Intrusion Prevention System Command Line Tools Reference

P/N 9034427-03

July 2014

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 19534
Tel: +1 408-579-2800

Toll-free: +1 888-257-3000

Software License Agreement
Enterasys ("Dragon") Intrusion Prevention System

This document is an agreement ("Agreement") between You, the end user, and Enterasys Networks, Inc., ("Enterasys") a wholly owned subsidiary of Extreme Networks, Inc., on behalf of itself and its Affiliates (as hereinafter defined) that sets forth your rights and obligations with respect to the Licensed Software. BY INSTALLING THE LICENSE KEY (IF APPLICABLE) FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO ENTERASYS OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT ENTERASYS OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS, Attn: LegalTeam@extremenetworks.com.

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Intrusion Detection System Software" shall refer to the application(s) authorized and licensed for use on the Network Sensor Appliances as authorized herein and as further defined within the product documentation. "Enterprise Management Software" shall refer to the software installed on one or more of Your Servers as authorized below that is used to manage IPS and IDS software and related Host Sensor Software. "Host Sensor Software" shall refer to the application software installed on Your servers and/or Network Sensor Appliances to monitor critical resources and detect potential compromises. "Server", for purposes of this license, shall mean a physical computer device or appliance, or virtual appliance as further described within the product documentation. "Licensed Materials" shall collectively refer to the licensed software (including the software included within IPS, IDS, the Host Sensor and Enterprise Management Software), Firmware, media embodying the software, and the documentation. "Firmware" refers to any software program or code embedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.

2. TERM. This Agreement is effective from the date on which You install the License Key or use the Licensed Software. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.

3. GRANT OF SOFTWARE LICENSE. Enterasys will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type and authorized entitlements purchased are specified on the invoice issued to You by Enterasys or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4. LICENSE TYPES.

- *Intrusion Prevention System ("IPS") Network Sensor Software.* Under the terms of the IPS license, the license granted to You by Enterasys when You install the License Key authorizes You to use the identified Licensed Software on any one, single Server, or any replacement for that Server, for internal use only, in a quantity of throughput as identified within the relevant invoice issued to you and corresponding to your quoted usage / size entitlements. Any additional authorization to use the IPS Software beyond the terms and conditions herein must be provided by Enterasys in writing.
- *Intrusion Detection System ("IDS").* Under the terms of the IDS license, the license granted to You by Enterasys when You install the License Key authorizes You to use the identified Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only, in a quantity as identified within the relevant invoice issued to you and corresponding to your quoted usage / size entitlements. Any additional authorization to use the IDS Software beyond the terms and conditions herein must be provided by Enterasys in writing.
- *Host Sensor Software License Terms.* Under the terms of the Host Sensor Software license, the license granted to You by Enterasys when You install the License Key authorizes You to use the identified Licensed Software on any one, single computer only, or any replacement for that computer, in connection with the overall management of systems by an authorized use of an Enterprise Management Software instance, in a quantity as identified within the relevant invoice issued to you and corresponding to your quoted license pack amounts. Any additional authorization to use the Host Sensor Software beyond the terms and conditions herein must be provided by Enterasys in writing.
- *Enterprise Management Software*. Under the terms of the Enterprise Management Software license, the license granted to You by Enterasys will authorize You to install the License Key for the Licensed Software on your authorized Server for management of the specific number of Nodes and/or per your defined Enterprise Size as shown on the relevant invoice issued to You for each Node and/or Enterprise Size that You order from Enterasys or Your dealer, if any, to access the application software. A separate license is required for each additional instance of Enterprise Management Software. Any additional authorization to use the Enterprise Management Software beyond the terms and conditions herein must be provided by Enterasys in writing.

5. AUDIT RIGHTS. You agree that Enterasys may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Enterasys for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for unlicensed usage over and above

those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to Enterasys. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Enterasys employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Enterasys' prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7. TITLE AND PROPRIETARY RIGHTS

(a) The Licensed Materials are copyrighted works and are the sole and exclusive property of Enterasys, any company or a division thereof which Enterasys controls or is controlled by, or which may result from the merger or consolidation with Enterasys (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

(b) You further acknowledge that in the event of a breach of this Agreement, Enterasys shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Enterasys shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Enterasys.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Enterasys relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Enterasys' exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Enterasys' prior written approval, and shall return such information and data to Enterasys at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Enterasys or of information which has been or subsequently is made public by Enterasys, or a third party having authority to do so.

You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Enterasys or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Enterasys. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Enterasys of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Enterasys or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Enterasys Service and Maintenance Agreement, if Enterasys and You enter into such an agreement. Except as specifically set forth in such agreement, Enterasys shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Enterasys, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Enterasys may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Enterasys and You.

(a) Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Enterasys the original and any copies of the Licensed Materials, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Enterasys.

(b) Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.

11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that

has jurisdiction over such export, import, transmission or Use.

12. ~~UNITED STATES GOVERNMENT RESTRICTED RIGHTS~~. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13. ~~LIMITED WARRANTY AND LIMITATION OF LIABILITY~~. The only warranty Enterasys makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Enterasys in good faith determines that the media and proof of payment of the license fee are returned to Enterasys or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.

NEITHER ENTERASYS NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL ENTERASYS OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF ENTERASYS OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL ENTERASYS OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. ~~JURISDICTION~~. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15. ~~GENERAL~~.

(a) This Agreement is the entire agreement between Enterasys and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.

(b) This Agreement may not be changed or amended except in writing signed by both parties hereto.

(c) You represent that You have full right and/or authorization to enter into this Agreement.

(d) This Agreement shall not be assignable by You without the express written consent of Enterasys. The rights of Enterasys and Your obligations under this Agreement shall inure to the benefit of Enterasys' assignees, licensors, and licensees.

(e) Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

(f) The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.

(g) Enterasys' waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

(h) Should You have any questions regarding this Agreement, You may contact Enterasys at the address set forth below. Any notice or other communication to be sent to Enterasys must be mailed by certified mail to the following address:

Extreme Networks, Inc.,
145 Rio Robles.
San Jose, CA 95134 United States.
ATTN: General Counsel

Contents

About This Guide

The Extreme Networks Intrusion Prevention System (IPS) is a solution consisting of an Intrusion Detection System (IDS), active response, and intrusion prevention. Extreme Networks IPS administrators can configure a variety of IPS elements. Administrators are responsible for configuring Network Sensors, Host Sensors, and the management tools of the Enterprise Management Server (EMS). Depending on your administrative role, you have access to the root of the operating system, XML, and/or the GUI configuration methods. It is recommended that all configuration available through the GUI be performed using the GUI. XML configuration is described in the latter chapters of the book. You may be responsible for placement of Extreme Networks IPS components within your network and for the systems with which Extreme Networks IPS communicates to execute alerts.

This document describes the forensics command line tools you can use to analyze a single dragon.db file or the dragonevents database. You can also use the IPS GUI to analyze events.

Intended Audience

This document is intended for experienced network administrators who are responsible for implementing and maintaining an Intrusion Defense System.

Related Documents

For related IPS manuals, visit:

www.extremenetworks.com/support/enterasys-support/

Conventions

The following conventions are used in this document.

bold type	Actual user input values or names of screens and commands.
blue type	Indicates a hypertext link. When reading this document online, click the text in blue to go to the referenced figure, table, or section.
italic type	User input value required.
`courier`	Used for command-level input or output.

Getting Help

For additional support, contact Extreme Networks using one of the following methods:

Website	www.extremenetworks.com/support/
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 To find the Extreme Networks Support toll-free number in your country: www.extremenetworks.com/support/enterasys-support/contact/
Email	support@enterasys.com

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches, and rebooting the unit.)
- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (for example, layout, and cable type)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, have you returned the device before, is this a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

1

Forensics Command Line Tools

This chapter describes the command line tools you can use to analyze a single dragon.db file.

Overview

Dragon Database Agent

The Dragon Database agent reads events from Network Sensors and Host Sensors and records the events, along with any packets associated with that event, to a local Dragon database. This Dragon database is used by the Reporting tools and forensics command line tools for event reporting.

The Dragon DB Agent should be installed and activated on any Sensor/EFP (Linux only) device node that is expected to provide any reporting functionality.

Dragon DB Log Format

The Dragon DB agent writes to the directory */installdir*/**dragon/DB**, which contains subdirectories named for the date a log was collected. In each subdirectory, there is a single file named **dragon.db** that contains all of the events that occurred on that day. For example, a Network Sensor would have its DB directory in */usr/dragon/DB*, which contains subdirectories, named *2014May12*, *2014May13*, and *2014May14*. The dragon.db files contain packets, sessions, Network Sensor information such as port scan data, Host Sensor information such as modified MD5 file information, SYSLOG file excerpts and diagnostic and performance information.

Using the Command Line Tools

The command line tools are designed to operate on a single dragon.db file or on the dragonevents database. Typically, you will change directory to the location of a particular dragon.db file and execute the desired command. Each of these tools opens up the dragon.db file and processes it until the entire file has been read. The dragon.db files can be moved from system to system for more in-depth analysis.

Note: You must run the command line tools from the <installdir>/tools directory. If you call the tools from a script, change the working directory to the <installdir>/tools directory within the script.

Command Line Tools

sum_db — Summarize dragon.db File Information

During a user session, it is trivial to conduct a listing of files to determine file size of dragon.db files. However, there is other information, such as the total number of events seen, that are hard to determine. The **sum_db** tool summarizes this information. The tool also lists the active Network Sensor names found in each dragon.db file, as shown in the Example section below.

