

## Penetration Testing and Network Defense (Cisco Press): Ch 5 - Host Recon

del.icio.us

Discuss in Forums {mos\_smf\_discuss:Book Reviews}

Penetration testing is a growing field but there has yet to be a definitive resource that instructs ethical hackers on how to perform a penetration test with the ethics and responsibilities of testing in mind. Although published by Cisco Press, this vendor-neutral book offers detailed steps on how to emulate an outside attacker in order to assess the security of a network. This practical guide to simulating, detecting, and responding to network attacks also features real-world examples and step-by-step procedures.

Reproduced from the book "Penetration Testing and Network Defense" by Andrew Whitaker, Daniel Newman; Published by Cisco Press; ISBN: 1587052083; Published: Oct 31, 2005; Copyright 2006; Pages: 624; Edition: 1st. Reproduced by permission of Pearson Education, Inc., 800 East 96th Street, Indianapolis, IN 46240. For more info from the publisher: <http://www.ciscopress.com/title/1587052083>

Free Chapter in PDF format - Chapter 5: Performing Host Reconnaissance

From the back cover:

Unlike other books on hacking, this book is specifically geared towards penetration testing. It includes important information about liability issues and ethics as well as procedures and documentation. Using popular open-source and commercial applications, the book shows you how to perform a penetration test on an organization's network, from creating a test plan to performing social engineering and host reconnaissance to performing simulated attacks on both wired and wireless networks.

Penetration Testing and Network Defense also goes a step further than other books on hacking, as it demonstrates how to detect an attack on a live network. By detailing the method of an attack and how to spot an attack on your network, this book better prepares you to guard against hackers. You will learn how to configure, record, and thwart these attacks and how to harden a system to protect it against future internal and external attacks.

## Features

- Create step-by-step testing plans
- Learn to perform social engineering and host reconnaissance
- Evaluate session hijacking methods
- Exploit web server vulnerabilities
- Detect attempts to breach database security
- Use password crackers to obtain access information
- Circumvent Intrusion Prevention Systems (IPS) and firewall protections and disrupt the service of routers and switches
- Scan and penetrate wireless networks
- Understand the inner workings of Trojan Horses, viruses, and other backdoor applications
- Test UNIX, Microsoft, and Novell servers for vulnerabilities
- Learn the root cause of buffer overflows and how to prevent them
- Perform and prevent Denial of Service attacks