Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Prelude as a Hybrid IDS Framework

Organizations both Large and Small are constantly looking to improve their posture on security. While most organizations deploy security equipment, they still encounter the challenge of monitoring and reviewing the security events. Due to the nature of network security events, they require analysis as close to real time as possible.

Copyright SANS Institute
Author Retains Full Rights

AD

Prelude as a Hybrid IDS Framework

GCIA Gold Certification

Author: Curt Yasm, c_yasm@yahoo.com

Adviser: Brent Deterding

Accepted:

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

1. ABSTRACT 3

2. WHAT IS PRELUDE? 4

3. BENEFITS AND RISKS OF PRELUDE 4

3.1 REGULATORY COMPLIANCE 5

3.2 UNIVERSAL COMPATIBILITY 7

3.3 REAL-TIME EVENT MONITORING 9

3.4 REDUCED SECURITY COSTS 9

3.5 POTENTIAL WEAKNESSES 11

5. PRELUDE COMPONENTS 15

5.1 PRELUDE MANAGER: 15

5.2 LIBPRELUDE: 19

5.3 LIBPRELUDEDB: 19

5.4 PRELUDE-LML: 20

5.5 PRELUDE-CORRELATOR: 21

5.6 PREWIKKA: 21

5.7 PFLOGGER: 32

6. INSTALLATION 33

7. BENEFITS OF PRELUDE (CASE STUDIES) 35

8. REFERENCES 39

APPENDIX A 41

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

1. Abstract

Organizations both Large and Small are constantly looking to improve their posture on security. While most organizations deploy security equipment, they still encounter the challenge of monitoring and reviewing the security events. Due to the nature of network security events, they require analysis as close to real time as possible. In this paper, I will discuss the Open Source Security Information Management (SIM) system known as Prelude.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

2. What is Prelude?

In 1998, Yoann Vandoorselaere created the Prelude Open Source Intrusion Detection System (IDS). Since then Prelude has seen many contributions from Security Professionals all around the world. This widespread support for the software has molded Prelude into a Universal "Security Information Management" (SIM) system. Prelude collects, normalizes, sorts, aggregates, correlates, and reports all security-related events independently of the product brand or license ("Universal SIM," 2005).

This independent log aggregation system provides immense flexibility to organizations. Organizations no longer require any special licensing or software in order to efficiently and accurately manage their device logs. This type of flexibility can also allow organizations to easily implement and monitor devices from various vendors without additional expense.

3. Benefits and Risks of Prelude

Prelude can make monitoring and responding to network incidents easier and more efficient. By implementing Prelude organizations can:

- Achieve Regulatory Compliance

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- Reduce Security Costs
- Monitor all Devices
- Monitor Events in Real-Time

3.1 Regulatory Compliance

The following are a couple of the ways that Prelude can benefit organizations that are trying to meet Regulatory Compliance.

- Prelude normalizes all System Events into a single format.
- Prelude stores all logs in a central location.
- Prelude maintains a forensic trail.

Prelude normalizes all events into the Intrusion Detection Message Exchange Format (IDMEF) ("Universal SIM", 2005). "The purpose of the Intrusion Detection Message Exchange Format (IDMEF) is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems that may need to interact with them" (The Intrusion Detection Message Exchange Format (IDMEF), 2007, Abstract). IDMEF is an experimental data format intended to enable interoperability between commercial, open source, and research systems. It uses a XML Based Data model to define a standard

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

representation of alerts. This standardized representation is what enables interoperability among different devices. A standardized log format also allows data from different devices to be stored centrally.

Normalization allows events from different devices to be stored in a structured format. Essentially, it allows all collected events to be stored in the same database in the same format. Normalization also makes the storage of events easier and streamlined because there is no need for multiple storage devices to maintain all processed data.

By providing a centralized log location, there is no need for manually consolidating system logs. Centralized storage also allows easy creation of reports. Prelude allows the user to send the reports to an e-mail address as a .pdf or allows exporting them directly from the Prewikka Interface (covered later). The ability to generate reports allows an organization to present their auditors with visual representation of their security data. The data provided may help the organization substantiate their security policies.

Prelude also has the ability to provide a forensic trail for events. It stores a copy of all of the events in its database. This can protect against accidental deletion or tampering on the source

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

device. This information is available by running a report or pulling directly from the database.

3.2 Universal Compatibility

Prelude is capable of interoperating with virtually any device on the network. Prelude provides a C, C++, Python, Ruby, Lua, and Perl framework. This ensures that existing security applications can be converted to use the Prelude systems Native compatibility ("Prelude Compatibility", 2005). The following is a list of natively supported third party sensors (taken directly from Prelude's website).

AuditD	The Linux Audit Daemon
Nepenthes	A versatile tool to collect malware
NuFW	An identity access management solution at the network level
OSSEC	An Open Source Host-based Intrusion Detection System
Pam	Linux Pluggable Authentication Modules
Samhain	A file integrity checker
Sancp	A network traffic statistical information collector
Snort	The Defacto Standard Open Source IDS

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

In addition to the above natively supported sensor's prelude can monitor nearly any type of log file. Below is an example of the various types of logs and devices that Prelude can monitor again take directly from the Prelude website ("Prelude Compatibility", 2005).

Firewall, Routers & VPN	BIG-IP, Check Point, CISCO ASA, CISCO IOS, CISCO Router, CISCO VPN, D-Link, Ipchains, IpFw, Juniper Networks NetScreen, Linksys WAP11, ModSecurity v2, Netfilter, SonicGuard SonicWall
Switchs	CISCO CSS
IDS	CISCO IPS, Portsentry, Shadow, Tripwire
Monitoring	APC-EMU, ArpWatch, Dell OpenManage, Nagios
AntiVirus/AntiSpam	ClamAV, P3Scan, SpamAssassin
Database	Microsoft SQL Server, Oracle
SMTP/POP Server	Exim, Postfix, Qpopper, Sendmail, Vpopmail
FTP Server	ProFTPD, WU-FTPD
Web Server	Apache
Vulnerability Scanner	Nessus
Honeypots	Honeyd, Honeytrap, Kojoney
Authentication	OpenSSH, Su
Applications	Asterisk, Cacti, Libsafe, Shadow Utils, Squid, Sudo
OS (security tools)	GrSecurity, PaX, SELinux
Miscellaneous	Unix specific logs, Webmin, Windows Server, Arbor, Linux bonding, Microsoft Cluster Service, NetApp ONTAP, NTSyslog, OpenHostAPD, Rishi,

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

	Suhosin

Prelude's ability to monitor virtually any type of file or device makes implementation into a pre-existing network simple. Depending on the device, if no native support is available it can be configured to log to Syslog and Prelude will monitor the log files.

3.3 Real-Time Event Monitoring

Prelude allows organizations to view real-time events via the Prewikka web interface. In the past, manual review of logs could easily result in missed attacks. Analyzing events in real time allows decreased response time to incidents. This also allows organizations to see up to date activity on their entire network easily. The web page is set to refresh automatically showing the most recent events.

3.4 Reduced Security Costs

Prelude can help reduce Security Costs by increasing efficiency and reducing overhead. Prelude has the potential to provide a very good Return on Investment (ROI). Since Prelude is Open-Source, there are no licensing fees and no limit to the number of sites. Organizations are therefore only required to pay for customizations and maintenance associated with the customizations.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The positive ROI is the not only the result of the software being open source (free) but the increases in efficiency. The SIEM solution records the events, filters them to remove non-threatening alerts (reducing volumes by up to 300x), and correlates them to see if threats are connected (Jean-FRANÇOIS DÉCHANT, December 2006). Once properly configured and base lined Prelude will typically only generate an alert on events of interest. This reduces the amount of time that is spent on analyzing unimportant logs. It also let analysts focus more time on threat analysis.

