

## Book Review: BackTrack 4: Assuring Security by Penetration Testing

by Jason Haddix

Don't have the cash for a \$2000 - 3000 penetration testing course? Don't know which tools are outdated or relevant? Lost in the sea of Backtrack options? You learn better on your own anyway?

No problem!

BackTrack 4: Assuring Security by Penetration Testing (BASPT), authored by Shakeel Ali and Tedi Heriyanto, is a 12-chapter compendium on everyone's favorite hacking distribution, Backtrack 4. Filling the need for a refresher to older titles on abandoned projects like Knoppix or Auditor (see somewhat outdated: Penetration Tester's Open Source Toolkit, Vol. 2), BASPT gives syntax and usage tips on a plethora of different tools included in the suite and is broken down into the generic pentesting methodology with which most people today are familiar. Not only that, but also the book itself reads like some of those intro to penetration testing classes we have all been to costing many more times the cost of a single book.

Intrigued? Let's take a closer look.

[del.icio.us](http://del.icio.us)

[Discuss in Forums {mos\\_smf\\_discuss:Book Reviews}](#)

BASPT is broken into three parts, each containing appropriate chapters to the given subject matter. Part I: Lab Preparation and Testing Procedures contains the first two chapters.

## Chapter 1: Beginning with BackTrack

Chapter 1 of BASPT is a fast track to setting up the distro in its various forms, getting network connectivity up and running, and updating/installing auxiliary tools. Nothing novel here, but it is helpful to a novice user. However, the book was lacking when it came to setting up secondary useful pentesting services like apache, telnet/ftp, ssh, etc. While some curriculums consider these services pre-requisite \*nix knowledge, BASPT came across at an instructional level that should have included them and their usefulness but didn't.

## Chapter 2: Penetration Testing Methodology

Chapter 2 of BASPT was a primer on assessment types and methodologies. While generally informative and educational, it missed the mark on a few descriptions and definitions. While I have no doubt that the authors referenced industry standard methodologies like OSSTMM and ISSAF, sometimes these are just too abstract or plain outdated for someone doing real pentesting nowadays. For example, their classifications of Blackbox = external and Whitebox = internal testing are erroneous.

The final section of Chapter 2 brought it all together with the "Backtrack" testing process which is very similar to what you'll see in the real world:

Image from p52 of the Book

These chapters could have used some descriptions for the differentiators between Netpen vs Webpen, internal vs external tests, but, all in all, it had a very good synopsis of industry standards. It also introduced a beginning tester to all the references needed to start general pentesting.

Part II of BASPT is the Penetration Testers Armory covering the bulk of the contents of the book. For brevity's sake, we'll only cover chapters three and four.

## Chapter 3: Target Scoping

Along with permission from the owner of the network being attacked, scoping and project management (and eventually documentation and reporting) is what separates criminals from security professionals. Although titled Target Scoping, this section covers scoping as well as PM. It was actually very well written and adequately describes what is needed therein.

## Chapter 4: Information Gathering

While I'm a huge proponent of Open Source Intelligence (OSINT) and was happy to see it represented right away, it is also a good illustration of where there's kind of a mixed bag inside BASPT. BASPT is a Backtrack 4 book that also tries to be an all-inclusive pentesting book. While going over document gathering you get a glimpse of Metagoofil, but anyone doing OSINT as part of their assessment regime knows that, barring its Windows nature, Fingerprinting Organizations with Collected Archives (FOCA) is a superior (and more often stable) metadata extraction tool.

Chapter 4 is also where the reader runs into "man page hell," where the book reads more like a series of categorized man pages with minor syntax variances, and less like an in-depth explanation of what and why you are doing what you are doing. In addition, there is quite a bit of tool overlap. One such example is why would a pentester ever need so many DNS tools (6) is mystery to me, as fierce usually does everything I need. Then again, that's the Backtrack way, "Give em everything, let em use what they want."

Part II: Penetration Testers Armory continues with the following chapters:

- Target Discovery
- Enumerating Target
- Vulnerability Mapping
- Social Engineering
- Target Exploitation
- Privilege Escalation
- Maintaining Access
- Documentation and Reporting

While I could go over every chapter, the comments from the previous paragraph echo on. Each chapter goes through the Backtrack menu providing a simple man-page-style usage and output for tools in each section. Some sections had much less structure and tool context, such as "Vulnerability Mapping," but other sections that have a much more rigid and defined role were rock solid. Not all areas were so dry, as there were numerous drills contained in certain areas of Part II (which included some post exploitation stuff with Metasploit... Bravo!). Of those that had drills, I thought they were great.

Finally we come to Part III: Extra Ammunition that includes two appendices for Supplementary Tools and Key Resources. The auxiliary tool section contained a few extra installs including a good netcat walkthrough, while the resources included were sparse but useful. These additions will be very welcome to a beginning pentester.

## The Skinny

While sometimes disorganized and trying to tackle a bit too much, BASPT is a great pentest reference book for beginners. Although BackTrack 5 was recently released, this book still stands as the most up-to-date book published on pentest tool usage in existence, and one would be hard pressed to find a better price tag for what you get.

BASPT is technical and benefits from its reference nature. Even day-job testers do not get to exercise all of these tools because of differences in engagement types, so it's useful to have one place organizing them all with some usage cases to give context.

If you are just getting into pentesting, or are interested in the gazillion tools in Backtrack and what their differences are, I highly recommend picking up the book. All in all I thought the book represented a good updated intro to the tools and general methods in today's pentesting arsenal. Was it the 1337est, most ninja book ever? No, but it's going on my bookshelf anyway.