Team10 - Moritz Rupp, Viktor Brandl

Kontrollfragen

Bearbeitet von Moritz Rupp und Victor Brandl

Frage 3.1

> Worin unterscheiden sich die INPUT,FORWARD und OUTPUT Chain?

Input beschreibt die auf die Maschine eingehenden Verbindungen, Output die davon ausgehenden und Forward die von einer anderen Maschine kommen und auf eine andere weitergeleitet werden sollen.

Frage 3.2

> Wie können Sie eine Regel angeben, die nur für einen einzigen Host gilt?

Bei Destination Address wird eine konkrete IP angegeben

Frage 3.3

> Wie können Sie eine Regel angeben, die für ein ganzes Netzwerk gilt?

Bei Destination Address wird ein IP-Netz angegeben

Frage 3.4

> Welche Informationen werden benötigt, um eine Regel eindeutig zu bestimmen(5-Tupel)?

Protokoll, Startadresse, Startport, Zieladresse, Zielport

Frage 3.5

> Wie stellen Sie fest, ob ihre Regeln unerwünscht viel Verkehr blocken und welcherVerkehr dies ist? Wie haben Sie geprüft, ob ihre Clients ihren Nameserver erreichen können?

Indem man den Syslog durchsucht oder Dienste auf ihre Funktion überprüft.
Den Nameswerver überprüft man indem man andere VMs mittels ihres Namens und nicht ihrer IP anpingt.

Frage 3.6

> Warum funktioniert der ping Befehl, ohne dass Sie jemals eine Regel dafür angelegt hatten?

Da der Ping-Befehl das ICMP-Protokoll verwendet. Dieses Läuft über die dritte Netzwerkschicht und unterhalb der vierten werden keine Ports benötigt.

Frage 3.7

> Weshalb ist es ausreichend, eine Regel für den Verbindungsaufbau von Ihren VMs zum Webserver auf lab99 zu erstellen? Weshalb ist keine Regel für die Rückrichtung nötig?

Nachdem der Verbindungsaufbau von VMs zu Webserver steht, reicht dieser Tunnel für allen nachfolgenden Traffic!