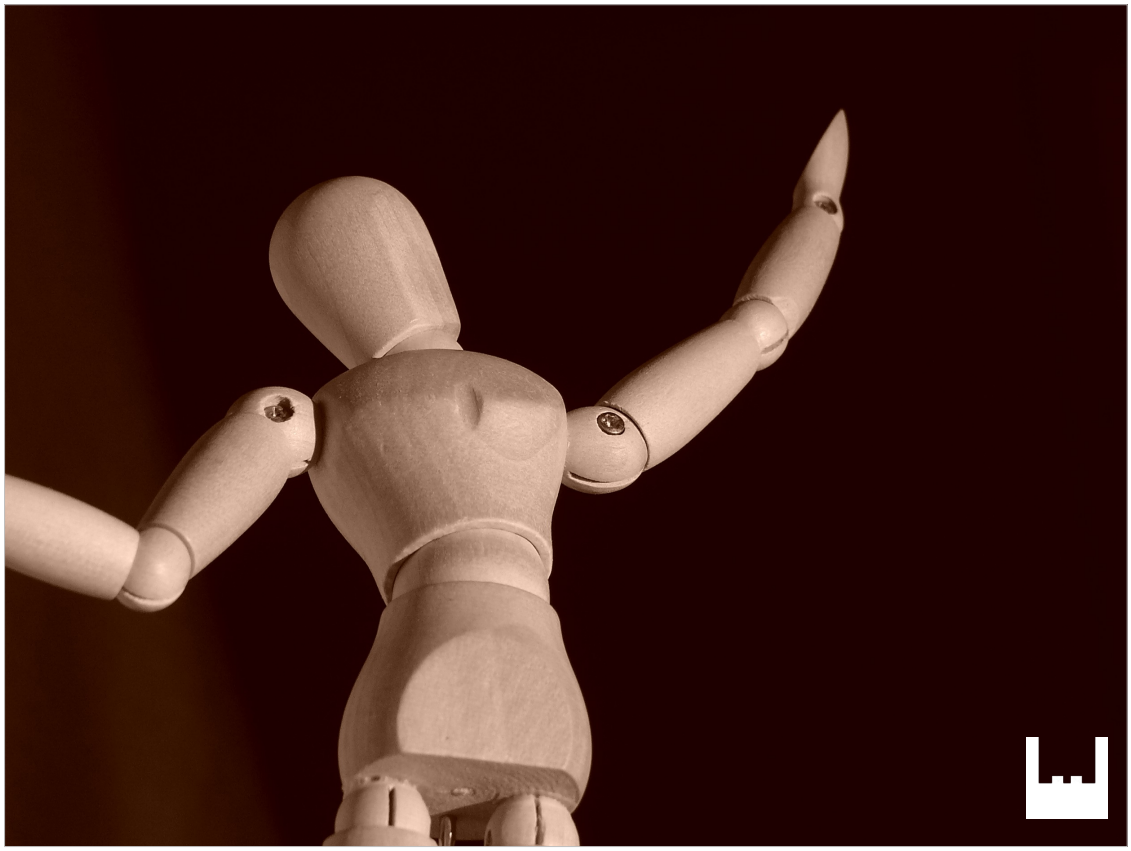
Thorsten Robers
OpenSource Training Ralf Spenneberg

Schulungen zum Thema Monitoring:
Netzwerk- und Systemmonitoring mit Nagios, Munin & Co
Advanced Monitoring

Vortragsfolien:
https://ostlogd.spenneberg.net

Secure Linux Administration Conference 2009

Dynamisches Monitoring mit Nmap und Nagios/Icinga



Thorsten Robers
OpenSource Training Ralf Spenneberg

B. Sc. Angewandte Informatik
Administrator und Trainer im OpenSource/Linux-Umfeld mit den Themenschwerpunkten: Monitoring mit OpenSource, Apache 2.X, VPN

http://www.os-t.de
https://ostlogd.spenneberg.net

Nmap

- OpenSource Port- und Netzwerkscanner
- Hosterkennung
- Portscanning
- OS- und Service-Detection
- Mehrere Anwendungen

Während ein
$ nmap tagesschau.de
zu der Annahme verleitet, dass tageschau.de nicht verfügbar ist, führt der Aufruf
nmap -PN -PS -n -T4 tagesschau.de –host-timeout 15000
Zu der realistischeren Einschätzung, dass der Server Dienste anbietet.

