

You're logged in as: e c Edit your Profile | Log-out

ADVERTISEMENT

Research and compare laptops before buying






The Web's best resource for security channel professionals

IT CHANNEL NETWORKING CHANNEL **SECURITY CHANNEL** STORAGE CHANNEL SYSTEMS CHANNEL

HOME · NEWS · TOPICS · ITKNOWLEDGE EXCHANGE · TIPS · ASK THE EXPERTS · WEBCASTS · WHITE PAPERS · CAREERS · BLOGS

SEARCH this site and the web ADVANCED SEARCH | SITE INDEX

Search Powered by Google

ADVERTISEMENT Learn more about the security channel topics you care about most - activate your membership to SearchSecurityChannel.com now.

Home > Snort's installation prerequisites for Red Hat Enterprise Linux 5

Step-by-Step Guide:

[EMAIL THIS](#) [LICENSING & REPRINTS](#)

Snort's installation prerequisites for Red Hat Enterprise Linux 5

31 Jul 2007 | SearchEnterpriseLinux.com

By James Turnbull

Once you've confirmed that the IDS sensor Snort can run on your customer's hardware, the next step is ensuring that the proper software has been installed on Red Hat Enterprise Linux 5 to support Snort – this includes MySQL/PostgreSQL and PHP. This step lays the groundwork for installing Snort, compiling Snort and then configuring Snort by setting up its network intrusion detection rules.

Snort has a number of prerequisites that you will need to install depending on how you want to configure it. The most common is MySQL, though you could also use PostgreSQL if you prefer. Snort uses MySQL to store events and alerts. If you wish to add a console, such as BASE, to your Snort installation you will also need to install PHP, including MySQL integration for PHP and a Web server like Apache. In this tip, we're going to use MySQL to store events. For the Snort installation with MySQL, we need to add the following RPMs (best done using your package management mechanism as it will prompt you to install additional packages):

- mysql-server
- mysql-bench
- mysql-devel
- mysqlclient10
- libpcap
- libpcap-devel
- pcre-devel

After installing MySQL, start the server up by using the init script. Remember to change the MySQL password when MySQL starts up.

```
# /etc/init.d/mysqld start
```

After installing the prerequisites, you can install Snort. Snort is available in RPM packages, both binary and source, from Sourcefire or it can be compiled. On the Sourcefire site, RPMs are currently only available for RHEL 4. Until RHEL 5 RPMs are available, you'll need to compile Snort from source or build your own RPMs using the Snort spec file. In this scenario, we're going to compile Snort from source.

```
#####
1. Intrusion detection with Snort on Red Hat Enterprise Linux 5
2. Introduction to network intrusion detection and prevention using
   Snort
```

• Network Intrusion Detection (IDS)

How to test Snort
Snort hardware and network requirements for Red Hat Enterprise Linux 5
Snort's installation prerequisites for Red Hat Enterprise Linux 5
Configuring Snort for Red Hat Enterprise Linux 5
Editing the snort.conf file for Red Hat Enterprise Linux 5
Compiling Snort and configuration with MySQL for Red Hat Enterprise Linux 5
Snort Report
Output options for Snort data
Trend Micro warns of substantial Trojan attack
Snort command line output modes

① RELATED RESOURCES

- 2020software.com, trial software downloads for accounting software, ERP software, CRM software and business software systems
- Search Bitpipe.com for the latest white papers and business webcasts
- Whatis.com, the online computer dictionary

DISCLAIMER: Our Tips Exchange is a forum for you to share technical advice and expertise with your peers and to learn from other enterprise IT professionals. TechTarget provides the infrastructure to facilitate this sharing of information. However, we cannot guarantee the accuracy or validity of the material submitted. You agree that your use of the Ask The Expert services and your reliance on any questions, answers, information or other materials received through this Web site is at your own risk.

[HOME](#) • [NEWS](#) • [TOPICS](#) • [ITKNOWLEDGE EXCHANGE](#) • [TIPS](#) • [ASK THE EXPERTS](#) • [WEBCASTS](#) • [WHITE PAPERS](#) • [CAREERS](#) • [BLOGS](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Site Index](#) | [RSS](#)

SEARCH

SEARCH

TechTarget provides enterprise IT professionals with the information they need to perform their jobs - from developing strategy, to making cost-effective IT purchase decisions and managing their organizations' IT projects - with its network of technology-specific Web sites, events and magazines.

[TechTarget Corporate Web Site](#) | [Media Kits](#) | [Reprints](#) | [Site Map](#)

All Rights Reserved, Copyright 2006 - 2007, TechTarget | [Read our Privacy Policy](#)



- [Acquiring Snort rules](#)
- [Activating Snort rules](#)
- [Loading rules](#)

About the author

Richard Bejtlich is founder of [TaoSecurity](#), author of several books on network security monitoring, including *Extrusion Detection: Security Monitoring for Internal Intrusions*, and operator of the [TaoSecurity blog](#).



Rate this Tip

(BAD) ☐ ☐ ☐ ☐ ☐ (EXCELLENT)

1 2 3 4 5

Share - Digg This! Bookmark with Del.icio.us

SECURITY CHANNEL RELATED LINKS
Ads by Google**McAfee Worm Protection**

Shield Your PC & Prevent Attacks. Essential Protection. Official Site
www.McAfee.com

Security Assessment

Instant ISO 17799 ISMS assessment Comparison to standard & your peers
benchmark.wolcottgroup.com

SCADA Security Course

Hands on SCADA security course learn to assess and secure
InfoSecInstitute.com/SCADA_sec

Security Certifications

Today's Top Choices for Security Certifications
www.genieseeker.com

Security auditing

Download Free IT White Papers about Auditing, General Security & More
www.FindWhitePapers.com

RELATED CONTENT
• **Open Source Security Tools**

- [How to test Snort](#)
- [How to run IDS Snort on Red Hat Enterprise Linux 5](#)
- [Working with Snort's unified output](#)
- [Output options for Snort data](#)
- [Snort IDS installation basics and tips for security resellers](#)
- [Snort IDS upgrade and tips on the Snort.conf file](#)
- [Detect events without Snort IDS rules](#)
- [Understand the Snort IDS Concurrent Versions System and 2.7 Beta 1 installation](#)
- [Nmap Tutorial: An introduction for VARs and security consultants](#)
- [Nmap Tutorial: How to use the open source network scanner](#)

