

Forum:[Hack Forums](#)

Thread: [\[TuT\] How to deface websites](#)[\[TuT\]](#)

ne0x25 - April 25, 2011, 5:21 am

Steps To Deface A Webpage

First of all, I do not deface, I never have (besides friends sites as jokes and all in good fun), and never will. So how do I know how to deface? I guess I just picked it up on the way, so I am no expert in this. If I get a thing or two wrong I apologize. It is pretty simple when you think that defacing is just replacing a file on a computer. Now, finding the exploit in the first place, that takes skill, that takes knowledge, that is what real hackers are made of. I don't encourage that you deface any sites, as this can be used get credit cards, get passwords, get source code, billing info, email databases, etc.. (it is only right to put up some kind of warning. now go have fun ;)

This tutorial will be broken down into 3 main sections, they are as followed:

1. Finding Vuln Hosts.
2. Getting In.
3. Covering Your Tracks

It really is easy, and I will show you how easy it is.

1. Finding Vuln Hosts

This section needs to be further broken down into two categories of script kiddies: ones who scan the net for a host that is vuln to a certain exploit and ones who search a certain site for any exploit. The ones you see on alldas are the first kind, they scan thousands of sites for a specific exploit. They do not care who they hack, anyone will do. They have no set target and not much of a purpose. In my opinion these people should either have a cause behind what they are doing, ie. "I make sure people keep up to date with security, I am a messenger" or "I am spreading a political message, I use defacements to get media attention". People who deface to get famous or to show off their skills need to grow up and realize there is a better way of going about this (not that I support the ones with other reasons either). Anyways, the two kinds and what you need to know about them:

Scanning Script Kiddie: You need to know what signs of the hole are, is it a service? A certain OS? A CGI file? How can you tell if they are vuln? What version(s) are vuln? You need to know how to search the net to find targets which are running whatever is vuln. Use altavista.com or google.com for web based exploits. Using a script to scan ip ranges for a certain port that runs the vuln service. Or using netcraft.com to find out what kind of server they are running and what extras it runs (frontpage, php, etc..) nmap and other port scanners allow quick scans of thousands of ips for open ports. This is a favorite technique of those guys you see with mass hacks on alldas.

Targetted Site Script Kiddie: More respectable than the script kiddies who hack any old site. The main step here is gathering as much information about a site as possible. Find out what OS they run at netcraft or by using: telnet [www.site.com](#) 80 then GET / HTTP/1.1 Find out what services they run by doing a port scan. Find out the specifics on the services by telnetting to them. Find any cgi script, or other files which could allow access to the server if exploited by checking /cgi /cgi-bin and browsing around the site (remember to index browse)

Wasn't so hard to get the info was it? It may take awhile, but go through the site slowly and get all the information you can.

2. Getting In

Now that we got the info on the site we can find the exploit(s) we can use to get access. If you were a scanning script kiddie you would know the exploit ahead of time. A couple of great places to look for exploits are Security Focus and packetstorm. Once you get the exploit check and make sure that the exploit is for the same version as the service, OS, script, etc.. Exploits mainly come in two languages, the most used are C and perl. Perl scripts will end in .pl or .cgi, while C will end in .c To compile a C file (on *nix systems) do gcc -o exploit12 file.c then: ./exploit12 For perl just do: chmod 700 file.pl (not really needed) then: perl file.pl. If it is not a script it might be a very simple exploit, or just a theory of a possible exploit. Just do a little research into how to use it. Another thing you need to check is whether the exploit is remote or local. If it is local you must have an account or physical access to the computer. If it is remote you can do it over a network (internet).

Covering Your Tracks

So by now you have gotten the info on the host in order to find an exploit that will allow you to get access. So why not do it? The problem with covering your tracks isn't that it is hard, rather that it is unpredictable. Just because you killed the sys logging doesn't mean that they don't have another logger or IDS running somewhere else. (even on another box). Since most script kiddies don't know the skill of the admin they are targeting they have no way of knowing if they have additional loggers or what. Instead the script kiddie makes it very hard (next to impossible) for the admin to track them down. Many use a stolen or second isp account to begin with, so even if they get tracked they won't get caught. If you don't have the luxury of this then you MUST use multiple wingates, shell accounts, or trojans to bounce off of. Linking them together will make it very hard for someone to track you down. Logs on the wingates and shells will most likely be erased after like 2-7 days. That is if logs are kept at all. It is hard enough to even get a hold of one admin in a week, let alone further tracking the script kiddie down to the next wingate or shell and then getting a hold of that admin all before the logs of any are erased. And it is rare for an admin to even notice an attack, even a smaller percent will actively pursue the attacker at all and will just secure their box and forget it ever happened. For the sake of argument let's just say if you use wingates and shells, don't do anything to piss the admin off too much (which will get them to call authorities or try to track you down) and you delete logs you will be safe. So how do you do it?

