Monitoring Network Traffic From Intrusion Detection Systems

Supported by NSF LUCID: A Spectator Targeted Visualization System to Broaden Participation at Cyber Defense Competitions (Grant ID: NSF-DUE 1303424)

Mahfoudh M. Batarfi, Department of Computer Science, Bowie State University
Dr. Jie Yan, Department of Computer Science, Bowie State University

INTRODUCTION

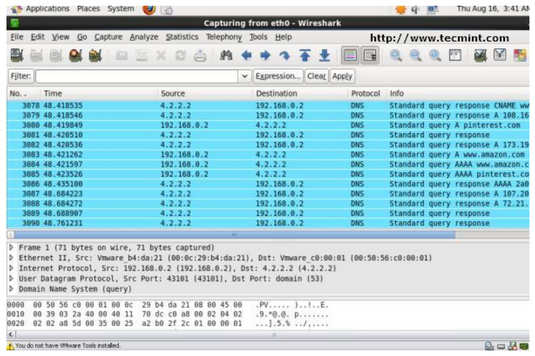
Network traffic is an important component of the information needed to investigate and troubleshoot a network when an intrusion event occurs. Since analyzing intrusion detection events are such an important aspect of network security, it is important to understand the Monitoring tools used to view, monitor and analyze data from network traffic that is generated by intrusion detection systems. We compare seven, open source network monitoring tools used to analyze network traffic in the event of an intrusion. The tools include **Wireshark**, **Cacti**, **Linux Dash** , **Observium, Icinga, Sysstat** and **Sarg**. There are many more tools developed to analyze network traffic. However, the tools we chose are a starting point for the discussion of monitoring tools designed for network traffic analysis.

Wireshark – Network Protocol Analyzer

Wireshark is an analyzer desktop program which is used to analyze network packets and to monitor network connections. It's written in C with the GTK+ library and released under the GPL license.

Features of Wireshark:

- Cross-platform: it works on Linux, BSD , Mac OS X and Windows.
- Command line support: there's a command line based version from Wireshark to analyze data.
- Ability to capture VoIP calls, USB traffic, network data easily to analyze it.
- Available in most Linux distributions repositories.



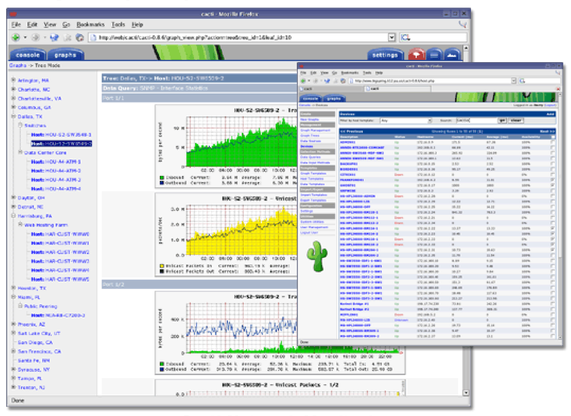
Monitor Local Network Traffic

Cacti – Network and System Monitoring

Cacti is nothing more than a free & open-source web interface for RRDtool, it is used often to monitor the bandwidth using SNMP (Simple Network Management Protocol), it can be used also to monitor CPU usage.

Features of Cacti:

- Free & open-source, released under GPL license.
- Written in PHP with PL/SQL.
- A cross-platform tool, it works on Windows and Linux.
- User management; you may create different users accounts for Cacti.

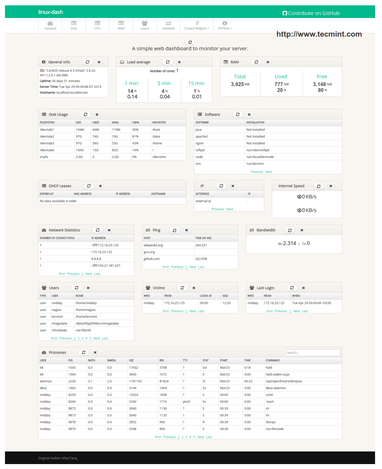


Cacti Network Monitoring

MONITORING TOOLS

Linux Dash – Linux Server Performance Monitoring

From its name, "**Linux Dash**" is a web dashboard that shows you the most important information about your Linux systems such as RAM, CPU, file-system, running processes, users, bandwidth usage in real time, it has a nice GUI and it's free & open-source.



linux-dash: Server Monitoring Tool

Observium – Network Management and Monitoring

Observium is also a network monitoring tool, it was designed to help you manage your network of servers easily, there are 2 versions from it; Community Edition which is free & open-source and Commercial version which costs £150/year.

Features of Observium :

Written in PHP with MySQL database support.
Has a nice web interface to output information and data.
Ability to manage and monitor hundreds of hosts worldwide.
The community version from it is licensed under QPL license.
Works on Windows, Linux, FreeBSD and more.

