MNM
TEAM
Munich Network Management Team

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

Praktikum IT-Sicherheit
Übungsblatt 03

Für alle folgenden Versuche wird der Versuchsaufbau aus Abbildung 1, Seite 3 verwendet.

9. **Umstellung der Netztopologie**

   Konfigurieren Sie Ihre Rechner der neuen Topologie entsprechend. Verwenden Sie nun auch die Default-Route und fassen Sie ggf. Routen zusammen.
   Die physischen Änderungen an der Topologie werden von den Betreuern für Sie durchgeführt. Stichtag zur Umstellung ist die zu dieser Übung gehörende Vorlesung.

10. **Statische Paketfirewalls**

    In diesem Praxis-Teil werden die Dienste FTP (TCP Port 20 und 21), Telnet (TCP Port 23), SSH (TCP Port 22), DNS (nur Abfragen, UDP Port 53) und NTP (UDP Port 123), SMTP (TCP Port 25) und der TCP-Proxy-Port 3128 durch Paketfilterregeln abgesichert.
    Alle für diese Versuche benötigten Netfilter-Pakete sind schon auf den Rechnern installiert.

    (a) Auf dem Rechner `secserver` ist ein DNS-Dienst aktiv, tragen Sie diesen in Ihrem Rechner als DNS-Server ein.

    (b) Stellen Sie sicher, dass die standardmäßig eingerichtete Firewall-Konfiguration Ihrer Distribution nicht aktiv ist und lassen Sie sich die Regeln aller Ketten anzeigen (`man iptables`).

    (c) Erstellen Sie eine rein **statische** Firewall-Konfiguration mit folgenden Eigenschaften:

    - Verbindungen über das Managementinterface `eth0`, insbesondere SSH (TCP Port 22), sind erlaubt.

      Achtung: Blockierende Regeln auf diesem Interface machen die Maschine für Sie im schlimmsten Fall unerreichbar!

    - Die Unix-Kommandos `ping <IP-Adresse>` und `traceroute <IP-Adresse>` sind für alle Rechner erlaubt und müssen nicht geloggt werden. Andere als die für diese Kommandos benötigten ICMP-Meldungen sollen nicht erlaubt sein.
    - Das Logging soll, falls in den folgenden Aufgaben verlangt, bei erlaubten TCP-Verbindungen immer so eingestellt werden, dass immer nur der Verbindungsaufbau einen Eintrag ins Systemlog erzeugt. Beim UDP-Logging ist, falls verlangt, jedes Paket mitzuprotokollieren.
    - Für Rechner mit gerader Ordnungsnummer sind zusätzlich folgende Kriterien zu realisieren:
      - Erlauben folgender Dienste vom eigenen Rechner aus zu allen anderen Rechnern:
        * Telnet, FTP, SSH, und SMTP mit Logging.
        * TCP-Port 3128 ohne Logging.
        * DNS-Abfragen mit Logging.
        * NTP-Abfragen ohne Logging.
      - Erlauben folgender eingehender Dienste:
        * Telnet mit Logging nur für Ihren Partnerrechner und den Rechner `secserver`.
        * SSH für alle Rechner im Netz `192.168.216.0/24` mit Logging.
        * FTP ohne Logging für alle Rechner.
    - Für Rechner mit ungerader Ordnungsnummer sind zusätzlich folgende Kriterien zu realisieren:
      - Erlauben aller vom eigenen Rechner ausgehenden Verbindungen bzw. Anfragen auf allen Ports zu allen anderen Rechnern. Alle TCP-Dienste außer Port 3128 sollen geloggt werden, UDP-Dienste nicht.

  - Erlauben von eingehenden Telnet- und SSH-Verbindungen für Ihren Partnerrechner und den Rechner `secserver`, mit Logging.
  - Eingehende Verbindungen für die Dienste FTP, SMTP sowie DNS- und NTP-Abfragen und der TCP-Port 3128 sind zwischen allen Rechnern im Netz `192.168.216.0/24` freizuschalten ohne Logging, TCP-Kommunikation zu anderen Netzen (Internet) ist nur mit Verbindungsaufbau aus `192.168.216.0/24` zulässig und erfordert Logging.
- Für alle Rechner gilt außerdem:
  Alle für die oben erlaubten Regeln nicht benötigten Pakete sind zu verwerfen. Dabei sollen alle Verbindungsanfragen unbeantwortet bleiben, nur Anfragen auf den auth/identd-Dienst müssen mit `Connection refused` beantwortet werden. Geloggt werden sollen bis auf Zugriffe auf den auth/identd-Dienst alle Zugriffe auf unerlaubte Ports, also insbesondere bei TCP nicht nur Pakete zum Verbindungsaufbau.

(d) Überprüfen Sie Ihre Firewall durch Austesten der benötigten Dienste und mit Hilfe eines Portscanners.

