# Einfache Angriffserkennung

## scanlogd

protokolliert erkannte Scans per syslogd mit der Kategorie daemon.alert

Start des Dienstes über init nach der Aktivierung der Netzkarte und dem Start von syslogd

Funktionsweise:

- scanlogd besetzt einen Socket zur Überwachung aller empfangenen IP-Datagramme
- ein "Scan" wird interpretiert bei bei der Ansprache von mindestens 7 verschiedenen privilegierten oder 21 nichtprivilegierten Ports im Abstand von maximal 3 Sekunden durch den gleichen Absender.
- Um dies als Ereignis zu protokollieren, müssen mindestens 5 Scans innerhalb von 20 Sekunden erfolgen.

```
notebookneu:~ # tail -f /var/log/messages
Feb  2 16:38:56 notebookneu scanlogd: 172.16.2.100 to 172.16.2.200 ports
13, 17, 21, 22, 23, 25, ..., fSrpauxy, TOS 00, TTL 128 @16:38:56
```

## arpwatch

Das Tools arpwatch überwacht die Zuordnung zwischen Ethernet- und IP-Adressen. Beim Einsatz lernt es alle neuen IP-Ethernet Zuordnungen, trägt diese in eine Liste ein und informiert root via Mail über jeden neuen Host. Sobald sich eine bekannte Kombination ändert wird root via Mail gewarnt. Zudem werden diese und weitere Äuffälligkeiten auch im syslog vermerkt.

ARPwatch zählt nicht zur den Vollwertigen IDS Programmen sondern zur der Software die sich auf eine spezielle Art von Angriffen spezialisiert haben. So ist ARPwatch nur in der Lage solche Angriffe zuerkennen die durch eine Manipulation des ARP Protokolls durchgeführt werden. Zur solchen Angriffen zählt zum Beispiel ARP Spoofing.

Funktionsweise:
Arpwatch erstellt auf Grund der ARP-Broadcasts eine Datenbank mit MAC-Informationen. Stellt z.B. doppelte oder sich ständig ändernte IP-Adressen fest. Das Ergebnis wird in einem File 'arp.dat' gesammelt und parallel ins syslog-File geschrieben. Hierüber erfolgt eine weitere Auswertung und Eskalation über Logsurfer
Im Verzeichniss /var/lib/arpwatch/ speichert es in einer Textdatei alle MAC-IP-Paarungen die schon einmal vorgekommen sind. Neue Paarungen werden hier hinein geschrieben.

Problem:
Arpwatch funktioniert nur innerhalb einer Broadcast Domaene, also nicht ueber Router, L3-Switches, WAN-Verbindungen hinweg. Moegliche Ansätze um dieses 'Problem' zu umgehen

1. falls es eine geswitchte L3-Umgebung ist, das Netzwerk-Interface im VLAN-Modus betreiben.
2. am Router entsprechende ARP-Request und Reply gezielt durchlassen.

```
notebookneu:~ # tail -f /var/log/messages
Feb  2 17:59:16 notebookneu arpwatch: listening on eth0
Feb  2 17:59:43 notebookneu arpwatch: new station 172.16.2.250 0:50:7f:f:46:5e
Feb  2 17:59:43 notebookneu arpwatch: new station 172.16.2.200 0:2:3f:db:4c:23
Feb  2 18:00:03 notebookneu arpwatch: new station 172.16.2.100 0:e:a6:b5:57:5a
```