

Re: The legal / illegal line?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2007-03/msg00061.html>

- *From:* "Higinio Orsini" <orsinih@xxxxxxxx>
 - *Date:* Tue, 6 Mar 2007 15:42:55 -0300
-

Hi everybody,

Sometimes the companies are not really aware of the implication of a whole pen-test and the legal/illegal line is in confrontation with the real goals that the test itself needs to reach. For example if we agreed with a company to make a port scanning and a defacing of a Web Server, it may be possible to have a Webserver down for several hours, and this thing could be very severe for the company. Using this example as a guideline, don't you think that the legal/illegal line issue should be checked when the pre-project is being reviewed with the customer ? I think that a wrong scope definition could have legal implications, even if the written contract is being respected to the letter, because we are supposed to be the specialists and not the customer.

Then the legal issues are all solved and the contract/test could be conducted normally.

Best regards,
Higinio.

2007/3/5, Craig Wright <cwright@xxxxxxxxxxxxxx>:

Hi Chris,

I have no issue with you scanning with permission and if you can get them to do so – great (however I would try to get a written contract – CYA – if anything goes wrong, you are still liable for negligence if you have not explicitly disavowed the possibility of damage).

An issue is that the system admin is not generally the legal possessor of the site and an email from this person stating that you can go ahead does not necessarily make the action legal (although it may go to damages). At least with a contract from the firm, you are covered for misrepresentation in cases where the admin oversteps his/her authority.

Next, consideration can not follow the agreement. If you have not agreed a price in advance (or at least a method to determine one) that you can not ask for and expect payment.

If you are going about offering services at no cost, (I would be

Re: The legal / illegal line?

personally a little worried if I was the one being approached with this proposal) good for you. It is a large risk however, and you may find that you become liable for some web app that falls over during the scan leaving you liable to pay the firm.

Finally, there is the issue of risk. Risk is a function of vulnerability or an exploit condition being used by a threat to create an impact on the firm. The chances of finding a vulnerability with a real impact to the firm are best addressed by assessing the risk in a more formalised manner.

Pen tests can be used to support this process, but not supplant it. Doing the external test may help get this idea into the management of the firm, but it is more likely that the management will now be satisfied that they have addressed the issues and pay little concern to the areas of real concern to the firm. Thus the effect may oft be a real reduction of awareness.

Web page defacements (and other basic Internet focused attacks that are the aim of a scan) have a cost and can be embarrassing; however they are rarely the greatest cost that a firm will have to contend with. The greatest risks are to systems that have a real impact to the firm and need to be addressed with a view to assessing the business risk from a material perspective, a view that is difficult if not impossible to see from outside.

Is it really worth the risk to yourself when there is negligible gain in many cases to the firm? Would it not be better to apply your skills to a firm that truly seeks to address the issues? You may find some, but the chances are smaller than when approaching with business risk in mind.

Thanks,
Craig

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>]
On Behalf Of Chris Travers
Sent: Tuesday, 6 March 2007 6:50 AM
To: Craig Wright
Cc: Barry Fawthrop; pen-test@xxxxxxxxxxxxxxxxxxxxx
Subject: Re: The legal / illegal line?

Craig Wright wrote:

- > Do you have an explicit agreement with the third party?
- >
- > If the answer is No, than all access is prohibited.
- >

Agreed. But those who unintentionally hide their heads in the sand often will give you permission if asked. My approach is:

- 1) "I am concerned about..."

Re: The legal / illegal line?

2) When told that it is under control, I will usually challenge them. Get them a little defensive. "How sure are you? Is it really worth your risk?"

3) I will usually then ask via email "so if you are sure this isn't a problem, would it be OK with you if I take a look and check it out? I am pretty sure I can x, y, and z."

Then when I get the go-head, they can't say I didn't have permission. I asked and got it. I just don't go outside of doing what I said I would.

I used this technique once to show a web-based software developer that I could break into all servers with his software installed. He didn't believe me, so I goaded him into giving me permission. I didn't do anything outside the scope of the permission, but I did demo the problem to him and he did fix it as a result...

