

Re: Limited vs full blown testing

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-06/0149.html>

From: Richard Rager (*kb8rln_at_penguinmaster.com*)

Date: 06/24/04

Date: Thu, 24 Jun 2004 04:14:03 -0600 (MDT)

To: Toby Barrick <TBLinux@covad.net>

> *What has been the experience of the members on this list?*

I have done very small reports just using only nmap and some banner advertisements checking, billing for 4 hours of time. I have a default report the fits most companies at this level of care. Just enough to get them talking.

> *Do you just gleefully accept the check and any limitations imposed on testing –*

Simple: If someone is give you money they are the customer. Do what they ask or you will not get money from them. Something is better then nothing, remember it your job to help secure them to the best you can with the scope limit. This could come down too they did not have the money to spend at this time. Your report will end up at the board meeting and will be talk about. If there is too much unknown risk to the company they will call you back and add you as a budget item.

> *or do you push for a "complete" suite of tests?*

No, after you get money from them getting more money is easier. Think about it as a working interview. You get paid to show off. When doing the report you can say. One of my tools found your system could have this problem but because of the limited scope we did not test futher. If you would like we can futher investigate this possiable problem more in a later engagement.

On last thing on this subject. Pen-testing need to be policies overview as well as technique overview. When you get more time with the client you need to understand their needs with their network. One organization I will talk about here needed to be HIPPA compliance, they had alot of security problems. I lost future work by tell the client about a security problems with a PDAs they where using as the CFO held up a PDA and ask what the security problems are with it. The feedback I got was that I scared the hell out of them. Because of what I said about the PDA they kill a pet project of the IT manager. He said I put them back 5 years when it came to email. Even what I said was correct about the PDAs and

SecurityFocus Penetration: Re: Limited vs full blown testing

their security problems. I guess I need to understand the politics more and the talk about the truth less. Sound like congress.

Well have fun in this field.

Enjoy,

Richard Rager
<http://penguinman.com>