• **Open Source Security Software**

- [How to test Snort](#)
- [How to run IDS Snort on Red Hat Enterprise Linux 5](#)
- [Snort hardware and network requirements for Red Hat Enterprise Linux 5](#)
- [Snort's installation prerequisites for Red Hat Enterprise Linux 5](#)
- [Editing the snort.conf file for Red Hat Enterprise Linux 5](#)
- [Configuring Snort for Red Hat Enterprise Linux 5](#)
- [Compiling Snort and configuration with MySQL for Red Hat Enterprise Linux 5](#)
- [Snort Report](#)
- [Output options for Snort data](#)
- [Snort command line output modes](#)

• **Snort****REFERENCE DESK****Open Source Security Software****NEWS, TIPS & MORE**

- [Editing the snort.conf file for Red ... \(STEP-BY-STEP GUIDE\)](#)
- [Configuring Snort for Red Hat ... \(STEP-BY-STEP GUIDE\)](#)
- [How to run IDS Snort on Red Hat Enterprise Linux 5 \(TIP\)](#)
- [Snort ... \(SNORT IDS TIPS FOR VARs AND SYSTEMS INTEGRATORS\)](#)
- [VIEW MORE](#)

For Today's Security-Focused
VARs, Systems Integrators and Resellers

**Get Daily Insights on
Hot Projects,
Vendor Programs
and Channel News**

SEE ALSO

- **Related Topics:**
[Open Source Security Software](#), [Security Reseller Concerns](#), [Security Vendors](#)
- **Site Highlights:**
[Increasing Business Partner Productivity](#)
[UTM: A necessity for the mid-market](#)

GET E-MAIL UPDATES

Submit your e-mail below to receive Security Channel-related news, tech tips and more, delivered to your inbox.

☐ **Security Channel Advisor**
☐ **Channel This Week**
☐ **Channel News Wire**

E-mail:

Not a member? We'll activate your FREE membership with your subscription.

How to test Snort
How to run IDS Snort on Red Hat Enterprise Linux 5
Editing the snort.conf file for Red Hat Enterprise Linux 5
Output options for Snort data
Snort command line output modes
Snort.conf output options
Snort IDS installation basics and tips for security resellers
Snort IDS upgrade and tips on the Snort.conf file
Detect events without Snort IDS rules
Understand the Snort IDS Concurrent Versions System and 2.7 Beta 1 installation

RELATED RESOURCES

- 2020software.com, trial software downloads for accounting software, ERP software, CRM software and business software systems
- Search Bitpipe.com for the latest white papers and business webcasts
- Whatis.com, the online computer dictionary

DISCLAIMER: Our Tips Exchange is a forum for you to share technical advice and expertise with your peers and to learn from other enterprise IT professionals. TechTarget provides the infrastructure to facilitate this sharing of information. However, we cannot guarantee the accuracy or validity of the material submitted. You agree that your use of the Ask The Expert services and your reliance on any questions, answers, information or other materials received through this Web site is at your own risk.

[HOME](#) • [NEWS](#) • [TOPICS](#) • [ITKNOWLEDGE EXCHANGE](#) • [TIPS](#) • [ASK THE EXPERTS](#) • [WEBCASTS](#) • [WHITE PAPERS](#) • [CAREERS](#) • [BLOGS](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Site Index](#) | [RSS](#)

SEARCH



SEARCH

TechTarget provides enterprise IT professionals with the information they need to perform their jobs - from developing strategy, to making cost-effective IT purchase decisions and managing their organizations' IT projects - with its network of technology-specific Web sites, events and magazines.

[TechTarget Corporate Web Site](#) | [Media Kits](#) | [Reprints](#) | [Site Map](#)

All Rights Reserved, Copyright 2006 - 2007, TechTarget | [Read our Privacy Policy](#)



- Installation
- Sniffer mode
- Packet logger mode
- Intrusion detection mode
- Conclusion

About the author

Richard Bejtlich is founder of TaoSecurity, author of several books on network security monitoring, including *Extrusion Detection: Security Monitoring for Internal Intrusions*, and operator of the TaoSecurity blog (taosecurity.blogspot.com).

Rate this Tip

(BAD) ☐ ☐ ☐ ☐ ☐ (EXCELLENT)

1 2 3 4 5

Share - Digg This! Bookmark with Del.icio.us

SECURITY CHANNEL RELATED LINKS**Ads by Google****Configuration Manager**

Web-based Configuration Mgmt tool for Routers Switches Firewalls etc
deviceexpert.com/network-config

IP6 Vulnerability Scanner

How vulnerable are your networks? Find out with the Saint Scanner.
www.saintcorporation.com

Network Configuration.

Free Network Config. Mgt. Roadmap. Learn Best Practices. Download now!
Voyence.com/Network_Compliance

Protect Confidential Data

Leader in data loss prevention. Contact us for a free demo.
www.orchestria.com

Network Behavior Analysis

Secure your internal network with Mazu's behavior-based monitoring
www.mazunetworks.com

**RELATED CONTENT**• **Open Source Security Software**

- How to test Snort
- How to run IDS Snort on Red Hat Enterprise Linux 5
- Snort hardware and network requirements for Red Hat Enterprise Linux 5
- Snort's installation prerequisites for Red Hat Enterprise Linux 5
- Editing the snort.conf file for Red Hat Enterprise Linux 5
- Configuring Snort for Red Hat Enterprise Linux 5
- Compiling Snort and configuration with MySQL for Red Hat Enterprise Linux 5
- Snort Report
- Output options for Snort data
- Snort command line output modes

• **Open Source Security Tools**

- How to test Snort
- How to run IDS Snort on Red Hat Enterprise Linux 5
- Working with Snort's unified output
- Output options for Snort data
- Snort IDS upgrade and tips on the Snort.conf file
- Detect events without Snort IDS rules
- Understand the Snort IDS Concurrent Versions System and 2.7 Beta 1 installation
- Nmap Tutorial: An introduction for VARs and security consultants
- Nmap Tutorial: How to use the open source network scanner
- Nessus Tutorial: Using the open source vulnerability scanning tool

REFERENCE DESK**Open Source Security Software****NEWS, TIPS & MORE**

- Editing the snort.conf file for Red ... (STEP-BY-STEP GUIDE)
- Configuring Snort for Red Hat ... (STEP-BY-STEP GUIDE)
- How to run IDS Snort on Red Hat Enterprise Linux 5 (TIP)
- Snort ... (SNORT IDS TIPS FOR VARs AND SYSTEMS INTEGRATORS)
- VIEW MORE

For Today's Security-Focused
VARs, Systems Integrators and Resellers

**Get Daily Insights on
Hot Projects,
Vendor Programs
and Channel News**


SearchSecurityChannel.com

SEE ALSO

- **Related Topics:**
Open Source Security Software , Security Reseller Concerns, Security Vendors
- **Site Highlights:**
Increasing Business Partner Productivity
UTM: A necessity for the mid-market

GET E-MAIL UPDATES

Submit your e-mail below to receive Security Channel-related news, tech tips and more, delivered to your inbox.

