Klaus Gerhardt – Linux Seiten

iptables und Stealth Scans

iptables und Stealth Scans

Copyright, Nutzungsbedingungen, Haftungsausschluss

Feedback ist willkommen

Feedback ist willkommen. Feedback, Fehlermeldungen, Korrekturen, etc. bitte senden an:

k-gerhardt@gmx.de

iptables und Stealth Scans

Ich habe das Verhalten von iptables bezüglich Port-Scans und insbesondere auch bezüglich Stealth Scans untersucht. Die gute Nachricht vorneweg: iptables konnte alle von mir durchgeführten Scans entdecken und zeigte in den Log-Dateien die entsprechenden Pakete an.

Die Erklärung zu den einzelnen Scan-Typen fndet man in dem Dokument "TCP-Flags, Handshakes, Stealth-Scans" auch auf dieser Webseite bei dem Thema "Security Spikzettel".

Der Versuchsaufbau

Der Scanner ist ein Rechner mit:

SuSE Version 8.0
nmap-2.54BETA30-75

Der Zielhost ist ein Rechner mit:

SuSE Version 9.0
iptables-1.2.8-71

Entscheidend für das Verhalten von iptables und die Beurteilung sind 3 Regeln in der Firewall:

iptables -A INPUT -i $IF -d $LOCIP -m state --state NEW,INVALID -j LOG --log-prefix "FW-INCM: => " --log-level 5

iptables -A INPUT -i $IF -m state --state NEW,INVALID -j DROP

iptables -A INPUT -j LOG --log-prefix "FW-REMAIN: => " --log-level 5

Es gibt noch mehr Regeln, die spielen aber bei dieser Betrachtung keine Rolle.

* Die erste Regel ist für das Logging der Pakete nach /var/log/messages zuständig.
    * Es werden alle Pakete in die Logdatei geschrieben die den Zustand NEW oder INVALID aufweisen.
    * Die Einträge in /var/log/messages werden alle mit dem –log-prefix "FW-INCM" versehen.

    Wenn man sich die Logeinträge unten ansieht, weisen diese alle den –log-prefix "FW-INCM" auf.

* Die zweite Regel verwirft schlicht und einfach alle Pakete die den Zustand NEW oder INVALID aufweisen.

* Die dritte Regel wiederum erstellt Logeinträge von allen Paketen, die alle Filterregeln passiert haben, auf die aber keine Filterregel zutraf. Dabei erhalten diese Pakete den –log-prefix "FW-REMAIN".

Da es bei den Logeinträgen keine Einträge mit dem –log-prefix "FW-REMAIN" gibt, müssen die Pakete also schon vorher von einer Filterregel verworfen worden sein. Dies geschieht hier durch meine zweite Regel.

Daraus ersieht man, dass die State Machine bzw. das Connection Tracking von iptables sehr wohl in der Lage ist Stealth Scans zu erkennen und die Pakete aus dem Scan zu verwerfen. Als kleiner Nebeneffekt wird dabei nmap auch noch so getäuscht, dass es glaubt die gescannten Ports seien im Zustand "open". Dies ist eigentlich nicht in unserem Sinne. Denn das könnte den Angreifer ja zu weiteren Aktionen ermutigen.

Anmerkung!

Von dem TCP Connect Scan mal abgesehen, funktionieren die Scans mit nmap nur einwandfrei wenn die Option -P0 verwendet wird.

Die Dokumentation der Scans

TCP Connect Scan ohne Firewall

Hier zuerst ein ganz normaler TCP Connect Scan, ausgeführt mit nmap gegen den Rechner 192.168.1.2. Der Rechner ist nicht durch eine Firewall geschützt.. Hier sieht man auch welche Ports wirklich geöffnet sind und kann dies dann mit den Ergebnissen der unten folgenden b Scans vergleichen.

```
pc686-lin:~ # nmap -sT 192.168.1.2

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on athlon-lin.local (192.168.1.2):
(The 1540 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
80/tcp     open        http
111/tcp    open        sunrpc
139/tcp    open        netbios-ssn
631/tcp    open        cups
845/tcp    open        unknown
991/tcp    open        unknown
2049/tcp   open        nfs
6000/tcp   open        X11

Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

Da es keine Firewall gibt, gibt es auch keine LOG-Einträge in /var/log/messages..

TCP Connect Scan mit Firewall

Jetzt der TCP Connect Scan mit nmap gegen den Rechner 192.168.1.2. Dieser hat eine Firewall, realisiert mit iptables. Der Befehl beschränkt sich auf eine Auswahlwahl von Ports die mit dem Parameter -p übergeben werden.

