

RenaissanceCore IDS

**The Stateful
Network Intrusion Detection System**

RenaissanceCore IDS

Vulnerability exploits are continually becoming more stealthy and effective. The security tools available to analysts for protecting information technology assets must keep up the pace.

RenaissanceCore IDS

Security Tools

- **Information technology security tools are host or network based**
- **Protection/intrusion prevention: Access controls**
 - SELinux, Router ACLs, Firewalls
- **Monitoring: Warn of intrusions, help harden protection**
 - Tripwire, NIDS
- **Scanners: Probe to find vulnerabilities**
 - Coverity, Nessus, Metasploit

RenaissanceCore IDS

Security Tool Issues

- **Host based:** The most effective—until compromised—but are less dynamic than the organization's environment
- **Network protection:** Assume attack points are known in advance
- **Monitoring:** False positives, false negatives
- **Scanners:** Snapshot view of the data center

RenaissanceCore IDS

Security Tool Issues

- **More is better, but information overload is worse**
- **There are no social engineering firewalls**
 - **Never forget that the capabilities of security tools are limited**
- **Security funding is frequently low to non-existent**

RenaissanceCore IDS

Project Philosophy

- **IT environments are increasingly complex and exploits are increasingly sophisticated**
- **Security tools must provide more bang for the buck:**
 - **Perform sophisticated, automated analysis**
 - **Provide information about security environment**
 - **Provide maximum information about intrusion attempts**
 - **Provide tracking capability to help analysts build on experience**

RenaissanceCore IDS

Network Intrusion Detection Systems

The case for NIDS

- **External source of information, less likely to be compromised**
- **Aggregated knowledge of exploits by researchers**
- **Zero day exploit detection**

RenaissanceCore IDS

Network Intrusion Detection Systems

Current NIDS Technology

- **Based on individual packets (minimal reassembly)**
- **Overabundance of false positives**
- **False negatives**
 - **How can you know what you do not know?**
- **Inefficient use of data points**
 - **Correlation of multiple pieces of data is what provides analysts with useful information**

RenaissanceCore IDS

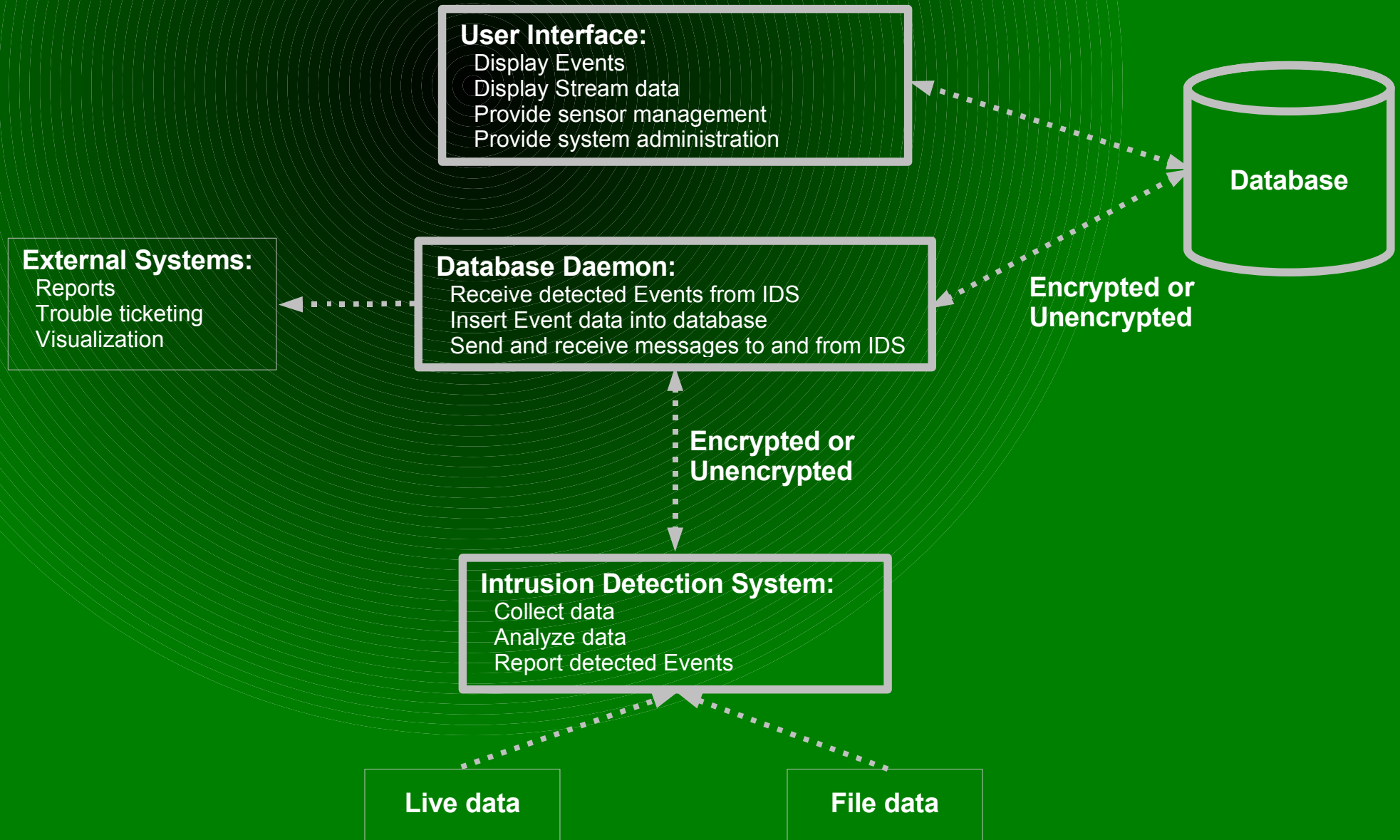
- **RenaissanceCore is Free software: All code is licensed under GPLv2+**
- **The IDS is built on the RenaissanceCore Analysis Engine library**
- **Detected security events are stored in a PostgreSQL database**
- **The User Interface uses the Eclipse Standard Widget Toolkit**

