JUNE 18–20, 2008

Audit and IDS

Steve Grubb, Red Hat

Linux Audit and Intrusion Detection Systems

- Review audit system
- Learn a little about some threats
- Overview of IDMEF
- Introduction to prelude

Audit System's Uses

- Watch file accesses
- Monitor system calls
- Record commands run by user
- Record security events
- Search for events
- Run summary reports

Audit Requirements

Shall be able to record at least the following:

- Date and time of event, type of event, subject identity, and outcome
- Sensitivity labels of subjects and objects
- Be able to associate event with identity of user causing it
- All modifications to audit configuration and attempted access to logs
- All uses of authentication mechanisms
- Changes to any trusted database
- Attempts to import/export information
- Be able to include/exclude events based on user identity, subject/object labels, other attributes

Syscall Audit Rules

Follows the general form:

-a filter,action -S syscall -F field=value -k “rule-note”

Example to see opens by users that failed due to permission:

-a exit,always -S open -F exit=-EACCES -F auid>=500 -F auid!=4294967295

-F can be one of: a0, a1, a2, a3, arch, auid, devmajor, dir, devminor, exit, user/group ids, filetype, inode, msgtype, object/subject context parts, path, perms, pid, ppid, or success.

“and” created by adding more “-F” name/value pairs. An “or” is created by adding a new rule.

Results are evaluated by the filter to decide if event is auditable

File System Audit Rules

File system audit rules take the general form of:

-w /full/path-to-file -p wrxa -k “rule note”

Can also be expressed as syscall audit rule:

-a exit,always -F path=/full/path-to-file -F perm=wrxa -k “rule note”

The perm field selects the syscalls that are involved in file writing, reading, execution, or attribute change.

Trusted Apps

- All entry point programs must set loginuid
- Apps that modify trusted databases were updated to send audit event records:
  - amtu, aide
  - at, vixie-cron
  - coreutils
  - dbus, glibc (nscd)
  - gdm, kdm, xdm.
  - openssh, pam, util-linux, vsftpd
  - passwd, shadow
  - nss

Pam IDS updates

pam_tally2

- Locks out an account for consecutive failed login attempts
- Sends ANOM_LOGIN_FAILURES

pam_access

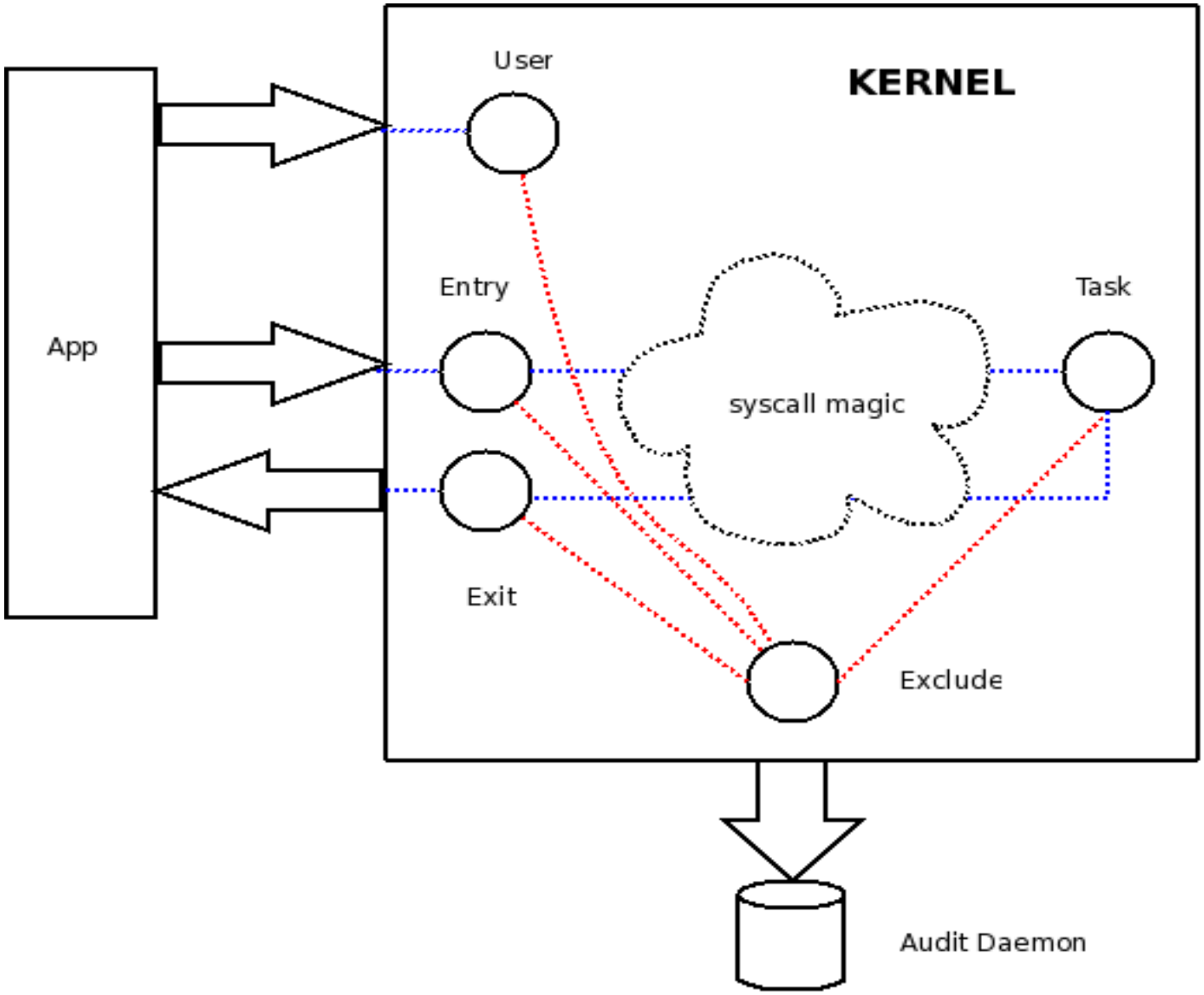
- Used to forbid logins from certain locations, consoles, and accounts
- /etc/security/access.conf controls its config
- Sends ANOM_LOGIN_ACCT and ANOM_LOGIN_LOCATION

pam_time

- Used to forbid logins during non-business hours
- /etc/security/time.conf controls its config
- Sends ANOM_LOGIN_TIME

pam_limits

- Used to limit maximum concurrent sessions and other user restrictions
- /etc/security/limits.conf controls its config
- Sends ANOM_LOGIN_SESSIONS


User
KERNEL
App
Entry
Task
syscall magic
Exit
Exclude
Audit Daemon

ausearch results

type=PATH msg=audit(06/06/2008 14:15:19.373:3588) : item=1 name=/tmp/svck4.tmp/svd8l.tmp inode=168834 dev=08:07 mode=file,600 ouid=sgrubb ogid=sgrubb rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0

type=PATH msg=audit(06/06/2008 14:15:19.373:3588) : item=0 name=/tmp/svck4.tmp/ inode=168794 dev=08:07 mode=dir,775 ouid=sgrubb ogid=sgrubb rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0

type=CWD msg=audit(06/06/2008 14:15:19.373:3588) : cwd=/home/sgrubb

type=SYSCALL msg=audit(06/06/2008 14:15:19.373:3588) : arch=x86_64 syscall=unlink success=yes exit=0 a0=7fff66ec9340 a1=7fff66ec92a0 a2=14 a3=3e831eadc0 items=2 ppid=4030 pid=4041 auid=sgrubb uid=sgrubb gid=sgrubb euid=sgrubb suid=sgrubb fsuid=sgrubb egid=sgrubb sgid=sgrubb fsgid=sgrubb tty=(none) ses=1 comm=simpress.bin exe=/usr/lib64/openoffice.org/program/simpress.bin subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=delete