Der erste Aufruf versucht zunächst mit einem Ping die Verfügbarkeit zu testen. Eine vorgeschaltete Firewall jedoch schluckt ICMP-Echo Request und antwortet nicht darauf. TCP-SYN-Ping jedoch versucht jedoch mittels SYN-Packet eine Verbindung aufzubauen. Jegliche Antwort, deutet auf die Verfügbarkeit des Systems hin.
TCP-ACK-Ping machen ähnliches, jedoch lediglich mit ACK-Packeten.


Portscanning
7
9
11
13
15
17
19
21
8
10
12
14
16
18
20
22
24

Nmap Scripting Engine

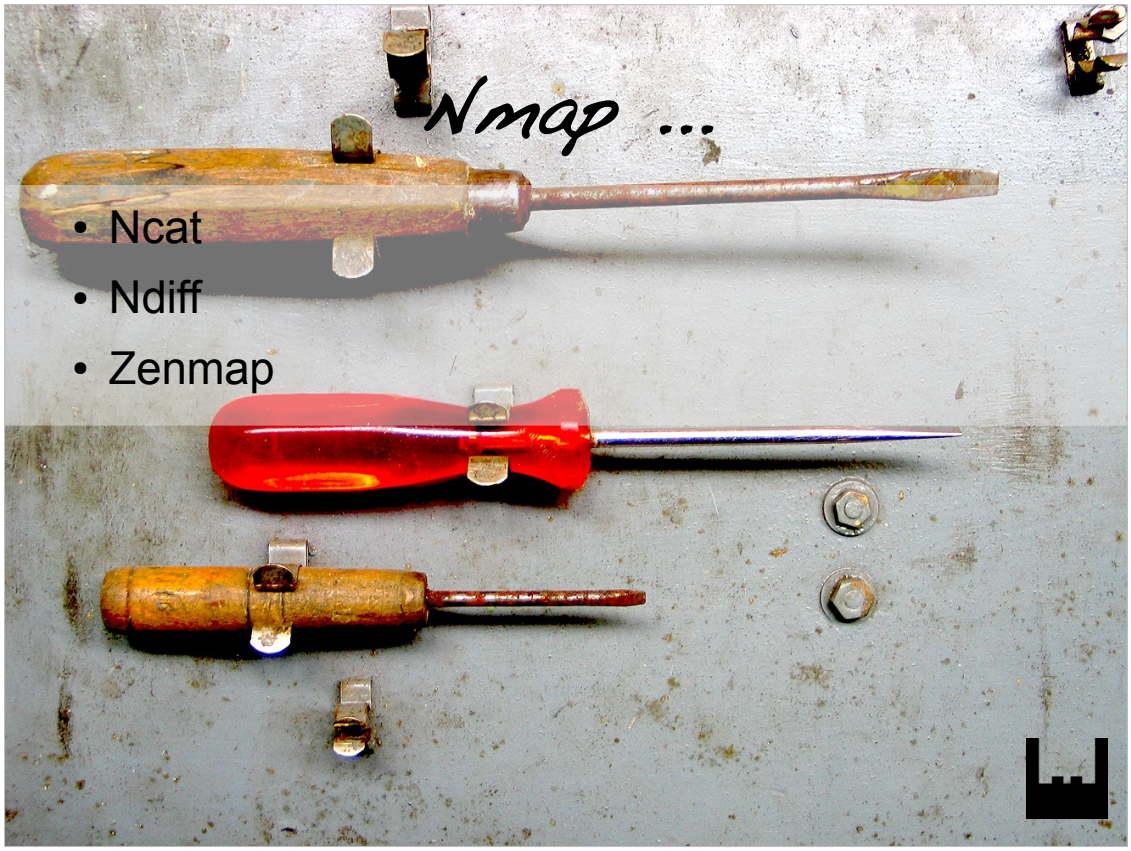
- Gliederung durch Klicken hinzufügen

Die Nmap Scripting Engine NSE) erlaubt die Ausführungvon LUA-Code zur Analyse eines nmap-Scans.