Options

-f <*filename*> **--file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
-B *YYYY-MM-DD* **--database** *YYYY-MM-DD*	Specifies to search the dragonevents database for the specified date. Enter the date in YYYY-MM-DD format.
-u **--help** **-?**	Prints out the usage information.
-v **--version**	Prints out version information.

Example

This example shows the output from running the **sum_db** command on the dragon.db file located in **/usr/dragon/DB/2014May06**.

```
root@dragon:/usr/dragon/tools# ./sum_db -f ../DB/2014May06/dragon.db

** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Summarize Database Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Using file ../DB/2010May10/dragon.db as the 'dragon.db' file

Date of file:  Monday May 10, 2014
```

```
Sensor Name ..... devtest20
Internal Events ..... 87
External Events ..... 0
Inbound Events ..... 0
Outbound Events ..... 0
Total Bytes ..... 5220

Sensor Name ..... devtest20-HIDS
Internal Events ..... 101
External Events ..... 0
Inbound Events ..... 0
Outbound Events ..... 0
Total Bytes ..... 6461

Sensor Name ..... devtest20-VS1
Internal Events ..... 95
External Events ..... 0
Inbound Events ..... 0
Outbound Events ..... 0
Total Bytes ..... 18492

Sensor Name ..... jpk-desktop
Internal Events ..... 86
External Events ..... 0
Inbound Events ..... 0
Outbound Events ..... 0
Total Bytes ..... 5332

Total Events ..... 369
First Event Time  ..... 11:59
Last Event Time ..... 13:34
```

sum_event — Summarize dragon.db Events

The **sum_event** program summarizes all of the events in the dragon.db file and prints the results to standard out. This is a very useful tool, because all of the event types for a particular day can be viewed in one report. Suspicious activity can stand out in a report like this and allow an IPS administrator to quickly focus on unusual events.

The number of each distinct event is listed. By default, sum_event also prints out extra information about each event. This information includes the time and IP addresses of the first and last events. The sum_event tool also prints out a 24-hour bar chart for each unique event. An event's activity over a 24-hour period can be easily assessed, as shown in the Example section.

Options

-**a** *H*[*H:MM:SS*] --**after** *H*[*H:MM:SS*]	Specifies to use events that have occurred after a certain time. Times are in 24-hour military time. All events that occur prior to the times specified here will be ignored. Use of this option with the -b option can specify a specific window of time. For -**a**, times are specified in HH:MM:SS format. Padding is not required for single digit times. For example, to only see events after nine o'clock you can enter -a 9 or -a 09:00.
-**b** *H*[*H:MM:SS*] --**before** *H*[*H:MM:SS*]	This option has exactly the same format as -**a**, except it specifies to use events that have occurred before a certain time. When used together, a time window can be specified. For example, to find all events that have occurred between 7:00 AM and 1:00 PM, the arguments -a 07:00 -b 13:00 would be used.
-B *YYYY-MM-DD* **--database *YYYY-MM-DD***	Specifies to search the dragonevents database for events occurring on the specified date.
-**d** {**0** |**1**	**2**	**3** --**direction** {**0** |**1**	**2**	**3**}	Filters all events that are not of this direction. When Extreme IPS is configured, it requires the definition of a protected network. All packets can then be labeled as to their relative direction. A value of **0** defines packets that are exterior to the protected networks. That is, both their destination and source addresses are not in the protected list. A value of **1** indicates that the packet is from a protected network. A value of **2** indicates that the packet is going to a protected network. A value of **3** indicates that the packet is from and going to a protected network.
-**D** {**0** |**1**	**2**	**3**} **--direction-info** {**0** |**1**	**2**	**3**}	Prints out an event group summary for each direction (From (1), To (2), Internal (3), and External (0)).
-**f** <*filename*> **--file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
-**F** **--from**	Only apply the -i and -I options if the event is *from* the specific IP address. For example, arguments of -F -I 10.100.100.10 only prints out events that are *not from* 10.100.100.10. Without the -F option, all events not from and not to 10.100.100.10 would be processed.
-**g** **--group-only**	Organize the output by event group as specified in the dragon.conf file.
-**G** <*filename*> **--group-file** <*filename*>	Specify a dragon.conf file to use for event group data.
-**h** **--disable-headers**	With this option, table headers are suppressed which can be useful for post processing scripts.
-**i** <*IP address*> **--ip** <*IP address*>	Only summarize event data to or from this IP address or CIDR block.
-**I** <*IP address*> **--exclude-ip** <*IP address*>	Only summarize event data that is not to or from this IP address or CIDR block.
-**n** **--no-extra**	Do not print any extra data about events. Specifically, this option suppresses the first and last event information.
-**N** **--number-sort**	Organize events based on the number of times an event has occurred instead of the order that they occurred.

-p --no-pretty	Do not pretty print any IPv6 addresses.
-**r** **--report**	Output a report format which is a convenient combination of data for each event (used by Extreme IPS Reporting).
-**s** <*sensor name*> --**sensor** <*sensor name*>	Only process events from this Network Sensor.
-**T** **--to**	Only apply the -i and -I options if the event is *to* the specific IP address. This option is exactly opposite of the -F option and only applies if the -i or -I options are used.
-**u** **-?** --help	Prints usage information.
-**v** **--version**	Prints out version information.

Example

This example shows partial output from running the sum_event command on the dragon.db file located in **/usr/dragon/DB/2014May10**.

Note that the following example has been modified to fit into the page. Your display will be wider. When IPv6 addresses are displayed, they will be displayed on two lines. For example:

```
====================
FIRST
SOURCE IP
====================
FDE0:6477:1E3F:0000
:0000:0000:0001:001E


root@dragon238:/usr/dragon/tools# ./sum_event -f ../DB/2014May10/dragon.db

** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Summarize Events Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Using ../DB/2010May10/dragon.db as a dragon.db file
** Using file dragon.conf as the 'dragon.conf' file
```

```
=============================================================================================================================
EVENT                          FIRST    FIRST            FIRST            LAST      LAST            LAST
NAME                         COUNT TIME     SOURCE IP        DEST IP          TIME      SOURCE IP       DEST IP
=============================================================================================================================
[ATSNMP:PUBLIC]               3373 00:03:30  134.141.93.36  => 134.141.97.231   23:55:07  134.141.90.207 => 134.141.94.176
[PC:ATSNMP:PUBLIC]            3373 00:03:30  134.141.93.36  => 134.141.97.231   23:55:07  134.141.90.207 => 134.141.94.176
[SNMP:PUBLIC]                 3373 00:03:30  134.141.93.36  => 134.141.97.231   23:55:07  134.141.90.207 => 134.141.94.176
[AXTESTS]                      224 16:33:45  134.141.103.8  => 134.141.90.110   23:54:22  134.141.103.8  => 134.141.90.110
[XTESTSATTACK2]                 15 16:50:42  134.141.103.8  => 134.141.90.110   23:50:41  134.141.103.8  => 134.141.90.110
[HEARTBEAT]                     50 00:00:00  0.0.0.0        => 0.0.0.0          23:28:32  134.141.90.110 => 134.141.90.110
[ICMP:L3-RETRIEVER]            160 00:31:58  134.141.93.57  => 134.141.94.168   20:03:01  134.141.93.21  => 134.141.90.52
```

```
[SSH:VERSION-1]              6 16:28:32  134.141.98.251  => 134.141.90.110    16:30:22  134.141.98.251  => 134.141.90.110
[HOST:LINUX:PROMISC]         4 10:34:32  134.141.90.110  => 134.141.90.110    16:25:32  134.141.90.110  => 134.141.90.110
[HOST:LINUX:PROMISC-LEFT]    4 10:34:32  134.141.90.110  => 134.141.90.110    16:25:32  134.141.90.110  => 134.141.90.110
```

sum_ip — Summarize IP Address Information

The sum_ip program summarizes all of the different IP addresses found in the dragon.db file or the dragonevents database, for a maximum of 120,000 different IP addresses. It tracks the number of events each IP address was involved in as well as its first and last event timestamp. The options for this command are similar to the sum_event options.

Options

-a *H*[*H:MM:SS*] **--after** *H*[*H:MM:SS*]	Specifies to use events that have occurred after a certain time. Times are in 24-hour military time. All events that occur prior to the times specified here will be ignored. Use of this option with the -b option can specify a specific window of time. For -**a**, times are specified in HH:MM:SS format. Padding is not required for single digit times. For example, to only see events after nine o'clock you can enter -a 9 or -a 09:00.
-b *H*[*H:MM:SS*] **--before** *H*[*H:MM:SS*]	This option has exactly the same format as -**a**, except it specifies to use events that have occurred before a certain time. When used together, a time window can be specified. For example, to find all events that have occurred between 7:00 AM and 1:00 PM, the arguments -a 07:00 -b 13:00 would be used.
-B *YYYY-MM-DD* **--database** *YYYY-MM-DD*	Specifies to search the dragonevents database for events occurring on the specified date.
-**C** **--cidr-sort**	Prints out the list of valid IP addresses by Class C CIDR block instead of unique IP addresses.
-**d** {**0** |**1** | **2** | **3** --**direction** {**0** |**1** | **2** | **3**}	Only summarize data with DIRECTION equal to: A value of **0** defines packets that are exterior to the protected networks. That is, both their destination and source addresses are not in the protected list. A value of **1** indicates that the packet is from a protected network. A value of **2** indicates that the packet is going to a protected network. A value of **3** indicates that the packet is from and going to a protected network.
-**D** **--dns-resolve**	Resolve any DNS names.
-**e** <*event name*> **--event** <*event name*>	Only filters for events of this type. Only events of this type will be processed. If desired, only the first few characters need to be matched for a positive match. For example, using an argument of -e WEB will match any event that starts with WEB.
-**E** <*event name*> **--exclude-event** <*event name*>	Don't print events of this type. Opposite of the -e option. Both -e and -E can be used simultaneously, and the longer event is dominant. For example, arguments of -e WEB -E WEB:CGI will print all events that start with WEB, but none that start with WEB:CGI.
-**f** <*filename*> **--file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
-**F** **--from**	Only apply the -i and -I options if the event is *from* the specific IP address. For example, arguments of -F -I 10.100.100.10 only prints out events that are not from 10.100.100.10. Without the -F option, all events not from and not to 10.100.100.10 would be processed.

