Studienarbeit

Cheops für VNUML
Erstellen und beobachten einer VNUML-Simulation per Mausklick

Martin Bayer
März 2012

Universität Koblenz-Landau
Abteilung Koblenz

Fachbereich 4 – Informatik
AG Rechnernetze

Betreuer:
Prof. Dr. Christoph Steigner
Dipl. Inf. Frank Bohdanowicz

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Studienarbeit selbständig verfasst und keine anderen als die von mir angegebenen Quellen und Hilfsmittel verwendet habe.

	Ja	Nein
Mit der Einstellung der Arbeit in die Bibliothek bin ich einverstanden	◯	◯
Der Veröffentlichung dieser Arbeit im Internet stimme ich zu.	◯	◯

Koblenz, den 28.03.2012

Martin Bayer

Zusammenfassung

Cheops für VNUML - Erstellen und beobachten einer VNUML-Simulation per Mausklick

Es wird untersucht, wie Virtual Network User Mode Linux (VNUML), eine Software zur Simulation von Rechnernetzen, die aus virtualisierten Linux Instanzen aufgebaut werden, für den Benutzer besser handhabbar gemacht werden kann. Mit dem Linux-Paket VNUML, welches die dateigesteuerte Konfiguration virtueller Betriebssysteminstanzen ermöglicht, erhält der Anwender die Möglichkeit, komplexe Netzwerktopologien zu simulieren. Verschiedene Netzwerküberwachungsprogramme werden auf ihre Fähigkeit hin untersucht, eine laufende VNUML-Simulation zu erfassen und sinnvoll abzubilden. Dabei soll der Benutzer einen schnellen Überblick über die Funktion der simulierten Netzwerkumgebung, sowie nach Möglichkeit auch über deren Topologie erhalten können.

Das Programm Cheops, welches der Netzwerküberwachung dient, wird erweitert, um nicht nur eine laufende Simulation abbilden und beobachten zu können, sondern darüber hinaus in der Lage zu sein, in jedem Schritt der Arbeit mit VNUML eingesetzt zu werden. Das erweiterte Programm gestattet sowohl die Erstellung der VNUML-Topologiedatei, als auch das Starten und Steuern der Simulation. Damit werden der lange Kommandozeilenaufruf, sowie das Editieren der Konfigurationsdatei, durch einfach zu benutzende Funktionen in einer grafischen Oberfläche (GUI) ersetzt. Zur schnellen Kontrolle der vollen Funktionsfähigkeit der gestarteten Simulation sind keine weiteren Eingaben oder Konfigurationen nötig. Ebenso kann eine differenzierte Beobachtung verschiedener Netzwerkdienste während der Laufzeit der Simulation erfolgen. Die hierzu nötigen Werkzeuge sind im Paket Cheops für VNUML ebenfalls enthalten und speziell zur Anwendung mit VNUML-Simulationen vorkonfiguriert.

Inhalt

1. Einleitung

1.1. Die Netzwerksimulationssoftware VNUML

Das Programmpaket Virtual Network User Mode Linux (VNUML) [1] richtet sich an Anwender im Laborbetrieb an höheren Bildungsstätten. Die Entwickler der Software am Institut für Telematische-Systeme der Polytechnischen Universität Madrid (UPM) [2] sehen das Programmpaket primär als Werkzeug zur Einsatzerprobung neuer Netzwerkprotokolle, ursprünglich war das Programmpaket für die frühe Erprobung von IPV6 unter Linux gedacht.

Abb.1: Logo des VNUML Projektes an der Polytechnischen Universität Madrid

Von einer reinen Simulationsumgebung unterscheidet sich VNUML hierbei dadurch, dass das Netzwerksubsystem komplett vorhanden ist und auf einem vollständigen Linux-Kernel ausgeführt wird. In einer sonst üblichen reinen Simulation werden von beidem meist nur bestimmte Teile einbezogen und ausgeführt. VNUML gewährleistet hier also einen vollständigen Ansatz, da alle auf einem Linux-System zum Einsatz kommenden Prozesse mit berücksichtigt werden können.

Das VNUML System bedient sich hierbei der Programmumgebung User Mode Linux [3], die es erlaubt, Linux Systeme virtuell auf einem Linux Gastgeber-System im Benutzermodus ausführen zu können. Die Besonderheit liegt hier darin, dass die virtuelle Umgebung nur im Benutzermodus läuft, sie beinhaltet keine Systemprogramme oder Dienste. Hierdurch ist der Betrieb in Umgebungen möglich, in denen dem Benutzer kein privilegierter Zugang gewährt werden kann, insbesondere in allgemein benutzbaren Computerräumen (Computerpools), die an solchen Einrichtungen gemeinhin zur Verfügung stehen.

In der Arbeitsgruppe Rechnernetze der Universität Koblenz-Landau am Standort Koblenz wird das Programmpaket VNUML [4] sowohl zur Anschauung von grundlegenden Netzwerkfunktionen und den dafür vorgesehenen Befehlen des Betriebssystems Linux in der Lehre eingesetzt, als auch zum Simulieren von lokalen Netzen, also solchen Netzen, die innerhalb von Autonomen Systemen vorzufinden sind und in welchen Routing Protokolle für Intra-Domain-Routing [5] zum Einsatz kommen.

Zum Einsatz kommt hier insbesondere der von oben genannter Arbeitsgruppe entwickelte Routing Algorithmus „Routing Information Protocol with Metric-based Topology Investigation“ (RMTI) [6], welcher das verbreitete Protokoll RIPv2 [7] erweitert und insbesondere den Umgang mit dem als „Counting to Infinity“ [8] bekannten Problem erheblich verbessert. Die Ergebnisse, die dieser neue Algorithmus erzielt, können in der VNUML-Umgebung auf ver-

schiedene Größen, wie etwa der Konvergenzzeit hin, untersucht werden und darüber hinaus ist auch der direkte Vergleich mit anderen Routing-Protokollen möglich.

1.2. Das Programmpaket Cheops für VNUML - Motivation

Zur Erstellung und Kontrolle von VNUML-basierten Simulationen ist das Programmpaket Cheops für VNUML entwickelt worden. Es beinhaltet, mit dem Programm NAGIOS [24], ein am Markt verbreitetes System zur Netzwerküberwachung[1] sowie eine angepasste Version des Open Source Programms Cheops-NG von Brent Priddy, welches sich im Besonderen zur Anwendung auf VNUML-simulierte Netzwerke eignet. Dieses Programm bildet den Hauptteil der Arbeit. Es wurde aus mehreren zur Verfügung stehenden Netzwerküberwachungsprogrammen ausgewählt. Auch die anderen untersuchten Programme werden später kurz vorgestellt.

Die vorgenommenen Änderungen dienen der Steuerung der VNUML-Simulation vom Netzwerküberwachungsprogramm aus. Anschließend wurde auch die Möglichkeit der Erstellung von VNUML-Simulationen implementiert. Das Programm dient so in jeder Simulationsphase, der Unterstützung bei der Arbeit mit VNUML-Simulationen.

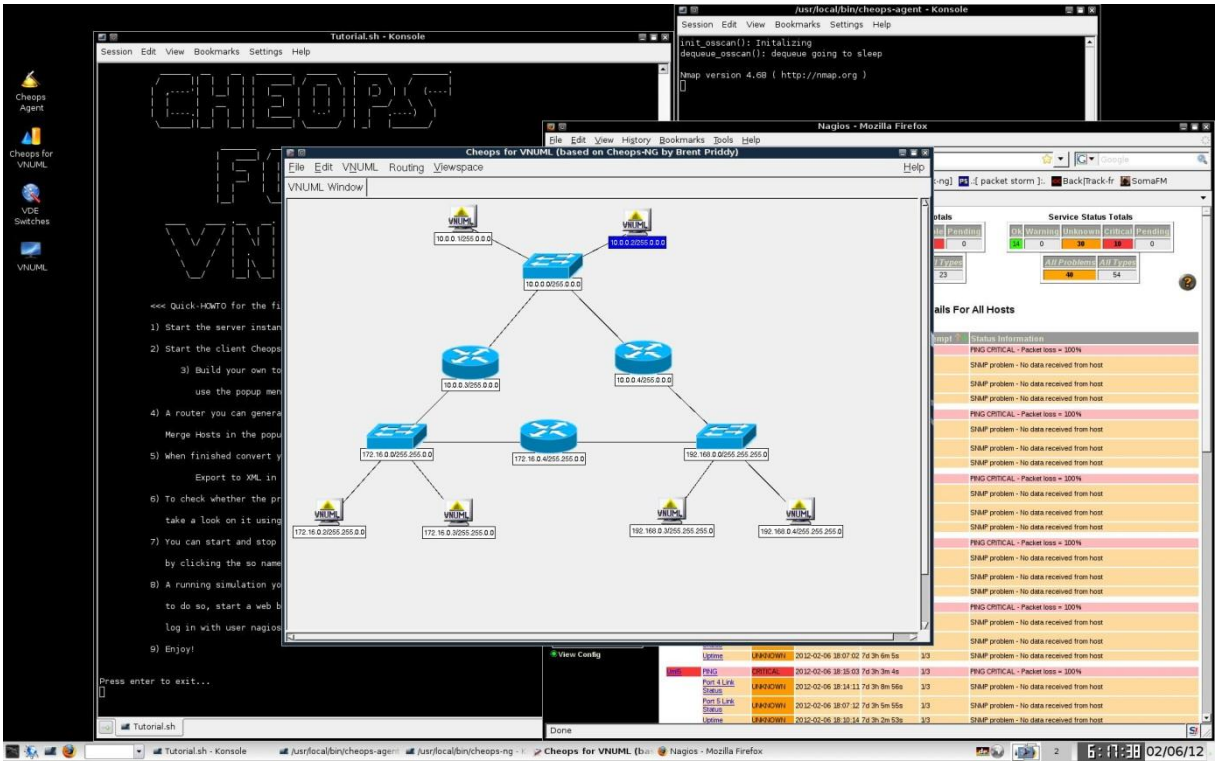


Abb. 2: Cheops für VNUML bei der Simulation einer Netzwerktopologie, im Hintergrund sind alle Komponenten des vollständigen Cheops für VNUML Programmsystems sichtbar

1: später auch mit dem gebräuchlichen englischen Begriff „Network Monitoring“ bezeichnet.