RenaissanceCore IDS

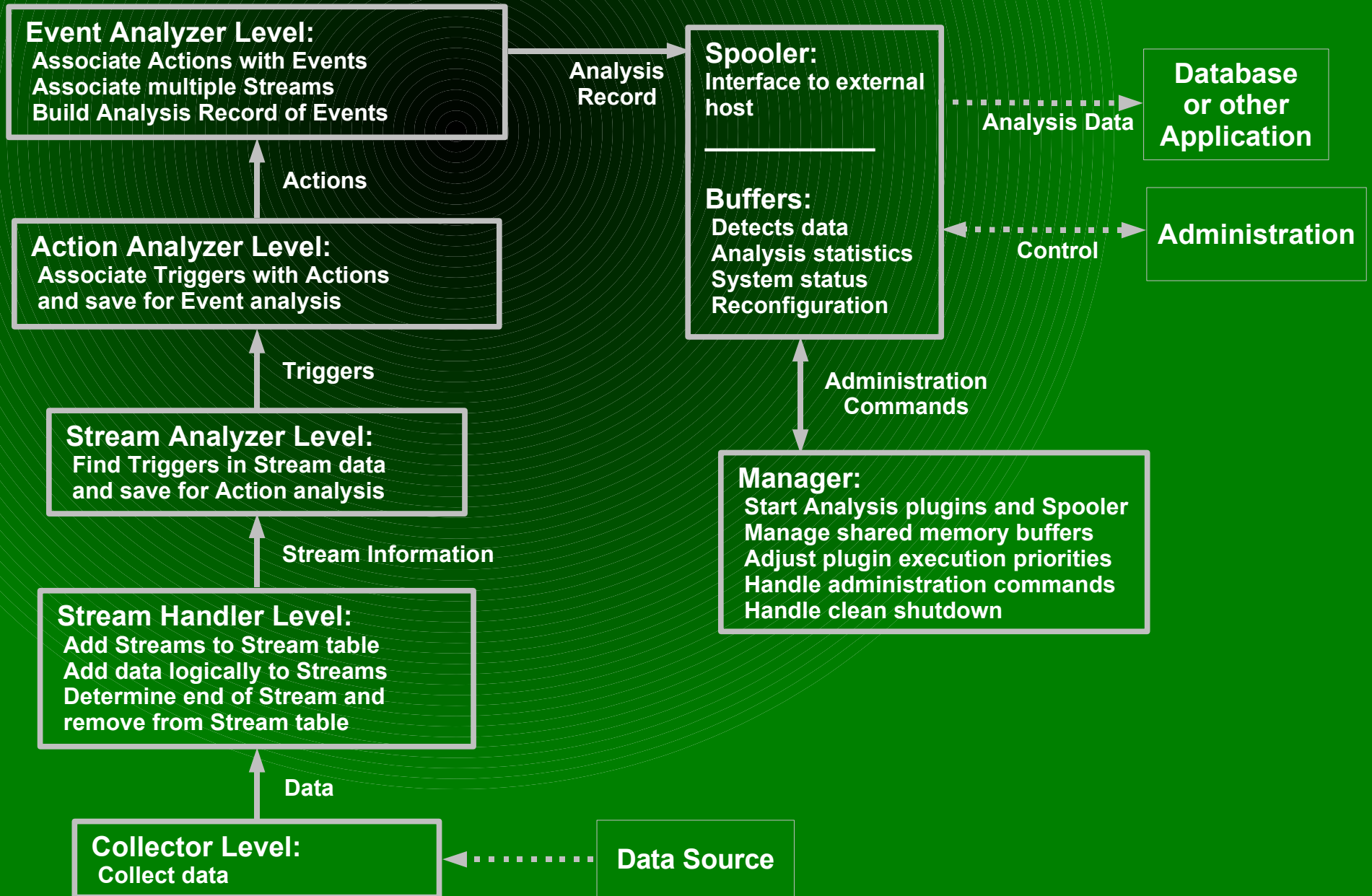
Ritasa IDS Technology

- **Stateful**
 - Maintains information about entire data stream
 - Associates data streams to analyze both halves of TCP session
 - Can associate other data streams, such as FTP control and data
- Significant reduction of false positives
- User interface provides trends tracking
- Definitive evidence of intrusions

