Anonymity

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

I can see you hiding in the shadows over there and so can the logs of all the web sites, FTP servers and other nooks and crannies you visit on the web. The sort of information gathered by these logs and which is available to the webmasters of the sites you visit include the address of the previous site you visited, your IP address, your computer's ID name, your physical location and the name of your ISP along with less personal details such as the operating system you're using and your screen resolution. If someone was snooping through your dustbin to gather information on consumer trends or tracking your every move to see where it is you go everyday you wouldn't be too chuffed would you. Well the web is no different, it's still an invasion of privacy and a threat to security and you don't have to put up with it.

Proxy servers:
Every time you visit a web site, detailed information about your system is automatically provided to the webmaster. This information can be used by hackers to exploit your computer or can be forwarded to the market research departments of consumer corporations who by tracking your activities on the internet are better equipped to direct more relevant spam at you. Your best defence against this is to use what is known as a proxy server, which will hide revealing information from the web sites you visit, allowing you to surf the web anonymously. These work by altering the way in which your browser retrieves web pages or connects to remote servers. With a proxy server set up, whenever you 'ask' IE or Netscape to look at a web page, the request is first sent through an external server which is completely independent of your ISP's servers. This third party server then does the requesting on your behalf so that it appears that the request came from them rather than you and your real IP address is never disclosed to the sites you visit. There is nothing to download and the whole process takes less than a minute.

There are two different ways to use proxy servers and both have their advantages and disadvantages. The first method is to use a web based service. What this involves is visiting the proxy's home page each time you want to browse a web site anonymously. The core component of such a system is the dialog box where you enter the address of the web site you want to visit. Each time you enter the URL of the site you want to browse via the proxy into this box, your personal information, IP address and so on is first encrypted before being sent to the site allowing you to maintain your anonymity. Two of the best examples of this type of web based proxy service are Code:
hxxp://www.rewebber.com/
and hxxp://www.anonymizer.com/.

Obviously one disadvantage of using a web based service like Rewebber or Anonymizer, however, is that you have to visit the proxies home page each time you want to surf anonymously. You could choose to select this page as your default home page, but it's still quite awkward if you're forever site hopping at the speed of light. The second main 'con' is that you often have to put up with extra adverts on the pages you visit. These are automatically inserted into the pages by the proxy - they have to pay for service somehow. More sophisticated and convenient solutions are also on offer yet they come with a price tag.

The second method you can use to protect your privacy via a proxy server involves adjusting the settings of your web browser so that you can surf anonymously without having to visit the home page of your proxy each time. To do this you will first need to know the name of your proxy server and the port number it uses. This information can be gleaned from either a public proxy server list or the FAQ referring to a private subscription based service. Once you have the name of the proxy server you wish to use, select 'Internet Options' from the 'Tools' menu of your browser. Now select 'Connections' followed by 'Settings' and tick the 'use a proxy server' check box. To finish the job all you have to do now is enter the name of the server in the 'address' box, the port which it uses in the 'port' box and go forth and surf anonymously.

Free, manual proxy servers as advertised on anonymity sites, if you can find one at all, are likely to be highly oversubscribed, and as a result the speed at which they retrieve web pages can deteriorate. In which case you can go in pursuit of a public proxy server list and select an alternative from it, which can then be set up manually. To locate such a list you can investigate sites such as Code:
hxxp://www.proxys4all.com/

however, this method isn't problem free either, so before you get too carried away and go jumping on the anonymity bandwagon there are a few things you should be aware of. It's very easy to use proxies to protect your privacy, but often the disadvantages of using them far out weigh the benefits. You see, the problem is that, like the proxy servers provided Rewebber et al, free, public proxies are nearly all over subscribed and so they can slow down web browsing considerably. Digging out fast reliable proxy servers is an art form in itself and is a skill which takes considerable practice. You could find a list of public proxy servers and then experiment with each one until you find one that runs at a reasonable speed, but this can be very time consuming and frustrating. Instead, your search would be much more efficient if you got a dedicated program to carry out this task for you. There are literally dozens of proxy seeking programs around which can do just that, and many of them are available as freeware. What these do is scan the internet for public proxy servers. These servers are then tested for speed and anonymity (not all of them are truly anonymous, even if they claim to be!) and once you find one which suits your requirements you can select it as your default proxy with the click of a button.

One of the most significant advantages of using an automated tool to locate proxy servers is that you do not have to keep editing your proxy settings manually each time you wish to try out a new one. Instead, what you do is enter 'localhost' or '127.0.0.1' into the 'address' box and '8088' into the 'port' box of your browser's proxy settings menu and then forget about it. All future proxy switching is then orchestrated from within your proxy seeking software, which subsequently relays the information to your browser or whatever type of application you are attempting to make anonymous. For those of you who are curious 'localhost' and the IP address '127.0.0.1' are the names by which every computer on the internet refers to itself.
Here's a good selection of links, which should help you to get started - Code:
hxxp://www.a4proxy.com/ Anonymity 4 Proxy
hxxp://www.helgasoft.com/hiproxy/ Hi Proxy
hxxp://www.proxy-verifier.com/ Proxy Verifier
hxxp://www.photono-software.de/ Stealther.