☐ Security Channel Advisor

☐ Channel This Week

☐ Channel News Wire

E-mail:

Not a member? We'll activate your FREE membership with your subscription.

The DDOS Specialist

Identify and block DDOS attacks automatically
and in real time.
www.riorey.com

Intrusion Prevention ROI

Free IPS ROI Whitepaper: Achieve Over 100%
Return Utilizing IPS
www.NitroSecurity.com

IT Security Professionals

Network Infrastructure Security Microsoft and
Cisco Partners
www.dccorporation.com

[Snort Install](#) [Snort Windows](#) [Snort Sensor](#) [Download Snort](#) [Snort Alerts](#) [Snort Conf](#)

HARDCORE IDS

What is Hardcore IDS?

[HOME](#)[NEWS](#)[IN THE NOW](#)[HARDCORE IDS](#)[FORUMS](#)

Hardcore IDS builds a secured GNU/Linux operating system and intrusion detection system using Fedora Core 5 with Snort 2.6.1.3 and Aanval 2.3 as an optional front-end to monitor your network for attacks and vulnerabilities. Hardcore IDS uses the Snort and Bleeding Edge Snort rules.

You can setup Hardcore IDS on one host or many. There are three install types to choose from so you have the ability to roll out your IDS solution how you see fit.



Console



Sensor



Console + Sensor

Latest News

- 3-30-07 Hardcore IDS 1.2 released for Fedora Core 5.
- 8-28-06 Hardcore IDS 1.1 released for Fedora Core 5.
- 8-22-06 Hardcore IDS 1.1 released for Fedora Core 4. See the ChangeLog for details.
- 7-31-06 Hardcore IDS 1.0 to be released at Defcon 14.
- 7-30-06 Development of Hardcore IDS for Fedora Core 5 is underway.

Download

Installer Type	Checksum	Last Modified	File
Hardcore IDS 1.2 for Fedora Core 5	MD5	Mon Apr 2 22:34:00 2007	hardcore-1.2-fc5.tar.gz

Support

Post any questions or comments in the forums. If you like Hardcore IDS and it was useful for you, optionally you can make a donation to support the work of the project.

[Make a Donation](#)[E-MAIL](#)

Questions, Comments or Suggestions

You're logged in as: e c Edit your Profile | Log-out

Learn to solve the current technology-specific problems you face.



The Web's best resource for security channel professionals

IT CHANNEL

NETWORKING CHANNEL

SECURITY CHANNEL

STORAGE CHANNEL

SYSTEMS CHANNEL

HOME NEWS TOPICS ITKNOWLEDGE EXCHANGE TIPS ASK THE EXPERTS WEBCASTS WHITE PAPERS CAREERS BLOGS

SEARCH this site and the web

SEARCH

ADVANCED SEARCH | SITE INDEX

Search Powered by Google

Learn more about the security channel topics you care about most - activate your membership to SearchSecurityChannel.com now.

Home > Security Channel Tips > Snort Report > Snort IDS installation basics and tips for security resellers

Security Channel Tips:

EMAIL THIS

TIPS & NEWSLETTERS TOPICS

SNORT REPORT

Snort IDS installation basics and tips for security resellers

Richard Bejtlich

04.30.2007

Rating: -3.33- (out of 5)

RSS FEEDS: Enterprise IT tips and expert advice



Add to Google

Welcome to the first edition of Snort Report. The goal of this column is to provide value-added resellers (VARs) and security consultants with suggestions for the productive use of Snort, an open source intrusion detection and intrusion prevention system developed by Marty Roesch and his team at Sourcefire. To provide a solid foundation for future articles, this issue concentrates on installation and fundamentals.

Before discussing technical details, it's important to consider what Snort is – and what it is not – so you can "sell" the open source IDS/IPS to reluctant customers and properly set their expectations.

First, Snort is a network traffic inspection program and, when suitably configured, an access control system. Snort is not a "badness-ometer." One cannot expect to run Snort on an arbitrary network location and simply start discovering malicious activity. While it is possible to accomplish this goal, proper understanding of Snort's capabilities, limitations and deployment model is required for effective use. That's where you come in. You cannot simply drop Snort into place on your customer's network and leave it up to them to efficiently manage.

Second, Snort is not "lightweight." When Marty Roesch wrote his 1999 paper on Snort, his use of the term "lightweight" intended to convey the idea that Snort did not use many system resources. "Lightweight" never meant "ineffective." Today, Snort is extremely powerful, but effective use of these powers requires a dedicated system with plenty of RAM (1 GB or more is recommended) and quality components.

Third, although Snort originally relied on content matching in order to identify malicious activity, the program has advanced considerably beyond that simple technique and incorporates today's technologies. Snort indeed uses rules for core functionality, but some of those signatures are exceedingly complicated. Rules work alongside non-signature based decoders and preprocessors to alert users of many sorts of suspicious and malicious activities.

Snort: Fundamentals and installation tips for the channel

Introduction

LEAVE REQUEST

Prepare one request only and submit it to your Line Supervisor and Nancy. The original request should be returned to Lisa for her records, with copies distributed to the employee and line supervisor.

I request the following: Vacation ☒ Admin. ☐ Holiday ☐ Sick ☐ AWOP ☐ Other ☐ (Please indicate)

Day/Hours(s) desired: Sept 21st thru Sept 21st

Add'l. Info.:

Eileen Paulin 08/30/07
Employee's Signature Date

Foy Harper 8/30/07
Line Supervisor Date

Nancy Romero 8-30-07
Nancy Romero COB Date

(Circle Choice)

(Approved/Deny)

(Approved/Deny)



Internet Explorer cannot display the webpage

Most likely causes:

- You are not connected to the Internet.
- The website is encountering problems.
- There might be a typing error in the address.