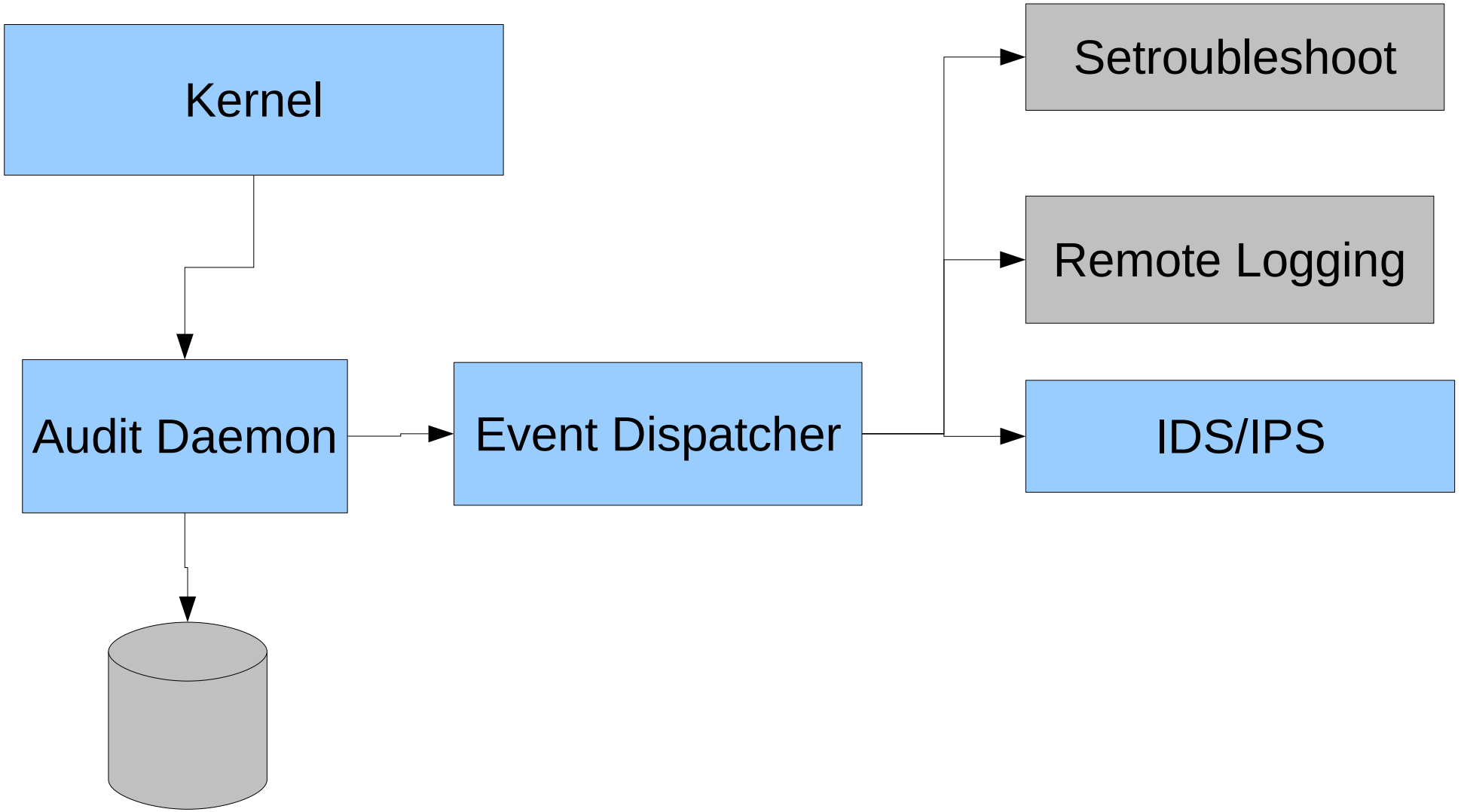
aureport results

Summary Report
======================
Range of time in logs: 05/27/2008 09:28:34.600 - 06/07/2008 09:31:58.719
Selected time for report: 06/06/2008 00:00:00 - 06/07/2008 09:31:58.719
Number of changes in configuration: 113
Number of changes to accounts, groups, or roles: 0
Number of logins: 4
Number of failed logins: 0
Number of authentications: 17
Number of failed authentications: 0
Number of users: 2
Number of terminals: 13
Number of host names: 4
Number of executables: 115
Number of files: 41551
Number of AVC's: 10
Number of MAC events: 8
Number of failed syscalls: 1284
Number of anomaly events: 3
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 4
Number of process IDs: 1006
Number of events: 44470

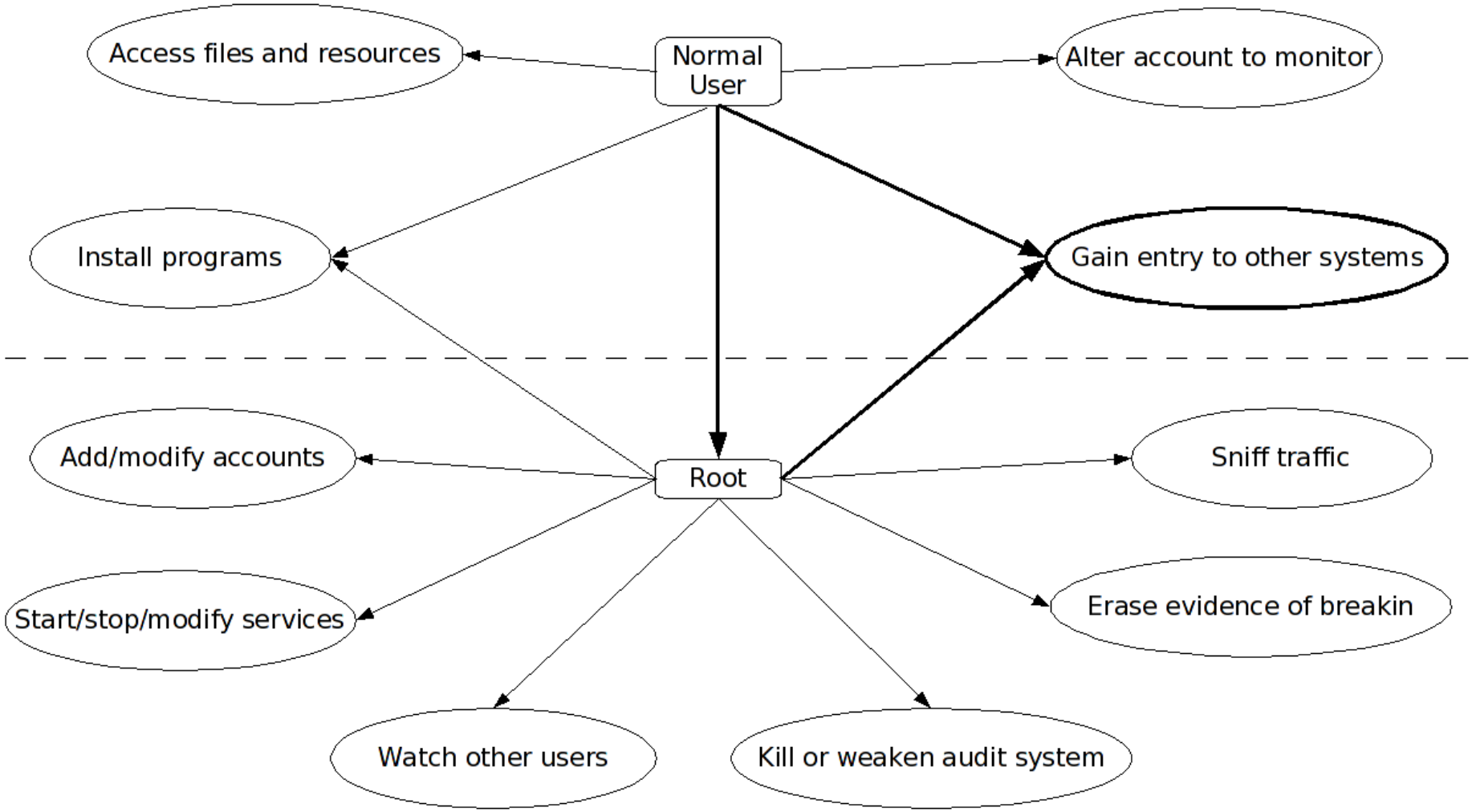
aureport --file

File Summary Report
==========
total file
==========
776 /usr/bin/
763 /usr/lib64/
690 /var/lib/PackageKit/
690 /var/lib/PackageKit/transactions.db-journal
670 /usr/include/linux/
366 /usr/share/mimelnk/application/
254 /usr/share/apps/katepart/syntax/
248 /usr/share/doc/HTML/en/kdelibs-apidocs/kio/bookmarks/html/
182 /dev/.udev/queue/
166 /var/run/hald/
166 /var/run/hald/acl-list
140 /usr/share/services/
108 /lib/modules/2.6.25.4-30.fc9.x86_64/kernel/drivers/ata/
41 /var/run/ConsoleKit/database~