RenaissanceCore IDS



RenaissanceCore IDS



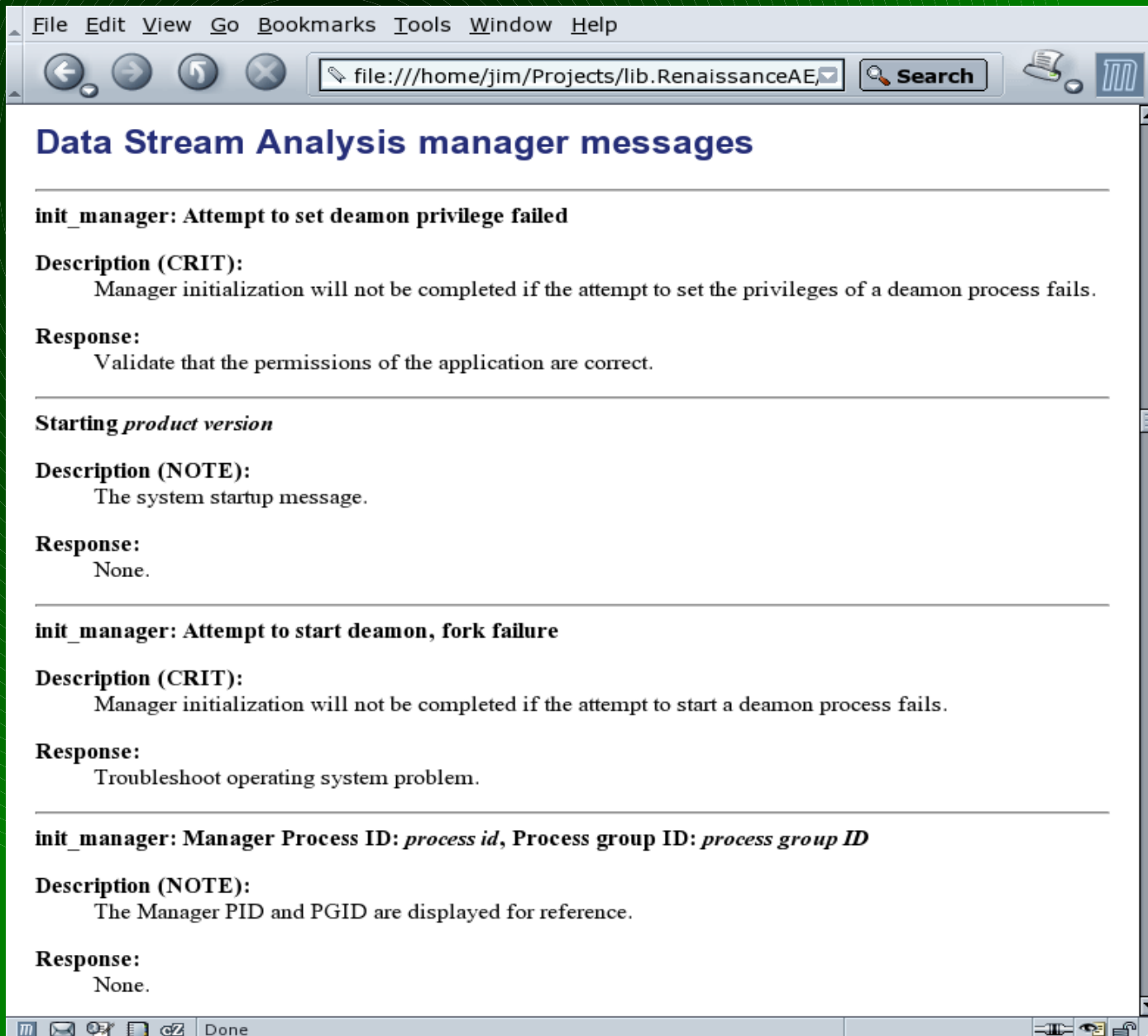
RenaissanceCore IDS

- **The analysis engine static library includes the following features:**
 - **Interprocess communication using shared memory**
 - **XML file handling and macros for simplified parsing**
 - **Networking for encrypted and unencrypted sessions**
 - **Memory management for multiple processes**
 - **Load balancing of multiple processes**
 - **Efficient string matching**

RenaissanceCore IDS

**Messages in the Analysis Engine
and the NIDS are documented
using Doxygen**

RenaissanceCore IDS



The screenshot shows a web browser window with the following content:

File Edit View Go Bookmarks Tools Window Help

file:///home/jim/Projects/lib.RenaissanceAE/ Search

Data Stream Analysis manager messages

init_manager: Attempt to set daemon privilege failed

Description (CRIT):
Manager initialization will not be completed if the attempt to set the privileges of a daemon process fails.

Response:
Validate that the permissions of the application are correct.

Starting *product version*

Description (NOTE):
The system startup message.

Response:
None.

init_manager: Attempt to start daemon, fork failure

Description (CRIT):
Manager initialization will not be completed if the attempt to start a daemon process fails.

Response:
Troubleshoot operating system problem.

init_manager: Manager Process ID: *process id*, Process group ID: *process group ID*

Description (NOTE):
The Manager PID and PGID are displayed for reference.

Response:
None.

Done

RenaissanceCore IDS

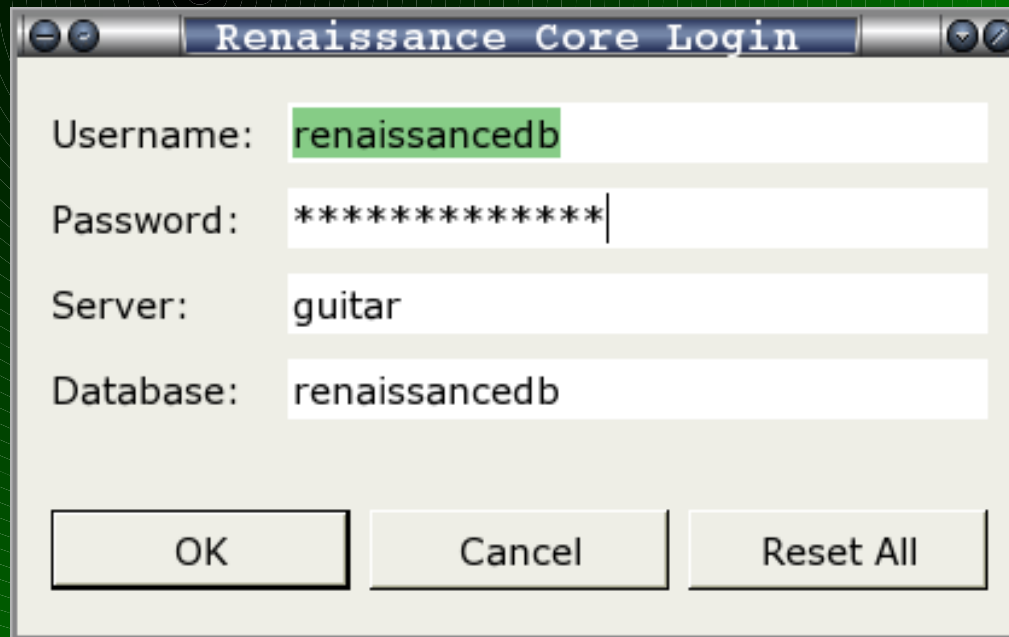
```
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) Starting Renaissance Intrusion Detection System 0.1.0
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) init_manager: Manager Process ID: 30533 Process group ID: 30533
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) interrupts_init: Interrupt initialization complete
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) manager_parser: Parsing manager configuration
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) spool_init: Spooler started (30534, 30533)
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) dispatch_plugin: Child process started: ids_evtu (30535, 30533)
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) Component 'Event Analyzer' initialized
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) dispatch_plugin: Child process started: ids_acta (30536, 30533)
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) Component 'Action Analyzer' initialized
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) dispatch_plugin: Child process started: ids_stra_tcp (30537, 30533)
Feb 18, 2007 21:05:37 Renaissance Analysis Manager (NOTE) dispatch_plugin: Child process started: ids_stra_udp (30538, 30533)
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (NOTE) dispatch_plugin: Child process started: ids_stra_ip4 (30539, 30533)
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (NOTE) dispatch_plugin: Child process started: ids_stra_data (30540, 30533)
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (NOTE) Component 'Stream Analyzer' initialized
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (NOTE) dispatch_plugin: Child process started: ids_strh (30541, 30533)
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (NOTE) Component 'Stream Handler' initialized
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (NOTE) dispatch_plugin: Child process started: ids_coll (30542, 30533)
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (NOTE) Component 'Collector' initialized
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (NOTE) init_manager: Data Stream Analysis initialized
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (NOTE) manager: Initialization complete, starting Data Stream Analysis
Feb 18, 2007 21:05:38 Renaissance Analysis Manager (SPOOL) (NOTE) init_ssl: SSL environment initialized
Feb 18, 2007 21:05:47 Renaissance Analysis Manager (NOTE) manager_shutdown: Stopping Data Stream Analysis
Feb 18, 2007 21:05:59 Renaissance Analysis Manager (SPOOL) (NOTE) spooler_shutdown: Stopping Spooler
```

logs/manager.log lines 1-24/24 (END)

RenaissanceCore IDS

**The Analysis Reports are stored
in the PostgreSQL database and
examined using the User Interface**

RenaissanceCore IDS



A screenshot of a Windows-style dialog box titled "Renaissance Core Login". The dialog box contains four text input fields and three buttons. The "Username" field is highlighted in green and contains the text "renaissancedb". The "Password" field contains ten asterisks "*****" followed by a vertical cursor. The "Server" field contains the text "guitar". The "Database" field contains the text "renaissancedb". At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Reset All".

