

Open Source  
Security Information Management  
(OSSIM)  
Version 0.9.7

Console Configuration  
Version 2

Ken Gregoire

September 22, 2004



Copyright (c) 2004 Ken Gregoire.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Many thanks to the OSSIM Team for providing input and reviewing the document for accuracy.

## Table of Contents

1.	Introduction.....	5
2.	Overview.....	5
3.	Description of Components .....	6
3.1.1.	OSSIM Web Interface Components .....	7
3.2.	Top Level.....	7
3.3.	Control Panel .....	9
3.3.1.	Metrics .....	9
3.3.2.	Alarms.....	9
3.3.3.	Alerts.....	9
3.3.4.	Vulnerabilities.....	9
3.3.5.	Anomalies .....	9
3.4.	Policy .....	10
3.4.1.	Policy .....	10
3.4.2.	Hosts .....	10
3.4.3.	Networks.....	10
3.4.4.	Sensors .....	11
3.4.5.	Signatures.....	11
3.4.6.	Priority & Reliability .....	11
3.4.7.	Ports .....	11
3.5.	Reports .....	12
3.5.1.	Host Report .....	12
3.5.2.	Security Report .....	12
3.5.3.	Incidents.....	12
3.6.	Monitors.....	13
3.6.1.	Session & Network .....	13
3.6.2.	Availability .....	13
3.6.3.	Riskmeter .....	13
3.7.	Configuration .....	14
3.7.1.	Main .....	14
3.7.2.	Users .....	14
3.7.3.	Directives .....	14
3.7.4.	Correlation .....	14
3.7.5.	RRD Config .....	15
3.7.6.	Host Scan .....	15
3.7.7.	Riskmeter .....	15
3.8.	Tools .....	16
3.8.1.	Scan.....	16
3.8.2.	Backlog .....	16
3.8.3.	Rule Viewer .....	16
3.8.4.	Backup .....	16
4.	Configuring OSSIM.....	17
5.	Using OSSIM.....	17
6.	Glossary .....	18

7.	Appendixes .....	24
7.1.	Appendix 1 - Signatures.....	24
7.2.	Appendix 2 - Directives .....	25
7.3.	Appendix 3 - RRD Attributes .....	26
7.4.	Appendix 4 – Plugin IDs.....	27
7.5.	Appendix 5 - Screenshots .....	28
7.5.1.	ACID.....	28
7.5.2.	ACID Detail .....	29
7.5.3.	ACID Search.....	30
7.5.4.	Alarm Console .....	30
7.5.5.	Directives 1 .....	31
7.5.6.	Directives 2 .....	31
7.5.7.	Incidents 1 .....	32
7.5.8.	Incidents 2.....	32
7.5.9.	Inventory 1 .....	33
7.5.10.	Inventory 2.....	34
7.5.11.	Metrics 1 .....	34
7.5.12.	Metrics 2 .....	35
7.5.13.	NTop RRD .....	36
7.5.14.	NTop Services.....	37
7.5.15.	NTop Sessions .....	37
7.5.16.	Operating Systems .....	38
7.5.17.	Riskmeter .....	39
7.5.18.	RRD Profile .....	40
7.5.19.	Rule Editor .....	41
7.5.20.	Security Reporting 1 .....	41
7.5.21.	Security Reporting 2 .....	42
7.5.22.	Security Reporting 3 .....	43
7.5.23.	Users .....	44
7.5.24.	Vulnmeter .....	44
7.5.25.	Worm .....	45
7.6.	Appendix 5 – Reference Documents .....	46
7.7.	Appendix 6 - GNU Free Documentation License.....	47



# 1. Introduction

The purpose of this document is to provide a layman's understanding of how to use Open Source Security Information Management (OSSIM). Although OSSIM can support very large networks, it can be used in small and home-based networks. Even small and home-based networks require protection from attacks from the Internet. Normally your network service provider or Internet Service Provider (ISP) does not provide any type of Intrusion Detection or protection of your Internet connection.

Since OSSIM is Open Source, potential customers are usually leery about using Open Source or free software because of the lack of documentation, which relates to higher implementation and operating costs. Hopefully this will aid in the implementation and support of OSSIM in your large, small or home-based network.

If you are new to OSSIM then I would recommend that you read the following in the order below.

All can be found at: <http://ossim.net/docs.php>

1. OSSIM Fast Guide
2. OSSIM - General System Description
3. OSSIM Console Configuration – this one.
4. Install it! If on FC2 use this Installation Guide.
5. Users Manual by Kevin Milne to configure OSSIM.
6. A Practice of OSSIM.
7. Correlation engine explained (RPC DCOM example)
8. Correlation engine explained (Worm example)

If you have trouble with some of the terms, look in the attached Glossary.

## 2. Overview

OSSIM provides a central management console to provide system and network alert and alarm management. The strength of OSSIM is its ability to correlate attacks between various sensors like Snort, Arpwatch and NTop. This correlation helps eliminate false positive Alarms and provides a better perspective of attacks.

OSSIM can read and correlate Alerts from:

- Snort,
- Real Secure,
- Spade,
- NTop,
- Firewall-1,
- IPtables,
- Apache,
- IIS,
- Cisco routers,
- Unix servers.



### 3. Description of Components

The following is a description of the components that are used in OSSIM.

Component	Purpose	Description
ACID	Console	Analysis Console for Intrusion Databases (ACID) or Management and Reporting Console for Snort logs.
ArpWatch	Detect	Program that discovers the MAC Address of a network interface.
Hosts	Network	Computer asset you're trying to protect.
Nessus	Scan	Software that scans a computer and provides a report that includes system information and potential system vulnerabilities.
Network	Network	Either the External Network (the Internet) or an Internal Network that your internal systems are connected to and Network Assets that you are trying to protect.
NTop	Monitor	A program that monitors network traffic between computers.
OpenNMS	Monitor	Software that monitors computers and reports uptime and availability of hardware and software components.
OSSIM	Correlate	Correlation and Management Console
RRDTool	Detect	Round Robin Database Tool collects time series of network packets in a Round Robin fashion.
Sensor	Detect	Software that runs on a computer that monitors traffic and activity and usually with Rules can detect attacks and define the type of attack. If all components were installed on one Host, then this Host would be a Sensor.
Snort	Detect	Network-based Intrusion Detection System that can act as a network sniffer and packet logger.
Snort-inline <sup>1</sup>	Block	A program that blocks access on the Host if a specific action is detected based on a Snort rule.
Snortsam <sup>1</sup>	Block	A program that will take action on a port or IP address based on a modified Snort rule. Usually to block or drop the IP address and/or port. Snortsam can support sensors on various devices including Cisco routers, Firewall 1, Checkpoint and IPtables on Hosts.
Spade	Detect	Statistical Packet Anomaly Detection Engine (SPADE) is a preprocessor for Snort that detects general packet anomalies.

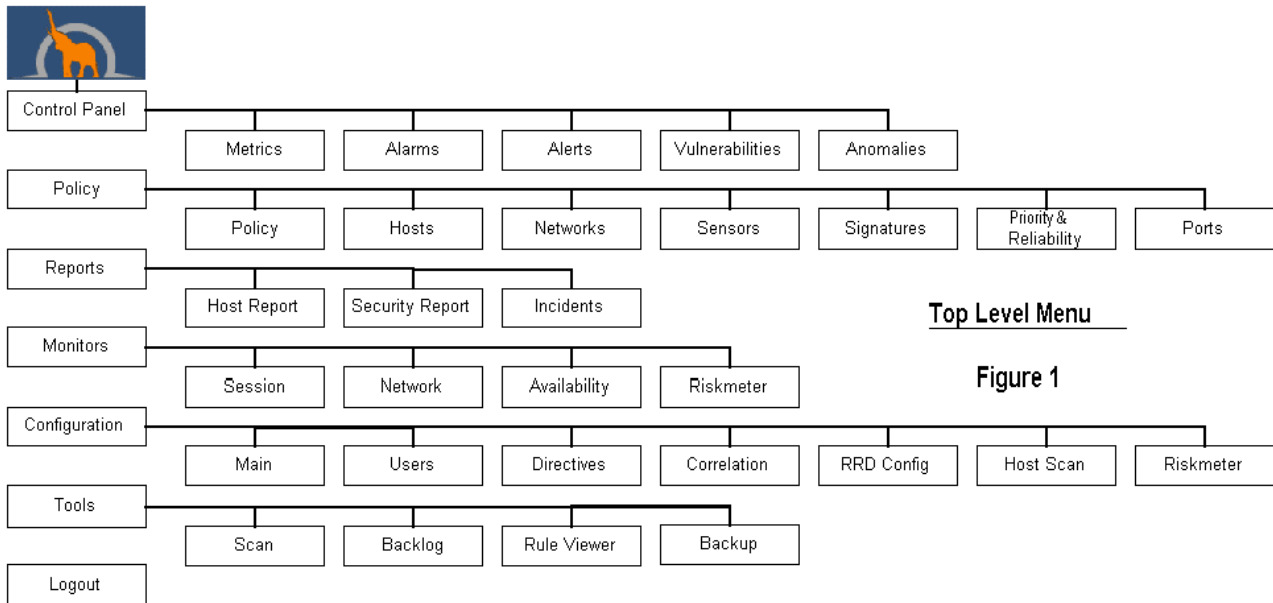
<sup>1</sup> Currently not implemented in OSSIM but being considered.



### 3.1.1. OSSIM Web Interface Components

OSSIM is accessed through a web interface. The following outlines the OSSIM web interface.

### 3.2. Top Level



OSSIM consists of six top-level sections:

1. Control Panel – provides:
  - Metrics of global, networks and hosts of compromises and attacks;
  - Alarms;
  - Alerts from Snort through the ACID console;
  - Vulnerabilities which are the Nessus scans; and
  - RRD Anomalies and Operating System (OS) and network card (MAC) changes.
2. Policy – provides the ability to:
  - Add and reload Policies;
  - Add, modify and delete Hosts, Networks, Sensors, Signatures, Ports and Port Groups;
  - Reload all of the above into the OSSIM database;
  - Change the Priority & Reliability settings for Plugins.
3. Reports – provides:
  - Detailed Host Reports;
  - Top-Level Security Report and Graphs.
  - Incident Handling ticket-like system.



4. Monitors – provides:
  - Network traffic statistics provided by NTop;
  - Availability provided by OpenNMS;
  - Riskmeter graph of Global, Networks and Hosts.
  
5. Configuration – provides:
  - Add, modify and delete users and change their permissions.
  - Reload of all policies, hosts, networks and sensors into the OSSIM database.
  - View and change the Priority and Reliability of all Plugins.
  - View the Correlation between Plugins.
  - Add and modify the RRD Configuration of Threshold, Priority, Alpha, Beta and Persistence.
  - Add and delete Host Scans for NMAP and Nessus.
  - Change the Riskmeter Recovery Level and Threshold and Graph.
  
6. Tools – provide:
  - Scan tool that allows you to scan a group of IP addresses.
  - Backlog Alert viewer.
  - OSSIM Rule Viewer.
  - Backup or restore databases.



### 3.3. Control Panel

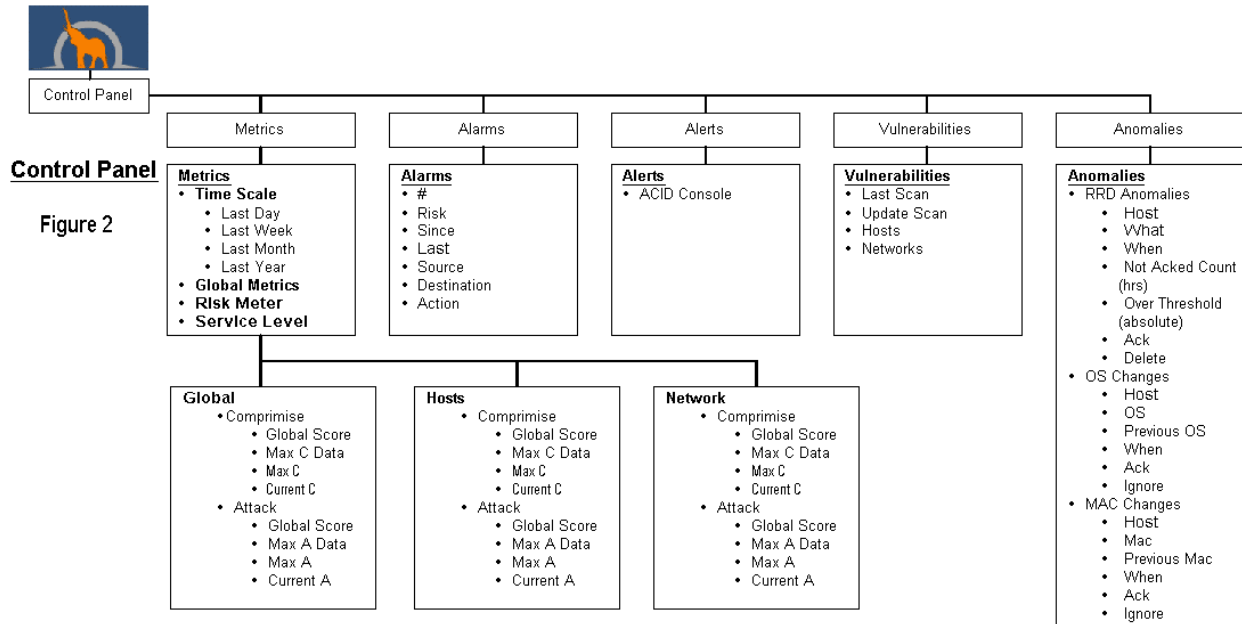


Figure 2

The main function of the Control Panel is to provide the ability to view overall Metrics, Alarms, Alerts, Vulnerabilities and Anomalies.