Best Wishes,
Chris Travers

- > There is no license (implied or otherwise) to pen test a site unless it
- > is explicitly granted. There are civil penalties at the least.
- >
- > You are more likely asking if the action is criminal in nature or not
- > and this will vary on the act and jurisdiction. Without express
- > permission for the owner/possessor of the property, it is illegal.
- > Criminal and Illegal are not the same thing. All criminal activity is
- > illegal, though some illegal actions are not criminal.

>
> Regards,
> Craig

>
> -----Original Message-----
> From: listbounce@xxxxxxxxxxxxxxxxxxxxx
> [mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]
> On Behalf Of Barry Fawthrop
> Sent: Friday, 2 March 2007 12:47 PM
> To: pen-test@xxxxxxxxxxxxxxxxxxxxx
> Subject: The legal / illegal line?

- >
> Hi All
>
> Curious to hear other views, where does the legal and illegal line stand
> in doing a pen test on a third party company?
> Does it start at the IP Address/Port Scanning Stage or after say once
> access is gained?? very vague I know
>

Re: The legal / illegal line?

- >
- > I'm also curious to hear from other external/3rd party pen-test
- > consultants, how they have managed to solve the problem
- > Where they approach a client who is convinced they have security, and
- > yet there is classic signs that they don't?
- > You know that if you did a simple pen-test you would have the evidence
- > to prove your point all would be mute
- >
- > But from my current point that would be illegal, even if no access was
- > gained. (maybe I'm wrong) ??
- >
- > Perhaps this is just a problem here where I am or perhaps it exists
- > elsewhere also?
- >
- > I look forward to your input
- >
- > Barry
- >
- >
- >

> This List Sponsored by: Cenzic

- >
- > Need to secure your web apps?
- > Cenzic Hailstorm finds vulnerabilities fast.
- > Click the link to buy it, try it or download Hailstorm for FREE.

- >
- >
- > http://www.cenzic.com/products_services/download_hailstorm.php?camp=7016
- > 00000008bOW

>

>

> Liability limited by a scheme approved under Professional Standards
Legislation in respect of matters arising within those States and
Territories of Australia where such legislation exists.

>

> **DISCLAIMER**

> The information contained in this email and any attachments is
confidential. If you are not the intended recipient, you must not use or
disclose the information. If you have received this email in error,
please inform us promptly by reply email or by telephoning +61 2 9286
5555. Please delete the email and destroy any printed copy.

>

> Any views expressed in this message are those of the individual
sender. You may not rely on this message as advice unless it has been
electronically signed by a Partner of BDO or it is subsequently
confirmed by letter or fax signed by a Partner of BDO.

>

> BDO accepts no liability for any damage caused by this email or its

Re: The legal / illegal line?

attachments due to viruses, interference, interception, corruption or unauthorised access.

>
>

> This List Sponsored by: Cenzic

>

> Need to secure your web apps?

> Cenzic Hailstorm finds vulnerabilities fast.

> Click the link to buy it, try it or download Hailstorm for FREE.

>
>

http://www.cenzic.com/products_services/download_hailstorm.php?camp=70160000008bOW

>

>
>
>
>

Liability limited by a scheme approved under Professional Standards Legislation in respect of matters arising within those States and Territories of Australia where such legislation exists.

DISCLAIMER

The information contained in this email and any attachments is confidential. If you are not the intended recipient, you must not use or disclose the information. If you have received this email in error, please inform us promptly by reply email or by telephoning +61 2 9286 5555. Please delete the email and destroy any printed copy.

Any views expressed in this message are those of the individual sender. You may not rely on this message as advice unless it has been electronically signed by a Partner of BDO or it is subsequently confirmed by letter or fax signed by a Partner of BDO.

BDO accepts no liability for any damage caused by this email or its attachments due to viruses, interference, interception, corruption or unauthorised access.

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

http://www.cenzic.com/products_services/download_hailstorm.php?camp=70160000008bOW

Re: The legal / illegal line?

--

Higinio Orsini – Arkenaton IT
Novedades tecnologicas en
<http://arkenaton.com.ar/blog>
orsinih@xxxxxxxxx

This List Sponsored by: Cenzic

Need to secure your web apps?
Cenzic Hailstorm finds vulnerabilities fast.
Click the link to buy it, try it or download Hailstorm for FREE.

http://www.cenzic.com/products_services/download_hailstorm.php?camp=70160000008bOW

Re: The legal / illegal line?