Für die Konfiguration ist es ratsam, alle erforderlichen Befehle in ein Shellscript zu schreiben und dieses zur Aktivierung der Policy aufzurufen.
Legen Sie sich auch ein Script an, welches alle Firewall-Regeln entfernt und die Default-Policy auf ACCEPT zurücksetzt, um Dienste oder das Zusammenspiel mit den anderen Rechnern besser testen zu können. Natürlich gilt diese Vorgehensweise nur innerhalb der Praktikumsumgebung, in der realen Welt darf eine Firewall nicht einfach so geöffnet werden können!

(e) Richten Sie Ihren Rechner so ein, dass die Firewall beim Starten noch vor den Netzwerkkarten aktiviert wird.

(f) Überprüfen Sie Ihre Firewall erneut durch Austesten der benötigten Dienste und mit Hilfe eines Portscanners.

11. **Dynamische Paketfilterfirewalls**

(a) Stellen Sie ihr statisches Regelwerk nun auf **dynamische** Paketfilterung um, die Funktionsweise Ihrer Firewall soll sich dabei nicht ändern. Erstellen Sie dazu eine neue Konfigurationsdatei und löschen Sie die Konfiguration der statischen Filterung nicht!

(b) Überprüfen Sie Ihre Firewall wieder durch Austesten der benötigten Dienste und mit Hilfe des Portscanners.

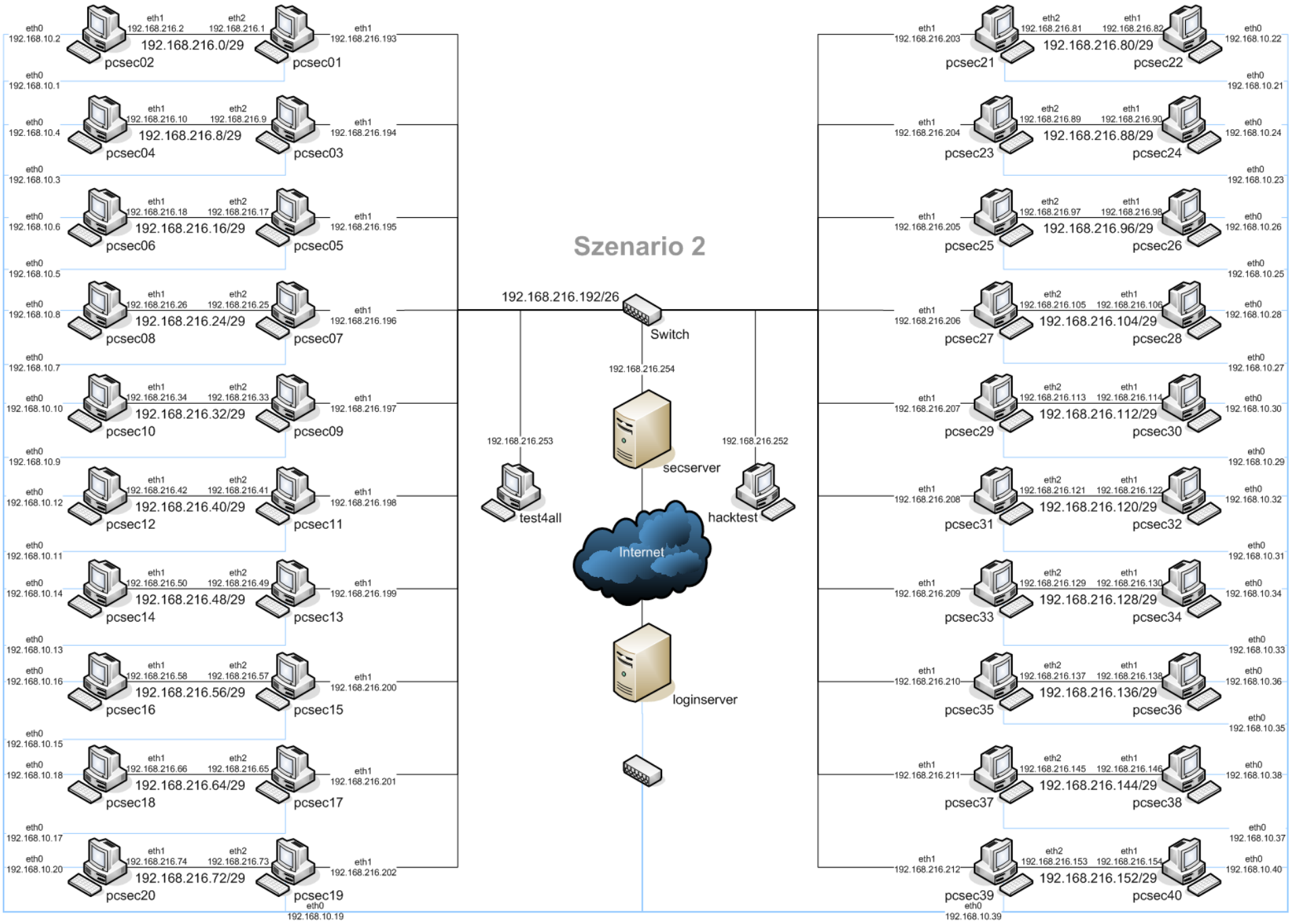

Abbildung 1: Die geänderte Netztopologie