Institut für
Technische Informatik und
Kommunikationsnetze
Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

Communication Networks
Einleitung Praktikum 4: Firewall

Willkommen zum vierten Praktikum der Vorlesung “Communication Networks”. In diesem Praktikum beleuchten wir Aspekte der Netzwerksicherheit. Wir werden ein Netzwerk mit einer Firewall schützen.

Ziel:

Im Laufe dieses Nachmittages lernen Sie eine einfache Firewall zu konfigurieren.

Theoretische Einführung:

Dieses Praktikum ist relativ aufwändig. Für die erfolgreiche Durchführung ist eine gründliche Vorbereitung unbedingt notwendig .

- Das eingesetzte Lehrbuch "Computer Networks" von Peterson und Davie behandelt Firewalls im Kapitel 8.4, Seiten 608 bis 613.

Die Firewall wird mit Hilfe des Tools *iptables* auf Linux aufgesetzt. Eine detaillierte Anleitung zur Verwendung von *iptables* finden Sie im "packet-filtering-HOWTO" unter:
http://www.netfilter.org/documentation/HOWTO/de/packet-filtering-HOWTO.html.

Kapitel 3, 6, 7 dieses Dokumentes müssen sorgfältig studiert werden. Danach sollten Sie fähig sein, die Fragen in Kapitel 2 der Praktikumsanleitung zu beantworten. Sie benötigen dazu ungefähr 2 Stunden.

Tip: Kapitel 7 des *IPTABLES-HOWTO* ist sehr hilfreich für die Bearbeitung der Praktikumsanleitung. Sie können auch *iptables -h* oder *man iptables* benutzen um die Syntax Ihrer iptables Version herauszufinden.

Institut für
Technische Informatik und
Kommunikationsnetze
Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

Communication Networks
Anleitung Praktikum 4: Firewall

Willkommen zum vierten Praktikumsnachmittag. Das heutige Praktikum gliedert sich in folgende Teilgebiete:

- Aufbau des Netzes und Grundkonfiguration der Versuchsanordnung
- Konfigurieren der Firewall
- Testen der Firewall

Für das heutige Praktikum benötigen sie drei Rechner und drei Hubs. Ein Rechner (die Firewall) ist mit drei Netzwerkkarten ausgestattet. In den beiden anderen (Server, interner Client) sind jeweils deren zwei installiert. Da pro Gruppe drei Rechner vorhanden sein müssen, werden Sie für das heutige Praktikum maximal sechs Gruppen bilden. Die Konfiguration Ihres Arbeitsplatzes unterscheidet sich wesentlich von den früheren Praktika.

