

Internet Security 2009W

Protokoll

Google Analytics

Manuel Mausz, Matr. Nr. 0728348
manuel-tu@mausz.at

Wien, am 22. Oktober 2009

Inhaltsverzeichnis

Vorbereitung.....	3
Konfiguration des Webservers.....	3
PHP-Script.....	4
Erstellen des Dokument-Verzeichnisses.....	4
Starten des Webservers.....	5
Umlenkung der Domain.....	5
Aufruf verschiedener Webseiten sowie Auswertung der CSV-Datei.....	6

Vorbereitung

Unsere Aufgabe ist es, die HTTP-Anfragen an Google Analytics umzulenken und statt dessen unser eigenes Javascript auszuliefern, das die Anfragen anzeigt und/oder speichert.

Wir benötigen für diese Aufgabe eine Webserver-Software, die das Javascript per HTTP ausliefert. Da auf meinem Rechner bereits *Apache* Version 2.2.4 installiert ist, muss dieser lediglich entsprechend konfiguriert werden.

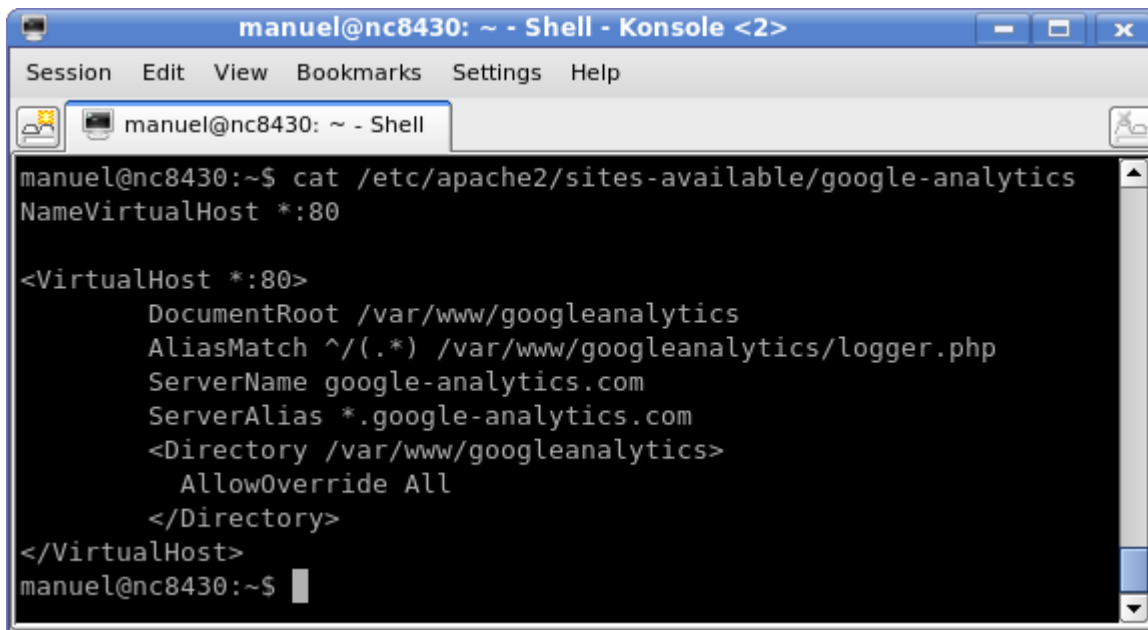
Um die Zugriffen auf Google Analytics zu speichern, wird anstatt einer Javascript-Datei, eine PHP-Datei vom Webserver ausgeliefert. Die PHP-Datei soll die Daten des Besuchers in einer CSV-Datei speichern.

Die Umlenkung der Domain von Google Analytics auf unseren Webserver wird über die Datei `/etc/hosts` bewerkstelligt.

Konfiguration des Webserver

Damit der Webserver Anfragen für eine Domain überhaupt annimmt, muss ein entsprechender VirtualHost erzeugt werden. Google Analytics verwendet die Domain „*www.google-analytics.com*“ bei HTTP und „*ssl.google-analytics.com*“ bei HTTPS. Über die Direktive *ServerName* und *ServerAlias* können wir entsprechende Domains für den VirtualHost bzw. direkt sämtliche Subdomains einer Domain akzeptieren.

