

# **Intrusion Detection Systems with Snort**

Advanced IDS Techniques Using  
Snort, Apache, MySQL, PHP, and ACID

## BRUCE PERENS' OPEN SOURCE SERIES

- ◆ *Managing Linux Systems with Webmin: System Administration and Module Development*  
Jamie Cameron
- ◆ *Implementing CIFS: The Common Internet File System*  
Christopher R. Hertel
- ◆ *Embedded Software Development with eCos*  
Anthony J. Massa
- ◆ *The Linux Development Platform: Configuring, Using, and Maintaining a Complete Programming Environment*  
Rafeeq Ur Rehman, Christopher Paul
- ◆ *Intrusion Detection Systems with Snort: Advanced IDS Techniques with Snort, Apache, MySQL, PHP, and ACID*  
Rafeeq Ur Rehman

# **Intrusion Detection Systems with Snort**

Advanced IDS Techniques Using  
Snort, Apache, MySQL, PHP, and ACID

*Rafeeq Ur Rehman*



Prentice Hall PTR  
Upper Saddle River, New Jersey 07458  
[www.phptr.com](http://www.phptr.com)

## Library of Congress Cataloging-in-Publication Data

A CIP catalog record for this book can be obtained from the Library of Congress.

Editorial/production supervision: *Mary Sudul*

Cover design director: *Jerry Votta*

Cover design: *DesignSource*

Manufacturing manager: *Maura Zaldivar*

Acquisitions editor: *Jill Harry*

Editorial assistant: *Noreen Regina*

Marketing manager: *Dan DePasquale*



© 2003 Pearson Education, Inc.

Publishing as Prentice Hall PTR

Upper Saddle River, New Jersey 07458

This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, v1.0 or later (the latest version is presently available at <http://www.opencontent.org/openpub/>).

Prentice Hall books are widely used by corporations and government agencies for training, marketing, and resale.

The publisher offers discounts on this book when ordered in bulk quantities. For more information, contact Corporate Sales Department, Phone: 800-382-3419; FAX: 201-236-7141;

E-mail: [corpsales@prehall.com](mailto:corpsales@prehall.com)

Or write: Prentice Hall PTR, Corporate Sales Dept., One Lake Street, Upper Saddle River, NJ 07458.

Other product or company names mentioned herein are the trademarks or registered trademarks of their respective owners.

Printed in the United States of America

1st Printing

ISBN 0-13-140733-3

Pearson Education LTD.

Pearson Education Australia PTY, Limited

Pearson Education Singapore, Pte. Ltd.

Pearson Education North Asia Ltd.

Pearson Education Canada, Ltd.

Pearson Educación de México, S.A. de C.V.

Pearson Education — Japan

Pearson Education Malaysia, Pte. Ltd.

To open source and free software developers



---

# CONTENTS

<b>Chapter 1</b>	<b>Introduction to Intrusion Detection and Snort</b>	<b>1</b>
1.1	What is Intrusion Detection?	5
1.1.1	<i>Some Definitions</i>	6
1.1.2	<i>Where IDS Should be Placed in Network Topology</i>	8
1.1.3	<i>Honey Pots</i>	9
1.1.4	<i>Security Zones and Levels of Trust</i>	10
1.2	IDS Policy	10
1.3	Components of Snort	12
1.3.1	<i>Packet Decoder</i>	13
1.3.2	<i>Preprocessors</i>	13
1.3.3	<i>The Detection Engine</i>	14
1.3.4	<i>Logging and Alerting System</i>	15
1.3.5	<i>Output Modules</i>	15
1.4	Dealing with Switches	16
1.5	TCP Stream Follow Up	18
1.6	Supported Platforms	18
1.7	How to Protect IDS Itself	19
1.7.1	<i>Snort on Stealth Interface</i>	20
1.7.2	<i>Snort with no IP Address Interface</i>	20
1.8	References	21

---

<b>Chapter 2</b>	<b>Installing Snort and Getting Started</b>	<b>23</b>
2.1	Snort Installation Scenarios	24
2.1.1	<i>Test Installation</i>	24
2.1.2	<i>Single Sensor Production IDS</i>	24
2.1.3	<i>Single Sensor with Network Management System Integration</i>	25
2.1.4	<i>Single Sensor with Database and Web Interface</i>	25
2.1.5	<i>Multiple Snort Sensors with Centralized Database</i>	26
2.2	Installing Snort	28
2.2.1	<i>Installing Snort from the RPM Package</i>	28
2.2.2	<i>Installing Snort from Source Code</i>	29
2.2.3	<i>Errors While Starting Snort</i>	43
2.2.4	<i>Testing Snort</i>	43
2.2.5	<i>Running Snort on a Non-Default Interface</i>	51
2.2.6	<i>Automatic Startup and Shutdown</i>	52
2.3	Running Snort on Multiple Network Interfaces	54
2.4	Snort Command Line Options	55
2.5	Step-By-Step Procedure to Compile and Install Snort From Source Code	56
2.6	Location of Snort Files	56
2.7	Snort Modes	58
2.7.1	<i>Network Sniffer Mode</i>	58
2.7.2	<i>Network Intrusion Detection Mode</i>	65
2.8	Snort Alert Modes	66
2.8.1	<i>Fast Mode</i>	67
2.8.2	<i>Full Mode</i>	68
2.8.3	<i>UNIX Socket Mode</i>	68
2.8.4	<i>No Alert Mode</i>	69
2.8.5	<i>Sending Alerts to Syslog</i>	69
2.8.6	<i>Sending Alerts to SNMP</i>	69
2.8.7	<i>Sending Alerts to Windows</i>	70
2.9	Running Snort in Stealth Mode	71
2.10	References	73
<b>Chapter 3</b>	<b>Working with Snort Rules</b>	<b>75</b>
3.1	TCP/IP Network Layers	76
3.2	The First Bad Rule	77
3.3	CIDR	78
3.4	Structure of a Rule	79