While Prelude does have the ability to reduce costs, organizations should consider the initial costs before calculating ROI. Possible upfront costs may include:

- Installation
- Employee Training
- Customization fees (if applicable)
- Maintenance fees
- Additional Hardware costs (if applicable)
- Facility costs (if applicable)

Since Prelude is open-source, there is no initial maintenance

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

provided. Therefore, maintenance and customizations are available for purchase through Prelude Technologies. Prices depend on the size of the organization and level of customization.

The organization will also need to consider the hardware related costs to run Prelude. Again, depending on the environment additional hardware may be required to deploy Prelude. The costs associated with hardware also include facility-based costs (power, cooling, space etc.).

3.5 Potential Weaknesses

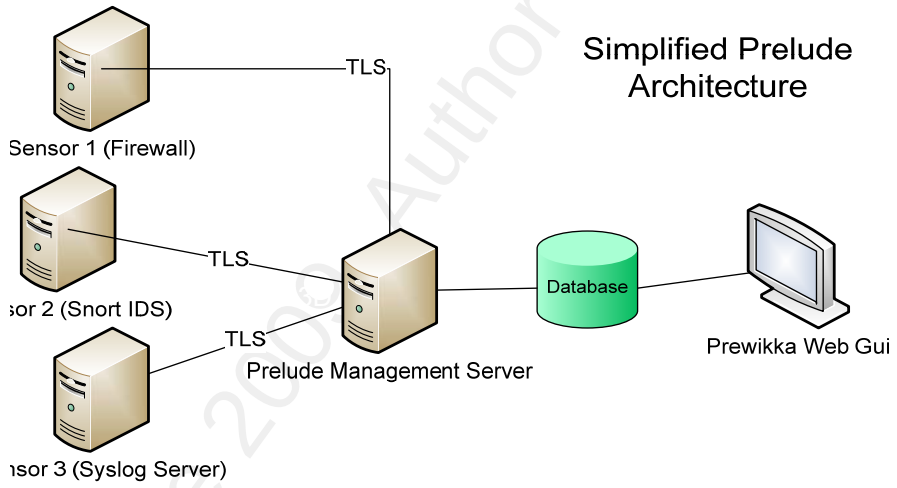
Security Information Management systems provide organizations with many features. Just like any other technology, Prelude has its potential weaknesses and drawbacks. The following are some items that an organization should consider before implementing a system like prelude:

- Requires in depth training for analysis
- Performance Limitations of current systems
- Protocol Analysis Vulnerabilities
- Potential Prelude Vulnerabilities
- Maintenance not included
- Centralized Logging (Potential Single Point of Failure)

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

4. Prelude Architecture

Prelude provides a centralized reporting location for all network devices. In the center of this is the Prelude Management Server. Each sensor connects to the management server utilizing the (SSL/TLS) Protocol ("Architecture Overview", 2008). This ensures data transmission between the Management Server and the Sensor is secure.



The above diagram is an example of a simple installation of Prelude with a single Management Server and three sensors. A Sensor is any device that reports logs to the Prelude Management Server. Any of the following could be considered a sensor IDS, Firewall, Syslog Server, Workstation, or any other logging device. Prelude can receive logs by directing the device to log to Prelude-LML, using the native compatibility link, or using one of the Programming Frameworks to

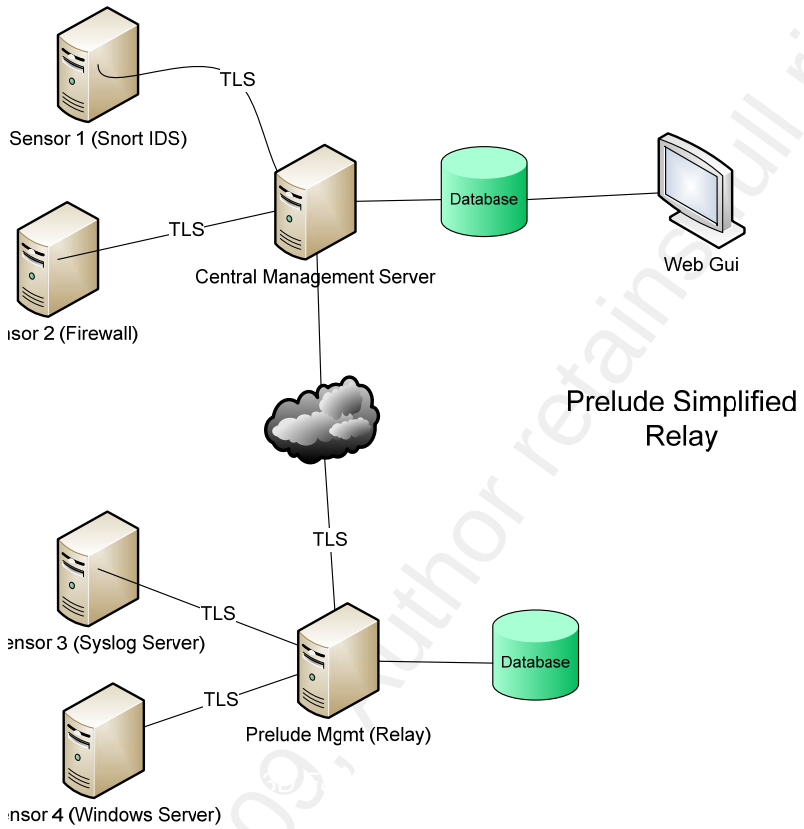
© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

develop native compatibility (directly connect or fetch).

Prelude is a distributed architecture that allows total security coverage even across a WAN (“Universal SIM,” 2005). Each additional site requires a Management Server. These servers relay their events to the central location. In order to ensure redundancy each site contains a database for that location (“Architecture Overview”, 2008).

The Management Server writes the events to the local database and sends them to the central server. This prevents data loss if there are any communication issues between the relay and central server. The following diagram is a Simplified view of what a multiple site implementation would look like.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.



Installing Prewikka on the Management Servers at each site would allow the local Security Personnel to view the current events at their site. Analysts at the central location would be able to view all events from each site reporting in. This setup would be the desired configuration for organizations that are interested in having a dedicated SOC to monitor the events in real-time as well as keeping the local personnel up to date with current events.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

5. Prelude Components

Prelude consists of seven distinct components. The components include the Prelude Manager, Libprelude, LibprelueDB, Prelude-LML, Prelude-Correlator, Prewikka Interface, and Prelude-PFLogger. Only four (Prelude Manager, Libprelude, LibpreludeDB, and Prewikka) of the previously mentioned are required in order to successfully setup and run Prelude. The other components merely provide additional functionality and interoperability.

5.1 Prelude Manager:

Prelude-Manager is the Server that accepts all secure connections from either the sensors or other managers. The Prelude Management Server is capable of listening on a UNIX domain socket, or IPv4 or IPv6 address. The management server is in charge of processing the events and if necessary converting them from the Prelude binary IDMEF format to the user specified output format ("Prelude Components", 2005). As of this writing Prelude supports the following output plugins:

- DB- A database Plugin (MySQL, PostgreSQL, SQLite)
- **Xmlmod** - An XML Reporting Plugin

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- **Textmod** - A text reporting Plugin
- **Relaying** - A plugin, which relays alerts to another manager
- **SMTP** - Send (user defined) textual alerts through your SMTP server

The prelude-manager.conf file is the location where the user can specify which output plugin to use ("Prelude Manager", 2005). Prelude allows multiple instances of a particular plugin to run by giving each instance a unique name. This allows reporting alerts to multiple locations in multiple formats. Prelude-Manager also supports a scheduler option. This ensures that all sensors logs are processed.