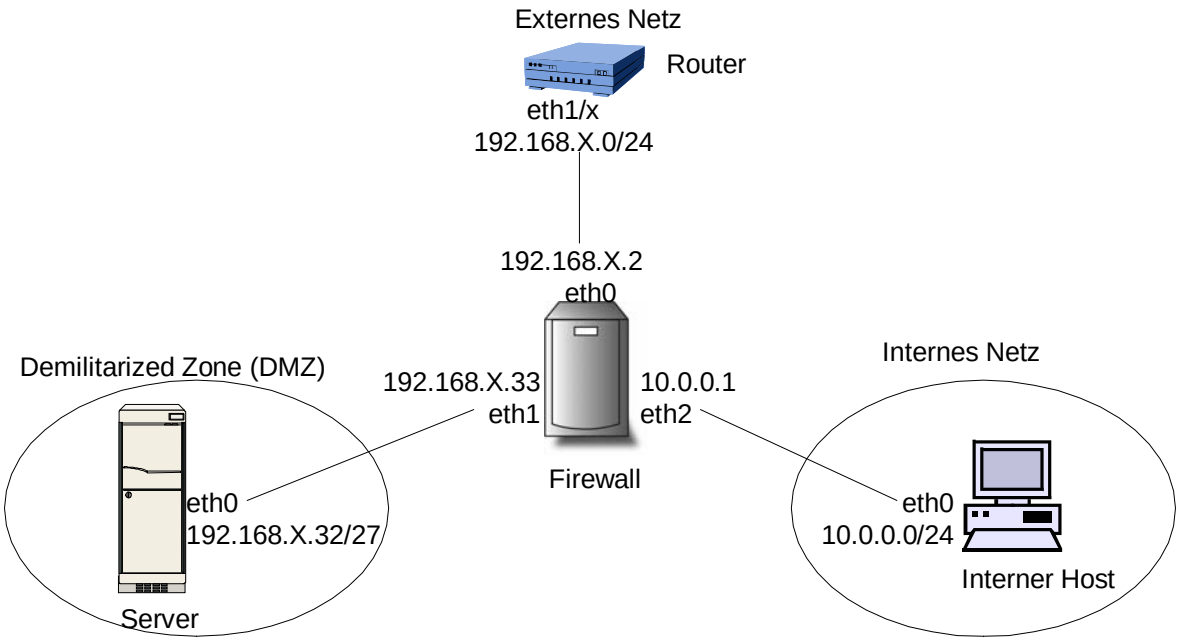

Abb. 1: Aufbau des Praktikumsnetzwerks

1 Aufbau und Grundkonfiguration der Versuchsanordnung

Als erstes baut jede Gruppe eine Umgebung auf, die in drei Subnetze unterteilt ist.
(Die Bedeutung der entsprechenden Netze wird später erläutert.)

- Internes Netz
- Demilitarized Zone (DMZ)
- Externes Netz

Dazu verbinden Sie die Rechner entsprechend dem Schema [Abb. 1]. Das Interface des Routers (eth1/1, eth1/2, eth1/3) wählen Sie entsprechend Ihrer Gruppennummer und dem Schema, dass Sie bereits aus den früheren Praktika kennen.

Beachten Sie, dass Sie für jedes Subnetz einen Hub benötigen, da keine gekreuzten Kabel verwendet werden.

Die drei zur Verfügung stehenden Rechner werden mit Linux gebootet. Jeder Rechner übernimmt eine gewisse Aufgabe, die später noch genau beschrieben wird. In der Folge werden die Rechner entsprechend ihrer Aufgabe benannt.

- Firewall (3 Netzwerkkarten)
- Interner Host
- Server

Konfiguration des internen Hosts

- Loggen Sie sich für die Konfiguration mit dem Login *root* und Password *root* in das System ein. Öffnen sie danach im Start-Menü des Window Managers eine neue Shell.

- Konfigurieren sie den internen Host mit den folgenden Befehlen. Ersetzen Sie X stets durch Ihre Gruppennummer:

```
hostname intHost-gX
ifconfig eth0 10.0.0.2 netmask 255.255.255.0 up
route add default gw 10.0.0.1
```

- Kontrollieren Sie die korrekte Konfiguration mit:

```
ifconfig -a
route -n
```

Konfiguration des Servers

- Loggen Sie sich für die Konfiguration mit dem Login *root* und Password *root* in das System ein. Öffnen sie danach im Start-Menü des Window Managers eine neue Shell.

- Konfigurieren sie den Server mit den folgenden Befehlen. Ersetzen Sie X stets durch Ihre Gruppennummer:

```
hostname server-gX
ifconfig eth0 192.168.X.34 netmask 255.255.255.224 up
route add default gw 192.168.X.33
```

- Kontrollieren Sie die korrekte Konfiguration mit:

```
ifconfig -a
route -n
```

Konfiguration der Firewall

- Loggen Sie sich für die Konfiguration mit dem Login *root* und Password *root* in das System ein. Öffnen sie danach im Start-Menü des Window Managers eine neue Shell.

- Konfigurieren Sie die Interfaces der Firewall mit den folgenden Befehlen. Ersetzen Sie X stets durch Ihre Gruppennummer:

```
ifconfig eth0 192.168.X.2 netmask 255.255.255.224 up
```

```
ifconfig eth1 192.168.X.33 netmask 255.255.255.224 up
ifconfig eth2 10.0.0.1 netmask 255.255.255.0 up
route add default gw 192.168.X.1
```

- Kontrollieren Sie die korrekte Konfiguration mit:

```
ifconfig -a
route -n
```

2 Grundsätzliches zur Firewall im Linux-Kernel

Komponenten

Bevor Sie mit der eigentlichen Konfiguration der Firewall beginnen, sollten Sie die elementaren Komponenten, die im Linux-Kernel die Funktion der Firewall zur Verfügung stellen, verstanden haben. Es geht dabei um die verschiedenen Tables - vor allem um Routing, (De-)Masquerading und die drei Standard-Chains (INPUT, OUTPUT, FORWARD) der filter-table. Die folgenden Aufgaben dienen Ihnen zur Kontrolle, ob Sie die Grundfunktionen der Linux-Firewall verstanden haben. Sie sind während der Praktikumsvorbereitung zu Hause zu lösen.