Lua ist eine Interpretersprache.

Mittels Nmap und der NSE lässt sich somit auch eine Prüfung eines Netzwerkes auf die Anwesenheit bestimmter Malware testen. Der folgende Aufruf führt eine Prüfung auf eine Infektion mit den Conficker-Wurm durch.

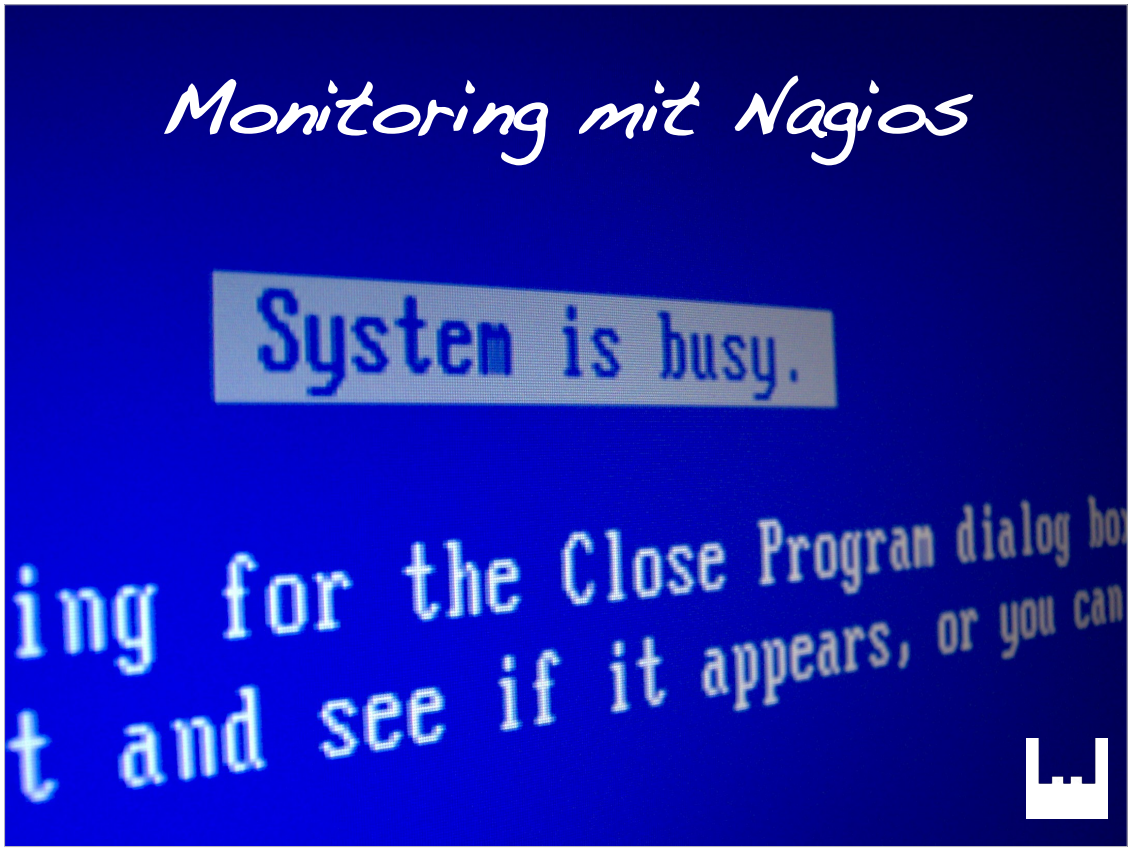
```
nmap -PN -p139,445 -n -v --script=smb-check-vulns
  --script-args safe=1 <host>
```



Neben Nmap werden durch Nmap weitere Tools zur Verfügung gestellt. Mittels ncat können zum Beispiel als root beliebige Ports mit belibigen Programmen versehen. Als unpriviligierter User ist es nur mit Ports jenseits des Ports 1024 möglich.