By default, Prelude processes one hundred events before moving on to the next sensors events. Additionally event priority determines the order in which they are processed. The amount of events processed and the number processed based on priority is configurable to meet the organizations needs.

In addition to the output plugins, the Prelude Manager supports the following filtering plugins:

- IDMEF Criteria Filtering Plugin - Filtering events
- Thresholding Filtering Plugin - Event suppression and

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

thresholding

The IDMEF Criteria Filtering Plugin allows the user to filter events based on the various IDMEF Fields ("Filtering Plugins", 2005). Below are some examples of IDMEF Fields:

alert.messageid=abc123456789

alert.analyzer(0).analyzerid=hq-dmz-analyzer01

alert.analyzer(0).node.category=dns

alert.analyzer(0).node.location=Headquarters DMZ Network

alert.analyzer(0).node.name=analyzer01.example.com

alert.create_time=0xbc723b45.0xef449129

alert.source(0).ident=a1b2c3d4

alert.source(0).node.ident=a1b2c3d4-001

alert.source(0).node.category=dns

alert.source(0).node.name=badguy.example.net

alert.source(0).node.address(0).ident=a1b2c3d4-002

alert.source(0).node.address(0).category=ipv4-net-mask

alert.source(0).node.address(0).address=192.0.2.50

alert.source(0).node.address(0).netmask=255.255.255.255

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

```
alert.target(0).ident=d1c2b3a4

alert.target(0).node.ident=d1c2b3a4-001
```

If an event matches the filter criteria, the system applies the specified action to the event. As mentioned before Prelude has the ability to run multiple output plugins at one time. This provides flexibility by sending different alert types for different events. Instead of having Prelude just send an event directly to the database, it can simultaneously send an alert to the SMTP output plugin.

When the SMTP output plugin is used, it will immediately send an e-mail to the address defined when an alert matches the filter. The other filtering plugin that Prelude supports is the Thresholding Filtering Plugin. This plugin allows suppression of events based on their content. This plugin also gives the option to threshold the event for a specified amount of time up to a specified occurrence.

A Thresholding filter is a good choice when dealing with events that could potentially generate numerous False Positives if each occurrence generated an alert. For example, an Analyst would not want to see an event for every logon failure on a server or workstation. Considering users forget their passwords all the time having two or three failures is likely benign activity and should not generate an

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

alert.

The greatest amount of flexibility comes from the ability for Prelude to stack filters. Stacking filters can allow a wide range of customizations for event handling. For more information on filters and stacking filters, please see Appendix I.

5.2 Libprelude:

Libprelude provides an Application Programming Interface (API) that allows third party software to communicate with the Prelude sub-systems. The libraries included in this package also provide the necessary functionality for generating IDMEF formatted events. Libprelude also ensure that re-transmission of data is performed if an interruption occurs between any of the components in the system. The Libprelude package is a requirement for any device acting as a sensor or manager. It is required to convert the logs into Preludes Binary IDMEF format. Lastly, Libprelude ensures that the Sensors and Management Servers communicate using secure transmissions Secure Socket Layer/Transport Layer Security (SSL/TLS) ("Prelude Components", 2005).

5.3 LibpreludeDB:

LibpreludeDB is the library that provides an abstraction layer

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

for storing IDMEF alerts in a database. This library simplifies management of the database by hiding the inner workings to allow the user to access the database independent of the log format. In order to use the Prewikka Web Interface the hosting machine is required to have LibPreludeDB installed ("Prelude Components", 2005).

5.4 Prelude-LML:

Prelude-LML is the component that allows Prelude to analyze various different types of logs. The Prelude-LML log analyzer uses a rule-set to determine whether activity within the logs is malicious. Prelude-LML is comparable to the way Snort uses a rules file to analyze packets. In the case of Prelude-LML its rules files attempt to match data within log files instead of network packets.

As mentioned before Prelude is capable of monitoring any type of log (Syslog, flat file, system logs, etc.). Prelude-LML has two primary modes of operation:

- Watch Log Files
- Receive UDP Syslog Messages

This functionality makes Prelude extremely flexible and easy to implement into any organizations network. If a device does not have native compatibility with Prelude, it can be configured to log to a

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Syslog server that Prelude-LML is monitoring (“Prelude-LML”, 2005).

5.5 Prelude-Correlator:

Prelude-Correlator is the component that allows correlation of events between multiple Prelude Management servers. This component allows the users to write correlation rules using the LUA programming language. If streams of events match a correlation rule, a correlation alert is generated. Correlation alerts can simplify and speed up analysis by rolling up user defined activity into a single alert (“Prelude Components”, 2005).

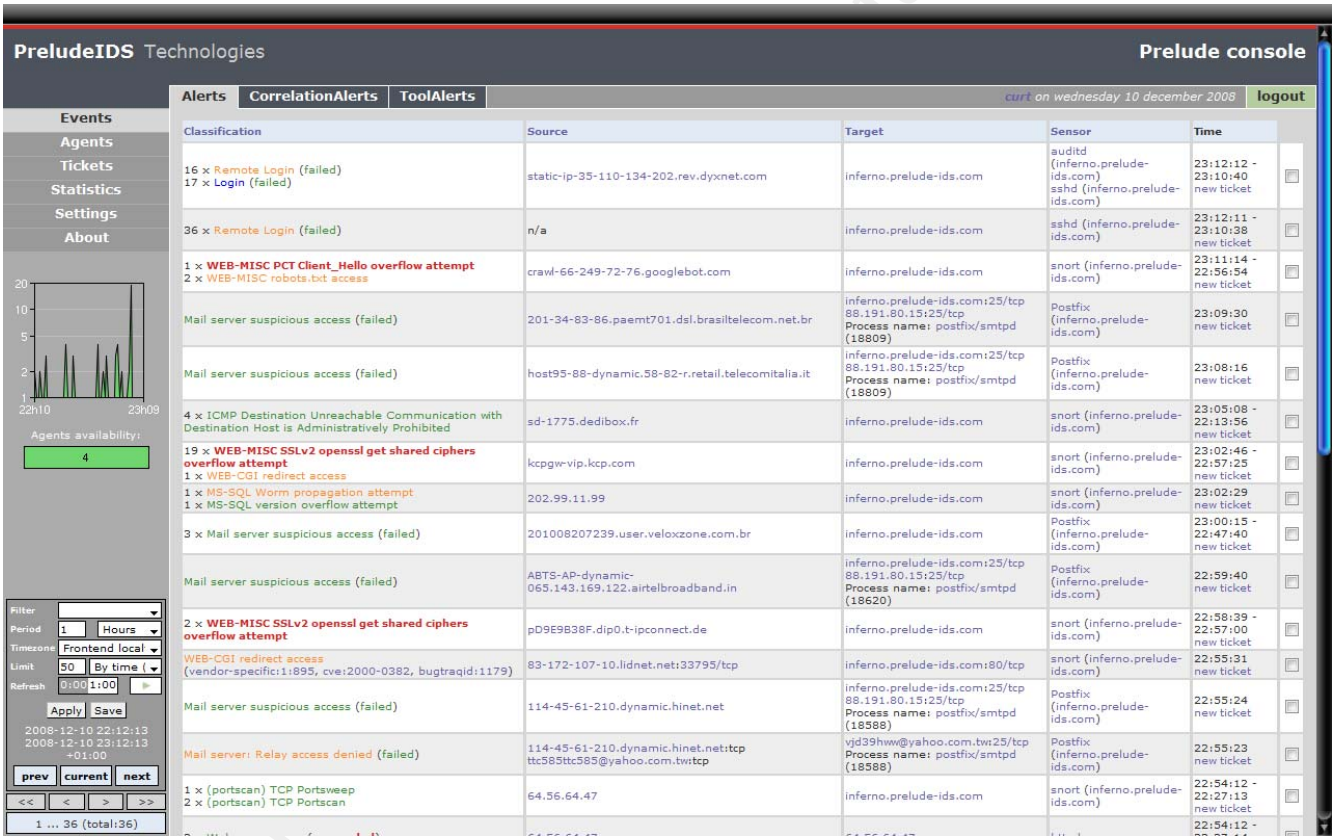
5.6 Prewikka:

The Prewikka Interface is the Web Based Graphical User Interface (GUI) for Prelude. There are two versions of the Prewikka Interface the free version and the Commercial version also known as the Pro version. The Pro interface adds additional functionality such as an integrated ticketing system, remote sensor management, fully interactive graphical statistics, virtual alert views, exporting of alerts to a pdf file, and secured authentication from a LDAP Server (“Prewikka Manual”, 2008).

The Events Tab is the default page after logging into Prewikka. This page shows all of the events within the last hour. From here,

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

the user has the option to specify the events that are listed by minute, hours, days, months, years, or unlimited. Accessing the Settings Tab gives the option to create pre-defined view filters. This will only present the user with the information defined in the view filter.



The CorrelationAlerts tab displays any alerts that match a custom Correlation Rule. The correlation engine pulls events from remote Prelude Managers and compares them to the correlation rules. Correlation Alerts are beneficial for larger organizations because it

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

allows analysts to see if related activity is occurring across multiple sites. Unfortunately, the lab in use did not have multiple Prelude Managers setup so there is no screenshot of what a Correlation Alert looks like.

The Tool Alert class (IDMEF) carries additional information related to the use of attack tools or malevolent programs such as Trojan horses. It groups one or more previously sent alerts together, to say, "These alerts were all the result of someone using this tool" (Audrey Girard, PreludeIDS Technologies). An example of this would be if an Attacker were using Nessus to scan the network. The Tool Alert tab would then display an alert indicating that groups of alerts were all the result of the Nessus tool.

In order to view more information about a particular event the user can click on the event summary under the Classification column. This link will display all of the events that match that particular event description, source, target, and sensor. The main Events page lists the events as (number x, event summary, result). If all of the events are similar, the system displays them as one clickable event on the summary page. This consolidation prevents the summary page from being flooded with the same alerts.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Alerts | CorrelationAlerts | ToolAlerts — admin on tuesday 09 december 2008 — logout

Classification *	Source	Target *	Sensor	Time	
Multiple Windows audit failure events. (succeeded)		(Win2003) 192.168.0.103	OSSEC (OSSEC Management Server)	18:56:34	
Multiple Windows audit failure events. (succeeded)		(Win2003) 192.168.0.103	OSSEC (OSSEC Management Server)	18:56:34	

Delete

In order to see the actual event detail the user has to click on the event summary link again. This displays a nice graphical view of the event.

Alerts | CorrelationAlerts | ToolAlerts

Alert

Create time	Analyzer time
2008-12-09 18:56:34.91390 -06:00	2008-12-09 18:56:34.91390 -06:00

MessageID
63dcbeec-c655-11dd-bb90

Text	Severity	Completion	Type	Description
Multiple Windows audit failure events.	medium	succeeded	other	Multiple Windows audit failure events.

Analyzer #1

Model	Name	Analyzerid	Version	Class	Manufacturer
Ossec	OSSEC	795235897350635	v1.6.1	Host IDS, File Integrity Checker, Log Analyzer	http://www.ossec.net

Node name	Operating System
OSSEC Management Server	Linux 2.6.23.17-88.fc7

Process	Process Path	Process PID
ossec-analysisd	/var/ossec/bin/ossec-analysisd	28577

Analyzer Path (1 not shown)

Target(0)

Node name (resolved)	Node address
(Win2003) 192.168.0.103	(Win2003) 192.168.0.103

Additional data

Meaning	Value
Source file	(Win2003) 192.168.0.103->WinEvtLog
Full Log	WinEvtLog: Security: AUDIT_FAILURE(861): Security: NETWORK SERVICE: NT AUTHORITY: CEREBUS: The Windows Firewall has detected an application listening for incoming traffic. Name: - Path: C:\WINDOWS\system32\svchost.exe Process identifier: 428 User account: NETWORK SERVICE User domain: NT AUTHORITY Service: Yes RPC server: No IP version: IPv4 IP protocol: UDP Port number: 64768 Allowed: No User notified: No

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The event detail page contains a verbose view of the alert including the timestamps, analyzer details, analyzer path, additional data, and the target and source details. Some of this will vary depending on the source of the alert and type of device reporting the alert.

Again, due to the restrictions of the lab there is no example of this field. This field displays the path that the alert took before reaching its destination. If an organization has an external IDS as well as an Internal IDS and the packets traversed both of the sensors this field would contain the sensors that saw the traffic.

As an example of the different information provided in the different alerts the next screenshot shows the additional data in a Snort alert. It contains an easy to read view of the packet as seen by the sensor. The alert contains the IP information, the Payload in Hex, and an easy to read ASCII translation of the payload.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Additional data

Meaning	Value
snort_rule_sid	1
snort_rule_rev	0

Network centric information

IP

Version	Header length	TOS	Length	Id	RF	DF	MF	Ip offset	TTL	Protocol	Checksum	Source address	Target address
4	5	0	162	0		X		0	0	255	63213	192.168.0.125	192.168.0.162