You may find that even when using these programs you have difficulty finding good proxy servers. It is for this reason that many people choose only to use proxy servers temporarily whilst doing something which may land them in trouble with their ISP, or in a worst case scenario with the law. The most obvious example of a situation in which you would want to cover your tracks is when scanning for public FTP servers and subsequently uploading to them. Most other net activities are unlikely to incur serious consequences so under these circumstances you can safely surf the web without a proxy. If you're really serious about protecting your privacy, however, your best bet is probably to invest in a dedicated, stable proxy such as the ones offered by Code:
hxxp://www.ultimate-anonymity.com/ Ultimate Anonymity

These aren't free, but may be worth the expense if you aren't keen on continuously switching proxy servers.

Before splashing out though it may be worth checking if your current ISP has a proxy server of its own which you can use. These aren't there to help you to commit cyber crimes and get away with it, they actually have a legitimate purpose as well - otherwise they wouldn't exist. You see, proxy servers were originally designed to help speed up web page loading times. Proxy servers contain a cache of all the web pages which have been requested via the browsers of the people using the proxy. When someone surfs the web using a proxy, the proxy first checks to see if it already has a copy of the web page stored in its cache. If this version of the page is bang up to date, it is sent to your computer and appears in your browser. If the page found in the cache of

the proxy server is older than the one stored on the server hosting the page, a new request to the web server is made and the page is updated in the cache of the proxy before being sent to you. Because these servers use very fast internet connections they can retrieve web pages at much greater speeds than you can via your modest home setup. If these servers are located physically nearer to your home than the web host servers you wish to retrieve web pages from, the speed at which you browse the web will be accelerated.

Anonymity - Cookies

One last important point you need to be aware of before jumping in with both feet is that different programs have to be setup in different ways before being able to make external connections via a proxy server. For example, you can surf the web anonymously by modifying the settings in Internet Explorer or Netscape Navigator as explained earlier in this tutorial, but this will only affect your browser. If you then used Flash FXP to copy a batch of 0-day releases from one FTP server to another, this isn't going to protect you in the slightest. What you have to do is enter the name of the proxy server into each application you wish to make anonymous before making any external connections. This can usually be done by browsing through the preferences of your program to see if there is a 'use proxy server' option available. If there is, make sure you use it!

Cookies:

You have little to fear from the edible variety, but the digital ones can be a major threat to your security and privacy. A cookie is a tiny text file (usually less than 1kb in size), which is created and stored on your hard drive whenever you visit a dynamic (or an interactive if you like) web site. These are used to log your personal details so that you can access members only areas of web sites without having to type in a password every time, or to retain your customised settings so that they are available the next time you visit. If you're using a shared computer, anyone who visits the same site that you have previously logged in to can access your accounts. This is particularly worrying if you have entered your credit card details into a form on an e-commerce site. If your browser is set to automatically fill in these details whenever you return to a previously visited site, this information could be clearly visible - you don't need me to explain the problems this could entail.

The solution to this problem is to delete any cookies which contain sensitive data once you have completed your transactions. Your cookies will be stored in a different place depending on which operating system you are using so you will have to use your detective skills to find them. As an example, in Windows XP they are located in your 'c:\Documents and Settings\Kylie Minogue\Cookies' directory (that is if your name is Kylie Minogue. Mine isn't in case you're wondering!). If you look in this directory, in some cases it is easy to identify which cookie is associated with which web site, but in other cases it's not so obvious. The cookie which was created when you visited Yahoo.com to check your email may be called kylie minogue@yahoo.txt for example. Unfortunately some cookies refer to the IP address of the site you visited and so look more like kylie minogue@145.147.25.21. These cookies can be selectively deleted one at a time if it's obvious which ones are causing a threat to your security, or you can just wipe out the whole lot in one fell swoop and have them recreated as and when they are required. However, if
you're really struggling to find your cookie jar, you could delete your cookies via your browser's tool bar instead. In Internet Explorer this can be done through the 'Tools' > 'Internet Options' menu items.

If all this sounds like too much hassle, you can always find a labour saving program which will be happy to take the job off your hands. These 'cookie crunching' programs allow you to be more selective when editing, viewing and deleting cookies from your system, and some of them will even prevent cookies from being created in the first place. Yes, I know you're hungry for links so I won't deprive you. Have a look here - Code:
hxxp://www.rbaworld.com/Programs/CookieCruncher/ Cookie
Cruncher
hxxp://www.thelimitsoft.com/ Cookie Crusher
hxxp://www.angove.com/ Cookie Killer
hxxp://www.kburra.com/ Cookie Pal
and

hxxp://www.cookiecentral.com/ Cookie Web Kit.