18. Analyse-Tools

18. Analyse-Tools

Überwachen und Testen

- **Globale Systemüberwachung: nagios**
- DNS: nslookup, dig, host
- Lauschen: tcpdump, snoop, wireshark(ethereal), ntop
- Testen: nmap, nessus, OpenVAS
- Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)
- NetBIOS Informationen ausspähen: nbaudit

Hacken

Lokal

- Passworte entschlüsseln: crack, john

Netzwerk

- TCP Hijack Tool: juggernaut
- Tool für DdoS Attacken: trinoo
- Ping Programm: ping of death

18. Analyse-Tools

NAGIOS

Problematik

Kann man warten bis ein Anwender einen Fehler meldet?
Kann man warten bis man merkt, daß der Abzug nicht gelaufen ist?
Will man von jeder erfolgreichen Aktion eine Information?
.....

Nein

Was brauchen wir?

Ein Werkzeug das Gewöhnliches registriert und Ungewöhnliches registriert und meldet z.B. mittels Mail, SMS, ...

18. Analyse-Tools

NAGIOS

Was brauchen wir?

Tool, was in regelmäßigen Abständen überprüft, ob verschiedene Dienste auf den verschiedenen Rechnern noch korrekt funktionieren.

Zu überwachende Dienste:

- Mail, DNS, NIS, Plattenkapazität, Load, WWW, Zeitgeber, Zertifikate
- eigene Dienste, Erreichbarkeit, ...

Was soll das Tool machen:

- Fehler sofort melden!!!
- Status bei Bedarf anzeigen
- Vergangenheit merken und bei Bedarf anzeigen

18. Analyse-Tools

NAGIOS

Was ist NAGIOS?

Nagios = **N**etwork + h**agios** (der Heilige)

Programmpaket von Ethan Galstad – Freeware mit eingetragenem Warenzeichen (Name Nagios und Nagios-Logo)

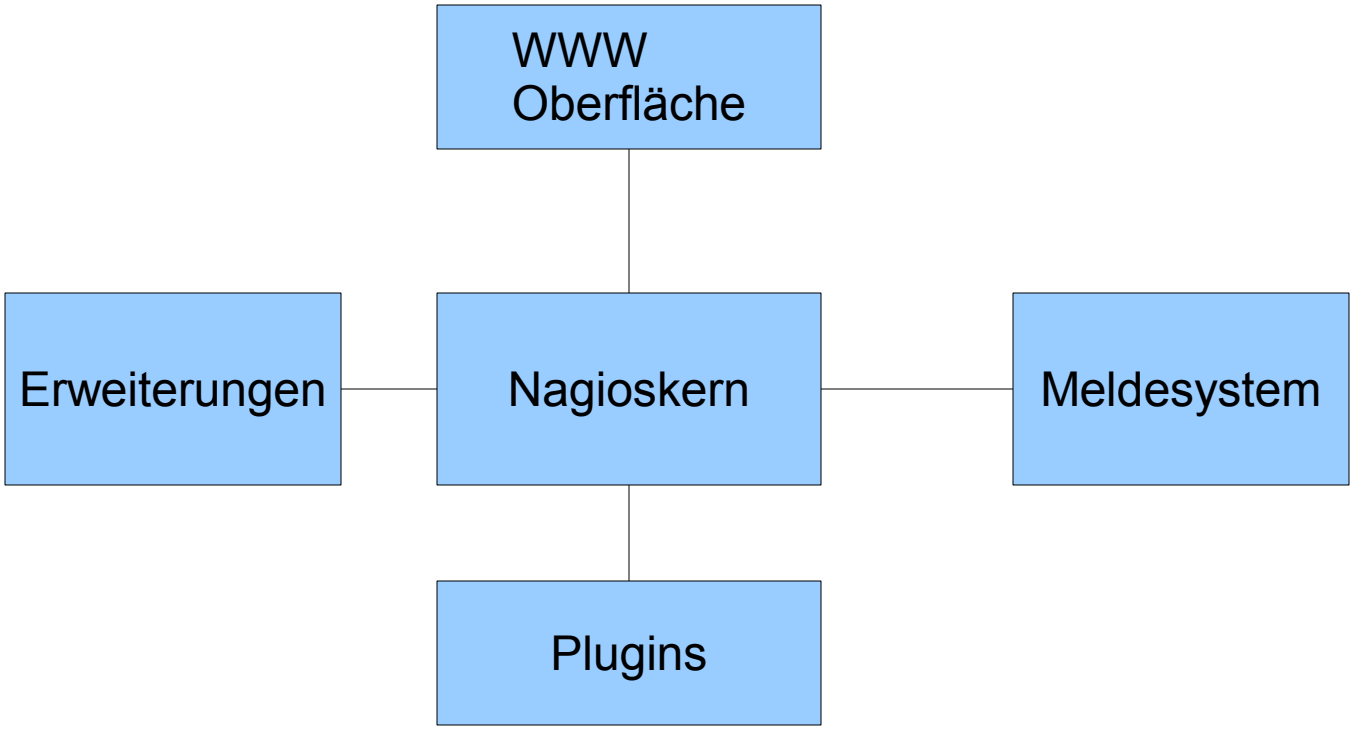
Was ist Nagios?