-**h** **--disable-headers**	With this option, table headers are suppressed which can be useful for post processing scripts.
-**i** <*IP address*> **--ip** <*IP address*>	Summarize event data to or from this IP address or CIDR block only.
-**I** <*IP address*> **--exclude-ip** <*IP address*>	Summarize event data that is NOT to or from this IP address or CIDR block.
-**n** **--no-extra**	Do not print any extra data about events. Specifically, this option suppresses the first and last event information.
-p --no-pretty	Do not pretty print any IPv6 addresses.
-**s** <*sensor name*> **--sensor** <*sensor name*>	Only process events from this Network Sensor.
-**t** <*seconds*> **--dns-timeout** <*seconds*>	Do not wait longer than this value in seconds to resolve DNS. On some architectures, such as Linux, this feature does not work. Typically though, any DNS resolution time-out longer than specified will be skipped. This can be handy when resolving several hundred IP addresses. For example, arguments of -t 3 would cause this tool to drop any DNS resolutions that take longer than 3 seconds.
-**T** **--to**	Only apply the -i and -I options if the event is *to* the specific IP address. This option is exactly opposite of the -F option and only applies if the -i or -I options are used.
-**u** **-?** --help	Prints usage information.
-**v** **--version**	Prints out version information.

Example

This example shows partial output from running the sum_ip command on the dragon.db file located in **/usr/dragon/DB/2014May10** and using the -D option to suppress DNS name resolution.

Note that IPv6 addresses are displayed over two lines.

```
root@dragon:/opt/dragon/tools# ./sum_ip -D -f ../DB/2014May10/dragon.db

** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Summarize IPs Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Using ../DB/2014May10/dragon.db as a dragon.db file
================================================
ADDRESS                COUNT   START    FINISH
================================================
0.0.0.0                 5542 00:00:29 23:59:54
```

```
10.10.70.110              2 09:04:36 09:04:38
134.141.103.8          7052 00:02:41 23:33:48
134.141.104.82            8 15:31:52 22:13:50
134.141.104.83           65 00:30:52 20:33:51
134.141.224.25            5 12:21:03 12:21:14
134.141.98.96            22 01:30:50 22:30:50
134.141.98.97            22 01:30:50 22:30:50
134.141.99.30           205 00:09:04 23:59:08
169.254.229.108           1 08:35:18 08:35:18
224.0.0.252              15 12:45:21 15:47:54
239.255.255.250         123 01:03:37 23:20:41
FE80:0000:0000:0000       2 09:32:33 09:32:36
:1C3C:54A6:73BA:9674
FE80:0000:0000:0000       5 07:10:42 07:11:08
:3C3B:CCCF:27A0:6DEA
FE80:0000:0000:0000     208 07:44:11 16:55:28
:5068:2FD5:7457:23D2
FE80:0000:0000:0000       6 08:01:31 08:02:03
:79A8:EE6D:4586:F966
FE80:0000:0000:0000      18 08:53:07 19:08:38
:A41A:6A48:0F0D:C549
FE80:0000:0000:0000       7 08:35:18 15:28:05
:A4B2:3A01:45A7:E56C
FE80:0000:0000:0000       9 07:45:53 09:22:39
:B1E8:0D7D:E7EE:06D0
FE80:0000:0000:0000      15 13:28:17 14:49:33
:CCDB:2AFB:09FC:EACD
FE80:0000:0000:0000       6 07:29:48 14:15:52
:E0F7:2403:7B37:E5F2
FE80:0000:0000:0000       9 14:11:32 14:49:48
:EC1F:93E9:00E3:E698
FE80:0000:0000:0000     212 08:27:35 18:20:48
:F0EE:633D:F632:7882
FE80:0000:0000:0000       7 07:34:16 14:13:57
:F9F0:F56E:973A:387C
FE80:0000:0000:0000       4 08:01:17 10:41:51
:FC7A:0852:3B97:E870
FF02:0000:0000:0000     508 07:10:42 19:08:38
:0000:0000:0000:000C
```

mkalarm — Score All Events for Each IP Address

The **mkalarm** tool simply takes each IP address and accumulates a weighted score of events. Each event belongs to a specific group within the **dragon.conf** file. Each group has a specific score file. These scores are relative to each other. The **mkalarm** tool adds up all of the score values for each

event into an IP address's running total. When **mkalarm** concludes analyzing the dragon.db file, it displays the IP addresses with the highest scores as shown in the examples below. These scores are completely relative and can be modified by the end user. When the totals are printed out, a list of events and occurrences by event group is also included.

The **mkalarm** program is highly optimized for speed, but as a hard limit, can only analyze the first 750,000 unique IP addresses. If this is not sufficient, we recommend use of the -C option that specifies a CIDR block for analysis. The -C option also greatly increases mkalarm's speed for large dragon.db files.

The **mkalarm** tool includes a -m option. This option finds events that occur in specific Class C CIDR blocks more than a specific amount of time. For example, the command, mkalarm -m 5, would list each event per Class C CIDR block that occurred on 5 or more unique IP addresses in that CIDR block. This process is highly iterative and can take 2-3 minutes in some cases.

Note: This command does not support IPv6 addresses.

Options

-**a** *H*[*H:MM:SS*] **--after** *H*[*H:MM:SS*]	Specifies to use events that have occurred after a certain time. Times are in 24-hour military time. All events that occur prior to the times specified here will be ignored. Use of this option with the -b option can specify a specific window of time. Times are specified in HH:MM:SS format. Padding is not required for single digit times. For example, to only see events after nine o'clock you can enter -a 9 or -a 09:00.
-**b** *H*[*H:MM:SS*] **--before** *H*[*H:MM:SS*]	This option has exactly the same format as -**a**, except it specifies to use events that have occurred before a certain time. When used together, a time window can be specified. For example, to find all events that have occurred between 7:00 AM and 1:00 PM, the arguments -a 07:00 -b 13:00 would be used.
-B *YYYY-MM-DD* **--database** *YYYY-MM-DD*	Specifies to search the dragonevents database for events occurring on the specified date.
-**C** *x.x.x.x*[*/m*] **-i** *x.x.x.x*[*/m*] **--ip***x.x.x.x*[*/m*]	Print all data to or from this IP address. Any type of CIDR block with the x.x.x.x/m format may optionally be specified. For example, 10.0.0.0/8, 10.10.10.2/8, 10.10.10.2, and 208.192.100.0/24 would all be valid entries. If a mask is specified, only IP addresses to or from the specified CIDR block will be considered.
-**D** **--dns-resolve**	Resolve any DNS names.
-**d** {**0** |**1**	**2**	**3**} **--direction** {**0** |**1**	**2**	**3**}	Process data that is the specified direction. A value of **0** defines packets that are exterior to the protected networks. That is, both their destination and source addresses are not in the protected list. A value of **1** indicates that the packet is from a protected network. A value of **2** indicates that the packet is going to a protected network. A value of **3** indicates that the packet is from and going to a protected network.
-**f** <*filename*> --**file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.

-**F** **--from**	Only apply the -i and -I options if the event is *from* the specific IP address. For example, arguments of -F -I 10.100.100.10 only prints out events that are not from 10.100.100.10. Without the -F option, all events not from and not to 10.100.100.10 would be processed.
-**I** <*IP address*> **--exclude-ip** <*IP address*>	Only process event data that is **not** to or from this IP address or CIDR block.
-**m** *num* **--mult** *num*	Specifies the threshold of unique events to search for in each active Class C CIDR block. For example, -m 5 would list each event per Class C CIDR block that occurred on 5 or more unique IP addresses in that CIDR block.
-r <*path/to/dragon.conf*> **--conf** <*path/to/dragon.conf*>	Specifies the path to the dragon.conf file.
-**s** <*sensor name*> -**-sensor** <*sensor name*>	Only process events from this Network Sensor.
-t *sec* **--dns-timeout** *sec*	Timeout in seconds when resolving DNS.
-**T** **--to**	Only apply the -i and -I options if the event is *to* the specific IP address. This option is exactly opposite of the -F option and only applies if the -i or -I options are used.
-**u** **-?** **--help**	Prints usage information.
-**v** **--version**	Prints out version information.