Ein einfacher Echo-Server sind dann wie folgt aus:

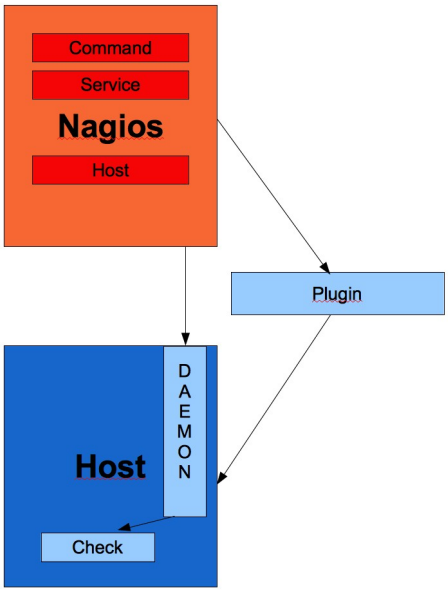
ncat -l 7 –exec “/bin/cat“


Monitoring mit Nagios
System is busy.
ing for the Close Program dialog box
t and see if it appears, or you can

In dem meisten Fällen wird Nagios im wesentlichen zu einer proaktiven Verfügbarkeitsprüfung eingesetzt. Hierbei werden sowohl Hosts als auch Serverdienste kontinuierlich getestet.

Zusätzlich kann mit Nagios beispielsweise auch die Abarbeitung von Cronjobs überwachen.

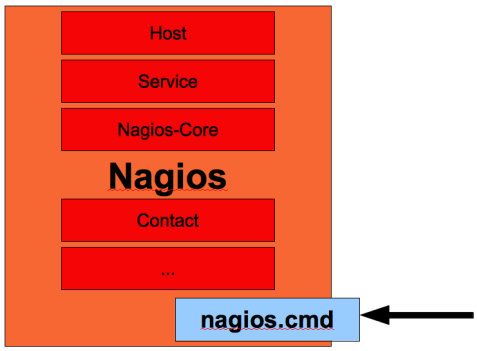
Funktionsweise



Für die Prüfung muss Nagios entweder selbst Checks auf die Systeme und Dienste durchführen, dies geschieht im wesentlichen über entsprechende Plugins.

Müssen lokale Ressourcen auf Remote-Systemen überwacht werden. So wendet sich Nagios meist an einen Daemon auf den Remote-Host, welcher wiederum die entsprechenden Checks ausführt. Auch eine SSH-Verbindung kann zur Ausführung von derartigen Checks verwendet werden.

External Commands



Bei der externen Kommandoschnittstelle handelt es sich um eine Pipe im lokalen Dateisystem des Nagios-Servers. Nagios liest regelmässig aus dieser Pipe um die externen Kommandos zu verarbeiten.

Mittels der externen Kommandoschnittstelle kann eine Nagios-Instanz im laufenden Betrieb in ihrem Verhalten beeinflußt werden. Aber auch passive Check-Ergebnisse werden über diesen Weg an Nagios übermittelt.

Alle externen Kommandos zeigt:
http://old.nagios.org/developerinfo/externalcommands/comm

Makros

- Standard-Makros
- Customize Makros
  - _
  - $_HOST...