Überwachunstool, das mit Hilfe von Konfigurationsfiles konfiguriert wird und über eine WEB-Oberfläche die Ergebnisse darstellen und gleichzeitig gesteuert werden kann. Es führt mittels Plugins lokale Überwachungsoperationen aus oder fragt Ereignisse mittels zusätzlicher kleiner Überwachungsserver (nrpe), die auf entfernten Systemen laufen, ab. Die Plugins sind jeweils eigene Kommandos – in beliebiger Programmiersprache. Über besondere Ereignisse wird ein Administrator benachrichtigt.

18. Analyse-Tools

NAGIOS

Was ist NAGIOS?



18. Analyse-Tools

NAGIOS

Plugins

- Externe, selbständige Programme
  - Nur kommandozeilenorientiert
- Anforderungen an Plugins
  - Ausgabe besteht nur aus einzeiligen Textinformationen für WEB und Admin
  - Rückgabewert: 0 -ok (grün), 1 – Warnung (gelb), 2 – Critical (rot), 3 – unknown (orange)
  - Schwellwerte werden durch Parameter an das Plugin übergeben
- Programme aller Art sind zugelassen
  - Shell, Perl, Phyton, kompilierte Programme, bat-Dateien unter Windows

18. Analyse-Tools

NAGIOS

Plugins

Beispiel:

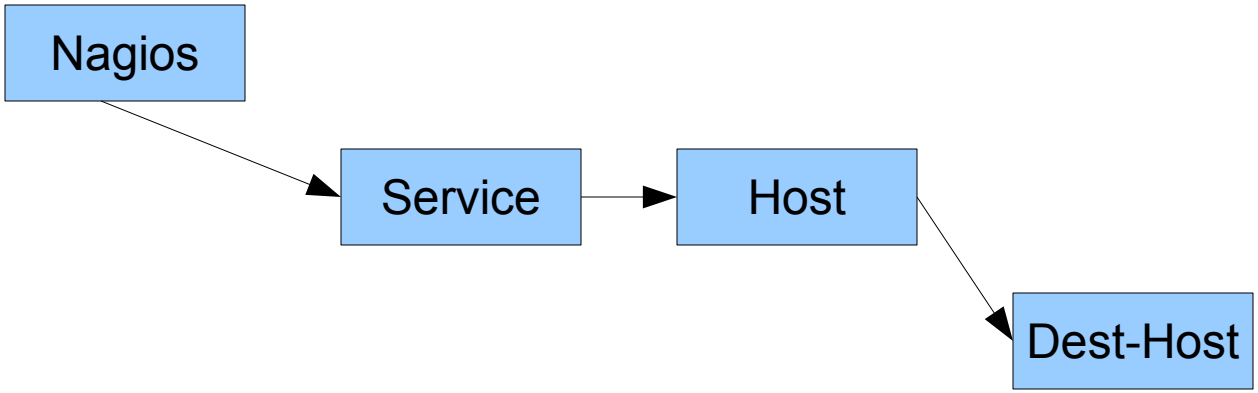
```
check_smtp -H host -p port -w 10 -c 20

check_icmp -H host -w 100.00 -c 2000.000

check_disk -w 10%  -c 5%  /tmp
```