1.3. Die Netzwerküberwachungssoftware Cheops

Die erste Fassung der Software Cheops stammt von Mark Spencer aus dem Jahr 2001 [9]. Dieses Programm war schon mit allen Eigenschaften ausgestattet, die Cheops in seiner weiteren Entwicklung beibehielt und verbesserte. Von Mark Spencer stammte auch das Mantra [10] der Cheops-Software, nämlich das „Schweizer Taschenmesser für Netzwerke“ [33] zu sein. Hierbei stellte Spencer vor allem heraus, dass im Gegensatz zu den meisten am Markt verbreiteten Lösungen, von denen später eine repräsentative Auswahl vorgestellt wird, bei denen jeweils ein erheblicher Einrichtungszeitaufwand besteht, um die vorhandenen Netzwerkgeräte der jeweiligen Netzwerküberwachungssoftware bekannt zu machen, dieses bei der Software Cheops durch die integrierte automatische Erkennung der Netzwerkgeräte entfällt. Damit kann die Einsatzweise der Cheops Software als eine direktere angesehen werden, das Tool ist sozusagen „ad hoc“ einsetzbar, auch ganz ohne Kenntnis der gegebenen Netzwerkinfrastruktur.
Mark Spencer war zur Zeit der Entwicklung des Programms Cheops bei der Firma Adtran Inc. im Bereich Netzwerkmanagement eingestellt. Die Firma ist Betreiber-Ausrüster[2] im Telekommunikationsbereich und beschäftigt sich sowohl mit der Weiterentwicklung von Glasfaserstandards als auch der von DSL-Techniken, zurzeit insbesondere mit der Arbeit am VDSL-2-Standard. Mark Spencer wurde bei der Entwicklung des Programms von seinem früheren Arbeitgeber unterstützt, bot die Software allerdings auf einer eigenen Webseite an. Diese Webseite ist inzwischen leider nicht mehr erreichbar, Quellen und installierbare Pakete der originalen Cheops Software der Versionen bis 0.61 sind noch in alten Linux Distributionen [9] oder in Archiven von FTP-Servern auffindbar.

1.4. Die Architektur des Programms Cheops-NG

Eine Neuauflage erfuhr die Software zuletzt in den Jahren 2003 bis 2005 durch Brent Priddy. Dieser schrieb das bis dato monolithische Programm in eine Client-Server Architektur um. Programmiersprache blieb weiterhin Standard C, die Oberfläche wurde weiterhin mit Hilfe der Bibliothek GTK implementiert. Diese neue Version, welche von 2003 bis 2005 in den Versionen 0.1.11 bis 0.2.3 veröffentlicht worden ist, wurde von Priddy als Cheops-NG bezeichnet [11]. Cheops-NG benötigt das Vorhandensein der Software NMAP [18] als installiertes Binary-Paket, in der Version von Mark Spencer wurde der benötigte Quellcode von NMAP noch dem eigenen Quellcode beigegeben. Der erste Teil der Software besteht aus dem, von Priddy als „Cheops-NG Agent“ bezeichneten Server, der auf einem beliebigen geeigneten Linux System laufen kann und sowohl Aufgaben zur Netzwerkerkennung durchführt, als auch eingehende Rückmeldungen annimmt und aufzeichnet. Dieses Programm ist ein Kommandozeilenprogramm und eignet sich dazu, unter Linux als sogenannter „daemon“ zu laufen. Also als Programm, welches üblicherweise beim Systemstart oder automatisch gestartet wird und dann ohne weiteres Zutun selbständig weiterläuft, wie dies bei einem Betriebssystemdienst der Fall ist, etwa der Druckerwarteschlange.

2: Oft mit dem gängigen englischen Begriff „Carrier Supplier“ bezeichnet

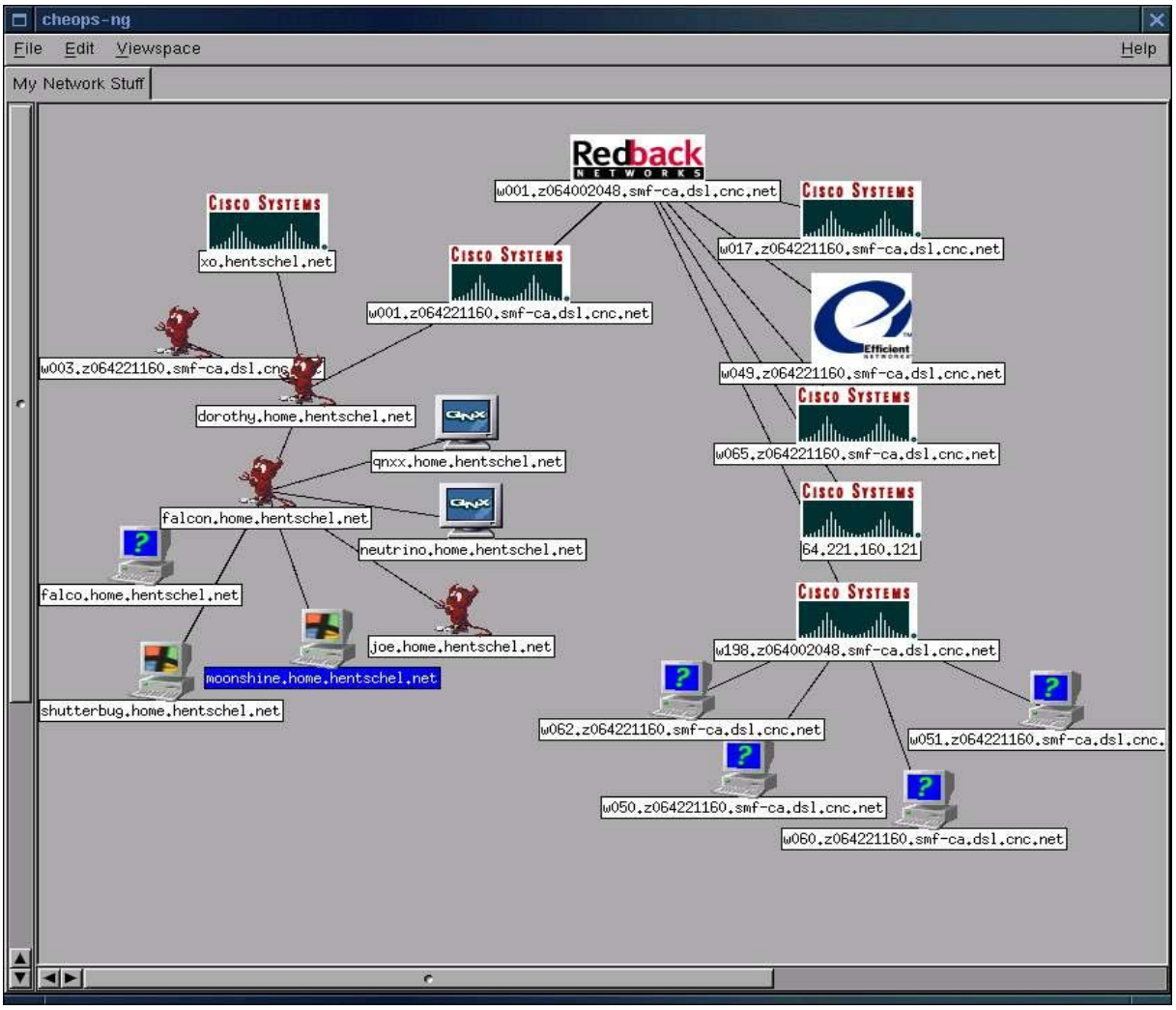


Abb. 3: Cheops-NG zeigt ein erkundetes Netzwerk an.

Als zweiten Teil stellt Cheops-NG einen Clienten mit grafischer Benutzeroberfläche zur Verfügung. Aufgabe der Benutzeroberfläche ist es, dem Anwender ein Werkzeug bereitzustellen, mit welchem er Aufträge zur Netzwerkerkundung erstellen kann, die dann an das Server-Programm „Cheops-NG Agent“ zugeteilt werden. Ebenso werden schon empfangene Ergebnisse vom Server-Programm abgerufen und dargestellt. Natürlich ist es mit dieser Architektur möglich, dass die Server-Instanz und der Client auf verschiedenen Computern ausgeführt werden.

Der Vorteil dieser Architektur liegt weiterhin darin, dass eine Entkopplung von Auftragserstellung und Weitergabe zur Abwicklung der eingehenden Ergebnisse stattfindet. Da Netzwerkoperationen und insbesondere die Erkundung eines Netzwerkes, oft mit langen Verzögerungen einhergehen, ist die Abtrennung der abwickelnden Einheit in diesem Szenario sehr sinnvoll. Der Client arbeitet zu jedem Zeitpunkt mit dem ihm vorliegenden Daten, es kommt zu keinen Verzögerungen zwischen Anfrage und Eingang von neuen Daten. Signalisiert der Agent das Vorliegen neuer Daten, werden diese in eine, das erkannte Netzwerk wiederspiegelnde, Datenstruktur übernommen und dargestellt. Auf der Agenten Seite ermöglicht es das streng sequentielle Abarbeiten der Erkundungsaufträge, denn es macht hierbei nur Sinn,

eine begrenzte Anzahl von Geräten im Netzwerk abzufragen: Bei einer zu hohen Anzahl von Abfragen behindert der so erzeugte Netzwerkverkehr die Rückantworten und ausgehenden Abfragen und die sehr große Anzahl von offenen Sockets [12] bedingen eine zu große Verschlechterung der Systemgeschwindigkeit des Computers. Daher werden immer nur eine bestimmte Anzahl von Abfragen simultan ausgeführt und die weiteren anhängigen Abfragen solange aufbewahrt.

Um diesen Mechanismus richtig bewerten zu können, gilt es zu beachten, dass die Abfrage großer Netzwerk-Adressbereiche unter Umständen eine sehr große Anzahl von IP-Adressen umfasst, auch wenn die später gefundene Anzahl von antwortenden Netzwerkgeräten deutlich kleiner sein kann. Liegt zum Beispiel gar keine Kenntnis vom benutzten Netzwerkbereich eines lokalen Netzwerks vor und wird, was natürlich keine sinnvolle Lösung des Problems darstellt, der gesamte Adressraum von IPv4 durchsucht, so stehen sehr viele Aufträge zur Abarbeitung an, die niemals eine Rückmeldung erbringen werden. Auch wenn die benutzten Timeouts des Cheops-NG Agenten hier natürlich deutlich geringer sind, als die sonst üblichen Timeouts bei der Nichtauffindung eines Hosts, so ist dennoch von einer großen Anzahl anhängiger Abfragen ausgehen. Als Zahlenbeispiel: Es ist sicherlich unsinnig alle 4.294.967.296 möglichen Hosts des IPv4 Adressraums abzufragen, um 20 lokale Hosts aufzufinden. Sinnvoll wäre es hier vielmehr, nur die bekannten, für die lokale Benutzung reservierten Adressbereiche [13] und diese nach Möglichkeit in Stichproben abzuarbeiten.

