

## Re: By passing surf control

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-02/0156.html>

---

**From:** thomas adams (tgadams\_at\_bellsouth.net)

**Date:** 02/26/04

Date: 26 Feb 2004 19:15:46 -0000

To: pen-test@securityfocus.com

('binary' encoding is not supported, stored as-is) In-Reply-To: <403D4886.6010203@gci.net>

Most of the techniques involving obfuscation no longer work (with newer versions of SurfControl). Key question here, is what version of SurfControl are you running? Is it possible the user is not even really bypassing SurfControl but more bypassing a firewall rule? I am aware SurfControl can monitor several ports, but what ports do you have it set to monitor? If you are just monitoring 80/443 then a user could very well setup a box outside the network to listen on say port 22. By 'bouncing' to this box he can very easily 'bypass' SurfControl. But, like I said that isn't really bypassing SurfControl as it is a firewall rule. Cant remember if this was mentioned or not, but the Web Report Server should also be disabled. It is vulnerable to several different attacks that could allow remote compromise. Doing this, the user could then add a rule to allow him anywhere/anytime. But, this all depends on your version.

>Received: (qmail 24785 invoked from network); 26 Feb 2004 14:45:52 -0000  
>Received: from outgoing3.securityfocus.com (205.206.231.27)  
> by mail.securityfocus.com with SMTP; 26 Feb 2004 14:45:52 -0000  
>Received: from lists.securityfocus.com (lists.securityfocus.com [205.206.231.19])  
> by outgoing3.securityfocus.com (Postfix) with QMQP  
> id 831D6A350D; Thu, 26 Feb 2004 07:55:30 -0700 (MST)  
>Mailing-List: contact pen-test-help@securityfocus.com; run by ezmlm  
>Precedence: bulk  
>List-Id: <pen-test.list-id.securityfocus.com>  
>List-Post: <mailto:pen-test@securityfocus.com>  
>List-Help: <mailto:pen-test-help@securityfocus.com>  
>List-Unsubscribe: <mailto:pen-test-unsubscribe@securityfocus.com>  
>List-Subscribe: <mailto:pen-test-subscribe@securityfocus.com>  
>Delivered-To: mailing list pen-test@securityfocus.com  
>Delivered-To: moderator for pen-test@securityfocus.com  
>Received: (qmail 9392 invoked from network); 25 Feb 2004 19:04:15 -0000  
>Date: Wed, 25 Feb 2004 16:14:47 -0900  
>From: Charles Hamby <fixer@gci.net>  
>Subject: Re: By passing surf control  
>In-reply-to:  
> <F208B303021DED40BEFB5F2AF6F75CA42E4845@usilchexch01.universalaccess.net>  
>To: "McNutt, Jacob" <JMcNutt@universalaccess.net>  
>Cc: Kudakwashe Chafa-Govha <KChafa-Govha@bankunitedfla.com>,  
> pen-test@securityfocus.com

## SecurityFocus Penetration: Re: By passing surf control

>Message-id: <403D4886.6010203@gci.net>  
>MIME-version: 1.0  
>Content-type: text/plain; charset=ISO-8859-1; format=flowed  
>Content-transfer-encoding: 7BIT  
>X-Accept-Language: en-us, en  
>User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5)  
> Gecko/20031007  
>References:  
> <F208B303021DED40BEFB5F2AF6F75CA42E4845@usilchexch01.universalaccess.net>  
>  
>Have you tried checking to see if IP address obfuscation works?  
>  
>In case anyone's not familiar with this...  
>  
>Using <http://www.amazon.com> as an example. If I wanted to go there but  
>it was blocked, I would find out what the IP address of [www.amazon.com](http://www.amazon.com)  
>is (say using ping).  
>  
>In this case it happens to be 207.171.181.16. I would then convert each  
>octet into hex individually. (207 is CF, 171 is AB, 181 is B5 and 16 is 10)  
>Then I would put CFABB510 into my calculator (Windows calculator works  
>just fine for this, by the way) and convert it to decimal again. I would  
>come up with 3484136720  
>I would open up my web browser and put in <http://3484136720> and up comes  
>Amazon.com.  
>  
>Charles Hamby  
>  
>McNutt, Jacob wrote:  
>  
>>SSH tunneling/port forwarding to a proxy might work if they have access to it. Also, we have a problem  
>>with AOL client browsers that can bypass Websense all together.  
>>  
>>-----Original Message-----  
>>From: Kudakwashe Chafa-Govha [mailto:KChafa-Govha@bankunitedfla.com]  
>>Sent: Wednesday, February 25, 2004 3:04 PM  
>>To: pen-test@securityfocus.com  
>>Subject: By passing surf control  
>>  
>>Hello Group,  
>>  
>>  
>>Does anyone have any information on how to by pass a web content filter? We use Surf Control to monitor  
>>and filter web content. However, I have one of my users who was able to by pass this. We tried using a proxy  
>>to by pass just for testing purposes but it did not work. I am still trying to figure out what other method he  
>>used to do so. If anyone has any information , it will be greatly appreciated.  
>>  
>>Thanks  
>>  
>>Kuda  
>>

Re: By passing surf control

SecurityFocus Penetration: Re: By passing surf control

>> \*\*\*\*\*  
>> *The contents of this email and any attachments are confidential.*  
>> *It is intended for the named recipient(s) only.*  
>> *If you have received this email in error please notify the system manager or the sender immediately.*  
*Unless you are the intended recipient or his/her representative you are not authorized to, and must not, read, copy, distribute, use or retain this message or any part of it.*  
>> \*\*\*\*\*  
>>  
>>  
>>-----  
>>-----  
>>  
>>  
>>  
>>  
>>-----  
>>-----  
>>  
>>  
>>  
>>  
>  
>  
>  
>-----  
>-----  
>  
>  
  
-----  
-----