#### 3.3.1. Metrics

Metrics provides a Global view of Compromises and Attacks grouped by Global (meaning all), by Network and by Hosts. It provides the ability to look at Compromises and Attacks by various time scales: Last Day, Last Week, Last Month and Last Year.

#### 3.3.2. Alarms

Alarms provide the list of all Alarms and the ability to Acknowledge (clear) the Alarm. Alarms are Alerts that are correlated with Directives thus eliminating False Positives.

#### 3.3.3. Alerts

Alerts provide access to the ACID Console to display stored Detector and Monitor Alerts.

#### 3.3.4. Vulnerabilities

Vulnerabilities are the access point to the Nessus scans.

#### 3.3.5. Anomalies

Anomalies provide RRD Console access, which are RRD Anomalies. NTop uses the Round Robin Database (RRD) Tool to collect and store packet data in a time series format. OSSIM applies Rules to the RRDDTool data to determine RRD Anomalies. These Rules are configured under Configuration → RRD Config. Network card MAC address changes and Operating System (OS) changes are shown here too.



### 3.4. Policy

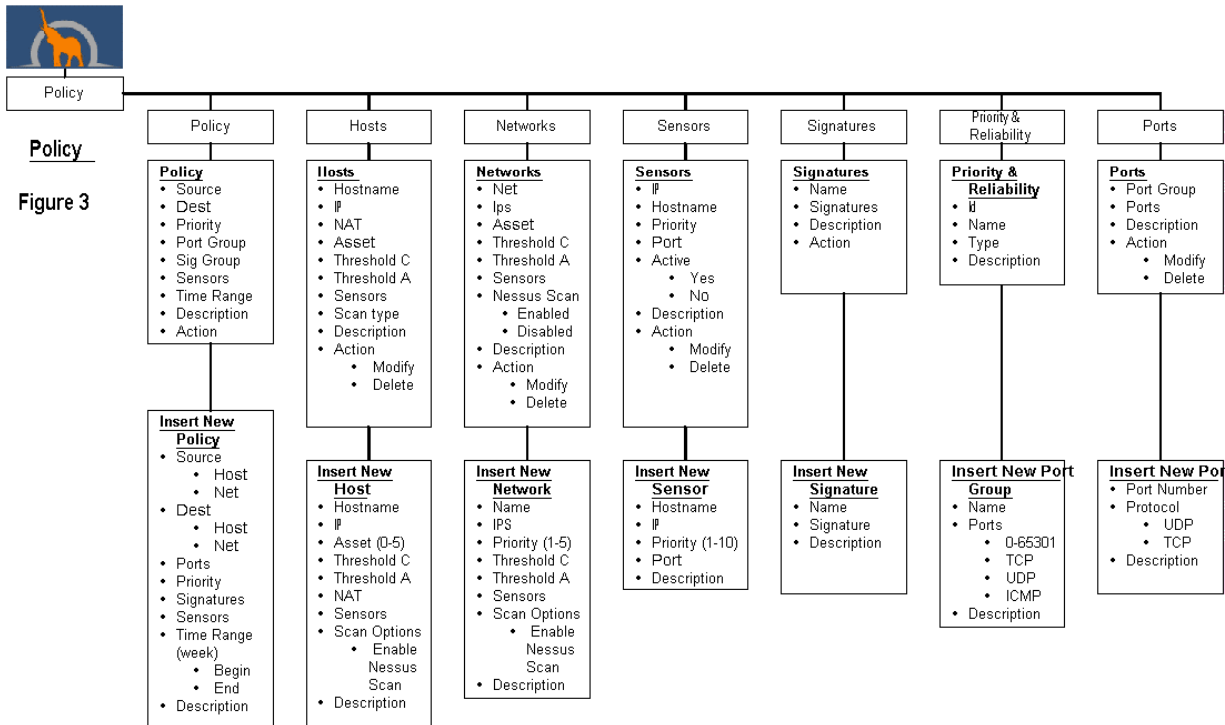


Figure 3

The main function of the Policy panel is to provide the ability to configure and tune OSSIM. It allows you to:

- Add, modify and delete Policies, Hosts, Networks, Sensors, Signatures, Ports and Port Groups.
- Display lists of Policies, Hosts, Networks, Sensors and Ports.
- Access the details by Hosts, Networks.

#### 3.4.1. Policy

Here you can add, delete or modify a policy. Policies can be related to any Source, Destination, Sensor, Signatures, Ports or Time Range.

#### 3.4.2. Hosts

Here you can add, delete or modify any Hosts. Hosts can be setup for Nessus and NMAP scans and what RRD Profile is to be used for this Host.

#### 3.4.3. Networks

Here you can add, delete or modify any Network. Networks can be added as a group of IP's; for example 192.168.1.0/24 adds all the Hosts on this network group. Nessus scans can also be enabled for all the Hosts on this Network. An individual IP address can also be added usually done to provide remote IDS monitoring. In this case additional Sensors can be added to the Hosts or network devices (routers/firewalls) to provide local collection of Alerts and can be passed back to the OSSIM system.



### **3.4.4. Sensors**

Here you can add, modify or delete Sensors. OSSIM on a computer is considered a Sensor.

### **3.4.5. Signatures**

A Signature is a group of Rules and any Rule can be associated with a Signature. A Signature is used to determine an Attack.

### **3.4.6. Priority & Reliability**

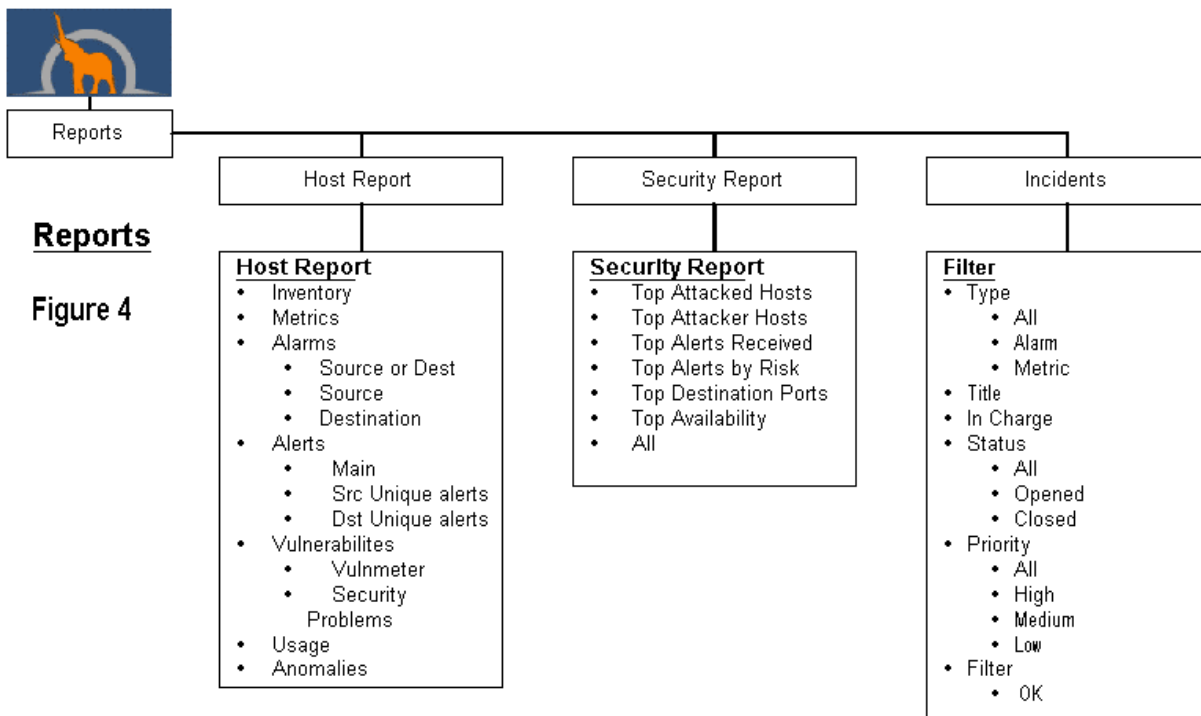
Here you can adjust the Priority and Reliability for each event generated by any given Plugin or Generator.

### **3.4.7. Ports**

Here you can modify the current Ports that are assigned to a Port Group. Setting UDP and TCP to zero selects all ports. A new Port Group can be setup to monitor certain UDP or TCP ports.



## 3.5. Reports



### Reports

Figure 4

The Reports tab provides basically three types of reports: Host, Security and Incidents.

### 3.5.1. Host Report

A report on Hosts that include reports from Nessus and Snort. From this Host report, it is expected that you fix the security holes that are reported and then re-scan with Nessus to update the report.

### 3.5.2. Security Report

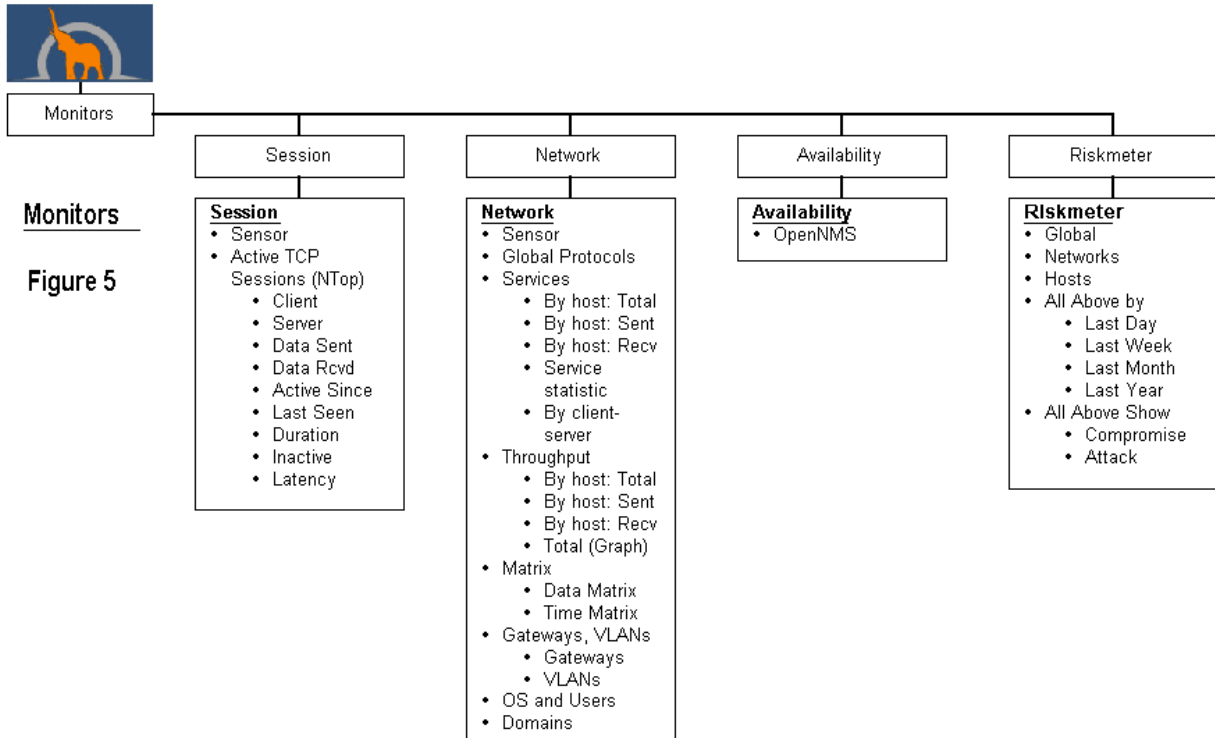
Is a report of the top attacked Hosts, top attackers, top Alerts and Availability. This is a very good overall report on your Attackers and most vulnerable Hosts.

### 3.5.3. Incidents

Are like trouble tickets that are generated by OSSIM that require a response or action.



### 3.6. Monitors



Monitors

Figure 5

Monitors provide real-time monitoring.

#### 3.6.1. Session & Network

Are the reports provided by NTop which displays all network traffic in real-time.