```
pc686-lin:~ # nmap -sT -P0 -p 20,21,22,23,25,80,111,119,123,139 192.168.1.2

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on athlon-lin.local (192.168.1.2):
Port       State       Service
```

```
20/tcp     filtered    ftp-data
21/tcp     filtered    ftp
22/tcp     filtered    ssh
23/tcp     filtered    telnet
25/tcp     filtered    smtp
80/tcp     filtered    http
111/tcp    filtered    sunrpc
119/tcp    filtered    nntp
123/tcp    filtered    ntp
139/tcp    filtered    netbios-ssn


Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

Alle Ports werden von nmap als "filtered" klassifiziert. Daran sieht man, dass die Firewall funktioniert. Hier ein Auszug aus /var/log/messages. Die Port-Scans werden von iptables erkannt. Man sieht, dass das SYN-Flag gesetzt ist.

```
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=51206 DF PROTO=TCP SPT=4164 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=62160 DF PROTO=TCP SPT=4165 DPT=21 WINDOW=5840 RES=0x00 SYN URGP=0
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=27824 DF PROTO=TCP SPT=4166 DPT=20 WINDOW=5840 RES=0x00 SYN URGP=0
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=24881 DF PROTO=TCP SPT=4167 DPT=111 WINDOW=5840 RES=0x00 SYN URGP=0
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=56509 DF PROTO=TCP SPT=4168 DPT=80 WINDOW=5840 RES=0x00 SYN URGP=0
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=40423 DF PROTO=TCP SPT=4169 DPT=22 WINDOW=5840 RES=0x00 SYN URGP=0
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=41261 DF PROTO=TCP SPT=4170 DPT=25 WINDOW=5840 RES=0x00 SYN URGP=0
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=37741 DF PROTO=TCP SPT=4171 DPT=139 WINDOW=5840 RES=0x00 SYN URGP=0
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=23559 DF PROTO=TCP SPT=4172 DPT=119 WINDOW=5840 RES=0x00 SYN URGP=0
Jun  6 22:36:42 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=35350 DF PROTO=TCP SPT=4173 DPT=123 WINDOW=5840 RES=0x00 SYN URGP=0
```

Bei allen weiteren Scans ist die Firewall auf dem Zielrechner aktiv.

TCP SYN Scan bzw. Half-Open Scan

Jetzt ein TCP SYN Scan. Das Ergebnis von nmap ist das gleiche.

```
pc686-lin:~ # nmap -sS -P0 -p 20,21,22,23,25,80,111,119,123,139 192.168.1.2

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on athlon-lin.local (192.168.1.2):
Port       State       Service
20/tcp     filtered    ftp-data
21/tcp     filtered    ftp
22/tcp     filtered    ssh
23/tcp     filtered    telnet
25/tcp     filtered    smtp
80/tcp     filtered    http
111/tcp    filtered    sunrpc
119/tcp    filtered    nntp
123/tcp    filtered    ntp
139/tcp    filtered    netbios-ssn


Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

Die Logeinträge in /var/log/messages sehen auch aus wie bei dem TCP Connect Scan. Da bei beiden Scan -Typen das SYN-Flag gesetzt ist, ist dies ja auch nicht verwunderlich.

```
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=21009 PROTO=TCP SPT=49797 DPT=20 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=47104 PROTO=TCP SPT=49797 DPT=119 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=18159 PROTO=TCP SPT=49797 DPT=22 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=22543 PROTO=TCP SPT=49797 DPT=23 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=7347 PROTO=TCP SPT=49797 DPT=21 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=49866 PROTO=TCP SPT=49797 DPT=139 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=12732 PROTO=TCP SPT=49797 DPT=111 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
```