What you can try:

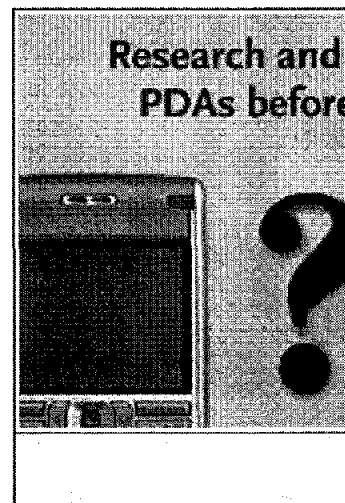
- Diagnose Connection Problems
- ▾ More information

REFERENCE DESK

Open Source Security So

NEWS, TIPS & MORE

- Editing the snort.conf file for Red Hat (GUIDE)
 - Configuring Snort for Red Hat ...
 - How to run IDS Snort on Red Hat ...
 - Snort ... (SNORT IDS TIPS FOR V INTEGRATORS)
- VIEW MORE



SEE ALSO

- **Related Topics:**
Open Source Security Software
Concerns, Security Vendors
- **Site Highlights:**
Increasing Business Partner Pro
UTM: A necessity for the mid-m

GET E-MAIL UPDATES

Submit your e-mail below to receive related news, tech tips and more, t

- ☐ Security Channel Advisor
- ☐ Channel This Week
- ☐ Channel News Wire

E-mail:

Not a member? We'll activate your membership with your sub

[HOME](#) · [NEWS](#) · [TOPICS](#) · [ITKNOWLEDGE EXCHANGE](#) · [TIPS](#) · [ASK THE EXPERTS](#) · [WEBCASTS](#) · [WHITE PAPERS](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Site Index](#) | [RSS](#)

SEARCH

TechTarget provides enterprise IT professionals with the information they need to perform their jobs - from developing strategy, to making purchase decisions and managing their organizations' IT projects - with its network of technology-specific Web sites, events and magazines.

[TechTarget Corporate Web Site](#) | [Media Kits](#) | [Reprints](#) | [Site Map](#)

All Rights Reserved, Copyright 2006 - 2007, TechTarget | [Read our Privacy Policy](#)

- [Snort hardware and network setup requirements](#)
- **Snort's installation prerequisites**
- [Compiling Snort and configuration with MySQL](#)
- [Configuring Snort and setting up rules](#)
- [Editing the snort.conf file](#)

About the author

James Tumbull works for the National Australia Bank as a Security Architect. He is also the author of *Hardening Linux*, which focuses on hardening Linux hosts including the base operating system, file systems, firewalling, connections, logging, testing your security and securing a number of common applications including e-mail, FTP and DNS. He is an experienced infrastructure architect with a background in Linux/Unix, AS/400, Windows, and storage systems. He has been involved in security consulting, infrastructure security design, SLA and service definition and has an abiding interest in security metrics and measurement.

Share - [Digg This!](#)  [Bookmark with Del.icio.us](#)

 SECURITY CHANNEL RELATED LINKS**Ads by Google****Massachusetts Linux**

Register Today for Information Technology Training & Certification
www.butrain.com

Red Hat Linux Software

Find Red Hat Linux Software now See our Linux Software guide
LinuxSoftware.CompareBeyond.com

Free Virtualization

Download Virtual Iron for Free Compare to VMware. Enterprise-Class
www.virtualiron.com

Easy Linux Monitoring

"Product of the Year" - TechWorld Easy to Install & Use - Free Trial
www.uptimesoftware.com

1U 14" Server for \$475

Thermal Efficient 1U for AMD, Intel Linux: Servers, Storage, Support
www.ironsystems.com

 RELATED CONTENT• **Network Intrusion Detection (IDS)**

- [How to test Snort](#)
- [Snort hardware and network requirements for Red Hat Enterprise Linux 5](#)
- [Compiling Snort and configuration with MySQL for Red Hat Enterprise Linux 5](#)
- [Configuring Snort for Red Hat Enterprise Linux 5](#)
- [Editing the snort.conf file for Red Hat Enterprise Linux 5](#)
- [Snort Report](#)
- [Output options for Snort data](#)
- [Trend Micro warns of substantial Trojan attack](#)
- [Snort command line output modes](#)
- [Snort.conf output options](#)

• **Open Source Security Software**

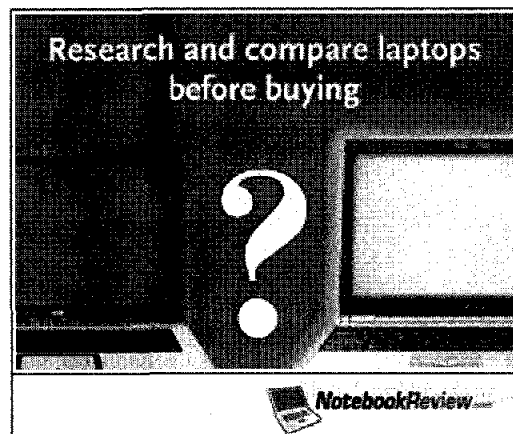
- [How to test Snort](#)
- [How to run IDS Snort on Red Hat Enterprise Linux 5](#)
- [Snort hardware and network requirements for Red Hat Enterprise Linux 5](#)
- [Compiling Snort and configuration with MySQL for Red Hat Enterprise Linux 5](#)
- [Editing the snort.conf file for Red Hat Enterprise Linux 5](#)
- [Configuring Snort for Red Hat Enterprise Linux 5](#)
- [Snort Report](#)
- [Output options for Snort data](#)
- [Snort command line output modes](#)
- [Snort.conf output options](#)

 RELATED RESOURCES

- [2020software.com](#), trial software downloads for accounting software, ERP software, CRM software and business software systems
- [Search Bitpipe.com](#) for the latest white papers and business webcasts
- [Whatis.com](#), the online computer dictionary

REFERENCE DESK**Network Intrusion Detection (IDS)****NEWS, TIPS & MORE**

- [How to test Snort \(TIP\)](#)
- [Compiling Snort and configuration ... \(STEP-BY-STEP GUIDE\)](#)
- [Snort's installation prerequisites ... \(STEP-BY-STEP GUIDE\)](#)
- [Snort hardware and network ... \(STEP-BY-STEP GUIDE\)](#)
- [VIEW MORE](#)

**SEE ALSO**

- **Related Topics:**
 - [Network Intrusion Detection \(IDS\)](#) , [Denial of Service Prevention](#)
- **Site Highlights:**
 - [Increasing Business Partner Productivity](#)
 - [UTM: A necessity for the mid-market](#)

GET E-MAIL UPDATES

Submit your e-mail below to receive Security Channel-related news, tech tips and more, delivered to your inbox.