Da Google Analytics kürzlich den Namen des einzubindenden Javascripts geändert hat und dies jederzeit wieder vorkommen kann, definieren wir über die Direktive *AliasMatch*, dass sämtliche Anfragen für den VirtualHost an unser PHP-Script geschickt werden, unabhängig von der tatsächlichen URL.



```
manuel@nc8430: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
manuel@nc8430: ~ - Shell
manuel@nc8430:~$ cat /etc/apache2/sites-available/google-analytics
NameVirtualHost *:80

<VirtualHost *:80>
    DocumentRoot /var/www/googleanalytics
    AliasMatch ^/(.*) /var/www/googleanalytics/logger.php
    ServerName google-analytics.com
    ServerAlias *.google-analytics.com
    <Directory /var/www/googleanalytics>
        AllowOverride All
    </Directory>
</VirtualHost>
manuel@nc8430:~$
```

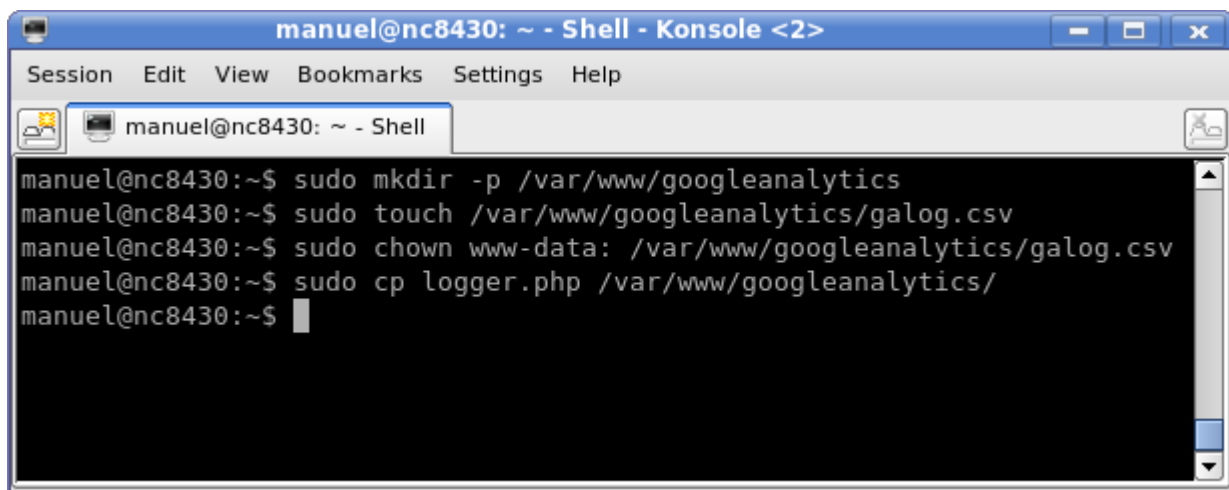
PHP-Script

Das PHP-Script hat die Aufgabe jede Auslieferung des Javascript-Codes an einen Browser zu protokollieren. Abgesehen von dem Zeitpunkt der Auflieferung wird die IP-Adresse, der dynamische Port, die angefragte URL, den HTTP Referer und User Agent sowie sämtliche Cookies für diese Domain im CSV-Format am Webserver selbst gespeichert.

```
1  <?php
2
3  $fp = fopen('galog.csv', 'a');
4  $fields = array(
5      time(),                // current time
6      $_SERVER["REMOTE_ADDR"], // ipaddress
7      $_SERVER["REMOTE_PORT"], // port
8      $_SERVER["REQUEST_URI"], // request uri
9      $_SERVER["HTTP_REFERER"], // referer
10     $_SERVER["HTTP_USER_AGENT"], // useragent
11     $_SERVER["HTTP_COOKIE"], // cookies
12 );
13 fputcsv($fp, $fields, "\t");
14 fclose($fp);
15
16 ?>
```