18. Analyse-Tools

NAGIOS

Service- und Host-Checks

- Service-Checks werden regelmäßig ausgeführt
- Host-Checks werden nur bei Bedarf ausgeführt
- Ping kann als Service-Check definiert werden – sollte man



18. Analyse-Tools

NAGIOS

Netzwerktopologie und Meldesystem

Mittels der Nagioskonfigurationsfiles kann die Netzwerktopologie nachgebildet werden, so daß Fehler genau lokalisiert werden können. Dadurch können Fehlerzustände besser dargestellt werden. Nagios meldet dann nur die primären Fehlerzustände (down). Nachfolgende Zustände werden als unknown gemeldet.

Zustandswechsel werden sofort angezeigt. Kritische Zustände werden aber erst nach zwei aufeinanderfolgende gleiche Fehler gemeldet.

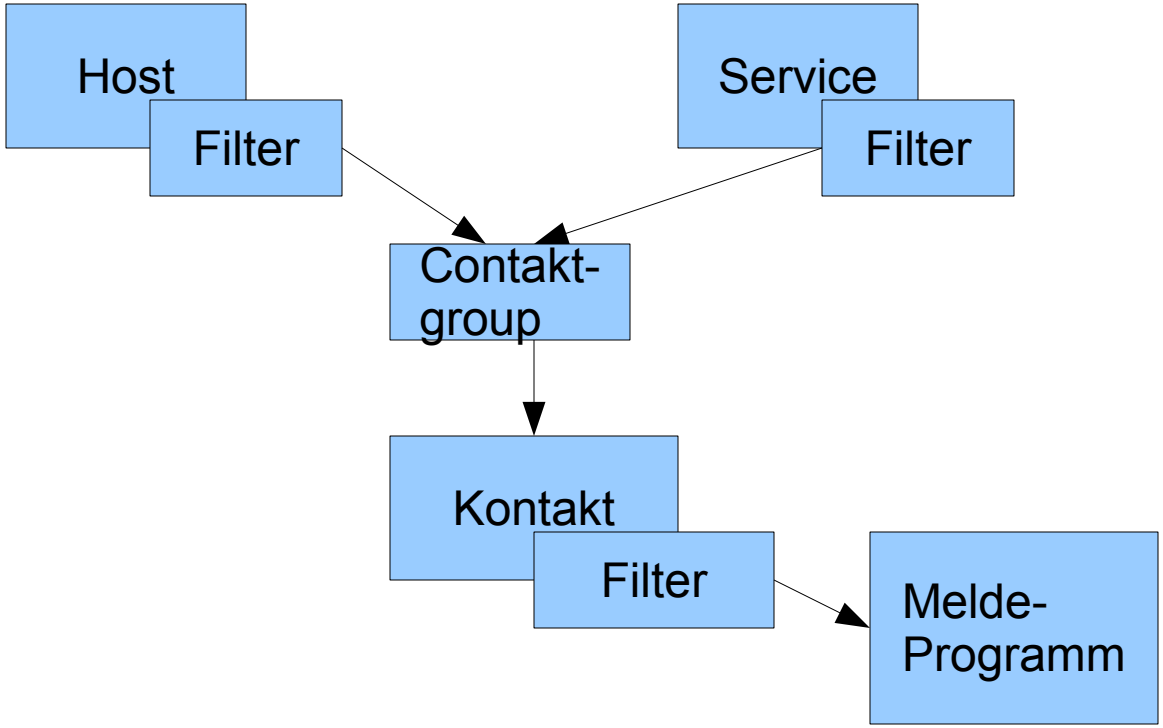
Benachrichtigung erfolgt an über Kontaktgruppen (Menge von Kontakten).