#### 3.6.2. Availability

Is a link to the OpenNMS Console. OpenNMS provides availability and monitoring statistics on Hosts.

#### 3.6.3. Riskmeter

Is OSSIM's calculated Risk by Global, Networks and Hosts.



### 3.7. Configuration

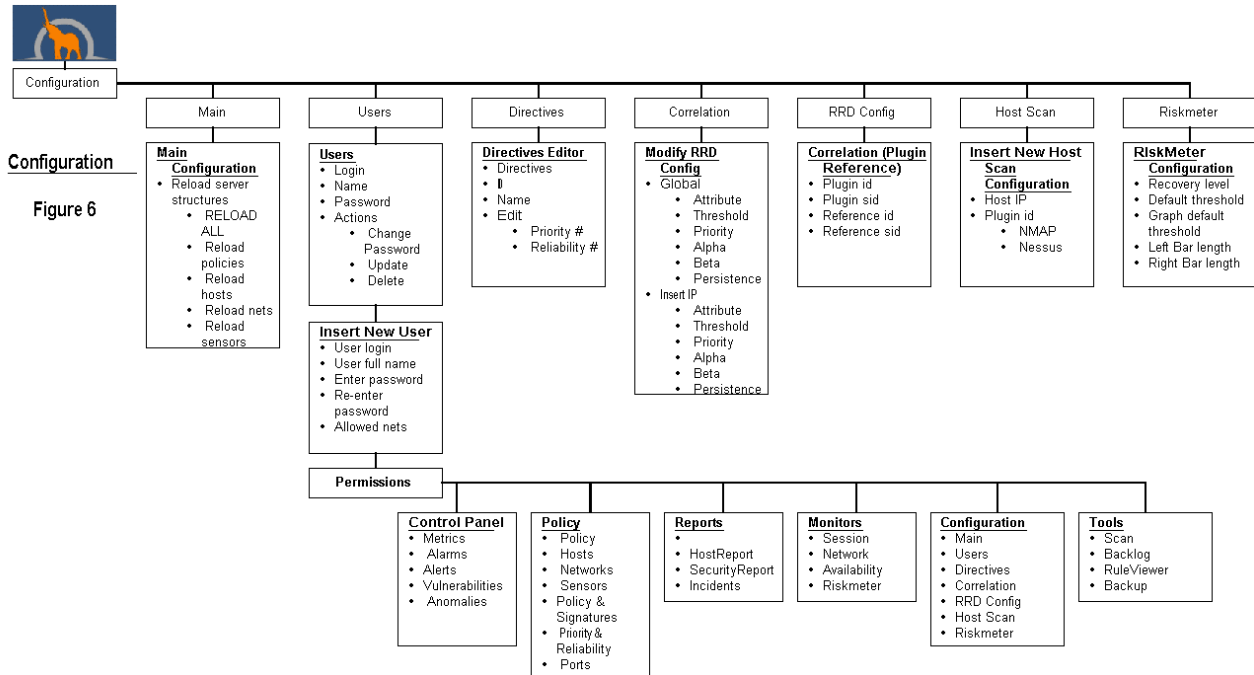


Figure 6

This is the main Configuration panel for OSSIM.

#### 3.7.1. Main

Provides the ability to reload any changes you have made.

#### 3.7.2. Users

Add, Delete Modify users. Users can be granted a granularity of access. This provides the ability to add Users who are only allowed to view reports and do not have the ability to modify or take action on alerts.

#### 3.7.3. Directives

Here you can edit the OSSIM Directives. Directives provide correlation between Rules. The Priority & Reliability of these Directives can also be modified from this panel.

#### 3.7.4. Correlation

View the correlation of Plugins between Snort and Nessus.



### 3.7.5. RRD Config

See Appendix 3 - RRD Attributes

Configure or modify the RRD Attributes. A time series is a fixed amount of time where packets with certain parameters log data to a Round Robin Database (RRD). RRD Attributes are used by RRDTool to log time series network packet information. NTop does this but OSSIM correlates RRD Anomalies with Snort Rules.

Here are the parameters that can be modified.

- Threshold: Absolute value above which is being alerted.
- Priority: Resulting impact if threshold is being exceeded.
- Alpha: Intercept adaptation parameter.
- Beta: Slope adaptation parameter.
- Persistence: How long has this event to last before we alert. (20 minutes)

### 3.7.6. Host Scan

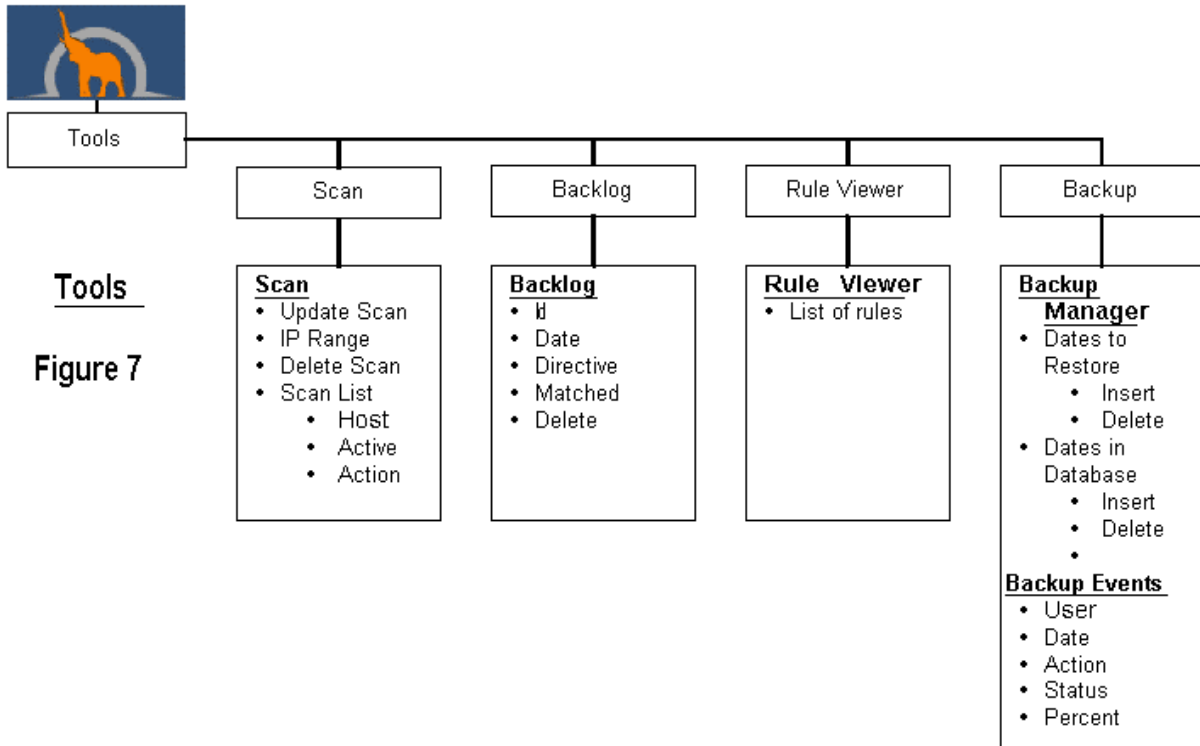
Add or delete a Host to be scanned by Nessus or NMAP.

### 3.7.7. Riskmeter

Configure the look of the Riskmeter graph.



## 3.8. Tools



**Tools**  
**Figure 7**

The Tools menu consists of a set of tools that provide Scan, Backlog, Rule Viewer and Backup.

### 3.8.1. Scan

Provides the ability to Scan a group of IP addresses. This is very useful in finding and adding Hosts. Once scanned the Hosts can be added to OSSIM. Setup Nessus scans.

### 3.8.2. Backlog

View Backlog of Alarms. Alarms can be sorted by ID, Date, Directive or Deleted. Backlog is Incidents that have been Closed or Deleted.

### 3.8.3. Rule Viewer

Provides the ability to view Snort Rules.

### 3.8.4. Backup

Backup or load a particular Snort database. Here you can add an archived database which has been previously archived by the script backupdb.pl. This script was added to the scheduled tasks (crontab -e) during the installation and was set to run once every day.



## 4. Configuring OSSIM

The best source to learn how to initially configure OSSIM is to use the Users Manual by Kevin Milne. This will configure OSSIM as one Sensor monitoring any Hosts on specified Networks.

In a more complex environment, additional Sensors and Plugins can be added to Hosts and devices (routers and firewalls) to monitor an enterprise.

Additionally, the OSSIM database or ACID database can be located on another system.

## 5. Using OSSIM

OSSIM is a comprehensive collection of many tools that can all be accessed independently. What OSSIM provides is:

- The correlation of different rules,
- Access of all the underlying tools,
- An overall view of Attacks and Compromises, and
- The generation of Incidents.



## 6. Glossary

Term	Association	Description
ACID	Alerts	A front-end web-based console to display results from Snort or other Generators.
Alarms	OSSIM, Snort	Are Alerts that exceed a threshold. In OSSIM usually correlated with other Alerts with the OSSIM Directives.
Alerts	OSSIM, Snort	Any sort of activity by an intruder that matches a Rule.
Alpha (RRD)	NTop	Intercept adaptation parameter.
Anomalies	OSSIM, Snort, RRD	A series of events over time that predict a pattern that is usually different from normal activities.
Arpwatch	Network	Arpwatch is a tool that monitors Ethernet activity and keeps a database of Ethernet/IP address pairings.
Asset (Value)	OSSIM	A Value between 0 (lowest) to 5 (highest) of a Host. This will be taken into account when OSSIM ranks Attacks and Compromises.
Attack	OSSIM, Snort	An electronic attack of a computer or network by an outside source. Attacks are attempts to breach computers and networks to obtain information about your networks and computers or to cause malicious damage by placing virus type software on your computers to disrupt the operation of your networks and computers.
Availability	OpenNMS	Percent of time that a Host or Network was available to applications and users.
Backlog	OSSIM	Previous Alarms.
Beta (RRD)	NTop	Slope adaptation parameter.
CALM	OSSIM	Compromise and Attack Level Monitor (CALM) is an assessment that uses event accumulation with recovery over time. Its input is a high volume of events and its output is a single indicator of the general state of security.
Compromise	OSSIM	A Host's security level has been Compromised by an Attack.



<b>Term</b>	<b>Association</b>	<b>Description</b>
Correlation	OSSIM	Correlation means the ability to view all events in all systems in one place and in the same format, and from this privileged vantage point compare and process the information, thereby allowing us to improve detection capabilities, prioritize events according to the context in which they occurred, and monitor the security situation of our network.
Destination	OSSIM, Snort	A network IP address and port that an attack is made on or information is sent to.
Detector Rules	OSSIM	Detector Rules are those received automatically from the agent as they are recorded. This includes Snort, Spade, Apache, etc.
Detectors		A program that processes information in real-time.
Directives	OSSIM	OSSIM uses Directives to correlate Alerts, Attacks and Compromises between various Alerts from Snort, Nessus and NTop.
External Network	Snort, NTop	Usually the Internet.
False Negatives	Snort	Alerts that are attacks that go unnoticed.
False Positives	Snort	Alerts that actually do not correspond to real attacks.
Gamma (RRD)	NTop	Seasonal adaptation parameter.
Global	OSSIM	Usually the whole network and systems that OSSIM is monitoring.
HIDS	Osiris	Host-based Intrusion Detection System (HIDS) usually monitors applications and operating systems (locally) on a computer.
Home Network	Snort	Your internal network which you are trying to protect.
Host	OSSIM	A computer that is added to OSSIM.
Host Report	OSSIM	A report provided by OSSIM that includes information and consolidation of reports from SNORT/ACID and Nessus.
ICMP	Network	Internet Control Message Protocol (ICMP) usually used to ping a computer to see if a particular network interface or



<b>Term</b>	<b>Association</b>	<b>Description</b>
		port is active. NMAP uses ICMP.
IDS	IDS	Intrusion Detection System, like OSSIM.
Immediate Risk	OSSIM	Usually real-time risks.
Incident	OSSIM	An Attack or Compromise that requires a response or resolution. Like a trouble ticket generated by OSSIM.
Intrinsic Risk	OSSIM	Measurement of the potential risk.
MAC	Network	A unique number of a network card.
Monitor Rules	NTop	Rules are real-time Monitoring Rules and are related to NTop.
NAT	Network	Network Address Translation (NAT) is the mapping of a Home Network mapped to an External Network.
Nessus	Scan	Software that scans a computer and provides a report that includes system information and potential system vulnerabilities.
NIDS	IDS	Network-based Intrusion Detection System, like OSSIM, monitors network traffic as it flows between computers and networks.
NMAP	Scan	Program that scans a computer to identify active and open ports.
OpenNMS	Monitor	Software that monitors computers and reports uptime and availability of hardware and software components.
OS	Hosts	Operating System
Osiris	HIDS	Host-based Intrusion Detection System (HIDS)
OSSIM Rule	OSSIM	A rule that is correlated with other sensors and rules to determine an attack or compromise.
Persistence (RRD)	NTop	The length of time of an Event.
Plugin	OSSIM	Software that provides monitoring and reports information back to a host program. Or a program that executes commands received from a host program.
Plugin ID	OSSIM, Snort	A unique identifier that corresponds with that program or entity that may generate events. In Snort, any event