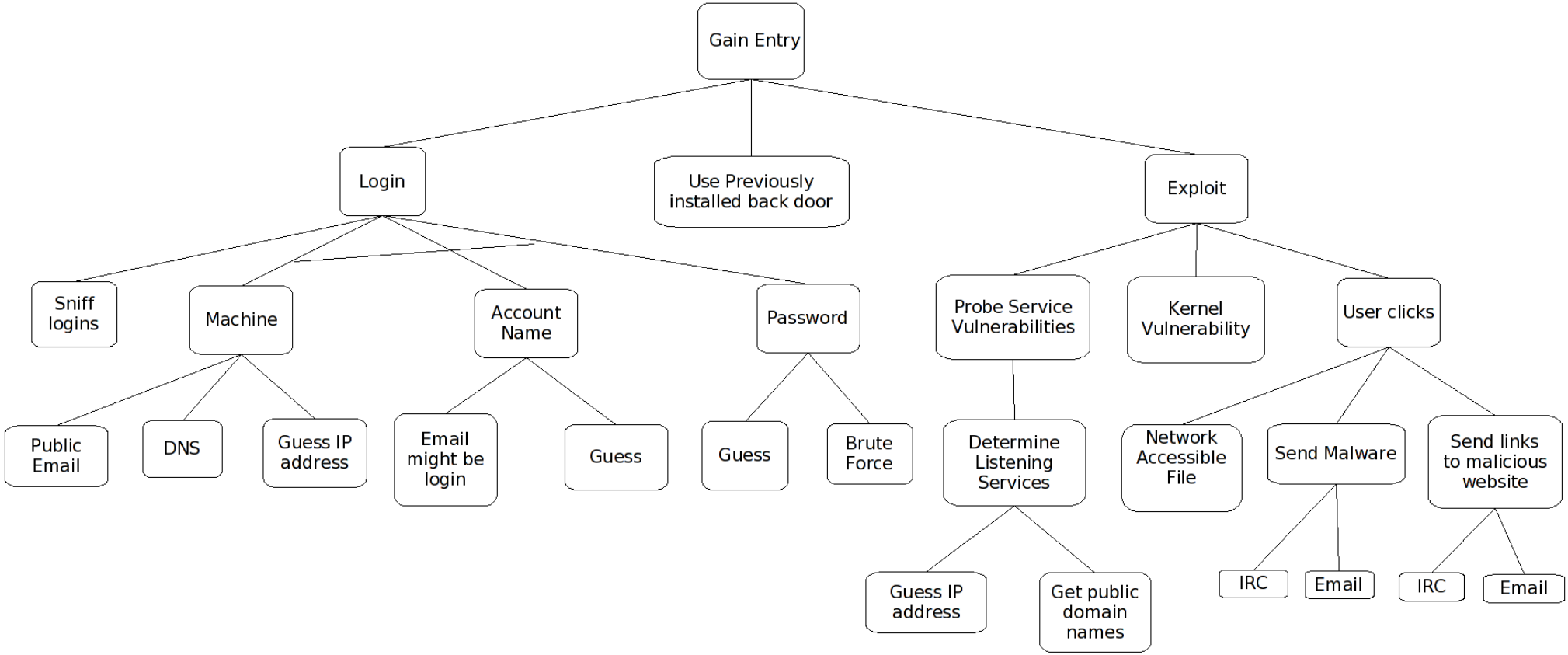
Audit System Data Flow



Intrusion Goals

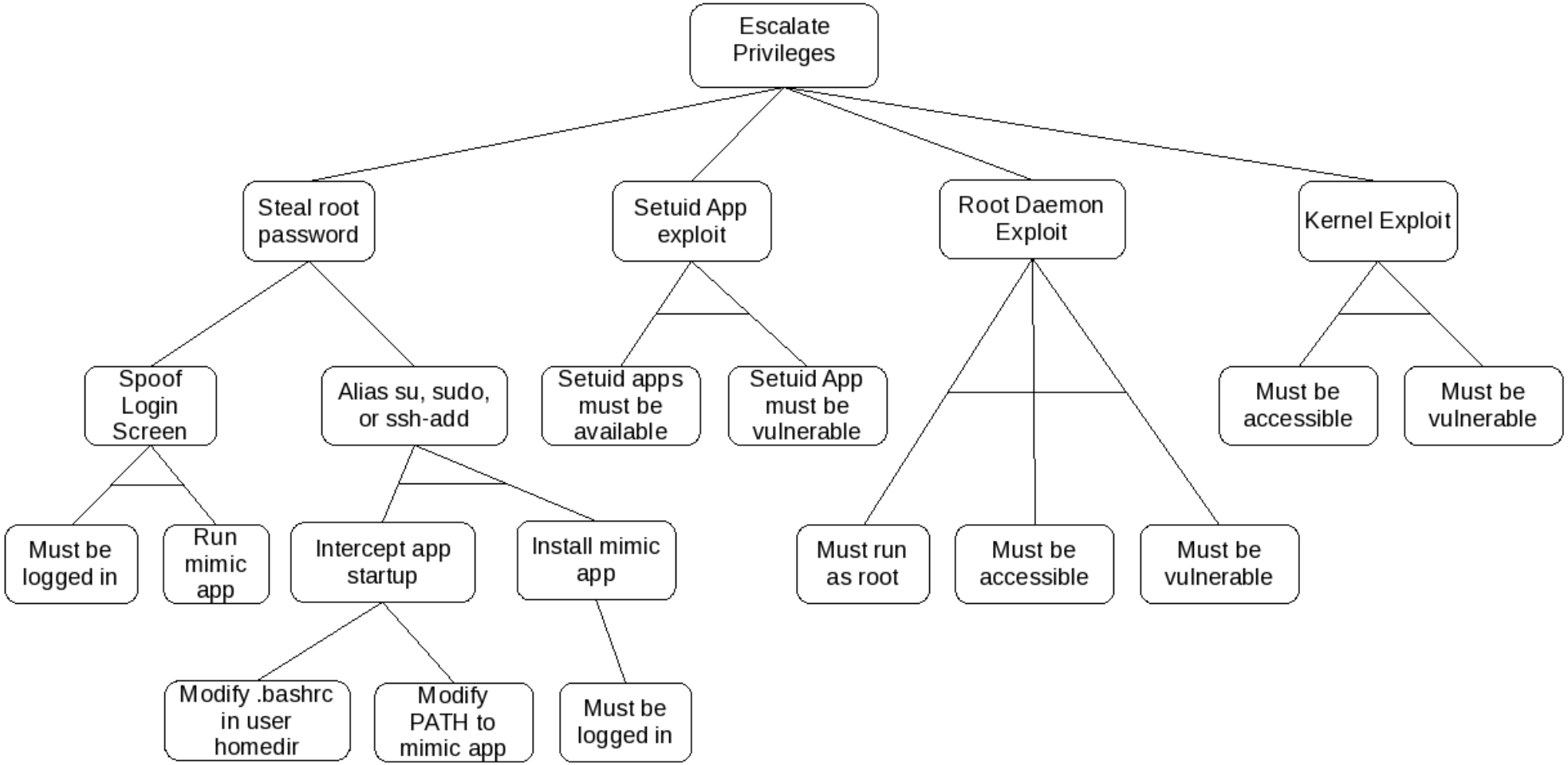


Network Intrusion Attack Tree



Steve Grubb, Red Hat

Privilege Escalation Attack Tree



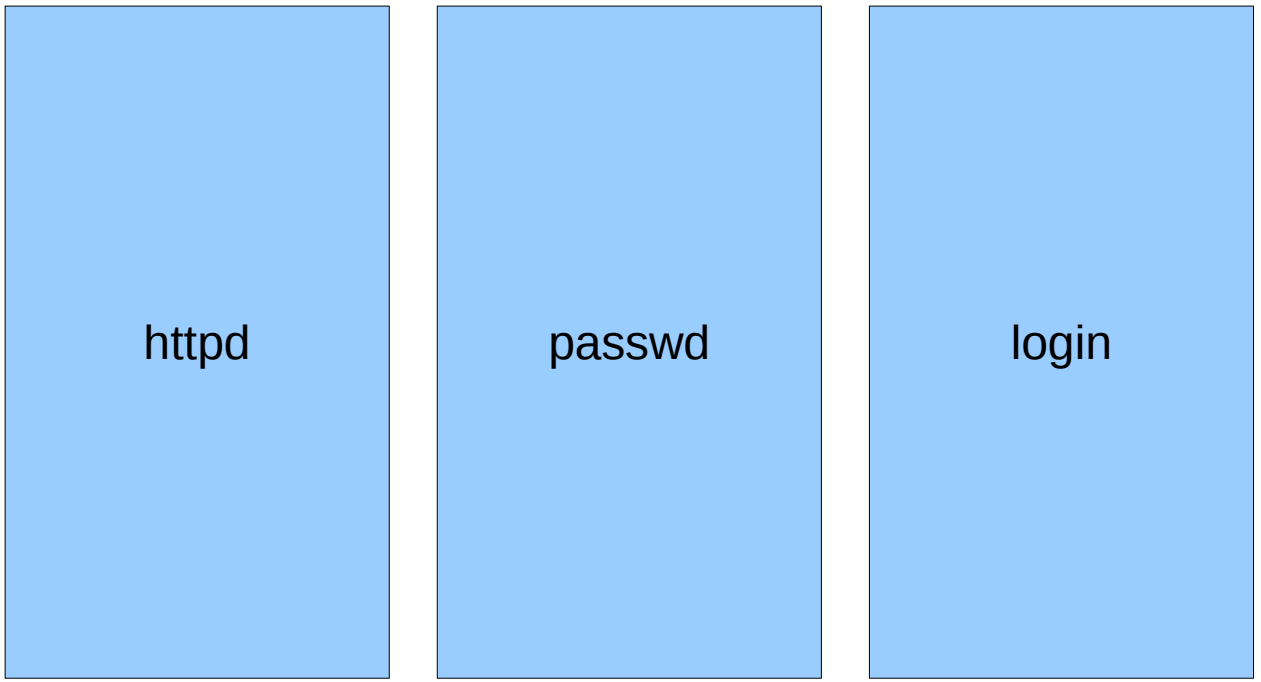
audisp-prelude

- Audispd plugin that reads audit stream
- Identifies suspicious events
- Sends most interesting ones to prelude-manager
- Has 15 different configurable detections
- Has a test mode so that it can be checked
  - Takes input from stdin
  - Must be raw log format (ausearch –raw > ./test.log)
  - /sbin/audisp-prelude –test < ./audit-test.log | less