Payload

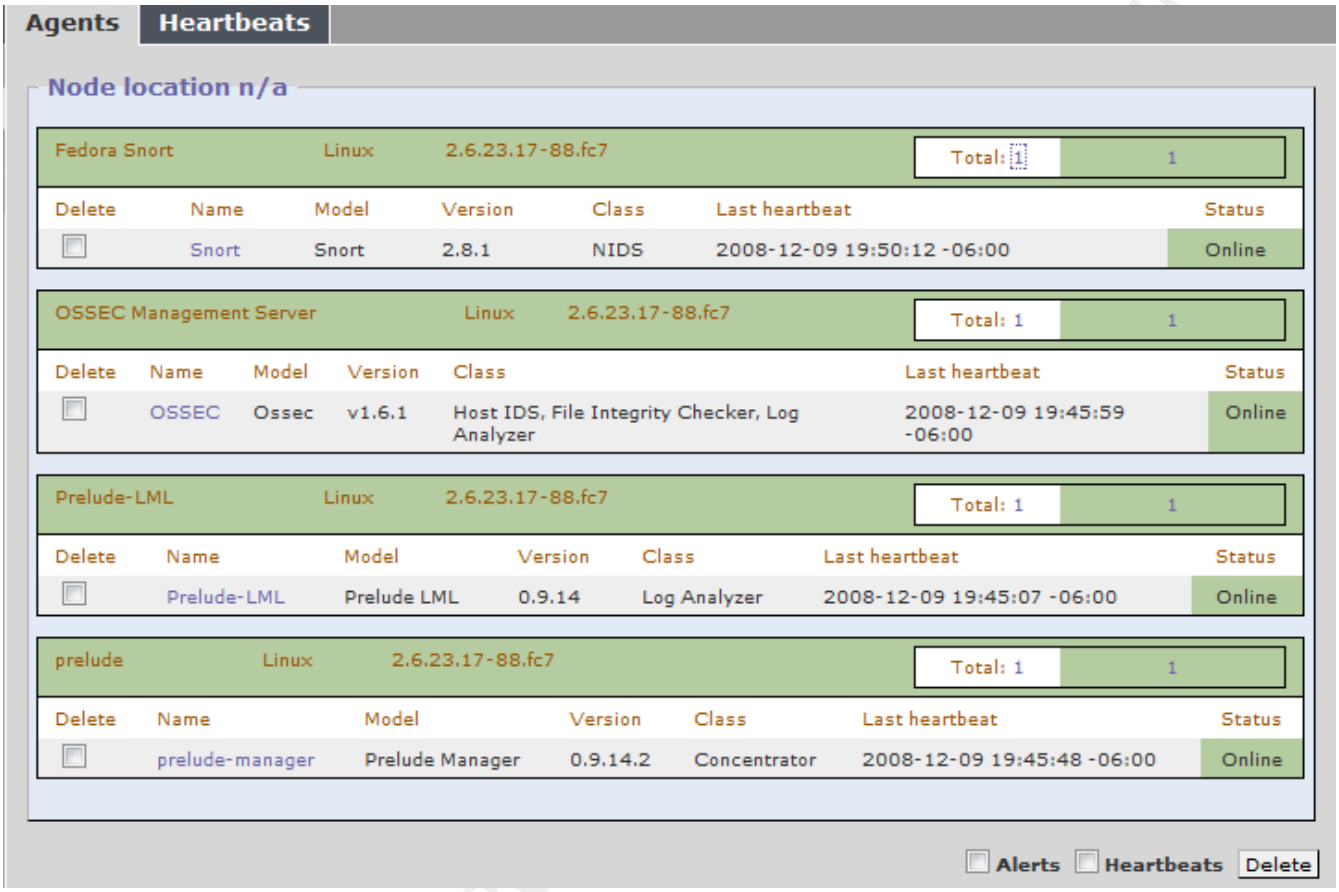
```
0000:    50 72 69 6f 72 69 74 79 20 43 6f 75 6e 74 3a 20    Priority Count:
0010:    35 0a 43 6f 6e 6e 65 63 74 69 6f 6e 20 43 6f 75    5.Connection Cou
0020:    6e 74 3a 20 35 0a 49 50 20 43 6f 75 6e 74 3a 20    nt: 5.IP Count:
0030:    31 0a 53 63 61 6e 6e 65 72 20 49 50 20 52 61 6e    1.Scanner IP Ran
0040:    67 65 3a 20 31 39 32 2e 31 36 38 2e 30 2e 31 32    ge: 192.168.0.12
0050:    35 3a 31 39 32 2e 31 36 38 2e 30 2e 31 32 35 0a    5:192.168.0.125.
0060:    50 6f 72 74 2f 50 72 6f 74 6f 20 43 6f 75 6e 74    Port/Proto Count
0070:    3a 20 35 0a 50 6f 72 74 2f 50 72 6f 74 6f 20 52    : 5.Port/Proto R
0080:    61 6e 67 65 3a 20 38 30 3a 39 31 30 30 0a          ange: 80:9100.
```

ASCII Payload

```
Priority Count: 5
Connection Count: 5
IP Count: 1
Scanner IP Range: 192.168.0.125:192.168.0.125
Port/Proto Count: 5
Port/Proto Range: 80:9100
```

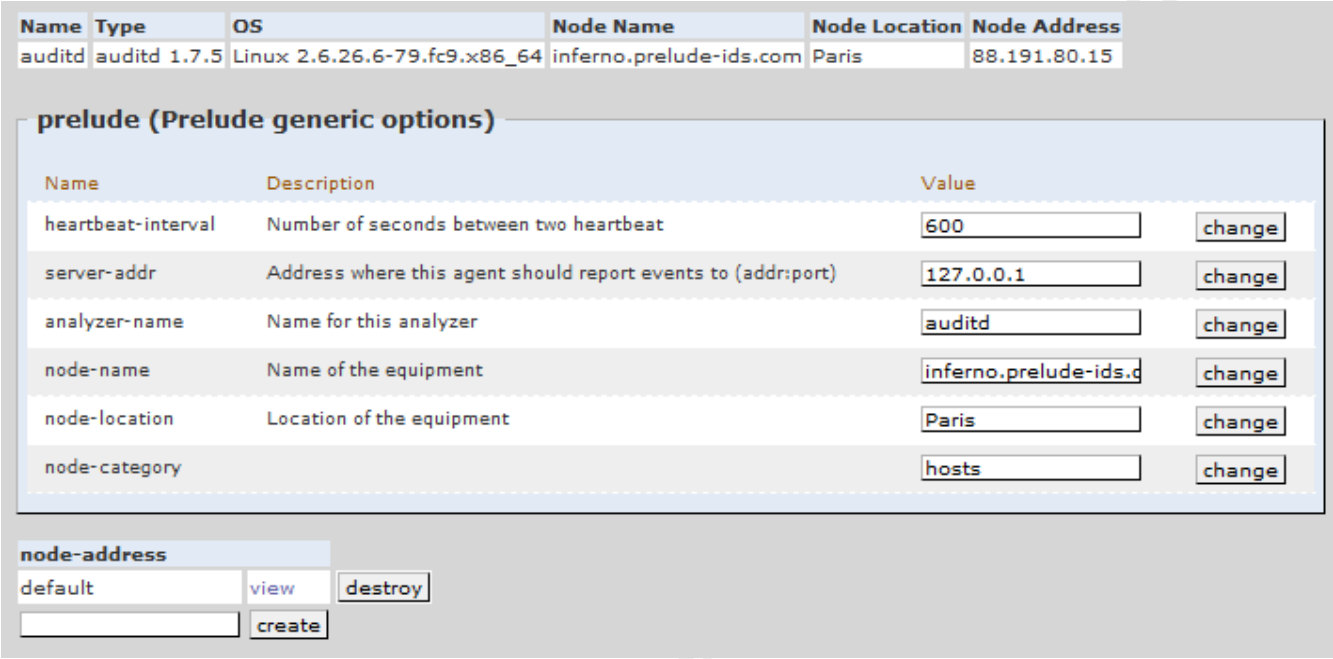
The Agents tab provides a detailed view of the agents that have reported to the Prelude Management Server. The system shows whether a sensor is currently offline or online. Clicking on the device causes a sub menu to appear that displays the alert listing, heartbeat analysis, and heartbeat listing. The Pro version of Prewikka also provides a configuration screen for the agent.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.



The device configuration page allows easy configuration of the selected sensor and its options. The heartbeat-interval, server-address, analyzer-name, node-name, node-location, node-category, and node-address are configurable. This particular feature makes the management of the sensors easier because it does not required direct editing of each configuration file.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.



The Heartbeat tab provides a list of the recent heartbeats that the Management Server has received ("Agents", 2008). Heartbeats are simply a message indicating that the agent is running and reporting. If an organization has an IDS on a quiet segment of the network it may rarely see traffic or generate an alert. Having the heartbeat message sent ensures that the device is working properly, even though it is not generating alerts.

