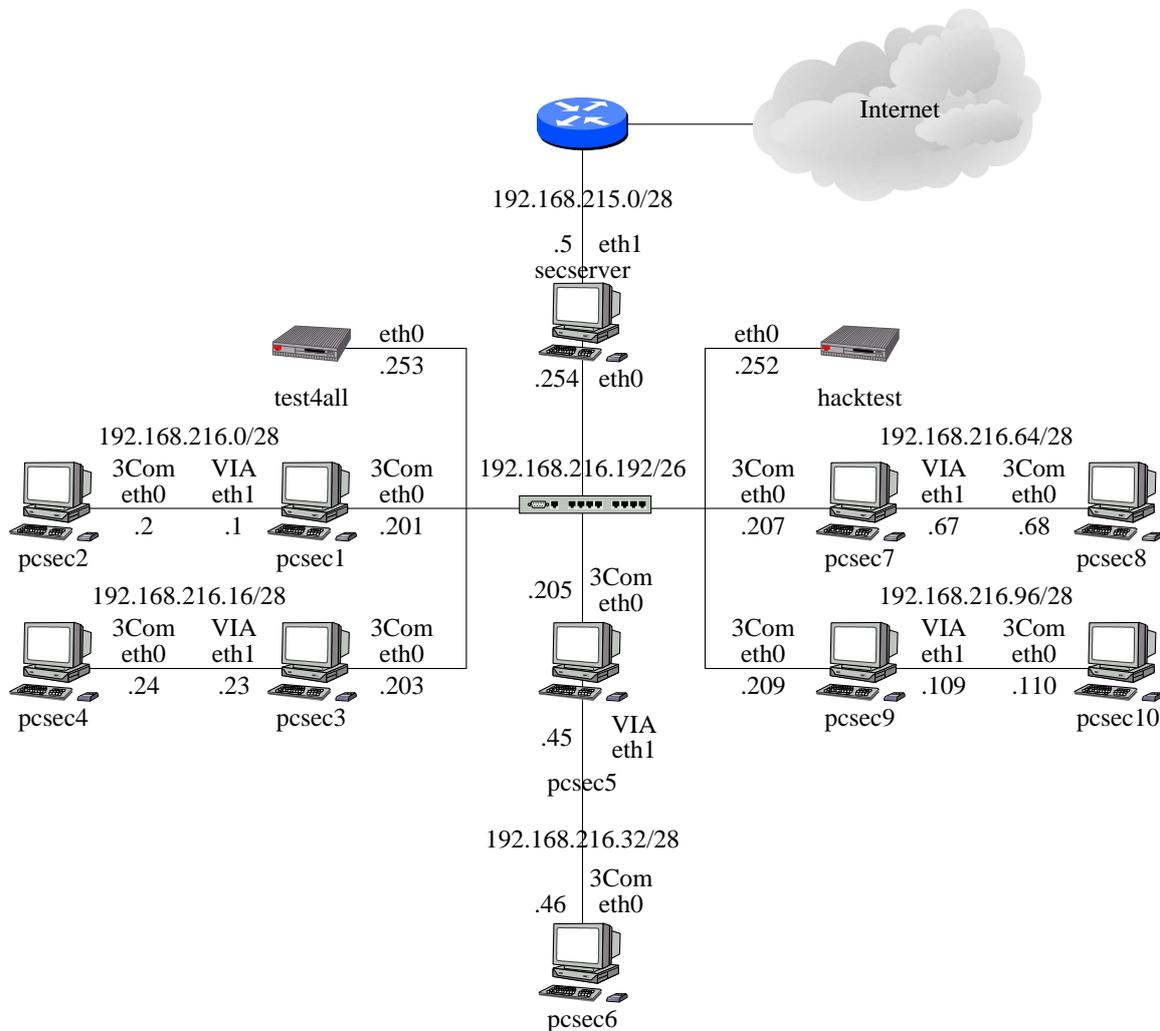


Abbildung 64: Der Versuchsaufbau für die weiteren Versuche des Praktikums

### 6.5.2 Konfiguration Bind

1. Installieren Sie über YaST2 das Softwarepaket BIND 8 vom Installserver. Nach der Installation finden Sie das Nameserverbinary unter `/usr/sbin/named`, die Konfigurationsfiles unter `/var/named/`. Die Dienste werden bei Suse über den YaST2 konfiguriert, um beim Booten gestartet zu werden. Dabei werden Links von den Runlevelverzeichnissen

- /etc/init.d/rc0.d
- /etc/init.d/rc1.d
- /etc/init.d/rc2.d
- /etc/init.d/rc3.d
- /etc/init.d/rc4.d
- /etc/init.d/rc5.d
- /etc/init.d/rc6.d
- /etc/init.d/rcS.d

die im Startscript `/etc/init.d/named` angegeben sind, auf das zu startende Startfile gelegt.