☐ **Security Channel Advisor**

☐ **Channel This Week**

☐ **Channel News Wire**

E-mail:

Not a member? We'll activate your FREE membership with your subscription.

[HOME](#) · [NEWS](#) · [TOPICS](#) · [ITKNOWLEDGE EXCHANGE](#) · [TIPS](#) · [ASK THE EXPERTS](#) · [WEBCASTS](#) · [WHITE PAPERS](#) · [CAREERS](#) · [BLOGS](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Site Index](#) | [RSS](#)

SEARCH

SEARCH

TechTarget provides enterprise IT professionals with the information they need to perform their jobs - from developing strategy, to making cost-effective IT purchase decisions and managing their organizations' IT projects - with its network of technology-specific Web sites, events and magazines.

[TechTarget Corporate Web Site](#) | [Media Kits](#) | [Reprints](#) | [Site Map](#)



All Rights Reserved, Copyright 2006 - 2007, TechTarget | [Read our Privacy Policy](#)

You're logged in as: e c Edit your Profile | Log-out

Learn to solve the current technology-specific problems you face.



The Web's best resource for security channel professionals

IT CHANNEL

NETWORKING CHANNEL

SECURITY CHANNEL

STORAGE CHANNEL

SYSTEMS CHANNEL

HOME · NEWS · TOPICS · ITKNOWLEDGE EXCHANGE · TIPS · ASK THE EXPERTS · WEBCASTS · WHITE PAPERS · CAREERS · BLOGS

SEARCH this site and the web

SEARCH

ADVANCED SEARCH | SITE INDEX

Search Powered by Google

Learn more about the security channel topics you care about most - activate your membership to SearchSecurityChannel.com now.

Home > Security Channel Tips > Snort Report > Snort IDS rules

Security Channel Tips:

EMAIL THIS

TIPS & NEWSLETTERS TOPICS

SNORT REPORT

Snort IDS rules

Richard Bejtlich

04.04.2007

Rating: --- (out of 5)

RSS FEEDS: Security Channel Update



Add to Google

When Marty Roesch originally wrote Snort, he considered shipping it without any rules. Marty envisioned that Snort users would write their own rules, customized for their environment. Keep this in mind when you're deploying Snort on your customer's network. In the first Snort Report I wrote, "Snort is not a 'badness-ometer.' One cannot expect to run Snort on an arbitrary network location and simply start discovering malicious activity." Rules represent a rule writer's best approximation of a means to detect a certain type of network event.

Snort rules -- and any similar mechanism that performs some degree of matching against a packet or stream of packets -- are designed to alert an operator to a network event of interest. The two critical components in this statement are "network event" and "of interest." Snort rules often represent an inference -- sometimes even an educated guess -- that a particular network event has occurred. This network event is usually identified as a suspicious or malicious activity, but some of the network events could be utterly benign. Given the right combination of matching and/or inspection, Snort rules can be told to identify any sort of packet -- or even stream of packets -- desired by the rule author. In some cases, however, the means by which the rule author chooses to identify a network event might apply to traffic that is not what he wanted to identify. I'll return to this thought when I discuss false positives.

The second important part of the statement above is "of interest." One Snort operator might think a certain rule or set of rules is absolutely critical to his environment, while another Snort operator couldn't care less. There is no right or wrong answer here. This is one of the main reasons Marty Roesch didn't want to ship rules with Snort. Who could say that an operator of Microsoft Windows IIS Web servers would want to run a set of rules detecting attacks against Apache Web servers, or vice versa?

Snort Report -- IDS Snort rules

- Introduction
- False positives
- Sourcefire rules
- Bleeding Edge Threats rules

Request ID	0000951	Submitter	RDHENDERSON	Last Modified By	RDHENDERSON
Status	New	Create Date	10/1/2007 2:40:43 PM	Modified Date	10/1/2007 2:40:43 PM
Priority	Medium	Projected Completion			

Clear User Information

User Information

User Last Name	Barnes
User First Name	Olivia
Novell Login	
Department	3rd District
Division	
Phone Number	
User Location	
User Email	obarnes@rcbos.org

Problem Information

Problem Categor	Other
Description	OBBARNES from the 3rd district requested a surge protector
Work History	
Solution	

Device Information

Device Type	
Device Location	
Device Name	

Vendor Information

Vendor Name	
Vendor Req #	
Vendor Contact	
Vendor Phone	
Vendor Email	

Tracking Information

Assigned To	Caroline, Etienne
Related Req ID	
Find Related Request	
Audit Trail	

Attachment Field (5mb Limit)

--

to LL-9

IN ITEMS

NOT updating
updates

▲ bosltp-d210.rcbos.local	10.22.28.75
▲ boswks100.rcbos.local	10.22.28.113
▲ boswks101.rcbos.local	10.22.28.111
▲ boswks106.rcbos.local	10.22.28.81
▲ boswks115.rcbos.local	10.22.28.76
▲ boswks118.rcbos.local	10.22.28.99
▲ boswks138.rcbos.local	10.22.28.124
▲ boswks139.rcbos.local	10.22.28.130
▲ boswks141.rcbos.local	10.176.53.27
▲ boswks143.rcbos.local	10.22.28.120
▲ boswks144.rcbos.local	10.22.28.89
▲ boswks145.rcbos.local	10.22.28.117
▲ boswks207.rcbos.local	10.22.28.119

- From desk

LISA

RCIT

Does not allow access

RCIT

L405

209

2800

SPICEWORKS

Novell iPrint Client

Name	Installed On	Version	Product Id	Product Key
boswks112		v04.05.00	10.22.28.69	Permitted denied
boswks126		v04.05.00	Eric Stone	
boswks123		v04.05.00	123	
boswks124		v04.05.00	124	

AGENDA
MONDAY, SEPTEMBER 17, 2007
BOARD OF SUPERVISORS – COUNTY OF RIVERSIDE
1st FLOOR – COUNTY ADMINISTRATIVE CENTER
BOARD CHAMBERS
4080 Lemon Street, Riverside, Calif.
(Clerk 951-955-1060)

8:30 A.M.