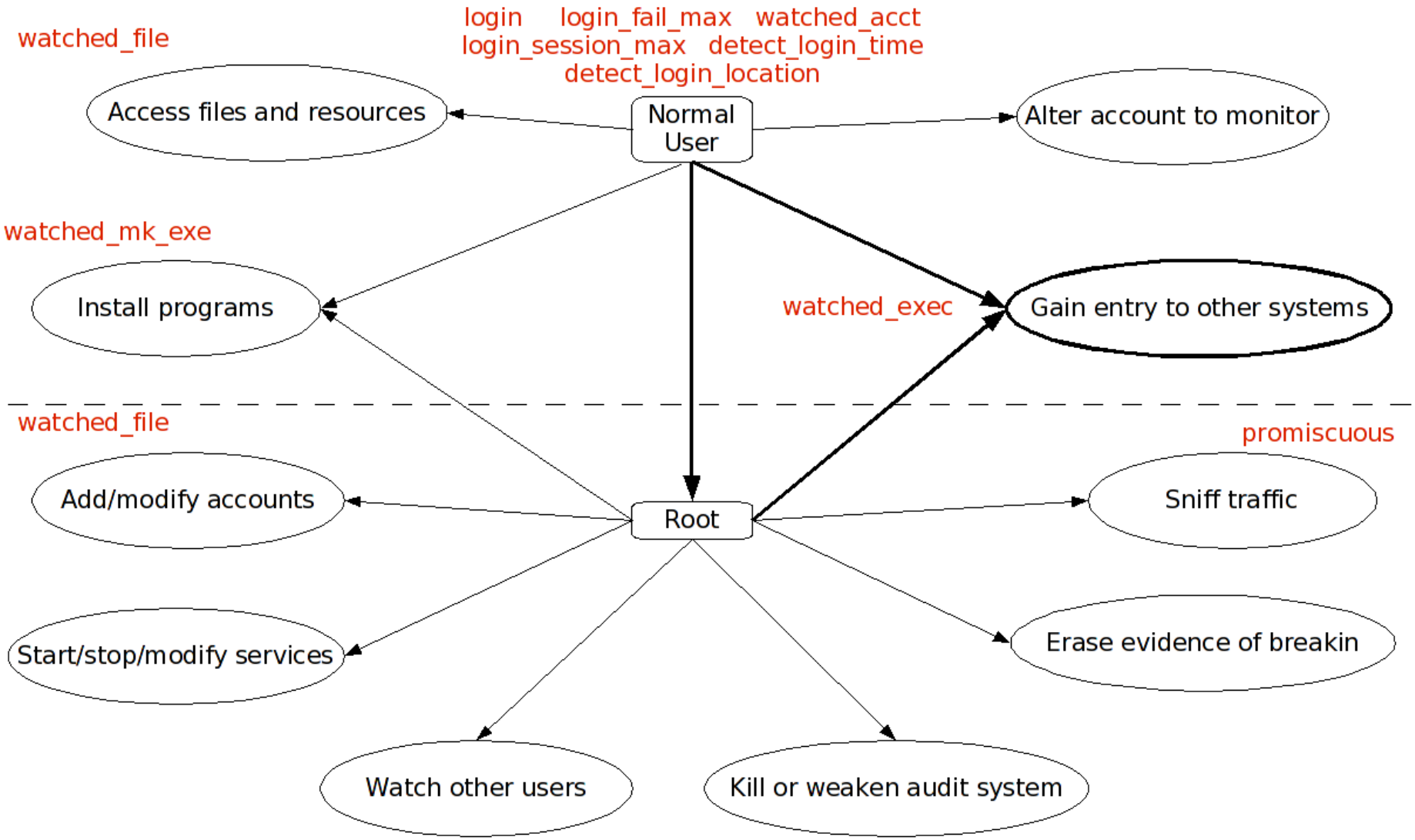
Audisp-prelude Detections

Controlled by /etc/audispd/audisp-prelude.conf
detect_avc – SE Linux AVCS
detect_logins – detects any login
detect_login_fail_max – detects output from pam_tally2
detect_login_session_max – detects output from pam_limits
detect_login_location – detects output from pam_access
detect_login_time – detects output from pam_time
detect_abend – detects any abnormal terminations: segv, abort
detect_promiscuous – detects opening of promiscuous socket
detect_mac_status – detects changes in SE LINUX configuration
detect_group_auth – detects failures in group password auth
detect_watched_acct – detects any login for account being watched
detect_watched_file – detects access to file being watched
detect_watched_exec – detects execution of specific programs
detect_watched_mk_exe – detects the creation of executables

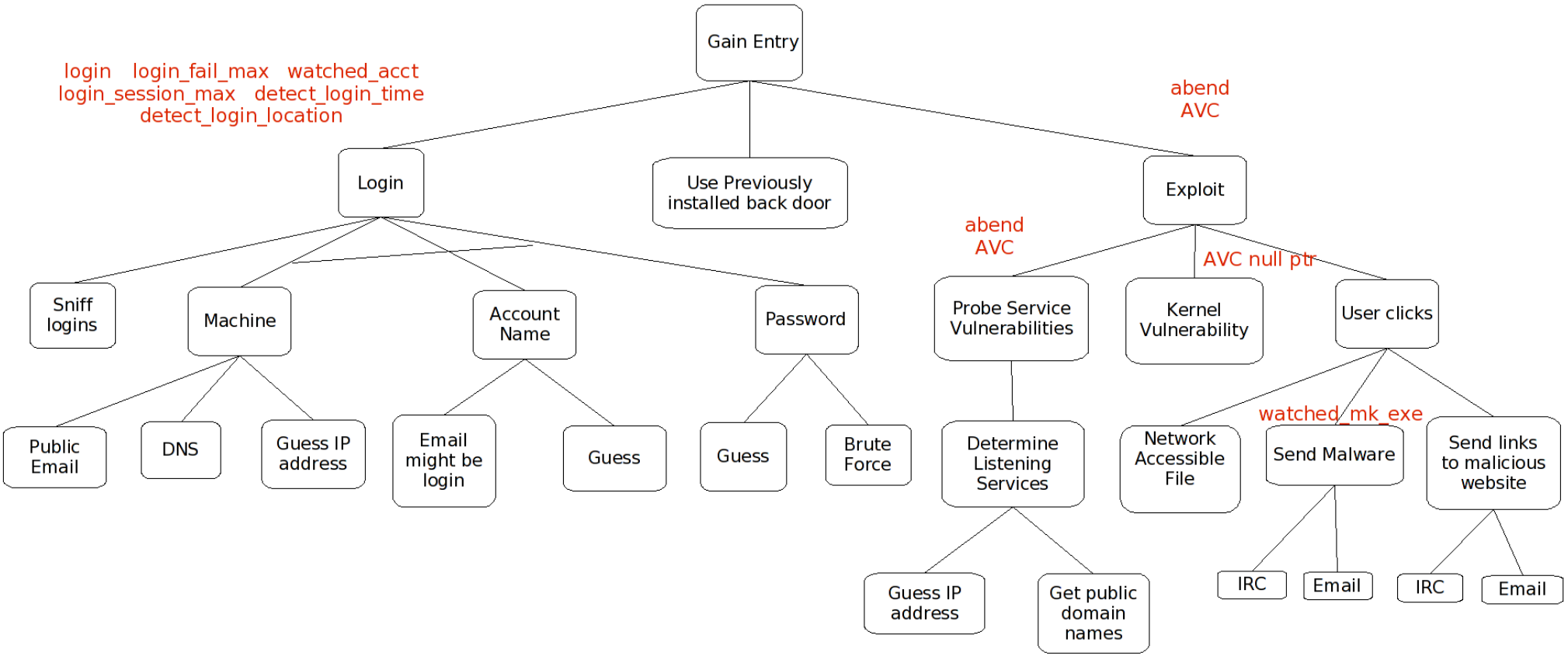
SE Linux records a program's behavioral model



