

## Re: Scan virtual hosts

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-08/0337.html>

---

**From:** Pete Herzog ([lists\\_at\\_isecom.org](mailto:lists_at_isecom.org))

**Date:** 08/27/05

Date: Sat, 27 Aug 2005 18:41:38 +0200

To: pen-test@securityfocus.com

Hi,

To bruteforce all domains in the HOST field would mean having a list of all domains. Scraping together that list to completeness could be an interesting task.

I recommend first:

Is the website of the hosting provider listing it's hosted websites on their website? Did googling for that IP lead to anything? Do the Pointer and A records on DNS for that IP or a range of the IPs under the hosting provider's control provide you with fodder to bf the Host header (including using the IPs, 127.0.0.1, and 0.0.0.0 in the Host header)?

If the answer to any of these is no, then you might be up the creek. I have looked into this before and I couldn't figure out a \*good\* way except to actually get an account on that web server and view the /home (or similar) directory.

Sincerely,  
-pete.

matt wrote:

```
>
>> On 8/24/05, Geert VAN ACKER <geert.vanacker@pandora.be> wrote:
>>
>>
>>> Dear list,
>>>
>>> is it possible to enumerate all virtual hosts on a given IP address ? I
>>> prefer Linux soft.
>>>
>
> It is possible, you could brute force the Host: header, however I dont
> personally know any tool that currently does this I am afraid. It would
> be pretty trivial
> to implement though.
```

SecurityFocus Penetration: Re: Scan virtual hosts

- >
- > *Regards*
- >
- > *Matt*
- > *Learn Security Online, Inc.*
- >
- > *\* Security Games \* Simulators*
- > *\* Challenge Servers \* Courses*
- > *\* Hacking Competitions \* Hacklab Access*
- >
- > <http://www.learnsecurityonline.com>
- >
- >
- >