Zusammenfassend ist zu sagen, dass das Programm Cheops-NG eine Network Monitoring Software mit einem besonderen, gegenüber anderen Softwaresystemen dieses Bereichs abweichenden, Funktionsumfang darstellt. Verglichen mit den später kurz vorgestellten Programmen, stellt Cheops-NG nicht nur die üblichen Funktionen zur Überwachung von Netzwerkgeräten zur Verfügung, sondern legt sein Hauptgewicht vielmehr auf die automatische Erkundung von Netzwerkbereichen, oft bezeichnet als „Autodiscovery“, außerdem auf die Erkennung des ausgeführten Betriebssystems und die grafische Darstellung.

Cheops-NG bedient sich hier verschiedener Hilfsmittel, wie dem populären Portscanner NMAP [vgl. Kapitel 4.2.] oder verschiedener, unter Open Source stehender Routinen, die mit sogenannten Raw Sockets dazu in der Lage sind, nicht nur entfernte Rechner, sondern auch Netzwerktopologien als solche erkennen zu können. Mit Raw Sockets wird dabei, die weniger oft benutzte Teilgruppe der Standard-Netzwerk-Programmierschnittstelle Sockets bezeichnet, welche weder TCP noch UDP als Protokoll benutzt, sondern lediglich den Zugriff auf die vom ICMP Protokoll beschriebenen Funktionen ermöglicht [14].

Das Programmpaket Cheops-NG wurde im Laufe dieser Arbeit erweitert, um speziell auf die Anforderungen beim Monitoring von VNUML-simulierten Netzen eingehen zu können und darüber hinaus Steuerungseinrichtungen und weitere Funktionen für den Umgang mit der Simulationsumgebung VNUML bieten zu können. Die erweiterte Fassung trägt den Namen Cheops für VNUML und wird im nächsten Kapitel genauer vorgestellt.

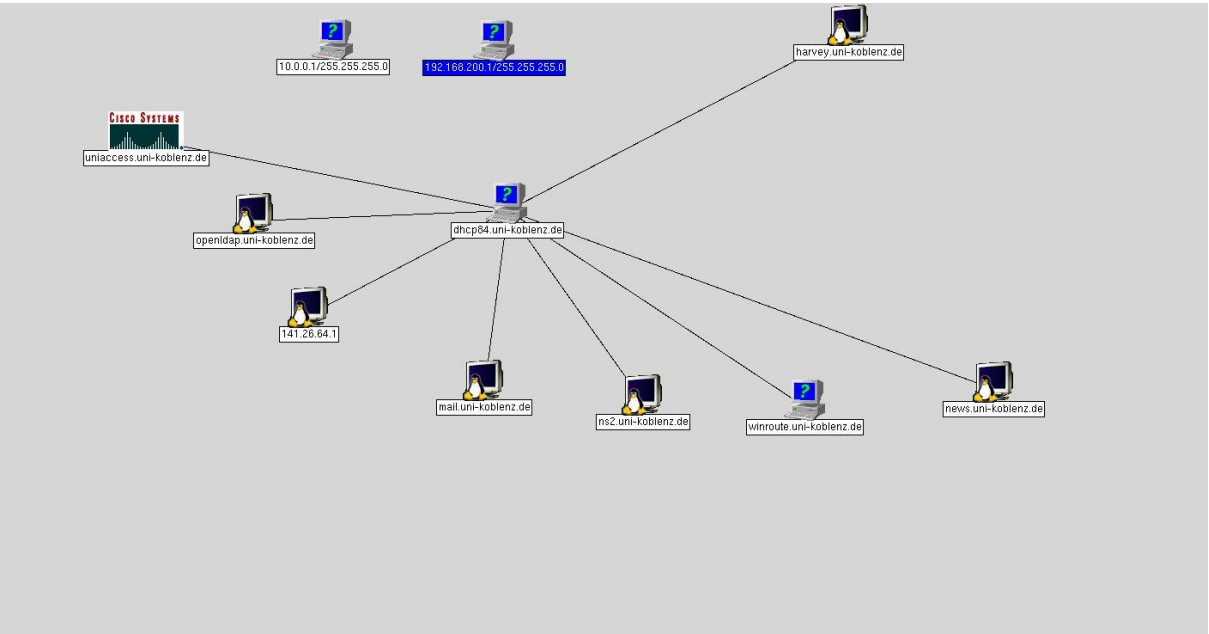


Abb. 4: Cheops-NG nach der Erkundung der ersten 10 IP-Adressen des Adressbereichs der Universität Koblenz.

1.5. Die Funktionsweise von Cheops für VNUML

Die Funktionsweise des Programms Cheops für VNUML soll nun beschrieben werden. Das Paradigma der Benutzung sieht vor, Netzwerkgeräte zu definieren, die sodann auf der Oberfläche dargestellt werden. Dabei werden die Netzwerkgeräte mit Hilfe von IP-Adresse und Subnetzmaske vom Benutzer eingegeben. Auf diese Weise wird ein virtuelles Netzwerkgerät definiert. Diese sind Grundbestandteil der zur Simulation mit VNUML aufgebauten Netzwerke.

Die zweite unterstützte Möglichkeit zur Definition von Netzwerkgeräten besteht darin, diese über Erkundungsmaßnahmen auffinden zu lassen. Die gefundenen Objekte repräsentieren real vorhandene Netzwerkgeräte des angeschlossenen physikalischen Netzwerks.

Sind mit Hilfe dieser beiden Möglichkeiten erst einmal Netzwerkgeräte hinzugefügt worden, so werden diese im Weiteren von Cheops-NG als gleichberechtigt angesehen und nach einer jeden Zufügung eines Gerätes, gleichgültig ob durch manuelle Eingabe oder durch Erkundung eines realen Netzwerks, wird das Cheops-System versuchen, diese mit den schon definierten Geräten zu verbinden.

Die nötigen, beziehungsweise möglichen, Netzwerkverbindungen zwischen den Geräten werden von Cheops-NG jeweils, anhand der angegebenen oder ermittelten IP-Adressen, berechnet und dargestellt. Hierbei ist natürlich darauf zu achten, dass Netzwerkgeräte mit geeigneten IP-Adressen und Subnetzbereichen versehen werden, da natürlich Netze, welche vom Benutzer versehentlich so gewählt wurden, dass sie in verschiedenen Subnetzbereichen zu liegen kommen, von Cheops für VNUML nicht verbunden dargestellt werden können. Dieses Problem stellt sich als solches vor allem dann dar, wenn erkannte reale Netzwerkberei-

che mit virtuellen Netzwerkbereichen gemeinsam in einer Topologie dargestellt werden sollen.

Wird ein Netzwerkgerät manuell definiert, so stellt es erst einmal einen Host mit nur einer Netzwerkanbindung dar. Soll nun ein Router definiert werden, so wird erst einmal temporär ein Host als Objekt mit der IP-Adresse für die zweite Netzwerkschnittstelle des Routers definiert. Dieser zweite Host wird mit einer Verschmelzungsfunktion dem ersten Host hinzugefügt. In diesem Arbeitsschritt entsteht nach dem Cheops Paradigma der Router, der in diesem Fall über zwei Netzwerkschnittstellen verfügt, nämlich genau die zwei Schnittstellen der verschmolzenen Hosts.

Wird nun ein weiteres Objekt anhand seiner IP-Adresse hinzugefügt und liegt es innerhalb eines Subnetzes zusammen mit einer der vorhergehend definierten Schnittstellen, so zeichnet das Cheops für VNUML-System automatisch das verbindende Netz zwischen den entsprechenden Hosts oder Routern ein.

Zur Darstellung ist zu sagen, dass im Programm Cheops-NG generische Symbole für Hosts verwendet werden und die Netze ohne Bezeichnung zwischen den erstellten oder erkundeten Hosts eingezeichnet werden. Bei den erkundeten realen Hosts kommen Symbole zum Einsatz, die das jeweilige Betriebssystem des entfernten Hosts kennzeichnen. Dieses wird im Zuge der Erkundung der entfernten Hosts durch eine spezielle Routine des eingebundenen Programms NMAP erkannt und vom Programm Cheops-NG ausgewertet.

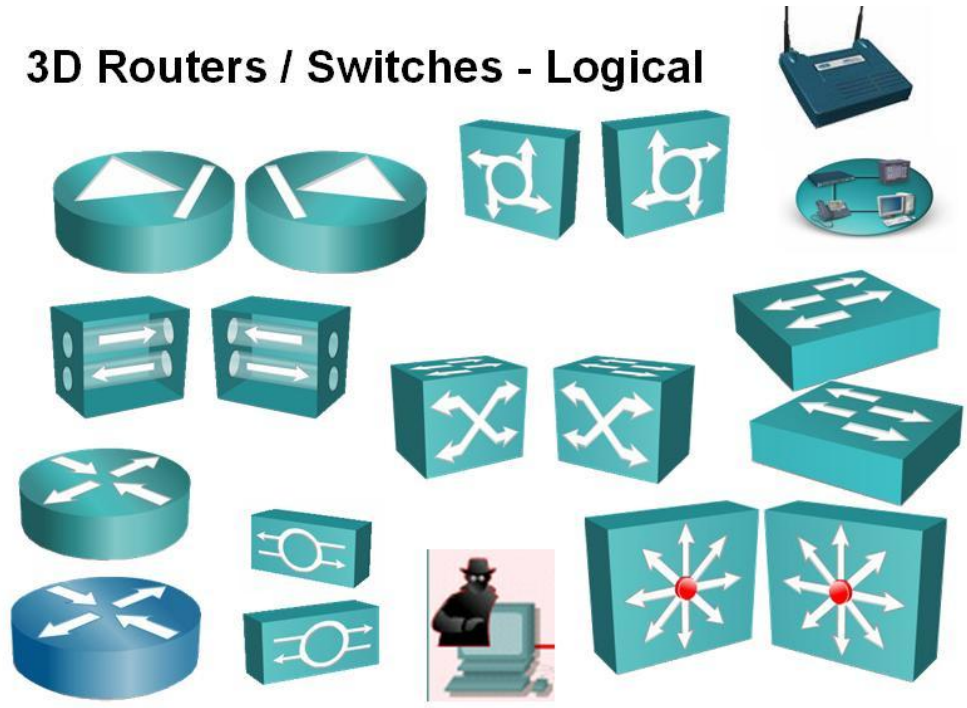


Abb. 5: Darstellung der aktuellen Norm-Symbole der Firma Cisco Systems, 3D-Ansicht

In der erweiterten Fassung Cheops für VNUML kommen genormte Netzwerksymbole der Firma Cisco Systems zum Einsatz [vgl. Abb. 5]. Die manuell definierten Hosts sind mit einer Kennzeichnung „VNUML“ versehen, um sie als virtuelle Hosts erkennbar zu machen. Automatisch erkundete Hosts werden weiterhin mit Kennzeichnung des vorgefundenen Betriebssystems dargestellt. Router werden mit dem dafür vorgesehenen Symbol in der Cisco Systems-eigenen Nomenklatur für Netzwerksymbole dargestellt. Zusätzlich werden in der erweiterten Fassung zur besseren Übersicht die verbindenden Netze durch Cisco Systems genormte Switch-Symbole dargestellt. Wenngleich Switches nicht in der Simulation betrachtet werden sollen, sind die Switch-Symbole dem Verständnis förderlich, um einen sichtbaren Verteiler-Knoten zu haben, an dem die zu einem bestimmten Netzwerk gehörenden Geräte angezeichnet sind. Ebenso wird die Netzwerkadresse, auch bezeichnet als Netzwerk-ID, des verbindenden Netzwerks am Switch angetragen, um dieses schnell erkennbar zu machen.