Intrusion Goals & Detections

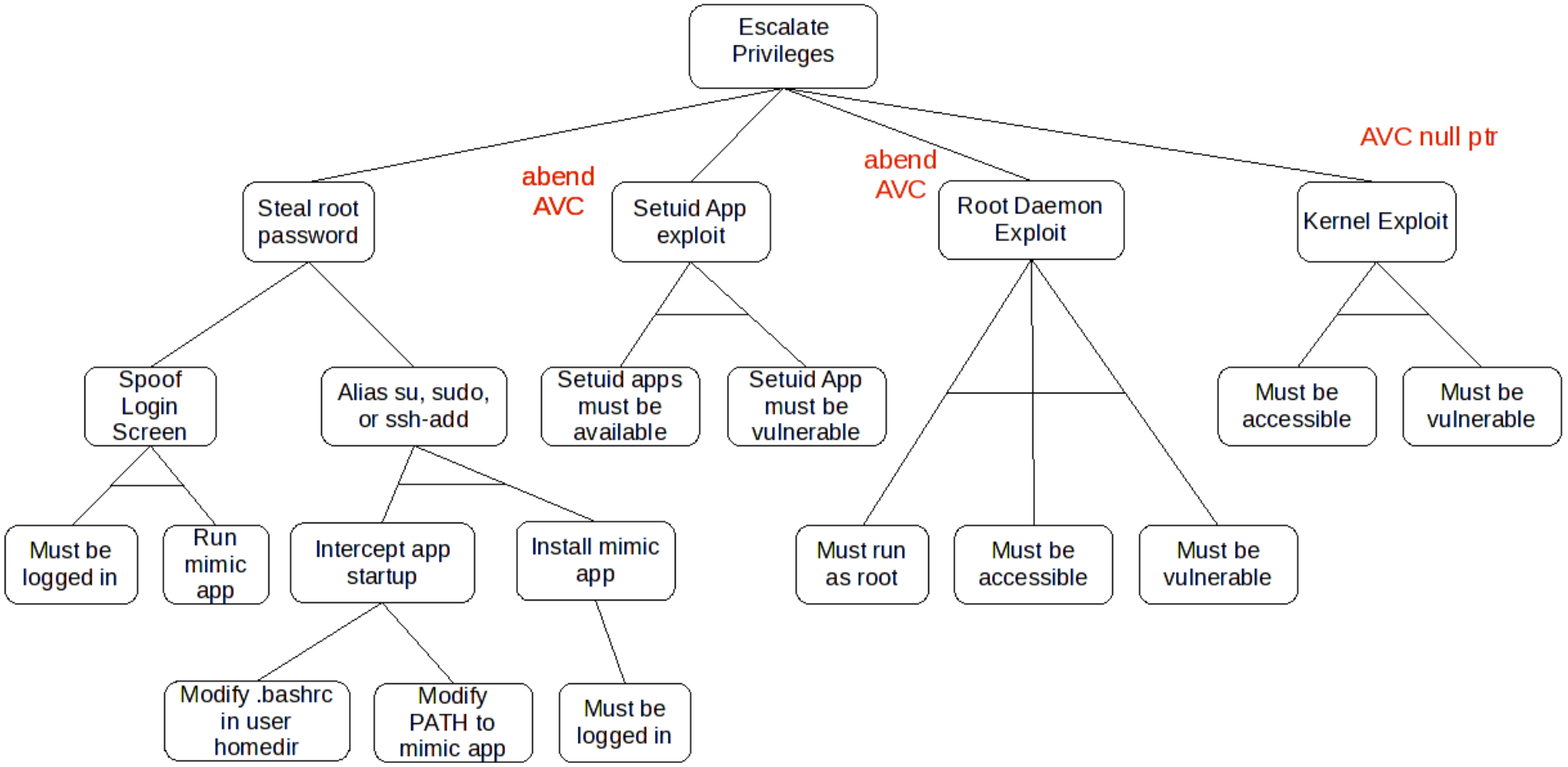


Network Intrusion Attack Tree & Detections



Steve Grubb, Red Hat

Privilege Escalation Attack Tree & Detections



Watched File, exec, mk_exe

- Requires special audit rules
  - -k ids-type-severity
    - Ids gets the attention of key processor
    - Type - file, exec, or mkexe
    - Severity - info, low, med, or hi

```
-a exit,always   -F path=/full-path/file   -F perm=wa   -k ids-file-med
-a exit,always   -F path=/full-path/file   -F perm=x   -k ids-exec-med
-a exit,always  -S chmod  -F dir=/home -F a1&0111  -F filetype=file  -k ids-mkexe-hi
```

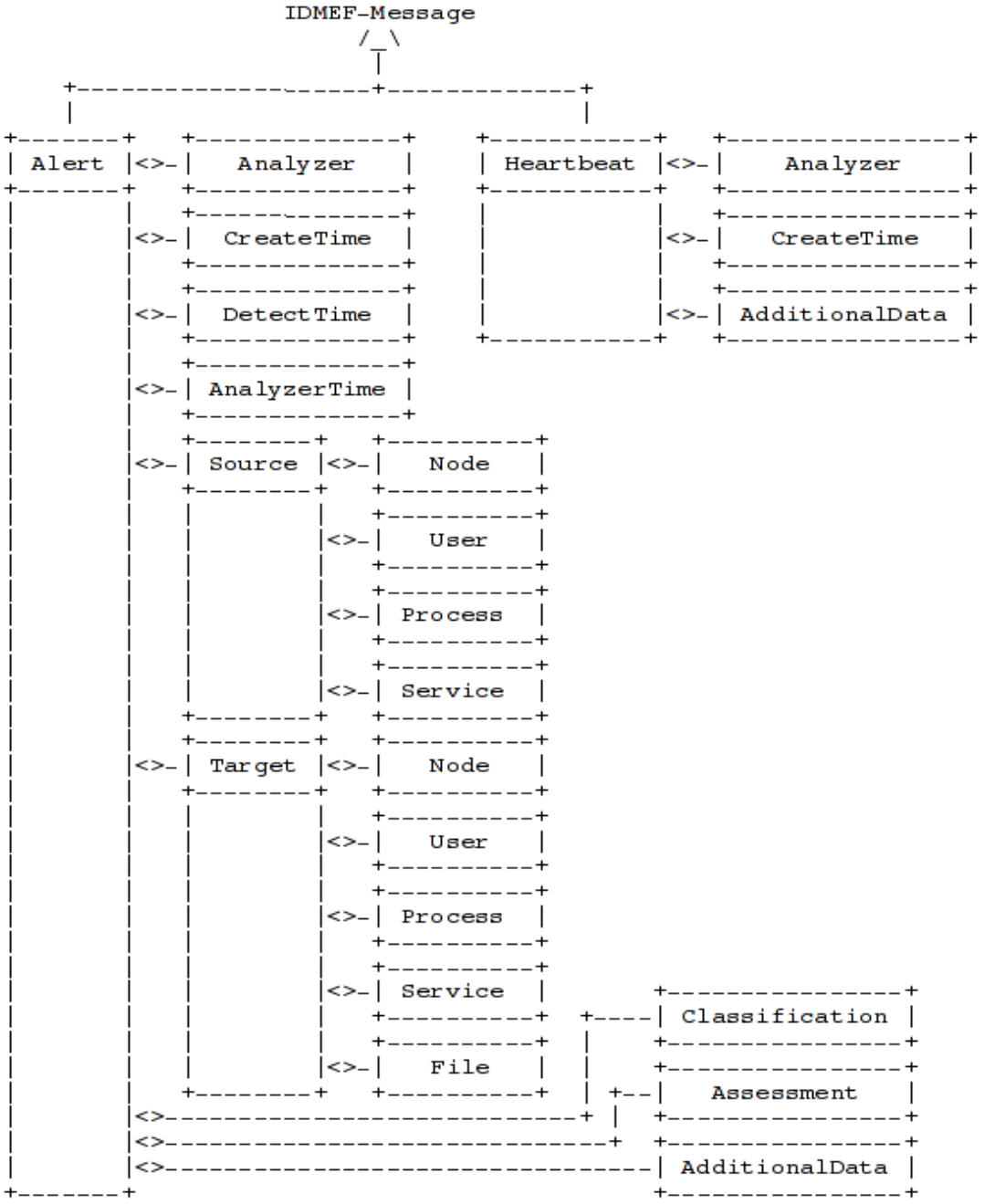
What to do with this info?

- Audit system is now an active component
- Have the ability to pick out events
- Hard to watch all machines
- Many events overwhelm people because hard to pick out what's important

- The key is central collection, escalation, and correlation

IDMEF

- Intrusion Detection Message Exchange Format
- Governed by IETF RFC 4765
- Describes XML format
  - What parameters are available
  - How to represent values
  - Network protocol
- Normalizes events so programs from different vendors, OS, and devices can in theory interoperate
- libprelude.so provides a complete and mature IDMEF library


IDMEF-Message
Alert
Analyzer
CreateTime
DetectTime
AnalyzerTime
Source
Node
User
Process
Service
Target
Node
User
Process
Service
File
Heartbeat
Analyzer
CreateTime
AdditionalData
Classification
Assessment
AdditionalData

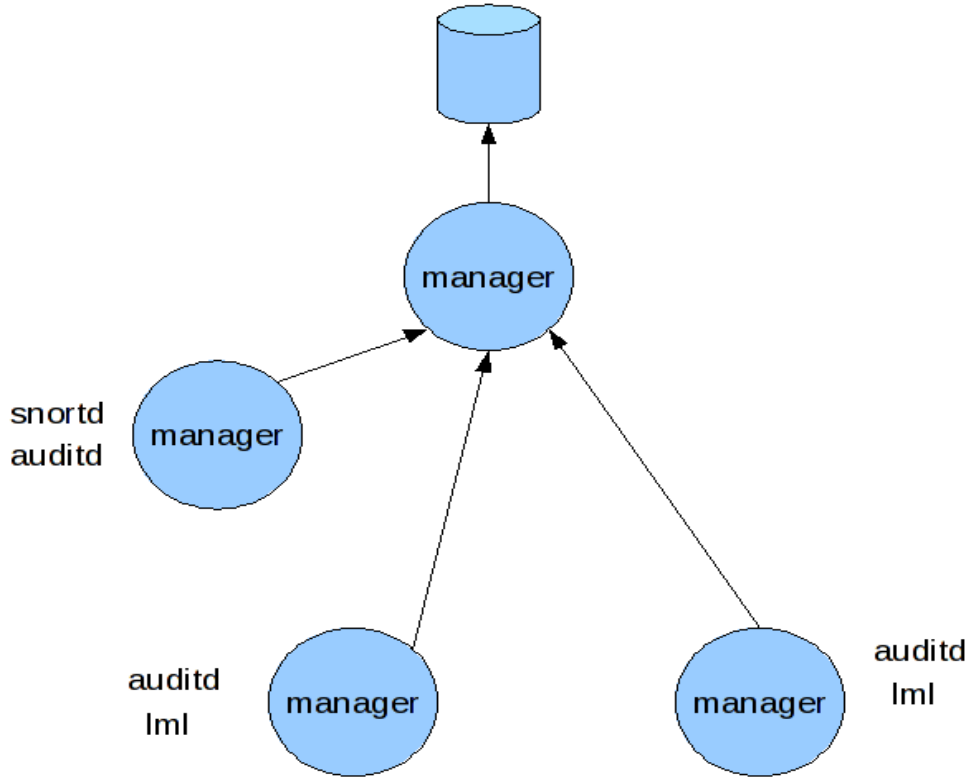
Prelude

- Full featured Hybrid-IDS
- Has many sensors
- Has event aggregation
- Correlate many events
- Can alert in realtime
- Event notification pop-ups

Hybrid IDS

- Host Based IDS not very prone to false positives
  - Event either happened or it didn't
  - You have full context of what the event means
- Network Based IDS can generate false positives
  - New protocols can look like attack
  - Can only report what it sees
  - Might not be able to decrypt some traffic
  - Limited context about what really happening
- Hybrid Mixes the two