Invocation by Maria Vasquez, Board Assistant, Clerk of the Board Office

Pledge of Allegiance to the Flag

CONCURRENT EXECUTIVE SESSION-COUNTY OF RIVERSIDE, REDEVELOPMENT AGENCY, REGIONAL PARK AND OPEN SPACE DISTRICT, FLOOD CONTROL AND WATER CONSERVATION DISTRICT, WASTE RESOURCES MANAGEMENT DISTRICT, HOUSING AUTHORITY, PERRIS VALLEY CEMETERY DISTRICT, IN-HOME SUPPORTIVE SERVICES PUBLIC AUTHORITY AND COMMUNITY FACILITIES DISTRICTS:

With respect to every item of business to be discussed in closed session pursuant to Government Code Section 54956.9:

Conference with legal counsel-anticipated litigation:

Initiation of litigation pursuant to subdivision (c) of Government Code Section 54956.9:

A.1 Three potential cases.

With respect to every item of business to be discussed in closed session pursuant to Government Code Section 54956.9:

Conference with legal counsel-anticipated litigation:

Significant exposure to litigation pursuant to subdivision (b) of Government Code Section 54956.9:

B.1 One potential case.

With respect to every item of business to be discussed in closed session pursuant to Government Code Section 54957.6:

C.1 Conference with labor negotiator:

Agency negotiator – Ron Komers

Employee organization – RSA, LIUNA, Management, and Unrepresented

With respect to every item of business to be discussed in closed session pursuant to Section 54957(b)(1):

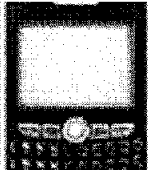
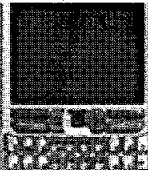
D.1 Public Employee Appointment

Title: Director of Public Social Services

You're logged in as: e

ADVERTISEMENT

Research and compare PDAs before buying



Brigl



The Web's best resource for security channel professionals

IT CHANNEL

NETWORKING CHANNEL

SECURITY CHANNEL

STORAGE CHANNEL

HOME · NEWS · TOPICS · ITKNOWLEDGE EXCHANGE · TIPS · ASK THE EXPERTS · WEBCASTS · WHITE PAPERS

SEARCH this site and the web

SEARCH

ADVANCED SEARCH | SITE INDEX

Se

ADVERTISEMENT

Learn more about the security channel topics you care about most - activate your membership to SearchSecurityChannel.com

Home > Configuring Snort for Red Hat Enterprise Linux 5

Step-by-Step Guide:

 EMAIL THIS

Configuring Snort for Red Hat Enterprise Linux 5

31 Jul 2007 | SearchEnterpriseLinux.com

By James Turnbull

Once you've confirmed that the IDS sensor *Snort* can run on your customer's hardware under Red Hat Enterprise Linux 5, ensured that the *proper software for Snort* has been installed, and configured Snort with MySQL, the next step is to configure Snort's configuration directory and logging directory. This paves the way for the final step of editing the *snort.conf* file.

We need to configure *Snort* and add some detection rules. We start by creating a configuration directory, */etc/snort*, and a logging directory, */var/log/snort*. We then add the example configuration files from the package to */etc/snort*.

```
# mkdir /etc/snort
# mkdir /var/log/snort
# chown snort:snort /var/log/snort
# cd snort-2.6.1.5/etc
# cp *.conf *.config *.map sid generators /etc/snort
```

Now, we make a directory to hold the rules and signature documents and then download a set of rules.

```
# mkdir /etc/snort/rules
```

Snort rules come in a variety of flavours:

- a default set that is available at the time of a Snort release,
- a set available to unregistered users, a set available to users who register on the Sourcefire site,
- a set of community created rules

- and finally, a set for users who buy a subscription from Sourcefire.

We're going to grab the unregistered user set initially:

```
# wget http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_pr/
snortrules-pr-2.4.tar.gz
```

You can go to the Sourcefire site and register, or buy a subscription to get the other rule sets. The other sets contain a more recent collection of rules. New rules are available and are added to these sets much quicker.

Next, we unpack the rules and signatures in the archive and moved them into the `/etc/snort` directory.

```
# tar -xvzf snortrules-pr-2.4.tar.gz
# mv doc rules /etc/snort
```

- Intrusion detection with Snort on Red Hat Enterprise Linux 5**
- [Introduction to network intrusion detection and prevention using Snort](#)
 - [Snort hardware and network setup requirements](#)
 - [Snort's installation prerequisites](#)
 - [Compiling Snort and configuration with MySQL](#)
 - **Configuring Snort and setting up rules**
 - [Editing the snort.conf file](#)

About the author

James Turnbull works for the National Australia Bank as a Security Architect. He is also the author of [Hardening Linux](#), which focuses on hardening Linux hosts including the base operating system, file systems, firewalling, connections, logging, testing your security and securing a number of common applications including e-mail, FTP and DNS. He is an experienced infrastructure architect with a background in Linux/Unix, AS/400, Windows, and storage systems. He has been involved in security consulting, infrastructure security design, SLA and service definition and has an abiding interest in security metrics and measurement.

Share - [Digg This!](#)  [Bookmark with Del.icio.us](#)

SECURITY CHANNEL RELATED LINKS

Ads by Google

IT Security Professionals

Network Infrastructure Security Microsoft and Cisco Partners
www.dccorporation.com

Security network

Structured Cabling Solutions for CCTV & Surveillance. Contact Us Now
www.NetClear.com/ESS

Security Certified Fast.

CISSP, CheckPoint FW-1, Hacking All-Inclusive. Hands-on training.
www.technow.com

Network Security

Optimize network bandwidth and Accelerate your applications.
www.BandwidthOptimizations.com

Central Endpoint Security

Protect assets, lockdown USB, policy-based security. Free eval.
www.futuresoft.com

i RELATED CONTENT**• Open Source Security Software**

- How to test Snort
- How to run IDS Snort on Red Hat Enterprise Linux 5
- Snort hardware and network requirements for Red Hat Enterprise Linux 5
- Snort's installation prerequisites for Red Hat Enterprise Linux 5
- Editing the snort.conf file for Red Hat Enterprise Linux 5
- Compiling Snort and configuration with MySQL for Red Hat Enterprise Linux 5
- Snort Report
- Output options for Snort data
- Snort command line output modes
- Snort.conf output options

• Network Intrusion Detection (IDS)

- How to test Snort
- Snort hardware and network requirements for Red Hat Enterprise Linux 5
- Snort's installation prerequisites for Red Hat Enterprise Linux 5
- Compiling Snort and configuration with MySQL for Red Hat Enterprise Linux 5
- Editing the snort.conf file for Red Hat Enterprise Linux 5
- Snort Report
- Output options for Snort data
- Trend Micro warns of substantial Trojan attack
- Snort command line output modes
- Snort.conf output options

i RELATED RESOURCES

- 2020software.com, trial software downloads for accounting software, ERP software, CRM software and business software systems
- Search Bitpipe.com for the latest white papers and business webcasts
- Whatis.com, the online computer dictionary

