Backtrack Penetration Testing: Introduction

What is Penetration Testing?

Penetration testing is the legal and authorized attempt to exploit a computer system with the intent of making a network or system more secure. The process includes scanning systems looking for weak spots, and launching attacks and prove that the system is vulnerable to attack from a real hacker.

Penetration Testing has several names:

- Pen Testing
- Ethical Hacking
- White Hat Hacking

As you learn more about the art of hacking, you will see three terms used a lot. The white hats, the black hats, and the gray hats. The white hats are the “good guys”. They hack systems and networks so that the black hats (“bad guys”) can not. The black hats, also known as “crackers” are those that use hacking with malicious intent. They’re the ones that want to steal company secrets or your credit card information. For this reason, it is important for the white hats to know the tools and tricks of the black hats to stay a step ahead of them. As for the gray hats, they’re a combination of white and black. They often hack just because they can or like the challenge.

By now you may want to download and install backtrack Linux on your computer. You can learn how to do that at Installing Backtrack.

If you have been following the security world, you may have hear of Kali Linux, also know as the newest Backtrack. Any lessons here can be used in both Backtrack 5 and Kali. I will be writing an article about any differences between the two sometime soon.

Recommended Reading: The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy

A great book for anyone just learning how to hack or just wants to know more about security. Covers a lot of what you’ll find here plus a lot more. I can’t recommend this enough for beginners.
Hacking Lab

Having a place to practice is necessary to learn how to hack. This is were your own home hacking lab comes in. It is a place where you can control your attacks without harming any other systems. We want out lab to be isolated and have no chance of escaping to targets we didn’t mean to attack.

Option 1:

- Two computes
- Ethernet Cable
- A switch

Option 2:

Use Virtual Machines

You will need 3 or more virtual machines. One for backtrack, one for a windows machine, and one for another linux box. The linux box will act as out victim server: SSH, Webserver, FTP, etc.

Option 1 is in case you have older hardware that can’t handle running more than one VM. However, these days, modern hardware can handle them. Option 2 is the better choice because you only need one computer.

Steps in Penetration Testing

- Reconnaissance
- Scanning
- Exploitation
- Maintaining Access