Mailserver

PortSentry installieren

PortSentry kann man mittlerweile von SourceForge runterladen.
Dazu sucht man sich auf der Seite http://sourceforge.net/projects/sentrytools/ das Tool PortSentry aus, und folgt einfach den Links.

Wenn PortSentry nach /usr/src runtergeladen wurde, kann man nun fortfahren.

```
# cd /usr/src
# tar -xzf portsentry-1.2.tar.gz
```

In der Datei portsentry_config.h kann man schon einiges konfigurieren, wie z.B. den Pfad zur Konfigurationsdatei, und die Syslog Einstellungen.
Beachten sollte man hierbei, dass die Bretterkreuze (#) nicht als Kommentarzeichen dienen, sondern Anzeiger für Compilerbefehle sind, also nicht löschen!

Um meiner Empfehlung der Installation nach /usr/local/portsentry zu folgen, sollte die Datei wiefolgt abgeändert werden.

```
#define CONFIG_FILE "/usr/local/portsentry/portsentry.conf"
```

Nun muss die portsentry.conf editiert werden, dazu die Einträge suchen und abändern:

```
IGNORE_FILE="/usr/local/portsentry/portsentry.ignore"
HISTORY_FILE="/usr/local/portsentry/portsentry.history"
BLOCKED_FILE="/usr/local/portsentry/portsentry.blocked"
```

Um den Angreifer via Packet Filter zu blocken (empfohlene Methode), muss eine der Optionen KILL_ROUTE aktiviert werden.
Ich persönlich benutze IpTables, darum nehme ich das Kommentar vor

```
KILL_ROUTE="/usr/sbin/iptables -I INPUT -s $TARGET$ -j DROP
```

weg und ändere /usr/sbin/iptables auf den Pfad zu IpTables in meinem System.
Dieser Pfad lässt sich leicht mit

```
# whereis iptables
```

herausfinden.

Wer will, kann noch den Text der Variable PORT_BANNER ändern und das Kommentar davor löschen.

Nun muss die Datei portsentry.ignore bearbeitet werden.
Hier muss mindestens 127.0.0.1, 0.0.0.0 und die IP des Servers rein.
Wenn die IP-Adresse (wie beim 1&1 Rootserver) via DHCP vergeben wird, muss hier auch die Adresse des DHCP-Servers rein.
Diese DHCP-Adresse kann man mittels

cat /var/state/dhcp/dhcpcd-eth0.info | grep DHCPSIADDR

herausfinden.

Die Datei portsentry.ignore kann dann so aussehen:

```
# lo
127.0.0.1

#
0.0.0.0

# IP des Servers
217.xx.xx.xx

# IP des DHCP-Servers
217.xx.xx.xx
```

---

2. Kompilieren/Installieren
Um den Installationspfad auf /usr/local/portsentry zu setzen, muss Makefile noch abgeändert werden.
Dazu muss ungefähr in Zeile 40 die Variable INSTALLDIR auf /usr/local gesetzt werden.

Dann wieder in der Konsole:

```
# make linux
# make install
```

Nun ist PortSentry unter /usr/local/portsentry installiert.

---

3. Automatisierung
Im Moment wird der Angreifer solange geblockt, bis die Filterregeln manuell entladen werden.
Um das Entladen zu vereinfachen, habe ich noch ein kleines Perlscript geschrieben, das man in das PortSentry Installationsverzeichnis mit rein packt.

```
# cd /usr/local/portsentry
# wget http://www.rob-schulze.de/informatik/tutorials/portsentry/filtermgr
# chmod 700 filtermgr
```

Im Script muss unbedingt eine Variable angepasst werden.
Je nachdem, in welches Verzeichnis man das Script packt, muss die Variable $BASE_DIR entsprechend angepasst werden.
Ich gehe hier von dem Verzeichnis aus, in das ich auch PortSentry installiert habe.
Hier bitte aufpassen, dass kein Slash am Ende steht und das Semikolon nicht

vergessen.

my $BASE_DIR="/usr/local/portsentry";

Nun muss das Script mit PortSentry verbunden werden.
Dazu öffnet man die /usr/local/portsentry/portsentry.conf und löscht erstmal (oder kommentiert) alle KILL_ROUTE Einträge. Außerdem muss man sich noch folgende Einträge suchen und folgend abändern, damit nun lediglich das Script blockt, PortSentry dient nun ausschließlich zum Erkennen der Scans.

BLOCK_UDP="2"
BLOCK_TCP="2"

KILL_RUN_CMD="/usr/local/portsentry/filtermgr -a $TARGET$"

Die Zeit, nachdem eine geblockte IP wieder zugelassen werden soll, kann man innerhalb des Scripts einstellen.
Dazu einfach mit einem Editor öffnen und den Wert hinter $BLOCK_TIMEOUT (Standard habe ich als 30 Minuten festgelegt) ändern.
Achtung, die Zeit wird dort in Sekunden angegeben, man kann aber ohne Probleme die Übersicht halten, in dem man einfach z.B. 1 Stunde als 60*60 schreibt.
Hier bitte keine Anführungsstriche benutzen und das Semikolon nicht vergessen.

Um regelmäßig das Löschen der alten IPs zu veranlassen, reicht ein kleiner Cronjob.
Also die eine Datei /etc/cron.d/filtermgr erzeugen und Folgendes reinschreiben:

Jede halbe Stunde das Loeschen alter IPs veranlassen (portsentry)

*/30 * * * * /usr/local/portsentry/filtermgr -d

So nun fehlt bloß noch eins, nämlich ein Startskript, sodass PortSentry bei jedem Start automatisch geladen wird.

cd /etc/init.d
wget http://www.rob-schulze.de/informatik/tutorials/portsentry/rcportsentry
chmod 700 rcportsentry

Das Script muss nun bloß noch ins Runlevel 3 gelinkt werden:

cd /etc/init.d
ln -s /etc/init.d/rcportsentry /etc/init.d/rc3.d/S08portsentry
ln -s /etc/init.d/rcportsentry /etc/init.d/rc3.d/K17portsentry

Fertig.

Eindeutige ID: #1001

Mailserver

Verfasser: Michael Stender
Letzte Änderung: 2007-08-08 02:47