Security & Firewalls: Portscan-Honeypot mit iptables

Problem:

Ein typisches Symptom bevor es zu einem DoS-Angriff oder ähnliches kommt ist ein Portscan. Dabei werden systematisch alle wesentlichen Ports einer IP angeklopft um dahinter stehende Software-Versionen zu erkennen und ggf. auf Schwachstellen zu finden.

Lösung:

Neben vielen Tools und Honeypot-Funktionen läßt sich sowas auch ganz einfach mit Linux-Boardmitteln erledigen. Wir nutzen dafür ein paar `iptables`-Regeln:

```
#!/bin/sh

HP_IPT='/sbin/iptables'
HP_Port=23
HP_Time=600

$HP_IPT -N honeypot
$HP_IPT -A INPUT -s ! 127.0.0.1 -j honeypot
$HP_IPT -A honeypot -m recent --update --seconds $HP_Time --name portscan -j DROP
$HP_IPT -A honeypot -p tcp -m tcp --dport $HP_Port -m recent --name portscan --set -j
LOG --log-prefix "IPTABLES -- HONEYPOT -- P $HP_Port " --log-level 6 --log-ip-options
$HP_IPT -A honeypot -p tcp -m tcp --dport $HP_Port -m recent --name portscan --set -j
DROP
$HP_IPT -A honeypot -j RETURN
```

Hier wird Port 23 (Telnet) als Honeypot eingesetzt. Wer dort anklopft wird erstmal für 600 Sekunden (== 10 Minuten) geblockt.

Achtung!

Da wohl manche Leute es mit ihrer Experimentierfreudigkeit etwas zu weit treiben, hier die Warnung:

Sperrt nicht Euren SSH-Port!!!!

Weitere Links:

- Beitrag von Nikosch in der er die Beispiele aus der Manpage von iptables zu einem Script zusammen fügt und deshalb auf eine explizite Erwähnung an dieser Stelle besteht.
- Diskussion über die Anwendung im Server Support Forum.

Security & Firewalls: Portscan-Honeypot mit iptables

Eindeutige ID: #1354
huschi
2009-04-06 23:32