Regeln gegen PortScans

Diese vier `iptables`-Befehle dienen der Absicherung des Servers gegen unübliche Netzwerkpakete. Sie werden häufig eingesetzt, um **Port-Scans** (Sondierungen durch Angreifer) zu erkennen, zu protokollieren (loggen) und zu blockieren.

1. Null-Scan-Erkennung und Ratenbegrenzung

```
iptables -A INPUT -p tcp --tcp-flags ALL NONE -m limit --limit 1/h -j ACCEPT
```

- **`-A INPUT`**: Hängt die Regel an die `INPUT`-Kette an (gilt für alle eingehenden Pakete).
- **`-p tcp`**: Filtert nur den TCP-Netzwerkverkehr.
- **`--tcp-flags ALL NONE`**: Überprüfe alle TCP-Flags (SYN, ACK, FIN, RST, URG, PSH), aber keines davon darf gesetzt sein (`NONE`). Ein TCP-Paket ohne jegliche Flags ist laut Netzwerkstandard (RFC) ungültig. Angreifer nutzen dies für einen sogenannten **„Null-Scan“**, um offene Ports zu finden.
- **`-m limit --limit 1/h`**: Nutzt das Limit-Modul. Diese Regel greift nur maximal **1-mal pro Stunde** (`1/h`).
- **`-j ACCEPT`**: Lässt das Paket durch (erlaubt es).
- **Sinn dieser Regel:** Sie erlaubt maximal ein einziges solches "Null-Scan"-Paket pro Stunde (z. B. für legitime Messungen oder Toleranz bei Übertragungsfehlern). Alle weiteren Null-Scan-Pakete, die innerhalb dieser Stunde eintreffen, ignorieren diese Regel und fallen in der Firewall-Liste weiter nach unten, wo sie in der Regel durch eine allgemeine BLOCK-Regel blockiert werden.

---

2. Xmas-Scan-Erkennung und Ratenbegrenzung

```
iptables -A INPUT -p tcp --tcp-flags ALL ALL -m limit --limit 1/h -j ACCEPT
```

- **`--tcp-flags ALL ALL`**: Überprüfe alle TCP-Flags, und **alle** müssen gleichzeitig gesetzt sein (`ALL`). Ein Paket, bei dem alle Flags aktiv sind, ist im normalen Netzwerkverkehr unmöglich. Man nennt dies einen **„Xmas-Scan“** (Weihnachtsbaum-Scan), weil das Paket quasi „wie ein Weihnachtsbaum leuchtet“. Auch dies wird von Angreifern zur Erkennung des Betriebssystems oder offener Ports genutzt.

- **`-m limit --limit 1/h -j ACCEPT`**: Wie beim ersten Befehl wird auch hier maximal 1 solches Paket pro Stunde akzeptiert, um Fehlalarme oder minimale Tests zuzulassen. Der Rest wird durch nachfolgende Regeln blockiert.

---

3. Ungültige Verbindungsaufbaue protokollieren (Loggen)

```
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j LOG --log-prefix "Stealth Scan"
```

- **`! --syn`**: Das Ausrufezeichen steht für eine Verneinung (NOT). Es bedeutet: Das TCP-Paket hat das `SYN`-Flag **nicht** gesetzt.
- **`-m state --state NEW`**: Das Paket versucht laut Verbindungsverfolgung (Connection Tracking) eine **neue** (`NEW`) Verbindung aufzubauen.
- **Sinn dieser Kombination:** Ein regulärer, legaler TCP-Verbindungsaufbau (Three-Way-Handshake) **muss** zwingend mit einem `SYN`-Paket beginnen. Wenn ein Paket eine neue Verbindung anfordert (`NEW`), aber kein `SYN`-Flag trägt (`! --syn`), ist das technisch unmöglich und deutet stark auf einen Port-Scan (z. B. FIN- oder ACK-Scan) oder einen Angriffsversuch hin.
- **`-j LOG --log-prefix "Stealth Scan"`**: Dieses Paket wird nicht blockiert, sondern im System-Log (meist `/var/log/messages` oder `dmesg`) mit dem Präfix „Stealth Scan“ protokolliert, damit der Administrator den Angriffsversuch nachvollziehen kann.

---

4. Ungültige Verbindungsaufbaue blockieren (Droppen)

```
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
```

- **Match-Kriterien (identisch zu Befehl 3):** Es sucht wieder nach TCP-Paketen, die eine neue Verbindung aufbauen wollen, ohne das `SYN`-Flag zu besitzen.
- **`-j DROP`**: Dieses Paket wird sofort und kommentarlos verworfen (gelöscht).
- **Zusammenspiel mit Befehl 3:** Diese beiden Befehle (3 und 4) werden in genau dieser Reihenfolge hintereinander in die Firewall eingepflegt. Dadurch wird das verdächtige Paket zuerst registriert und im Logbuch vermerkt (Befehl 3) und direkt im nächsten Schritt blockiert (Befehl 4).

Hier nochmal zusammengefaßt

```
iptables -A INPUT -p tcp --tcp-flags ALL NONE -m limit --limit 1/h -j ACCEPT
iptables -A INPUT -p tcp --tcp-flags ALL ALL -m limit --limit 1/h -j ACCEPT
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j LOG --log-prefix "Stealth Scan: "
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
```

Created 2026-06-24 11:10:58 UTC by Mich3l
Updated 2026-06-24 11:19:59 UTC by Mich3l