<b>Term</b>	<b>Association</b>	<b>Description</b>
		generator.
Plugin SID	OSSIM, Snort	A unique identifier for each event that could be generated by any given Plugin (ID). For Snort's detection engine, individual Rules are also referenced as Plugin SIDs.
Policies	OSSIM	A group of rules that defines what action is to be taken.
Policy	OSSIM	A rule that defines what action is to be taken.
Port	Network	A unique number on a network adapter that a service will run on to communicate with either internal or external programs. Ports can be internal to a computer or external to other computers.
Port Group	Network	A group of Ports typically defined for the same purpose.
Preprocessors	Snort	A program that processes network packets prior to being sent to Snort, like Spade.
Priority	OSSIM	The importance of the Network or Host from 1 to 5 with 5 being the highest priority.
Protocol	Network	Network protocol, TCP, UDP, ICMP.
Reference ID	OSSIM	A unique ID number that identifies a Rule.
Reference SID	Snort	A Snort Rule (identified by the SID number) that is used as the reference for correlating attacks with other rules.
Reliability	OSSIM	The level of certainty of a detector when it receives a warning of a possible event.
Reload	OSSIM	Reloads the parameters and databases with the new values.
Risk Assessment	OSSIM	The evaluation of an event in relation to its associated risk and the probability that it is real.
Riskmeter	OSSIM	Graphical indication of Compromises and Attacks of Global (overall), Networks or Hosts.
RRD	NTop, OSSIM	Round Robin Database (RRD) is network packet data collected in a time series database by NTop.
Rule	Snort, Nessus	A rule used by Snort or Nessus.
Rule Viewer	OSSIM	An OSSIM component that allows you to view a Rule that



<b>Term</b>	<b>Association</b>	<b>Description</b>
		lists the Rule characteristics.
Scan	Nessus	Scanning of Networks or Hosts for computers done by Nessus providing a Vulnerability Report (see Vulnmeter).
Security Report	OSSIM	A summary report of Attacked Hosts, Attackers, Alerts Received and by Risk, Destination Ports and Availability.
Sensitivity	OSSIM	Capability of a detector with extensive and complex analysis of identifying possible attacks.
Sensor	OSSIM	Software either on the OSSIM system or on another Host or other node like a router that provides intrusion detection, anomaly detection or real time monitoring.
Session	NTop	NTop activity.
Signature	Snort	An algorithm that defines a type of attack. This Signature is used to identify attacks and type.
Signature Group	Snort	A group of Signatures.
Snort	Snort	Network-based Intrusion Detection System.
Source	OSSIM, Snort	The Source (network IP address and computer) of an Attack.
Spade	Snort	Statistical Packet Anomaly Detection Engine (SPADE) is a preprocessor for Snort that detects general packet anomalies.
TCP	Network	Transmission Control Protocol (TCP) network protocol is used for connection-oriented and reliable data transfer from source to destination. Most commonly used network protocol.
Threshold	OSSIM	A number that when exceeded will create an alternative action. Thresholds in OSSIM are varied depending on the threshold within each component.
UDP	Network	User Datagram Protocol (UDP) network protocol is used for connectionless data transfer.
Usage	NTop	Provides a summary report of Traffic, Protocols and Ports of a Host.
Vulnerabilities	Nessus	Report by Nessus of the security vulnerabilities of a Host.



Term	Association	Description
Vulnmeter	Nessus	Nessus scan results.



## 7. Appendixes

### 7.1. Appendix 1 - Signatures

Signatures in Snort.

Signatures			
attack-responses	fw1-reject	policy	virus
backdoor	icmp	pop2	web-attacks
bad-traffic	icmp-info	pop3	web-cgi
chat	imap	porn	web-client
ddos	info	rpc	web-coldfusion
deleted	local	rservices	web-frontpage
dns	misc	scan	web-iis
dos	multimedia	shellcode	web-misc
experimental	mysql	smtp	web-php
exploit	netbios	snmp	x11
finger	nntp	spade	
ftp	oracle	sql	
fw1-accept	other-ids	telnet	
fw1-drop	p2p	tftp	

Non-official bleeding Snort Signatures:

- bleeding.rules.
- bleeding-malware.rules.
- bleeding-virus.rules.



## 7.2. Appendix 2 - Directives

Directives are used by OSSIM to correlate various Rules to create Alarms.

Directives		
Id Name	Id Name	Id Name
1 Possible intrusion	24032 Possible Bunker-Hill trojan	24073 Possible CDK Trojan
2 Possible Trojan	24033 Possible Taskman trojan	24074 Possible SniperNet trojan
3 Web attack	24034 Possible Eclipse trojan	24075 Possible DP trojan
4 Possible Worm	24035 Possible Enterprise trojan	24076 Possible GayOL trojan
5 Possible Plague	24036 Possible Storm backdoor	24077 Possible AimSpy trojan
6 Peer anomaly. Worm ? P2P ?	24037 Possible Prosiak trojan	24078 Possible Dark Shadow trojan
7 Strange host behaviour	24038 Possible Exploiter exploit	24079 Possible Direct Connection trojan
8 Strange global behaviour	24039 Possible NetRaider trojan	24080 Possible Bowl trojan
9 Compromised host compromising other host	24040 Sockets des Troie trojan	24081 Possible Le Gardien trojan
10 Possible Worm port 80	24041 Possible Death trojan	24082 Possible Vampire trojan
24001 Possible Doly Trojan	24042 Possible Senna Spy FTP Server exploit	24083 Possible Jade trojan
24002 Possible SubSeven Trojan	24043 Possible Shaft trojan	24084 Possible Remote Storm trojan
24003 Possible GateCrasher Trojan	24044 Agent 40421 backdoor	24085 Possible Multidropper trojan
24004 Possible DoomJuice Trojan	24045 Possible DRAT backdoor	24086 Possible BLA Trojan
24005 Possible Netbus Trojan	24046 Possible DMSetup trojan	24087 Possible Rasmin trojan
24006 Possible DeepThroat Trojan	24047 Possible RemoConChubo trojan	24088 Possible MiniCommand trojan
24007 Possible Dagger Trojan	24048 Possible ProMail trojan	24089 Possible The Thief trojan
24008 Possible Infector Trojan	24049 Possible Happy99 backdoor	24090 Possible Xtreme trojan
24009 Possible HackAttack Trojan	24050 Possible Tiny Telnet Server	24091 Possible Orion backdoor
24010 Possible Girlfriendaccess Trojan	24051 Possible I love You virus	24092 Possible Kaos trojan
24011 Possible WinHole backdoor	24052 Possible Matrix trojan	24093 Possible VooDoo Doll trojan
24012 Possible Remote Administrator Tool	24053 Possible CDK trojan	24094 Possible Scarab trojan
24013 Possible Contact trojan	24054 Possible CGI Backdoor	24095 Possible Project nEXT trojan
24014 Possible NetSphere Trojan	24055 Possible Hidden Port trojan	24096 Possible PhaseZero Trojan
24015 Possible Terror Trojan	24056 Possible Kazimas trojan	24097 Possible NETrojan trojan
24016 Possible PC Crasher trojan	24057 Possible God Message worm	24098 Possible Millenium Worm
24017 Possible Bad Blood trojan	24058 Possible Net Controller trojan	24099 Possible Trinoo trojan
24018 Possible NetMonitor trojan	24059 Possible Farnaz trojan	24100 Possible SpySender trojan
24019 Possible Glacier trojan	24060 Possible Chode trojan	24101 Possible w00w00 Trojan
24020 Possible Portal of Doom trojan	24061 Possible NetTaxi trojan	24102 Possible HidePark Trojan
24021 Possible InCommand trojan	24062 Possible WinCrash Trojan	24103 Possible HideSource Trojan
24022 Possible Host Control trojan	24063 Possible A-Trojan	24104 Possible Hack-a-tack Trojan
24023 Possible PC Invader backdoor	24064 Possible Backage trojan	24105 Possible Fragroute Trojan
24024 Net Demon backdoor	24065 Possible Breach trojan	24106 Possible win-trin00 Trojan
24025 Possible SubZero backdoor	24066 Possible TCP Wrappers trojan	24107 Possible Trinity Trojan
24026 Possible CrazyNet trojan	24067 Possible Hackers Paradise trojan	24108 Possible Remote PC Trojan
24027 Possible Chupacabra trojan	24068 Possible RPC Backdoor	24109 Possible Typot Trojan
24028 Possible Moonpie backdoor	24069 Possible Fatal Connections trojan	
24029 Possible BackConstruction Trojan	24070 Possible Net666 trojan	
24030 Possible NetMetro Trojan	24071 Possible 711 trojan	
24031 Possible Back Orifice 2000 backdoor	24072 Possible Secret Service trojan	



### 7.3. Appendix 3 - RRD Attributes

RRD Attributes are used by RRDTOOL to log time series network packet information. NTop does this but OSSIM correlates RRD Anomalies with Snort Rules.

RRD Attributes	
activeHostSendersNum	IP_SSHBytes
arpRarpBytes	IP_TelnetBytes
broadcastPkts	IP_WinMXBytes
ethernetBytes	IP_X11Bytes
ethernetPkts	knownHostsNum
fragmentedIpBytes	mail_sessions
icmpBytes	multicastPkts
igmpBytes	nb_sessions
ipBytes	otherBytes
ipv6Bytes	otherIpBytes
ipxBytes	stpBytes
IP_DHCP-BOOTPBytes	synPktsRcvd
IP_DNSBytes	synPktsSent
IP_eDonkeyBytes	tcpBytes
IP_FTPBytes	totContactedRcvdPeers
IP_GnutellaBytes	totContactedSentPeers
IP_HTTPBytes	udpBytes
IP_KazaaBytes	upTo1024Pkts
IP_MailBytes	upTo128Pkts
IP_MessengerBytes	upTo1518Pkts
IP_NBios-IPBytes	upTo256Pkts
IP_NFSBytes	upTo512Pkts
IP_NNTPBytes	upTo64Pkts
IP_SNMPBytes	web_sessions



## 7.4. Appendix 4 – Plugin IDs

Here is a listing of all currently supported Plugin IDs.

Priority and Reliability Detectors			
Id	Name	Type	Description
1001	snort	Detector (1)	Snort Rules
1002	snort_tag	Detector (1)	Snort Tagging
1100	spp_portscan	Detector (1)	Portscan1
1101	spp_minfrag	Detector (1)	Minfrag
1102	http_decode	Detector (1)	HTTP decode ½
1103	spp_defrag	Detector (1)	First defragmenter
1104	spp_anomsensor	Detector (1)	SPADE
1105	spp_bo	Detector (1)	Back Orifice
1106	spp_rpc_decode	Detector (1)	RPC Preprocessor
1107	spp_stream2	Detector (1)	2nd stream preprocessor
1108	spp_stream3	Detector (1)	3rd stream preprocessor
1109	spp_telnet	Detector (1)	Telnet option decoder
1110	spp_unidecode	Detector (1)	Unicode decoder
1111	spp_stream4	Detector (1)	Stream4 preprocessor
1112	spp_arpspoof	Detector (1)	Arp Spoof detector
1113	spp_frag2	Detector (1)	2nd fragment preprocessor
1114	spp_fnord	Detector (1)	NOP detector
1115	spp_asn1	Detector (1)	ASN.1 Validator
1116	snort_decoder	Detector (1)	Snort Internal Decoder
1117	spp_portscan2	Detector (1)	Portscan2
1118	spp_conversation	Detector (1)	Conversation
1119	spp_tba	Detector (1)	TBA
1120	spp_tba2	Detector (1)	TBA
1121	spp_snmp	Detector (1)	SNMP decoder
1501	apache	Detector (1)	Apache
1502	iis	Detector (1)	IIS
1503	iptables	Detector (1)	Iptables
1504	fw1	Detector (1)	FW1
1506	realsecure	Detector (1)	Real Secure
1507	rrd_threshold	Detector (1)	RRD Threshold
1508	rrd_anomaly	Detector (1)	RRD Anomaly
1509	threshold	Detector (1)	Threshold exceeded
1510	cisco	Detector (1)	Cisco router
1511	p0f	Detector (1)	Passive OS fingerprinting tool
1512	arpwatch	Detector (1)	Ethernet/FDDI station monitor daemon
3001	nessus	Other (3)	Nessus
3002	nmap	Other (3)	Nmap



## 7.5. Appendix 5 - Screenshots

Here are a few screenshots of OSSIM. Hopefully this will provide a better perspective of the features of OSSIM.