Vorgabe:

Nehmen Sie an, ein Paket kommt auf einem Interface an. Je nachdem, wohin das Paket gesendet werden soll, wird es unterschiedlich verarbeitet. Beantworten Sie dazu die folgenden Fragen:

Frage:

In welcher Reihenfolge durchläuft das Paket die folgenden Komponenten (allgemeiner Fall): input-Chain, output-Chain, forward-Chain, Routing, Masquerading und Demasquerading?

Frage:

Wo wird entschieden, ob das Paket für den lokalen Rechner bestimmt ist?

Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

Regeln (rules)

Sie haben im packet-filtering-HOWTO gelesen, dass für jedes Paket die Regeln in den entsprechenden Chains jeweils linear abgearbeitet werden. Wenn das Paket eine Regel erfüllt, so wird die entsprechende Anweisung (target) ausgeführt (ACCEPT, DROP, REJECT,...). Lösen Sie dazu bitte folgende Aufgaben:

Vorgabe:

Nehmen Sie an, alle Regeln einer Chain sind abgearbeitet worden und ein Paket erfüllt keine der Regeln.

Frage:

Was passiert nun mit diesem Paket?

Vorgabe:

Die Anweisungen DROP und REJECT haben beide zur Folge, dass ein Paket verworfen wird, wenn es die entsprechende Regel erfüllt.

Frage:

Was ist der Unterschied zwischen DROP und REJECT?

Aufgabe:

Grundsätzlich gibt es zwei verschiedene Strategien, wie eine Firewall konfiguriert werden kann. Entweder Sie akzeptieren alle Pakete per default (Policy: ACCEPT) und wählen die Regeln so, dass Sie alles verwerfen, was Sie nicht durchlassen möchten. Bei der anderen Strategie blockieren Sie erst mal alles (policy: DROP) und beschreiben mit Ihren Regeln welche Pakete Sie durchlassen wollen.

Geben Sie für jede Strategie ein sinnvolles Szenario an und diskutieren Sie die Vor- und Nachteile.

3 Was wollen wir eigentlich schützen?

Bevor man eine Firewall konfigurieren kann ist es wichtig zu wissen, was man denn überhaupt schützen will. Die im Praktikum untersuchte Anordnung (internes Netz, externes Netz und DMZ) ist eine recht einfache, aber durchaus sinnvolle Methode, wie man eine Firewall einsetzen kann. Prinzipiell wollen wir mit der Firewall die folgenden Ziele erreichen:

- Das interne Netz soll von aussen nicht sichtbar sein. Dies ist durchaus sinnvoll, denn wir wollen nicht, dass auf den internen Rechnern irgendwelche Server laufen, die von aussen angesprochen werden können. Weiter wollen wir verhindern, dass das interne Netz von aussen gescannt werden kann. Deshalb verwenden wir eine private Netzaddresse, genauer das 10.0.0.0/24 Subnetz (/24 bedeutet das gleiche wie die Netzmaske 255.255.255.0). Dies würde es uns erlauben, 253 Rechner anzuschliessen; in der Praktikumsanordnung wird genau ein Rechner im internen Netz verwendet (10.0.0.2). Um vom internen Netz auf Rechner im Internet zugreifen zu können, verwenden wir Network Address Translation (NAT), welches in der Linux-Firewall mit IP-Masquerading bezeichnet wird.
- Der Server in der DMZ soll sowohl von extern als auch von intern sichtbar sein. Damit können wir in der DMZ diejenigen Dienste anbieten, auf welche die Aussenwelt Zugriff haben soll (meist sind dies Web- und Mailserver). Die DMZ ist ein eigenes Subnetz mit der Adresse 192.168.X.32/27. Die DMZ kann im dargestellten Fall 29 verschiedene Rechner beinhalten; im Praktikum nehmen wir an, alle Services laufen auf genau einem Rechner (192.168.X.34).
- Das externe Netz ist von der DMZ und vom internen Netz sichtbar.