---

3.5	Rule Headers	81
3.5.1	<i>Rule Actions</i>	81
3.5.2	<i>Protocols</i>	83
3.5.3	<i>Address</i>	84
3.5.4	<i>Port Number</i>	86
3.5.5	<i>Direction</i>	88
3.6	Rule Options	88
3.6.1	<i>The ack Keyword</i>	89
3.6.2	<i>The classtype Keyword</i>	89
3.6.3	<i>The content Keyword</i>	93
3.6.4	<i>The offset Keyword</i>	94
3.6.5	<i>The depth Keyword</i>	95
3.6.6	<i>The content-list Keyword</i>	95
3.6.7	<i>The dsize Keyword</i>	95
3.6.8	<i>The flags Keyword</i>	96
3.6.9	<i>The fragbits Keyword</i>	97
3.6.10	<i>The icmp_id Keyword</i>	98
3.6.11	<i>The icmp_seq Keyword</i>	98
3.6.12	<i>The itype Keyword</i>	98
3.6.13	<i>The icode Keyword</i>	99
3.6.14	<i>The id Keyword</i>	100
3.6.15	<i>The ipopts Keyword</i>	100
3.6.16	<i>The ip_proto Keyword</i>	101
3.6.17	<i>The logto Keyword</i>	102
3.6.18	<i>The msg Keyword</i>	103
3.6.19	<i>The nocase Keyword</i>	103
3.6.20	<i>The priority Keyword</i>	103
3.6.21	<i>The react Keyword</i>	104
3.6.22	<i>The reference Keyword</i>	104
3.6.23	<i>The resp Keyword</i>	105
3.6.24	<i>The rev Keyword</i>	107
3.6.25	<i>The rpc Keyword</i>	107
3.6.26	<i>The sameip Keyword</i>	108
3.6.27	<i>The seq Keyword</i>	108
3.6.28	<i>The flow Keyword</i>	108
3.6.29	<i>The session Keyword</i>	109
3.6.30	<i>The sid Keyword</i>	110
3.6.31	<i>The tag Keyword</i>	110
3.6.32	<i>The tos Keyword</i>	111
3.6.33	<i>The ttl Keyword</i>	111

3.6.34	<i>The uricontent Keyword</i>	111
3.7	<b>The Snort Configuration File</b>	112
3.7.1	<i>Using Variables in Rules</i>	112
3.7.2	<i>The config Directives</i>	114
3.7.3	<i>Preprocessor Configuration</i>	116
3.7.4	<i>Output Module Configuration</i>	116
3.7.5	<i>Defining New Action Types</i>	117
3.7.6	<i>Rules Configuration</i>	117
3.7.7	<i>Include Files</i>	117
3.7.8	<i>Sample snort.conf File</i>	118
3.8	<b>Order of Rules Based upon Action</b>	119
3.9	<b>Automatically Updating Snort Rules</b>	120
3.9.1	<i>The Simple Method</i>	120
3.9.2	<i>The Sophisticated and Complex Method</i>	122
3.10	<b>Default Snort Rules and Classes</b>	125
3.10.1	<i>The local.rules File</i>	127
3.11	<b>Sample Default Rules</b>	127
3.11.1	<i>Checking su Attempts from a Telnet Session</i>	127
3.11.2	<i>Checking for Incorrect Login on Telnet Sessions</i>	128
3.12	<b>Writing Good Rules</b>	128
3.13	<b>References</b>	129
 <b>Chapter 4 Plugins, Preprocessors and Output Modules</b>		 <b>131</b>
4.1	<b>Preprocessors</b>	132
4.1.1	<i>HTTP Decode</i>	133
4.1.2	<i>Port Scanning</i>	134
4.1.3	<i>The frag2 Module</i>	135
4.1.4	<i>The stream4 Module</i>	136
4.1.5	<i>The spade Module</i>	137
4.1.6	<i>ARP Spoofing</i>	138
4.2	<b>Output Modules</b>	139
4.2.1	<i>The alert_syslog Output Module</i>	140
4.2.1	<i>The alert_full Output Module</i>	143
4.2.1	<i>The alert_fast Output Module</i>	143
4.2.1	<i>The alert_smb Module</i>	143
4.2.1	<i>The log_tcpdump Output Module</i>	144
4.2.1	<i>The XML Output Module</i>	146
4.2.1	<i>Logging to Databases</i>	150
4.2.1	<i>CSV Output Module</i>	151