Renaissance Core Login

Username: renaissancedb

Password: *****|

Server: guitar

Database: renaissancedb

OK Cancel Reset All

RenaissanceCore IDS

**Examine detected security events
displayed in the main analysis window**

RenaissanceCore IDS

The screenshot displays the Renaissance Console - Toolbox interface. The window title is "Renaissance Console - Toolbox". The menu bar includes "File", "Edit", "Admin", and "Rules". The main area is divided into a left sidebar and a main content area. The main content area has tabs for "Analyze", "Summarize", "Report", "Query", and "Probe". The "Analyze" tab is active, showing a list of network events and their associated rules. The events are listed in a table-like format with columns for date, time, protocol, source IP, source port, destination IP, and destination port. The rules are listed below each event, with their names and action weights. The status bar at the bottom indicates "Session streaming completed!".

Date	Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Rule Name	Action Weight
2007-02-09	00:44:26	TCP	192.168.1.5	:49338	192.168.1.10	:41523		
2007-02-09	00:47:33	TCP	192.168.1.5	:49348	192.168.1.10	:21	3Com 3CDaemon FTP Username Remote Overflow	100
2007-02-09	00:47:44	TCP	192.168.1.10	:617	192.168.1.5	:49356	Arkeia Network Backup Client Default Password	100
						Arkeia default login	20	
						Dest 617		
						Arkeia default login		
						Arkeia Network Backup Client Default Password	100	
						Arkeia login success	20	
						Src 617		
						Arkeia login success		
2007-02-09	00:48:28	TCP	192.168.1.5	:49387	192.168.1.10	:10000	VERITAS Backup Exec Remote Agent for Windows CONNECT_CLIENT_AUTH Remote Overf	
2007-02-09	00:48:39	TCP	192.168.1.5	:49396	192.168.1.10	:10000		
2007-02-09	00:48:50	TCP	192.168.1.5	:49405	192.168.1.10	:41523		
2007-02-10	01:38:55	TCP	192.168.1.5	:50342	192.168.1.10	:4105	Computer Associates Message Queuing Buffer Overflow Vulnerability	
						CA CAM log_security Stack Overflow	30	
2007-02-10	07:27:41	TCP	192.168.1.5	:50774	192.168.1.10	:80		
2007-02-11	11:14:31	TCP	192.168.1.10	:20031	192.168.1.5	:51013	BakBone NetVault Remote Heap Overflow Vulnerability	100
2007-02-13	03:03:45	TCP	192.168.1.5	:52434	192.168.1.10	:10616		

Session streaming completed!

RenaissanceCore IDS

The screenshot displays the Renaissance Console - Toolbox interface. The main window shows a list of network incidents with columns for date, time, protocol, source IP, source port, destination IP, and destination port. A context menu is open over one of the incidents, listing options: Playback Session..., Create/View Report..., Order Incidents By..., and Refresh.

Date	Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action Weight
2007-02-09	00:44:26	TCP	192.168.1.5	:49338	192.168.1.10	:41523	
2007-02-09	00:47:33	TCP	192.168.1.5	:49348	192.168.1.10	:21	
3Com 3CDaemon FTP Username Remote Overflow							
2007-02-09	00:47:44	TCP	192.168.1.10	:617	192.168.1.5	:49356	100
Client Default Password							
Trigger Weight: 20							
Arkeia Network Backup Client Default Password							
Action Weight: 100							
Arkeia login success							
Trigger Weight: 20							
Src 617							
Arkeia login success							
2007-02-09	00:48:28	TCP	192.168.1.5	:49387	192.168.1.10	:10000	
VERITAS Backup Exec Remote Agent for Windows CONNECT_CLIENT_AUTH Remote Overf							
2007-02-09	00:48:39	TCP	192.168.1.5	:49396	192.168.1.10	:10000	
2007-02-09	00:48:50	TCP	192.168.1.5	:49405	192.168.1.10	:41523	
2007-02-10	01:38:55	TCP	192.168.1.5	:50342	192.168.1.10	:4105	
Computer Associates Message Queuing Buffer Overflow Vulnerability							
Action							
CA CAM log_security Stack Overflow							
Trigger Weight: 30							
2007-02-10	07:27:41	TCP	192.168.1.5	:50774	192.168.1.10	:80	
2007-02-11	11:14:31	TCP	192.168.1.10	:20031	192.168.1.5	:51013	
BakBone NetVault Remote Heap Overflow Vulnerability							
Action Weight: 100							
2007-02-13	03:03:45	TCP	192.168.1.5	:52434	192.168.1.10	:10616	

Session streaming completed!

RenaissanceCore IDS

Session Playback: 192.168.1.10:617 -> 192.168.1.5:40205

Bytes Transferred	Packets Transferred
35	10

```
[0x00]'[0x00][0x04][0x00]`  
[0x00][0x04][0x00]C[0x00]  
[0x00][0x00]C[0x00][0x00]  
[0x00]C[0x00][0x00][0x00]t  
[0x00][0x04][0x00]t[0x00]  
[0x04][0x00]t[0x00][0x04]ABC
```

```
[0x00]A[0x00][0x00][0x00][0x00][0x00]p[0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x7F][0x00][0x00]  
[0x01][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x01][0x00][0x00][0x7F]ARKFS[0x00]root[0x00]root[0x00]  
[0x00][0x00]4.3.0-1[0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00][0x00]s[0x00][0x00][0x00][0x00][0x00][0x0C]2  
[0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00]a[0x00][0x04][0x00][0x01][0x00][0x1A][0x00][0x00]1106659543  
[0x00]EN[0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00]b[0x00][0x01][0x00][0x02][0x00][0x1D]  
ARKFS_BACKUP_ALL[0x00]1[0x00][0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00][0x00][0x00][0x00]c[0x00][0x04][0x00][0x03][0x00]  
[0x15]1[0x00]1[0x00]1[0x00]0:3,[0x00][0x00][0x00][0x00][0x00]  
[0x00][0x00][0x00][0x00][0x00][0x00][0x00]f[0x00][0x04][0x00][0x04]  
[0x00][0xC0]TPs_allowedfs[0x00]NORMAL_FS[0x00]Ps_crypt[0x00]  
NO_CRYPT[0x00]Ps_cpres[0x00]NO_COMPRESS[0x00]Ps_filoc[0x00]/tmp/  
xyz[0x00]Ps_locat[0x00]/[0x00]Ps_cmpnt[0x00]/tmp/xyz[0x00]Ps_host  
[0x00]piano[0x00]Pn_bkpsid[0x00]1172260701[0x00]Ps_volum[0x00]/  
[0x00]Pn_det[0x00]3[0x00]Ps_pluga[0x00]file[0x00]PRECOVERY[0x00]0  
[0x00]E
```

