



Monitoring Anything and Everything with Nagios

Chris Burgess

chris@chrisburgess.com.au

<http://www.chrisburgess.com.au>

What We Will Cover



- What is Nagios?
- The variety of “things” Nagios can monitor
- Why monitoring is important for security
- Nagios as a security tool?
- How Nagios works
- Types of checks
- Live demonstration
- Extending Nagios with security tools
- Where to find more information



Bah, Nagios Shmagios!

Well, you might be interested, even if:

- you use another monitoring product
- you are working outside a security focus

What is Nagios?



- Nagios is an Open Source monitoring application written by **Ethan Galstad**
- Nagios is easily obtained using your OS' package system (apt-get, rpm, Ports etc.) or source
- Nagios is easily extensible
- Nagios is incredibly useful as source of system documentation
- There are several popular monitoring applications. In my travels, Nagios is the most commonly used.
- Nagios has a healthy community following
- There are dozens of third party apps that leverage off of Nagios (hint: search SourceForge)

The Variety of “things” Nagios can Monitor

- Hosts
- Services
- Interactions
- Logs
- Connectivity
- Environment (HVAC)
- We can monitor anything!

Why Monitoring is Important for Security



- We can automate system interrogation
- We can automate anomaly detection
- We can set sensors on high risk systems
- The best security tools in the world are useless without someone/something monitoring (and acting on) the results
- It can improve intrusion detection and incident response
- It can greatly improve forensics
- We can get a good real-time view of a network

The title is centered at the top of the slide. It is flanked by five circles of varying shades of light purple. The first circle is solid, the second is an outline, the third is solid, the fourth is an outline, and the fifth is solid.

Is Nagios a Security Tool?

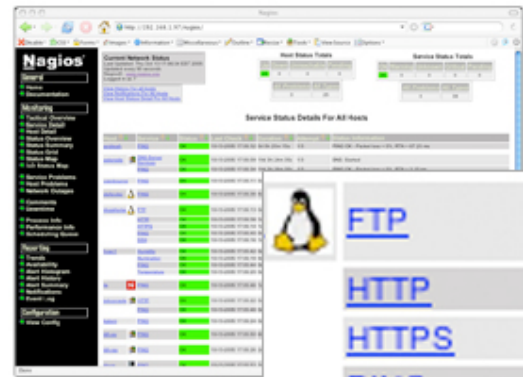
- Yes, I think it is.
- Even if you wouldn't classify Nagios as a security tool per se, you can easily integrate your "security" tools of choice into a Nagios framework.

How Nagios Works




- You create a list of hosts and services
- You choose what you want to check, Nagios supports both Active and Passive checks
- Hosts can have hierarchical relationships
- Nagios runs (and talks to) *plugins* that do all sorts of checks. We will cover what sorts of checks a little later.
- You can view status information at any time and configure notifications, typically email and SMS
- Nagios uses an object and template based configuration system
- This is really the tip or the iceberg, Nagios epitomises flexibility.

