Defacing Websites Part I : A Step By Step Process By Ankit Fadia ankit@bol.net.in

Date Released: 29th June 2001

In the past I have received a number of queries like: How do I deface websites? How do I replace someone else's web page with my own? Questions like these had become very common. After procrastinating this manual for some weeks, I finally have got down to bringing it out.

Before we move on with this manual, it is important to note that this manual explores only one method of defacing websites and the described process will not necessarily work on all target systems. Also note that we take an imaginary target system X for the below steps.

Identifying a Vulnerable host

A number of system administrators have a tendency to keep even those ports on their system open, which have no useful daemon running on them. One tip given to all system administrators is to close all those ports or disable all those daemons/services, which have no great use. However, many system administrators around the world are both too carefree and ignorant or lack the knowledge required to be able to get a list of running services and disabling the not useful ones. In effect they keep their system vulnerable to outside attacks by keeping even those ports open, which could have been done without.

The first step to be able to deface a website successfully is to identify a vulnerable host, against which you can carry out attacks. The defacing process described in this manual requires for the Port 21 or the FTP port of the target system to be open and allowing anonymous logins. In effect, you first step would be to port scan the target system X and find out whether or not the FTP port is open, and if the FTP port is open, then whether it allows for anonymous logins or not.

When I port scanned X, I find that Port 21 is open and it indeed has the FTP daemon running. I then use the FTP MS-DOS utility to ftp to port 21 of X.

```
C:\WINDOWS>ftp X
Connected to X
220 X FTP server (Digital UNIX Version 5.60) ready.
User (X:(none)):
```

FTP'ing to the port 21 of the target system brings up a prompt which asks for a Username. Now, let us try to login anonymously:

```
User (X:(none)): anonymous
331 Guest login ok, send ident as password.
```

The daemon did not get an error message, thus it does allow anonymous logins. Now, I just enter any fake email address as my password and login:

```
Password: fake_email@fake_domain.com
```

```
230 Guest login ok, access restrictions apply.
ftp>
```

Actually, one does not need to login anonymously for this method to work. Even if you have a normal account with the target system, using which you can login to the FTP daemon and if the system is vulnerable, then this method will still work. If your target system does not allow anonymous logins and if you do not even have an account with them, then another thing that you could try is: Trying to login using the default password of the FTP daemon running on the target system. (For more information regarding default passwords, read: http://hackingtruths.box.sk/defaultpasswd.htm) However, the fact remains that the method described in this manual works the best with servers, which have anonymous logins, enabled.

The Vulnerability Itself

In the above paragraphs, I have mentioned the term: ‘the method’, several times. So what exactly is this method and what vulnerability does it exploit?

Ideally, the FTP port should be disabled unless it is really of some use. If one does have to necessarily keep the FTP daemon running, then typically each user’s file access should be limited to a particular directory. For example, like my ISP gives an FTP account to each subscriber, with each subscriber having file access to the following directory:

```
/bin/users/username
```

However, sometimes both anonymous logins and normal logins give the user access to the entire directory structure. This means that each and every user can login to the Port 21 of the vulnerable system and browse through all directories and access all files on that particular system. In such cases, the attacker tries to lay his hands on the /etc/passwd file. But that is not we lay the stress on, in this manual.

On top of all this, many servers have world write-able directories, to which all users have access to, due to the above problem. The directories being world write-able, means that all users can login and upload any files of their choice onto the target system. Or in other words, anyone can write to the target system. Thus, you not only have access to all directories on the target system, but you can save and delete or even replace all files on that system, just as if it were your local hard disk.

****

HACKING TRUTH: How do I know whether my target system’s FTP port gives me access to world write-able directories? If you are able to upload any file to the target system, then it probably means that the directory into which logged in is at least write-able by you.

****

This vulnerability can be used by an attacker to access the directory where the pages of the website hosted by the target system are stored. Once the attacker knows which directory stores the web pages of the target system then he can easily edit their pages or even replace their entire site with his own, with the help of a simple command:

```
ftp> mput filename
```

Please note that if you FTP to a system and find that you are able to upload files, then it could also mean that your particular directory is write-able by you, while you do not have privileges to write to other directories. Such a scenario is quite common in the case of Webspace providers, in which each subscriber is given a particular space to store files or in other words each other member is given a write-able directory to which he can upload files. The gist being, having write privileges in one directory does not give you write privileges in all directories.

With this we come to the end of the first in the series of guides to Defacing websites. Thanks for reading and till the next update, take care. J

Ankit Fadia
Ankit@bol.net.in

http://hackingtruths.box.sk

Wanna ask a question? Got a comment to make? Criticize, Comment and more…..by sending me an Instant Message on MSN Messenger. The ID that I use is: ankit_fadia@hotmail.com

Wanna learn Hacking? Wanna attend monthly lectures and discussions on various Networking/Hacking topics? Lectures, Debates and Discussions, get it all by simply joining **The Hacking Truths club** by clicking Here

Take the **HTCH examination** to give recognition to your Hacking Skills. Click Here