### 7.5.1. ACID

<input type="checkbox"/>	ID	<Signature>	<Timestamp>	<Source Address>	<Dest. Address>	<Asst>	<Prio>	<Risk>	<Rel>	<Layer 4 Proto>
<input type="checkbox"/>	#0-(13-15894744)	[cve][icat][arachNIDS][snort] ICMP redirect host	2004-08-31 11:56:04	192.168.2.1	192.168.2.203	--	--	--	--	ICMP
<input type="checkbox"/>	#1-(13-15894743)	url[snort] BLEEDING-EDGE P2P ed2k file request answer	2004-08-31 11:56:03	[redacted]:8886	192.168.2.203:63401	--	--	--	--	TCP
<input type="checkbox"/>	#2-(13-15894724)	[cve][icat][arachNIDS][snort] ICMP redirect host	2004-08-31 11:56:01	192.168.2.1	192.168.2.203	2	1	0	1	ICMP
<input type="checkbox"/>	#3-(13-15894742)	[snort] Spade: Non-live dest used	2004-08-31 11:56:00	192.168.2.203:21183	[redacted]:7854	2	1	0	1	UDP
<input type="checkbox"/>	#4-(13-15894741)	[snort] Spade: Non-live dest used	2004-08-31 11:56:00	192.168.2.203:21183	[redacted]:10202	2	1	0	1	UDP
<input type="checkbox"/>	#5-(13-15894740)	[snort] Spade: Non-live dest used	2004-08-31 11:56:00	192.168.2.203:21183	[redacted]:7830	2	1	0	1	UDP
<input type="checkbox"/>	#6-(13-15894739)	[snort] Spade: Non-live dest used	2004-08-31 11:56:00	192.168.2.203:21183	[redacted]:7854	2	1	0	1	UDP
<input type="checkbox"/>	#7-(13-15894738)	[snort] Spade: Non-live dest used	2004-08-31 11:56:00	192.168.2.203:21183	[redacted]:10202	2	1	0	1	UDP
<input type="checkbox"/>	#8-(13-15894737)	[snort] Spade: Non-live dest used	2004-08-31 11:56:00	192.168.2.203:21183	[redacted]:7830	2	1	0	1	UDP
<input type="checkbox"/>	#9-(13-15894736)	[snort] Spade: Rare but open dest port used	2004-08-31 11:56:00	192.168.2.203:21183	[redacted]:7854	2	3	1	1	UDP
<input type="checkbox"/>	#10-(13-15894735)	[snort] Spade: Rare but open dest port used	2004-08-31 11:56:00	192.168.2.203:21183	[redacted]:6540	2	3	1	1	UDP



## 7.5.2. ACID Detail

<b>Meta</b>	<b>ID #</b>	<b>Time</b>		<b>Triggered Signature</b>													
	13 - 15894743	2004-08-31 11:56:03		url[snort] BLEEDING-EDGE P2P ed2k file request answer													
	<b>Sensor</b>	<b>name</b>	<b>interface</b>	<b>filter</b>													
	192.168.2.175	eth0	none														
	<b>Alert Group</b>	none															
<b>IP</b>	<b>source addr</b>	<b>dest addr</b>	<b>Ver</b>	<b>Hdr Len</b>	<b>TOS</b>	<b>length</b>	<b>ID</b>	<b>flags</b>	<b>offset</b>	<b>TTL</b>	<b>chksum</b>						
	8	192.168.2.203	4	5	0	132	51753	0	0	111	58538						
	<b>FQDN</b>	<b>Source Name</b>		<b>Dest. Name</b>													
	p83.129.69.171.tisdip.tiscali.de		Unable to resolve address														
	<b>Options</b>	none															
<b>TCP</b>	<b>source port</b>	<b>dest port</b>	<b>R1</b>	<b>R0</b>	<b>URG</b>	<b>ACK</b>	<b>PSH</b>	<b>SYN</b>	<b>FIN</b>	<b>seq #</b>	<b>ack</b>	<b>offset</b>	<b>res</b>	<b>window</b>	<b>urp</b>	<b>chksum</b>	
	8886	63401			X	X				1569411353	3375174684	5	0	32550	0	56818	
	<b>Options</b>	none															
<b>Payload</b>	length = 92																
	<pre> 000 : E3 3F 00 00 00 59 DC 7D EC D9 2E F8 D9 B3 02 D7 .?...Y.)..... 010 : B5 73 9B C3 24 16 2C 00 70 69 6E 6B 5F 74 72 79 .s..\$.pink_try 020 : 5F 74 68 69 73 5F 72 65 74 61 69 6C 5F 66 6F 72 _this_retail_for 030 : 5F 77 77 77 2E 67 6F 6C 64 65 73 65 6C 2E 74 6F _www.goldesel.to 040 : 2E 72 61 72 E3 13 00 00 50 DC 7D EC D9 2E F8 .rar.....P.).... 050 : D9 B3 02 D7 B5 73 9B C3 24 16 00 00 .....s.\$... </pre>																



### 7.5.3. ACID Search

[ Back ]

**Meta Criteria**

Sensor: { any sensor } | Alert Group: { any Alert Group }

Signature: { signature } = { }  
Classification: { any Classification }

Alert Time: { time } { month } { year } : : : ADD Time

Priority: Risk: { any risk } | Priority: { any Priority } | Type: { any }  
Asset: { any Asset } | Reliability: { any Reliability }

**IP Criteria**

Address: { address } = { } ADD Addr

Misc: { field } = { } ADD IP Field

Layer-4: TCP | UDP | ICMP

**Payload Criteria**

Input Criteria Encoding Type: { Encoding } | Convert To (when searching): { Convert To }

{ payload } ADD Payload

Sort order: none | timestamp (ascend) | timestamp (descend) | signature  
Query DB

[Loaded in 0 seconds]

ACID v0.9.6b23 ( by Roman Danyliw as part of the AirCERT project )

### 7.5.4. Alarm Console

20	Possible Worm	2	2004-06-17 17:43:39	2004-06-17 17:44:54	:137	:137	Ack
21	Possible Worm	2	2004-06-17 15:52:39	2004-06-17 15:54:43	:33240	:139	Ack
22	Possible Worm	2	2004-06-17 15:45:40	2004-06-17 15:46:35	1:0:137	:137	Ack
23	Possible Worm	2	2004-06-17 13:25:18	2004-06-17 13:27:56	:137	:137	Ack
24	Possible Worm	2	2004-06-17 11:56:43	2004-06-17 11:57:45	srta_pepis:4204	Kotri:445	Ack
25	Possible Worm	2	2004-06-17 11:56:42	2004-06-17 11:57:37	srta_pepis:4201	1:139	Ack
2004-06-16							
26	Possible Worm	4	2004-06-16 11:34:44	2004-06-16 11:45:26	infected:46596	:445	Ack
27	Possible Worm	2	2004-06-16 09:50:31	2004-06-16 09:51:17	:36454	:445	Ack
28	Possible Worm	2	2004-06-16 09:49:44	2004-06-16 09:50:49	kaneda:3911	:445	Ack
29	Possible Worm	2	2004-06-16 09:49:41	2004-06-16 09:50:41	kaneda:3912	1:139	Ack
30	Possible Worm	2	2004-06-16 09:50:10	2004-06-16 09:50:21	:35975	:30	Ack
31	Possible Worm	2	2004-06-16 09:43:41	2004-06-16 09:44:19	infected:35642	:445	Ack
32	Possible Worm	2	2004-06-16 09:39:14	2004-06-16 09:40:13	infected:63754	:445	Ack
2004-06-15							
33	SHELLCODE x86 inc ebx NOOP	3	2004-06-15 16:18:01	2004-06-15 16:18:01	:1382	kaneda:445	Ack
2004-06-10							
34	SHELLCODE x86 inc ebx NOOP	3	2004-06-10 13:58:18	2004-06-10 13:58:18	:139	:4847	Ack
35	SHELLCODE x86 inc ebx NOOP	3	2004-06-10 13:35:27	2004-06-10 13:35:27	1:1040	kaneda:139	Ack
36	Possible Worm port 80	8	2004-06-10 10:42:17	2004-06-10 11:22:09	infected:40630	:445	Ack



## 7.5.5. Directives 1

Rules (Directive 1)										
Name	Priority	Reliability	Time_out	Occurrence	From	To	Port_from	Port_to	Plugin ID	Plugin SID
Intrusion rule matched		1		1	ANY	ANY	ANY	ANY	snort (1001)	113 122 124 126 128 131 133 134 135 136 137 138 140 142 143 149 156 159 166 167 168 169 170 171 172 173 174 175 179 180 181 182 186 187 188 189 190 191 192 193 194 196 197 198 199 200 201 202 203 204 205 206 207 258 268 272 273 275 276 277 278 287 289 293 295 296 297 298 299 318 319 333 337 338 340 341 342 343 345 346 348 349 350 351 352 353 361 363 569 570 571 573 647 650 652 653 656 657 674 675 690 695 696 697 698 699 700 701 702 703 704 705 707 1274 1276 1277 1278 1282 1289 1293 1294 1295 1296 1297 1326 1327 1377 1378 1379 1409 1421 1424 1634 1635 1755 1780 1792 1821 1842 1844 1845 1902 1903 1904 1919 1920 1930 1934 1936 1937 1938 1972 1973 1974 1976 1993 2190 2191 2192
More than 10 secs persistence		+4	30		1:SRC_IP	1:DST_IP	1:SRC_PORT	1:DST_PORT	tcptrack (2006)	3
More than 5 min. persistence		+3	500		1:SRC_IP	1:DST_IP	1:SRC_PORT	1:DST_PORT	tcptrack (2006)	3
Attacked host's C raised		+3	600		1:DST_IP				ossim (2001)	1
Attack response		+5	10		1:DST_IP	1:SRC_IP	1:DST_PORT	1:SRC_PORT	snort (1001)	125 127 129 130 132 148 150 154 163 164 165 177 1464 1882 1900 1901 2123
More than 5 min. persistence		+3	500		1:SRC_IP	1:DST_IP	1:SRC_PORT	1:DST_PORT	tcptrack (2006)	3
Attacked host's C raised		+3	600		1:DST_IP				ossim (2001)	1

## 7.5.6. Directives 2

[Control Panel >] [Policy >] [Reports >] [Monitors >] [Configuration >] [Tools >] [Logout]  
 [Main] [Users] [Directives] [Correlation] [RRD Config] [Host Scan] [Riskmeter]

Directives list

Generic ossim

Id	Name
1	Possible intrusion
2	Possible Trojan
3	Web attack
4	Possible Worm
5	Possible Plague
6	Peer anomaly. Worm ? P2P ?
7	Strange host behaviour
8	Strange global behaviour
9	Compromised host compromising other host
10	Possible Worm port 80

Trojans

Directives Editor

Edit New

Rules (Directive 1)										
Name	Priority	Reliability	Time_out	Occurrence	From	To	Port_from	Port_to	Plugin ID	Plugin SID
Intrusion rule matched		1		1	ANY	ANY	ANY	ANY	snort (1001)	Expand / Collapse
More than 10 secs persistence		+4	30		1:SRC_IP	1:DST_IP	1:SRC_PORT	1:DST_PORT	ntop (2005)	248
More than 5 min. persistence		+3	500		1:SRC_IP	1:DST_IP	1:SRC_PORT	1:DST_PORT	ntop (2005)	248
Attacked host's C raised		+3	600		1:DST_IP				ossim (2001)	1
Attack response		+5	10		1:DST_IP	1:SRC_IP	1:DST_PORT	1:SRC_PORT	snort (1001)	125 127 129 130 132 148 150 154 163 164 165 177 1464 1882 1900 1901 2123
More than 5 min. persistence		+3	500		1:SRC_IP	1:DST_IP	1:SRC_PORT	1:DST_PORT	ntop (2005)	248
Attacked host's C raised		+3	600		1:DST_IP				ossim (2001)	1



## 7.5.7. Incidents 1

[Control Panel >] [Policy >] [Reports >] [Monitors >] [Configuration >] [Tools >] [Logout]  
 [Host Report] [Security Report] [Incidents]

### Incidents

Filter					
Type	Title	In charge	Status	Priority	Filter
ALL			ALL	ALL	OK
Alarm			Open	High	
Metric			Closed	Medium	
				Low	

Ticket	Date	Last Modification	Title	In Charge	Status	Priority
MET010	2004-08-25 15:00:50	2004-08-25 15:00:50	Metric Threshold: C level exceeded (Net red_interna)	admin	Open	4
ALA07	2004-08-25 14:15:34	2004-08-30 11:19:59	Possible Worm	dfgh	Open	6
MET06	2004-08-25 12:03:46	2004-08-25 12:04:35	Metric Threshold: C level exceeded (Net red_interna)	rEDES	Open	1
ALA05	2004-08-25 11:29:31	2004-08-25 11:29:31	Possible intrusion	Refde	Open	3
ALA04	2004-08-25 09:30:52	2004-08-25 09:30:52	Possible intrusion	admin	Open	8
ALA03	2004-08-25 09:19:40	2004-08-25 09:19:40	BACKDOOR DeepThroat 3.1 E-Mail Info From Server	admin	Open	5
MET01	2004-08-24 11:50:15	2004-08-24 11:50:15	Metric Threshold: A level exceeded (Host 192.168.2.77)	admin	Open	2