Kontakte sind Personen (Mailadresse, SMS-Nummber,...). Die Benachrichtigung übernimmt ein externes Programm.

18. Analyse-Tools

NAGIOS

Benachrichtigungssystem



18. Analyse-Tools

NAGIOS

Woher kommt das Ganze?

www.nagios.org

Files:

nagios-3.2.3.tar.gz - Quellfiles für Nagios
nagios-plugins-1.4.15.tar.gz - Quellen für Plugins
nrpe-2.12.tar.gz - Quellen für Hilfsserver nrpe

18. Analyse-Tools

NAGIOS

Konfigurationsfiles

nagios unter /etc/nagios:

objects	- Directory für Konfigurationsfiles
cgi.cfg	- Hauptkonfigurationsfile
nagios.cfg	- Basiskonfigurationsfile
hosts.cfg	- Hostbeschreibung
services.cfg	- Beschreibung der Services
commands.cfg	- Beschreibung von Kommandos
resource.cfg	- Beschreibung der Ressourcen
contacts.cfg	- Beschreibung der Kontakte
timeperiods.cfg	- Definition von Zeiträumen

18. Analyse-Tools

NAGIOS

Konfigurationsfiles nrpe /etc/nagios

nrpe.cfg - Alles Informationen für nrpe

Weitere Directories und Files

/usr/lib/nagios/plugins oder /usr/lib/nagios/libexec - Plugins
/usr/lib/nagios/cgi - CGI-Files für Apache
/etc/apache2/conf.d/nagios - www-Konfiguration
/usr/share/nagios - www-Directory

18. Analyse-Tools

NAGIOS

Was braucht Nagios sonst noch?

- apache2
- libssl
- openssl
- ssh
- zlib
- wget
- bzip2
-

18. Analyse-Tools

NAGIOS

Installation und Konfiguration - nagios

- apache2 /etc/apache2/conf.d/nagios
- Nagios cfg-Files modifizieren
- Nagios starten: /etc/init.d/nagios start
- Apache starten: /etc/init.d/apache2 start

Installation und Konfiguration – nrpe

- /etc/nagios/nrpe.cfg
- /etc/init.d/nrpe start

18. Analyse-Tools

Überwachen und Testen

- Globale Systemüberwachung: nagios
- **DNS: nslookup, dig, host**
- Lauschen: tcpdump, snoop, wireshark(ethereal), ntop
- Testen: nmap, nessus, OpenVAS
- Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)
- NetBIOS Informationen ausspähen: nbaudit

Hacken

Lokal

- Passworte entschlüsseln: crack, john

Netzwerk

- TCP Hijack Tool: juggernaut
- Tool für DdoS Attacken: trinoo
- Ping Programm: ping of death

18. Analyse-Tools

DNS: nslookup, dig

nslookup – Interaktive Abfrage des DNS (alt)

- nslookup [optionen] hostname
- nslookup
  - Subkommandos
    - exit
    - set type=[A | MX | PTR | NS | SOA | ANY]
    - server NAME
    - optional:
    - ls [-a | -h | -s | -d]
    - domainname=NAME
    - domain=NAME

18. Analyse-Tools

DNS: nslookup, dig

dig – DNS Lookup-Tool (neu)

dig [@*server*] [-t *type*] ... [*name*] [*type*] [*qoption*]

qoption - +trace, ...

dig @141.20.1.3 mail.informatik.hu-berlin.de +trace

host – Host Lookup-Tool(neu)

host *hostname*

host *ip-adresse*

host -t mx *ip-adresse server*

18. Analyse-Tools

Überwachen und Testen

- Globale Systemüberwachung: nagios
- DNS: nslookup, dig, host
- **Lauschen: tcpdump, snoop, wireshark(ethereal), ntop**
- Testen: nmap, nessus, OpenVAS
- Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)
- NetBIOS Informationen ausspähen: nbaudit

Hacken

Lokal

- Passworte entschlüsseln: crack, john

Netzwerk

- TCP Hijack Tool: juggernaut
- Tool für DdoS Attacken: trinoo
- Ping Programm: ping of death

