RE: Some technical errors

Source: http://www.derkeiler.com/Mailing−Lists/securityfocus/security−basics/2006−04/msg00137.html

- *From*: "Craig Wright" <cwright@xxxxxxxxxxxxx>
- *Date*: Thu, 6 Apr 2006 15:47:44 +1000

Hello,
Sorry I forgot to also add, you can scan your own servers anywhere any time. This is not an issue of rights violations anywhere. You can scan your own property as there is nothing to stop you. You own it, if you scan it, you have given implied permission to yourself. No issues in law.

The legal issues only occur when another person who you have not granted permission scans the server.

Regards
Craig

−−−−−Original Message−−−−−
From: Tomas Korcak [mailto:korczis@xxxxxxxxx]
Sent: 6 April 2006 3:13
To: Craig Wright; security−basics@xxxxxxxxxxxxxxxxx
Subject: Re: Some technical errors

Hi there,
viz. my notes in text.

On 4/6/06, Craig Wright <cwright@xxxxxxxxxxxxx> wrote:

> Hello Tomas,
> You have missed a few other posts by Ansgar. You have to look to some of the previous posts as well. It was stated.
>
> If the SMTP server is not running on port 25 TCP it is not a public system. You thus have no right to access it at all. There is not a standard way to access it and DNS will not give the port.
>
> In this case the connection without prior express authorisation is illegal and may even be criminal. Use of the SMTP server is access and

use of a private computer. So sending mail is not using a public server, but a private one. This is a criminal offence under the Cyber crime convention rules. This means that it is an offence in Europe, the US, Australia etc.

Are you sure about that? I am not sure about that, because I am origanally living in central europe (czech republic), i think i am little−bit−security−aware, i hava some friends with same subject of interrest and i never ever heard about that (maybe). I agree than there can be lot of companies (also one which i am working for) which puts this things (connecting to the service not running on well−known port number) "out−of−law" but i dont think that is so general how said because legislative is not same in all countries arround the world and that is general problem of our internet (laws).... Next one example: I have right to run any application on nonprivileged port, i had runned some server application on this non−privileged port, i have arrived at home and forgot the selected (non−privileged) port number which i have selected sooner (on remote system). What i may to do now? May i scan this system? Or is that illegal (criminal ofense) ?

Hope this useful,
korCZis

If the server was advertised as being public, that would be express permission to send mail using the site (as per it's terms). This is still not a right to scan the server and in fact this would not be required as you have been given the details.

In some organisations I have been involved with, we have run SMTP servers on separate ports. SMTP 25 receives map and than SMAP forwards

it (from port 26 in a particular case). Trying to access TCP 26 is a violation of the site policy to use of mail. The TCP 25 port is valid and public ally allowed, not any other port.

The case above used a gauntlet firewall, so this was restricted, but even if not it would not become a valid action.

Regards
Craig

−−−−−Original Message−−−−−
From: Tomas Korcak [mailto:korczis@xxxxxxxxx]
Sent: 6 April 2006 10:28
To: Craig Wright
Subject: Re: Some technical errors

Hi there,
excuse me for not−so−technical answer, but first of all I think Craig is not answering on "question". I dont have read the whole Ansgar's issue (maybe that's wrong) but I think Craig is putting words (which Ansgar never said) in Ansgar's mouths. Nobody said you MUST to scan ports. That is my non−technical response to your mail, but now follows little−bit−more−technical answer. I am continuing with using your example of sending email via some smtp server. Smtp server is *OBVIOUSLY* running at the port number 25. But there is lot of another

smtp servers *NOT RUNNING* at the port number 25. There is lot of reasons why is done. First one is you dont have enough privelegies to run some application listening on port lower that 1024. Second one is than you will to run more than only application with dedicated (well−know) port number (for example two [maybe different] smtp servers)... I think in this case *WOULD NOT* be scanning illegal.... (Just my opinion)

Hope this is useful,
korCZis

On 4/3/06, Craig Wright <cwright@xxxxxxxxxxxxx> wrote:

> Hello all,
> Ansgar wrote..."Wrong. The only technical differences between a portscanner and dig are:A portscan will report that a port is open/closed/filtered, whereas dig will retrieve data after the

connect.

> − A portscan may be run against a range of ports and/or a range of hosts (giving you an overview of the network), whereas dig will only

> connect to a single port on a single host."
>
> Last time I checked, a port scanner and dig did completely different

> tasks. So did an email client and a port scanner.
>
> Next, it has been proposed that an Internet user would need to port scan to send e−mail. A selection of a header is attached below as answer to the statement that this (a port scan) is needed. The header attached is one from a security focus message. The header

demonstrates

that the email is sent from a mail client. The mail client has connected without needing to complete a port scan. In fact we can see that the sender changed the sender email address in order to accomplish this (in the X−Authentication field) and the servers message ID <20060330023800.A1848@xxxxxxxxxxxxxxxx> is included in the header as demonstration that the message

Now being the user in question generally sends email using a mail client. That the user does not have to port scan the site to send mail

and that the act of sending mail is not aided in any manner from a port scan, how can port scanning a server to see if it runs SMTP be (to a reasonable man) considered valid.