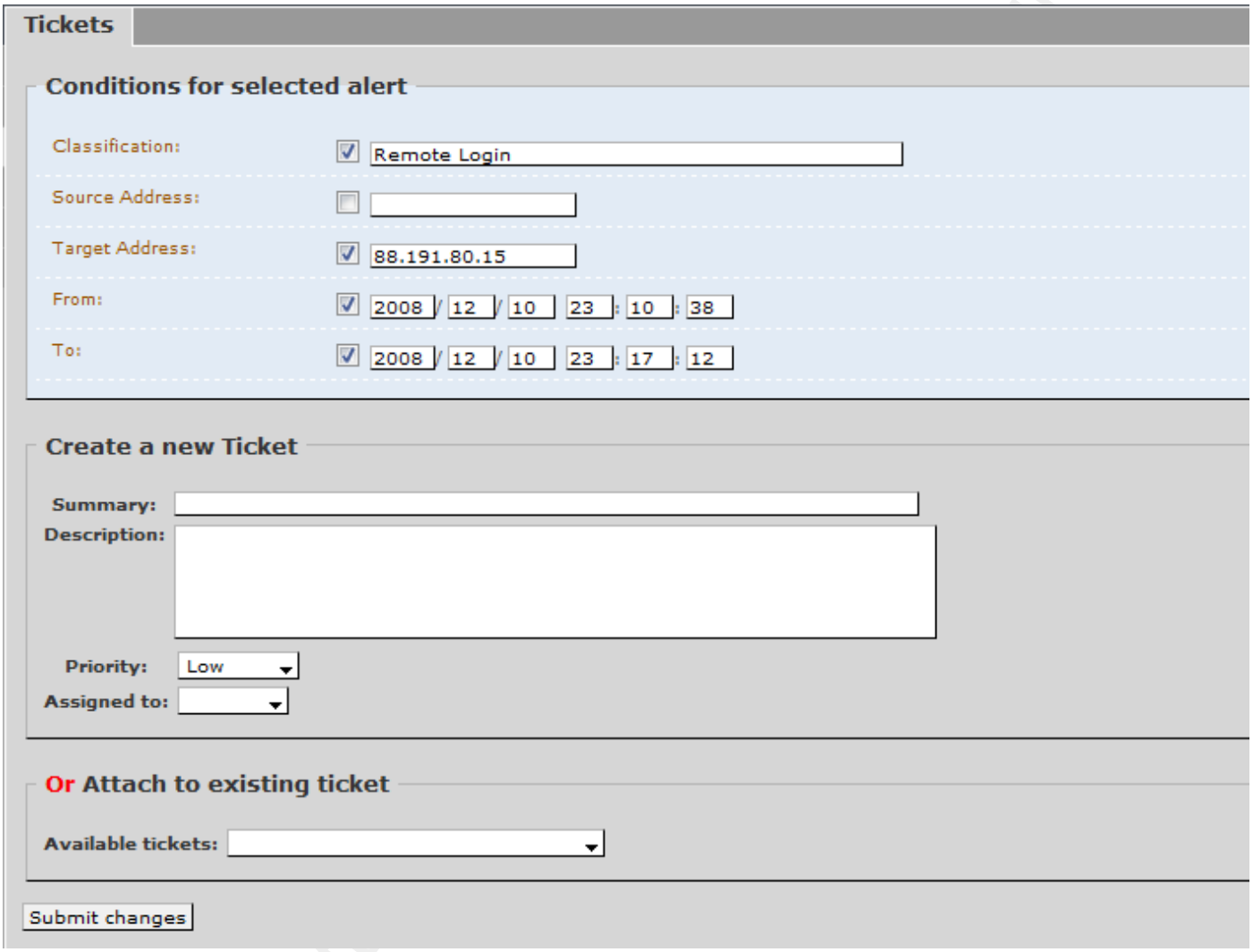
© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Agents | Heartbeats | admin on wednesday 10 december 2008 | logout

Agent	Node address	Node name	Model	Time	
prelude-manager	n/a	prelude	Prelude Manager	16:35:03	
Prelude-LML	n/a	Prelude-LML	Prelude LML	16:29:07	
Snort	n/a	Fedora Snort	Snort	16:28:43	
OSSEC	n/a	OSSEC Management Server	Ossec	16:26:47	
prelude-manager	n/a	prelude	Prelude Manager	16:25:03	
prelude-manager	n/a	prelude	Prelude Manager	16:24:54	
Snort	n/a	Fedora Snort	Snort	07:30:15	
OSSEC	n/a	OSSEC Management Server	Ossec	07:26:13	
prelude-manager	n/a	prelude	Prelude Manager	07:26:12	
Prelude-LML	n/a	Prelude-LML	Prelude LML	07:25:16	
Snort	n/a	Fedora Snort	Snort	07:20:15	
OSSEC	n/a	OSSEC Management Server	Ossec	07:16:13	
prelude-manager	n/a	prelude	Prelude Manager	07:16:12	
Prelude-LML	n/a	Prelude-LML	Prelude LML	07:15:16	
Snort	n/a	Fedora Snort	Snort	07:10:15	
OSSEC	n/a	OSSEC Management Server	Ossec	07:06:13	
prelude-manager	n/a	prelude	Prelude Manager	07:06:12	
Prelude-LML	n/a	Prelude-LML	Prelude LML	07:05:16	
Snort	n/a	Fedora Snort	Snort	07:00:12	
OSSEC	n/a	OSSEC Management Server	Ossec	06:56:13	
prelude-manager	n/a	prelude	Prelude Manager	06:56:12	

The Pro Version of Prewikka features an integrated Ticketing System. This system provides an easy way to track the progress of Security Incidents from inception to remediation. The ticketing system allows the creation of tickets from the real-time events screen. If there is already, a ticket created the system provides the option to append new occurrences to the existing ticket.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

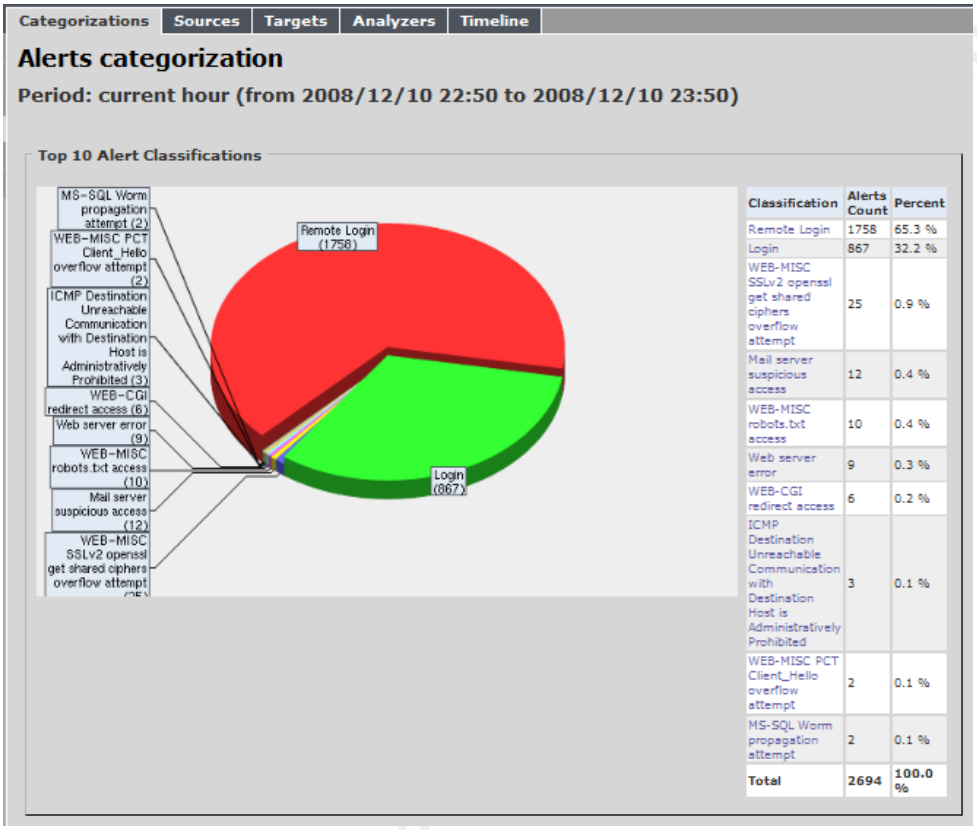


The ticket itself provides various options such as setting the Classification, assigning the source, target, and timeframe. The user can also define the Summary and description of the ticket.