```
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=44455 PROTO=TCP SPT=49797 DPT=123 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=60549 PROTO=TCP SPT=49797 DPT=80 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:28 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=9869 PROTO=TCP SPT=49797 DPT=25 WINDOW=4096 RES=0x00 SYN URGP=0
Jun  6 22:41:34 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1
```

Stealth FIN Scan

Als nächstes der Stealth FIN Scan. Das Ergebnis von nmap sieht allerdings etwas merkwürdig aus. Jetzt sollen plötzlich alle Ports offen sein? nmap lässt sich hier durch seinen eigenen Mechnismus täuschen. Bei Stealth FIN Scans (und auch allen anderen Stealth Scans) geht nmap von dieser Sachlage aus:

* Wenn der Port offen ist, wird das Paket des Scanners vom Zielrechner ignoriert.
* Wenn der Port geschlossen ist, antwortet der Zielrechner mit einem RST-Paket.

iptables ist hier aber so konfiguriert, dass es das Paket verwirft ohne eine Nachricht an den Quellhost zu senden. nmap lässt sich davon iritieren und zeigt alle Ports als "open" an.

```
pc686-lin:~ # nmap -sF -P0 -p 20,21,22,23,25,80,111,119,123,139 192.168.1.2

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on athlon-lin.local (192.168.1.2):
Port       State       Service
20/tcp     open        ftp-data
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
119/tcp    open        nntp
123/tcp    open        ntp
139/tcp    open        netbios-ssn


Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds
```

Und hier jetzt die Log-Einträge in /var/log/messages. Man sieht deutlich, dass es sich um den FIN Scan handelt, da nur das FIN-Flag gesetzt ist:

```
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=48523 PROTO=TCP SPT=49361 DPT=80 WINDOW=2048 RES=0x00 FIN URGP=0
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=42015 PROTO=TCP SPT=49361 DPT=20 WINDOW=2048 RES=0x00 FIN URGP=0
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=29957 PROTO=TCP SPT=49361 DPT=23 WINDOW=2048 RES=0x00 FIN URGP=0
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=23975 PROTO=TCP SPT=49361 DPT=22 WINDOW=2048 RES=0x00 FIN URGP=0
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=38434 PROTO=TCP SPT=49361 DPT=139 WINDOW=2048 RES=0x00 FIN URGP=0
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=30645 PROTO=TCP SPT=49361 DPT=21 WINDOW=2048 RES=0x00 FIN URGP=0
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=47551 PROTO=TCP SPT=49361 DPT=119 WINDOW=2048 RES=0x00 FIN URGP=0
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=49970 PROTO=TCP SPT=49361 DPT=25 WINDOW=2048 RES=0x00 FIN URGP=0
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=21997 PROTO=TCP SPT=49361 DPT=111 WINDOW=2048 RES=0x00 FIN URGP=0
Jun  6 22:28:26 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=42811 PROTO=TCP SPT=49361 DPT=123 WINDOW=2048 RES=0x00 FIN URGP=0
```

Stealth Xmas Tree Scan

Das gleiche Ergebnis beim Stealth Xmas Tree Scan:

```
pc686-lin:~ # nmap -sX -P0 -p 20,21,22,23,25,80,111,119,123,139 192.168.1.2

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on athlon-lin.local (192.168.1.2):
Port       State       Service
20/tcp     open        ftp-data
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
```

```
119/tcp    open        nntp
123/tcp    open        ntp
139/tcp    open        netbios-ssn


Nmap run completed -- 1 IP address (1 host up) scanned in 13 seconds
```

Bei den Logeinträgen sieht man wieder deutlich, dass der Xmas Tree Scan erkannt wurde. Es sind die Flags URG, PSH und FIN gesetzt.

```
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=3093 PROTO=TCP SPT=37196 DPT=25 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=35838 PROTO=TCP SPT=37196 DPT=21 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=22133 PROTO=TCP SPT=37196 DPT=111 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=23437 PROTO=TCP SPT=37196 DPT=119 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=10444 PROTO=TCP SPT=37196 DPT=22 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=31015 PROTO=TCP SPT=37196 DPT=23 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=56283 PROTO=TCP SPT=37196 DPT=139 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=11282 PROTO=TCP SPT=37196 DPT=80 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=52604 PROTO=TCP SPT=37196 DPT=20 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
Jun  6 22:48:13 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=839 PROTO=TCP SPT=37196 DPT=123 WINDOW=4096 RES=0x00 URG PSH FIN URGP=0
```

Stealth Null Scan

Das gleiche Ergebnis beim Stealth Null Scan:

```
pc686-lin:~ # nmap -sN -P0 -p 20,21,22,23,25,80,111,119,123,139 192.168.1.2

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on athlon-lin.local (192.168.1.2):
Port       State       Service
```

```
20/tcp     open        ftp-data
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
119/tcp    open        nntp
123/tcp    open        ntp
139/tcp    open        netbios-ssn

Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds
```

Bei den Logeinträgen sieht man auch hier wieder, dass der Null Scan erkannt wurde. Es sind überhaupt keine Flags gesetzt.