Wir definieren nun genauer, welche Dienste von wem genutzt werden dürfen. Mit entsprechender Konfiguration der Firewall sollen Sie dann garantieren, dass auch wirklich nur die folgenden Dienste verfügbar sind und dementsprechend die Pakete durchgelassen oder ausgefiltert werden.

Vom internen Netz:

- Webzugriff zum Webserver in der DMZ und zu Webservern im Internet (HTTP, HTTPS)

- Mail senden zum Mailserver (SMTP) und Mail abholen vom Mailserver (POP3) in der DMZ
- Zugriff auf Secure-Shell-Server (SSH) im Internet
- Zugriff auf DNS-Server im Internet und in der DMZ
- Traceroute auf Rechner im Internet
- Ping auf den Server in der DMZ, auf die Firewall und auf beliebige Rechner im Internet

Vom externen Netz:

- Webzugriff zum Webserver in der DMZ (HTTP, HTTPS)
- Mail senden zum Mailserver (SMTP) in der DMZ

Von der DMZ:

- Mail senden zu Mailservern (SMTP) im Internet
- Zugriff auf DNS-Server

Von der Firewall selbst:

- Ping auf jeden beliebigen Rechner
- Traceroute auf jeden beliebigen Rechner
- Zugriff auf DNS-Server

Generell:

- Antworten auf erlaubte Anfragen
- Sonst nichts

4 Grundsätzliche Überlegungen zur Konfiguration

Es ist nicht sinnvoll, dass Sie jede der Regeln stets manuell eingeben. Vielmehr sollten Sie die einzelnen Regeln in einem Shell-Script zusammenfassen, wo Sie auch die notwendigen Kommentare anbringen können. Ein Shell-Script ist ein executable file (kann mit `'chmod u+x` *filename*`'` erreicht werden) und enthält je einen von der Shell ausführbaren Befehl pro Zeile. Das Script sollte einen sinnvollen Namen (z.B. `firewall.sh`) und als erste Zeile den Eintrag `#!/bin/sh` enthalten. Beginnt eine Zeile mit #, so wird sie von der Shell ignoriert (Kommentare). Das Shell-Script können Sie dann einfach wie ein normales Programm in der Shell starten (`./firewall.sh`).

- Fragen Sie einen Betreuer wie Sie die Datei `fw_template.sh` erhalten. Kopieren Sie diese nach `firewall.sh`.

  cp fw_template.sh firewall.sh

- Machen Sie die Datei 'executable'.

  chmod u+x firewall.sh

Diese Datei enthält bereits einige Regeln. Sie werden diese im Verlaufe des Praktikums ergänzen.

Anmerkung: Sie können sich das Skript mit den Regeln am Schluss des Praktikums per e-mail zusenden. Sie müssen also nicht alle Regeln zusätzlich in diese Unterlagen schreiben.

Prinzipiell hat man drei Standard-Chains für das Packetfiltering zur Verfügung, bei denen man Regeln eintragen kann. Unsere Firewall hat zwei verschiedene Aufgaben. Einerseits sollen Pakete von einem Interface zu einem anderen geroutet werden (die Pakete sind also nicht für die Firewall selbst bestimmt), und andererseits wird die Firewall an sich selbst adressierte Pakete erhalten. Diese beiden Aufgaben kann man recht gut separat lösen. Die für die Firewall bestimmten Pakete werden durch die INPUT-Chain laufen, entsprechend müssen wir sie dort behandeln. Von der Firewall ausgehende Pakete laufen durch die OUTPUT-Chain. Alle anderen Pakete durchlaufen die FORWARD-Chain.

Jetzt müssen wir noch die Pakete vom Internen Netz mit NAT maskieren. Das findet nach dem eigentlichen Paketfiltering in der nat-Table statt.

5 Policies und Flushen der Chains

In diesem ersten Schritt werden wir die Policy jeder der drei Standard-Chains setzen. Anschliessend flushen wir die Chains, damit alle Regeln und benutzerdefinierten Chains aus der Firewall entfernt werden.

Setzen der Policies

Bevor Sie irgendwelche Pakete durchlassen oder rausfiltern, sollten Sie die Standard-Policies der INPUT-, OUTPUT- und FORWARD-Chains entsprechend setzen. In unserem Fall setzen wir alle auf DROP. Damit erreichen wir, dass (wenn nicht explizit erlaubt) nichts von der Firewall geforwarded wird und auch nichts in sie hinein oder hinausgehen kann. Dies bedeutet auch, dass wir in jeder Chain nur diejenigen Pakete behandeln müssen, die wir durchlassen möchten. Die Policy der Chain wird automatisch Pakete ablehnen, die nicht in einer der Regeln explizit akzeptiert wurden.