Hier soll angemerkt werden, dass bei der Erkennung von physikalischen Netzwerken zwar Switches als solche erkannt werden können, da das Cheops für VNUML-System aber Funktionen auf Layer-3 des Netzwerkschichtenmodells darstellen soll, wird auf jede Funktionalität bezüglich darunterliegender Schichten verzichtet. Sollte ein Switch anhand seiner Management-Schnittstelle erkannt werden, so deutet zumindest das identifizierte Betriebssystem auf diese Tatsache hin. So werden etwa Switches der Firma Cisco Systems als Hosts mit dem Betriebssystem Cisco IOS dargestellt. Werden dann im weiteren Erkundungsprozess keine weiteren, von diesem Gerät abgehenden Schnittstellen erkannt, so kann davon ausgegangen werden, dass es sich nicht um einen Router - der zur weiteren Betrachtung von Interesse wäre, sondern eben um einen Switch oder ein anderes Gerät der Firma Cisco Systems, etwa eines zum Netzwerkmanagement im weiteren Sinne, handeln muss.

1.6. Die Erkennung von Netzwerkgeräten

Zur Erkennung eines Netzwerkgerätes nutzt Cheops für VNUML das Programm NMAP als installiertes Paket, dabei werden in den Erkundungsaufträgen die Funktionen aus den entsprechenden NMAP-Bibliotheken benutzt und vom Cheops für VNUML-Programm aufgerufen. Im einfachsten Fall wird NMAP die Funktion ICMP Ping verwenden, da diese jedoch auf vielen Routern aus Sicherheitsgründen und zur Traffic-Begrenzung abgeschaltet ist, werden auch andere Möglichkeiten genutzt um eine Antwort von einem Netzwerkgerät zu erhalten. In der Standardeinstellung wird jeder IP-Adresse ein ICMP ECHO-REQUEST sowie ein TCP ACK Paket an Port 80 zugesandt, alternativ kann das TCP ACK Paket auch an Port 135 gesendet werden. Sollte ICMP Ping auf dem entfernten Gerät aktiviert sein, so wird diese Antwort als Lebenszeichen des Gerätes angesehen. Sollte ICMP Ping deaktiviert oder der Port geschlossen sein, so würde ein Betriebssystem mit einem, nicht in besonderem Maße geschützten TCP/IP-Stack [15] mit einem RST und einer Fensternummer antworten, in aller Regel mit „RST WIN=0“.

Die Möglichkeit ein TCP SYN auf Port 135 zu senden, um auch die besonders geschützte Rechner wie Firewalls erkennen zu können, wird von Cheops für VNUML in der Standardaus-

führung nicht angewendet, wohl aber ist es möglich, im Quellcode die Einstellung für den Funktionsaufruf von NMAP dahingehend anzupassen. Hierbei würde ein TCP SYN auf Port 135 gesendet, was vom entfernten Rechner mit einem SYN ACK und einer Sequenznummer SEQ sowie einer neuen Fensternummer WIN beantwortet würde. Der erkundende Rechner sendet nun sein RST mit seiner Fensternummer WIN. Da es sich bei einer Erkundung per TCP SYN „nur“ um einen TCP Handshake handelt, kommt hierbei der geringstmögliche Traffic zustande - Ebenso hinterlässt die Suche keine Spuren, da der korrekt abgeschlossene Handshake in aller Regel von keiner Firewall als besonderes Ereignis aufgezeichnet wird - im Gegensatz zu einem abgebrochenen Handshake oder bestimmter ICMP Nachrichten die ansonsten verwendet werden könnten.

Im nächsten Schritt der Verarbeitung, wird den als „lebendig“[3] erkannten Netzwerkgeräten eine Auswahl an Paketen geschickt, um nähere Daten über deren Betriebssystem und Eigenschaften zu ermitteln. Da hierin eine der Kernkompetenzen der Software NMAP besteht, ist dies eine größere Ansammlung von etwa 50 Anfragen pro Host in einer bestimmten Sequenz, wobei manche Anfragen parallel und einige hintereinander ausgeführt werden müssen. Hintergrund hiervon ist, dass es sich herausgestellt hat, dass verschiedene Betriebssysteme unterschiedlich mit bestimmten Anfragen umgehen und dadurch unterscheidbar werden. Diese Funktion wird gemeinhin als „OS Fingerprinting“[4] bezeichnet. Genauer handelt es sich um ein TCP/IP-Stack-Fingerprinting. Es werden, um eine deutsche Umschreibung zu versuchen, Fingerabdrücke des entfernten Systems erstellt. Analog zu dieser Übersetzung sucht NMAP die Ergebnisse in einer aktuell über 1000 Einträge umfassenden Fingerabdruck-Datenbank für die unterschiedlichen TCP/IP-Stacks von Betriebssystemen.

Als Beispiel für die verschiedenen signifikanten Antworten, die ausgewertet werden können, soll hier die Vorhersagbarkeit von TCP-Sequenznummern angeführt werden. Bei frühen Betriebssystemen wurde gerade auf die „Nicht-Vorhersagbarkeit“ nur wenig Wert gelegt, dies führte dazu, dass TCP-Datenverkehr kompromittierbar wurde, durch Angriffe wie „Stealthing“ oder „Man-in-the-middle“ [vgl. Kapitel 4.4]. Dieses Problem betraf vor allem die alten Versionen von Microsoft Windows und Apple Mac OS, bei Windows etwa bis zur Programmversion Windows 2000.

Bei modernen Betriebssystemen wird versucht, die Vorhersagbarkeit zu verhindern. Hierzu werden jedoch Algorithmen benutzt, die sich in Ihren Auswirkungen rückwirkend wiederum einem Betriebssystem oder einer Betriebssystemversion fest zuordnen lassen – wenngleich die „Nicht-Vorhersagbarkeit“ mit unterschiedlicher Qualität gegeben ist. Eine ungefähre Vorhersage dieser Qualität in Form einer Punkte-Bewertung wird von NMAP selbst, nach der Detektion des Betriebssystems, im ausführlichen Modus dieses Programms, ausgegeben.

3: meist mit dem englischen Begriff „alive“ bezeichnet

4: OS-Fingerprinting von engl. Operating System für Betriebssystem und engl. Fingerprinting für das Abnehmen von Fingerabdrücken

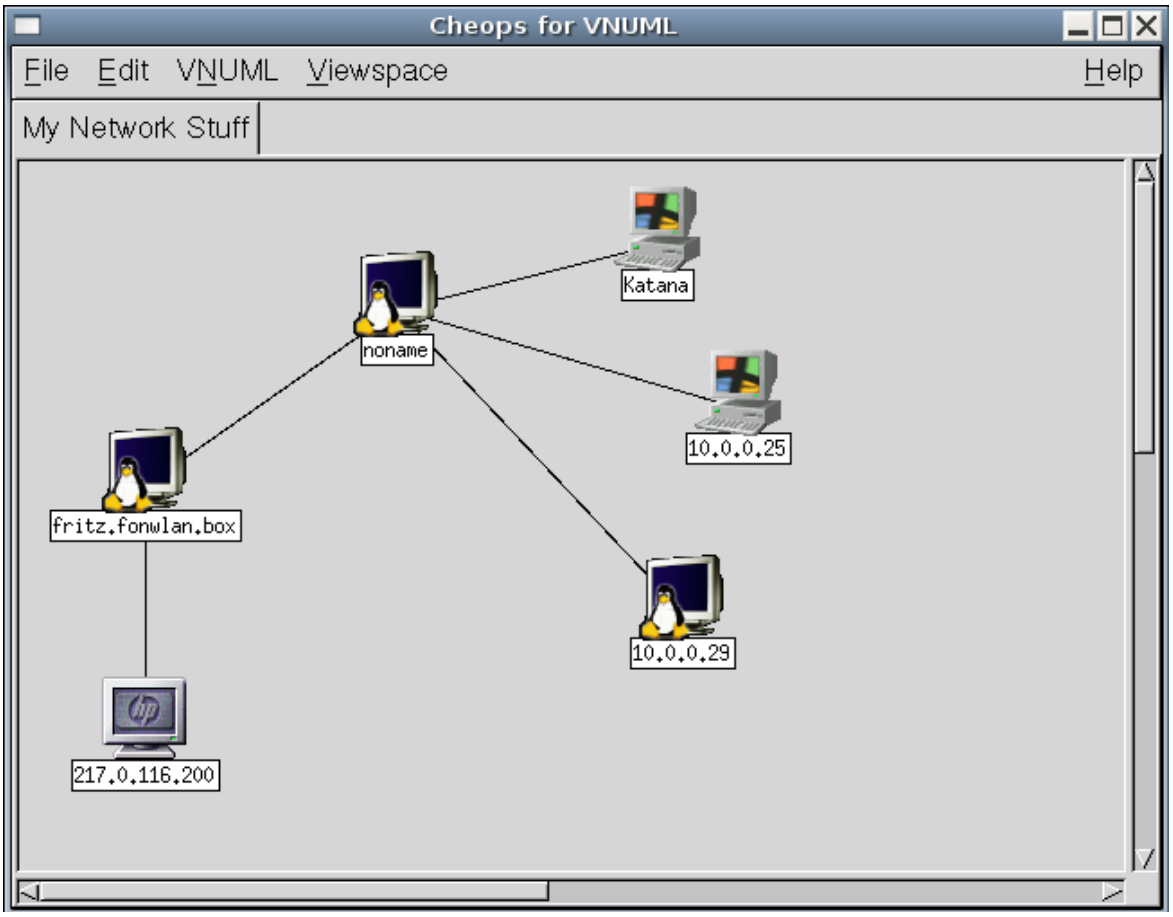


Abb. 6: Erkannte Betriebssysteme in einem Heimnetzwerk, zu erkennen sind Linux- und Windows-PC, eine unter Linux operierende Appliance im Heimnetzwerk (Fritz!Box der Firma AVM) und eine von der Firma Hewlett Packard hergestellte Appliance des Netzbetreibers

2. Einführung in die Programmbenutzung

2.1. Benutzung der Linux-Distribution Backtrack

Es folgt eine kurze Einführung in die praktische Benutzung des Programmpakets Cheops für VNUML. Der erste Teil besteht aus der Beschreibung des Starts des Cheops für VNUML-beherbergenden Betriebssystems und einem kurzen Kennenlernen der Linux Sicherheits-Distribution Backtrack. Die Motivation der Verknüpfung des Programms Cheops für VNUML und der Distribution Backtrack bestand dabei darin, dass Backtrack sowohl Programme mitbringt, die für die Funktion von Cheops für VNUML erforderlich sind, zu nennen ist hier insbesondere das Programm NMAP, als auch in dem Umstand, dass Backtrack viele Programme enthält, die als Einzelprogramme Aufgaben erfüllen, die auch in Cheops für VNUML im Funktionsumfang enthalten sind. So wird sowohl eine Kontrolle der mit Cheops für VNUML erzielten Ergebnisse, als auch eine sinnvolle Erweiterung der Informationssuche ermöglicht. Weitere Synergien werden im Kapitel über die Distribution Backtrack herausgearbeitet.