Die vorhandenen Standard-Makros sind zu finden unter:

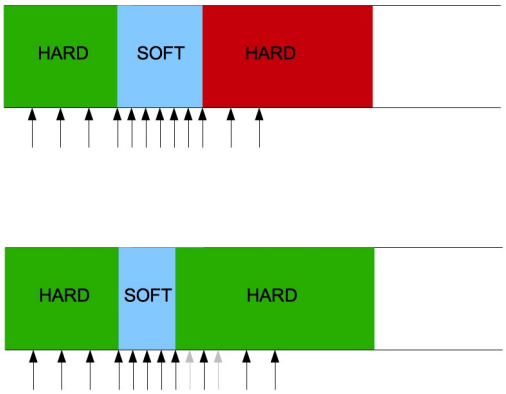
•http://nagios.sourceforge.net/docs/3_0/macrolist.html

•Customize Macros

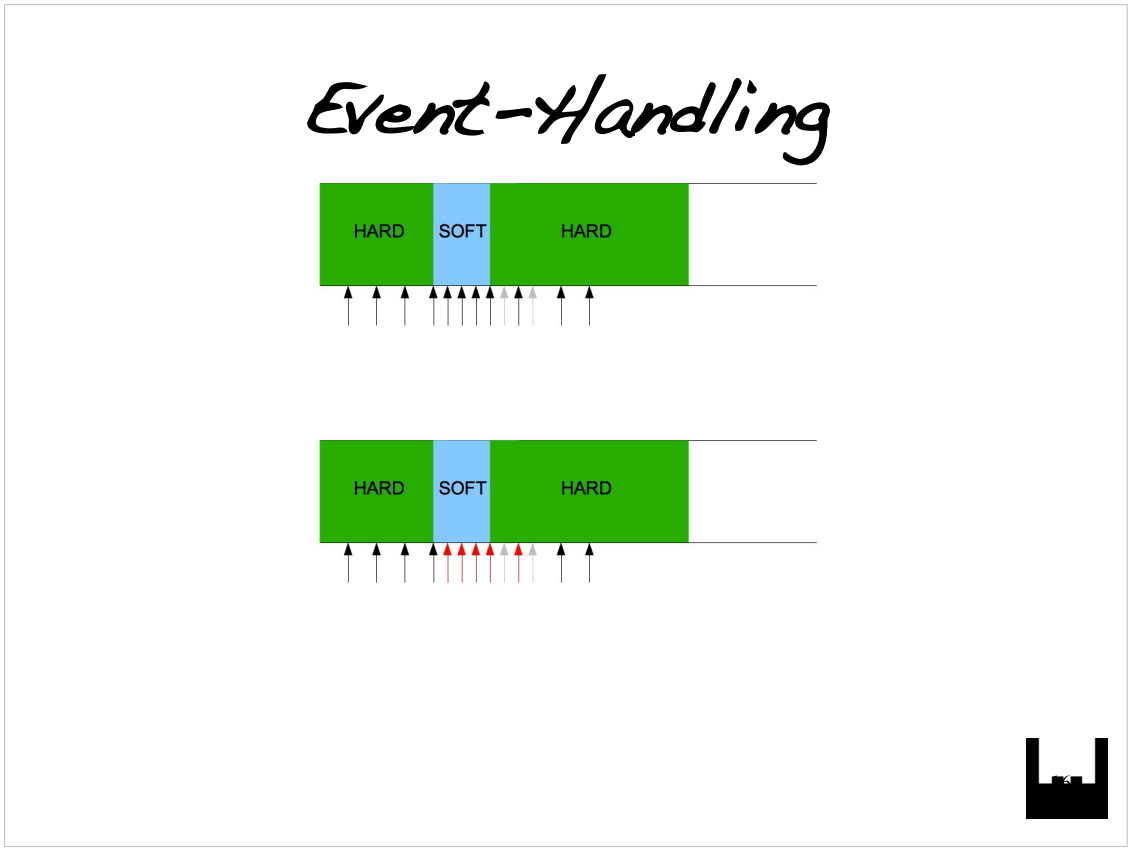
Userspezifische Makros können in der Definition aller Nagios-Objekte verwendet werden. Sie beginnen immer mit einem . Dies soll ein Überschreien der vorhanden Makros verhindern. Angewendet werden diese Makros unter der Bezeichnung: $_<NAGIOSOBJEKT>MAKRO$