TOSHIBA

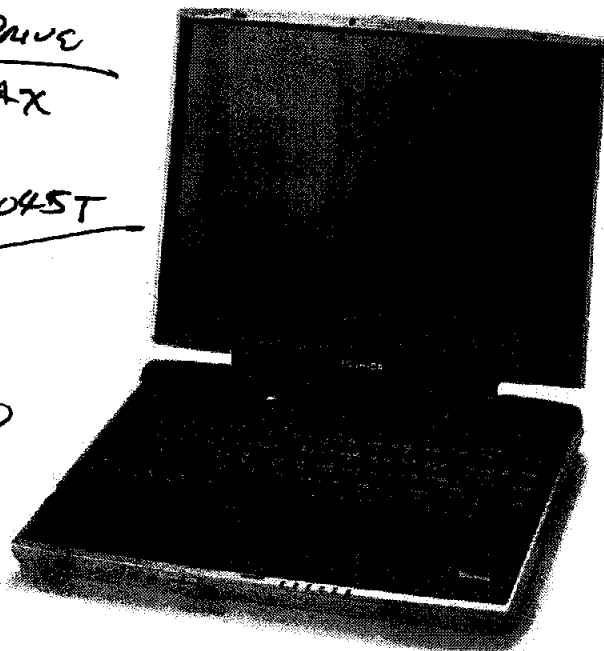
The future-proof computing platform
offering wireless connectivity

TECRA 9100

- Enhanced portability and new design with robust magnesium casing configurable from 2.2kg
- Cutting-edge performance with up to Mobile Intel® Pentium® 4 Processor 2.00GHz-M, SD Media slot and i.LINK (IEEE 1394) port
- Complete mobile communication center with built-in modem, 10/100Mbps Ethernet, optional wireless LAN and Bluetooth™ module kits¹ with SPANworks™ software
- Brilliant graphics capability with 14.1" TFT color display and 16MB Video Memory
- Versatile Slim SelectBay design offers flexible expansion with optional 2nd HDD, 2nd Battery, DVD-ROM, CD-R/RW or CD-RW/DVD-ROM drives
- Common set of drivers, hardware components, expansion options support and standard software for lower Enterprise Cost of Ownership

40 GIG Hard Drive
MIK 4019 GAX
HDD 2171
S/N 52010045T

VIDEO CARD
ATI GRAPHICS -
CPAD 128 PRO

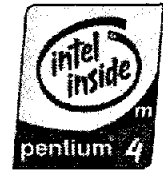


Toshiba recommends Microsoft® Windows® XP Professional for business.

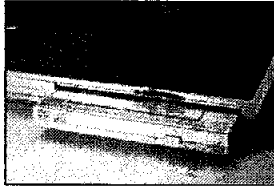
Choose freedom.

TECRA 9100

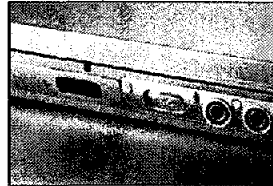
The new TECRA 9100 is built around a future-proofed platform concept that protects your investment and allows you to plan for the future with confidence. By incorporating high-powered Mobile Intel® Pentium® 4 Processor-M, common expansion options support, and latest communication technologies, including optional wireless LAN Card Kit¹, Bluetooth module kit¹ and SD Media slot, it opens up a whole new world of mobility and wireless connectivity in a new stylish, lightweight case.



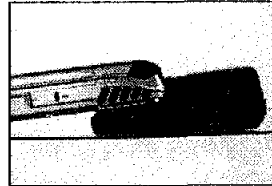
Toshiba recommends Microsoft® Windows® XP Professional for Business.



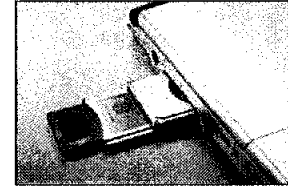
Versatile: use the SelectBay slot to swap CD, DVD, CD-R/RW and CD-RW/DVD drives, hard disks, battery pack and weight saver. Built-in SD Media slot enhances communications between portable digital devices.



Wireless connectivity becomes a reality with the built-in antenna and optional Wireless LAN Card Kit¹ or/and Bluetooth™ Module Kit¹, allowing users to access data anytime, anywhere without the need for cable.



Common docking support: The Advanced Port Replicator offers convenience one-touch docking solution for your office peripherals and is fully compatible with PORTEGE 4000/4010 and Satellite Pro 6000/6100.



Hands-on security: an optional Fingerprint PC Card protects the TECRA 9100 at both BIOS and OS level, enhancing data security and simplifying access for authorized users without any need to remember numerous passwords.

