

## Re: Security Audit

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0083.html>

---

**From:** H Carvey ([keydet89@yahoo.com](mailto:keydet89@yahoo.com))

**Date:** 09/11/01

Date: 11 Sep 2001 03:12:09 -0000  
Message-ID: <20010911031209.15682.gmail@securityfocus.com>  
From: H Carvey <[keydet89@yahoo.com](mailto:keydet89@yahoo.com)>  
To: [pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)  
Subject: Re: Security Audit

- > *A zero knowledge pen test*
- > *should be the starting point of an audit,*

I couldn't disagree more. A pen test is not an audit. An audit, by its very nature, assumes that the information infrastructure is being compared to some standard. Ideally, this standard will be supplied by the available corporate information security policies. Absent these (as is the case many times), some other more arbitrary standard must be used. This alternate standard should be based on the consultant's understanding of the business needs of the client.

The entire information infrastructure should be examined in this audit (what I referred to in an earlier post as a vulnerability assessment). This includes informal and undocumented procedures and processes, as well as actual host settings and configurations.

A pen test, by its very nature, only focuses on a relatively small portion of the infrastructure, that being the public interface of the organization. So much more information can be learned by examining as much of the infrastructure as possible (including interviews of key personnel, etc). This data is then analyzed in the context of the client's business, and then the final deliverable presents that analysis in a manner that is useful and pertinent to the client.

## SecurityFocus Penetration: Re: Security Audit

The only real usefulness of a pen test is to test the reactions of the incident response team. If a router ACL or host configuration setting is applied and verified, you don't then need someone to try and break in from the outside just to verify it again.

Further benefits of a vulnerability assessment include the knowledge transfer that goes on between the consultant and the client. The consultant does no one any good if he disappears into a room and produces a magical report in a vacuum. Consultants must work closely with sysadmins at the client site...after all, after the consultants are gone, the sysadmins are left with whatever's there, whether they understand it or not. Besides, working closely with the admins builds trust and adds credibility...which leads to a relationship and follow-on work.

> *Regarding studies like CSI/FBI survey,*

For the sake of the readers and the moderators alike, I will refrain from my usual diatribe regarding quoting such things as this survey...and particularly this survey.

> *more or less, the 1st test will cover*  
> *about 20–30% of the potential attackers while*  
> *the 2nd will cover the others*  
> *70–80%.*

I would argue that a well-planned vulnerability assessment, if delivered properly, and if the necessary changes are made, will result in protecting the client from 90% or more of both internal and external threats.

I say this b/c the reports I have delivered stress the need for policies, and for recognizing that security is a process, that must be continually maintained.

> *The 1st test should be much longer in time and*  
> *resources, and usually the*  
> *clients here don't understand quiet well where*  
> *their money goes.*

So why should they pay it?

## SecurityFocus Penetration: Re: Security Audit

- > *So most of*
- > *the times clients prefer to contract the 2nd*  
test only, because it takes
- > *less time and money. Also, that's why after that*  
their systems are still
- > *vulnerable.*

That doesn't make any sense. Even if the second test is contracted only, the final deliverable should be clear enough such that if the documented issues are addressed, the client won't be *\_as vulnerable\_* as they were.

- > *It is important for the client that a little*  
education is provided,

Again, I disagree. It is important for a client that *\_a lot\_* of education is provided. This means not only up front during the sales process, but also during the assessment, and afterward, when the deliverable is presented, as well.

- > *And also,*
- > *why pen tests should be regular, each month or 2*  
or 6 or whatever ...

I agree with regular testing...but is it really necessary? See below...

- > *An*
- > *audit will only cover a specific period of time,*  
so it is not anyway and not
- > *anyhow a guarantee that in the (short) future*  
problems will not happen.

Of course not. That goes without saying for the security professionals, and should be clearly communicated to the client. However, if the consulting firm does its job and adequately communicates the concept that security is an ongoing process ("Mr. Client, you need to install these patches, and in the future you may also need to install others...as they come out."), then it's in the clients hands. At that point, if they choose not to follow the advice...so be it.

- > *At the technical side and at the commercial side*  
for both parts (consultant
- > *and client), the more audits in a period of time*  
are made, the better the
- > *investment and the results.*

Re: Security Audit

That's not necessary. The disruption to a client's infrastructure is unacceptable. The appropriate way to conduct these things is to conduct a comprehensive vulnerability assessment...planned so as not to engage any one portion of the infrastructure for too long...and provide the recommendations in the deliverable. The client can then map out a timeframe for completing what he feels are the necessary steps, as communicated by the consulting firm. This could be 6 months, or a year. Re-examining the infrastructure after a specified period is advisable.

Remember, it's the client that drives the boat, not the consulting firm. The client pays, therefore the golden rule applies.

- > *Some security consulting companies will not give away clients references,*
- > *because keeping confidential other companies with past or present security*
- > *problem is part of the contract with a client.*

Security companies that provide references (and many do) do so only after their clients approve. Simply b/c a security consulting company does an audit doesn't mean that the client had a "security problem" at all. In fact, many companies use comprehensive audits/assessments performed by big named firms to show due diligence.

Basically, the way it works is this...security company "A" asks client "B" if they can use the client as a reference. Client "B" says yes, with stipulations that the exact nature of the work not be described ("we did a security assessment for client B"). Then potential client "C" calls client "B", and client "B" says, "yes, these guys do good work." Simple, yes, but that's basically it.

If someone had a "security problem" (i.e., an "incident")...no, of course they wouldn't want it publicly known. But the security firm that did the work wouldn't ask, either.

- > *Other problem can be also giving away*
- > *models and methods, because there are many smartasses that are just looking*
- > *after knowledge to do the job themselves.*

## SecurityFocus Penetration: Re: Security Audit

By "smartasses", I guess you mean "potential clients". Yes, these folks are out there...I've seen them, as I'm sure others have. Yet there is nothing to prevent either party from requiring NDAs before going forward.

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

- ***Previous message:*** [Sameer Saxena: "Re: How to Tackle the Legal Tangle?"](#)
- ***Maybe in reply to:*** [H Carvey: "Re: Security Audit"](#)
- ***Next in thread:*** [R. DuFresne: "Re: Security Audit"](#)
- ***Reply:*** [R. DuFresne: "Re: Security Audit"](#)
- ***Reply:*** [Phil Cracknell: "Re: Security Audit"](#)
- ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)