

# Review: Penetration Testing with BackTrack by Offensive Security Part 1

I have had the opportunity to enroll in the "Pentesting With BackTrack" course from Offensive Security. Over the next 30 days, I will be posting an update a week with my thoughts on the content that I have worked through in the previous week, along with experiences with labs, support, and also personal revelations. At the end, I am going to give a more objective report on the entire class, listing what I see as strengths, weaknesses, as well as benefits and deficits compared to other classes I've taken. So follow along, as I go from the period before the class starts, all the way through the exam.

The course is described by Offensive Security as, "'Pentesting with BackTrack' (previously known as Offensive Security 101) is an online course designed for network administrators and security professionals who need to get acquainted with the world of offensive security. This penetration testing course introduces the latest hacking tools and techniques, and includes remote live labs for exercising the material presented to the students. This course gives a solid understanding of the penetration testing process, and is equally important for those wanting to either defend or attack their network. The course can be taken from your home, as long as you have a modern computer with high speed internet."

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

Discuss in Forums {mos\_smf\_discuss:Linn}

## Registration to Class Start

Registering for the course was pretty straight forward. I started off by putting my info into the website to start the process. Offensive Security requires some personal information about who you are, and I wasn't sure what it was going to be used for initially, but as the registration process and course delivery process continued, it made a lot more sense. After the registration, I waited a while and got a confirmation email that I had been registered for the class.

Being registered for the class is just the beginning of the pre-course process. From there I was directed to go to a legal page and agree to the rules of the course and, after agreeing, I was taken to the payment pages. In addition to giving information on how to agree to the legal information and pay, the initial email also contained information on how to test connectivity to the lab environment. I am taking this course using BackTrack4 on my Mac, which I didn't have with me when I got the email, so I let this sit for a day or two. When I re-read the email, I noticed a small nugget of information which it seems is critical for adequately testing your connectivity to the lab environment. As it turns out, it clearly says in capitals, obviously cloaked to be easy to miss, that my test credentials "WILL EXPIRE IN 48 HOURS". Guess who waited more than 48 hours to test connectivity?

Luckily the information also tells you how to get access if you wait for too long. The connectivity test comes with a manual which gives clear instructions for how to setup and troubleshoot connectivity with the lab. It was seamless and easy to setup if you have very basic \*nix skills.

There was additional information about how to register on the course forums and where to find the IRC channel, as well as some other contact information. I went ahead and registered, but was surprised that you don't actually get access until the course starts. I was a bit bummed about that, as I was excited to see what was ahead. But in retrospect, many of the exercises are discussed on the forum, so it makes sense that you have to wait to get in and read about the content of the course. I also hopped on IRC and started lurking, and the course admins spend time on IRC helping folks out with problems and chatting. The IRC conversations are about what I expect out of IRC channels, folks helping out others, asking questions, with the occasional banter and fun. It appears to be a friendly environment where past, present, and future course takers are taking part and eager to help.

All course times are done in the GMT +0 timezone, so the night before I expected to get my course material, I got the email that all was ready. The email contained information about how to download the course material, the lab guide, and new connectivity information to the lab environment. I read this email much more carefully after my last encounter with lack of reading comprehension, discovered that these materials are only available for 72 hours. After that time you have to pay to have new materials generated. Each set of materials is watermarked for an individual, so sharing will make it pretty obvious where the materials came from. Due to the 72 hour lifetime of the materials online I made sure to make backups.

From here, I tested connectivity again, logged into the student portal, and made sure I could get to my Windows XP box in the class lab. I wanted to start the material fresh, so after glancing over the lab manual and reading the content creator's thoughts about the course, I stopped there. At this point I have everything I need to start the class: The course material in flash format, the lab manual in pdf format, and connectivity to the lab network via VPN.

Stay tuned for more coming up... next chapter - Information Gathering!

Ryan Linn, CISSP, MCSE, GPEN - Ryan is currently an Information Security Engineer at SAS Institute. Employed in the computer industry since 1997, he has held positions ranging from web developer to Unix Systems Programmer at a large university to his current position in Information Security. Ryan has been responsible for working with large scale deployments of various flavors of \*nix, high availability web and database clusters, as well as for application programming in high availability environments. In the past few years, Ryan has incorporated Windows security into his responsibilities, and is now part of the team responsible for information security globally in one of the largest privately held software companies in the world.