```
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=40773 PROTO=TCP SPT=43542 DPT=111 WINDOW=3072 RES=0x00 URGP=0
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=38115 PROTO=TCP SPT=43542 DPT=22 WINDOW=3072 RES=0x00 URGP=0
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=12753 PROTO=TCP SPT=43542 DPT=23 WINDOW=3072 RES=0x00 URGP=0
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=10920 PROTO=TCP SPT=43542 DPT=80 WINDOW=3072 RES=0x00 URGP=0
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=4270 PROTO=TCP SPT=43542 DPT=25 WINDOW=3072 RES=0x00 URGP=0
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=6114 PROTO=TCP SPT=43542 DPT=119 WINDOW=3072 RES=0x00 URGP=0
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=22157 PROTO=TCP SPT=43542 DPT=123 WINDOW=3072 RES=0x00 URGP=0
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=1366 PROTO=TCP SPT=43542 DPT=21 WINDOW=3072 RES=0x00 URGP=0
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=24674 PROTO=TCP SPT=43542 DPT=139 WINDOW=3072 RES=0x00 URGP=0
Jun  6 22:51:12 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=50 ID=40464 PROTO=TCP SPT=43542 DPT=20 WINDOW=3072 RES=0x00 URGP=0
```

ACK Scan

Und zuletzt der ACK Scan. Dieser liefert wieder eine korrekte Klassifizierung. Alle Ports sind im Zustand "filtered". Das heisst die Firewall arbeitet korrekt!

```
pc686-lin:~ # nmap -sA -P0 -p 20,21,22,23,25,80,111,119,123,139 192.168.1.2

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on athlon-lin.local (192.168.1.2):
Port       State       Service
20/tcp     filtered    ftp-data
21/tcp     filtered    ftp
22/tcp     filtered    ssh
23/tcp     filtered    telnet
25/tcp     filtered    smtp
80/tcp     filtered    http
111/tcp    filtered    sunrpc
119/tcp    filtered    nntp
123/tcp    filtered    ntp
139/tcp    filtered    netbios-ssn

Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

Und hier die Logeinträge. Nur das ACK-Flag ist gesetzt.

```
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=38424 PROTO=TCP SPT=34677 DPT=25 WINDOW=1024 RES=0x00 ACK URGP=0
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=59059 PROTO=TCP SPT=34677 DPT=139 WINDOW=1024 RES=0x00 ACK URGP=0
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=27571 PROTO=TCP SPT=34677 DPT=111 WINDOW=1024 RES=0x00 ACK URGP=0
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=11197 PROTO=TCP SPT=34677 DPT=123 WINDOW=1024 RES=0x00 ACK URGP=0
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=22085 PROTO=TCP SPT=34677 DPT=22 WINDOW=1024 RES=0x00 ACK URGP=0
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=5465 PROTO=TCP SPT=34677 DPT=23 WINDOW=1024 RES=0x00 ACK URGP=0
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=51928 PROTO=TCP SPT=34677 DPT=20 WINDOW=1024 RES=0x00 ACK URGP=0
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
```

```
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=34066 PROTO=TCP SPT=34677 DPT=21 WINDOW=1024 RES=0x00 ACK URGP=0
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=47942 PROTO=TCP SPT=34677 DPT=119 WINDOW=1024 RES=0x00 ACK URGP=0
Jun  6 23:05:45 athlon-lin kernel: FW-INCM: => IN=eth0 OUT= MAC=00:0c:6e:d0:8e:66:00:40:95:45:8f:86:08:00 SRC=192.168.1.1 DST=192.168.1.2
LEN=40 TOS=0x00 PREC=0x00 TTL=56 ID=20314 PROTO=TCP SPT=34677 DPT=80 WINDOW=1024 RES=0x00 ACK URGP=0
```