Wird die Linux-Sicherheits-Distribution Backtrack gestartet, so wird zuerst der Boot Manager Grub-2 ausgeführt. Hier gibt es, wie bei den meisten Linux Distributionen, eine Auswahl, die dazu dient, bestimmte Fehlerzustände beim Startvorgang von Linux zu vermeiden oder bestimmte Versionen von Kernel oder Hardwareunterstützung auszuwählen. Dies sind entweder Probleme beim Umgang mit dem Motherboard des PC und dessen BIOS, also meist eine Umgehung der automatischen Zuweisung von Hardware-Interrupts an die Geräte an den verschiedenen Bussen oder Probleme bei der Steuerung von Geräten und Stromspareinrichtungen des BIOS über ACPI. Als zweite Maßnahme steht in aller Regel eine Möglichkeit zur Umgehung der grafischen Benutzeranmeldung bei Problemen mit der Erkennung oder beim Wechsel der Grafikkarte des PC zur Verfügung.

Bei der Distribution Backtrack steht zudem eine weitere wichtige Auswahlmöglichkeit zur Verfügung, auf die auch im Kapitel 4 tiefer eingegangen wird. Bei dieser wird vor dem Start des Betriebssystems entschieden, ob Änderungen, die bei der Benutzung des Systems vorgenommen werden, dauerhaft gespeichert werden sollen oder ob ein sogenannter „LIVE“-Betrieb, ohne die Möglichkeit Änderungen vorzunehmen, ausgeführt werden soll. Die erste Auswahl muss bei Installation der Distribution durch eine für den entsprechenden Computer geeignete Methode modifiziert werden. Dabei steht dem Installateur sowohl die Auswahl einer eigenen Partition für Änderungen, als auch die Benutzung einer Änderungsdatei, die dann selbst ein XFS-Dateisystem enthält, zur Verfügung. Da diese Einrichtungen auch auf einem USB-Stick liegen können, ist es generell sinnvoll, auch auf einem Wechselmedium die Speicherung der Änderungen anzubieten. Auch eine LIVE-DVD, kann so auf einen zusätzlichen USB-Stick Änderungen speichern und zu einem vollwertigen Arbeitsmedium werden.

Die möglichen Auswahlmöglichkeiten heißen „BT4 Using Memory ONLY“ für die „LIVE“-Version und „BT4 Persistent Changes“ für die Version mit abgespeicherten Änderungen.

Benutzt der Anwender ein Wechselmedium und ist sich über das gemachte Angebot der Speicherung seiner Änderungen nicht im Klaren, so kann er durch Drücken der Tab-Taste einen Klartext der entsprechenden Startbefehl-Zeile erhalten. Er kann somit nachschauen, auf welchem Datenträger die Änderungen gespeichert werden.

In der zu dieser Arbeit analog aufgebauten Installation auf einem Dell Optiplex PC wird als Medium aus Performance-Gründen eine Festplatte mit EXT2-Dateisystem benutzt. Auf dem mit dieser Arbeit für interessierte Anwender abgegebenen USB-Stick, ist nur ein FAT32-Dateisystem eingerichtet, hier wird eine einzelne Änderungsdatei mit einem darin enthaltenen XFS-Dateisystem benutzt.

In der Implementation auf diesen beiden Referenzgeräten, kommt nicht mehr die Auswahlmöglichkeit zum Einsatz, die Backtrack Distribution ganz ohne die Cheops für VNUML-Erweiterung zu starten. Sollte dies jedoch trotzdem gewünscht sein, so kann wie oben erwähnt mit der Tab-Taste die Startzeile ausführlich angezeigt werden. Es wäre dann lediglich der Parameter „load=cheops_sources“ zur Umgehung des Ladens der Programmiersprache GNU C sowie der Programmierumgebung KDEVELOP und der Quelldateien des Cheops für VNUML-Pakets, zu entfernen. Analog wäre die Vorgehensweise mit dem Parameter „load=cheops_changes“ zur Umgehung des Ladens von Cheops für VNUML Ausführungsdateien, Bibliotheken und Einstellungsdateien, sollte dies gewünscht sein.

Ist eine Startversion ausgewählt worden, so erfolgt der normale Linux-Start. Die Distribution Backtrack baut seit der Version 4 auf einem Ubuntu-Linux auf [vgl. Kapitel 4]. Ist das Linux gestartet, so erscheint ein Hilfetext, sich mit den Standard-Benutzerdaten der Backtrack Distribution anzumelden. Nach der erfolgreichen Anmeldung wird ein Hilfetext zu weiteren möglichen Vorgehensweisen ausgegeben, hier sollte mit Eingabe von „startx“ die KDE-basierte Oberfläche gestartet werden. Des Weiteren stehen auch Auswahlen für eine besonders ressourcensparende Oberfläche sowie zur Arbeit von der Konsole aus zur Verfügung. Letztere Möglichkeit wird angeboten um die Anpassung an die vorhandene PC-Hardware zu vereinfachen. Die Referenzinstallation auf dem Dell Optiplex PC besitzt einen Drittanbieter-Grafiktreiber der Firma Nvidia. Es werden jedoch auch andere Grafiksysteme mit den weiteren, in der Backtrack Distribution vorhandenen X-Window-System-Treibern erkannt. Sollten Probleme bei der Inbetriebnahme der grafischen Benutzeroberfläche bestehen, so kann hierzu auch die Problembehandlung der Distribution Ubuntu etwa über die Webseite „ubuntuusers.com“ in Anspruch genommen werden.
Nach erfolgreichem Start des X-Windows Systems und dem anschließenden Laden des Fenstermanagers KDE, öffnet sich der Cheops für VNUML Desktop. Es öffnet sich ferner ein Hilfefenster „Erste Schritte“ - folgt der Benutzer diesen Anweisungen, so wird er beim Start des Programms Cheops für VNUML sowie bei der Erstellung einer ersten Anwendung angeleitet.
Im Startmenü sind, wie in der Backtrack Distribution üblich, die Backtrack eigenen Anwendungen nach bestimmten Sicherheits-Kategorien aufgeführt. Eine Einführung in die angebotenen Sicherheitspakete und Tools findet sich ebenfalls im Kapitel 4 zur Backtrack Distribution.

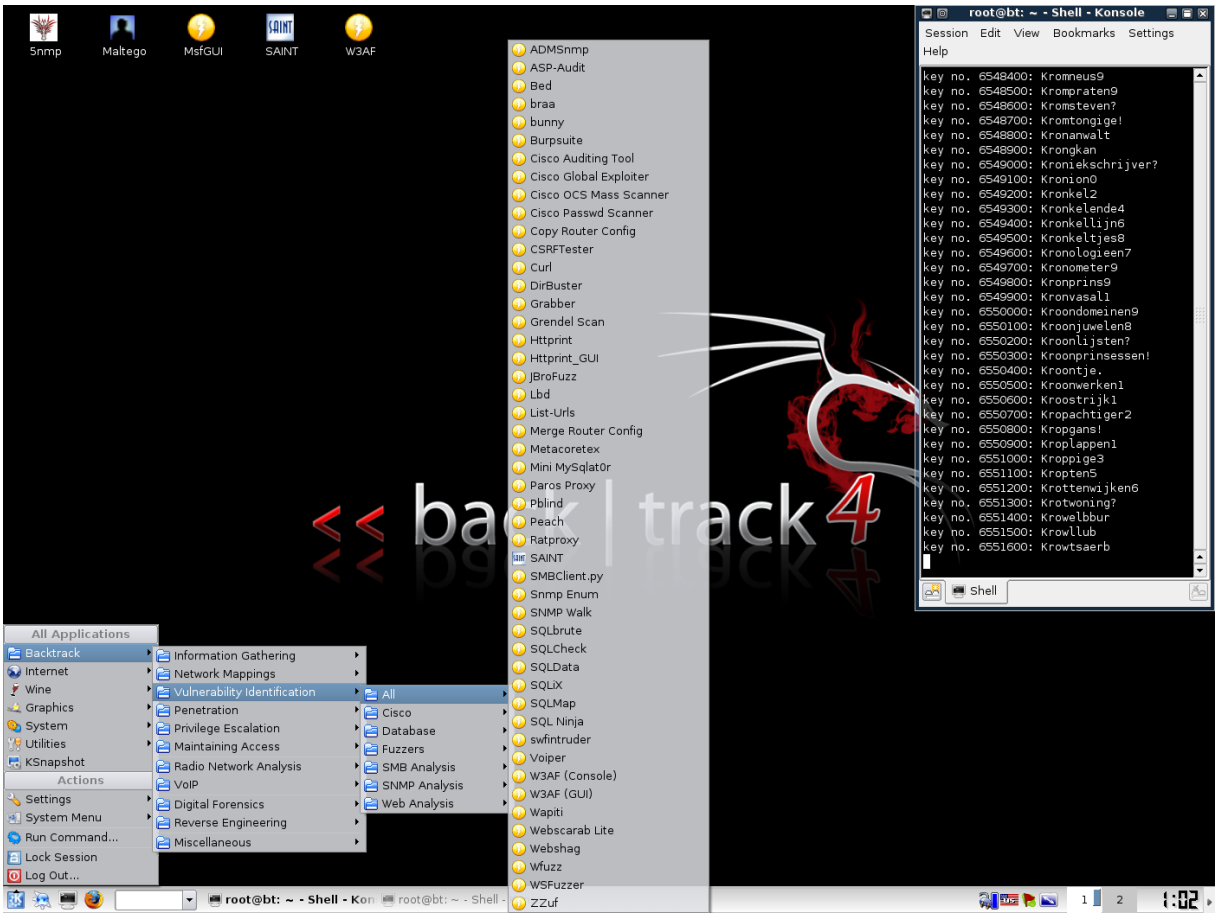


Abb. 7: Backtrack 4 – Menü „Vulnerability Identification“ und die Ausgabe eines Wörterbuch-Angriffs auf einen passwortgeschützten Bereich

2.2. Benutzung von Cheops für VNUML

Es folgt eine Beschreibung zur Benutzung des Programmsystems Cheops für VNUML. Auf dem angepassten Desktop der Backtrack Distribution befinden sich alle, zur Benutzung des Cheops für VNUML-Systems relevanten Verknüpfungen. Die Verknüpfungen „VDE-Switches“ [31] und „VNUML“ stellen hierbei Konsolenverknüpfungen dar, um manuell auf benutzte VDE-Switches oder VNUML-Szenarien Einfluss zu nehmen. Insbesondere sind beide Verknüpfungen zur Fehlersuche gedacht, etwa zum manuellen Starten eines root-Dateisystems mit VNUML.