2. Was sehen Sie mit `netstat -an` und wie ist das zu interpretieren (Informationen über Manpage und / oder Internet)?
3. Ihr Nameserver soll folgende Eigenschaften erfüllen:
  - (a) Der Daemon soll auf das Produktivinterface `eth0` hören. Nach einem Neustart des Dienstes durch das Startscript überprüfen Sie mit `netstat -an` und `telnet IP-Adresse 53` und anhand des Logfiles, ob Ihre Konfiguration erfolgreich war.
  - (b) Für die Domain `secp.nm.informatik.uni-muenchen.de` ist der `pcsec4` als Master zuständig, für die Reverse-Zonen unseres Netzbereichs `192.168.216.0/24` ist der `pcsec10` als Master zu konfigurieren. Alle anderen sind Slave für diese Zonen. Übrprüfen Sie Ihre Konfiguration anhand der Logfiles und mittels Zonentransfers: `host -l -a secp.nm.informatik.uni-muenchen.de ip-adresse-nameserver`. Namensgebung: z.B. `pcsec1 (192.168.216.201)`, `pcsec1-eth1 (192.168.216.1)` und so weiter.
  - (c) Für `uni-muenchen.de` verweisen Sie auf `test4all`. Somit ist der `test4all` für diese Domain als Forwarder einzutragen. Überprüfen Sie Ihre Konfiguration wieder anhand der Logfiles und mit den bereits bekannten Tools `host`, `dig` und / oder `nslookup`.
  - (d) Zonentransfer soll nur von der IP-Adresse des `secservers (192.168.216.254)` und Ihres Partnerrechner erlaubt sein. Was hat das für Konsequenzen bzgl. der Masterzonen? Was ist hier zu beachten (siehe Seite 162)?
  - (e) DNS Queries sollen nur von der eigenen Maschine und dem `secserver` erlaubt sein. Überprüfung mittels `nslookup` Abfragen. Welche Konsequenzen hat das für die Zonen, für die man Master oder Slave ist? Was ist hier zu beachten und an der Konfiguration zu ändern? (Siehe auch Seite 162 und in den im Literaturverzeichnis angegebenen Quellen).
  - (f) Für alle anderen Anfragen ist der `secserver` als Forwarder einzutragen. D.h. es ist so zu verfahren, wie auf Seite 158 beschrieben ist.

4. Tragen Sie Ihren Nameserver in die `/etc/resolv.conf` ein. Welche Auswirkungen hat das?
5. Überprüfen Sie im Logfile, ob Ihr Nameserver korrekt starten konnte und dokumentieren Sie das in Ihrer Ausarbeitung.
6. Überprüfen Sie die Funktionalität Ihres Nameservers mit `host` und `nslookup` und dokumentieren Sie das in Ihrer Ausarbeitung.

Weitere Informationen zu den Befehlen `host`, `dig` und `nslookup` finden Sie in den Manpages.

### 6.5.3 Übungen zu Telnet und SSH

1. Stoppen Sie alle verfügbaren Dienste und testen Sie das Ergebnis mit `nmap`. Was sehen Sie? Aktivieren Sie zur Zeit nur Ihren Nameserver. Was sehen Sie mit `nmap`?
2. Starten Sie Telnet so, daß er vom `tcpwrapper` und `inetd` kontrolliert wird und sich User nur von der IP-Adresse Ihres Partnerrechners und vom `secservice` einloggen können.
3. Installieren Sie den SSH Daemon und konfigurieren Sie ihn so, daß er nur auf Ihrem Interface `eth0` hört und nur von Ihrem Partnerrechner und dem `secservice` aus angesprochen werden kann. Wie können Sie die Richtigkeit Ihrer Konfiguration überprüfen? Was sehen Sie, wenn Sie mit `nmap` alle Ihre Interface anschauen? Was sehen Sie mit `netstat -an` und wie ist das zu interpretieren?
4. Verfolgen Sie mittels Programmen zum Netzsniffen sowohl eine Telnet, wie auch eine SSH Verbindung. Wenn Sie eine SSH Sitzung mittels `tcpdump` mitsniffen, was ist der Unterschied zu Telnet?

Informationen zu `nmap`, `tcpd`, `inetd` und so weiter finden Sie in den Manpages.