## 7.5.8. Incidents 2

[Control Panel >] [Policy >] [Reports >] [Monitors >] [Configuration >] [Tools >] [Logout]  
 [Host Report] [Security Report] [Incidents]

Ticket	Incident	In Charge	Status	Priority	Action
MET01	Name: Metric Threshold: A level exceeded (Host 192.168.2.77) Type: Metric Target: Host 192.168.2.77 - Metric Type: Attack - Metric Value: 851	admin	Open	2	Edit Delete

Date	User / Description / Action	Priority	Status	In Charge	Transferred	Copy	Action
2004-08-24 11:50:15	User: admin Description: Metric Threshold: A level exceeded (Host 192.168.2.77) Action:	2	Open	admin	-	-	Increase Priority Decrease Priority Close Delete
Tuesday 31-Aug-2004	Description <input type="text"/> Action <input type="text"/>	Priority 2	status Open	In charge: admin Transfer <input type="text"/> Copy (e-mail) <input type="text"/>			Add



## 7.5.9. Inventory 1

### Inventory - 192.168.14.135

Host Info	
Name	hkgnts40dpt01
Ip	<b>192.168.14.135</b>
Operating System	Windows NT 4.0
MAC	0:30:6e:21:62:fb
Netbios Name	HKGNTS40DPT01
Netbios Work Group	PEEHK
Host belongs to:	
Net	hkg
Sensor	ossim-server-an
Port / Service iformation (Active) [ update ]	
Service	Version
http (80/tcp)	Microsoft IIS webserver 4.0
msrpc? (135/tcp)	
netbios-ssn (139/tcp)	
https? (443/tcp)	
http-rpc-epmap? (593/tcp)	
vnc-http (5800/tcp)	WinVNC (Server: hkgnts40dpt01; Resolution 640x512; VNC TCP port: 5900; May be standard or TightVNC)
vnc (5900/tcp)	VNC (protocol 3.3)
VeritasBackupExec? (6101/tcp)	
RETS-or-BackupExec? (6103/tcp)	
irc? (6667/tcp)	
irc? (6668/tcp)	



## 7.5.10. Inventory 2

Host Report

Inventory - 192.168.1.103

**Inventory**

Metrics

Alarms

Source or Dest  
Source  
Destination

Alerts

Main  
Src Unique alerts  
Dst Unique alerts

Vulnerabilites

Vulnmeter  
Security Problems

Usage

Anomalies

Host Info	
Name	Pruebas Fabio
Ip	192.168.1.103
Operating System	Linux 2.4/2.6
MAC	0:50:fc:a6:e2:96 Edimax Technology Co., Ltd.
Host belongs to:	
Net	Red_Interna
Sensor	elefante
Sensor	golgotha
Active services and aplicacions names/versions	
Service	Version
http	Apache httpd 2.0.48 ((Fedora))
mysql	MySQL (unauthorized)
netbios-ssn	Samba smbdc 3.X (workgroup: IPSOLUCIONES)
rpcbind	2 (rpc #100000)
ssh	OpenSSH 3.6.1p2 (protocol 1.99)
status	1 (rpc #100024)

## 7.5.11. Metrics 1

[Last Day] [Last Week] [Last Month] [Last Year]

Riskmeter	Service Level
	76.45%

Global				Global			
Global	Max C date	Max C	Current C	Global	Max A date	Max A	Current A
GLOBAL SCORE	2004-06-16 10:00:00	28534	768	GLOBAL SCORE	2004-06-16 10:00:00	28567	0

Networks				Networks			
Network	Max C date	Max C	Current C	Network	Max A date	Max A	Current A
red_bilbao	2004-06-18 14:00:00	0	0	red_bilbao	2004-06-18 14:00:00	0	0
red_interna	2004-06-17 18:00:00	9189	2864	red_interna	2004-06-16 10:00:00	36770	1666
dmz	2004-06-15 18:30:00	1216	0	dmz	2004-06-14 11:00:00	0	0

Hosts				Hosts			
Host	Max C date	Max C	Current C	Host	Max A date	Max A	Current A
Router	2004-06-17 18:00:00	4404	766	srta_pepis	2004-06-17 18:00:00	309	0
infected	2004-06-16 13:00:00	2694	0		2004-06-17 14:30:00	526	0
golgotha	2004-06-16 13:00:00	1491	0		2004-06-17 13:30:00	512	0
	2004-06-16 09:30:00	1343	0	wayreth	2004-06-16 13:00:00	1023	0
correo	2004-06-15 18:30:00	1210	0	golgotha	2004-06-16 12:00:00	2147	0
	2004-06-15 17:00:00	615	2		2004-06-16 09:30:00	28540	0



## 7.5.12. Metrics 2

Applications Actions Tue Aug 31, 11:38

OSSIM

File Edit View Go Bookmarks Tabs Help

Back Home http://192.168.2.175/ossim/top.php?menu=control\_panel Go Find

[Control Panel] [Policy] [Reports] [Monitors] [Configuration] [Tools] [Logout]  
 [Metrics] [Alarms] [Alerts] [Vulnerabilities] [Anomalies]

### Metrics

[Last Day] [Last Week] [Last Month] [Last Year]

Riskmeter		Service Level	
73.69%			

#### Global

Global	Max C date	Max C	Current C	Global	Max A date	Max A	Current A
GLOBAL SCORE [i]	2004-08-30 16:45:00	8128	614	GLOBAL SCORE [i]	2004-08-30 16:45:00	889	3

#### Networks

Network	Max C date	Max C	Current C	Network	Max A date	Max A	Current A
red_dmz [i]	2004-08-30 23:00:00	1	0	red_dmz [i]	2004-08-30 23:00:00	1	0
red_interna [i]	2004-08-30 16:45:00	12309	983	red_interna [i]	2004-08-30 15:30:00	1689	0
red_sancha [i]	2004-08-30 16:45:00	12278	976	red_sancha [i]	2004-08-30 15:30:00	1686	0

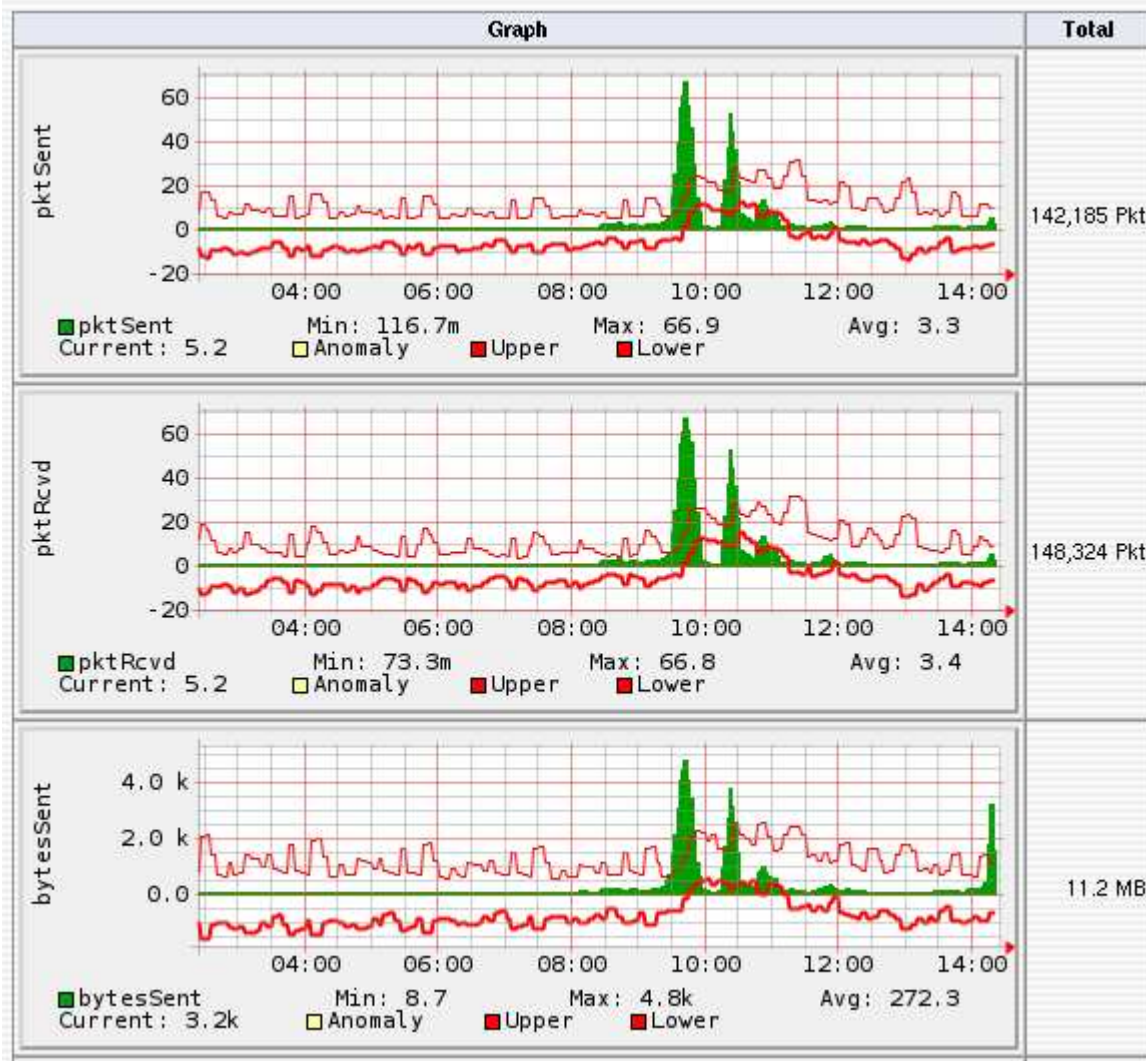
#### Hosts

Host	Max C date	Max C	Current C	Host	Max A date	Max A	Current A
192.168.2.159 [i]	2004-08-30 16:45:00	738	0	DK [i]	2004-08-30 15:20:00	451	0
DK [i]	2004-08-30 15:35:00	7651	611				

dgil@golgotha: /opt/ossim/www/ses X-Chat [2.0.10]: dgil@kornbluth.free OSSIM



### 7.5.13. NTop RRD





## 7.5.14. NTop Services

Network Traffic [TCP/IP]: Local Hosts - Data Sent+Received																			
Hosts: [All] [Local Only] [Remote Only]																			Data: [All] [Sent Only] [Received Only]
Host	Domain	Data	FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS/AFS	X11	SSH	Gnutella	Kazaa	WinMX		
192.168.2.175		155.1 MB 33.4 %	8.1 KB	11.8 MB	129.6 MB	0	276	75.8 KB	0	74	74	148	222	11.7 MB	74	0	0		
golgotha	Local	154.7 MB 33.3 %	53.9 KB	111.6 MB	19.1 MB	0	0	0	0	0	0	15.3 MB	0	5.0 MB	0	0	0		
	Local	134.8 MB 29.0 %	0	7.6 KB	133.4 MB	0	988.9 KB	0	298.6 KB	0	0	0	0	0	0	0	0		
wayreth	Local	15.1 MB 3.2 %	0	0	14.8 MB	0	252.7 KB	0	0	0	0	0	0	0	0	0	0		
192.168.2.119		4.3 MB 0.9 %	0	2.2 MB	0	0	0	0	0	0	0	0	0	787.0 KB	0	0	0		
192.168.2.33		241.1 KB 0.1 %	0	0	0	0	241.1 KB	0	0	0	0	0	0	0	0	0	0		
192.168.2.200		236.6 KB 0.0 %	0	356	0	0	233.5 KB	0	0	0	0	0	0	0	0	0	0		
192.168.2.200		235.9 KB 0.0 %	0	444	141	0	235.1 KB	0	0	0	0	0	0	148	0	0	0		
harpo	Local	230.7 KB 0.0 %	0	0	0	0	230.7 KB	0	0	0	0	0	0	0	0	0	0		
memnon [NetBIOS]		68.6 KB 0.0 %	0	0	0	0	8.4 KB	0	0	0	0	0	0	0	0	0	0		
midkemia	Local	17.8 KB 0.0 %	0	60	0	0	17.8 KB	0	0	0	0	0	0	0	0	0	0		
d5qd101j	Local	13.8 KB 0.0 %	0	0	0	0	12.4 KB	0	1.3 KB	0	0	0	0	0	0	0	0		
carmen	Local	4.5 KB 0.0 %	0	0	0	0	4.5 KB	0	0	0	0	0	0	0	0	0	0		
portatil-oscar	Local	3.6 KB 0.0 %	0	0	0	0	3.6 KB	0	0	0	0	0	0	0	0	0	0		
port-icabrera	Local	1.7 KB 0.0 %	0	0	0	0	1.7 KB	0	0	0	0	0	0	0	0	0	0		
srtapepis [NetBIOS]		1.2 KB 0.0 %	0	0	0	0	1.2 KB	0	0	0	0	0	0	0	0	0	0		
jj [NetBIOS]		854 0.0 %	0	0	0	0	854	0	0	0	0	0	0	0	0	0	0		
192.168.2.203		480 0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
cosa2	Local	335 0.0 %	0	0	0	0	335	0	0	0	0	0	0	0	0	0	0		
atrullas	Local	335 0.0 %	0	0	0	0	335	0	0	0	0	0	0	0	0	0	0		
192.168.2.98		118 0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		