Aufgabe:

Setzen Sie die Policy der 3 Standard-Chains der filter-Table auf DROP .

Frage:

Welche drei iptables-Befehle tragen Sie in Ihr Shell-Script ein?

Flushen der Chains

Nun sollten Sie alle benutzerdefinierten Chains und alle Regeln, die zur Zeit in der Firewall gesetzt sein könnten, löschen.

Aufgabe:

Löschen Sie alle Regeln und alle benutzerdefinierten Chains.

Frage:

Welche beiden iptables-Befehle tragen Sie in Ihr Shell-Script ein?

Überprüfen der Konfiguration der Firewall

Sie sollten jetzt überprüfen, ob Sie Ihr Shell-Script ausführen können. Dabei sehen Sie auch, ob die Policies richtig gesetzt werden und ob alle vorhandenen Regeln entfernt wurden.

Aufgabe:

Führen Sie das Shell-Script aus. Bei der Ausführung sollte es keine Fehler geben. Wenn doch, dann müssen Sie diese zuerst beheben.

Zeigen Sie danach die Firewall-Konfiguration an. Wie sieht die Konfiguration aus?

Frage:

Welchen iptables-Befehl benutzen Sie, um die Konfiguration der Firewall anzuzeigen?

Tip: Vermeiden Sie Zugriffe auf den DNS-Server (Option -n), sonst kann eine grosse Verzögerung auftreten.

Aufgabe:

Machen Sie ein Ping vom Rechner in Ihrem internen Netz auf Ihren Server (192.168.X.34). Machen Sie dann ein Ping auf Ihre Firewall (10.0.0.1).

Frage:

Was ist das Ergebnis der beiden Pings? Entspricht dies Ihren Erwartungen? Erklären Sie das Verhalten!

Akzeptieren von Paketen die zu bestehenden Verbindungen gehören

Wenn wir ein Paket akzeptieren, dann möchten wir auch alles, was dazugehört, zulassen.

Aufgabe:

Für die drei Standard-Chains (INPUT, OUTPUT, FORWARD) sollen alle zu einer bestehenden Verbindung gehörenden Pakete akzeptiert werden. Hierzu muss mit states gearbeitet werden.

Frage:

Welche drei iptables-Befehle tragen Sie ein?

6 Konfiguration der FORWARD-Chain

Man könnte jetzt einfach die FORWARD-Chain mit Regeln vollstopfen, dies hat aber den grossen Nachteil, dass man leicht die Übersicht verliert. Viel besser ist es deshalb, die Regeln logisch aufzuteilen und benutzerdefinierte Chains zu verwenden. Da wir drei Interfaces (intern, extern, DMZ) haben, ist es sinnvoll, drei entsprechende Chains zu definieren. Auch sollte man den Chains sinnvolle Namen geben. Maximal stehen 31 Zeichen zur Verfügung.

Aufgabe:

Definieren Sie drei benutzerdefinierte Chains. Verwenden Sie die folgenden Bezeichnungen für die Chains: int, ext, dmz.

Frage:

Welche drei iptables-Befehle benutzen Sie, um die benutzerdefinierten Chains zu generieren?

Einbinden der benutzerdefinierten Chains in die FORWARD-Chain

Damit die benutzerdefinierten Chains auch in der Firewall verwendet werden, müssen sie als Anweisung (target) einer Regel in einer der Standard-Chains benutzt werden.

Aufgabe:

Tragen Sie die drei Regeln so in der FORWARD-Chain ein, dass Pakete (abhängig davon, woher sie kommen) die richtige, benutzerdefinierte Chain durchlaufen. Beachten Sie, dass Sie in der FORWARD-Chain das incoming interface sowie die source eines Paketes kennen.

Spezifizieren Sie die Regeln so, dass Sie die Pakete nur für oder von genau dem einen Rechner in der DMZ erlauben (192.168.X.34). Sie dürfen also nicht einfach das ganze Subnetz oder Interface freigeben. Hingegen sollte es möglich sein, neue Rechner im internen Netz hinzuzufügen, ohne dass die Firewallkonfiguration geändert werden muss.