Hide Hex

RenaissanceCore IDS

Define rules to detect exploits

RenaissanceCore IDS

Rules: Events

Target type: MSAPP
Attack type: THEFT
Severity: HIGH

Event Name: Arkeia Network Backup Client Default Passw
Threshold: 100
Threshold 2: 0
Threshold 3: 0
Threshold 4: 0
Sensor group: ALL
Vulnerability Links: http://osvdb.org/displayvuln.php?osvdb_id=
Information Links:
Active: True

Save Add Cancel Delete New

Target: MSAPP
Attack: THEFT
Action name: Arkeia default login
Weight: 50
Sequence: 0
Request: True
Reply: False
Support Action: False
NOT Action: False
XOR Action: False

Save Add Cancel Delete New

ACTION: Arkeia default login
Target:MSAPP Attack:THEFT ASSOCIATION
Wt:50 Seq:0 Req:T Rply:F N

ACTION: Arkeia login success
Target:MSAPP Attack:THEFT ASSOCIATION
Wt:50 Seq:0 Req:F Rply:T N

RenaissanceCore IDS

Rules: Actions

Target type: MSAPP

Attack type: THEFT

Action name: Arkeia default login

Action threshold: 20

Start of line:

End of line:

Save Add Cancel Delete New

Plugin name: data

Function: CMD

Trigger name: Arkeia default login

Weight: 10

Sequence: 0

Distance triggers: 0

Distance: 0

Distance type: False

Support Trigger: False

Same line: False

NOT Trigger: False

XOR Trigger: False

Save Add Cancel Delete New

TRIGGER: Arkeia default login
Plugin:data Function:CMD T
Loc:0 Len:0 Mix:F Glb:F Msk
ASSOCIATION
Wt:10 Sup:F Seq:0 EOL:F N
Dist:0 DisTp:F EOL:F Num:0
VALUE: ARKFS\x00root\x00ro

TRIGGER: Dest 617
Plugin:tcp Function:PORT Ty
Loc:2 Len:2 Mix:F Glb:T Msk
ASSOCIATION
Wt:10 Sup:T Seq:0 EOL:F N
Dist:0 DisTp:F EOL:F Num:0
VALUE: 617

RenaissanceCore IDS

Rules: Triggers

tcp

- FLNAME
- SIG
- URL
- CODE
- ESCODE
- CMD
- VALUE
- PROT

PORT

- Dest 10000
- Dest 10616
- Dest 135
- Dest 1364
- Dest 143
- Dest 20000
- Dest 20031
- Dest 21
- Dest 21700
- Dest 2221
- Dest 25
- Dest 3339

Plugin name: tcp

Function: PORT

Trigger Name: Dest 617

Trigger Type: Location

Value: 617

Location: 2

Length: 2

Mixed case: False

Regular expression: False

Global: True

Mask: False

Number comparison: False

Backspace: False

Backspace List:

Save Add Cancel Delete New

RenaissanceCore IDS

Rules: Triggers

▼ data

- FLNAME
- SIG
- ▶ URL
- ▶ CODE
- ESCODE
- ▼ CMD
- Arkeia default login**
- Arkeia login success
- Brightstor request
- EiQ License Add
- FTP login

VALUE

PROT

PORT

ADDR

FLAG

▼ tcp

- FLNAME
- SIG
- URL
- CODE

Plugin name: data

Function: CMD

Trigger Name: Arkeia default login

Trigger Type: String

Value: ARKFS\x00root\x00root\x00

Location: 0

Length: 0

Mixed case: False

Regular expression: False

Global: False

Mask: False

Number comparison: False

Backspace: False

Backspace List:

Save Add Cancel Delete New

RenaissanceCore IDS

Rules: Triggers

▼ data

- FLNAME
- SIG
- ▶ URL
- ▶ CODE
- ESCODE
- ▼ CMD
 - Arkeia default login
 - Arkeia login success**
 - Brightstor request
 - EiQ License Add
 - FTP login
- VALUE
- PROT
- PORT
- ADDR
- FLAG

▼ tcp

- FLNAME
- SIG
- URL
- CODE

Plugin name: data

Function: CMD

Trigger Name: Arkeia login success

Trigger Type: String

Value: \x00\x60\x00\x04

Location: 0

Length: 0

Mixed case: False

Regular expression: False

Global: False

Mask: False

Number comparison: False

Backspace: False

Backspace List:

Save Add Cancel Delete New

RenaissanceCore IDS

Define analysis statistics to be collected.

RenaissanceCore IDS

The screenshot displays the 'Statistics' window of the RenaissanceCore IDS, which is divided into four main sections for configuration and data viewing.

