MNM
TEAM
Munich Network Management Team

Ludwig-Maximilians-Universität München
und Technische Universität München
Prof. Dr. H.-G. Hegering

Praktikum IT-Sicherheit
Übungsblatt 01

1. Vorbereitungen

(a) Richten Sie auf ihrem Arbeitsrechner sowohl OpenVPN als auch SSH ein. Unter Windows ist zudem die Unixemulation Cygwin bzw. CygwinX hilfreich. Hilfe hierzu finden sie auf den entsprechenden Projektseiten.

(b) Verbinden Sie sich mit ihrem Rechner im Praktikumsnetz und melden Sie sich an. Ändern Sie das root Passwort ihrer Maschine, legen Sie einen zusätzlichen Benutzer namens `secpgast` an und teilen Sie ihrem Partner das Passwort für diesen Account mit.

2. IP-Adressen und Netzmasken

(a) Bestimmen Sie für die Netze des Versuchsaufbaues aus Abbildung 1 die in den Netzen verwendbaren IP-Adressen und die Broadcast-Adresse.

(b) Welche kleinst mögliche Netzadress/Netzmasken-Kombination beinhaltet alle IP-Adressen der internen Netze (ohne Managementnetz)?

3. Konfiguration der Netzwerkkarten

(a) Lassen Sie sich die ARP- (`man arp`) und die Routing-Tabelle (`man netstat`) sowie die Liste aller konfigurierten Interfaces (`man ifconfig`) Ihres Rechners anzeigen.

(b) Nennen Sie ein Beispiel für die praktische Verwendung des Loopback-Interfaces.

(c) Konfigurieren Sie nun die Netzwerkkarte(n) Ihres Rechners. Die Rechner sind mit zwei bzw. drei unterschiedlichen Karten ausgerüstet. Welche der Karten Sie wie konfigurieren müssen entnehmen Sie bitte Abbildung 1.

Hinweis:
Kopieren Sie das Template `/etc/sysconfig/network/ifcfg.template` zur Konfiguration der Netzwerkkarte (z.B. `eth1`) nach `ifcfg-eth1` im selben Verzeichnis und setzen Sie den Wert `STARTMODE` innerhalb der Datei auf „`auto`". Anschließend kann die Karte wie gewohnt mit einem Texteditor Ihrer Wahl konfiguriert werden.

Achtung: Erstellen Sie keine Konfiguration für die Karte `eth0`! Die Karte wird automatisch richtig konfiguriert. Falsche Konfigurationen auf dieser Schnittstelle können dazu führen, dass der Rechner für Sie nicht mehr erreichbar ist.

Versuchen Sie, andere Rechner im Netz zu erreichen. Welche Rechner antworten, welche nicht? Welche Meldung erhalten Sie, wenn sie versuchen, einen Rechner außerhalb Ihres Subnetzes zu erreichen?

(d) Wie haben sich ARP- und Routing-Tabelle verändert?

4. Konfiguration der statischen Routen

(a) Konfigurieren Sie nun die statischen Routen des Rechners so, dass Sie alle Rechner im Netz erreichen können. Arbeiten Sie dabei nicht mit Hostrouten für die einzelnen Rechner, sondern mit Netzrouten für die Netze aus Abbildung 1 und verwenden Sie keine Defaultroute. Lassen sich Routen zusammenfassen?

(b) Auf den Rechnern, die als Router arbeiten sollen, muss auch das Routing aktiviert werden.

(c) Überprüfen Sie nochmal ARP- und Routingtabelle. Welche Änderungen stellen Sie fest?

5. **Mithören des Netzwerkverkehrs**

Für die folgenden Versuche müssen auf Ihren Rechnern noch je ein FTP- und Telnet-Server installiert werden. Installieren Sie dazu das Paket `telnet-server` und einen FTP-Server ihrer Wahl und aktivieren Sie die beiden Dienste.

(a) Starten Sie nun in einem weiteren Terminal-Fenster das Programm `tcpdump` oder `ngrep`. Sinnvolle Optionen entnehmen Sie bitte den Man-Pages.

(b) Loggen Sie sich mit ftp (`man ftp`) auf einem benachbarten Rechner ein und laden Sie einige der dort gespeicherten Dateien herunter (User: `secpgast`). Achten Sie dabei darauf, sich keine lokalen Dateien zu überschreiben.
Was sehen Sie mit `tcpdump`/`ngrep` bei aktiver und nicht aktiver ftp-Verbindung? Versuchen Sie, das ftp-Passwort aufzuzeichnen.

(c) Was können Sie daraus bzgl. der Schicht 2-Infrastruktur in Ihrem Netzsegment schließen?

(d) Zeichnen Sie den TCP-Verbindungsauf- und -abbau zu einem beliebigen über IP erreichbaren Rechner im Netz auf und kennzeichnen Sie die mitgeschnittenen Pakete als zugehörig zu

- Verbindungsaufbau
- Datenübertragung
- Verbindungsabbau.