Examples

This example displays the IP addresses with the highest weighted score of events. Only a portion of the output is shown here.

```
root@dragon:/usr/dragon/tools# ./mkalarm -f ../DB/2014Apr29/dragon.db -r
dragon.conf


** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Make Alarm Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Using file dragon.conf as the 'dragon.conf' file
--------------------------------------------------------------------------------
172.26.2.50     130635
PROBE:          [SNMP:PUBLIC]x2903
UNKNOWN:        [ATSNMP:PUBLIC]x2903 [PC:ATSNMP:PUBLIC]x2903


--------------------------------------------------------------------------------
134.141.93.36   14130
PROBE:          [ICMP:L3-RETRIEVER]x9 [SNMP:PUBLIC]x305
UNKNOWN:        [ATSNMP:PUBLIC]x305 [PC:ATSNMP:PUBLIC]x305
```

```
--------------------------------------------------------------------------------
10.20.80.20     12740
ATTACKS:        [IIS:CMD.EXE]x5 [IIS:CODE-RED-II-ROOT.EXE]x2 [IIS:DECODE-BUG]x1
                [IIS:NIMDA-WORM]x2 [IIS:NIMDA.E-WORM]x2 [IIS:UNC-SOURCE-LIST]x1
                [LOTUS:DIR-TRAVERSAL]x3 [WEB:4D-TRAVERSAL-DRIVE]x1
                [WEB:CAT-ATTEMPT]x37 [WEB:CGI-DOT-DOT]x31 [WEB:ETCPASSWD]x1
                [WEB:HTACCESS]x1 [WEB:MAIL-ATTEMPT]x1 [WEB:NETSCAPE-WP]x1
                [WEB:NOVELL-CODE]x1 [WEB:NSIISLOG-OVERFLOW]x1
                [WEB:NULL-BYTE3]x1 [WEB:TRENDMICRO-FILE-DOWNLOAD]x2
PROBE:          [FRONTPAGE:DVWSSR.DLL]x1 [IIS:BOOT.INI]x37 [IIS:CODEBRWS]x2
                [IIS:COLD-FUSION]x1 [IIS:COLD-FUSION2]x1 [IIS:NEWDSN]x1
                [TCP-FLAGS]x28 [WEB:ANYFORM]x2 [WEB:APACHE-ASP]x1
                [WEB:CGI-AGLIMPSE]x1 [WEB:CGI-BBOARD]x1 [WEB:CGI-BIGBROTHER]x1
                [WEB:CGI-BIZDB]x1 [WEB:CGI-CAMPAS]x1 [WEB:CGI-FAXSURVEY]x1
                [WEB:CGI-HTMLSCRIPT]x1 [WEB:CGI-JJ]x1 [WEB:CGI-NPH]x1
                [WEB:CGI-PERL]x2 [WEB:CGI-PHF]x1 [WEB:CGI-PHP]x3
                [WEB:CGI-SAMBAR]x1 [WEB:CGI-SENDMAIL]x1 [WEB:CGI-TEST]x1
                [WEB:CGI-VIEWSOURCE]x1 [WEB:CGI-WEBGAIS]x1 [WEB:CGI-WEBSITE]x1
                [WEB:CGI-WWW-SQL]x1 [WEB:FINGER]x1 [WEB:FORMMAIL]x2
                [WEB:GUESTBOOK]x2 [WEB:INDEX-ROOT]x1 [WEB:JAVA-SHOWCODE]x1
                [WEB:JRUN-ACL-BYPASS]x1 [WEB:PIRANHA-PASSWD]x1
                [WEB:SGI-HANDLER]x1 [WEB:SGI-INFOSRCH]x1 [WEB:SGI-PFDISPALY]x2
                [WEB:SGI-WEBDIST]x1 [WEB:SGI-WRAP]x3 [WEB:SHELL]x1
                [WEB:SHELL-ZSH]x1 [WEB:SHELL2]x1 [WEB:SHELL3]x1 [WEB:SHELL4]x1
                [WEB:SHELL5]x1 [WEB:SHELL6]x1 [WEBSITE-PRO:ARGS]x1
                [WEBSITE-PRO:UPLOAD]x1
UNKNOWN:        [ATTACKS:XTESTSATTACK]x9
VULNERABILITY:  [CISCO:CMD-EXEC]x1
```

This example shows the mkalarm session using –m CIDR block searching for any unique event which occurred more than 3 times in a unique CIDR block.

```
root@dragon:/usr/dragon/tools# ./mkalarm -f ../DB/2014Apr29/dragon.db -r
dragon.conf -m 3

** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Make Alarm Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Using file dragon.conf as the 'dragon.conf' file
--------------------------------------------------------------------------------
134.141.90.0/24
[ATTACKS:XTESTSATTACK]          3 unique IP addresses
```

```
                                110 120 166
[DYNAMIC-UDP]                   4 unique IP addresses
                                110 120 200 207
[ICMP:L3-RETRIEVER]             11 unique IP addresses
                                34 52 90 91 115 126 170 193 239 244 251
-------------------------------------------------------------------------------
134.141.93.0/24
[ICMP:L3-RETRIEVER]             3 unique IP addresses
                                21 36 57
-------------------------------------------------------------------------------
134.141.94.0/24
[ICMP:L3-RETRIEVER]             7 unique IP addresses
                                129 141 159 160 167 168 170
-------------------------------------------------------------------------------
134.141.97.0/24
[DYNAMIC-UDP]                   3 unique IP addresses
                                76 231 237
[ICMP:L3-RETRIEVER]             4 unique IP addresses
                                30 98 100 215
-------------------------------------------------------------------------------
```

mklog — Make a Log Report

This program processes a list of events from a dragon.db file or the dragonevents database. It is designed to efficiently list event information, display raw event data, and decode packet event protocol information. For dragon.db files, this tool is used to list unique sets of events, or actually displays the contents of the event's record in the dragon.db file.

For packet analysis, the **mklog** tool displays the raw data in hex codes 20 bytes wide. A twenty-character column of corresponding printable ASCII characters follows this field. Non-printable characters are replaced with a period. For non-packet events, the text message is printed in an 80-character mode.

An additional option can decode packet information for events that were packets. The IP layer is completely decoded. The protocols UDP, TCP and ICMP are also completely decoded. Any payload data is presented in a similar manner as the raw data dump option.

Options

-**a** *H*[*H:MM:SS*] **--after** *H*[*H:MM:SS*]	Specifies to use events that have occurred after a certain time. Times are in 24-hour military time. All events that occur prior to the times specified here will be ignored. Use of this option with the -b option can specify a specific window of time. Times are specified in HH:MM:SS format. Padding is not required for single digit times. For example, to see only events after nine o'clock you can enter -a 9 or -a 09:00.
-**b** *H*[*H:MM:SS*] **--before** *H*[*H:MM:SS*]	This option has exactly the same format as -**a**, except it specifies to use events that have occurred before a certain time. When used together, a time window can be specified. For example, to find all events that have occurred between 7:00 AM and 1:00 PM, the arguments -a 07:00 -b 13:00 or -a 7 -b 13 could be used.

-A <*event id*> **--specify-event** <*event id*>	For internal use only.
-B *YYYY-MM-DD* **--database** *YYYY-MM-DD*	Specifies to search the dragonevents database for events occurring on the specified date.
-**D** **--dns-resolve**	Resolve any DNS names.
-**d** {**0** |**1**	**2**	**3**} **--direction** {**0** |**1**	**2**	**3**}	Process data that is the specified direction. A value of **0** defines packets that are exterior to the protected networks. That is, both their destination and source addresses are not in the protected list. A value of **1** indicates that the packet is from a protected network. A value of **2** indicates that the packet is going to a protected network. A value of **3** indicates that the packet is from and going to a protected network.
-**e** <*event name*> --**event** <*event name*>	Only filters for events of this type. Only events of this type will be processed.
-**E** <*event name*> --**exclude-event** <*event name*>	Don't print events of this type. Opposite of the -e option. Both -e and -E can be used simultaneously.
-**f** <*filename*> --**file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
-**F** **--from**	Only apply the -i and -I options if the event is *from* the specific IP address. For example, arguments of -F -I 10.100.100.10 only prints out events that are not from 10.100.100.10. Without the -F option, all events not from and not to 10.100.100.10 would be processed.
-**i** <*IP address*> --**ip** <*IP address*>	Only summarize event data to or from this IP address or CIDR block.
-**I** <*IP address*> **--exclude-ip** <*IP address*>	Only summarize event data that is not to or from this IP address or CIDR block.
-l **--dragon-log**	Print in “dragon.log” style.
-O *lines* --lines *lines*	Only process a *lines* amount of events. For example, -O 1000 would cause this tool to process the first 1000 events, then exit. You can use this option only in conjunction with the -l option.
-p --raw	Display raw packet data.
-P --decode	Decode packet data.
-**s** <*sensor name*> **--sensor** <*sensor name*>	Only process events from this Network Sensor.
-**t** <*seconds*> **--dns-timeout** <*seconds*>	Do not wait longer than this value in seconds to resolve DNS. On some architectures, such as Linux, this feature does not work. Typically though, any DNS resolution time-out longer than specified will be skipped. This can be handy when resolving several hundred IP addresses. For example, arguments of -t 3 would cause this tool to drop any DNS resolutions that take longer than 3 seconds.
-**T** **--to**	Only apply the -i and -I options if the event is *to* the specific IP address. This option is exactly opposite of the -F option and only applies if the -i or -I options are used.

-u **-?** **--help**	Prints usage information.
-v **--version**	Prints out version information.