Top-Left Configuration Panel:

- Host: guitar
- Network Address: 192.168.1.0
- Protocol: IPV4
- Subnet mask: 24
- Buttons: Save, Cancel, Delete, New

Bottom-Left Data List:

- 192.168.1.0 IPV4 24

Top-Middle Configuration Panel:

- Host: guitar
- Statistics Active: True
- Minimum data: 16384
- Hour 1: 7
- Minute 1: 0
- Hour 2: 15
- Minute 2: 0
- Hour 3: 23
- Minute 3: 0
- Buttons: Save, Cancel

Top-Right Configuration Panel:

- Host: guitar
- Protocol: IPV4
- Host address: 192.168.1.5
- Expire after: 2007-02-25
- Buttons: Save, Cancel

Bottom-Right Data List:

- 192.168.1.5 IPV4 2007-02-25
- 192.168.1.10 IPV4 2007-02-28
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV4 2007-02-23
- 0.0.0.0 IPV6 2007-02-23

Far-Right Configuration Panel:

- Host: guitar
- Protocol: TCP
- Port: 22
- Expire after: 2007-02-28
- Buttons: Save, Cancel

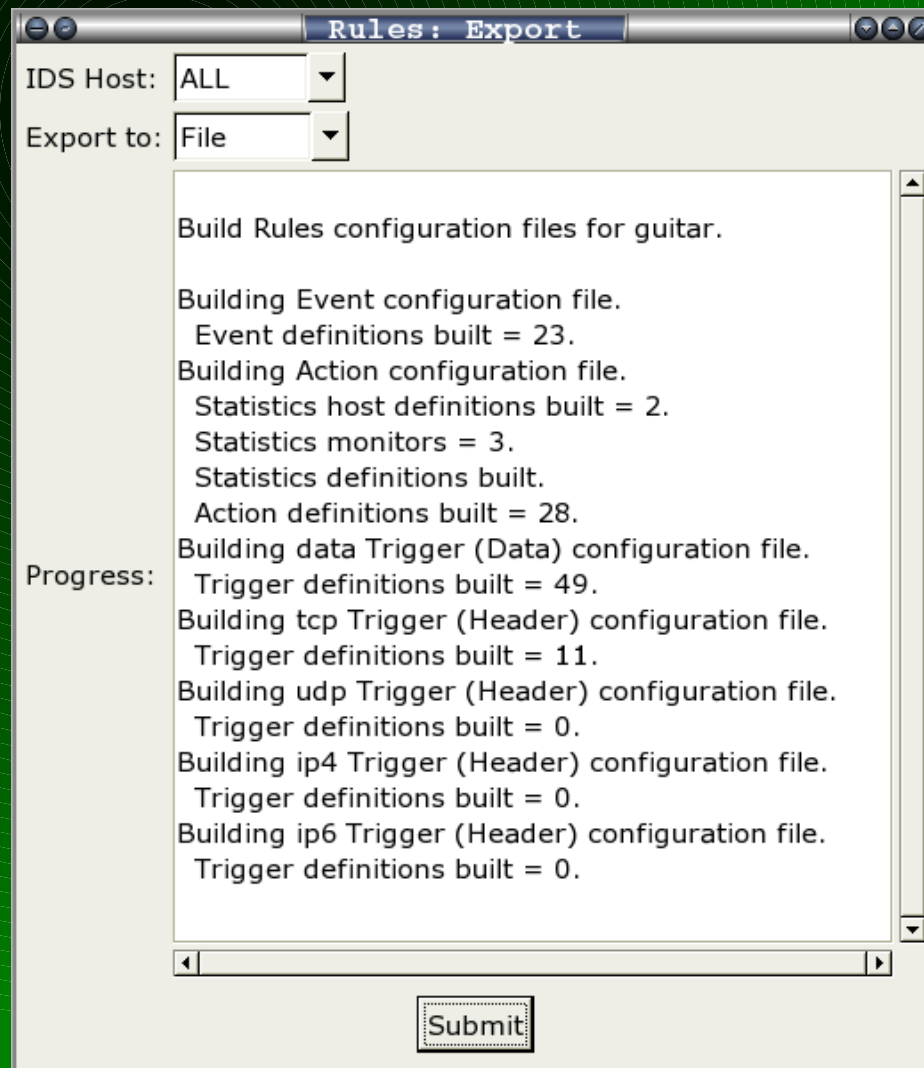
Bottom-Far-Right Data List:

- 22 tuCP 2007-02-28
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuCP 2007-02-23
- 0 tuDP 2007-02-23
- 0 tuDP 2007-02-23

RenaissanceCore IDS

Export analysis configuration files.

RenaissanceCore IDS



RenaissanceCore IDS

```
-rw-r--r-- 1 jim sansing 22677 Feb 18 15:01 rae_net_action_analyzer.xml
-rw-r--r-- 1 jim sansing 9608 Feb 18 15:01 rae_net_event_analyzer.xml
-rw-r--r-- 1 jim sansing 6497 Feb 18 15:01 rae_net_stream_analyzer_data.xml
-rw-r--r-- 1 jim sansing 282 Feb 18 15:01 rae_net_stream_analyzer_ip4.xml
-rw-r--r-- 1 jim sansing 282 Feb 18 15:01 rae_net_stream_analyzer_ip6.xml
-rw-r--r-- 1 jim sansing 2801 Feb 18 15:01 rae_net_stream_analyzer_tcp.xml
-rw-r--r-- 1 jim sansing 282 Feb 18 15:01 rae_net_stream_analyzer_udp.xml
jim)~/workspace/RenaissanceCore_Gui/guitar: █
```

RenaissanceCore IDS

```
<?xml version="1.0"?>
<!DOCTYPE raen_acta:ActionAnalyzer PUBLIC "-//ritasa.com//DTD RenaissanceCore v1.00.00 Ac
tionAnalyzer//EN" "rids_action_analyzer.dtd">
<raen_acta:ActionAnalyzer xmlns:raen_acta="rids_action_analyzer.dtd" DTDversion="1.0.0">

<raen_acta:ActionGroup>

<raen_acta:Action ID="1" Total="6" Threshold="30">
  <raen_acta:TriggerDef Support="YES">
    <raen_acta:ActTrigger Weight="10">500006</raen_acta:ActTrigger>
  </raen_acta:TriggerDef>
  <raen_acta:TriggerDef Support="YES">
    <raen_acta:TriggerCond>EDIST=229</raen_acta:TriggerCond>
    <raen_acta:TriggerCond>NDST=2</raen_acta:TriggerCond>
    <raen_acta:TriggerCond>SEQ</raen_acta:TriggerCond>
    <raen_acta:ActTrigger Weight="10">500001</raen_acta:ActTrigger>
  </raen_acta:TriggerDef>
  <raen_acta:TriggerDef>
    <raen_acta:TriggerCond>SEQ</raen_acta:TriggerCond>
    <raen_acta:ActTrigger Weight="10">500002</raen_acta:ActTrigger>
  </raen_acta:TriggerDef>
  <raen_acta:TriggerDef>
    <raen_acta:TriggerCond>SEQ</raen_acta:TriggerCond>
    <raen_acta:TriggerCond>XOR</raen_acta:TriggerCond>
    <raen_acta:ActTrigger Weight="5">500003</raen_acta:ActTrigger>
  </raen_acta:TriggerDef>
  <raen_acta:TriggerDef>
    <raen_acta:TriggerCond>SEQ</raen_acta:TriggerCond>
    <raen_acta:TriggerCond>XOR</raen_acta:TriggerCond>
    <raen_acta:ActTrigger Weight="5">500005</raen_acta:ActTrigger>
  </raen_acta:TriggerDef>
  <raen_acta:TriggerDef>
    <raen_acta:TriggerCond>SEQ</raen_acta:TriggerCond>
    <raen_acta:TriggerCond>XOR</raen_acta:TriggerCond>
    <raen_acta:ActTrigger Weight="5">500004</raen_acta:ActTrigger>
  </raen_acta:TriggerDef>
</raen_acta:Action>

<raen_acta:Action ID="2" Total="3" Threshold="30">
  <raen_acta:TriggerDef Support="YES">
    <raen_acta:ActTrigger Weight="10">500010</raen_acta:ActTrigger>
  </raen_acta:TriggerDef>
```