Prelude Architecture



Prelude Sensors

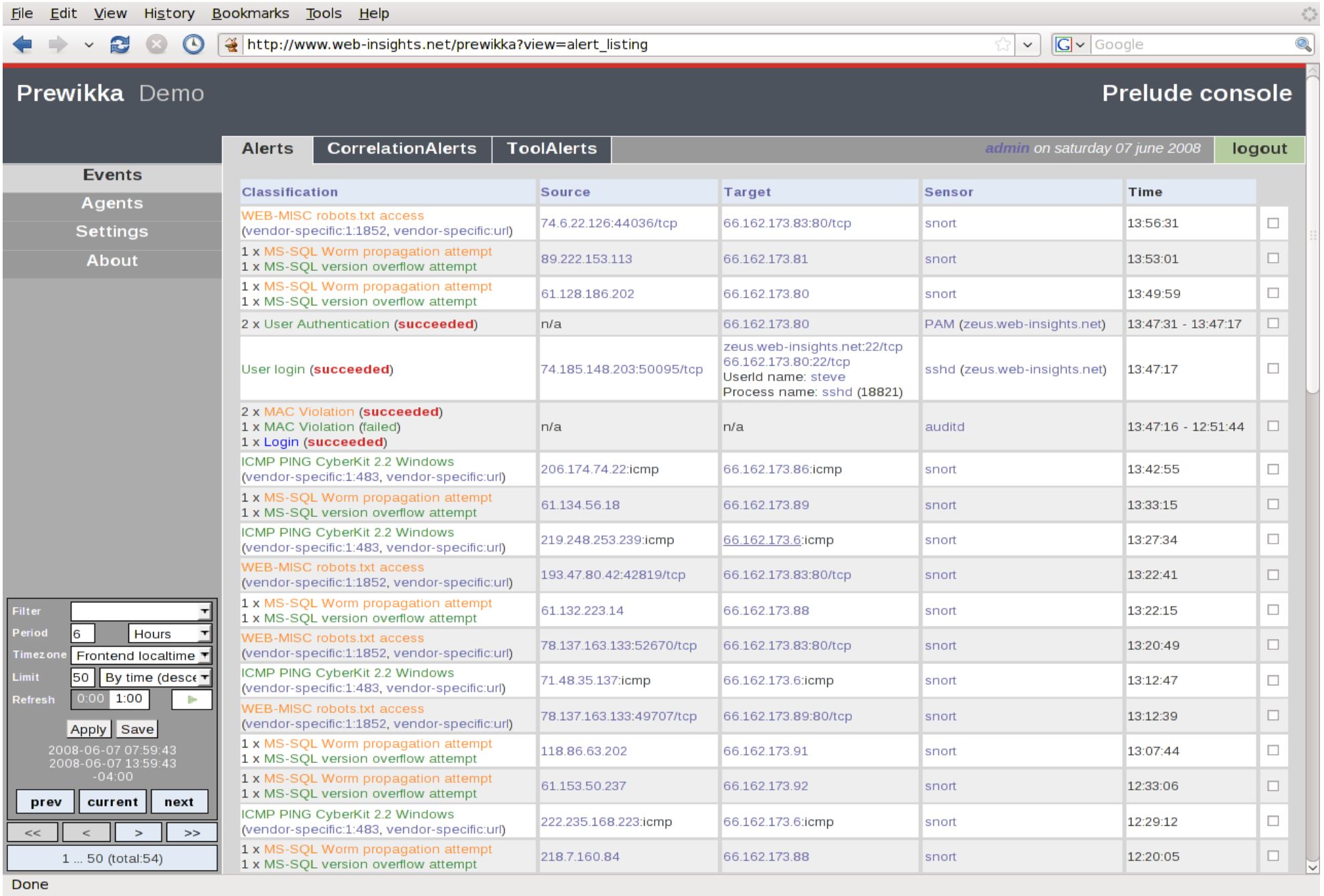
- Audit
- Snortd
- Samhain
- OSSEC
- Nepenthes
- NuFW
- LML
  - Pam
  - Apache
  - Syslog
  - Arpwatch
  - Cisco equipment
  - Asterisk
  - Clamav
  - Nagios
  - Portsentry
  - Postfix
  - Sonicwall
  - Spamassassin
  - webmin