Examples

This example displays the packet payloads of events to or from IP address 134.141.94.176. Only a portion of the output is shown here.

```
root@dragon:/usr/dragon/tools# ./mklog -f ../DB/2014Apr29/dragon.db -p -i
134.141.94.176


** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Make Log Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Using file ../DB/2010Apr29/dragon.db as a 'dragon.db' file
** Printing packet data
** Searching for all packets to/from 134.141.94.176
** Date: Thursday April 29 2010
================================================================================
v1  (Internal)                                                        00:23:33
SOURCE: 134.141.90.207
DEST:   134.141.94.176
--------------------------------------------------------------------------------
45 00 00 6a 04 7f 00 00 7f 11 70 6a 86 8d 5a cf 86 8d 5e b0 E..j......pj..Z...^.
04 11 00 a1 00 56 8b 78 30 4c 02 01 00 04 06 70 75 62 6c 69 .....V.x0L.....publi
63 a0 3f 02 02 03 bc 02 01 00 02 01 00 30 33 30 0f 06 0b 2b c.?..........030...+
06 01 02 01 19 03 02 01 05 01 05 00 30 0f 06 0b 2b 06 01 02 ............0...+...
01 19 03 05 01 01 01 05 00 30 0f 06 0b 2b 06 01 02 01 19 03 .........0...+......
05 01 02 01 05 00                                           ......
--------------------------------------------------------------------------------
EVENT1: [DYNAMIC-UDP]  (udp,sp=1041,dp=161)

EVENT2: [SNMP:PUBLIC]  (udp,sp=1041,dp=161)

================================================================================
v1  (Internal)                                                        22:05:06
SOURCE: 134.141.90.207
DEST:   134.141.94.176
--------------------------------------------------------------------------------
45 00 00 6a 53 dc 00 00 7f 11 21 0d 86 8d 5a cf 86 8d 5e b0 E..jS.....!...Z...^.
04 11 00 a1 00 56 85 77 30 4c 02 01 00 04 06 70 75 62 6c 69 .....V.w0L.....publi
```

```
63 a0 3f 02 02 04 c2 02 01 00 02 01 00 30 33 30 0f 06 0b 2b c.?..........030...+
06 01 02 01 19 03 02 01 05 01 05 00 30 0f 06 0b 2b 06 01 02 ............0...+...
01 19 03 05 01 01 01 05 00 30 0f 06 0b 2b 06 01 02 01 19 03 .........0...+......
05 01 02 01 05 00                                          ......
--------------------------------------------------------------------------------
EVENT1: [DYNAMIC-UDP]  (udp,sp=1041,dp=161)

EVENT2: [SNMP:PUBLIC]  (udp,sp=1041,dp=161)

EVENT3: [PC:SNMP:PUBLIC]  (udp,sp=1041,dp=161)
```

This example shows a mklog session that uses the -l and -e options to list [SNMP:PUBLIC] events.

```
root@dragon:/usr/dragon/tools# ./mklog -l -e SNMP:PUBLIC -f ../DB/2014Apr30/
dragon.db

** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Make Log Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Printing 'dragon.log' style data
** Printing events of type [SNMP:PUBLIC]
** Using file ../DB/2014Apr30/dragon.db as a 'dragon.db' file
** Date: Friday April 30 2014

00:01:53  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
00:03:31  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
00:05:07  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp,sp=1041,dp=161) (v1)
00:11:53  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
00:13:31  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
00:15:08  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp,sp=1041,dp=161) (v1)
00:21:53  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
00:23:31  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
00:25:08  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp,sp=1041,dp=161) (v1)
00:31:52  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp-stream,sp=1034,dp=161) (v1)
00:31:52  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
00:33:30  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp-stream,sp=1034,dp=161) (v1)
00:33:30  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
00:35:08  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp-stream,sp=1041,dp=161) (v1)
01:45:10  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp-stream,sp=1041,dp=161) (v1)
01:45:10  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp,sp=1041,dp=161) (v1)
01:51:53  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
01:53:31  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
02:43:30  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
```

```
02:45:10  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp,sp=1041,dp=161) (v1)
02:51:53  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp-stream,sp=1034,dp=161) (v1)
02:51:53  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
02:53:30  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp-stream,sp=1034,dp=161) (v1)
02:53:30  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
02:55:10  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp-stream,sp=1041,dp=161) (v1)
10:43:42  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp,sp=162,dp=162) (v1)
13:12:37  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp,sp=162,dp=162) (v1)
13:12:37  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp,sp=162,dp=162) (v1)
13:12:48  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp,sp=162,dp=162) (v1)
13:12:52  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp,sp=162,dp=162) (v1)
13:12:57  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp-stream,sp=162,dp=162) (v1)
13:12:57  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp,sp=162,dp=162) (v1)
13:12:57  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp,sp=162,dp=162) (v1)
13:22:08  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp,sp=162,dp=162) (v1)
13:27:39  [I]  172.26.2.50     134.141.90.200  [SNMP:PUBLIC] (udp,sp=162,dp=162) (v1)
16:01:54  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
16:03:30  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
16:05:17  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp,sp=1041,dp=161) (v1)
16:11:54  [I]  134.141.93.36   134.141.97.237  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
16:13:31  [I]  134.141.93.36   134.141.97.231  [SNMP:PUBLIC] (udp,sp=1034,dp=161) (v1)
16:15:17  [I]  134.141.90.207  134.141.94.176  [SNMP:PUBLIC] (udp,sp=1041,dp=161) (v1)
```

mkchart — Make Chart Report Tool

The **mkchart** tool produces a chart similar to a spreadsheet. Its goal is to show which events have occurred against which computers. Think of this as an output of the **sum_event** tool plotted against a horizontal list of IP addresses. That tool only summarizes the number of each distinct event. It is very difficult to quickly tell with that tool and possibly the **mklog** tool the exact distribution of each security event. The **mkchart** tool attempts to rectify this by charting the number of events that have occurred against a single class C network. A single class C network was chosen to keep the total number of possible hosts no more than 255.

The Y-Axis lists the various events that have occurred and the X-Axis marks the various target computers. Only computers that have had events are listed. Computers are identified by their last octet. For example, if a Class C address of 10.20.30.0 were specified, host 10.20.30.111 would be represented as .111 and be listed at the top of its column.

The goal of this chart is to find if security events have been applied to an entire network or just to a few hosts. One could imagine a web farm that is experiencing script kiddy probes using this tool to quickly determine which of the many different web servers have been probed.

Note: This command does not support IPv6 addresses.

Options

-**a** *H*[*H:MM:SS*] **--after** *H*[*H:MM:SS*]	Specifies to use events that have occurred after a certain time. Times are in 24-hour military time. All events that occur prior to the times specified here will be ignored. Use of this option with the -b option can specify a specific window of time. Times are specified in HH:MM:SS format. Padding is not required for single digit times. For example, to see only events after nine o'clock you can enter -a 9 or -a 09:00.
-**b** *H*[*H:MM:SS*] **--before** *H*[*H:MM:SS*]	This option has exactly the same format as -**a**, except it specifies to use events that have occurred before a certain time. When used together, a time window can be specified. For example, to find all events that have occurred between 7:00 AM and 1:00 PM, the arguments -a 07:00 -b 13:00 or -a 7 -b 13 could be used.
-B *YYYY-MM-DD* **--database** *YYYY-MM-DD*	Specifies to search the dragonevents database for events occurring on the specified date.
-**e** <*event name*> --**event** <*event name*>	Only filters for events of this type. Only events of this type will be processed. If desired, only the first few characters need to be matched for a positive match. For example, using an argument of -e WEB will match any event that starts with WEB.
-**E** <*event name*> --**exclude-event** <*event name*>	Don't print events of this type. Opposite of the -e option. Both -e and -E can be used simultaneously, and the longer event is dominant. For example, arguments of -e WEB -E WEB:CGI will print all events that start with WEB, but none that start with WEB:CGI.
-**f** <*filename*> --**file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
-**i** <*IP address*> --**ip** <*IP address*>	Specifies the class C block of IP addresses. A bit mask of 24 is automatically applied, so you could enter 1.1.1.0 or 1.1.1.1 and they would both be used to specify the class C CIDR block of 1.1.1.0/24.
-**s** <*sensor name*> **--sensor** <*sensor name*>	Only process events from this Network Sensor.
-**u** **-?** **--help**	Prints usage information.
-**v** **--version**	Prints out version information.
-w --dragon-fire	Web mode. The mkchart tool places HTML wrapping code around the event names and the last octet IP addresses. The HTML code contains keywords that Extreme IPS searches for and replaces to present dynamic HTML to the web browser. The HTML code provides CGI-BIN links to the mklog tool.

Example

This example charts the occurrence of events in the 192.168.1.0 network.

```
root@mardragon:/opt/dragon/tools# ./mkchart -f ../DB/2014Apr29/dragon.db  -i
192.168.1.0


** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Make Chart Tool
```

```
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Using file ../DB/2014Apr29/dragon.db as a 'dragon.db' file
** X-Axis will be packets to: 192.168.1.0/24
** Date: Tuesday April 29 2014
```

Events	total	.123	.129	.147	.159	.160	.167	.168	.176
[SNMP:PUBLIC]	169	1							168
[DYNAMIC-UDP]	143								143
[HEARTBEAT]	24			24					
[ICMP:L3-RETRIEVER]	55		6		7	32	6	4	
[SMB:NAME-WILDCARD]	27			23			4		
[NT:NULL]	6		6						
[DYNAMIC-TCP]	34		22	12					
[DYNAMIC-ICMP]	2		2						
[HOST:LINUX:PROMISC-LEFT]	1			1					
[HOST:LINUX:PROMISC]	1			1					

mkicmp — Make ICMP Report Tool

The **mkicmp** tool is based on **mklog**, but provides more in-depth analysis of captured ICMP traffic. It operates in two modes. The first analyzes ICMP packets in bulk and assigns them a score for their overall packet content. This can identify randomized ICMP payloads, ICMP payloads that are 100% ASCII, ICMP payloads that contain known patterns of network activity such as commercial pinging programs, and several other features. The second mode analyzes ICMP unreachable packets, which can be useful for finding DNS source-ported scans, UDP probes, strange denial of service attacks, and network failures.