•Beispiel: Host-Objekt: PORTS 80,22
Makro: $_HOSTPORTS$

Event-Handling

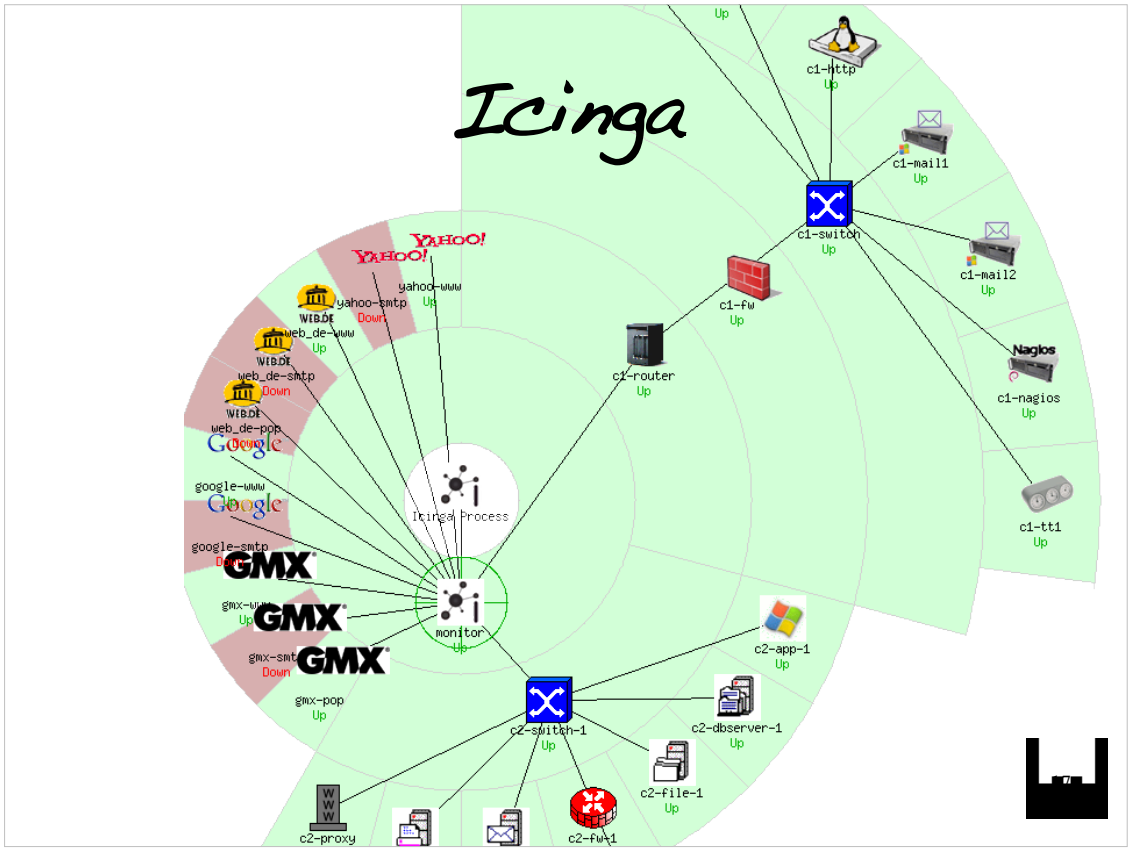


Nagios unterscheidet zwei unterschiedlichen Stati für die Stati der Hosts und Services. OK-Status ist generell Hard-State. Ein Soft-State liegt immer dann vor, wenn Nagios Wiederholungstests durchführt, um mögliche Plugin-Timeouts oder -Fehler auszuschließen. Erst nach der Durchführung aller Softstate-Tests wird Nagios einen fehlerhaften Hard-State Zustand benachrichtigen.



