Rechnernetze

Firewalling & Sniffing

HAW Hamburg

Steffen Giersch &

Maria Lüdemann

Praktikum 4

# 1. Paketfilterung (Firewalling)

a) "Auf einem Ihrer beiden Rechner soll der Zugang vom und zum Netzwerk 172.16.1.0/24 vollständig gesperrt werden"

#Setze das Standart-Verhalten auf ACCEPT

sudo /usr/sbin/iptables -P INPUT ACCEPT

sudo /usr/sbin/iptables -P OUTPUT ACCEPT

#Blocke alle ein- und ausgehenden Verbindungen auf 172.16.1.0/24

sudo /usr/sbin/iptables -A INPUT -s 172.16.1.0/24 -p all -j DROP

sudo /usr/sbin/iptables -A OUTPUT -d 172.16.1.0/24 -p all -j DROP

b) "Stellen Sie die Firewall des Rechners so ein, dass dort über das Netz 172.16.1.0/24 nur ein

TCP-Server (z.B. aus Aufgabe 1) auf Port 51000 genutzt werden kann. Alle anderen

Verbindungen über dieses Netz sollen gesperrt sein."

#######Erst werden alle Settings Deletet Externes Script#######

sudo /sbin/route add default gw 141.22.26.1 dev eth0

sudo /sbin/route add -net 172.16.1.0/24 gw 0.0.0.0 dev eth2

sudo /sbin/route add -net 127.0.0.0/8 gw 0.0.0.0 dev lo

####### ######

#Setze das Standart-Verhalten auf ACCEPT

sudo /usr/sbin/iptables -P INPUT ACCEPT

sudo /usr/sbin/iptables -P OUTPUT ACCEPT

#Nehme nur Verbindungen auf 172.16.1.0/24 an, die über TCP:51000 laufen und NEW oder ESTABLISHED sind

sudo /usr/sbin/iptables -A INPUT -s 172.16.1.0/24 -p tcp --dport 51000 -m state --state NEW,ESTABLISHED -j ACCEPT

sudo /usr/sbin/iptables -A INPUT -s 172.16.1.0/24 -p all -j DROP

#Lass Verbindungen auf 172.16.1.0/24 über TCP:51000 die ESTABLISHED sind heraus

sudo /usr/sbin/iptables -A OUTPUT -d 172.16.1.0/24 -p tcp --sport 51000 -m state --state ESTABLISHED -j ACCEPT

sudo /usr/sbin/iptables -A OUTPUT -d 172.16.1.0/24 -p all -j DROP

c) "Konfigurieren Sie den Rechner so, dass man keine dort laufenden TCP- Server über das

Netz 172.16.1.0/24 ansprechen kann. Alle anderen Verbindungen über dieses Netz sollen

hingegen möglich sein."

###Erst wird ein Script ausgeführt das die Einstellungen löscht###

#Setze das Standartverhalten auf ACCEPT

sudo /usr/sbin/iptables -P INPUT ACCEPT

sudo /usr/sbin/iptables -P OUTPUT ACCEPT

#Blockiere eingehende icmp-Verbindungen

sudo /usr/sbin/iptables -A INPUT -s 172.16.1.0/24 -p icmp -j DROP

d) "Stellen Sie die Firewall Ihres Rechners so ein, dass von dort ein ping auf andere

Rechner/Geräte im Netz 172.16.1.0/24 möglich ist, nicht aber umgekehrt!"

###Erst wird ein Script ausgeführt das die Einstellungen löscht###

#Setze das Standartverhalten auf ACCEPT

sudo /usr/sbin/iptables -P INPUT ACCEPT

sudo /usr/sbin/iptables -P OUTPUT ACCEPT

#Blockiere eingehende icmp-Verbindungen

sudo /usr/sbin/iptables -A INPUT -s 172.16.1.0/24 -p icmp -j DROP

# 2. Routing

"Konfigurieren Sie Ihre Rechner so, dass Sie den jeweils anderen Rechner im anderen Subnetz

erreichen können. (Prüfung mit dem ping-Befehl). Dabei soll der Netzwerkverkehr zwischen

diesen Rechnern entweder über den Router oder über die ISDN-Anlage laufen."

###Router von 17 auf 18###

./deleteSettings.sh

sudo /sbin/route add -net 192.168.18.0/24 gw 192.168.17.2 dev eth1

###Router von 18 auf 17###

./deleteSettings.sh

#Von 192.168.18.0/24 über den Router nach 192.168.17.0/24

sudo /sbin/route add -net 192.168.17.0/24 gw 192.168.18.2 dev eth1

###ISDN von 17 auf 18###

./deleteSettings.sh

sudo /sbin/route add -net 192.168.18.0/24 gw 192.168.17.1 dev eth1

###ISDN von 18 auf 17###

./deleteSettings.sh

sudo /sbin/route add -net 192.168.17.0/24 gw 192.168.18.1 dev eth1

"Was passiert, wenn Sie beim Weg über die ISDN-Anlage ein ping mit der Paketgrösse 1000

Byte durchführen? (Beobachtung im Sniffer und/oder Log von ping)"

Wir erhalten einen Error, da erwartet wird, dass das große Paket fragmentiert wird. Dies geschieht allerdings nicht.

DF = Don’t fragment Flag

Die beiden Hosts handeln aus wie groß die Fragmentierung sein söllte, beim ersten mal ist das DF Flag noch gesetzt und es wird nicht fragmentiert, sodass ein Fehler passiert. Für weitere Verbindungen ist die Größen dann ausgehandelt und der Ping funktioniert dann.

# 3. Sniffing & Firewalling

a) "Zeichnen Sie mit Wireshark (Netzwerksniffer) den Netzwerkverkehr zwischen Ihrem Chat-

Server auf dem Gegenstellenrechner und dem Chat-Client auf Ihrem Arbeitsplatzrechner auf."

b) "Starten Sie einen Browser und zeichnen Sie mit Wireshark den Netzwerkverkehr auf,

während Sie die Homepage www.dmi.dk besuchen. --- Von welchen anderen Web-Servern werden bei dieser Sitzung automatisch ohne Zutun des Benutzers zusätzlich Seiten angefordert?"

**Welche anderen Server:**

1.5.56.149.238

2.130.226.71.229

3.130.226.71.226

4.213.189.48.243

5.192.99.170.199

6.63.136.3.221

7.80.82.201.83

8.92.222.7.134

c) "Stellen Sie die Firewall so ein, dass über HTTP nur der Server www.dmi.dk erreicht werden

kann, nicht aber die Web-Server der fremden Seiten!"

d) "Was ist zu beachten, wenn sich nach dem Einstellen von c) später die IP-Adresse des

Servers www.dmi.dk ändert?"

Ändert sich die IP Adresse des Servers muss der Befehl ebenfalls geändert werden, und die IP Adresse wieder verboten werden, um zu verhindern dass eine andere Seite versehentlich durch kommt weil sie die Adresse bekommt.