18. Analyse-Tools

Lauschen: tcpdump, snoop, wireshark(ethereal), ntop

tcpdump

Standardtool zum Mitlesen des Netzwerkverkehrs an einer Konsole. Root Zugriffsrechte notwendig.

tcpdump -X -s 200 -i eth1 host ftp

18. Analyse-Tools

Lauschen: tcpdump, snoop, wireshark(ethereal), ntop

snoop

Standardtool zum Mitlesen des Netzwerkverkehrs an einer Console für Solaris. Root-Zugriffsrechte notwendig.

snoop -v -s 200 -d bge0 host ftp | grep FTP

18. Analyse-Tools

Lauschen: tcpdump, snoop, wireshark(ethereal), ntop

wireshark (ethereal)

Standardtool zum Mitlesen des Netzwerkverkehrs mit Hilfe einer grafischen Oberfläche – sehr gut zur Protokollanalyse geeignet, Life-Mitlesen.

root-Zugriffsrechte notwendig.

Aufruf:

wireshark &

18. Analyse-Tools

Lauschen: tcpdump, snoop, wireshark(ethereal), ntop

ntop

Installation:

- Programme installieren
- ntop -A -u root
- /etc/sysconfig/ntop - editieren Interface

Starten:

- /etc/init.d/ntop start
- Browser: http://localhost:3000/

18. Analyse-Tools

Überwachen und Testen

- Globale Systemüberwachung: nagios
- DNS: nslookup, dig, host
- Lauschen: tcpdump, snoop, wireshark(ethereal), ntop
- **Testen: nmap, nessus, OpenVAS**
- Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)
- NetBIOS Informationen ausspähen: nbaudit

Hacken

Lokal

- Passworte entschlüsseln: crack, john

Netzwerk

- TCP Hijack Tool: juggernaut
- Tool für DdoS Attacken: trinoo
- Ping Programm: ping of death

18. Analyse-Tools

Testen: nmap, nessus, OpenVAS

nmap

Werkzeug zum prüfen der Eigenschaften eines Rechners im Netz. Vorsicht die Benutzung dieses Werkzeuges kann als Angriff auf einen Rechner gewertet werden.

Installation: Standardtool

Aufruf:

```
nmap -P0 -sS 141.20.20.32
nmap -sT 141.20.20.32
nmap -sU -p 1-1023 141.20.20.32
nmap -sV 141.20.20.32
nmap -sV -p 22,53,110,143 garak
```

18. Analyse-Tools

Testen: nmap, nessus, OpenVAS

nessus, OpenVAS

Installation:

Programme installieren, Standardtool

Konfiguration:

nessus-mkcert # Zertifikat erzeugen

nessus-adduser # Nutzer hinzufügen, der nessus benutzen darf

Starten:

/etc/init.d/nessusd start

nessus &

18. Analyse-Tools

Überwachen und Testen

- Globale Systemüberwachung: nagios
- DNS: nslookup, dig, host
- Lauschen: tcpdump, snoop, wireshark(ethereal), ntop
- Testen: nmap, nessus, OpenVAS
- **Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)**
- NetBIOS Informationen ausspähen: nbaudit

Hacken

Lokal

- Passworte entschlüsseln: crack, john

Netzwerk

- TCP Hijack Tool: juggernaut
- Tool für DdoS Attacken: trinoo
- Ping Programm: ping of death

18. Analyse-Tools

Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)

Sammlung von Passwortsniffern und Spoofern

Installieren:

Quelle: http://naughty.monkey.org/~dugsong/dsniff

dsniff-2.3.tar.gz

dsniff-2.4b1.tar.gz

Libraries:

libnet 1.02a - Netzwerk

libnids 1.16 - intrusion detection

libssl

configure

make

Viele Tricks notwendig, da dsniff von 2003 stammt!!