RenaissanceCore IDS

```
<raen_acta:TriggerCond>SEQ</raen_acta:TriggerCond>
<raen_acta:ActTrigger Weight="10">500038</raen_acta:ActTrigger>
</raen_acta:TriggerDef>
<raen_acta:TriggerDef>
  <raen_acta:TriggerCond>SEQ</raen_acta:TriggerCond>
  <raen_acta:ActTrigger Weight="10">500060</raen_acta:ActTrigger>
</raen_acta:TriggerDef>
<raen_acta:TriggerDef>
  <raen_acta:TriggerCond>SEQ</raen_acta:TriggerCond>
  <raen_acta:ActTrigger Weight="10">500061</raen_acta:ActTrigger>
</raen_acta:TriggerDef>
</raen_acta:Action>

<raen_acta:Action ID="10000076" Total="2" Threshold="20">
  <raen_acta:TriggerDef Support="YES">
    <raen_acta:ActTrigger Weight="10">100080</raen_acta:ActTrigger>
  </raen_acta:TriggerDef>
  <raen_acta:TriggerDef>
    <raen_acta:ActTrigger Weight="10">1000512</raen_acta:ActTrigger>
  </raen_acta:TriggerDef>
</raen_acta:Action>

</raen_acta:ActionGroup>

<raen_acta:Network Mask="24" Proto="IPV4">192.168.1.0</raen_acta:Network>
<raen_acta:Statistics State="ON">
  <raen_acta:Interval>
    <raen_acta:IntervalHr1>7</raen_acta:IntervalHr1>
    <raen_acta:IntervalMin1>0</raen_acta:IntervalMin1>
    <raen_acta:IntervalHr2>15</raen_acta:IntervalHr2>
    <raen_acta:IntervalMin2>0</raen_acta:IntervalMin2>
    <raen_acta:IntervalHr3>23</raen_acta:IntervalHr3>
    <raen_acta:IntervalMin3>0</raen_acta:IntervalMin3>
  </raen_acta:Interval>
  <raen_acta:MinData>16384</raen_acta:MinData>
  <raen_acta:MonHost Proto="IPV4" Expire="2007-02-25">192.168.1.5</raen_acta:MonHost>
  <raen_acta:MonHost Proto="IPV4" Expire="2007-02-28">192.168.1.10</raen_acta:MonHost>
  <raen_acta:MonPort Proto="TCP" Expire="2007-02-28">22</raen_acta:MonPort>
</raen_acta:Statistics>

</raen_acta:ActionAnalyzer>
```

RenaissanceCore IDS

**Analysis statistics are formatted
in simple table displays.**

RenaissanceCore IDS

RenaissanceCore IDS Statistics Record

Start time: Fri Aug 11 16:00:00 2006
End time: Sat Aug 12 00:00:00 2006

Number of TCP ports: 5

Port	Bytes In	Bytes Out
80	612950709	16722805
22	10094	493904
443	33464	143662
110	51153	1772
15973	4664	13912

Number of TCP ports monitoring hosts: 1

Monitored port: 22

Number of TCP IPv4 port hosts: 2

Address	Bytes In	Bytes Out
66.35.250.89	0	493904
192.168.1.5	10094	0

Number of TCP IPv6 port hosts: 0

Number of UDP ports: 0

Number of UDP ports monitoring hosts: 0

Number of monitored IPv4 hosts: 3

Monitored host: 192.168.1.5

Number of connecting hosts: 77

Address	Port	Bytes In	Bytes Out
12.77.38.138	15973	4664	13912
12.130.60.2	80	41809	10216
12.152.67.4	80	83237	7505
12.152.67.28	80	266	326
63.146.109.204	80	17159	12522
63.236.73.20	80	4102827	375072
63.236.73.123	80	153921	7385
63.236.73.147	80	830	2665
64.28.75.210	80	434	644
64.28.75.214	80	42746	1726
64.62.161.195	80	18823639	62847

RenaissanceCore IDS

Create an incident report

RenaissanceCore IDS

Report Number <input type="text"/>	Events Whois Notes
Date/Time (GMT) 2007-02-09 00:47:44	Arkeia Network Backup Client Default Password Action Weight: 100 Arkeia default login Trigger Weight: 20 Dest 617 Arkeia default login
Site Test Site 1	Arkeia Network Backup Client Default Password Action Weight: 100 Arkeia login success Trigger Weight: 20 Src 617 Arkeia login success
Category <input type="text"/>	
Protocol TCP *AP*S*	
Source IP: 192.168.1.10 Hostname: piano.sansing.net Port: 617	
Destination IP: 192.168.1.5 Hostname: guitar.sansing.net Port: 49356	
Transferred Bytes: 35 Packets: 10	
<input type="button" value="Save Report"/> <input type="button" value="Cancel Report"/>	

RenaissanceCore IDS

Report Number	Events	Whois	Notes
<input type="text"/>	Source		
Date/Time (GMT)	OrgName: Internet Assigned Numbers Authority		
2007-02-09 00:47:44	OrgID: IANA		
Site	Address: 4676 Admiralty Way, Suite 330		
Test Site 1	City: Marina del Rey		
Category	StateProv: CA		
<input type="text"/>	PostalCode: 90292-6695		
Protocol	Country: US		
TCP	NetRange: 192.168.0.0 - 192.168.255.255		
*AP*S*	CIDR: 192.168.0.0/16		
Source	NetName: IANA-CBLK1		
IP: 192.168.1.10	NetHandle: NET-192-168-0-0-1		
Hostname: piano.sansing.net	Parent: NET-192-0-0-0		
Port: 617	<input type="text"/>		
Destination	Destination		
IP: 192.168.1.5	OrgName: Internet Assigned Numbers Authority		
Hostname: guitar.sansing.net	OrgID: IANA		
Port: 49356	Address: 4676 Admiralty Way, Suite 330		
Transferred	City: Marina del Rey		
Bytes: 35	StateProv: CA		
Packets: 10	PostalCode: 90292-6695		
Save Report	Country: US		
Cancel Report	NetRange: 192.168.0.0 - 192.168.255.255		
	CIDR: 192.168.0.0/16		
	NetName: IANA-CBLK1		
	NetHandle: NET-192-168-0-0-1		
	Parent: NET-192-0-0-0		
	<input type="text"/>		

