Security & Firewalls: Apache: DoS-Attacken abfangen

Problem:

Regelmäßig kommen auf gut besuchten Webseiten DoS (Denial of Service) Attacken vor. Entweder sind es spielende Script-Kiddies, schlecht programmierte Spider/Crawler oder echte Angriffe.

Funktion:

Ein (hier Web-)Server wird mit so vielen Anfragen bombardiert, daß er entweder ganz Langsam wird, oder auf Grund ausgehendem Speicher gar nicht mehr Antwortet.

Konsequenz ist häufig der Absturz des Serverdienstes oder manchmal sogar ein vollkommener Ausfall des Rechners selbst.

Abhilfe:

Um Apache selbst zu schützen, gibt es zwei Apache-Module:

1. mod_security

2. mod_evasive (Download auf huschi.net)

Während `mod_security` mehr für den Schutz vor seltsamen/verdächtigen Query-Strings zuständig ist, ist `mod_evasive` konkret gegen DoS-Angriffe.

mod_evasive erstellt eine interne Liste von IP-Adresse und angeforderten URLs. Sollten hier gewisse (frei definierbare) Schwellwerte überschritten werden, antwortet es automatisch mit einem 403, sperrt diese IP für 10 Sekunden und kann noch weitere Funktionen ausführen. (Z.B. Logging oder Warnungs-Mail versenden.)

Installation mod_security

Das Apache-Modul mod_security erhält man in den aktuellen Distributionen direkt als Software-Paket. So ist es z.B. unter Debian ganz schnell installiert:

```
apt-get install libapache2-mod-security
a2enmod mod-security
```

Es fehlen nur noch die richtigen Einstellungen in der `apache2.conf`:

```
‹IfModule mod_security.c›
  SecFilterEngine On
```

```
  # URL-Validierung aktivieren
  SecFilterCheckURLEncoding On
  # Unicode-Validierung aktivieren
  SecFilterCheckUnicodeEncoding On
  # HTTP-POST-Daten verarbeiten
  SecFilterScanPOST On
  # Standard-Aktion für zutreffende Filterregeln
  SecFilterDefaultAction "deny,log,status:403"
  # Filterregeln aus mod-security.d einbinden
  Include /etc/apache2/mod-security.d/[^.#]*
‹/IfModule›
```

Mit dem letzten Befehl wird ein Verzeichnis für die weiteren, selbst zu erstellenden Config-Files angegenben. Dort platzieren wir die eigentlichen Filter.

Beispiele finden wir bereits auf der Platte: `/usr/share/doc/libapache2-mod-security/examples/`.

Installation mod_evasive

Das Modul `mod_evasive` gibt es noch nicht als Distributions-Pakete. Also müssen wir es selber kompilieren.

Voraussetzung für jede Kompilation mit Apache ist natürlich das Apache-Devel-Paket!

```
#Prüfe auf Apache-Devel
whereis apxs
whereis apxs2
#Download und entpacken:
cd /usr/local/src/
wget http://www.huschi.net/download/mod_evasive_1.10.1.tar.gz
tar xzf mod_evasive_*
cd mod_evasive
```

Nun prüfen wir, ob es den angegebenen Mailer gibt (`whereis mail`) und welche Parameter er braucht. Das Modul ist auf `sendmail` ausgerichtet. Das Programm `/usr/bin/mail` kann aber auch der `mailx` sein.

In dem Fall darf der Parameter `-t` nicht verwendet werden und es wird in den Emails keine Subjekts angegeben.

```
edit mod_evasive20.c
#suche nach "#define MAILER" und korrigiere den Pfad.
```

Wer den `mailx` einsetzt, muss folgende Code-Änderungen machen:

```
#define MAILER "/usr/bin/mail -s \"HTTP BLACKLIST %s\" %s"
[....]
              snprintf(filename, sizeof(filename), MAILER, r->connection->remote_ip,
email_notify);
              file = popen(filename, "w");
              if (file != NULL) {
//              fprintf(file, "To: %s
", email_notify);
//              fprintf(file, "Subject: HTTP BLACKLIST %s

", r->connection->remote_ip);
                fprintf(file, "mod_evasive HTTP Blacklisted %s
", r->connection->remote_ip);
```

Nun bauen wir das Modul und binden es im Apache ein.

```
#Einfaches Compilieren mit Apache-Tool apxs:
apxs2 -cia mod_evasive20.c
#suchen wo das fertige Modul ist:
ls -l /usr/lib/apache2/mod_evasive*
ls -l /usr/lib/apache2/modules/mod_evasive*

#dementsprechend wird ein load-file angelegt:
echo "LoadModule evasive20_module  /usr/lib/apache2/mod_evasive20.so" ›
/etc/apache2/mods-available/mod_evasive.load
ln -s /etc/apache2/mods-available/mod_evasive.load /etc/apache2/mods-enabled/.
```

Nun fehlt nur noch die Datei `/etc/apache2/mods-available/mod_evasive.conf` die ebenfalls ins Verzeichnis `mods-enabled` gelinkt werden muß:

```
‹IfModule mod_evasive20.c›
    DOSHashTableSize    3097
    DOSPageCount        2
    DOSSiteCount        50
    DOSPageInterval     1
    DOSSiteInterval     1
    DOSBlockingPeriod   10
    DOSEmailNotify      webmaster@meine-domain.tld
‹/IfModule›
```

Security & Firewalls: Apache: DoS-Attacken abfangen

Achtung: im beiliegenden Readme steht auch noch die Direktive `DOSLogDir`. Die ist recht ungünstig benannt, da sie nichts mit Logfiles zu tun hat, sondern eher mit `Lock-Files`. Am besten läßt man sie per Default auf `/tmp/`. Falls man die Lockfiles doch woanders ablegen möchte (z.B. in `/var/lock/`) so sollte man sicherstellen, dass der Apache-User (`www-data` oder `wwwrun`) Schreibrechte darauf hat.

(Dies wird leider in einigen Howto's nicht erwähnt. Weshalb mod_evasive dann nicht funktioniert.)

Links:

- Bericht zu mod_security
- Artikel auf Heise.de: Web-Server mit mod_security absichern
- Artikel zu mod_evasive im Linux-Magazin
- Da auf NuclearElephant.com die Datei momentan nicht vorhanden ist, stelle ich sie hier zum Download zur verfügung.

Eindeutige ID: #1181
huschi
2009-01-21 23:15