Erstellen des Dokument-Verzeichnisses

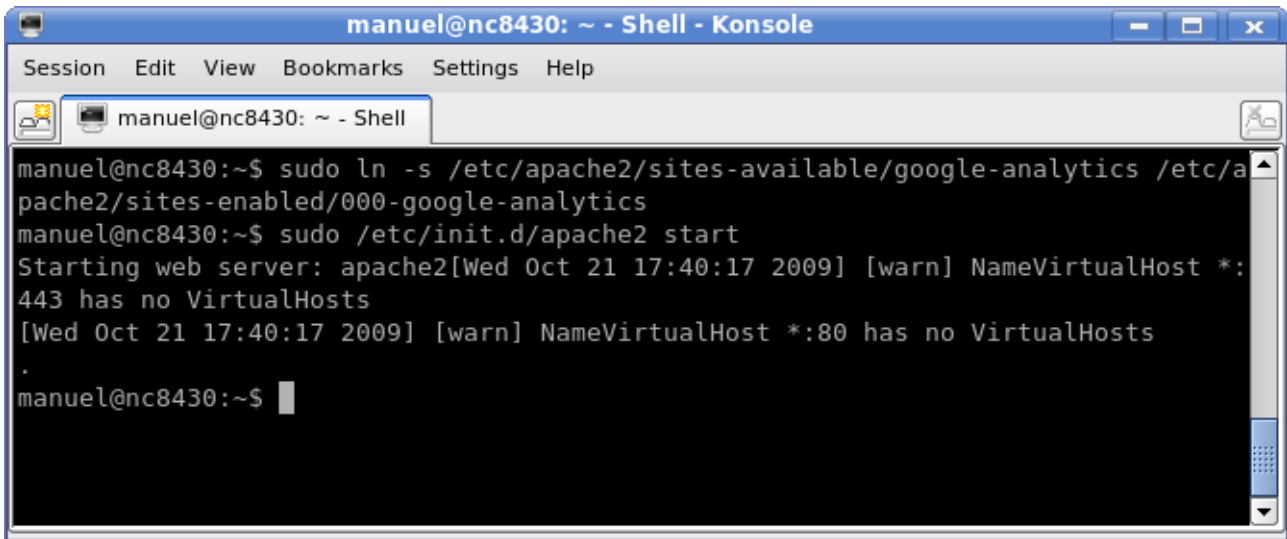
Diese Subaufgabe ist schnell erledigt. Das Verzeichnis (*DocumentRoot*) für den VirtualHost wird erstellt, das PHP-Script in das Verzeichnis kopiert und eine leere CSV-Datei erstellt. Damit der Webserver in diese Datei schreiben kann, muss noch der Besitzer geändert werden.



```
manuel@nc8430: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
manuel@nc8430: ~ - Shell
manuel@nc8430:~$ sudo mkdir -p /var/www/googleanalytics
manuel@nc8430:~$ sudo touch /var/www/googleanalytics/galog.csv
manuel@nc8430:~$ sudo chown www-data: /var/www/googleanalytics/galog.csv
manuel@nc8430:~$ sudo cp logger.php /var/www/googleanalytics/
manuel@nc8430:~$
```

Starten des Webservers

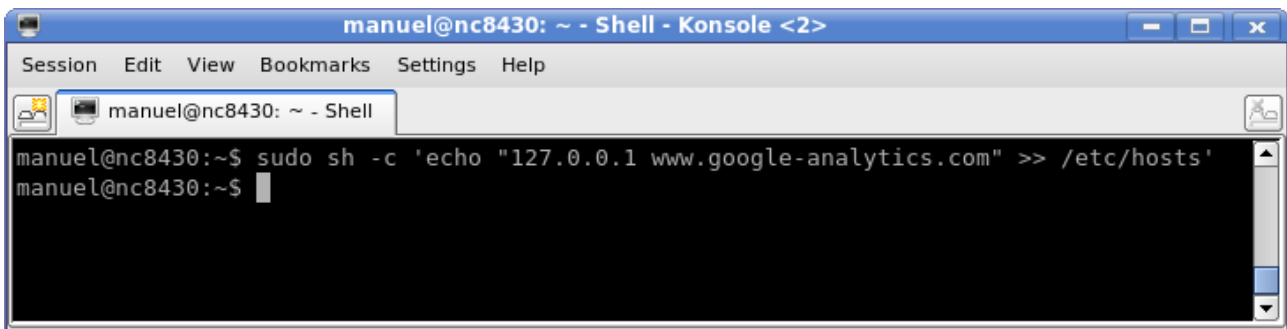
Dieser Punkt geht ebenfalls sehr schnell, da er nur aus einem Befehl besteht.



```
manuel@nc8430:~$ sudo ln -s /etc/apache2/sites-available/google-analytics /etc/a
pache2/sites-enabled/000-google-analytics
manuel@nc8430:~$ sudo /etc/init.d/apache2 start
Starting web server: apache2[Wed Oct 21 17:40:17 2009] [warn] NameVirtualHost *:
443 has no VirtualHosts
[Wed Oct 21 17:40:17 2009] [warn] NameVirtualHost *:80 has no VirtualHosts
.
manuel@nc8430:~$
```