RenaissanceCore IDS

Perform administrative tasks

RenaissanceCore IDS

The screenshot shows the Renaissance Console - Toolbox interface. The main window displays a list of detected events with columns for date, time, protocol, source IP, source port, destination IP, and destination port. A tree view on the left shows the details of the selected event, including the rule name and its trigger weight.

Menu: File Edit Admin Rules

Sub-menu: Users... Tables

Buttons: Analyze Summarize Report Query Probe

Date	Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action Weight
2007-02-09	00:44:26	TCP	192.168.1.5	:49338	192.168.1.10	:41523	
2007-02-09	00:47:33	TCP	192.168.1.5	:49348	192.168.1.10	:21	
3Com 3CDaemon FTP Username Remote Overflow Action Weight: 100							
2007-02-09	00:47:44	TCP	192.168.1.10	:617	192.168.1.5	:49356	
Arkeia Network Backup Client Default Password Action Weight: 100							
Arkeia default login Trigger Weight: 20							
Dest 617							
Arkeia default login							
Arkeia Network Backup Client Default Password Action Weight: 100							
Arkeia login success Trigger Weight: 20							
Src 617							
Arkeia login success							
2007-02-09	00:48:28	TCP	192.168.1.5	:49387	192.168.1.10	:10000	
VERITAS Backup Exec Remote Agent for Windows CONNECT_CLIENT_AUTH Remote Overf							
2007-02-09	00:48:39	TCP	192.168.1.5	:49396	192.168.1.10	:10000	
2007-02-09	00:48:50	TCP	192.168.1.5	:49405	192.168.1.10	:41523	
2007-02-10	01:38:55	TCP	192.168.1.5	:50342	192.168.1.10	:4105	
Computer Associates Message Queuing Buffer Overflow Vulnerability Action							
CA CAM log_security Stack Overflow Trigger Weight: 30							
2007-02-10	07:27:41	TCP	192.168.1.5	:50774	192.168.1.10	:80	
2007-02-11	11:14:31	TCP	192.168.1.10	:20031	192.168.1.5	:51013	
BakBone NetVault Remote Heap Overflow Vulnerability Action Weight: 100							
2007-02-13	03:03:45	TCP	192.168.1.5	:52434	192.168.1.10	:10616	

Session streaming completed!

RenaissanceCore IDS

Administration: Users

Sansing, James J (jjsansing)

First Name:	Dick
Middle Initial:	E
Last Name:	Richards
Database Username:	derichards
Email Address:	der@rencore.net
Role:	Analyst (analyst) ▼
Password:	
Password Again:	

RenaissanceCore IDS

Administration: Hosts

guitar.sansing.net (guitar)

Host Type:	Sensor (snsr) ▼
Host Enabled:	Yes ▼
Host Name:	guitar.sansing.net
Host Name Abbreviation:	guitar
IP Address:	192.168.1.5
OS:	Linux
OS Version Number:	2.6.5-7.257
Location:	home
Room:	na
Building:	na
Site:	Test Site 1 - Test1 ▼
Point of Contact:	Richards, Dick E (123-555-1234) ▼

Save Cancel Delete New

RenaissanceCore IDS

Administration: Sites

Test Site 1 (Test1)

Site Name: Test Site 1

Site Name Abbreviation: Test1

Site is Active: Yes

Site POC: Richards, Dick E. (123-555-1234)

Save Cancel Delete New

The image shows a screenshot of a web-based administration interface for RenaissanceCore IDS. The window title is "Administration: Sites". On the left, there is a list of sites, with "Test Site 1 (Test1)" selected and highlighted in green. The main area of the window displays the configuration details for this selected site. The fields are: "Site Name" with the value "Test Site 1", "Site Name Abbreviation" with the value "Test1", "Site is Active" with a dropdown menu set to "Yes", and "Site POC" with a dropdown menu set to "Richards, Dick E. (123-555-1234)". At the bottom of the configuration area, there are four buttons: "Save", "Cancel", "Delete", and "New".

RenaissanceCore IDS

Administration: Points of Contact

Richards, Dick E (123-555-1234)

First Name:	Dick
Middle Initial:	E
Last Name:	Richards
Phone Number:	123-555-1234
Pager Number:	
Cell Number:	
Email Address:	
Address:	na
POC Type:	IDS Admin (IAdm) ▼

Save Cancel Delete New

RenaissanceCore IDS

The image shows a 'Preferences' dialog box for RenaissanceCore IDS. The 'Login' tab is selected in the left sidebar. The main area contains three text input fields: 'Username' with the value 'renaissancedb', 'Server' with the value 'guitar', and 'Database' with the value 'renaissancedb'. At the bottom, there are four buttons: 'Restore Defaults', 'Apply', 'OK', and 'Cancel'.

Field	Value
Username:	renaissancedb
Server:	guitar
Database:	renaissancedb

RenaissanceCore IDS

System Requirements

- **Sensors:**
 - CPU and memory intensive
 - Disk size depends on network reliability
- **Server:**
 - CPU and IO intensive
 - Disk size depends on number of sensors

RenaissanceCore IDS

Future Directions

- **Protocol and application anomaly detection:** Based on expected request/reply interaction
- **Encrypted session detects:** Every session type has a unique pattern (interactive sessions have short requests followed by longer replies)
- **Server profiles and internal threats:** Statistics for specific servers allow unusual activity to be detected (high database activity outside normal working hours)

RenaissanceCore IDS

Future Directions

- **Reports: Charts and visualization software**
- **Export to other applications: Trouble ticketing systems, Wireshark (formerly Ethereal)**
- **Interface with network management systems: Nagios**
- **Use alternate database backends: Oracle, MySQL**

RenaissanceCore IDS

**The Stateful
Network Intrusion Detection System**