

SVS Bachelor-Projekt Network Security

Blatt 5: Beschreibung der Experimentierumgebung

Louis Kobras
6658699

Utz Pöhlmann
6663579

1 Netzwerkeinstellungen

1.2

ClientVM:

IP-Adresse (ifconfig -a):	Standard-Gateway (route -n):	DNS-Nameserver (nslookup ubuntu.com):
192.168.254.44	192.168.254.2	10.1.1.1

RouterVM:

eth0	eth1
172.16.137.222	192.168.254.2

ServerVM:

IP-Adresse der Server-VM: 172.16.137.144

2 Absichern eines Einzelplatzrechners mit iptables (ClientVM)

2.1

Anzeigen der Firewall-Regeln mit `sudo iptables -L`; alle Regeln löschen mit `sudo iptables -F1`; OpenSSH-Server nach Paketquellen-Update via `apt-get` installiert (automatisch gestartet).

2.2

Regelwerk siehe [2.2: ClientVM-Filterregeln (S. 4)].

`iptables` säubern mit `sudo iptables -F`, einladen der Regeln aus einem Textfile mit `sudo iptables-restore < /iptables` (Dateinhalt im Anhang ebenda).

2.3

- SSH-Verbindungsversuch von RouterVM mit `sudo ssh 192.168.254.44` erfolgreich
- SSH-Verbindungsversuch in die andere Richtung nicht erfolgreich (Connection refused)
- hosten eines Servers mit `netcat -l 5555` erfolgreich, Verbindung (`sudo netcat 192.168.254.44 5555`) erwartungsgemäß fehlgeschlagen
- Firefox ist bei DROP schneller als bei REJECT

2.4

Dynamische Regeln vgl. [2.4: ClientVM Stateful Filtering (S. 4)].

Man muss nicht jeden Port und jedes Protokoll einzeln abdecken. Stateful Filter sind effizienter, da sie sich nur die Paket-Header ansehen.

¹löscht alle Regeln nacheinander

3 Absichern eines Netzwerks (RouterVM)

3.1

Der Aufruf bedeutet (nach [1]): “Maskiere alles, was an eth0 ausgeht”.

Es wird die Adressumsetzung (NAT) aktiviert und die Schnittstelle markiert ([2]).

Source: 192.168.254.0; Maske: 24

3.2

Die Client-VM kann die Server-VM anpingen; umgekehrt geht dies nicht.

Vermutung: Die Client-VM ist von außen nicht direkt ansprechbar, da sie hinter der RouterVM versteckt ist.

3.3

3.4

3.5

.

3.6

.

4 SSH-Tunnel

4.1

.

4.2

.

4.3

.

4.4

.

5 OpenVPN

5.1

.

5.2

.

5.3

.

5.4

.

5.5

.

5.6

.

6 HTTP-Tunnel

6.1

.

6.2

.

6.3

.

6.4

.

6.5

.

6.6

.

Literatur

[1] www.netfilter.org/documentation/HOWTO/de/NAT-HOWTO-6.html

[2] <https://wiki.ubuntuusers.de/Router/>

ANHANG

2.2: ClientVM-Filterregeln

TODO: textfile

2.4: ClientVM Stateful Filtering

TODO: textfile