It is clear that there is no need to scan the system to see what else it may or may not be running. Was it necessary to connect using

telnet

for example to TCP 25 on mail.securityfocus.com. It would seem not as the message was not created using a Telnet session and typing the

message directly to the server.

So it would seem that the truth is not that the user needs to port scan to use a service nor that this is a general or even reasonable

response.

Rather, the argument is that the person 'wants' to do this. That there

is a ego gratification that occurs when the scan a server. The rights of the system owner are secondary to the perceived rights of the person doing the deed.

Regards
Craig

Dr Craig S Wright DTh MNSA MMIT CISA CISM CISSP ISSMP ISSAP G7799 GCFA AFAIM
Manager − Computer Assurance Services BDO Chartered Accountants & Advisers Level 19, 2 Market Street, Sydney, NSW 2001
Telephone: +61 2 9286 5555
Fax: +61 2 9993 9705
Direct: +61 2 9286 5497
<Mailto:CWright@xxxxxxxxxxxxx>

Received: from outgoing.securityfocus.com

(outgoing.securityfocus.com

[205.206.231.27])by synit−web−01.synergyit.com.au (Postfix)
with ESMTP id
9F5564600F0for <cwright@xxxxxxxxxxxxx>; Fri, 31 Mar 2006
09:10:03 +1000
(EST)
Received: from outgoing.securityfocus.com by
outgoing.securityfocus.com

via smtpd (for mail.bdosyd.com.au [203.41.196.145])
with ESMTP; Thu,
30 Mar 2006 14:43:53 −0800
Received: from lists.securityfocus.com (lists.securityfocus.com
[205.206.231.19])by outgoing3.securityfocus.com (Postfix)
with

QMQPid
CDE6E237553; Thu, 30 Mar 2006 15:04:12 −0700 (MST)
Mailing−List: contact security−basics−help@xxxxxxxxxxxxxxxxx; run by

ezmlm
Precedence: bulk
List−Id: <security−basics.list−id.securityfocus.com>
List−Post: <mailto:security−basics@xxxxxxxxxxxxxxxxx>
List−Help: <mailto:security−basics−help@xxxxxxxxxxxxxxxxx>
List−Unsubscribe:
<mailto:security−basics−unsubscribe@xxxxxxxxxxxxxxxxx>
List−Subscribe: <mailto:security−basics−subscribe@xxxxxxxxxxxxxxxxx>
Delivered−To: mailing list security−basics@xxxxxxxxxxxxxxxxx
Delivered−To: moderator for security−basics@xxxxxxxxxxxxxxxxx
Received: (qmail 31448 invoked from network); 30 Mar 2006 19:06:52
−0000

X−Authentication−Warning: kpnet.de: planetcobalt set sender to
bugtraq@xxxxxxxxxxxxxxxx using −f
Date: Thu, 30 Mar 2006 20:35:16 +0200
From: Ansgar −59cobalt− Wiechers <bugtraq@xxxxxxxxxxxxxxxx>
To: security−basics@xxxxxxxxxxxxxxxx
Subject: Re: application for an employment
Message−ID: <20060330203516.A23474@xxxxxxxxxxxxxxxx>
Mail−Followup−To: security−basics@xxxxxxxxxxxxxxxx
References: <20060330023800.A1848@xxxxxxxxxxxxxxxx>
<200603301749.JAA23418@xxxxxxxxxxxxxxxxx>
Mime−Version: 1.0
Content−Type: text/plain;
charset=us−ascii
Content−Disposition: inline
User−Agent: Mutt/1.2.5i
In−Reply−To: <200603301749.JAA23418@xxxxxxxxxxxxxxxxx>; from
gillettdavid@xxxxxxxx on Thu, Mar 30, 2006 at 09:52:06AM
−0800
X−imss−version: 2.5
X−imss−result: Passed
X−imss−scores: Clean:99.90000 C:2 M:19 S:5 R:5
X−imss−settings: Baseline:6 C:4 M:4 S:4 R:4 (1.0000 4.0000)
Return−Path:
security−basics−return−38957−cwright=bdosyd.com.au@xxxxxxxxxxxxxxxx
X−OriginalArrivalTime: 30 Mar 2006 23:09:58.0402 (UTC)
FILETIME=[10957E20:01C6544F]

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.

−−−

<notice>
Your Skills In Reading Have Improved +1 </notice>

<idea>
Some days you're the dog; some days you're the hydrant.
</idea>

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.

−−
<warning>
This e−mail is intended for the named recipient(s). It may contain
privileged and/or confidential information. If you are not one of the
intended recipients, please notify the sender immediately and destroy
this e−mail and attachment(s): you must not copy, distribute, retain or
take any action in reliance upon the email or attachment(s). While all
reasonable efforts are made to safeguard inbound and outbound e−mails,
Tomas Korcak cannot guarantee that attachments are virus−free or are
compatible with your systems, and does not accept liability in respect
of viruses or computer problems experienced. Thank you.
</warning>

<notice>
Your Skills In Reading Have Improved +1
</notice>

<idea>
Some days you're the dog; some days you're the hydrant.
</idea>

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.

−−−