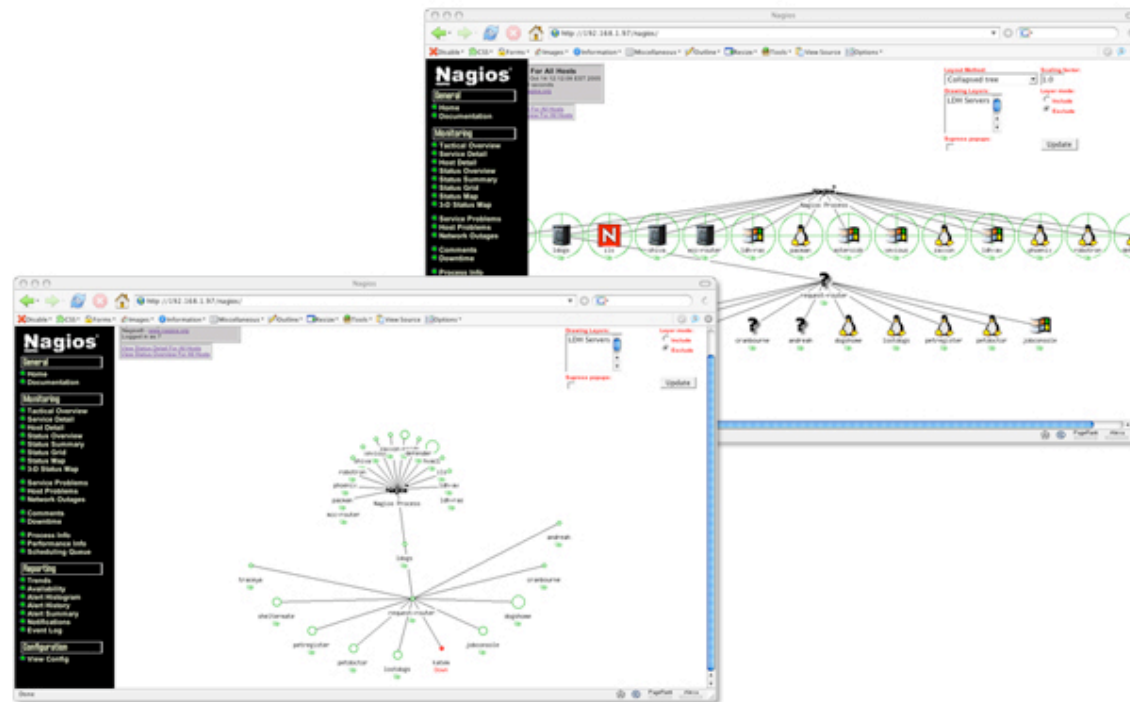
Viewing Status Information



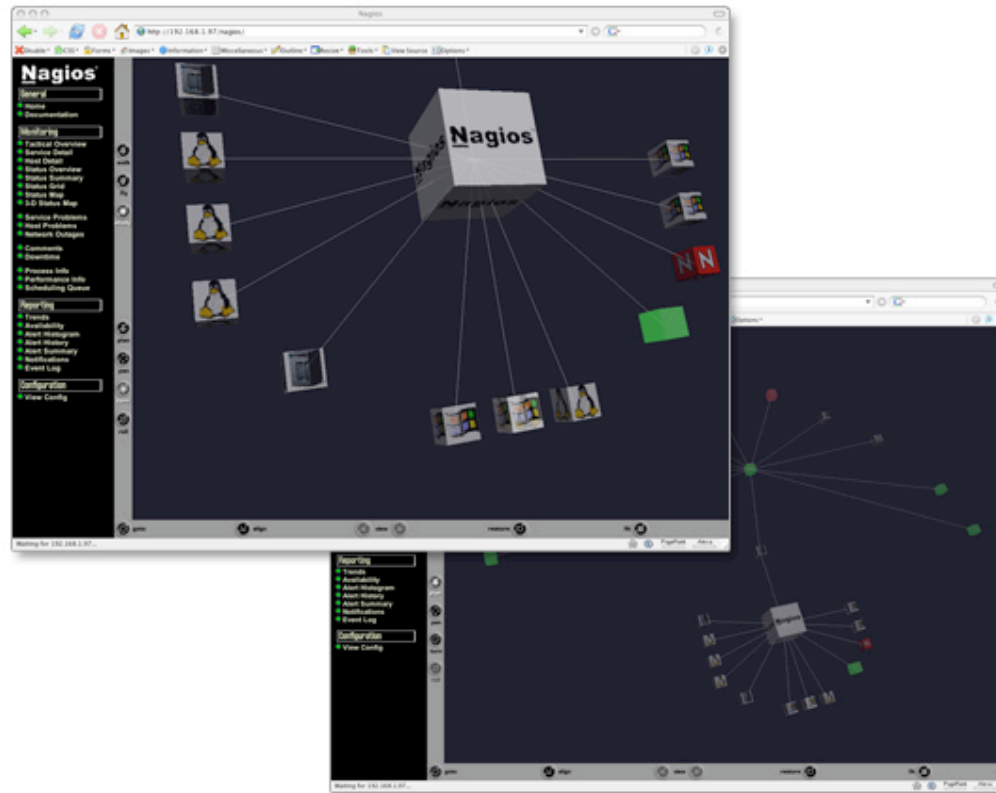
The screenshot shows the Nagios web interface. On the left is a navigation menu with categories like 'General', 'Monitoring', 'Hosts', and 'Services'. The main content area displays 'Service Status Details For All Hosts' with a table of service statuses. A tooltip window is overlaid on the right, showing a list of services with their status.