Achten Sie weiter darauf, dass nur neue Verbindungen aufgebaut werden können. Gebrauchen Sie dazu den NEW-state.

Bevor Sie die folgende Frage beantworten, müssen Sie verstanden haben, was die Optionen -s, -i und -m state machen.

Frage:

Welche drei iptables-Befehle tragen Sie in der FORWARD-Chain ein?

7 Masquerading des internen Netzes

Um diese Table richtig zu konfigurieren, muss man IP-Masquerading verstanden haben. Wenn ein Rechner im internen Netz einen Server im Internet kontaktiert, so wird er seine Pakete mit der eigenen IP-Adresse als Absender versehen. Da dies eine private Adresse ist und diese im Internet nicht geroutet werden können, ersetzt die Firewall (oder besser gesagt die NAT/Masquerading-Logik) die Senderadresse (10.0.0.2) mit ihrer eigenen (192.168.X.2). Die Antworten von dem kontaktierten Server werden dann auch entsprechend zuerst zur Firewall (192.168.X.2) gesendet, was nichts anderes bedeutet, als dass die Pakete für die Linux-Box selbst bestimmt sind. Die Demasquerading-Logik wird dann ein maskiertes Paket erkennen und es zum Rechner im internen Netz weitersenden.

Aufgabe:

Die entsprechenden Befehle sind bereits im `firewall.sh` Skript enthalten. Nur der eigentliche "Masquerading-Befehl" ist unvollständig. Ergänzen Sie ihn so, dass nur Pakete, die vom internen Netz ins externe Netz ausgehen, durch das Masquerading betroffen sind.

Frage:

Wie lautet der vollständige Befehl, um Pakete vom Internen Netz zu maskieren?

8 Konfiguration der int-Chain

Nachdem Sie die benutzerdefinierten Chains erzeugt haben und die Pakete von der FORWARD-Chain in die entsprechend korrekte benutzerdefinierte Chain geleitet werden, kommen wir zur eigentlichen Konfiguration der Firewall und damit der Eingabe der weiteren Regeln. Sie werden zuerst die erlaubten Pakete aus dem internen Netz akzeptieren.

Aus dem internen Netz wollen wir verschiedene Dinge zulassen (siehe Kapitel 3). Wir können hierbei 3 Fälle unterscheiden:

1. Pakete, die sowohl ins externe Netz als auch in die DMZ zugelassen werden.
2. Pakete, die nur in die DMZ zugelassen werden.
3. Pakete, die nur ins externe Netz zugelassen werden.

Aufgabe:

Wir wollen mit dem ersten Fall beginnen. Hierzu müssen http, https, ping (echo-request) und DNS erlaubt werden. Beachten Sie, dass DNS auf TCP und auf UDP läuft.

Info: Webserver laufen nicht immer nur auf den ports 80 (http) und 443 (https) sondern auch oft auf anderen ports, z.B. 8080. Wenn nun nur Pakete auf port 80 und 443 zugelassen werden, können nicht alle Webseiten angesehen werden. Darum werden Firewalls oft so konfiguriert, dass alle Verbindungsaufbaus von intern zugelassen werden.

Frage:

Welche 5 Regeln fügen Sie zum Skript (# int -> dmz / ext) hinzu?

Aufgabe:

Für den zweiten Fall müssen smtp und pop3 erlaubt werden.

Frage:

Welche 2 Regeln fügen Sie zum Skript (# int -> dmz) hinzu?

Aufgabe:

Für den dritten Fall müssen nun noch ssh und traceroute zugelassen werden. Beachten Sie, dass traceroute einerseits auf ICMP (was wir schon zugelassen haben) und andererseits auf UDP (ports 33434 - 33500) läuft.

Frage:

Welche 2 Regeln fügen Sie zum Skript (# int -> ext) hinzu?

9 Testen der int-Chain

Um zu testen, ob die Regeln korrekt sind, möchten wir gewisse Tests durchführen. Dazu führen Sie Ihr Skript bitte aus (damit die Regeln auch gesetzt werden). Sollte es dabei Fehler geben müssen Sie diese beheben (und das Skript erneut ausführen).