Umlenkung der Domain

Die Umlenkung der Domain bzw. Hostnames kann über mehrere Mechanismen erfolgen. Die einfachste ist die Manipulation der Datei /etc/hosts. Die Datei existiert auf allen derzeit relevanten Systemen, und benötigt keinerlei Aktivierung. Sie besteht aus einer Auflistung von IP-Adressen und dazugehörigem Hostname. Scheint ein aufzulösender Hostname in dieser Datei auf, wird direkt die dazugehörige IP-Adresse zurück geliefert. Ist der Hostname nicht enthalten, wird er ganz gewöhnlich über das DNS System aufgelöst.



```
manuel@nc8430:~$ sudo sh -c 'echo "127.0.0.1 www.google-analytics.com" >> /etc/hosts'
manuel@nc8430:~$
```

Aufruf verschiedener Webseiten sowie Auswertung der CSV-Datei

Die Umlenkung wurde zur Datengewinnung einige Stunden aktiviert und üblich mit dem Browser gesurft.

Folgend ein Auszug der dabei gesammelten Daten:

Zeitstempel	IP-Adresse	Port	URL	HTTP Referer	User Agent
1256146793	127.0.0.1	50698	/urchin.js	http://pastie.org/663812	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256146808	127.0.0.1	50707	/ga.js	http://flash.plasticthinking.org/	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256146812	127.0.0.1	50707	/ga.js	http://flash.plasticthinking.org/	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256146839	127.0.0.1	58444	/ga.js	http://ask.metafilter.com/80862/how-split-a	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256146883	127.0.0.1	58487	/ga.js	http://blogoscoped.com/archive/2007-12-13	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256147197	127.0.0.1	33199	/ga.js	http://www.geekology.co.za/blog/2009/02/1	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256149236	127.0.0.1	37575	/ga.js	http://www.google.com/talk/	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256149246	127.0.0.1	37575	/ga.js	http://www.google.com/support/forum/p/Ta	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256149273	127.0.0.1	37584	/ga.js	http://www.google.com/support/forum/p/Ta	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256149312	127.0.0.1	37585	/ga.js	http://www.google.com/support/forum/p/Ta	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256149333	127.0.0.1	37586	/ga.js	http://www.google.com/support/forum/p/Ta	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256149344	127.0.0.1	37586	/ga.js	http://www.google.com/support/forum/p/Ta	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256149349	127.0.0.1	37586	/ga.js	http://www.google.com/support/forum/p/Ta	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256150104	127.0.0.1	53518	/ga.js	http://twitpic.com/mdfpn	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256150117	127.0.0.1	53518	/ga.js	http://twitter.com/FlorianGasser	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256150124	127.0.0.1	56003	/ga.js	http://twitter.com/FlorianGasser	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256151067	127.0.0.1	44389	/ga.js	http://mail.google.com/support/bin/answer.	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256151100	127.0.0.1	44392	/ga.js	http://www.google.at/intl/en/options/	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256151111	127.0.0.1	44392	/ga.js	http://www.google.com/talk/	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256151118	127.0.0.1	44392	/__utm.gif?utmwv=1.3&utmnn=1563	http://www.google.com/talk/about.html	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256151129	127.0.0.1	44392	/ga.js	http://www.google.com/talk/	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256152734	127.0.0.1	38362	/__utm.gif?utmwv=4.5.8&utmnn=13	http://gameinformer.com/b/news/archive/2	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256153724	127.0.0.1	60670	/__utm.gif?utmwv=4.5.8&utmnn=561	http://twitpic.com/mdo43	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256157613	127.0.0.1	45259	/__utm.gif?utmwv=4.5.8&utmnn=104	http://www.webhostingtalk.com/showthrea	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256157613	127.0.0.1	45259	/__utm.gif?utmwv=4.5.8&utmnn=11	http://www.webhostingtalk.com/showthrea	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256157629	127.0.0.1	44568	/urchin.js	http://markmail.org/message/iuwev2edbbd	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256157647	127.0.0.1	44585	/__utm.gif?utmwv=4.5.8&utmnn=834	http://forums.cpanel.net/f43/421-too-many-	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256157647	127.0.0.1	44585	/__utm.gif?utmwv=4.5.8&utmnn=10	http://forums.cpanel.net/f43/421-too-many-	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256160954	127.0.0.1	35096	/__utm.gif?utmwv=4.5.8&utmnn=833	http://twitter.com/club2	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r
1256160954	127.0.0.1	35096	/__utm.gif?utmwv=4.5.8&utmnn=17	http://twitter.com/club2	Mozilla/5.0 (X11; U; Linux x86_64; en-US; r