Aufgabe 1 – Firewall mit IPTables (10 Punkte)

Installieren Sie auf einer der beiden virtuellen Maschinen, die Sie für Praktikum Nr. 1 eingerichtet haben, einen Webserver und eine Datenbank Ihrer Wahl (z.B. Apache, MySQL o.a.). **Protokollieren Sie Ihr Vorgehen mithilfe der Vorlage.**

a) Welche Ports verwenden die Programme zur Kommunikation? Wie ändert man die Standardeinstellungen? Ist dazu ein Neustart des Systems nötig?

b) Richten Sie eine restriktive Firewall ein (prohibitive Sicherheitspolitik). Es soll sichergestellt werden, dass ausschließlich der Port des Webservers von außen zugänglich ist. Die Firewall soll automatisch beim Start des Systems geladen werden. Nutzen Sie für die Lösung der Aufgabe ausschließlich die Kommandozeile und das Kommando `iptables`.

c) Nun soll `wireshark` verwendet werden. Pingen sie einen Rechner an und beobachten Sie den Netzwerkverkehr. Was geschieht, wenn Sie folgende Filterregel eingeben:

```
iptables -A INPUT -p icmp -j DROP
```

Wiederholen Sie den Vorgang mit der Policy `REJECT`. Was fällt auf? Wo sind die Unterschiede von `DROP` und `REJECT`, welche Vor- und Nachteile bieten sie jeweils? Löschen Sie nun wieder alle Regeln in `iptables`, setzen Sie die Policy zurück `ACCEPT` auf und beenden Sie wireshark.

d) Nun öffnen Sie mit `netcat` auf dem Rechner A (eine Ihrer VMs) ein oder zwei Ports zwischen 0 und 100. Nutzen Sie dafür den Befehl: `nc -l [Portnummer]`

`nmap` ist ein Portscanner, mit dem man u.a. die eigene Firewall auf Sicherheitslücken testen kann. Mit

```
nmap Zieladresse -p [Anfangsport]-[Endport]
```

kann nach offenen Ports in einem bestimmten Portbereich gescannt werden. Führen Sie nun einen Portscan auf VM A von VM B aus. Welches Ergebnis sehen Sie?

e) Definieren Sie nun Regeln mit `iptables`, die einen solchen Scan blocken. Dazu bietet es sich an, alle Pakete zu verwerfen, die ungewöhnlich schnell Verbindungsanfragen senden.

Sehen Sie sich die folgende Regel an und versuchen Sie zu verstehen, welchen Sinn die einzelnen Befehle erfüllen. Sie werden sie im Verlauf dieser Übung noch benötigen.

Tipps: (www.snowman.net/projects/ipt_recent).

```
iptables -A INPUT -p tcp -i eth1 -m state --state NEW -m recent --set
```

Wenden Sie diese Regel an.

Die zweite Regel soll nun bei genau solchen Paketen in der gleichen Liste nachsehen, ob die Adresse eines Paketes bereits eingetragen ist. Trifft dies zu, soll die letzte Zeitmarke upgedatet werden. Wenn nun ein und dieselbe Adresse versucht 20 oder mehr Verbindungsanfragen innerhalb von 10 Sekunden zu senden, sollen all diese Pakete verworfen werden. Wie sieht die entsprechende Regel aus? Testen Sie die Funktionalität der Regeln mit `nmap`.

Prof. Dr.-Ing. Martin Hoffmann
martin.hoffmann@fh-bielefeld.de

f) Nun sollen die Portscans mithilfe der LOG-Funktion protokolliert werden. Dazu kann zuerst eine neue Kette für Portscans mit Namen PORTSCAN o.ä. erstellt werden. Als zweites muss eine Regel definiert werden, die alle Pakete in dieser Kette protokolliert. Als Log-Prefix soll `"PORTSCAN erkannt --"` verwendet werden. `iptables` loggt i.d.R. in der Datei `/var/log/syslog`. Kontrollieren Sie, ob Ihre Ausgabe in der Logdatei erscheint.

g) `Hping3` ist ein Tool, um die eigene Firewall zu testen. Es kann benutzerdefinierte TCP-Pakete generieren und das auch mit langsamerer Geschwindigkeit als `nmap`. Schicken Sie einer VM mehrere TCP-Pakete mit gesetzter SYN-Flag beginnend bei Port 0.

Welchen Befehl verwenden Sie und woran erkennt man, welche Ports offen sind?

Prof. Dr.-Ing. Martin Hoffmann
martin.hoffmann@fh-bielefeld.de