RN-Praktikum 4 14.01.2016
Gruppe: Andreas Berks, Dimitri Meier

Protokoll

3 Paketfilterung (Firewalling)

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

-I : Fügt eine Regel vorne an die Tabelle an
-s : Gibt eine Source-Adresse an
-d : Gibt eine Destination-Adresse an
-p : Gibt an welches Protokoll gemeint ist
-j : Gibt an, was mit dem Paket geschehen soll, wenn der Filter diese Regel anwendet

Lösung:

- sudo /sbin/rcSuSEfirewall2 restart
  Firewall auf Ursprungszustand stellen
- iptables –I INPUT –s 172.16.1.0/24 –j DROP
  Alle eingehende Pakete der Source-Adresse werden abgefangen und verworfen
- iptables –I OUTPUT –d 172.16.1.0/24 –j DROP
  Alle ausgehende Pakete der Destination-Adresse werden abfangen und verworfen
- iptables –I FORWARD –s 172.16.1.0/24 –j DROP
  Alle Weiterleitungen der Source-Adresse werden abgefangen und verworfen
- iptables –I FORWARD –d 172.16.1.0/24 –j DROP
  Alle Weiterleitungen der Destination-Adresse werden abgefangen und verworfen

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 2/3) auf Port 51000 genutzt werden kann. Alle anderen Verbindungen über dieses Netz sollen gesperrt sein“

Lösung:

- sudo /sbin/rcSuSEfirewall2 restart
  Firewall auf Ursprungszustand stellen
- iptables --policy INPUT DROP
  Jede Art von eingehenden Paketen wird verworfen
- iptables --policy OUTPUT DROP
  Jede Art von ausgehenden Paketen wird verworfen
- iptables --policy FORWARD DROP
  Jede Art von Weiterleitungen wird verworfen

- iptables –I INPUT –p tcp 51000 –s 172.16.1.0/24 –m state --state NEW, ESTABLISHED –j ACCEPT
  Es werden nur TCP Anfragen über den Port 51000 aus dem Netzwerk 172.16.1.0/24 zugelassen
- iptables –I OUTPUT –m state --state ESTABLISHED,RELATED –j ACCEPT
  Es werden nur ausgehende TCP Pakete zugelassen, die keine Verbindungsaufbau beinhalten

c) „Konfigurieren Sie den Rechner so, dass man keine TCP-Server auf diesem Rechner über das Netz 172.16.1.0/24 ansprechen kann. Alle anderen Verbindungen über dieses Netz sollen dagegen möglich sein“

Lösung

- sudo /sbin/rcSuSEfirewall2 restart
  Firewall auf Ursprungszustand stellen
- iptables --policy INPUT ACCEPT
  Jede Art von eingehenden Paketen wird akzeptiert
- iptables --policy OUTPUT ACCEPT
  Jede Art von ausgehenden Paketen wird akzeptiert
- iptables --policy FORWARD ACCEPT
  Jede Art von Weiterleitungen wird akzeptiert

- iptables –I INPUT –p tcp –s 172.16.1.0/24 –m tcp –m state –state NEW –j DROP
  Eingehende Verbindungsaufbau TCP Pakete werden von der Source-Adresse verworfen
- iptables –I INPUT –p tcp –s 172.16.1.0/24 –m tcp –m state –state ESTABLISHED,RELATED –j DROP
  Eingehende