 FTP	OK
HTTP	OK
HTTPS	OK
PING	OK
SSH	OK

Viewing Status Information Visually

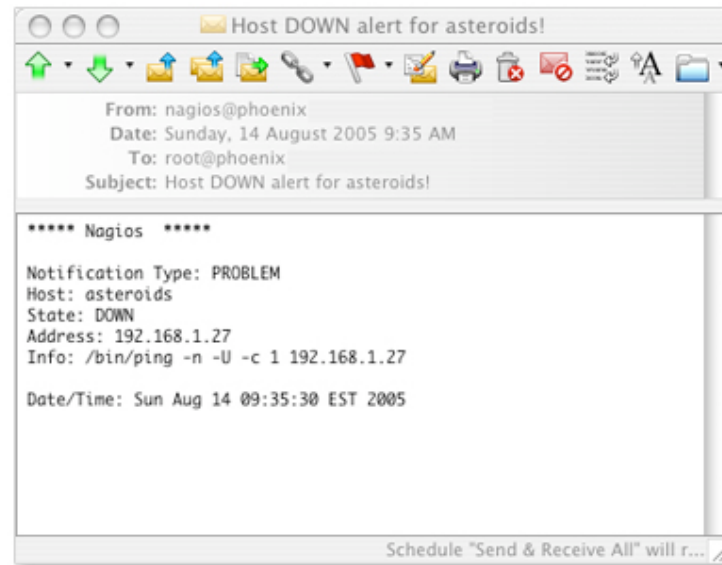


Viewing Status Information in 3D VRML



Alerts

- Email
- SMS



Other Types of Alerts



- Pager
- Voice
- IM
- Popup Windows
- Plus lots more...

Standard Types of Checks

- check_by_ssh.c
- check_dhcp.c
- check_dig.c
- check_disk.c
- check_dns.c
- check_dummy.c
- check_fping.c
- check_game.c
- check_hpic.c
- check_http.c
- check_icmp.c
- check_ide_smart.c
- check_ldap.c
- check_load.c
- check_mrtg.c
- check_mrtgtraf.c

- check_mysql.c
- check_nagios.c
- check_nt.c
- check_nwstat.c
- check_overcr.c
- check_pgsql.c
- check_ping.c
- check_procs.c
- check_radius.c
- check_real.c
- check_smtp.c
- check_snmp.c
- check_ssh.c
- check_swap.c
- check_tcp.c
- check_time.c
- check_udp.c

- check_ups.c
- check_users.c
- check_breeze.pl
- check_disk_smb.pl
- check_file_age.pl
- check_flexlm.pl
- check_ifoperstatus.pl
- check_ifstatus.pl
- check_ircd.pl
- check_log.sh
- check_mailq.pl
- check_ntp.pl
- check_oracle.sh
- check_rpc.pl
- check_sensors.sh
- check_wave.pl

More Checks

- check_apache.pl
- check_apc_ups.pl
- check_appletalk.pl
- check_arping.pl
- check_asterisk.pl
- check_axis.sh
- check_backup.pl
- check_bgpstate.pl
- check_breeze.pl
- check_cluster.c
- check_cluster2.c
- check_compaq_insight.pl
- check_cpqarray.c
- check_digitemp.pl
- check_disk_snmp.pl
- check_dlswcircuit.pl
- check_dns_random.pl
- check_email_loop.pl
- check_fan_cpq_present
- check_fan_fsc_present
- check_flexlm.pl
- check_frontpage
- check_hltherm.c
- check_hprsc.pl
- check_http-with-client-certificate.c

- check_hw.sh
- check_ica_master_browser.pl
- check_ica_metaframe_pub_apps.pl
- check_ica_program_neighbourhood.pl
- check_inodes-freebsd.pl
- check_inodes.pl
- check_ipxping.c
- check_javaproc.pl
- check_joy.sh
- check_linux RAID.pl
- check_lmmon.pl
- check_log2.pl
- check_lotus.pl
- check_maxchannels.pl
- check_maxwanstate.pl
- check_mem.pl
- check_ms_spooler.pl
- check_mssql.sh
- check_nagios.pl
- check_nagios_db.pl
- check_nagios_db_pg.pl
- check_netapp.pl
- check_nmap.py
- check_ora_table_space.pl
- check_oracle_instance.pl

- check_oracle_tbs
- check_pcpmetric.py
- check_pfstate
- check_qmailq.pl
- check_rbl.c
- check_remote_nagios_status.pl
- check_rrd_data.pl
- check_sap.sh
- check_smart.pl
- check_smb.sh
- check_snmp_disk_monitor.pl
- check_snmp_printer.pl
- check_snmp_process_monitor.pl
- check_snmp_procs.pl
- check_sockets.pl
- check_sybase
- check_temp_cpq
- check_temp_fsc
- check_timeout.c
- check_traceroute-pure_perl.pl
- check_traceroute.pl
- check_uptime.c
- check_vcs.pl
- check_wave.pl