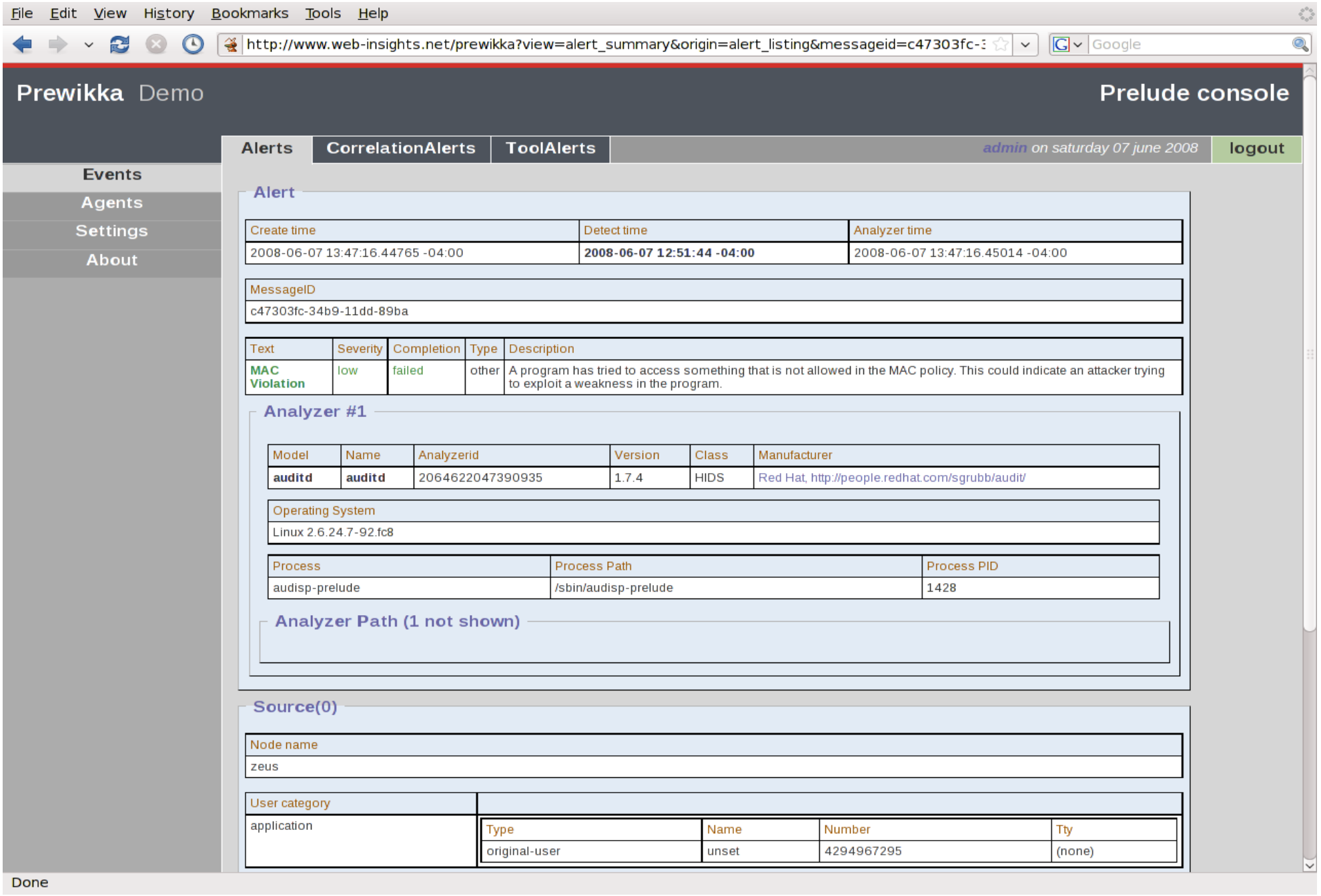
Libprelude communication

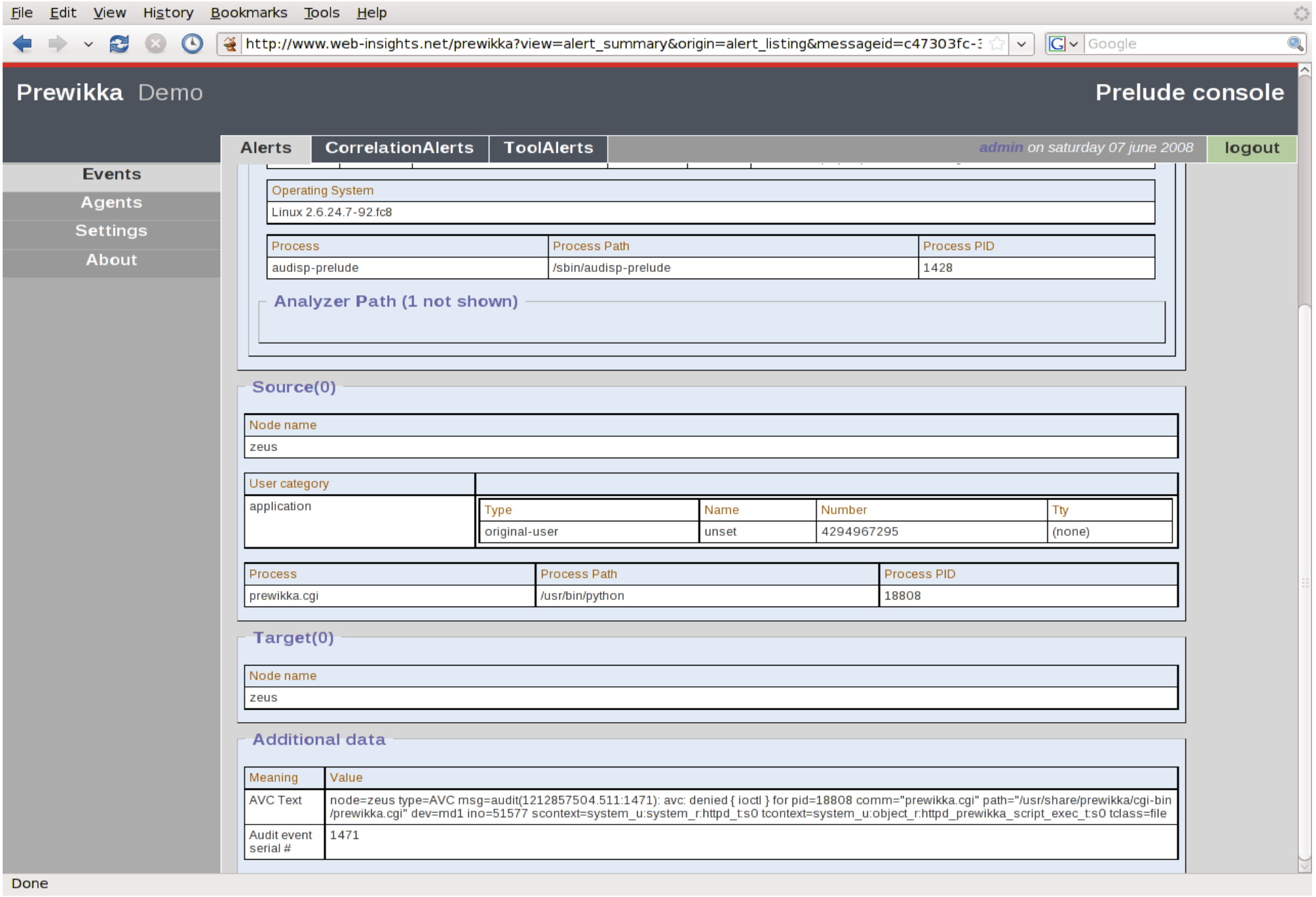
- Sensor must be registered to its manager
- Communication is encrypted
- Failover capability when cannot contact manager
- Relay events from manager to manager
- Reverse relay to keep DMZ secure

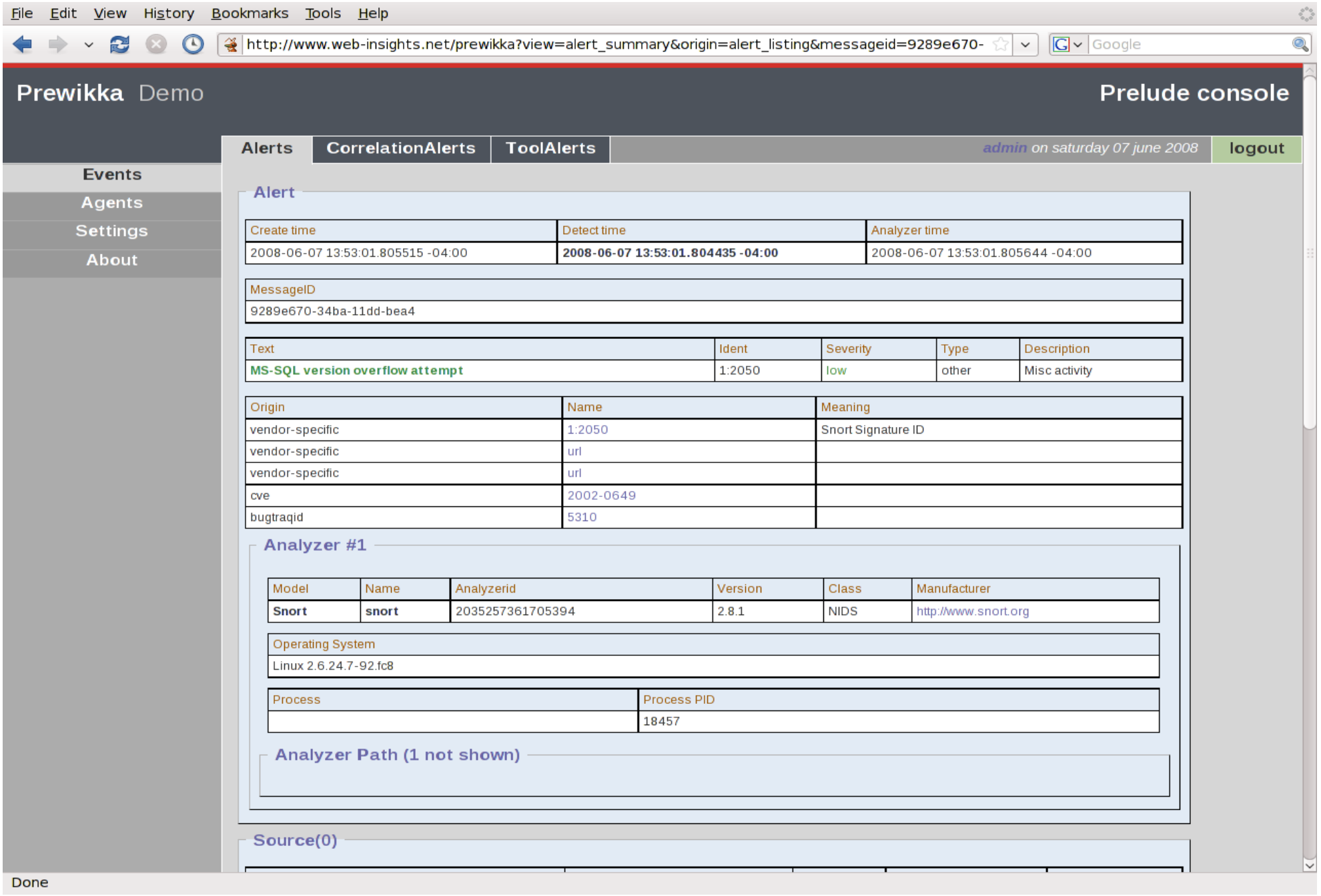
Visualize Alerts - Prewikka

- Apache based cgi-bin
- Has database of recent alerts
- Allows multiple users with different permissions
- Sort/select alerts by type, host, target, severity, sensor, and many more ways at the top of the columns.




File Edit View History Bookmarks Tools Help
http://www.web-insights.net/prewikka?view=alert_summary&origin=alert_listing&messageid=c47303fc-3
Google
Prewikka Demo
Prelude console
Alerts
CorrelationAlerts
ToolAlerts
admin on saturday 07 june 2008
logout
Events
Agents
Settings
About
Alert
Create time
Detect time
Analyzer time
2008-06-07 13:47:16.44765 -04:00
2008-06-07 12:51:44 -04:00
2008-06-07 13:47:16.45014 -04:00
MessageID
c47303fc-34b9-11dd-89ba
Text
Severity
Completion
Type
Description
MAC Violation
low
failed
other
A program has tried to access something that is not allowed in the MAC policy. This could indicate an attacker trying to exploit a weakness in the program.
Analyzer #1
Model
Name
Analyzerid
Version
Class
Manufacturer
auditd
auditd
2064622047390935
1.7.4
HIDS
Red Hat, http://people.redhat.com/sgrubb/audit/
Operating System
Linux 2.6.24.7-92.fc8
Process
Process Path
Process PID
audisp-prelude
/sbin/audisp-prelude
1428
Analyzer Path (1 not shown)
Source(0)
Node name
zeus
User category
application
Type
Name
Number
Tty
original-user
unset
4294967295
(none)
Done





File Edit View History Bookmarks Tools Help

http://www.web-insights.net/prewikka?view=alert_summary&origin=alert_listing&messageid=9289e670-

Google

Prewikka Demo

Prelude console

Alerts | CorrelationAlerts | ToolAlerts

admin on saturday 07 june 2008 | logout

- Events
- Agents
- Settings
- About

Source(0)

Node name (resolved)	Node address	Port	ip_version	Protocol
89.222.153.113	89.222.153.113	3067	4	udp

Target(0)

Node name (resolved)	Node address	Port	ip_version	Protocol
66.162.173.81	66.162.173.81	1434	4	udp

Additional data

Meaning	Value
snort_rule_sid	2050
snort_rule_rev	12

Network centric information

IP

Version	Header length	TOS	Length	Id	R F	D F	M F	Ip offset	TTL	Protocol	Checksum	Source address	Target address
4	5	0	404	44437				0	56	17	61568	89.222.153.113	66.162.173.81