The primary reason to conduct additional ICMP analysis is to discover network anomalies that may impact the security or operation of your network. The mkicmp tool was designed to help analyze dragon.db logs and discover:

- Backdoor Traffic (LOKI, LOKI2, BO2K, TFN, TRINOO, TFN2K)
- UDP port scans
- UDP source port scans
- ICMP denial of service attacks
- Firewall Admin-Filter packets

The **mkicmp** tool can be configured with additional signatures that help identify benign ICMP packets. These signatures can also help search dragon.db files for specific or unique patterns. The signatures are added to the **dragon.icmp** file (located in the <*installdir*>/**tools** directory) by simply listing the ICMP pattern name followed by the ASCII and binary data to search for. The pattern is specified with the same "/" technique used in configuring signatures. Wild cards and other advanced pattern matching are not available. The file also does not support the use of comments. The following example shows an example section from a **dragon.icmp** file.

Sample from dragon.icmp file

```
ALPHABET                ABCDEFGHIJKLMN
ALPHABET                abcdefghijklmn
ASCII-PATTERN           /20!"#$%&'()*+,-./2f0123
KEEP-ALIVE              KeepISPAlive
ISS-SCANER              ISSPNGRQ
NUMBERS                 01234567890123456789
PINGSWEEP               PingSweep/20Version
RTRCONFIG               Router/20Config
SIMPLEPING              Simple/20Ping/20Version
SNMPSWEEP               SNMPSweep/20Version
SOLARWINDS              SolarWinds
SUBNETLIST              SubnetList/20Version
WHATSUP                 Network/20Monitoring/20Tool/27s/20Ping/20Data
PING-BSD                /0a/0b/0c/0d/0e/0f/10/11/12/13/14/15/16/17/18/19/20/21
PING-OPENBSD            /30/31/32/33/34/35/36/37/00/00/00/00/00/00/00/00
PING-IOS-9.X            /ab/cd/ab/cd/ab/cd/ab/cd/ab/cd/ab/cd/ab/cd/ab/cd
NMAP                    No/20Data/00
TOOL-PINGER-WIN         /44/61/74/61/00/00/00/00/00/00/00/00/00/00/00/00
```

The output from **mkicmp** may seem cryptic at first, but it provides four indicators to quickly analyze the contents of any ICMP packet as described in Table 1-1.

Table 1-1 mkicmp Reporting Fields and Descriptions

Reporting Field	Description
INC|DEC|RPT|RND	The first indicator to be determined is the ICMP payload randomness. The algorithm works by counting the number of state changes from byte to byte for the entire payload. There are separate counters for increments, decrements and repeats. For example, the first byte of ICMP data is 0x10, the next byte is 0x11. When the end of the payload is reached, the counter with the highest value is used to score a packet. If the values for state increments and decrements are both close to 50%, the packet is considered full of random data.
ASC|BIN	A second loop is performed on the ICMP payload data to determine if it is 100% ASCII characters or not. If any of the bytes are non-printable characters, the packet gets an indicator of BIN. Otherwise, it gets an ASC rating.
REPEAT STRINGS	If the first indicator is random (RND), mkicmp will attempt to analyze the payload data further and count the number of the most commonly repeated character.
SIGNATURE MATCHES	If mkicmp can match any of the signatures in the dragon.icmp file, this name will be printed out in quotations.

The **mkicmp** tool has many of the same command line options as **mklog**, except that the tool only filters for ICMP packets. Options such as -a which filters events based on time, -i which filters events based on IP address and -e which filters for specific event names are all available.

Options

-**a** *H*[*H:MM:SS*] **--after** *H*[*H:MM:SS*]	Specifies to use events that have occurred after a certain time. Times are in 24-hour military time. All events that occur prior to the times specified here will be ignored. Use of this option with the -b option can specify a specific window of time. Times are specified in HH:MM:SS format. Padding is not required for single digit times. For example, to see only events after nine o'clock you can enter -a 9 or -a 09:00.
-**b** *H*[*H:MM:SS*] **--before** *H*[*H:MM:SS*]	This option has exactly the same format as -**a**, except it specifies to use events that have occurred before a certain time. When used together, a time window can be specified. For example, to find all events that have occurred between 7:00 AM and 1:00 PM, the arguments -a 07:00 -b 13:00 or -a 7 -b 13 could be used.
-B *YYYY-MM-DD* **--database** *YYYY-MM-DD*	Specifies to search the dragonevents database for events occurring on the specified date.
-**d** {**0** |**1** | **2** | **3**} **--direction** {**0** |**1** | **2** | **3**}	Process data that is the specified direction. A value of **0** defines packets that are exterior to the protected networks. That is, both their destination and source addresses are not in the protected list. A value of **1** indicates that the packet is from a protected network. A value of **2** indicates that the packet is going to a protected network. A value of **3** indicates that the packet is from and going to a protected network.
-**D** **--dns-resolve**	Resolve any DNS names.
-**e** <*event name*> --**event** <*event name*>	Only print events of this type. Only events of this type will be processed. If desired, only the first few characters need to be matched for a positive match. For example, using an argument of -e WEB will match any event that starts with WEB.
-**E** <*event name*> --**exclude-event** <*event name*>	Don't print events of this type. Opposite of the -e option. Both -e and -E can be used simultaneously, and the longer event is dominant. For example, arguments of -e WEB -E WEB:CGI will print all events that start with WEB, but none that start with WEB:CGI.
-**f** <*filename*> --**file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
-**F** **--from**	Only apply the -i and -I options if the event is *from* the specific IP address. For example, arguments of -F -I 10.100.100.10 only prints out events that are not from 10.100.100.10. Without the -F option, all events not from and not to 10.100.100.10 would be processed.
-**i** <*IP address*> --**ip** <*IP address*>	Only summarize event data to or from this IP address or CIDR block.
-**I** <*IP address*> **--exclude-ip** <*IP address*>	Only summarize event data that is not to or from this IP address or CIDR block.
-l **--dragon-log**	Print in "dragon.log" style.
-m *type* **--type** *type*	Filter ICMP packets based on type. It takes a single argument that must be between 0 to 255 or the word "ping." If the argument is a number, only ICMP packets of that type will be processed. If the argument is the word "ping," ICMP packets of type 0 and 8 will be processed.

-M *sub-filter* **--unreach-code** *sub-filter*	Filter on ICMP UNREACHABLE messages with this subfilter: • 0=net • 3=port • 5=src-route • etc
-O *lines* **--lines** *lines*	Only process a *lines* amount of events. For example, -O 1000 would cause this tool to process the first 1000 events, then exit.
-p --raw	Display raw packet data.
-P --decode	Decode packet data.
-**s** <*sensor name*> --**sensor** <*sensor name*>	Only process events from this Network Sensor.
-**t** <*seconds*> --**dns-timeout** <*seconds*>	Do not wait longer than this value in seconds to resolve DNS. On some architectures, such as Linux, this feature does not work. Typically though, any DNS resolution time-out longer than specified will be skipped. This can be handy when resolving several hundred IP addresses. For example, arguments of -t 3 would cause this tool to drop any DNS resolutions that take longer than 3 seconds.
-**T** **--to**	Only apply the -i and -I options if the event is *to* the specific IP address. This option is exactly opposite of the -F option and only applies if the -i or -I options are used.
-**u** **-?** **--help**	Prints usage information.
-**v** **--version**	Prints out version information.
-z <*path/to/dragon.icmp*> **--dragon-icmp** <*path/to/dragon.icmp*>	Specifies the location of the dragon.icmp file.

