Block Ads Using the hosts File

Online ads displayed in web pages are annoying. Is there a way to reduce or eliminate them at the system level instead of installing browser plugins?

One effective way to prevent ads from appearing is to prevent the computer from making connections to them in the first place. This conserves bandwidth because if no connection is made to the ad server, then its content cannot be downloaded.

A simple method to achieve this is by editing the **/etc/hosts** file.

What is /etc/hosts?

This is a text file that resolves domain names to IP addresses. Whenever a domain name is entered in the URL bar of a web browser, it must first be resolved into an IP address to find the site on the Internet.

Usually, this involves a DNS lookup by connecting to a DNS server, which returns the IP address. However, before the DNS lookup is performed over the Internet, Linux checks the /etc/hosts file to see if the domain name can be resolved locally. If so, Linux uses that IP address without any further DNS resolution.

How Is This Useful?

We can use this to our advantage by associating known ad domain names with null or local IP addresses.

For example, if Linux sees the domain name http://www.nastyadserver.ads, it will check to see if there is a valid entry in /etc/hosts and use the associated IP address if found. We can put a bogus IP address, such as 0.0.0.0, in /etc/hosts for the www.nastyadserver.ads domain, and Linux will use 0.0.0.0 instead of finding the real IP address through a DNS lookup. Since 0.0.0.0 goes nowhere, the ad is never loaded.

This helps conserve bandwidth. Rather than downloading everything and then filtering out the junk before display, blocking the junk at the DNS lookup level prevents it from downloading in the first place.

What Is Blocked?

Everything that requires a DNS lookup is blocked. This includes malicious scripts, web bugs, ad servers, cookies, page counters, Flash ads, and other tricks advertisers use to clutter a page and monitor a user.

Entire sites can be blocked. Don't like googleanalytics? Then, block it in /etc/hosts by mapping it to 0.0.0.0. Are some sites offensive? Block them too in the same way. Again, since the DNS lookup is never performed, the connection is never made.

Of course, this does not work with direct IP addresses. Entering 192.168.1.1 in a browser's URL bar will load whatever is located at 192.168.1.1 regardless of what /etc/hosts instructs.

Obtaining a Pre-Made hosts File

There is a project that seeks to maintain an updated hosts file containing a list of known ad servers. This page, titled Blocking Unwanted Parasites with a Hosts File, contains a host file for download and instructions for installation. Adding this list to the existing /etc/hosts will prevent ads from appearing by resolving their domain names to 127.0.0.1.

Strategy

1. Start with the latest hosts file, and append it to the existing /etc/hosts.

2. Not all ad servers on the Internet are blocked, so when a new one appears, find its domain name and add it to /etc/hosts. Continue to do this for all domains to block, not just ads.

3. Save the hosts file for future use.

Editing /etc/hosts

Open **/etc/hosts** in a text editor.

```
sudo gedit /etc/hosts
```

Something like this will appear:

```
192.168.1.1 mysystem # Added by NetworkManager
127.0.0.1 localhost.localdomain localhost
::1 mysystem localhost6.localdomain6 localhost6
127.0.1.1 mysystem
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Keep these lines, and do not edit them since they are needed for the system. Append any blocked domain names to the end of the file.

Other than the default lines shown above, /etc/hosts will be empty. Each blocked domain name exists on its own line with the IP address (0.0.0.0 or 127.0.0.1) first, and the domain name second and separated by a whitespace.

Examples:

```
0.0.0.0 www.nastyadserver.ads
0.0.0.0 fr.weliketospyonyou.nowhere
0.0.0.0 m.t.whatisthis.huh
0.0.0.0 ad.server.notagain
```

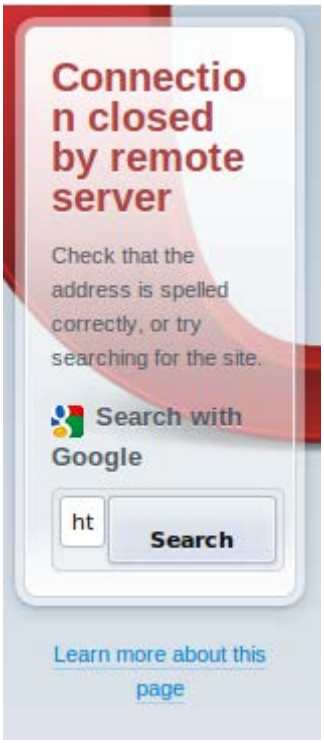
Before adding custom entries, begin by opening the downloaded hosts file in a text editor.

By default, domain names are mapped to 127.0.0.1. The null IP address 0.0.0.0 usually works better to avoid conflicts with any local servers that might be running on 127.0.0.1, so replace all 127.0.0.1 with 0.0.0.0 in the downloaded hosts file. Now, copy and paste the entire file into /etc/hosts after the system lines.

There is no need to reboot the system for the changes to take effect, but any open programs, such as web browsers, must be restarted.

What Happens?

Ads mapped to 0.0.0.0 will not appear. Other times, ad frames will display information similar to the “Connection closed by remote server” message seen in Opera.



A Blocked Site is Still Getting Through? Why?

There are two possible causes.

1. The /etc/hosts file might not be registered with open programs. Close all instances of the web browser. Check the System Monitor since there might be zombie processes of Firefox, for example, that are still running.

2. Check to make sure that the domain name is exact. If you wish to block uglyadsite.where, make sure it is spelled exactly as uglyadsite.where. Blocking is performed at the domain name level, so attempting to block a certain page will not work.
It could be that a different domain name or even a direct IP address is used for the connection. Some ads are sneaky, so double check. An entry in /etc/hosts might exist for y.lottaspam.fr.m, but the ad could be connecting directly to its server using an IP address. In this case, /etc/hosts will not help.

System-wide Use

The best part about /etc/hosts is that all programs requiring a DNS lookup check it by default. Whether it is an email client, web browser, media player, or whatever, any changes made to /etc/hosts affect them all. This saves time. Instead of editing each program one by one, a single entry added to /etc/hosts will be used by all programs.

Anti-Anti-Ad-Block

Some sites like to detect the Ad-Block addon for Firefox and deny access if Ad-Block is detected and enabled. Ad-Block is an excellent companion, but no site can detect and block the /etc/hosts file, so it should block access to known ad servers whether or not Ad-Block is installed.

Using with Windows

Another handy fact about /etc/hosts is that it is cross-platform compatible with the Windows hosts file. Windows performs DNS lookups in much the same way as Linux (local first, then remote). Any edits made on a Linux system are valid on a Windows system by copying the /etc/hosts file into Windows.

Different versions of Windows place the hosts file in different paths and add certain protections to the file, so consult the instructions for installation on the *Blocking Unwanted Parasites with a Hosts File* web page.

Conclusion

The /etc/hosts is effective in blocking connections to ad servers because it denies valid DNS lookups for specified domain names.

More ad-blocking strategies exists, so /etc/hosts is only one link in a much larger chain rather than a one-size-fits-all solution, but its common use by programs makes it an effective starting point.

Best of all, /etc/hosts is already present and editable without installing any browser plugins.

Source : https://delightlylinux.wordpress.com/2012/05/31/block-ads-using-the-hosts-file/