Die konfigurierten Event-Handler werden immer nach jedem Wiederholungstests im Soft-State und einmalig nach dem ersten Check nach der Wiederherstellung eines Service/Host.

Hierdurch können sowohl fehlerhafte und OK-Stati durch eine Flankierung mittels Event-Handlern weitere Aktionen initieren.



Icinga ist ein Nagios-Fork.

alpha.icinga.org

Anmeldung mittels guest/guestuser

Nun ein wenig Dynamik ...

Dynamisches Monitoring

- Motivation
- Umsetzung
- Sicherheit nicht Verfügbarkeit
- Erweiterbar nach OS-Abhängigkeit

Motiviation für die Beschäftigung mit dynamischem Monitoring stellte die Anforderung eines Kunden dar. Es sollte unternehmensweite Security Policy auch auf dem Cient proaktiv überwacht werden.

Es sollten sowohl die Aktivität von Virenscannern, die Existenz bestimmter Prozesse und weitere Details auch auf den Clients der Endanwender überwacht werden.

Nur sind diese Systeme nicht zu vorhersagbaren Zeiten verfügbar. So das eine dynamische Steuerung der Check-Intervalle realisiert werden musste.

Motivation für „Angriffe"

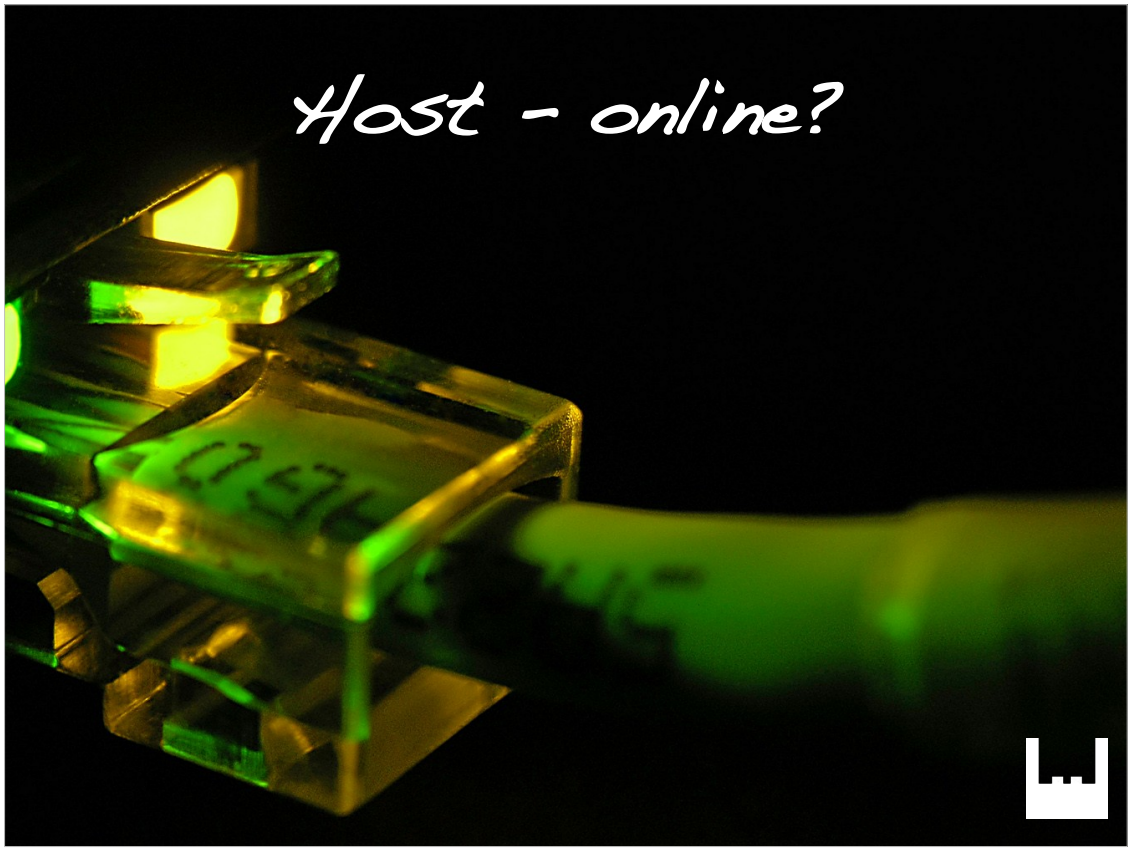
- Skript-Kiddies/ Wettbewerb/ Herausforderung
- Wirtschaftsspionage
- Politische Motivationen
- Persönliche Unzufriedenheiten