TECRA 9100			
Product Number	PT910L-5XPLK	PT910L-5XP29	PT910L-501V1
Processor ²	Mobile Intel® Pentium® 4 Processor 1.80GHz-M supports Enhanced Intel® SpeedStep® Technology, 400MHz PSB 20KB Integrated, 512KB L2 Integrated	Mobile Intel® Pentium® 4 Processor 1.80GHz-M supports Enhanced Intel® SpeedStep® Technology, 400MHz PSB 20KB Integrated, 512KB L2 Integrated	Mobile Intel® Pentium® 4 Processor 2.00GHz-M supports Enhanced Intel® SpeedStep® Technology, 400MHz PSB 20KB Integrated, 512KB L2 Integrated
Cache			
Chipset	Intel® 845MP	Intel® 845MP	Intel® 845MP
Memory	256MB PC2100 DDR SDRAM, expandable to 1024MB ³	256MB PC2100 DDR SDRAM, expandable to 1024MB ³	256MB PC2100 DDR SDRAM, expandable to 1024MB ³
Mass Storage	30GB S.M.A.R.T., up to 90GB if optional 2 nd HDD is installed ⁴	40GB S.M.A.R.T., up to 100GB if optional 2 nd HDD is installed ⁴	40GB S.M.A.R.T., up to 100GB if optional 2 nd HDD is installed ⁴
Hard Disk			
Optical Drive	Hot swappable 8X/8X/6X (max.) CDRW/DVD-ROM drive (max. 24X when CD-ROM is accessed)	Hot swappable 8X (max.) DVD-ROM drive (max. 24X when CD-ROM is accessed)	Hot swappable 8X/8X/6X (max.) CDRW/DVD-ROM drive (max. 24X when CD-ROM is accessed)
Diskette Drive	External USB 3.5", 1.44MB diskette drive	Optional External USB 3.5", 1.44MB diskette drive	Optional External USB 3.5", 1.44MB diskette drive
Display	14.1" TFT active matrix 16.7 million colors at 1,024 x 768 resolution		
External video modes	Max. 16.7M colors at 640 x 480 resolution, 800 x 600 resolution, 1,024 x 768 resolution Max. 64K colors at 1,280 x 1,024 resolution, 1,600 x 1,200 resolution		
Graphics Controller	S3 SuperSavage™ IXC-106, 128-bit 2D/3D graphics accelerator, 4x AGP Bus, 16MB Video Memory		
Integrated Communication Device	International V.90 software modem (56Kbps data, 14.4Kbps fax) and 10/100Mbps Ethernet (Wake-On-LAN and Remote Boot supported) Built-in antenna for Wi-Fi™ 802.11b Wireless LAN (with optional Wireless LAN Card Kit ¹) and Bluetooth™ (with optional Bluetooth™ Module Kit ¹) connectivity		
Keyboard	85-key Ergonomic Keyboard, AccuPoint II integrated pointing device with Scroll buttons, Windows® Key, Application Key and hot key functions, Toshiba Console button		
PC Card slots	Type III x 1 or Type II x 2 (Card Bus supported)		
Expansion Ports	Serial (16550UART), Parallel (ECP), RGB, USB x 2, PS/2 Keyboard/Mouse, Fast Infrared Port (4Mbps), i.LINK (IEEE 1394), SD Media slot, External Microphone, Headphone (stereo), NTSC/PAL TV-Out, RJ-11, RJ-45, Expansion Bus, DC-in		
Sound	Yamaha YMF753, 16-bit stereo SoundBlaster Pro and Windows Sound System compatible, 3D Sound supported, built-in stereo speakers, volume dial, internal Microphone (monaural)		
Power Supply	Universal 100-240V AC adaptor for worldwide usage		
Battery Type/Life ⁵	Exchangeable Lithium-Ion battery, up to 2.3H of battery life, up to 4.4H with optional 2 nd battery, up to 5.3H with optional 2 nd battery in SuperLongLife mode		
Security	Cable Lock port, Power on Password, Supervisor Password, Keyboard Lock, Screen Blank		
System Management	Toshiba Hibernation and Resume, SM BIOS V2.3, ACPI power management		
Pre-installed OS	Microsoft® Windows® XP Professional operating system		
Bundled software & CD	Toshiba Utilities, Microsoft® Internet Explorer, Microsoft® Media Player, InterVideo™ WinDVD, SPANworks2000 software suite, Toshiba Configuration Builder CD, Toshiba Management Console (available in Toshiba Configuration Builder CD)		
Dimensions (W x D x H) ⁶	310 x 269 x 32.2 / 37.5 mm (Front / Back)		
Weight ⁷	2.2kg (w/ battery pack and weight saver) 2.4kg (w/ battery pack and CD-RW/DVD-ROM drive)		
Warranty	3-year parts & labor, 1-year battery international limited warranty		
Options	PA3126U-1M12 PC2100 128MB Memory Kit PA3127U-1M25 PC2100 256MB Memory Kit PA3164U-1M51 PC2100 512MB Memory Kit ³ PA3178U-1BA5 Lithium-Ion Rechargeable Battery Pack PA3189U-1BA5 Slim SelectBay 2 nd Battery Pack PA3116U-1H30 2.5" Enhanced IDE 30GB 2 nd HDD Kit ⁴ PA3133U-1H40 2.5" Enhanced IDE 40GB (5,400rpm) 2 nd HDD Kit ⁴ PA3204U-1H60 2.5" Enhanced IDE 60GB (5,400rpm) 2 nd HDD Kit ⁴ PA3090U-1ETC Slim SelectBay HDD Adaptor PA3087U-1D0V Slim SelectBay 8X DVD-ROM Drive Kit PA3088U-3CD1 Slim SelectBay 8X/8X/24X CD-R/RW Drive Kit PA3162U-1CD2 Slim SelectBay 8X/8X/24X CDRW/DVD-ROM Drive Kit PA3083U-1ACA 75W Universal AC Adaptor PA3082U-1PRP Advanced Port Replicator PA3109U-1FDD USB FDD Kit PA3189U-1MPC Wireless LAN Card Kit ¹ PA3121U-3BTM Bluetooth™ Module Kit ¹ PA3068U-1PCG Toshiba PC Card Fingerprint Reader PA3079T-1PCG Toshiba 2GB Type II PC Card HDD		

¹ Applicable to countries where official Type Approval is obtained.
² CPU performance in your computer product may vary from specifications under some conditions. Please visit pc.toshiba-asia.com/support/cpunfo for more detailed information.
³ 1024MB is achieved by removing the standard 256MB Memory Kit and inserting the optional 512MB Memory Kits (2 memory slots are available).
⁴ The optional Slim SelectBay HDD Adaptor is necessary for installing the optional 2nd HDD Kit into the Select Bay.
⁵ Battery life may vary depending on applications, power management settings and features utilized. Recharge time varies depending on usage. Battery may not charge while computer is consuming full power.
⁶ After a period of time, the battery will lose its ability to perform at maximum capacity and will need to be replaced. This is normal for all batteries.
⁷ Thickness may vary at certain points on the system.
⁸ Weight may vary depending on SelectBay components.
 HDD calculation: 1GB means 1 billion bytes.

Please note that thin-film transistor (TFT) liquid crystal display (LCD) is made with high-precision technology. However, black or bright dots of light (red, blue or green) may appear on the LCD screen, and we call these dots non-conforming pixels. This is a technology limitation of TFT LCD and does not represent a defect. Toshiba warranty does not cover limitations of technology such as non-conforming pixels.

TSP December 2002, TSP-M02-P010330. The Intel Inside Logo and Pentium are registered trademarks of Intel Corporation. Microsoft, Windows and the Microsoft logo are trademarks or registered trademarks of Microsoft Corporation. Bluetooth is a trademark owned by Intel Corporation, L. Ericsson, Sweden and licensed to Toshiba Corporation. All other products and names mentioned are the property of their respective owners. Design and specifications are subject to change without notice. Availability and configurations may vary by country. Errors and omissions excepted.



The Standard for Wireless Fidelity.



Choose freedom.

pc.toshiba-asia.com

TOSHIBA