We will keep this very short and to the point, so we'll need to get a few wingates. Wingates by nature tend to change IPs or shutdown all the time, so you need an updated list or program to scan the net for them. You can get a list of wingates that is well updated at <http://www.cyberarmy.../lists/wingate/> and you can also get a program called winscan there. Now let's say we have 3 wingates:

```
212.96.195.33 port 23
202.134.244.215 port 1080
203.87.131.9 port 23
```

to use them we go to telnet and connect to them on port 23. we should get a response like this:

```
CSM Proxy Server >
```

to connect to the next wingate we just type in it's ip:port

```
CSM Proxy Server >202.134.244.215:1080
```

If you get an error it is most likely to be that the proxy you are trying to connect to isn't up, or that you need to login to the proxy. If all goes well you will get the 3 chained together and have a shell account you are able to connect to. Once you are in your shell account you can link shells together by:

```
[j00@server j00]$ ssh 212.23.53.74
```

You can get free shells to work with until you get some hacked shells, here is a list of free shell accounts. And please remember to sign up with false information and from a wingate if possible.

Alright, there are a few things on the server side that all script kiddies need to be aware of. Mostly these are logs that you must delete or edit. The real script kiddies might even use a rootkit to automatically delete the logs. Although lets assume you aren't that lame. There are two main logging daemons which I will cover, klogd which is the kernel logs, and syslogd which is the system logs. First step is to kill the daemons so they don't log anymore of your actions.

```
[root@hacked root]# ps -def | grep syslogd  
[root@hacked root]# kill -9 pid_of_syslogd
```

in the first line we are finding the pid of the syslogd, in the second we are killing the daemon. You can also use /etc/syslog.pid to find the pid of syslogd.

```
[root@hacked root]# ps -def | grep klogd  
[root@hacked root]# kill -9 pid_of_klogd
```

Same thing happening here with klogd as we did with syslogd.

now that killed the default loggers the script kiddie needs to delete themself from the logs. To find where syslogd puts it's logs check the /etc/syslog.conf file. Of course if you don't care if the admin knows you were there you can delete the logs completely. Lets say you are the lamest of the script kiddies, a defacer, the admin would know that the box has been comprimised since the website was defaced. So there is no point in appending the logs, they would just delete them. The reason we are appending them is so that the admin will not even know a break in has accurd. I'll go over the main reasons people break into a box:

To deface the website. - this is really lame, since it has no point and just damages the system.

To sniff for other network passwords. - there are programs which allow you to sniff other passwords sent from and to the box. If this box is on an ethernet network then you can even sniff packets (which contain passwords) that are destine to any box in that segment.

To mount a DDoS attack. - another lame reason, the admin has a high chance of noticing that you comprimised him once you start sending hundreds of MBs through his connection.

To mount another attack on a box. - this and sniffing is the most commonly used, not lame, reason for exploiting something. Since you now how a rootshell you can mount your attack from this box instead of those crappy freeshells. And you now have control over the logging of the shell.

To get sensitive info. - some corperate boxes have alot of valueable info on them. Credit card databases, source code for software, user/password lists, and other top secret info that a hacker may want to have.

To learn and have fun. - many people do it for the thrill of hacking, and the knowledge you gain. I don't see this as horrible a crime as defacing. as long as you don't destroy anything I don't think this is very bad. Infact some people will even help the admin patch the hole. Still illegal though, and best not to break into anyone's box.