The last feature that is included with the Pro Version is the real-time statistics page. This page displays graphs based on predefined criteria such as, categorizations, sources, targets,

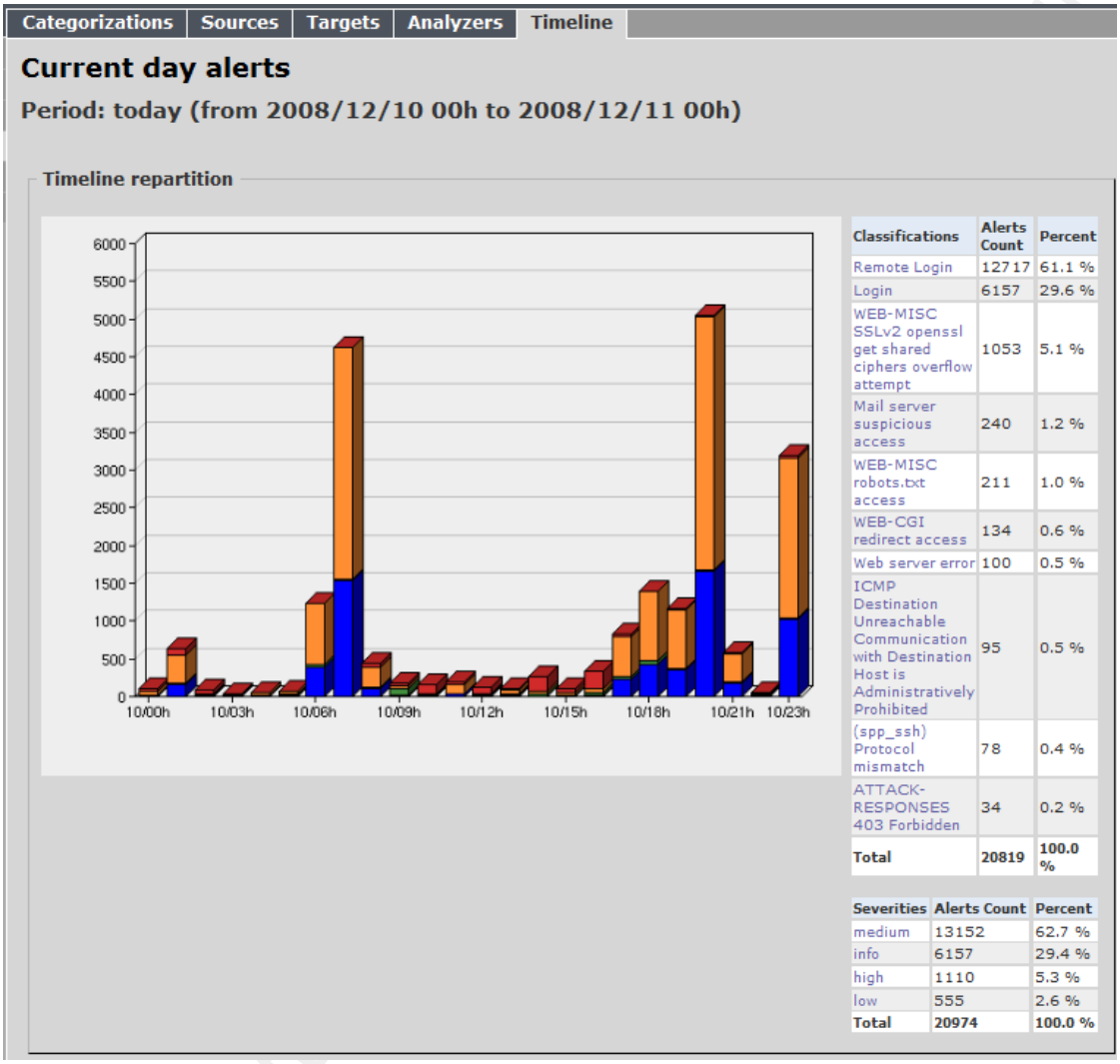
© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

analyzers, and a timeline.



The Statistics view is also configurable to filter data for various timeframes such as hour, day, and month. This allows viewing of attack trends over an extended period. Additionally the statistics view has a few predefined graphs that allow a better view of past activity based on (Categorizations, Sources, Targets, Analyzers, and Timeline).

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.



Classifications	Alerts Count	Percent
Remote Login	12717	61.1 %
Login	6157	29.6 %
WEB-MISC SSLv2 openssl get shared ciphers overflow attempt	1053	5.1 %
Mail server suspicious access	240	1.2 %
WEB-MISC robots.txt access	211	1.0 %
WEB-CGI redirect access	134	0.6 %
Web server error	100	0.5 %
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	95	0.5 %
(spp_ssh) Protocol mismatch	78	0.4 %
ATTACK-RESPONSES 403 Forbidden	34	0.2 %
Total	**20819**	**100.0 %**

Severities	Alerts Count	Percent
medium	13152	62.7 %
info	6157	29.4 %
high	1110	5.3 %
low	555	2.6 %
Total	**20974**	**100.0 %**

5.7 PFLogger:

The PFLogger is the component used to collect logs from OpenBSD’s PF software. Packet Filter (PF) is OpenBSD's system for filtering TCP/IP traffic and doing Network Address Translation (“PF: The OpenBSD Packet Filter,” 2009, Packet Filtering). When installed Prelude’s PFLogger listens at OpenBSD’s PF redirect logged packet,

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

and sends alerts to the Prelude Manager ("Prelude Components", 2005).

6. Installation

The difficulty of Prelude's installation solely depends on the Operating System chosen and its current support. The following is a brief overview of the installation. It is out of the scope of this paper to provide a systematic installation guide. Below is the list of items that are required on the system before attempting to compile Prelude's components ("Prelude Installation Requirements", 2005).

- GnuTLS (Required by Libprelude)
- Python (Required for Libprelude, LibpreludeDB Python bindings, and Prewikka)
- PCRE (Required by Prelude-LML)
- LUA (Required by Prelude-Correlator)
- Database (MySQL, PostgreSQL, SQLite)

Some Operating Systems already contain the Prelude Packages and only require installation via the included software management. If the OS chosen does not contain the pre-compiled packages, Prelude will require manual compilation. This takes a bit more time for installation but ultimately ensures that the software will work

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

properly with the current configuration. As of this writing, the following Operating Systems have packages for Prelude ("Package Installation", 2005)

- Debian
- Fedora
- FreeBSD
- Gentoo
- Mac OSX
- NetBSD
- OpenBSD

Once installation is complete, each sensor is required to register with the management server before successful communication. When initiating registration the Management Server will create a unique identity for the sensor, create a directory used by the sensor, and it will generate a signed X509 certificate to allow communication based on the set permissions ("Agent Registration", 2005).

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

7. Benefits of Prelude (Case Studies)

As mentioned previously, Prelude can help organizations:

- Achieve Regulatory Compliance
- Reduce Security Costs
- Monitor all Devices
- Monitor Events in Real-Time

Organizations are required to be compliant with various Government regulations. Depending on the organizations Industry, they must meet certain requirements or face fines and or other legal penalties. Today, all merchants using payment cards, including electronic commerce merchants and service providers must comply with the PCI Data Security Standard or they will face fines of up to $500,000 per incident of non-compliance (Nir Gertner, 2005). Prelude can help organizations meet compliance by giving them the information that they need to validate their policies. Since Prelude normalizes all logs and stores it in a centralized location organizations can easily generate reports from the Prewikka Interface.