Folgt der Anwender nach dem Start von Backtrack der Einführung „Erste Schritte“, so wird zuerst eine Cheops für VNUML Server-Instanz gestartet. Obwohl genauso gut als Linux-Dienst[5] implementierbar, wird der Cheops Agent hier bewusst mit einem Fenster geöffnet. Anhand des Ausgabefensters lässt sich später leicht nachvollziehen, auf welche Weise umfangreiche Sequenzen zur Erkundung eines Netzwerks zeitversetzt an die entsprechenden IP-Adressen versendet werden. Ebenso kann sich der Benutzer ein Bild vom zeitverzögerten Eintreffen der Ergebnisse machen. Der Cheops Agent überprüft gleich zu Anfang die Verfügbarkeit des Portscanners NMAP.

5: unter dem Betriebssystem Linux mit dem englischen Begriff „daemon“ bezeichnet

Zu beachten ist hier, dass beim etwaigen Neustart des Cheops Agenten, die neu gestartete Instanz des Servers, eintreffende Ergebnisse aus zuvor geschlossenen Instanzen automatisch weiterhin empfängt und auch für den Cheops Clienten zum Abruf bereit hält.

Auch der Cheops Client, der über die entsprechende Verknüpfung gestartet werden kann, nachdem der Cheops Agent gestartet wurde, öffnet neben der eigentlichen GUI ein Ausgabefenster für Programmmeldungen. Hier ist auch rasch der entsprechende Fehler zu erkennen, wenn kein Cheops Agent gefunden wurde. In diesem Fall fragt die Cheops GUI in einem Eingabefenster nach der IP-Adresse des Cheops Agenten, falls dieser mit Absicht auf einem entfernten Rechner gestartet wurde, so kann die entsprechende IP-Adresse an dieser Stelle eingegeben werden.

Ist der Cheops Agent gefunden worden und kann sich der Cheops Client mit dem Agenten verbinden, so erscheint nun die Cheops GUI und lädt jetzt das zuletzt benutzte Szenario. Es sollte bei Erstbenutzung des Cheops für VNUML-Programmpakets das später beschriebene Beispielszenario mit drei Routern sein.

2.3. Grafische Darstellung in Cheops für VNUML

Allgemein ist zur Darstellung zu sagen, dass für funktionale Netzwerkgeräte Symbole der Firma Cisco Systems benutzt werden, da dieser Symbolsatz zurzeit als Industriestandard angesehen werden kann. Für die angebundenen Hosts kommen Symbole mit den darauf vermuteten Betriebssystemen zum Einsatz. Bei einem VNUML-simulierten Host ist die Bezeichnung auf dem Symbol „VNUML“, weitere Beispiele für Hosts, die durch die Netzwerkerkundung und das OS-Fingerprinting erkannt werden, sind die Kennzeichnungen „Unix“ oder „Windows“ oder die Bezeichnung „Cisco“ für eine Appliance dieser Firma.

Zu den Prinzipien der grafischen Darstellung einer Netzwerktopologie ist zu sagen, dass alle erkannten Netze durch Switch-Symbole repräsentiert werden. Dies hat den Vorteil, dass etwa bei der Erstellung einer VNUML-Simulation, immer die Netz-ID und die Subnetzmaske, des gerade in Bearbeitung befindlichen Netzwerks, angezeigt werden und so Fehler, bei der Einschätzung des zur Verfügung stehenden Adressbereichs, weitgehend vermieden werden können. Sollte einmal eine Subnetzgrenze nicht sinnvoll eingehalten werden, so würde ein entsprechender Host automatisch an ein neues Netzwerk-Symbol angezeichnet werden und es wäre offensichtlich, dass die Netze nicht zusammenhängend sind. Alle korrekt in dem Netzbereich eines Netz-Symbols liegenden Hosts werden dagegen zuverlässig mit diesem Netzwerk-Symbol verbunden. Das Symbol für Switches wurde hierbei absichtlich gewählt, da es sich aktuell um die Standardverbindungsmethode innerhalb lokaler Netze handeln sollte. Da keine Layer-2 Funktionalität betrachtet wird, sollte das Symbol aber lediglich als Stellvertreter und zur besseren Einsicht, angesehen werden.

Den Funktionalen Teil, im Sinne der Verbindung von Netzen, übernehmen natürlich Router, die mit den entsprechenden Cisco Systems-Standardsymbolen eingezeichnet werden. Sie verbinden die Switch-Symbole unterschiedlicher Netze miteinander und können beliebig

viele Anbindungen zu gleichen und zu verschiedenen Netzen beinhalten. Durch einen Rechtsklick auf ein Router Symbol, zeigt dieses alle zugeordneten Schnittstellen mit IP-Adresse und Subnetzmaske an.

2.4. Repräsentation von speziellen Geräten

Das Paradigma, wie Router in der GUI aufgebaut werden, stammt aus dem ersten Cheops Programm von Mark Spencer und soll hier, wegen den Vorteilen, die es bei der Kombination von sowohl physikalisch erkannten, als auch simulierten Netzen bietet, weiter beibehalten werden. Die Methode ermöglicht es dem Anwender, ein in VNUML simuliertes Netzwerk, mit einem, durch Erkundung erfassten physikalischen Netzwerk, welches sich an der externen Netzwerkschnittstelle des Cheops für VNUML ausführenden Computers befindet, auf anschauliche Art verbinden zu können.

Die Funktionsweise der Cheops GUI sieht dabei vor, dass zwei als Hosts mit jeweils einer Netzwerkanbindung existierende Knoten, die wie beschrieben jeweils selbst angelegt oder durch Erkundung gefunden worden sein dürfen, mit Hilfe der Maus markiert werden und anschließend mit dem Menüpunkt des Popup-Menüs von einem der Geräte, durch die Funktion „Merge Hosts“ miteinander verbunden werden. Das daraus entstehende Gerät ist nach dem Cheops-eigenen Paradigma ein Router mit zwei Anbindungen und wird dementsprechend ab diesem Moment mit einem Router-Symbol in der GUI eingezeichnet. Dieser Vorgang ist wiederholbar, sodass dem Router durch Verschmelzung mit weiteren erstellten oder entdeckten Hosts, weitere Netzwerkverbindungen zugefügt werden können.

Eine Besonderheit beim Aufbau einer Topologie stellt das Einbringen eines externen Interface dar. Dies kann mit dem Menüpunkt „Add Hostif entry“ vorgenommen werden. Mit einem solchen externen Interface wird später eine Verbindung, zwischen den zur Simulation kreierten Netzwerkgeräten und etwaigen, durch Netzwerkerkundung gefundenen, real existierenden Geräten erstellt. Eine solche Verbindung zwischen VNUML-Simulation und an der externen Netzwerkschnittstelle des Gastrechners angeschlossenen Computern wird durch VNUML in der XML-Datei, die die Netzwerktopologie beschreibt, als Hostif Schnittstelle bezeichnet. Daher stammt auch die Benennung dieser Funktion. Sie ist als optional anzusehen und wird wohl in den meisten Simulationen nicht benutzt werden, stellt aber ein sehr mächtiges Mittel dar, um eine simulierte Problematik, etwa ein Routing-Problem im Zusammenspiel mit physikalischen Routern beobachten zu können. Erwähnt werden soll hier auch die Möglichkeit, die Netzwerkkarte des VNUML ausführenden Rechners, aus der Simulation heraus zu ändern, etwa um den Rechner zum Anschluss an ein experimentelles lokales Netzwerk, welches über einen anderen Adressbereich verfügt, als das produktive Netzwerk des Hosts, mit einer anderen externen Netzwerkadresse auszurüsten. Dies geschieht mit dem zu „hostif“ verwandten Schlüsselwort „physicalif“. Hierbei ist darauf zu achten, dass nach der Beendigung der Simulation, die externe Netzwerkschnittstelle nicht automatisch auf ihren Zustand vor der Simulation zurückgesetzt wird. Es gilt also die IP-Adresse aufzubewahren und später manuell erneut zu setzen, unter Linux üblicherweise mit dem Befehl „ifconfig“.

Für den Ansatz, eine Simulation mit der externen Netzwerkschnittstelle über das Schlüsselwort „hostif“ zu verbinden, ist dies jedoch nicht notwendig.