I'll go over the basic log files: utmp, wtmp, lastlog, and .bash_history

These files are usually in /var/log/ but I have heard of them being in /etc/ /usr/bin/ and other places. Since it is different on alot of boxes it is best to just do a find / -iname 'utmp'|find / -iname 'wtmp'|find / -iname 'lastlog'. and also search threw the /usr/ /var/ and /etc/ directories for other logs. Now for the explanation of these 3.

utmp is the log file for who is on the system, I think you can see why this log should be appended. Because you do not want to let anyone know you are in the system. wtmp logs the logins and logouts as well as other info you want to keep away from the admin. Should be appended to show that you never logged in or out. and lastlog is a file which keeps records of all logins. Your shell's history is another file that keeps a log of all the commands you issued, you should look for it in your \$ HOME directory and edit it, .sh_history, .history, and .bash_history are the common names. you should only append these log files, not delete them. if you delete them it will be like holding a big sign infront of the admin saying "You've been hacked". Newbie script kiddies often deface and then rm -rf / to be safe. I would avoid this unless you are really freaking out. In this case I would suggest that you never try to exploit a box again. Another way to find log files is to run a script to check for open files (and then manually look at them to determine if they are logs) or do a find for files which have been edited, this command would be: find / -ctime 0 -print

A few popular scripts which can hide your presence from logs include: zap, clear and cloak. Zap will replace your presence in the logs with 0's, clear will clear the logs of your presence, and cloak will replace your presence with different information. acct-cleaner is the only heavily used script in deleting account logging from my experience. Most rootkits have a log cleaning script, and once you installed it logs are not kept of you anyways. If you are on NT the logs are at C:\winNT\system32\LogFiles\, just delete them, nt admins most likely don't check them or don't know what it means if they are deleted.

One final thing about covering your tracks, I won't go to into detail about this because it would require a tutorial all to itself. I am talking about rootkits. What are rootkits? They are a very widely used tool used to cover your tracks once you get into a box. They will make staying hidden painfree and very easy. What they do is replace the binaries like login, ps, and who to not show your presence, ever. They will allow you to login without a password, without being logged by wtmp or lastlog and without even being in the /etc/passwd file. They also make commands like ps not show your processes, so no one knows what programs you are running. They send out fake reports on netstat, ls, and w so that everything looks the way it normally would, except anything you do is missing. But there are some flaws in rootkits, for one some commands produce strange effects because the binary was not made correctly. They also leave fingerprints (ways to tell that the file is from a rootkit). Only smart/good admins check for rootkits, so this isn't the biggest threat, but it should be considered. Rootkits that come with a LKM (loadable kernel module) are usually the best as they can pretty much make you totally invisible to all others and most admins wouldn't be able to tell they were compromised.

In writting this tutorial I have mixed feelings. I do not want more script kiddies out their scanning hundreds of sites for the next exploit. And I don't want my name on any shouts. I rather would like to have people say "mmm, that defacing crap is pretty lame" especially when people with no lives scan for exploits everyday just to get their name on a site for a few minutes. I feel alot of people are learning everything but what they need to know inorder to break into boxes. Maybe this tutorial cut to the chase alittle and helps people with some knowledge see how simple it is and hopefully make them see that getting into a system is not all it's hyped up to be. It is not by any means a full guide, I did not cover alot of things. I hope admins found this tutorial helpful aswell, learning that no matter what site you run you should always keep on top of the latest exploits and patch them. Protect yourself with IDS and try finding holes on your own system (both with vuln scanners and by hand).

Regretz for tutorial go to b0iler

You can download here C99 & JackalShell here: [Download](#)

The Stig - April 25, 2011, 5:24 am

<http://2ethicalhackers.wetpaint.com/page/Defacing+a+webpage>

Hmm..

a7mdrock - April 25, 2011, 5:47 am

Nice Thread Bro, i will use this Soon and i will Make Screenshot :)

SamuelAustin - April 26, 2011, 9:09 am

You stole this tut. just changed a little words around and etc.

404NameNotFound - May 4, 2011, 5:17 am

Sick post, This is very useful!

b0o - May 4, 2011, 5:24 am

You jacked this tut i am disappoint.

-coded32 - May 4, 2011, 7:05 am

This is totally a ripped tut from HaxZo my friend !! We wrote this a long time back ! this tut has been flanged many times and now there are more efficient tuts out there !

!stric_tags(\$userName) - May 9, 2011, 7:00 pm

Useful, I will use it sometime. Thanks :D.

Also, Don't steal posts. (If you did).

IRC - May 9, 2011, 7:04 pm

I will try this later.

That is really sad if you stole this post.

GreenEnergy - May 9, 2011, 10:32 pm

dud this is leeched :P

fuck yea

djkayz - July 18, 2011, 2:25 pm

Nice tut.

But I think, he doesn't mean to stole thread,...but he wanted to share with us.

Btw, next time, make sure you wrote the bottom line>>> Source:

<http://2ethicalhackers.wetpaint.com/page/Defacing+a+webpage>

blahblah...

Tnx