Example

The following example processes two lines and decodes the packet data.

```
root@mardragon:/usr/dragon/tools#./mkicmp -O 2 -P -f ../DB/2014May12/dragon.db

** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Make ICMP Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Only printing the first 2 lines
** Decoding protocol packet data
** Date: Wednesday May 12, 2014
```

```
================================================================================
dragon233-VS1  (Internal)
10:42:45
SOURCE: 192.168.2.8
DEST:   192.168.2.135
--------------------------------------------------------------------------------

IP HEADER:
     Version               4
     Header Length         5 (20 bytes)
     Type of Service       0
     Total Length          70 bytes
     ID Number             0x42D8
     Reserved Bit          0
     Don't Frag Bit        0
     More Frags Bit        0
     Fragment Offset       0
     Time To Live          64
     Protocol              ICMP
     Checksum              0xB1FF
     Source Address        192.168.2.8
     Destination Address   192.168.2.135

ICMP HEADER:
     Type                  Echo
     Code                  No Code
     Checksum              0x7946
     Identifier            0xCA15
     Sequence Number       0x0

ICMP PAYLOAD:
 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 abcdefghijklmnopqrst
 75 76 77 61 62 63 64 65 66 67 68 69 A0 00 00 00 00 00 00 00 uvwabcdefghi........
 00 00                                                       ..

--------------------------------------------------------------------------------
Event1: [DYNAMIC-ICMP] (echo_request,protocol=icmp) dragon233-VS1
================================================================================
dragonNetworkSensor  (Internal)                                      00:42:24
SOURCE: 134.141.93.57
DEST:   134.141.90.251
--------------------------------------------------------------------------------

IP HEADER:
     Version               4
```

```
     Header Length          5
     Type of Service        0
     Total Length           60 bytes
     ID Number              0x81DA
     Reserved Bit           0
     Don't Frag Bit         0
     More Frags Bit         0
     Fragment Offset        0
     Time To Live           29
     Protocol               ICMP
     Checksum               0x5698
     Source Address         134.141.93.57
     Destination Address    134.141.90.251

ICMP HEADER:
     Type                   ping
     Code                   0
     Checksum               0x9D9
     Identifier             0x200
     Sequence Number        0x4385

ICMP PAYLOAD:
41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 ABCDEFGHIJKLMNOPQRST
55 56 57 41 42 43 44 45 46 47 48 49                         UVWABCDEFGHI

--------------------------------------------------------------------------------
EVENT1: [ICMP:L3-RETRIEVER] (icmp,type=8,id=2)
2 LINE MAXIMUM
```

mkports — Make Reports of Active IP Protocols and TCP/UDP Ports

This tool processes all the packet events contained in a single dragon.db file or the dragonevents database for the specified date. It summarizes the total number of different IP protocols that have occurred. It also does this for TCP and UDP packets. For each TCP or UDP port, **mkports** summarizes the total number of source and destination ports. This produces four columns of port data. Only ports with an activity level greater than the default thresholds are printed. The default threshold is zero, which can be changed with the -C option. If port scans are present, all ports may have one or two events present. Filtering out all ports that have less than this value will filter out the port scan.

Options

-**a** *H*[*H:MM:SS*] **--after** *H*[*H:MM:SS*]	Specifies to use events that have occurred after a certain time. Times are in 24-hour military time. All events that occur prior to the times specified here will be ignored. Use of this option with the -b option can specify a specific window of time. Times are specified in HH:MM:SS format. Padding is not required for single digit times. For example, to see only events after nine o'clock you can enter -a 9 or -a 09:00.
-**b** *H*[*H:MM:SS*] **--before** *H*[*H:MM:SS*]	This option has exactly the same format as -**a**, except it specifies to use events that have occurred before a certain time. When used together, a time window can be specified. For example, to find all events that have occurred between 7:00 AM and 1:00 PM, the arguments -a 07:00 -b 13:00 or -a 7 -b 13 could be used.
-B *YYYY-MM-DD* **--database** *YYYY-MM-DD*	Specifies to search the dragonevents database for events occurring on the specified date.
-c *count* **--count** *count*	Only prints ports that have an amount of events greater than this value. For example, arguments of -c 10 only print port data that has had more than ten events.
-**e** <*event name*> -**-event** <*event name*>	Only filters for events of this type. Only events of this type will be processed. If desired, only the first few characters need to be matched for a positive match. For example, using an argument of -e WEB will match any event that starts with WEB.
-**E** <*event name*> -**-exclude-event** <*event name*>	Don't print events of this type. Opposite of the -e option. Both -e and -E can be used simultaneously, and the longer event is dominant. For example, arguments of -e WEB -E WEB:CGI will print all events that start with WEB, but none that start with WEB:CGI.
-**f** <*filename*> -**-file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
-**s** <*sensor name*> -**-sensor** <*sensor name*>	Only process events from this Network Sensor.
-**u** **-?** **--help**	Prints usage information.
-**v** **--version**	Prints out version information.

Example

This example shows the output of **mkports** for ports with more than 1000 events.

```
root@dragon:/usr/dragon/tools# ./mkports -f ../DB/2014May12/dragon.db -c 1000


** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Make Ports Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/
```

```
** Only printing out ports with more than 1000 events
---------------------
   IP        Protocol
Protocol       Count
---------------------
icmp             1046
tcp            271404
udp                65

-----------------------------------
             TCP           UDP
        Source  Dest  Source  Dest
Ports    Port   Port   Port   Port
-----------------------------------
1        2318   3375
21       8685  16122
22       4053   4576
23       3243   4445
25       4604  10721
53              1222
80      60090  92433
81       2531   3234
1025     2055   2884
1083     1981   1690
1433            1138
1863            1387
5001     3335   4081
5060     2109   1824
```

mksession — Make Lists of Active TCP/UDP Sessions and Replay Them

When a Network Sensor is running, it collects a lot of different packet data. Once an attack is detected, the Network Sensor will attempt to log many of the follow-on packets. It reconstructs these for inspection of new attacks, but in most cases, the raw follow-on packets are logged directly to the dragon.db file without any reconstruction. These packets are normally recorded as [DYNAMIC] events. Sessions that are contained in multiple packet streams are not identified in dragon.db files. They must be reassembled with the **mksession** tool.

When events occur, the Network Sensor continues to collect the following traffic from the attacker and target. The sensor can also be configured to collect all types of specific traffic and even traffic from static IP address ranges.

The bottom line is that a typical dragon.db file contains a lot of network traffic. The **mksession** tool can identify distinct network sessions and replay them with a variety of options.

Identifying sessions can be accomplished with a variety of tools. In general, the time and direction of traffic can be specified. However, most users like to directly enter the ports and IP addresses in use. Searching for sessions can be qualified with several techniques.

A common technique is to start with traffic based on IP addresses. Specifying a single IP address or CIDR block lists all sessions to or from that point. Specifying a second IP address or CIDR block narrows the search between those two endpoints. Also specifying the port narrows the search even further. Specifying the second port narrows the search to a single selection. A similar technique starts with list session by port, specifying an IP address then specifying a complete session.

When session summaries are displayed, they include the start and finish times of each session. They also include the number of bytes of payload data that was transferred between the two endpoints. The longest event name associated with each session is displayed if one is available. [DYNAMIC] events are not displayed.

It is also important to realize that the actual TCP or UDP session may have been ongoing for a long time before the Network Sensor recognized an attack or suspicious activity, and it may also have gone on much longer after the Network Sensor reached the programmed limit of follow-on packets to collect.

Replaying a session can be tricky if one does not understand what they are looking at. It can also be confounded even more because there is no guarantee that the packets have been recorded with perfect accuracy. The Network Sensor may also have moved onto something more interesting to capture instead of following this session to completion. If the Network Sensor does not seem to be recording enough session information, try to increase the number of cushion packets collected (configured as part of the Network Sensor Policy Dynamic Module).

One problem that confuses many Enterasys IPS users is that the dragon.db contains many types of information, but the **mksession** tool only processes events with packet information. Specifically, if the Network Sensor logs a TCP or UDP session fragment as part of an event's data, such as a Telnet session capture, the **mksession** tool cannot use this data. However, using the **mklog** tool with the **–p** option should print out the contents of that particular session. Many Enterasys IPS users monitoring protocols such as Telnet often run into this issue.

There are three options when replaying sessions. The first is to display non-printable values or to not display them. Non-printable characters such as the 0x00 and 0xff characters are displayed in parentheses like {00}{ff}. The second option chooses to display the second half of a conversation. Typically, sessions such as FTP and SMTP make more sense when the responses from the server are present. Lastly, an option is available to limit the width of any printed lines. This can help format session replays to fit better on a variety of different consoles.

Options

-**a** *H*[*H:MM:SS*] **--after** *H*[*H:MM:SS*]	Specifies to use events that have occurred after a certain time. Times are in 24-hour military time. All events that occur prior to the times specified here will be ignored. Use of this option with the -b option can specify a specific window of time. Times are specified in HH:MM:SS format. Padding is not required for single digit times. For example, to see only events after nine o'clock you can enter -a 9 or -a 09:00.
-**b** *H*[*H:MM:SS*] **--before** *H*[*H:MM:SS*]	This option has exactly the same format as -**a**, except it specifies to use events that have occurred before a certain time. When used together, a time window can be specified. For example, to find all events that have occurred between 7:00 AM and 1:00 PM, the arguments -a 07:00 -b 13:00 or -a 7 -b 13 could be used.
-B *YYYY-MM-DD H[H:MM:SS]* **--database** *YYYY-MM-DD H[H:MM:SS]*	Specifies to search the dragonevents database for events occurring on the specified date.
-**d** {**0** |**1**	**2**	**3**} --**direction** {**0** |**1**	**2**	**3**}	Only print data with DIRECTION equal to: A value of **0** defines packets that are exterior to the protected networks. That is, both their destination and source addresses are not in the protected list. A value of **1** indicates that the packet is from a protected network. A value of **2** indicates that the packet is going to a protected network. A value of **3** indicates that the packet is from and going to a protected network.
-**f** <*filename*> --**file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
-**h** **--nohex**	Suppresses printing of non-printable hex codes during replays. Without this setting, characters such as 0x10 are printed as {10}.
--**ip1** <*IP address*> -**1** <*IP address*>	Specifies an IP address or CIDR block to search for sessions. It also specifies the first IP address of a particular session to replay.
--**ip2** <*IP address*> -**2** <*IP address*>	Specifies an IP address or CIDR block to search for sessions when used with the --**ip1** argument. It also specifies the second IP address of a particular session to replay.
-**k** *KB* --**kilobytes** *KB*	Specifies the maximum session data to display when a session is replayed. Default is 500 KB.
-**m** *max* **--sessions** *max*	Specifies the maximum number of distinct sessions to identify before exiting. The default value is 1024, which can prevent large database files from generating thousands of output lines which can overload some Telnet and SSH user sessions.
--**p1** *portnum* **-3** *portnum*	Specifies the first port to search for sessions on. For replays, it specifies the first port in sessions to be replayed.
--**p2** *portnum* **-4** *portnum*	Specifies the second port to search for sessions. For replays, it also specifies the second port in sessions to be replayed. Replays one side of the specified session. If the -**ip1**, -**ip2**, -**p1** and -**p2** options are not specified, it will not replay the session.
-**r** **--replay**	Replay this session.
-**R** **--replay-both**	Replay both sides of this session.