UDP

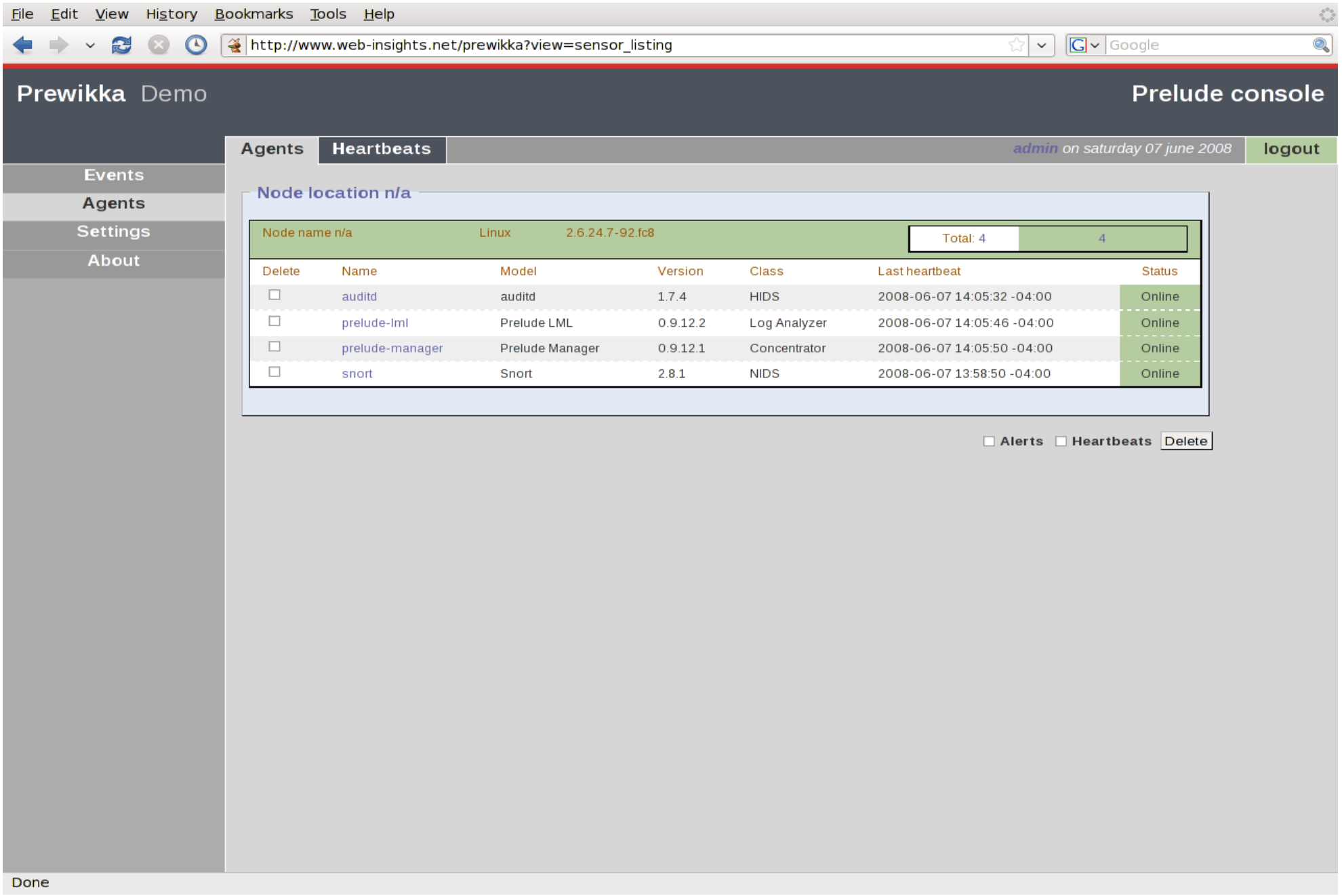
Source port	Target port	Length	Checksum
3067	1434	384	17933

Payload

Payload

```
0000:    04 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01    ................
0010:    01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01    ................
0020:    01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01    ................
0030:    01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01    ................
0040:    01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01    ................
0050:    01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01    ................
0060:    01 dc c9 b0 42 eb 0e 01 01 01 01 01 01 01 70 ae    ....B.........p.
0070:    42 01 70 ae 42 90 90 90 90 90 90 90 90 68 dc c9    B.p.B........h..
0080:    b0 42 b8 01 01 01 01 31 c9 b1 18 50 e2 fd 35 01    .B.....1...P..5.
0090:    01 01 05 50 89 e5 51 68 2e 64 6c 6c 68 65 6c 33    ...P..Qh.dllhel3
00a0:    32 68 6b 65 72 6e 51 68 6f 75 6e 74 68 69 63 6b    2hkernQhounthick
00b0:    43 68 47 65 74 54 66 b9 6c 6c 51 68 33 32 2e 64    ChGetTf.llQh32.d
00c0:    68 77 73 32 5f 66 b9 65 74 51 68 73 6f 63 6b 66    hws2_f.etQhsockf
00d0:    b9 74 6f 51 68 73 65 6e 64 be 18 10 ae 42 8d 45    .toQhsend....B.E
```

Done



Future Directions

- Add Brouette
  - Offers real-time alerts via libnotify
- Add mod_security2 log format parsing for LML
  - This is the biggest hole in HIDS capability now
- Add more sensors
  - Rogue DHCP detection
  - Integrate passive asset detection
- Add more detections for auditd sensor
  - Changing uid
  - Account changes
  - Test Failures (amtu, aide, RBAC, sectool)
  - Crypto failures

Future Directions

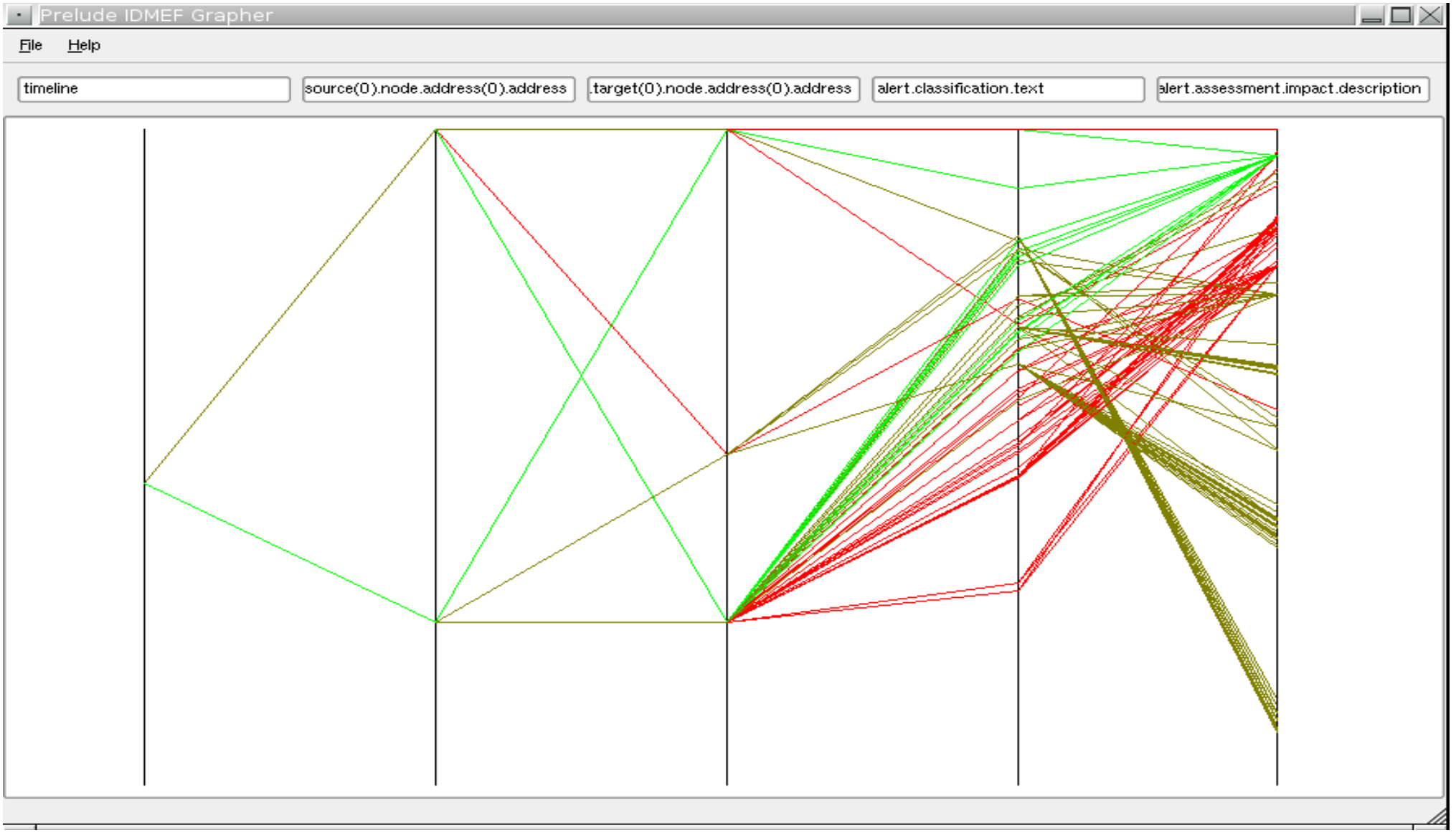
Correlation when Engine is ready

- Provide framework for higher level analysis
- Reconstruct sequence of events
- Detect Targets, Protocols, Tools, etc
- Adapt Severity Rating
- Allow filtering to suppress false positive
- Improve accuracy by scoring alerts
- Reactive Countermeasure

Visualization tools

- PIG – Prelude IDMEF Grapher

Nessus Scan


Prelude IDMEF Grapher
File
Help
timeline
source(0).node.address(0).address
target(0).node.address(0).address
alert.classification.text
alert.assessment.impact.description

Future Directions

There are weaknesses in the IDMEF spec

- Seems to have been designed from snort's PoV
- No way to express some HIDS concepts
  - Roles are not in spec
  - No concept of sensitivity
  - In the case of promiscuous socket target is network
  - Not allowed to say results were indeterminate
  - Data Source Identifier should be in spec
  - Can't say source of attack is a service or program
  - Access of shadow -is maore than just a FILE attack, its an attack on the credentials

Seems like a new spec is in order to fix these deficiencies

Questions ?

HOWTO

http://people.redhat.com/sgrubb/audit/prelude.txt

Audit Info

http://people.redhat.com/sgrubb/audit

Mail

sgrubb@redhat.com