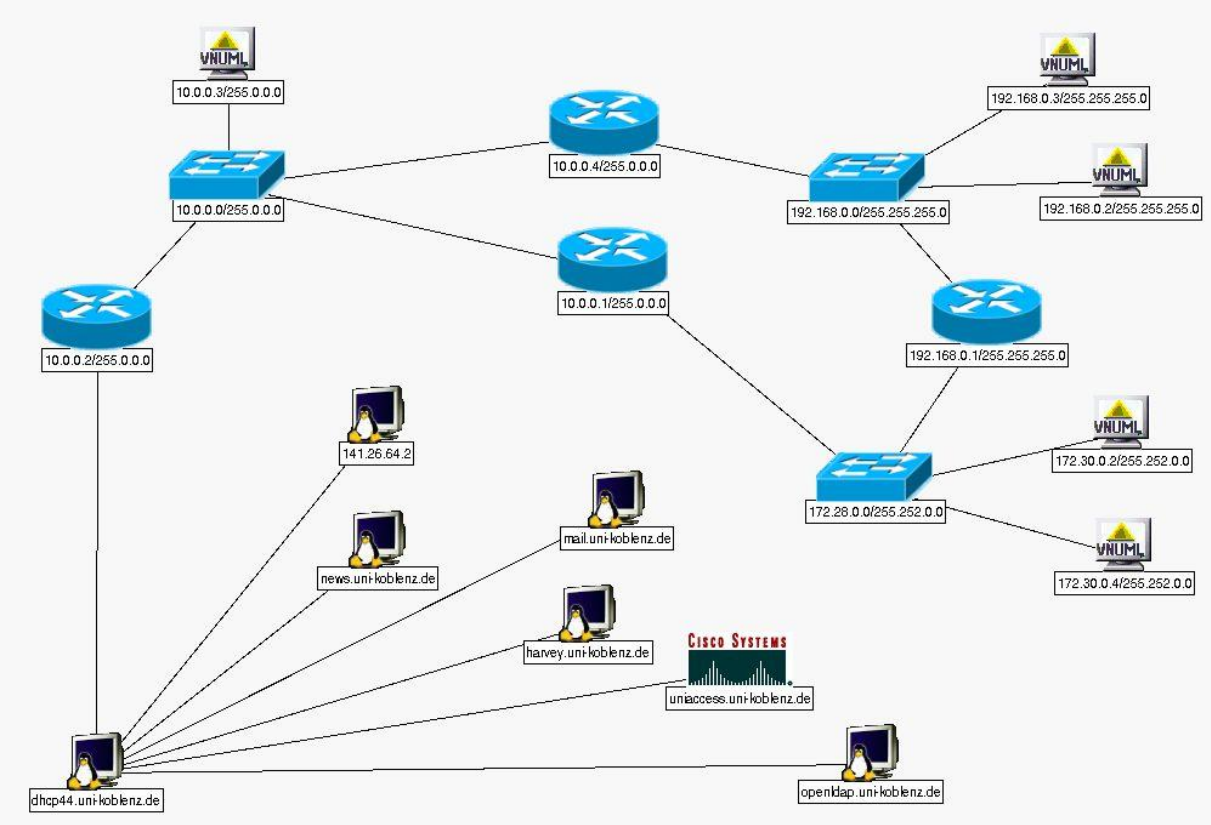


Abb. 8: VNUML-Topologie mit Anschluss des Netzwerkes der Universität Koblenz, sichtbar die ersten sieben erkannten Hosts des Adressbereichs.

In der Praxis gestaltet sich die Benutzung dieser übergreifenden Technik als recht unübersichtlich, diese sollte daher in die schnell überschaubare GUI übernommen werden. Hier können ohne weitere Wissen über die benachbarte Topologie auch die angrenzenden Netzwerkgeräte dargestellt und so die Anbindung der Simulation an diese, implizit vorgenommen werden, ohne sich durch andere Maßnahmen Informationen über Adressbereiche und Aufgaben der Geräte, beschaffen zu müssen.

2.5. Kommandos von Cheops für VNUML

Die Kommandos, die hierzu notwendig sind, finden sich unter dem Menü „Viewspace“ von Cheops für VNUML. Sie werden nun kurz vorgestellt: „Discover Host“ dient zum Einfügen eines bekannten Hosts, angeschlossen an der externen Netzwerkschnittstelle. Diese Funktion eignet sich, um einen schon bekannten Host an die Simulation anzuschließen. Der Host wird durch Auto-Discovery-Maßnahmen gesucht und nur wenn er erreichbar ist, eingefügt. Wie schon beschrieben wird nun das Betriebssystem erkannt und der Host dann mit dem geeigneten Symbol in der GUI dargestellt.

Die nächste Funktion „Discover Network“ erwartet die Eingabe eines zu erkundenden Netzwerks mit Netzwerk-ID und Subnetzmaske. In diesem Bereich werden alle IP-Adressen auf

das Vorhandensein von erreichbaren Hosts geprüft und diese dann ausgewertet und eingefügt. Diese Funktion setzt die Kenntnis über den Adressbereich des angeschlossenen lokalen Netzwerks voraus. Die vorhandenen Hosts werden dann selbständig, ohne weiteren Benutzereingriff zugefügt.

Die letzte Funktion „Discover Network Range“ bietet die mächtigste Funktionalität, indem sie einen frei wählbaren IP-Netzbereich durchsucht. Hier ist es nicht nötig, dass der Anwender die Adressierung des angeschlossenen Netzes kennt. Aufgrund der Zeitdauer und Netzwerkauslastung, die die automatische Suche benötigt, sollte der Bereich aber so eng wie möglich gefasst werden - etwa durch Kenntnis, ob es sich um einen der privaten Adressbereiche handelt oder einen mit dem Internet verbundenen Bereich. Alle in diesem Bereich gefundenen angeschlossenen Netze werden ausgewertet und in die GUI eingefügt.

Die Grundfunktionen der Cheops für VNUML GUI sind nun beschrieben und es kann eine Netzwerktopologie bestehend aus Routern und Hosts aufgebaut werden. Wird eine Topologie gespeichert, so werden die Symbole und deren Positionen ebenfalls gespeichert. Es ist darüber hinaus möglich, einen Screenshot von der angefertigten Topologie erstellen zu lassen, sowie die Darstellung mit Hilfe der Zoom-Funktion nachträglich anzupassen.

Nun zu den Funktionen, die mit der Simulation durch VNUML verbunden sind. Diese finden sich in einem eigenen Menü gleichen Namens. Eine sinnreiche Abfolge zur Simulation des aufgebauten Netzwerks wird im Folgenden beschrieben: Der erste Schritt besteht aus der Speicherung der konstruierten Topologie als XML Datei. Diese wird vom zentralen Script der VNUML-Simulation interpretiert. In ihr sind alle Eigenschaften der Netzwerkgeräte, insbesondere deren IP-Adressen festgelegt. Mit dem Befehl „Export XML“ wird eine zur Verarbeitung durch den VNUML-Parser geeignete Datei erzeugt. Diese kann zur Kontrolle über den Menüpunkt „View, Edit XML“ in einem Editor geöffnet und direkt dort überarbeitet werden, wenn dies nötig erscheint. Die von Cheops für VNUML erstellten XML-Dateien verfügen über erklärende Kommentare zu jedem Netzwerkgerät, so etwa eine Anmerkung in welchem Netzbereich die jeweilige IP-Adresse liegt.

Als weitere Funktionalität stellt der erste Teil des VNUML-Menüs eine Funktion zum Einlesen einer XML Datei, „Import XML“, zur Verfügung. Diese kann benutzt werden, um bestehende XML Dateien, auch bezeichnet als Topologie-Dateien, in die GUI einzulesen, um sie dort grafisch darstellen zu lassen. Solche XML-Dateien stehen im Labor Rechnernetze in größerer Zahl zur Verfügung, sie entstammen sowohl der Lehre, etwa aus Übungen zur Rechnernetze-Vorlesung, als auch aus Forschungsarbeiten zum Verhalten von Routing Algorithmen.

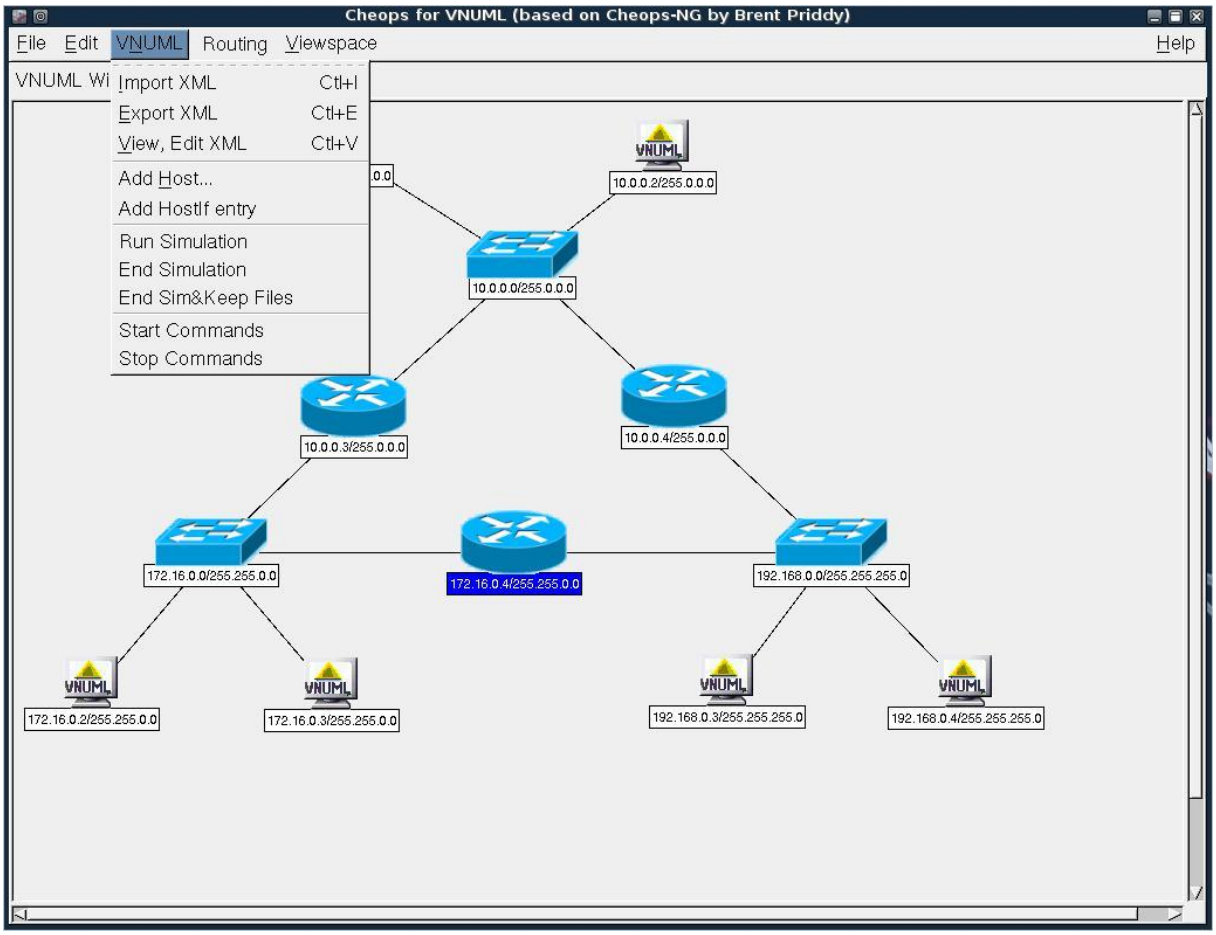


Abb. 9: Das Menü „VNUML“

Der nächste Abschnitt des VNUML-Menüs betrifft das Starten und Stoppen der Simulation. Hierbei wird durch die Cheops für VNUML-GUI das zentrale, in der Skriptsprache PERL [27] verfasste Programm des VNUML-Pakets mit dem Namen „vnumlparser.pl“ ausgeführt und dessen Ausgabe in das Ausgabefenster der Cheops für VNUML-GUI umgeleitet. Die simulierten Hosts erhalten eigene Konsolenfenster, diese können entweder auf dem ersten Desktop der Backtrack Distribution dargestellt werden oder leicht, mittels der Funktion „To Desktop:“ des entsprechenden Fenstermenüs, auf einen anderen Desktop verschoben werden.