- check_wins.pl
- checkciscotemp.pl
- mrtgext.pl
- nagios_sendim.pl
- packet_utils.pm
- rblcheck-dns
- rblcheck-web

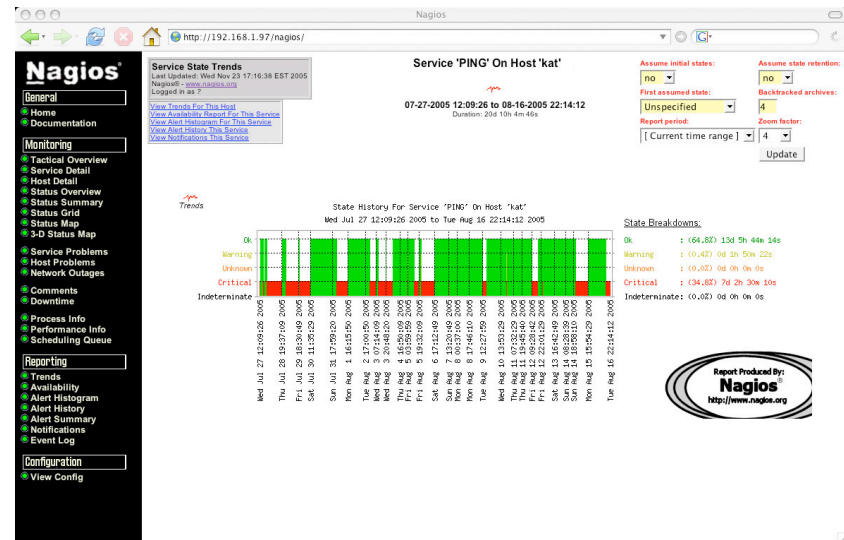
Acting on Events



- We can act on events by using Event Handlers
- Event handlers can do anything you want, some examples could be: shut down services, restart failed services, start applications, restart failed applications, run custom scripts

Reporting

- Useful for uptime reports
- Useful for SLA's
- Useful for giving clients or managers pretty pictures



Performance Data



- The standard plugins can be used to record useful performance data
- There are several extensions that enable Nagios to record very detailed performance statistics



Live Demonstration

Integrating Security Tools with Nagios



- Network Intrusion Detection Systems
- Malware Detection
- Integrity Checking
- New Host or Service Detection
- Watching Logs
- Your_Custom_Tool

Network Intrusion Detection Systems

- Snort
- PortSentry

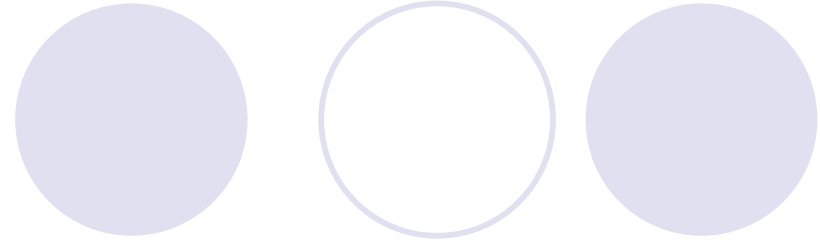
Malware Detection



- Anti Virus Applications (Clam, Trend, etc.)
- AMaViS
- chkrootkit

Integrity Checking

- Tripwire
- Package Tools
- Osiris
- Samhain



On the Lookout for New Hosts or Services



- Nmap
- Check to make sure that no new hosts have appeared on your subnet
- Check to make sure that no new services have appeared on particular hosts

Watching Logs



- It should go without saying that logging (ideally centralised logging) is critical in maintaining a secure infrastructure
- Syslog
- Syslog-NG
- Logwatch
- Swatch
- Logmuncher
- Can be logs from anything (backup app, transaction logs etc.)



Tales from the Trenches

- Logchecks on Honeypot Daemons
- Non-network Connected Servers
- Cacti/RRD Integration
- SNMP
- Java Application Monitoring
- WMI

More Information

- <http://www.Nagios.org>
- <http://www.NagiosExchange.org>
- <http://www.NagiosBook.org>