Warum bestand die Dringlichkeit der Client-Security-Überwachung.

Nach außen sind die meisten Firmen ausreichend abgesichert. Daher konzentrieren sich viele „Hacker“ darauf zunächst in die IT-Struktur einzudringen. Hierbei spielen gerade Clientsysteme eine wichtige Rolle.

http://www.heise.de/newsticker/meldung/Studie-Die-15-haeu

Bei Angriffen auf Unternehmensdaten rangiert die Installation von SpyWare auf Systemen auf Platz 2 der 15 häufigsten Angriffsmethoden.



Bei der Prüfung der Verfügbarkeit der Client-Systeme muss zum Teil auf nmap zurückgegriffen werden. Zum Beispiel unterbindet die Windows-Firewall standard ein Ping auf die Maschinen und dropt entsprehchende ICMP-Echo Request.

Portscanning

windows3	Port-Check	CRITICAL	2009-12-08 16:50:16	0d 0h 1m 15s	2/4	NOT AUTHORIZED PORTS: 554
windows1	Port-Check	WARNING	2009-12-08 16:31:08	0d 3h 48m 55s	4/4	No ports available. Missing Ports: 135,139,445,554

Das beigefügte Script realisiert eine Kombination aus customized Macros und einem Bash-Script zur Überwachung von offenen Ports auf einem Host. Hierbei werden alle Unterschiede signalisiert. Sowohl zusätzliche als auch nicht vorhandene Ports werden bemängelt.

Beachten Sie hierbei auch die Definition des Nagios-Host-Objektes.

Virenschutz?!

windows1	Antivir	CRITICAL	2009-12-08 17:31:04	0d 0h 2m 36s	3/4	ANTIVIR-CHECK CRITICAL - No AntivirusProduct installed
	Port-Check	WARNING	2009-12-08 17:31:08	0d 4h 45m 32s	4/4	Missing LISTEN-Ports: 554

Mit einem einfachen Programm wird auf Windows-Clients lokal die Verfügbarkeit, Aktualität und Aktivität von Antiviren-Produkten geprüft.

Für die meisten gängigen Linux-Distribution gibt es vorgefertigte Plugins zur Prüfung des Patch-Levels.

Auch für Windows-Systeme gibt es Möglichkeiten der Überwachung des Patch-Levels auf dem System.

Security Policy und Nagios

Mittels einer dynamischen Steuerung von Nagios können somit Security Policies für Client-Sysmte auch proaktiv überwacht werden.

Hierbei sind unterschiedliche Dinge denkbar:
- Virenschutz
- Host-IDS
- Installation von bestimmter SW prüfen
- Abwesenheit bestimmter SW prüfen

…

Dynamisierung

Das vorgestellte Konzept Nagios mittels Customize Macros, Event-Handler und externer Kommandoschnittstelle zur Laufzeit zur Steuerung kann auch auf andere Monitoring-Bereiche ausgedehnt werden.

So könnten die Customize Macros dazu verwendet werden, weitere Parameter zu konfigurieren um diese zur Laufzeit an Commandos oder Event-Handler zu übergeben.


Thorsten Robers
OpenSource Training Ralf Spenneberg
Schulungen zum Thema Monitoring:
Netzwerk- und Systemmonitoring mit Nagios, Munin & Co
Advanced Monitoring
Vortragsfolien:
https://ostlogd.spenneberg.net