MNM TEAM
Munich Network Management Team

Ludwig-Maximilians-Universität München
und Technische Universität München

Prof. Dr. D. Kranzlmüller
Dr. N. gentschen Felde

Praktikum IT-Sicherheit
Übungsblatt 01

1. **IP-Adressen und Netzmasken**

   (a) Bestimmen Sie für die Netze des Versuchsaufbaus (siehe Abbildung 1) die in den einzelnen Sub-Netzen verwendbaren IP-Adressen und die Broadcast-Adresse.

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

2. **Konfiguration der Netzkarten**

   (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) Konfigurieren Sie nun die Netzkarte(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.

   Achtung: Erstellen Sie keine Konfiguration für die Karte `eth0` bzw. ändern Sie die bestehende Konfiguration nicht ab! 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?

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

3. **Konfiguration statischer Routen**

   (a) Konfigurieren Sie nun statische Routen für ihre Rechner so, dass Sie alle Rechner im Praktikumsnetz erreichen können. Arbeiten Sie dabei nicht mit Hostrouten für die einzelnen Rechner, sondern mit Netzrouten für die Netze aus Abbildung 1. Lassen sich Routen zusammenfassen?

   (b) Auf den Rechnern, die als Router arbeiten sollen (durch 5 teilbare Ordnungsnummer), muss das Routing aktiviert werden. Als Default-Route soll auf diesen Rechnern der Rechner `secserver` eingetragen werden, alle anderen Rechner tragen den ihnen zugeordneten Router (durch 5 teilbare Ordnungsnummer) ein.

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

4. **Mithören des Netzverkehrs**
   Für die folgenden Versuche müssen auf Ihren Rechnern noch je ein FTP- und Telnet-Server installiert werden. Installieren Sie dazu die entsprechenden Pakete (`proftpd` und `telnetd`) und aktivieren Sie die beiden Dienste.
   Hinweis: Zur Paketinstallation müssen Sie zuvor den DNS-Server `10.153.255.58` zur Namensauflösung in die Datei `/etc/resolv.conf` eintragen.

   (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 per ftp (`man ftp`) auf einem benachbarten Rechner ein und laden Sie einige der dort gespeicherten Dateien herunter (User: `secpgast`). Achten Sie dabei darauf, dass Sie sich keine lokalen Dateien 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 (root-Passwort wie das initiale root-Passwort Ihrer Maschine laut Vorlesung).
- Zur Installation von Software auf dem lokalen Rechner muss das Routing korrekt funktionieren und eine Internetverbindung bestehen.
- Des Weiteren können Sie den Rechner `secserver` als Internet-Gateway verwenden.

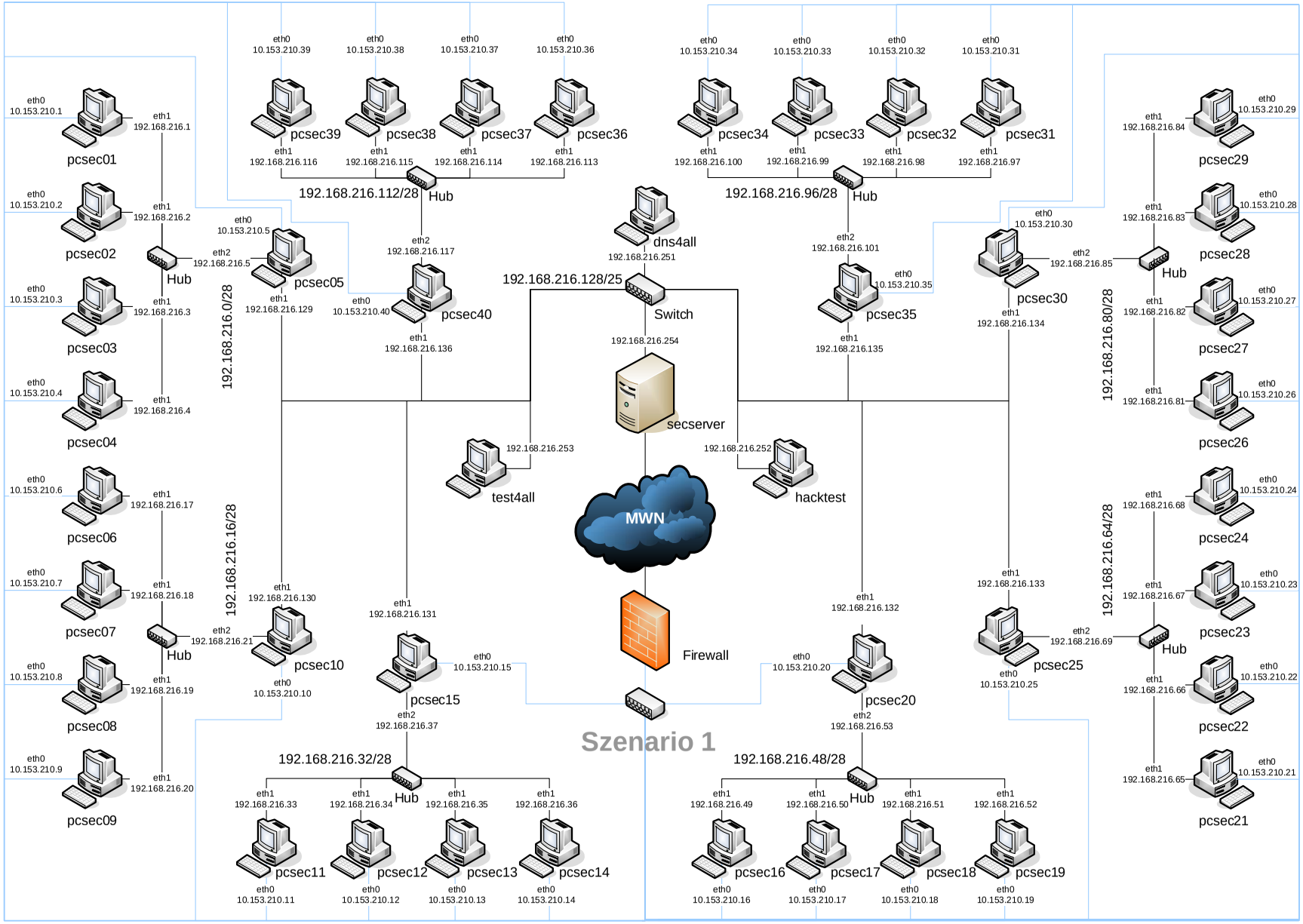

Abbildung 1: Versuchsaufbau zu Szenario 1