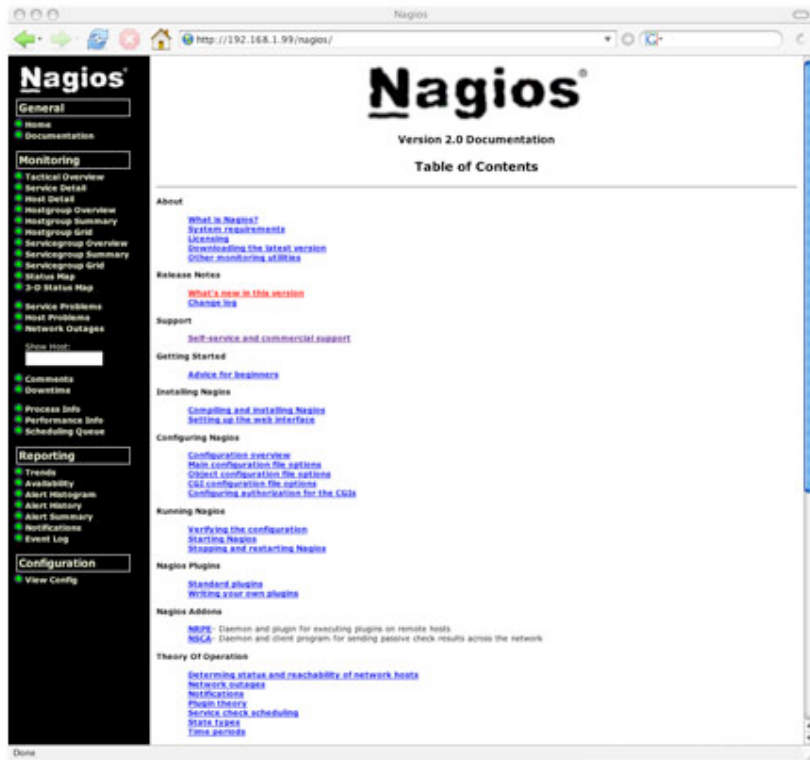


NagiosBook

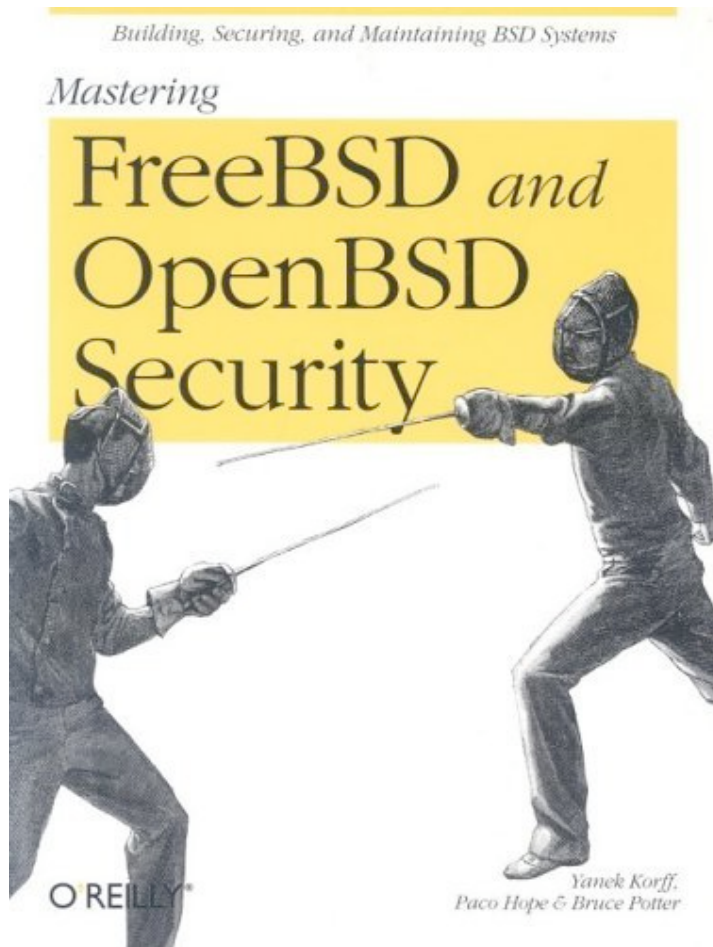


Recommended Reading

- Nagios
Documentation by
Ethan Galstad
Extremely thorough,
a must read



Recommended Reading



- Mastering FreeBSD and OpenBSD Security (O'Reilly) by Yanek Korff, Paco Hope, Bruce Potter

A great book covering both big picture and practical security

Recommended Reading



- Network Security Tools (O'Reilly) by Nitesh Dhanjani, Justin Clarke
Nagios isn't covered in this title, but great for building security tools



Technical Reviewers

A huge thank you to the following technical reviewers, both from the OSDC Team and the Nagios-Users mailing list.

- **Russell Adams**
- **Mark Limburg**
- **David Field**
- **Don Alfredo**



Thanks and Questions!

Chris Burgess

chris@chrisburgess.com.au

<http://www.chrisburgess.com.au>