Testvorbereitungen auf dem Server

Um zu kontrollieren, ob auf gewisse Ports des DMZ-Servers zugegriffen werden kann, starten Sie nun auf dem Server einen Echo-Dienst. Dieser kann mit `telnet IP_Adresse port-nummer` angesprochen werden. Der Echo-Dienst wird nichts anderes tun, als Ihnen die Portnummer zu bestätigen und Ihre Eingabe zurückzuliefern. Der Port, auf welchem der Echo-Dienst antwortet, kann von Ihnen gewählt werden. **Falls auf einem gewissen Port bereits ein**

Dienst läuft (z.B. ein Webserver auf Port 80), ist es nicht nötig den Echo-Dienst auf diesem Port zu starten.

- Wechseln Sie falls nötig ins Rootverzeichnis des Servers.

  cd /root/

- Starten Sie einen Echo-Dienst auf dem HTTP Port (80)

  ./echo-dienst.pl 80 &

- Starten Sie einen Echo-Dienst auf dem HTTPS Port (443)

  ./echo-dienst.pl 443 &

- Starten Sie einen Echo-Dienst auf dem SMTP Port (25)

  ./echo-dienst.pl 25 &

- Starten Sie einen Echo-Dienst auf dem POP3 Port (110)

  ./echo-dienst.pl 110 &

- Starten Sie einen Echo-Dienst auf dem FINGER Port (79)

  ./echo-dienst.pl 79 &

Tests vom internen Host ausgehend

- Versuchen Sie ein Ping auf den DMZ-Server. X ist wiederum durch Ihre Gruppennummer zu ersetzen.

  ping 192.168.X.34

- Versuchen Sie den HTTP Port des DMZ-Servers zu erreichen.

  telnet `192.168.X.34 80`

  Tippen Sie Ihren Namen und drücken Sie danach <Return>.

  Falls auf diesem port der Echo-Dienst läuft, sollte er sich jetzt mit *"This is the port 80 echo server in the DMZ. You typed:* IHR_NAME*"* melden.

  Falls Sie noch keine Antwort bekommen haben, dann drücken Sie nochmals <Return>. Sie werden nun eine Antwort vom Webserver erhalten.

- Versuchen Sie den Echo-Dienst auf dem HTTPS, SMTP, POP3 und FINGER Port zu erreichen. Vom FINGER Port sollten Sie keine Antwort erhalten!

- Versuchen Sie ein Ping auf einen Rechner im externen Netz.

  ping 129.132.200.35

- Starten Sie Mozilla und versuchen Sie 129.132.200.35 (www.ethz.ch) zu erreichen.
- Versuchen Sie mit Mozilla http://www.linux.org/ zu erreichen.
- Können Sie mit Mozilla http://babel.alis.com:8080/index.de.html erreichen. Warum (nicht)?
- Testen Sie, ob "traceroute-Pakete" durchkommen.

traceroute www.uiuc.edu

- Versuchen Sie sich auf Ihren Tardis Account einzuloggen.

  ssh -l USER_NAME TARDIS_RECHNER

10 Pakete aus der DMZ (dmz)

Von der DMZ aus soll kein Verbindungsaufbau ins interne Netz möglich sein, denn dies könnte von einem Angreifer ausgenutzt werden.

Aufgabe:

DNS und smtp sollen nach extern zugelassen werden.

Frage:

Welche beiden iptables-Befehle fügen Sie zum Skript (unter '#dmz -> ext') hinzu?

11 Pakete vom externen Netz (ext)

Vom externen Netz werden Verbindungsaufbaus nur in die DMZ gelassen. Niemand aussenstehendes sollte auf unser internes Netz zugreifen können (ausser er antwortet explizit auf eine Anfrage von innen). Alles, was wir aussenstehenden Personen an Services anbieten, läuft in der DMZ.

Aufgabe:

Es müssen http, https und smtp zugelassen werden.

Frage:

Welche iptables-Befehle fügen Sie zum Skript (unter # ext -> dmz) hinzu?

12 Pakete für die Firewall (INPUT)

Bis jetzt haben wir nur definiert, welche Pakete von der Firewall durchgelassen werden dürfen. Nun müssen wir noch definieren, welche an die Firewall gerichteten Pakete von der Firewall akzeptiert werden sollen.

Aufgabe:

Erlauben Sie ein ping vom internen Netz auf die Firewall.