Storing the information centrally makes the data easily accessible. This also creates a Forensic trail for the logs. For example, ABC Credit Union is a mid-size organization with 300

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

employees spread across three branches. Each branch has an independent connection to the internet as well as a site-to-site VPN. Let us pretend that ABC Credit Union has a break in at one of its branches.

The attacker was able to compromise one of the servers and gain admin privileges. In an attempt to cover, his or her tracks they decided to clear the log files of their activity. Since Prelude collects logs from all devices, the server still sent its logs to the Prelude Management server. This results in ABC Credit Union still having a trace of the server breach.

Prelude also has the ability to reduce costs by increasing efficiency and reducing the amount of time spent analyzing logs. According to Jean-FRANÇOIS DÉCHANT, a 2006 IBM survey reported that of 700 European IT managers questioned, over 45% receive over 4,000 security alerts every second from their IT systems. This makes it impossible for them to identify IT real threats. One in ten IT departments spend more than three days a week analyzing security log data (Jean-FRANÇOIS DÉCHANT, December 2006).

Let us consider ABC Credit Union again. Even though the organization only has 300 employees and 3 branches, it would not be impossible for the devices to generate millions of logs a day.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Considering that, a large part of the logs does not require any immediate attention there is no need to have many people trying to analyze them all.

Since Prelude increases efficiency, analysts are able to spend more time on real threats. Once the network has been base lined for normal activity, filters reduce the amount of alerts generated. All of the logs are still stored in the database but the security team will only need to analyze events of interest. Let us consider that ABC Credit Union has an External and Internal IDS, and a Firewall Between them.

The on duty Analyst begins to see some portscan events from the External IDS destined to internal servers. Using Prelude the Analyst can quickly determine whether this activity requires additional investigation by reviewing the events from the devices along the attack path. If the analyst sees firewall drop events then the firewall has done its job and blocked the attack thus requiring no further investigation.

Prelude is able to monitor all network devices regardless of the log format or device. This consolidates all monitoring into one system. It also requires no modifications to the existing environment. ABC Credit Union has devices from multiple vendors that

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

log differently. Preludes interoperability allows them to monitor their Firewalls, Servers, and Intrusion Detection Systems all from the Prewikka Console.

Prelude also benefits organizations by allowing real-time event viewing. Historically logs required manual review. Due to the various formats and amount, there was no way to accomplish this in real-time. Since Prelude automates the analysis of logs, users are able to see actionable items almost instantly thus reducing the amount of time that it takes to respond to an incident.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

8. References

DÉCHANT, Jean-FRANÇOIS, (December, 2006). View from the Top of IT Security. Retrieved on February 9, 2009, from Enterprise Networks and Servers: http://www.enterprisenetworksandservers.com/monthly/art.php?2848

H. Debar, D. Curry, B. Feinstein, (March, 2007). The Intrusion Detection Message Exchange Format (IDMEF). Retrieved on December 15, 2008, from IETF Web Site: http://www.ietf.org/rfc/rfc4765.txt

Prelude Solutions, (2005). "Universal SIM". Retrieved on October 7, 2008, from Prelude-IDS Web Site: http://www.prelude-ids.com/en/solutions/universal-sim/index.html

Prelude IDS, (October, 2007). Prelude User Manual. Retrieved on October 15, 2008, from Prelude-IDS Web Site: https://trac.prelude-ids.org/wiki/ManualUser

Prelude IDS, (2005). Prelude Manager. Retrieved on November 8, 2008, from the Prelude IDS Web Site: https://trac.prelude-ids.org/wiki/PreludeManager

Prelude IDS, (2005). Prelude-LML. Retrieved on November 8, 2008, from the Prelude IDS Web Site: https://trac.prelude-ids.org/wiki/PreludeLml

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Prelude IDS, (2005). Prelude Components.
Retrieved on November 16, 2008, from the Prelude IDS Web Site:
https://trac.prelude-ids.org/wiki/PreludeComponents

Prelude IDS, (2005). Package Installation.
Retrieved on December 6, 2008, from the Prelude IDS Web Site:
https://trac.prelude-ids.org/wiki/InstallingPackage

Prelude IDS, (2005). Agent Registration.
Retrieved on December 6, 2008, from the Prelude IDS Web Site:
https://trac.prelude-ids.org/wiki/InstallingAgentRegistration

Prelude IDS, (2005). Manual Prewikka "Agents".
Retrieved on December 23, 2008, from the Prelude IDS Web Site:
https://trac.prelude-ids.org/wiki/ManualPrewikka/Agents

OpenBSD FAQs, (2009, January 07). PF: The OpenBSD Packet Filter.
Retrieved on January 13, 2009, from OpenBSD Web Site:
http://www.openbsd.org/faq/pf/

Prelude IDS, (2005). Prelude Compatibility.
Retrieved on January 20, 2009, from the Prelude IDS Web Site
https://trac.prelude-ids.org/wiki/PreludeCompatibility

Nir Gertner, (August 8, 2005).PCI Compliance: Don't Become another
Headline. Retrieved on February 9, 2009, from ZDNet News Site:
http://news.zdnet.com/2100-1009_22-144105.html

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

APPENDIX A

IDMEF-Criteria Filter:

```
[idmef-criteria]
rule = alert.classification.text == User login failure
rule = alert.assessment.impact.severity == high
hook = smtp[default]
```

The above filter would use the SMTP output plugin "hook=smtp[default]" for events matching User Login failure "rule=alert.classification.text == User login failure" and classify it as high "alert.assessment.impact.severity == high".

Thresholding-Filter:

```
[thresholding]
path = alert.classification.text == Logon Failure,
alert.source.node.address.address == 192.168.0.1
threshold = 600
count = 20
hook = relaying[default]
```


© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The above filter will forward every twentieth event “count=20” within 600 seconds “threshold=600” that matches the unique combination of Logon Failure “path = alert.classification.text == Logon Failure,” and source IP of 192.168.0.1 “alert.source.node.address.address == 192.168.0.1” to the **default** instance of the **relaying** reporting plugin “hook=relaying[default]”. Additionally the use of Limit field can completely suppress alerts for the specified time period.

Stacked Filter:

```
[idmef-criteria-filter=sshbf]
rule = alert.classification.text == 'SSH Brute Force Attempt'
hook = thresholding[sshbf]

[thresholding=sshbf]
path = alert.classification.text,
alert.target(0).node.address(0).address
threshold = 1
seconds = 3600
hook = smtp[default]

[smtp]
sender = prelude@mycompanyname.com
```


© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

```
recipients = me@mycompanyname.com
smtp-server = mailserver.mycompanyname.com
```

The above filter looks for the string SSH Brute Force Attempt “rule = alert.classification.text == 'SSH Brute Force Attempt'” in an IDMEF alert called sshbf “[idmef-criteria-filter=sshbf]”. When a event matches the filter it is passed to the thresholding plugin “hook= thresholding[sshbf]”. The sshbf instance of the Thresholding Plugin “[thresholding=sshbf]” will then keep track of the SSH Brute Force Attempt text “rule=alert.classification.text == ‘SSH Brute Force Attempt’” along with the target IP address “alert.target(0).node.address(0).address”. Additionally the “threshold= 1” combined with the seconds of “seconds=3600” will cause only one alert to be sent to the SMTP plugin every hour.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**