

Re: pen test

Re: pen test

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-12/msg00149.html>

- *From:* Ken.Carty@xxxxxxxxxxxxxx
 - *Date:* Wed, 12 Dec 2007 11:26:19 -0600
-

Well said!

Ken

"Michael R.
Martinez"
<mike@security-bo To
unce.com> "Worrell, Brian"
Sent by: <BWorrell@xxxxxxxxxxxx>, "Marty
listbounce@securi Resnick" <marty@xxxxxxxxxxxx>,
tyfocus.com listbounce@xxxxxxxxxxxx,
"security-basics"
<security-basics@xxxxxxxxxxxx>
12/12/2007 08:12 cc
AM
Subject
Re: pen test
Please respond to
mike@security-bou
nce.com

Brian,

This whole question has evolved into something completely different, you asked a question here on the list, we tried to give you some pointers and

Re: pen test

Re: pen test

now some bizar reference to and nist doc and "the feds" have changed things in recent years.

When you make a reference to the NIST or "The Feds" please provide validation to your statements so we can further refernce your resources. If you are going to send me a document 178 pages long refernce the page to support your argument.

You are not providing any REAL question anymore. Your question was could you pen test your host, I could have said ask them, but instead provided many options and answers and now you try to evolve the original question into something completely different. Are you inadvertantly trying to seem robust to this list? To further that statement are you trying to use this list as a form of marketing for your partially completed site? Do you plan on "pen-testing" the websites that you install and configure? That's wrong already?

You then flip this whole thread around by providing advice to me, which furthers by point of you marketing yourself, when the initial question was posed by you. I am well aware of many things and your simple question was answered, you now throw risk assessment into the mix, tattered with nist documentation that is for IT infrastructure and has a nothing to do with your question, "can I pen-test my hosting provider". Does NIST have a document for pen-testing your hosting provider, if so read it it will probably answer your questions, if not take the lists advice and move on smartly.

And last but not least, your hosting provider is in Geismar, Louisiana and not the UK, so when you leave a link make sure it is a reference to the United States, laws are different.

I apologize if this sounds abrasive, but your question seems loaded. Here is the number to your hosting provider call them and ask them, or asl theplanet.com (second number) since they own the servers.

1-800-828-9231
1-866-325-0045

Michael R. Martinez
TF: 800-987-7307

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

From: "Worrell, Brian" <BWorrell@xxxxxxxxxxxx>

Date: Wed, 12 Dec 2007 07:45:49

To: <mike@xxxxxxxxxxxxxxxxxxxx>, "Marty Resnick"

<marty@xxxxxxxxxxxxxxxx>, <listbounce@xxxxxxxxxxxxxxxx>, "security-basics"

<security-basics@xxxxxxxxxxxxxxxx>

Subject: RE: pen test

Re: pen test

Re: pen test

Mike,

The Feds have changed things in recent years, in such that Pen testing on your own gear / apps is a suggesting thing. Go look at the Nist 800-100 document. Below is a copy of what they say you SHOULD do as part of a Vulnerability Identification step of a Risk Management plan.

System security testing, using methods such as automated vulnerability scanning tools; security, test, and evaluation (ST&E); and penetration testing can be used to augment the vulnerability source reviews and identify vulnerabilities that may not have been previously identified in other sources.

NIST 800-30 goes on to say **The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], sendmail relaying).**

I recall seeing a demo of a pen testing tool that did not exploit them, but did run checks to see if you were open to them.

All I am saying is that if you are suppose to do a Risk Assessment due to HIPAA or even the PCI-DSS, it has to be more than a port scan, you have to assess the patch level, known coding issues, etc, or you are not meeting the regs / laws. Still, I would work with your web host, and get a project plan together, and document and see. Who knows, maybe you just need to VM the box and pen test if off the VM not the live.

Thanks
Brian

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

From: Michael R. Martinez [<mailto:mike@xxxxxxxxxxxxxxxxxxxxxx>]
Sent: Tuesday, December 11, 2007 12:05 PM
To: Worrell, Brian; Marty Resnick; listbounce@xxxxxxxxxxxxxxxxxxxxxx;
security-basics
Subject: Re: pen test

Brian,

A vulnerability assessment is completely different as well. Yes, you can assess the vulnerability from a technological standpoint of your host. For example, an open port, let's say, port 80 is open on your host. What you are looking for is a vulnerability, port 80 "can" be vulnerability. My "want" to attack that port can, and the vulnerabilities associated with port 80, create the exploit. Basically, a vulnerability assessment is a test to see what ports are open and if any are open are they vulnerable to the attack. After which you begin to label the likelihood, high, med, low or scale it 1-10.

Re: pen test

Re: pen test

You are not wrong about the laws, such as PCI compliance that want you to test process, procedures and technology, but PCI is more than just testing ports, its identify process associated with how you handle personal identifiable information, privacy practices, physical access to servers, procedures, etc. Port scanning for vulnerabilities is a component of the overall compliance test.

You cannot ask your host to subvert there security measures but they will certainly deny you, you can however, ask that you run security scans because there are services for this such as comodo and scan alert.

I am well aware of the security certs out there and the C|EH as I am a certified ethical hacker among several other security certs, I just don't add them on because 1) there are guys with no certs that are just as good and 2) they mean I passed a test. From my answers I hope you can judge me and not my certs.

Having said that, I hope I clarified some of this for you and if not feel free to respond back.

Cheers!

Mike

Michael R. Martinez
TF: 800-987-7307

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

From: "Worrell, Brian" <BWorrell@xxxxxxxxxxxx>

Date: Tue, 11 Dec 2007 07:13:41

To: <mike@xxxxxxxxxxxxxxxxxxxx>, "Marty Resnick"

<marty@xxxxxxxxxxxxxxxx>, <listbounce@xxxxxxxxxxxxxxxx>, "security-basics"

<security-basics@xxxxxxxxxxxxxxxx>

Subject: RE: pen test

Michael,

Am I wrong, but there are lots of practices and in some cases laws that say that you need to run vulnerability assessments to be compliant. If you were to ask you web host in writing before doing it, that should solve the possible "legality" issue that it sounds like you talking about.

As far as I know, White Hat hacking has never been illegal, if done correctly and above board. If it was, why would SANS and other offer Certified Hacker classes and certs?

Re: pen test

Re: pen test

Thanks
Brian

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

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]
On Behalf Of Michael R. Martinez
Sent: Monday, December 10, 2007 7:54 PM
To: Marty Resnick; listbounce@xxxxxxxxxxxxxxxxxxxxx; security-basics
Subject: Re: pen test

Marty,

absolutely not, this is called hacking. Pen testing is actively exploiting a server, identifying a weakness exploiting gaining access. Are you talking about scanning ports? Could you provide a little more detail. If you mean pen-testing, then the answer is no.

Cheers

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

From: Marty Resnick
Sender: listbounce@xxxxxxxxxxxxxxxxxxxxx
To: security-basics
Sent: Dec 10, 2007 9:35 AM
Subject: pen test

Am I able to pen test or run a vulnerability assessment on my web hosting company. I got the idea after reading this article.
http://www.securitypark.co.uk/Security_article.asp?articleid=260173

--

Marty Resnick
Techmaking Inc.
(877) 291-1110 (office)
(661) 209-2089 (mobile)
(805) 512-9603 (fax)
marty@xxxxxxxxxxxxxxxxxxxxx

Michael R. Martinez
TF: 800-987-7307

Re: pen test