## 7.5.15. NTop Sessions

[Control Panel >] [Policy >] [Reports >] [Monitors >] [Configuration >] [Tools >] [Logout]  
 [Session] [Network] [Availability] [Riskmeter]

Sensor: Net: Interna

wayreth (192.168.2.69)

Client	Server	Data Sent	Data Rcvd	Active Since	Last Seen	Duration	Inactive	Latency
wayreth :37347	golgotha :ssh	920	7.8 KB	Tue Aug 31 13:58:37 2004	Tue Aug 31 13:58:39 2004	2 sec	2:11	
wayreth :38505	golgotha :www	4.3 KB	12.1 KB	Tue Aug 31 14:00:33 2004	Tue Aug 31 14:00:46 2004	13 sec	4 sec	0.2 ms
wayreth :38506	golgotha :www	3.1 KB	13.2 KB	Tue Aug 31 14:00:37 2004	Tue Aug 31 14:00:47 2004	10 sec	3 sec	0.2 ms

golgotha (192.168.2.97)

Client	Server	Data Sent	Data Rcvd	Active Since	Last Seen	Duration	Inactive	Latency
wayreth :37347	golgotha :ssh	920	7.8 KB	Tue Aug 31 13:58:37 2004	Tue Aug 31 13:58:39 2004	2 sec	2:13	
wayreth :38505	golgotha :www	4.3 KB	12.1 KB	Tue Aug 31 14:00:33 2004	Tue Aug 31 14:00:46 2004	13 sec	6 sec	0.2 ms
wayreth :38506	golgotha :www	3.1 KB	13.2 KB	Tue Aug 31 14:00:37 2004	Tue Aug 31 14:00:47 2004	10 sec	5 sec	0.2 ms
golgotha :33332	irc.freenode.net :ircd	735.0 KB	2.1 MB	Mon Aug 30 08:30:01 2004	Tue Aug 31 14:00:48 2004	1 day 5:30:47	4 sec	47.7 ms

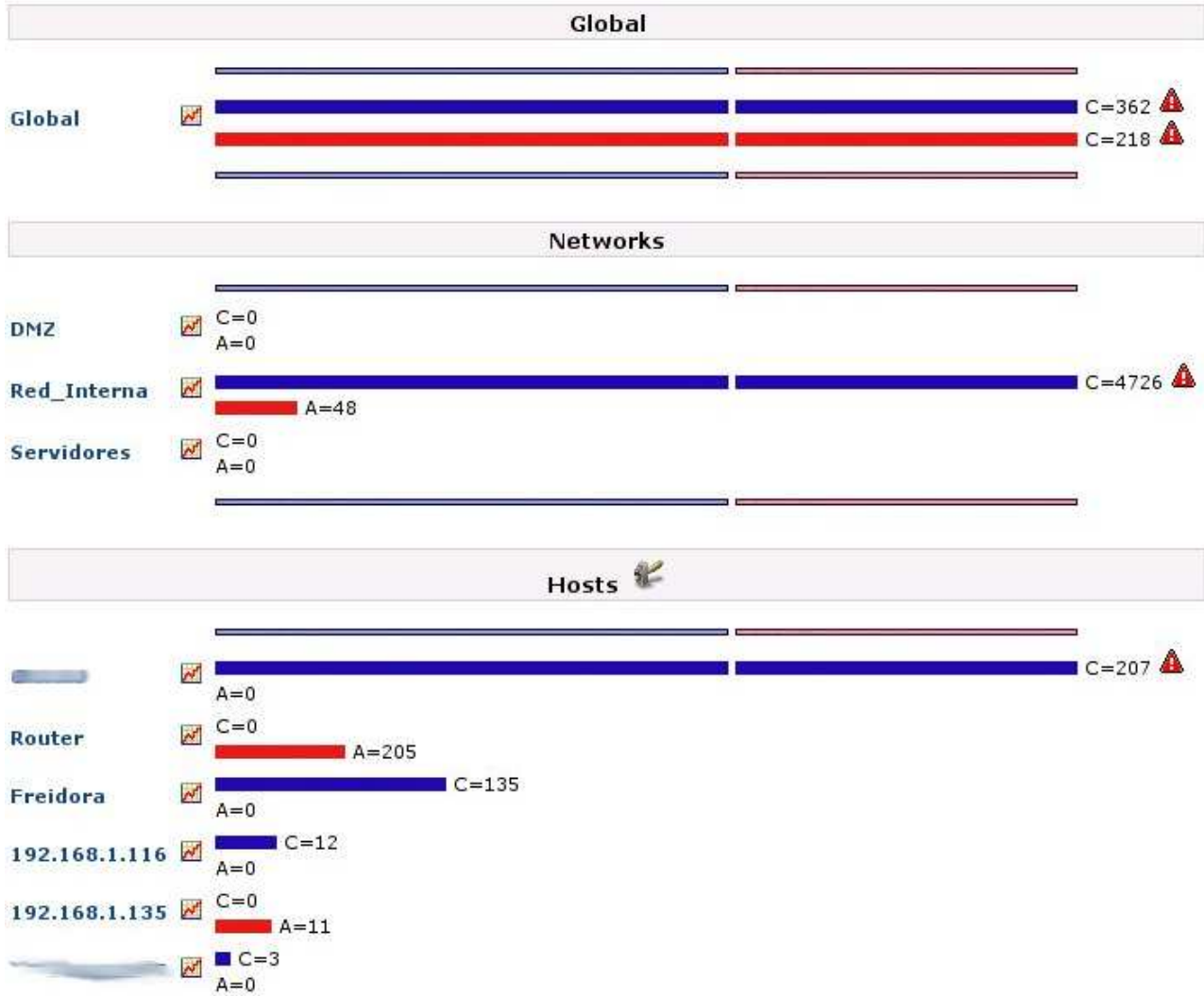


## 7.5.16. Operating Systems

OS Changes  [ Get list ]					
Host	OS	Previous OS	When	Ack	Ignore
golgotha	Linux 2.4/2.6	Linux 2.4/2.6	Tue Feb 3 22:17:21 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.81	Linux 2.4/2.6	Windows 2000 SP2+, XP SP1	Mon Feb 16 10:59:10 2004	<input type="checkbox"/>	<input type="checkbox"/>
Gestalt	Windows 98	FreeBSD 4.7-5.1 or MacOS X 10.2-10.3) (1	Wed Jan 28 19:15:10 2004	<input type="checkbox"/>	<input type="checkbox"/>
<del>192.168.1.100</del>	Linux 2.4/2.6	Windows 2000 SP4, XP SP1	Thu Feb 26 17:59:20 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.230	Linux 2.4/2.6	Windows XP Pro SP1, 2000 SP3	Thu Feb 12 11:46:06 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.70	Linux 2.4/2.6	Windows 2000 SP2+, XP SP1	Wed Feb 11 19:05:16 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.147	Linux 2.4/2.6	Windows 2000 SP2+, XP SP1	Wed Feb 4 10:45:08 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.115	Linux 2.4/2.6	Windows 2000 SP2+, XP SP1	Tue Jan 27 19:34:57 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.155	Linux 2.4/2.6	Windows XP Pro SP1, 2000 SP3	Thu Feb 19 21:37:07 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.13	Windows XP Pro SP1, 2000 SP3	Linux 2.4/2.6	Fri Feb 13 19:21:50 2004	<input type="checkbox"/>	<input type="checkbox"/>
Win2k	Linux 2.4/2.6	Windows 2000 SP2+, XP SP1	Fri Feb 13 18:55:23 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.116	Windows XP SP1, 2000 SP3	Linux 2.4/2.6	Tue Feb 17 16:11:51 2004	<input type="checkbox"/>	<input type="checkbox"/>
MacosX	FreeBSD 4.8-5.1 or MacOS X 10.2-10.3	FreeBSD 4.7-5.1 or MacOS X 10.2-10.3) (1	Thu Jan 29 16:11:54 2004	<input type="checkbox"/>	<input type="checkbox"/>
Fw_test	Windows 2000 SP4, XP SP1	Linux 2.4/2.6	Thu Feb 5 13:43:47 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.121	Linux 2.4/2.6	Windows 2000 SP2+, XP SP1	Mon Feb 2 18:28:46 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.16	Solaris 9	Windows XP/2000 while downloading	Wed Mar 3 17:27:38 2004	<input type="checkbox"/>	<input type="checkbox"/>
192.168.1.160	Windows XP SP1, 2000 SP3	Linux 2.4/2.6	Thu Feb 19 17:46:37 2004	<input type="checkbox"/>	<input type="checkbox"/>



## 7.5.17. Riskmeter





## 7.5.18. RRD Profile

Server						
Attribute	Threshold	Priority	Alpha	Beta	Persistence	Enable
activeHostSendersNum	500	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
arpRarpBytes	50	3	0.1	0.0035	4	<input checked="" type="checkbox"/>
broadcastPkts	500	3	0.1	0.0035	4	<input checked="" type="checkbox"/>
ethernetBytes	300000	3	0.1	0.0035	4	<input checked="" type="checkbox"/>
ethernetPkts	1000	3	0.1	0.0035	4	<input checked="" type="checkbox"/>
fragmentedIpBytes	100	1	0.1	0.0035	4	<input checked="" type="checkbox"/>
icmpBytes	5000	3	0.1	0.0035	4	<input checked="" type="checkbox"/>
igmpBytes	100	3	0.1	0.0035	4	<input checked="" type="checkbox"/>
ipBytes	1000000	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
ipv6Bytes	500	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
ipxBytes	100	1	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_DHCP-BOOTPBytes	1	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_DNSBytes	10000	3	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_eDonkeyBytes	1000	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_FTPBytes	1000000	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_GnutellaBytes	1000	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_HTTPBytes	100000	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_KazaaBytes	1000	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_MailBytes	2500	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_MessengerBytes	1000	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_NBios-IPBytes	200000	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_NFSBytes	100	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_NNTPBytes	100	1	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_SNMPBytes	20	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_SSHBytes	10000	5	0.1	0.0035	4	<input checked="" type="checkbox"/>
IP_TelnetBytes	500	5	0.1	0.0035	4	<input checked="" type="checkbox"/>



## 7.5.19. Rule Editor

[Hosts] [Scan] [RRD Config] [Networks] [Ports] [Sensors] [Signatures] [Rule Editor] [Policy] [Control Panel] [Riskmeter] [Graphs] [Forensics] [Usage] [Service availability] [Wizard] [Conf]

### OSSIM Framework

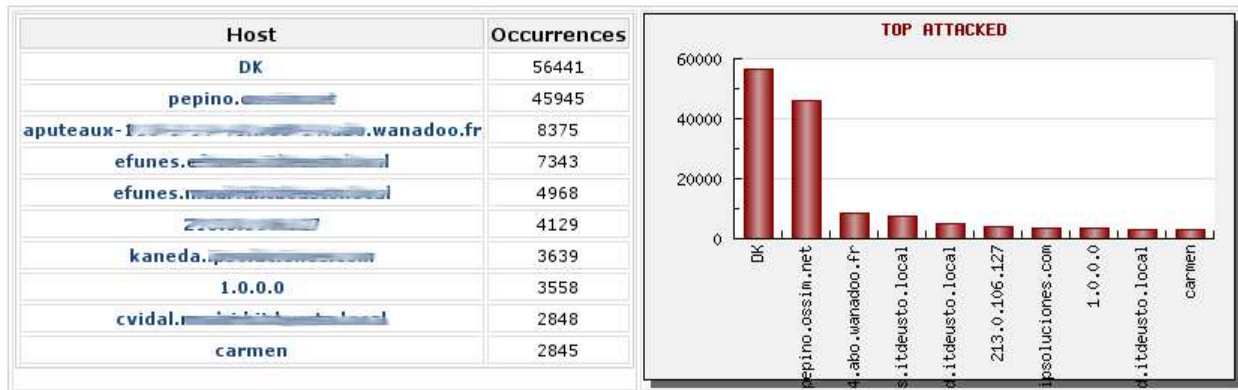
#### Rule editor

##### ftp.rules

Name	Action	Protocol	SRC IP	SRC Ports	Dir	DEST IP	DEST Ports	Content	Options
"FTP CEL overflow attempt"	alert	tcp	\$EXTERNAL_NET	any	->	\$HOME_NET	21	"CEL " !" 0a "	<b>rev:</b> 5 <b>classtype:</b> attempted-admin <b>flow:</b> to_server,established <b>nocase</b>
"FTP CWD overflow attempt"	alert	tcp	\$EXTERNAL_NET	any	->	\$HOME_NET	21	"CWD " !" 0a "	<b>rev:</b> 3 <b>classtype:</b> attempted-admin <b>flow:</b> to_server,established <b>nocase</b>
"FTP CMD overflow attempt"	alert	tcp	\$EXTERNAL_NET	any	->	\$HOME_NET	21	"CMD " !" 0a "	<b>rev:</b> 8 <b>classtype:</b> attempted-admin <b>flow:</b> to_server,established <b>nocase</b>