18. Analyse-Tools

Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)

Programme:

arpspoof - ARP spoofing, hebelt den Switch aus

arpspoof [-i interface] [-t target] destinationhost

dnsspoof – DNS spoofing

dnsspoof [-i interface] [-f hostsfile] tcpdump-expression

dsniff – Passwortsniffer

dsniff [-c] [-d] [-m] [-i interface] [-s snaplen] ... tcpdump-expresseion

filesnarf - belauscht Files bei NFS-Transport

filesnarf [-i] [[-v] pattern [expression]]

18. Analyse-Tools

Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)

Programme:

macof – Fluten eines geswitchten Netzes mit MAC-Adressen

macof [-i interface] [-s src] [-d dst] [-x sport] [-y dport] [-n times]

mailsnarf – fängt Mails ab und speichert sie in eine Mailbox

mailsnarf [-i interface] [[-v] pattern [expression]]

msgsnarf – belauscht CHAT-Messages

msgsnarf [-i interfacer] [[-v] pattern [expression]]

sshmitm – ssh man in the middle attack

18. Analyse-Tools

Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)

Programme

sshow – analysiert SSH1 und SSH2 Protokolle (Passwortlängen,..)

tcpkill – killt eine TCP-Verbindung im LAN

tcpkill [-i interface] [-1 .. 9] tcpdump-expression

tcpnice – Verlangsamt TCP-Verbindungen

tcpnice [-A] [-I] [-M] [-i interface] tcpdump-expression

urlsnarf – Protokolliert alle HTTP-Requests

urlsnarf [-n] [-i interface] [[-v] pattern [expression]]

18. Analyse-Tools

Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)

Programme

webmitm – WWW man in the middle attack mit dnsspoof

webspy – kopiert WWW-Request eines Anderen direkt
in den eigenen Browser (Netscape) – man kann mitlesen
webspy [-i interface] Zielhost

18. Analyse-Tools

Überwachen und Testen

- Globale Systemüberwachung: nagios
- DNS: nslookup, dig, host
- Lauschen: tcpdump, snoop, wireshark(ethereal), ntop
- Testen: nmap, nessus, OpenVAS
- Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)
- **NetBIOS Informationen ausspähen: nbaudit**

Hacken

Lokal

- Passworte entschlüsseln: crack, john

Netzwerk

- TCP Hijack Tool: juggernaut
- Tool für DdoS Attacken: trinoo
- Ping Programm: ping of death

18. Analyse-Tools

Nbaudit: NetBIOS Informationen ausspähen

-

18. Analyse-Tools

Überwachen und Testen

- Globale Systemüberwachung: nagios
- DNS: nslookup, dig, host
- Lauschen: tcpdump, snoop, wireshark(ethereal), ntop
- Testen: nmap, nessus, OpenVAS
- Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)
- NetBIOS Informationen ausspähen: nbaudit

Hacken

Lokal

- **Passworte entschlüsseln: crack, john**

Netzwerk

- TCP Hijack Tool: juggernaut
- Tool für DdoS Attacken: trinoo
- Ping Programm: ping of death

18. Analyse-Tools

crack – Passworte entschlüsseln

lokal einsetzbar

für Windows

crack

für Unix:

john-1.7.2

18. Analyse-Tools

Überwachen und Testen

- Globale Systemüberwachung: nagios
- DNS: nslookup, dig, host
- Lauschen: tcpdump, snoop, wireshark(ethereal), ntop
- Testen: nmap, nessus, OpenVAS
- Spähen: dsniff (Passwort-sniffer für ftp, telnet, smtp, nis ...)
- NetBIOS Informationen ausspähen: nbaudit

Hacken

Lokal

- Passworte entschlüsseln: crack, john

Netzwerk

- **TCP Hijack Tool: juggernaut**
- **Tool für DdoS Attacken: trinoo**
- **Ping Programm: ping of death**

18. Analyse-Tools

Netzwerk-Angriffstools (inspecting an hijacking)

juggernaut – TCP Hijack Tool

dnshijacker v1.3 , Hjksuit 0.1.99, HUNT v1.5

P.A.T.H. V0.7 (in Perl)

trinoo – Tool für DdoS Attacken

Ping of Death – Ping Programm