Security & Firewalls: Plesk-Firewall: Logging aktivieren

Problem:

Um das ein oder andere Problem zu analysieren, benötigt man auch schon mal die Logging-Option der `iptables`. Wer aber seine Firewall über Plesk administriert hat keinerlei Eingriffsmöglichkeit.

Hier eine Anleitung zum kurzfristigen aktivieren der Logging-Option

Lösung:

Ohne die Tiefen von `iptables` erklären zu wollen, hier der grobe Ablauf:

- 1. Wir erstellen eine eigene Chain für Drop-Anweisungen.
- 2. In dieser Chain werden die zwei Schritte ausgeführt: `LOG` und `DROP`
- 3. Wir ersetzten die letzte `iptables`-Rule der `INPUT`-Chain (nämlich den `DROP`) und aktivieren statt dessen unsere neue Chain.

Natürlich könnte man direkt die Firewall-Regeln von Plesk bearbeiten: `/usr/local/psa/var/modules/firewall/`. Da Plesk dies aber überschreibt, schreiben wir uns ein eigenes Script, welches unser Logging einfach dazu schaltet.

Automatisiert als eigenes Script sieht es wie folgt aus. Wer mag kann die einzelnen Zeilen auch in die Kommandozeile eintippen. (Geht manchmal schneller.)

```
#!/bin/sh

IPTABLES=/sbin/iptables

#Eigene Chain "LOGDROP" initialisieren (inkl Löschen falls vorhanden)
IPTABLES -F LOGDROP
IPTABLES -X LOGDROP
IPTABLES -N LOGDROP
IPTABLES -A LOGDROP -j LOG
IPTABLES -A LOGDROP -j DROP

#Wir suchen die letzte Zeile (DROP) der INPUT-Chain und ersetzten diese
```

```
INPUT_NUM=´IPTABLES --line-numbers -nL INPUT | tail -n1| cut -d' ' -f1´
IPTABLES -R INPUT INPUT_NUM -j LOGDROP
```

<!--
IPTABLES -D INPUT INPUT_NUM
#und setzten nun unsere LOGDROP-Chain dran
IPTABLES -A INPUT -j LOGDROP
//-->

Vorher sollte man überprüfen ob wirklich `DROP` als letzte Rule in der INPUT-Chain steht!

Eine mögliche Erweiterung wäre alle `DROP`-Anweisungen die evtl. auch dazwischen stehen zu ersetzten. Auch dies wäre mit einer kleinen `for`-Schleife und ohne den `tail -n1` machbar.

Um die original Plesk-Regeln wieder herzustellen startet man entweder das Script unter `/usr/local/psa/var/modules/firewall/` oder schaltet im Plesk-Panel die Firewall kurz aus und wieder an.

Weitere Links:

- Vorüberlegung: Macht eine Firewall auf einem Server Sinn?

Eindeutige ID: #1386
huschi
2010-05-27 09:18