

## Re: Pen-Test startup help

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-08/0133.html>

---

**From:** hellNbak ([hellnbak\\_at\\_nmrc.org](mailto:hellnbak_at_nmrc.org))

**Date:** 08/24/03

Date: Sun, 24 Aug 2003 14:42:53 -0500 (CDT)

To: Gerald Cody Bunch <[gbunch@gmx.net](mailto:gbunch@gmx.net)>

I think most experienced organizations have their own boiler plate report formats that they use. From a technical perspective here is what I do.

- 1.) Take screenshots of everything -- you can always delete the meaningless ones later
- 2.) Run a keystroke logger -- great for jogging your memory when you put in long sessions and forget things
- 3.) Keep vi, pico, notepad, whatever running in a window to make constant notes -- these aren't for the client but more for you to jot down things that might be important later or needed in the report.

The format of the report needs to reflect what the client wanted to get out of the Pen-Test. There is zero value in providing a 1000 pager full of stuff you know the client won't read. In general here is what you should have;

Abstract (explaining the work and why the client wants the work, their pains etc..)

Executive Summary (basically an overview of what was found focusing on what it means to the business. The person reading the exec summary won't care about the technical details but only the business impact and the high risk items.

Risk Analysis -- Detailed (more technical details on your findings along with remediation advise.

Various appendices -- (all your relevant screenshots and keystroke logs, nmap output ect...

Sometimes, companies will put in a "Next Steps" section which is usually just an attempt to sell more work but sometimes helpful.

On Sat, 23 Aug 2003, Gerald Cody Bunch wrote:

SecurityFocus Penetration: Re: Pen-Test startup help

> *Date: Sat, 23 Aug 2003 15:57:23 -0400*  
> *From: Gerald Cody Bunch <gbunch@gmx.net>*  
> *To: pen-test@securityfocus.com*  
> *Subject: Pen-Test startup help*  
>  
> *This may or may not be 100% on topic, but I believe that it would fit in*  
> *good. From what I have read pen-tests are supposedly well documented*  
> *from the start (or should be) and some form of report generated at the*  
> *end. My question is, what templates/procedures do the members of this*  
> *list use? Are there any standards for documentation, and/or publicly*  
> *available templates/procedures?*  
>  
> *Thanks,*  
>  
> *Gerald Cody Bunch*  
> *gbunch@gmx.net*  
>  
>  
>

---

> *Attend Black Hat Briefings & Training Federal, September 29-30 (Training), October 1-2 (Briefings) in*  
> *Tysons Corner, VA; the world's premier*  
> *technical IT security event. Modeled after the famous Black Hat event in*  
> *Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors.*  
> *Symantec is the Diamond sponsor. Early-bird registration ends September 6 Visit: [www.blackhat.com](http://www.blackhat.com)*  
>

>

--

-----  
The people you are after  
are the people you depend on.  
We develop your apps,  
we back up your data,  
we route your packets,  
we defend you while you sleep.  
DO NOT FUCK WITH US.  
nmrc.org  
-----

---

Attend Black Hat Briefings & Training Federal, September 29-30 (Training), October 1-2 (Briefings)  
technical IT security event. Modeled after the famous Black Hat event in  
Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors.  
Symantec is the Diamond sponsor. Early-bird registration ends September 6 Visit: [www.blackhat.com](http://www.blackhat.com)

---