Starten Sie dazu in einem Terminal-Fenster zuerst das Kommando

```
tcpdump -n host <Ziel-IP>
```

Über folgende Kommandos können Sie nun in einem weiteren Terminal-Fenster eine TCP-Verbindung (`telnet`, Port 23) zur `<Ziel-IP>` sauber auf- und wieder abbauen.

```
telnet <Ziel-IP>
Control-5 oder Control-AltGr-9
quit
```

`tcpdump` können Sie mit `Control-C` abbrechen.

Hinweise:

- Der Rechner `test4all` kann für Tests der Konfigurationen verwendet werden (Benutzer `secpgast`, Passwort `pcsec`).
- Zur Installation von Software auf dem lokalen Rechner liegt eine SuSE 10.2 DVD im Laufwerk `/dev/xvdc`. Diese ist bereits in der Datei `/etc/fstab` korrekt eingetragen und kann nach `/media` gemountet werden.
- Des Weiteren können Sie den Rechner `secserver` als Internet-Gateway verwenden.

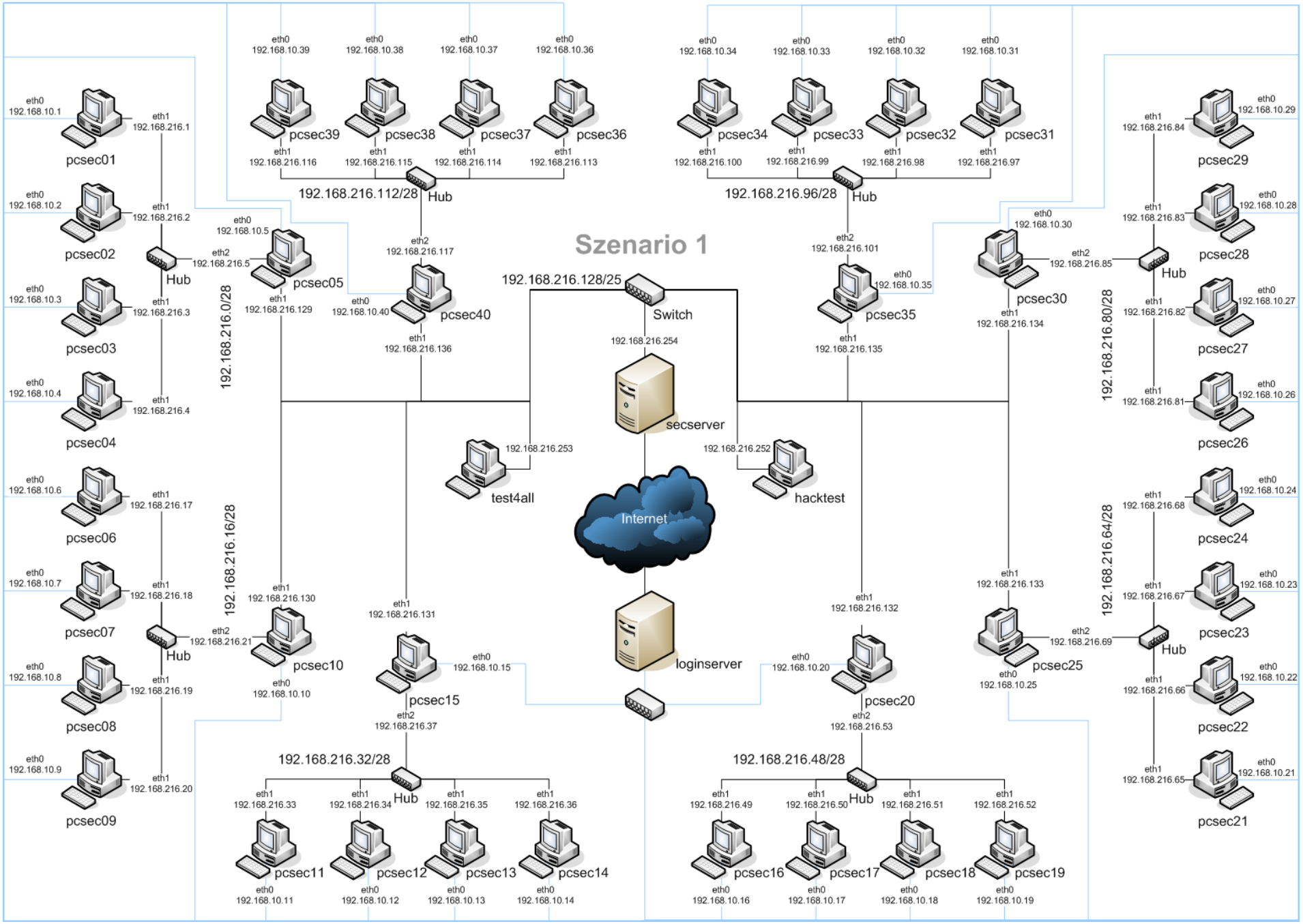

Abbildung 1: Der Versuchsaufbau