Frage:

Welchen iptables-Befehl fügen Sie zum Skript (unter # int -> firewall) hinzu?

13 Pakete von der Firewall (OUTPUT)

Als letztes müssen wir nun noch definieren, welche Pakete von der Firewall versendet werden dürfen.

Aufgabe:

Erlauben Sie ping, dns und traceroute.

Frage:

Welche iptables-Befehle fügen Sie zum Skript (unter # OUTPUT) hinzu?

14 Testen der Firewall zum Zweiten

Scanner/Konfigurationstester eignen sich sehr gut, um die Durchlässigkeit einer Firewall zu testen. Ein Scanner sucht einen Rechner nach verfügbaren Diensten ab, d.h. er versucht von den einzelnen Ports Antworten zu kriegen. *nmap, nessus* und *saint* sind Namen solcher frei verfügbarer Scanner. Der Leistungsumfang der einzelnen Tools ist unterschiedlich und geht zum Teil über das reine Scannen hinaus. Ein ausführlicher, umfassender Test unserer Konfiguration mit einem Scanner sprengt den Rahmen dieses Praktikums. Deshalb werden wir uns hier auf ein paar wenige, manuelle Tests beschränken.

Auch vor diesen Tests müssen Sie Ihr Skript wieder ausführen (und allfällige Fehler beheben).

Tests vom internen Host ausgehend

- Versuchen Sie ein Ping auf die Firewall.

  ping 10.0.0.1

Tests von der DMZ ausgehend:

- Versuchen Sie ein Ping auf die Firewall. Was erwarten Sie?

  ping 192.168.X.33

- Testen Sie, ob Sie den smtp Port eines Rechners im externen Netz erreichen können.

  telnet mailbox1.ethz.ch 25

- Können Sie vom DMZ-Server aus mit Mozilla surfen?

Tests von der Firewall ausgehend:

- Versuchen Sie ein Ping auf den internen Host.

  ping 10.0.0.2

- Versuchen Sie ein Ping auf DMZ-Server.

  ping 192.168.X.34

- Versuchen Sie ein Ping auf einen Rechner im externen Netz. Sie testen zugleich, ob der DNS-Zugriff funktioniert.

  ping www.ethz.ch

- Testen Sie, ob "traceroute-Pakete" zum internen Host durchkommen.

  traceroute 10.0.0.2

- Testen Sie, ob "traceroute-Pakete" zum DMZ-Server durchkommen.

  traceroute 192.168.X.34

- Testen Sie, ob "traceroute-Pakete" zu einem Rechner ins externe Netz durchkommen.

  traceroute 129.132.200.35

- Können Sie von der Firewall aus mit Mozilla surfen?

Tests vom externen Netz ausgehend (freiwillig):

Da wir mit privaten IP-Adressen arbeiten, können wir leider nicht von ausserhalb des Praktikumsnetzwerkes testen. Es ist jedoch möglich vom Praktikumsserver oder von einem Rechner einer anderen Gruppe oder von ihrem Tardis Account (wo sie mit ssh vom dem Praktikumsraum her einloggen) aus zu testen. Der zweite Fall ist aber nur sinnvoll, wenn dort keine Firewall läuft. Falls Sie nun noch genügend Zeit haben und Ihre Firewall noch von extern testen möchten, machen Sie die erforderlichen Tests.

Bonusfrage

Was bewirken die folgenden 2 Regeln, wenn Sie gerade nach 'iptables -N ext' hinzugefügt werden?

```
iptables -A ext -s 10.0.0.0/24 -j DROP
iptables -A ext -s 192.168.X.32/27 -j DROP
```

15 Abschluss

Zum erfolgreichen Abschliessen des Praktikums fällt noch eine letzte Aufgabe an. Löschen Sie bitte Ihr Skript, fahren Sie die drei Rechner hinunter und schalten Sie sie aus. Ihre Nachfolger werden Ihnen dankbar sein, wenn sie die Betriebssysteme korrekt hinunterfahren - die PC's also nicht einfach vom Strom trennen. Nehmen Sie nun die HUB's vom Netz und rollen die Kabel zusammen.

Sobald Ihr Arbeitsplatz wieder im gleichen Zustand ist, wie Sie ihn angetroffen haben, können Sie sich beim Betreuer melden und das Testat verlangen.