## 7.5.20. Security Reporting 1

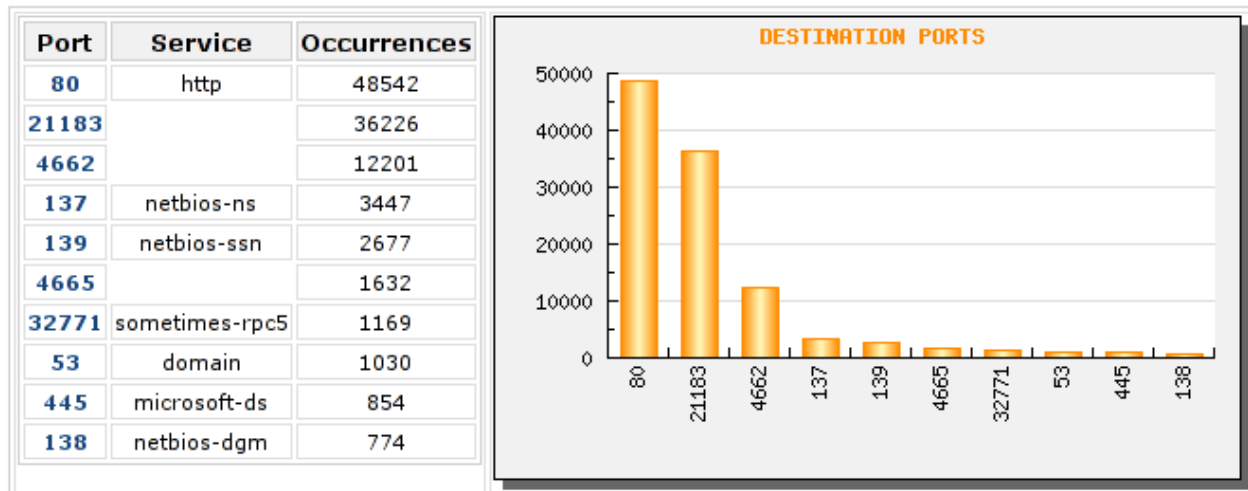
### Top 10 Attacked hosts





## 7.5.21. Security Reporting 2

Top 10 Used Ports

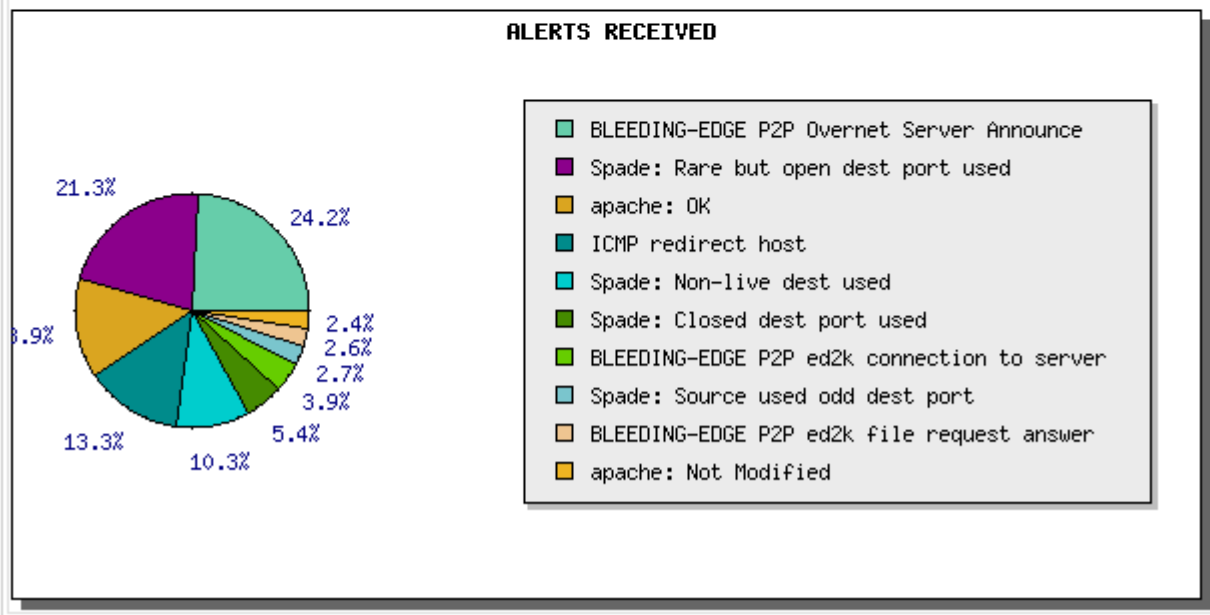




## 7.5.22. Security Reporting 3

### Top 10 Alerts

Alert	Occurrences
<b>BLEEDING-EDGE P2P Overnet Server Announce</b>	61659
<b>Spade: Rare but open dest port used</b>	54121
<b>apache: OK</b>	35348
<b>ICMP redirect host</b>	33929
<b>Spade: Non-live dest used</b>	26172
<b>Spade: Closed dest port used</b>	13741
<b>BLEEDING-EDGE P2P ed2k connection to server</b>	9997
<b>Spade: Source used odd dest port</b>	6765
<b>BLEEDING-EDGE P2P ed2k file request answer</b>	6631
<b>apache: Not Modified</b>	6228





## 7.5.23. Users

[Control Panel ▶] [Policy ▶] [Reports ▶] [Monitors ▶] [Configuration ▾] [Tools ▶] [Logout]

[Main] [Users] [Directives] [Correlation] [RRD Config] [Host Scan] [Riskmeter]

### Users

Login	Name	Password	Actions
admin	OSSIM admin	XXX	[Change Password]
dgil	David Gil	XXX	[Change Password] [Update] [Delete]
DK	Dominique	XXX	[Change Password] [Update] [Delete]
jcasal	Julio Casal	XXX	[Change Password] [Update] [Delete]
Insert new user			

## 7.5.24. Vulnmeter

### Vulnmeter - 192.168.1.97

#### Host Report

##### Inventory

Last scan

##### Metrics

##### Alarms

Source or Dest  
Source  
Destination

##### Alerts

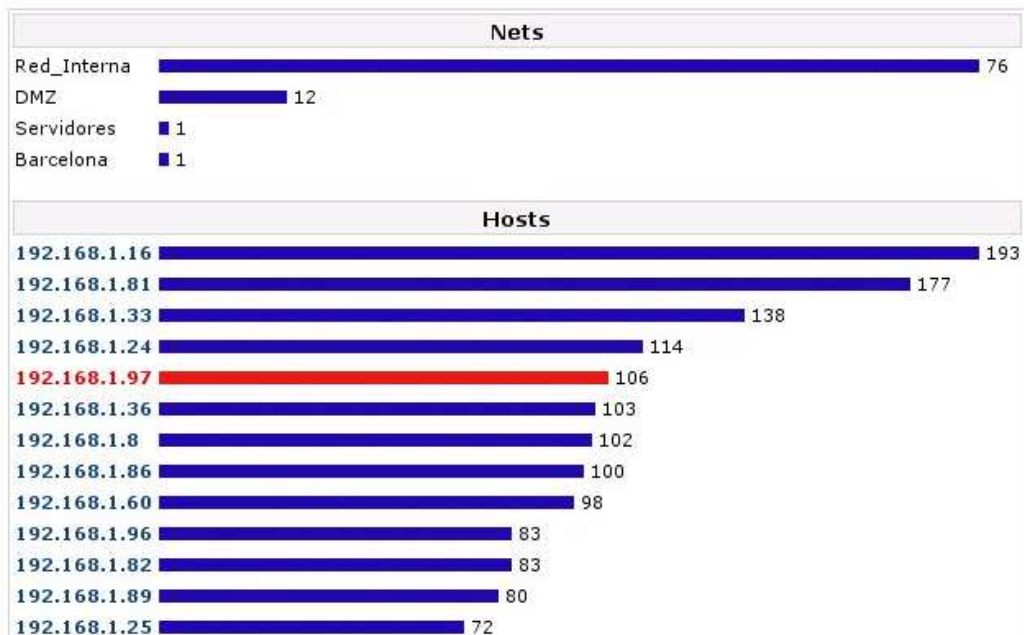
Main  
Src Unique alerts  
Dst Unique alerts

##### Vulnerabilites

Vulnmeter  
Security Problems

##### Usage

##### Anomalies





## 7.5.25. Worm

[Control Panel ▾] [Policy ▾] [Reports ▾] [Monitors ▾] [Configuration ▾] [Tools ▾] [Logout]  
 [Metrics] [Alarms] [Alerts] [Vulnerabilities] [Anomalies]

Back to main								
#	Id	Alarm	Risk	Date	Source	Destination	Correlation Level	Action
1	103928	Possible Worm	2	2004-09-01 09:53:29	Infectado:62806	192.168.2.1:445	2	Ack
Alarm Summary [ Total Alerts: 16 - Unique Dst IPAddr: 15 - Unique Types: 2 - Unique Dst Ports: ]								
1	103927	Spade: Closed dest port used	0	2004-09-01 09:53:26	Infectado:62806	192.168.2.130:445	2	Ack
2	103926	Spade: Closed dest port used	0	2004-09-01 09:53:21	Infectado:62806	192.168.2.124:445	2	Ack
3	103925	Spade: Closed dest port used	0	2004-09-01 09:53:03	Infectado:62806	fot-server:445	2	Ack
4	103924	Spade: Closed dest port used	0	2004-09-01 09:52:59	Infectado:62806	192.168.2.98:445	2	Ack
5	103923	Spade: Closed dest port used	0	2004-09-01 09:52:59	Infectado:62806	golgotha:445	2	Ack
6	103922	Spade: Rare but open dest port used	1	2004-09-01 09:52:58	Infectado:62806	192.168.2.95:445	2	Ack
7	103921	Spade: Rare but open dest port used	1	2004-09-01 09:52:54	Infectado:62806	192.168.2.90:445	2	Ack
8	103920	Spade: Rare but open dest port used	1	2004-09-01 09:52:41	Infectado:62806	jmenta:445	2	Ack
9	103919	Spade: Rare but open dest port used	1	2004-09-01 09:52:39	Infectado:62806	alexnet:445	2	Ack
10	103918	Spade: Closed dest port used	0	2004-09-01 09:52:36	Infectado:62806	wayreth:445	2	Ack
11	103903	Spade: Closed dest port used	0	2004-09-01 09:51:48	Infectado:62806	192.168.2.17:445	2	Ack
12	103902	Spade: Closed dest port used	0	2004-09-01 09:51:48	Infectado:62806	192.168.2.16:445	2	Ack
13	103901	Spade: Rare but open dest port used	1	2004-09-01 09:51:48	Infectado:62806	192.168.2.15:445	2	Ack
14	103895	Spade: Closed dest port used	0	2004-09-01 09:51:40	Infectado:62806	192.168.2.3:445	2	Ack
15	103894	Spade: Closed dest port used	0	2004-09-01 09:51:39	Infectado:62806	192.168.2.1:445	2	Ack
16	103893	Spade: Closed dest port used	0	2004-09-01 09:51:39	Infectado:62806	192.168.2.1:445	1	Ack



## **7.6. Appendix 5 – Reference Documents**

1. OSSIM – Open Source Security Information Management – General System Description – Version 0.18
2. OSSIM – ROADMAP
3. OSSIM Fast Guide – February 8, 2004
4. A Practice of OSSIM – DCOM Exploit Event Correlation Test
5. OSSIM – Correlation engine explained.
6. OSSIM User Manual – Kevin Milne, September 2, 2004
7. Intrusion Detection with Snort – Jack Koziol – SAMS
8. Intrusion Detection with Snort – Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID – Rafeeq Ur Rehman – Bruce Peren’s Open Source Services



## 7.7. Appendix 6 - GNU Free Documentation License

GNU Free Documentation License  
Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA  
Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

### 0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

### 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly



within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.



The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

## 2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

## 3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.



It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

#### 4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section



- may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

## 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".



## 6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

## 7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

## 8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

## 9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except



as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

## 10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

### ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.