-**s** <*sensor name*> --**sensor** <*sensor name*>	Only process events from this Network Sensor.
-**U** **--udp**	Searches and replays UDP sessions. The default is TCP.
-**u** **-?** **--help**	Prints usage information.
-**v** **--version**	Prints version information.
-**w** *chars* --**wrap** *chars*	Wraps any session replay data that attempts to display data that is larger than width specified. The default is 120 characters, but in text terminals, a width of 80 characters or any other width can be specified.
-**W** **--dragon-fire**	Specifies web mode. For summary of sessions, this tool adds additional HTML code around the size of the identified session. Clicking on the reported size results in a request to replay the particular session. This feature supports the IPS reporting GUI.

Note: For session replays, ip1 and p1 become the source IP address and port for the session, unless you are using the -R option.

Example

The following example shows a **mksession** listing active sessions on ports 21 (ftp) and 1053, then replaying an identified session.

```
root@dragon:/usr/dragon/tools# ./mksession --p1 1053 --p2 21 -f ../DB/2014May12/
dragon.db

** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Make Session Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Filtering for all packets between port 1053 and port 21

--------------------------------------------------------------------------------
   Source IP        Dest IP     Port1 Port2  Start     Stop    Size     Type
--------------------------------------------------------------------------------
111.222.73.207   128.82.4.66      1053     21   16:50  16:51 995 [FTP:RHOSTS]
111.222.74.212   216.35.17.230    1053     21   21:30  21:30 668 [FTP:USER-ANON]

root@dragon:/usr/dragon/tools# ./mksession --p1 1053 --p2 21 --ip1 111.222.73.207
--ip2 128.82.4.66 -r -f ../DB/2014May12/dragon.db

** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Make Session Tool
```

```
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Filtering for all packets between port 1053 and port 21
** Watching for sessions on 111.222.73.207
** Watching for sessions on 128.82.4.66
** Replaying this session

CWD .rhosts{D}{A}
CWD /{D}{A}
CWD /public_html{D}{A}./
PWD{D}{A}
PASV{D}{A}
LIST -aFl{D}{A}
CWD /public_html/private{D}{A}
PWD{D}{A}
PASV{D}{A}
LIST -aFl{D}{A}
PWD{D}{A}
PASV{D}{A}
NLST /public_html/private{D}{A}
TYPE A{D}{A}
PASV{D}{A}
STOR /public_html/private/message.txt{D}{A}
```

mkprecap — Pre-Event Collection

This tool displays data collected before the specified event occurred. Pre-event collection settings are configured for a Network Sensor using the Pre-Event Collection Settings tab.

Options

-**c** <*id*> **--precoll-id** <*id*>	Return the packet data associated with the event with the specified ID.
-**e** <*eventname*> --**event** <*eventname*>	Show only packets with specified event name.
-**f** <*filename*> --**file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
-**h** **--header**	Print header information and column names.
-**i** <*ipaddr*> --**ip** <*ipaddr*>	Print all data to or from this IP address (CIDR mask allowed).
-**l** <*ipaddr*> **--exclude-ip** <*ipaddr*>	Print all data NOT to or from this IP address (CIDR mask allowed).
-**s** <*sensor name*> --**sensor** <*sensor name*>	Show packets collected by this Network Sensor.
-**t** *HH:MM:SS* --**time-slice** *HH:MM:SS*	Show packets from this time slice only.
-**u** **-?** **--help**	Prints usage information.
-**v** **--version**	Prints version information.

Example

This example shows partial output of the command run against the current dragon.db file.

```
root@dragon:/usr/dragon/tools# ./mkprecap -h -f dragon.db

** Extreme Networks (R) Intrusion Prevention System [8.3.0] [300]
** Pre Event Collection Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/


ID       TIME     DIR SIP              DIP             EVENT               SENSOR         SIZE
=============================================================================================
6711     00:02:13  E  108.79.141.134   141.94.141.134  [SNMP:PUBLIC]      linux-VS1       108
6712     00:02:41  E  110.90.141.134   8.103.141.134   [PROXY:WEB-POST]   linux-VS1       1339
6712.1   00:02:41  E  110.90.141.134   8.103.141.134   [PROXY:WEB-POST]   linux-VS1       52
6714     00:02:41  E  8.103.141.134    110.90.141.134  [SUCCESS:WEB-OK]   linux-VS1       964
6715     00:02:41  E  110.90.141.134   8.103.141.134   [PROXY:WEB-GET]    linux-VS1       1083
6717     00:02:41  E  8.103.141.134    110.90.141.134  [SUCCESS:WEB-OK]   linux-VS1       1500
6718     00:02:42  E  110.90.141.134   8.103.141.134   [PROXY:WEB-GET]    linux-VS1       1083
6718.1   00:02:41  E  110.90.141.134   8.103.141.134   [PROXY:WEB-GET]    linux-VS1       52
6720     00:02:42  E  8.103.141.134    110.90.141.134  [SUCCESS:WEB-OK]   linux-VS1       1500
```

mktcpdump — Make TCP Dump File

For IP based events, this tool can export data collected in a dragon.db file or the events database to a TCPDUMP binary file. This is useful for running data collected by Extreme Networks IPS through third party tools.

Options

-**a** *H*[*H:MM:SS*] **--after** *H*[*H:MM:SS*]	Specifies to use events that have occurred after a certain time. Times are in 24-hour military time. All events that occur prior to the times specified here will be ignored. Use of this option with the -b option can specify a specific window of time. Times are specified in HH:MM:SS format. Padding is not required for single digit times. For example, to see only events after nine o'clock you can enter -a 9 or -a 09:00.
-**b** *H*[*H:MM:SS*] **--before** *H*[*H:MM:SS*]	This option has exactly the same format as -**a**, except it specifies to use events that have occurred before a certain time. When used together, a time window can be specified. For example, to find all events that have occurred between 7:00 AM and 1:00 PM, the arguments -a 07:00 -b 13:00 or -a 7 -b 13 could be used.
-B *YYYY-MM-DD* **--database** *YYYY-MM-DD*	Specifies to search the dragonevents database for events occurring on the specified date.
-**d** {**0** |**1** | **2** | **3**} --**direction** {**0** |**1** | **2** | **3**}	Only print data with DIRECTION equal to: A value of **0** defines packets that are exterior to the protected networks. That is, both their destination and source addresses are not in the protected list. A value of **1** indicates that the packet is from a protected network. A value of **2** indicates that the packet is going to a protected network. A value of **3** indicates that the packet is from and going to a protected network.
-**e** <*eventname*> --**event** <*eventname*>	Print only packets with specified event name.
-**E** <*event name*> --**exclude-event** <*event name*>	Don't print events of this type. Opposite of the -e option. Both -e and -E can be used simultaneously, and the longer event is dominant. For example, arguments of -e WEB -E WEB:CGI will print all events that start with WEB, but none that start with WEB:CGI.
-**f** <*filename*> --**file** <*filename*>	Specifies the dragon.db file to use. The file does not need to be named dragon.db.
--**ip1** <*IP address*> -**1** <*IP address*>	Specifies an IP address or CIDR block to search for sessions. It also specifies the first IP address of a particular session to replay.
--**ip2** <*IP address*> -**2** <*IP address*>	Specifies an IP address or CIDR block to search for sessions when used with the --**ip1** argument. It also specifies the second IP address of a particular session to replay.
-l <*length*> **--snaplen** <*length*>	Snapshot length for the capture. (Default is 65535.)
-o <*filename*> **--output** <*filename*>	Write the transmuted data to the specified output file.
-**s** <*sensor name*> --**sensor** <*sensor name*>	Only process events from this Network Sensor.

-**u** **-?** **--help**	Prints usage information.
-**v** **--version**	Prints version information.

Example

The following example creates an output file named “test.pcap,” using the data in a dragon.db file and filtering for packets sent between 134.141.90.92 and 134.141.103.8.

```
root@dragon:/opt/dragon/tools# ./mktcpdump -f ../DB/2014Jun15/dragon.db -1
134.141.90.92 -2 134.141.103.8 -o /pcaps/test.pcap


** Extreme Networks (R) Intrusion Prevention System [8.3.0] [333]
** Make TCP Dump Tool
** Copyright (C) 2001-2014 Extreme Networks
** general: http://www.extremenetworks.com
** support: http://www.extremenetworks.com/support/

** Using file ../DB/2014Jun15/dragon.db as the dragon.db file
** Using file /pcaps/test.pcap for output
** Filtering for all packets between IP 134.141.90.92 and IP 134.141.103.8
```