Observium: Linux Network Monitoring

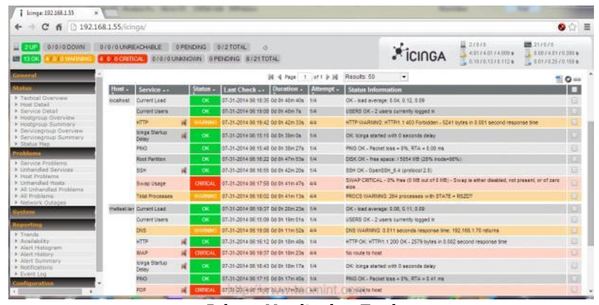
Icinga – Next Generation Server Monitoring

Unlike the other tools, **Icinga** is a network monitoring program, it shows you many options and information about your network connections, devices and processes, it's a very good choice for those who are looking for a good tool to monitor their networking stuffs.

Features of Icinga

- Icinga is also free and open-source.
- Very functional in monitoring everything you may have in networking.
- Support for MySQL and PostgreSQL is included.
- Real-time monitoring with A nice web interface.
- Very expendable with modules and extensions.
- Icinga supports applying services and actions to hosts.
- A lot more to discover..

MONITORING TOOLS



Icinga Monitoring Tool

Sysstat – All-in-One System Performance Monitoring

Another monitoring tool for your Linux system. **Sysstat** is not a real command in fact, it's just the name of the project, Sysstat in fact is a package that includes many performance monitoring tools like iostat, sadf, pidstat beside many other tools which shows you many statistics about your Linux OS.

Features of Sysstat

- Available in many Linux distributions repositories by default.
- Ability to create statistics about RAM, CPU, SWAP usage. Beside the ability to monitor Linux kernel activity, NFS server, Sockets, TTY and filesystems.
- Ability to monitor input & output statistics for devices, tasks.. etc.
- Ability to output reports about network interfaces and devices, with support for IPv6.
- Sysstat can show you the power statistics (usage, devices, the fans speed.. etc) as well.
- Many other features..

```
tecmint@tecmint ~ $ pidstat -p ALL

Linux 3.11.0-23-generic (tecmint.com)   Thursday 04 September 2014      _i686_

12:51:55  IST   UID       PID    %usr %system  %guest    %CPU   CPU  Command
12:51:55  IST     0         1    0.01    0.11    0.00    0.12     1  init
12:51:55  IST     0         2    0.00    0.00    0.00    0.00     0  kthreadd
12:51:55  IST     0         3    0.00    0.01    0.00    0.01     0  ksoftirqd
12:51:55  IST     0         5    0.00    0.00    0.00    0.00     0  kworker/0
12:51:55  IST     0         7    0.00    0.00    0.00    0.00     0  migration
12:51:55  IST     0         8    0.00    0.00    0.00    0.00     0  rcu_bh
12:51:55  IST     0         9    0.00    0.04    0.00    0.04     1  rcu_sched
12:51:55  IST     0        10    0.00    0.00    0.00    0.00     0  watchdog/
12:51:55  IST     0        11    0.00    0.00    0.00    0.00     1  watchdog/
12:51:55  IST     0        12    0.00    0.00    0.00    0.00     1  migration
12:51:55  IST     0        13    0.00    0.01    0.00    0.01     1  ksoftirqd
12:51:55  IST     0        15    0.00    0.00    0.00    0.00     1  kworker/1
12:51:55  IST     0        16    0.00    0.00    0.00    0.00     1  khelper
12:51:55  IST     0        17    0.00    0.00    0.00    0.00     0  kdevtmpfs
12:51:55  IST     0        18    0.00    0.00    0.00    0.00     0  netns
12:51:55  IST     0        19    0.00    0.00    0.00    0.00     0  writeback
12:51:55  IST     0        20    0.00    0.00    0.00    0.00     1  kintegrit
```

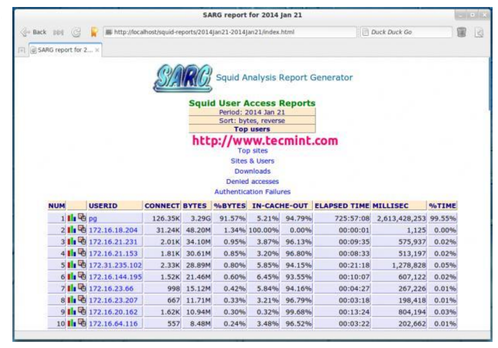
Sysstat: Linux Statistics Monitoring

Sarg – Squid Bandwidth Monitoring

Sarg (Squid Analysis Report Generator) is a free & open-source tool which act as a monitoring tool for your Squid proxy server, it creates reports about your Squid proxy server users, IP addresses, the sites they visit beside some other information.

Features of Sarg

Licensed under GPL 2 and available in many languages.
Works under Linux & FreeBSD.
Generates report in HTML format.
Very easy to install & use.



Sarg Monitors Squid Logs