

# RE: Respuesta: Penetration Testing Methodologies

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-12/0155.html>

---

**From:** rزالuski (rزالuski\_at\_ivolution.ca)

**Date:** 12/15/04

To: "'Omar Herrera'" <oherrera@prodigy.net.mx>, "'Adriel T. Desautels'" <atd@secnetops.com>  
Date: Tue, 14 Dec 2004 22:29:18 -0500

A Penetration Test entirely depends on the scope and depth of the operation and what has been agreed upon. Sometimes finding a vulnerable system is enough. It all depends on the level of intrusion of the Penetration Test.

My point is if you are Pen Testing a client's mission critical production systems do you really want to bring it / them down? It is entirely possible to do so costing a company potentially large amounts of money in the process. This is especially if the testing is taking place with anything that processes monetary transactions.

Richard Zaluski,  
CISO, Security and Infrastructure Services  
iVolution Technologies Incorporated

905.309.1911  
866.601.4678  
905.524.8450 (Pager)  
www.ivolution.ca  
rزالuski@ivolution.ca

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

From: Omar Herrera [mailto:oherrera@prodigy.net.mx]  
Sent: Tuesday, December 14, 2004 4:56 PM  
To: Adriel T. Desautels  
Cc: pen-test@securityfocus.com  
Subject: Respuesta: Penetration Testing Methodologies  
Importance: Low

----- Mensaje original -----

De: "Adriel T. Desautels" <atd@secnetops.com>

>

> *Greetings List,*

> *I am interested in collecting ideas as to what people feel an ideal*

> *penetration test is. What does the ideal methodology look like and*

> *what are the goals? I am asking you this because I have been running*

> *into interesting issues in certain markets. It would appear that some*

> *people view penetration tests as nothing more than basic network*

## SecurityFocus Penetration: RE: Respuesta: Penetration Testing Methodologies

- > *vulnerability audits while others view a penetration test for what it*
- > *is, a test designed to compromise target systems as PoC of*
- > *vulnerability.*

In my opinion, PenTests must include tests designed to compromise target systems manually. The added value of a PenTest is to have someone able to find (and exploit) vulnerabilities in custom applications (something beyond that of which most tools can do).

- >
- > *How do people feel about the use of automated tools and the weights*
- > *of their results? What about manual or custom testing? We have our*
- > *own methodology that we use for testing our client networks, but I am*
- > *always interested in learning what else might be done. I'd be happy*
- > *to engage anyone in a conversation about this subject.*
- >

Most consultants use automated tools to give you a standardized set of results that can be reproduced (with the same tools), but custom testing is important. I believe that any average PenTest consultant should be capable of determining common false positives and incorrect results with manual testing, such as IIS running on a Unix server or vulnerabilities for Apache web server for an IIS web server.

Tools make many mistakes, and the least you would expect is that the guy running the software knows what he is doing (and actually shows it).

Regards,  
Omar Herrera