Gestartet wird die Simulation mit dem Befehl „Run Simulation”. Es ist dabei zu beachten, dass bei jeder grafischen Änderung auch jeweils wieder eine entsprechende XML-Datei anzulegen ist. Nur die jeweils zuletzt angelegte XML-Datei wird vom „Run Simulation“-Befehl ausgeführt. Analog dazu dient der Befehl „End Simulation” zum Beenden einer laufenden Simulation. Die korrekte Beendigung kann ebenso wie der Start im Ausgabefenster der Cheops für VNUML-GUI mitverfolgt werden. Einen Sonderfall stellt die Benutzung des nächsten Befehls, „End Sim&Keep Files” dar, hier werden alle, sonst nur temporär während der Ausführung einer Simulation, erstellten Dateien behalten, um diese später auswerten oder etwaige Fehler analysieren zu können.

Teil einer VNUML-Simulation können weiterhin die zwei folgenden Elemente sein: Zum einen die Ausführung von Kommandosequenzen auf den einzelnen simulierten Hosts und zum anderen das An- und Abschalten bestimmter Dienste innerhalb der simulierten Hosts.

Dabei werden die Kommandosequenzen durch die GUI-Befehle „Start Commands“ und „Stop Commands” gestartet und gestoppt. Diese Kommandosequenzen können entweder ein bestimmtes Verhalten der simulierten Hosts, erst zu einem vom Benutzer bestimmten Zeitpunkt, nach dem Start der Simulation auslösen – etwa den Ausfall eines Routers nachdem in einem Verbund von Netzen, ein Routing Protokoll schon einen konsistenten Zustand erreicht hat. Es kann auch gerade in der Lehre nötig sein, bestimmte Vorgänge auf den simulierten Hosts, erst nach dem Start der Simulation auszulösen, um das angestrebte Verhalten explizit mit dem Verhalten zuvor oder danach vergleichen zu können. Im Anschluss wird ein Beispielszenario beschrieben, welches von Kommandosequenzen Gebrauch macht.

Der zweite Sonderfall wird von den Befehlen im Menü „Routing“ umgesetzt. Diese Befehle dienen dazu, den besonderen Anforderungen der Arbeitsgruppe Rechnernetze an der Universität Koblenz, gerecht zu werden und beinhalten die Auswahl eines geeigneten Routing Dienstes innerhalb der simulierten Hosts. Folgende Auswahl steht dem Benutzer zur Verfügung: „No Routing daemons” „OSPF Routing“ „RIP Routing” und „RIP-MTI Routing“.

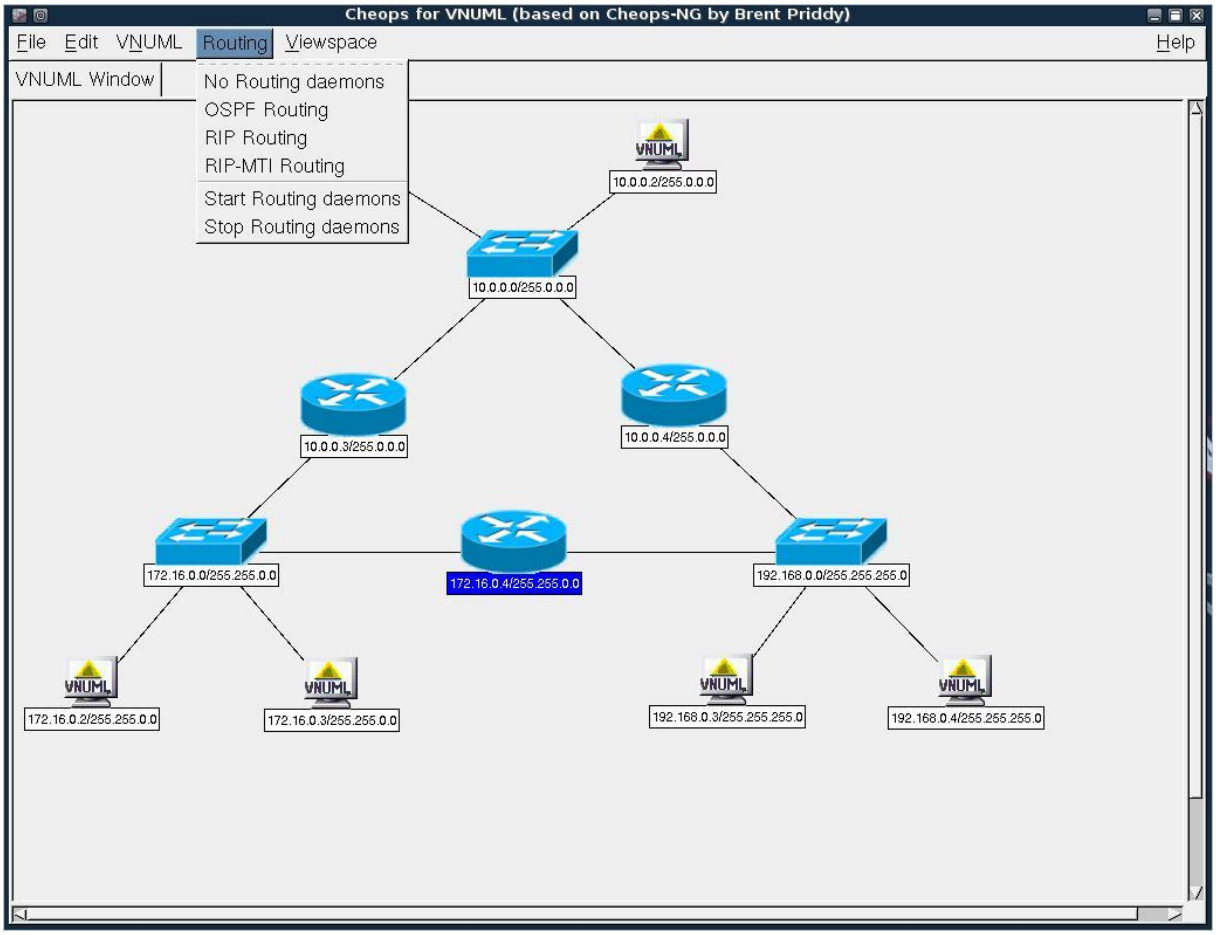


Abb. 10: Das Menü „Routing“

3. Das Beispielszenario

Dem Programmpaket Cheops für VNUML liegt ein Beispielszenario bei, welches bei der Erstbenutzung des Programms direkt geöffnet wird und als Anschauungsobjekt zur Einarbeitung in das Paradigma, das allen Cheops Versionen zugrunde liegt, dienen soll. Wie in der Einleitung zu den Vorgängerversionen von Cheops bereits angemerkt, nimmt das Programm an, dass existierende Netzwerkgeräte in einem Erkundungsdurchlauf in die GUI eingefügt werden. Die Funktionalität von Cheops setzt dann auf die vorhandenen Geräte auf – es ist daher einfacher, wenn vordefinierte Objekte manipuliert werden können, als dem Benutzer als ersten Schritt die Erstellung von Objekten abzuverlangen.

Anhand des Beispielszenarios kann der Benutzer ein logisch funktionierendes Szenario nach Belieben erweitern und eine Simulation durchführen, die eine schlüssige Netzwerktopologie aufbaut. Er kann sich darin üben, die Adressbereiche der vorhandenen Netzwerke zu erkennen und diesen dann weitere Hosts hinzuzufügen, sowie auch neue Netzwerke bekannt zu machen und diese mit den vorhandenen Netzen über Router zu verbinden.

3.1. Die Netzwerkgeräte des Beispielszenarios

Switch	10.0.0.0/255.0.0.0
Router	10.0.0.3/255.0.0.0 – 172.16.0.1/255.255.0.0
Host	10.0.0.1/255.0.0.0
Host	10.0.0.2/255.0.0.0
Switch	172.16.0.0/255.255.0.0
Router	172.16.0.4/255.255.0.0 – 192.168.0.1/255.255.255.0
Host	172.16.0.2/255.255.255.0
Host	172.16.0.3/255.255.255.0
Switch	192.168.0.0/255.255.255.0
Router	192.168.0.2/255.255.255.0 – 10.0.0.4/255.0.0.0
Host	192.168.0.3/255.255.255.0
Host	192.168.0.4/255.255.255.0

Abb. 11: Liste der Netzwerkgeräte des Beispielszenarios

3.2. XML-Datei des Beispielszenarios

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE vnuml SYSTEM "/usr/share/xml/vnuml/vnuml.dtd">
<!--    cheops-ng.map - a VNUML topology generated by Cheops for VNUML-->
<vnuml>
 <global>
        <version>1.8</version>
        <simulation_name>cheops-ng.map</simulation_name>
        <ssh_version>2</ssh_version>
        <ssh_key>~/.ssh/id_rsa.pub</ssh_key>
        <automac/>
        <vm_mgmt type="private" network="192.168.0.0" mask="24" offset="100">
                <host_mapping/>
        </vm_mgmt>
        <vm_defaults exec_mode="mconsole">
                <filesystem type="cow"> /usr/share/vnuml/filesystems/root_fs_tutorial
                </filesystem>
                <kernel>/usr/share/vnuml/kernels/linux</kernel>
                <console id="0">xterm</console>
                <!-- xterm>gnome-terminal,-t,-x</xterm -->
        <forwarding type="ip"/>
        </vm_defaults>
 </global>
```

Abb. 12: XML-Datei des Beispielszenarios, Sektion “global”

```
  <net name="Net0" mode="virtual_bridge" /> <!-- Network: 10.0.0.0/255.0.0.0-->

  <net name="Net1" mode="virtual_bridge" /> <!-- Network: 172.16.0.0/255.255.0.0-->

  <net name="Net2" mode="virtual_bridge" /> <!-- Network: 192.168.0.0/255.255.255.0-->
```

Abb. 13: XML-Datei des Beispielszenarios, Definition der Netzwerke

```
  <vm name="Uml1">          <!-- Hostname: 192.168.0.4/255.255.255.0-->
        <if id="1" net="Net2">
                <ipv4 mask="255.255.255.0">192.168.0.4</ipv4>
        </if>
        <exec seq="start" type="verbatim">snmpd</exec>
  </vm>
```

Abb. 14: XML-Datei des Beispielszenarios, Definition des Hosts „192.168.0.4“

```
<vm name="Uml3">        <!-- Hostname: 172.16.0.4/255.255.0.0-->
    <if id="1" net="Net1">
        <ipv4 mask="255.255.0.0">172.16.0.4</ipv4>
    </if>
    <if id="2" net="Net2">
        <ipv4 mask="255.255.255.0">192.168.0.1</ipv4>
    </if>
    <exec seq="start" type="verbatim">snmpd</exec>
</vm>
```

Abb. 15: XML-Datei des Beispielszenarios, Definition des Routers „192.168.0.1“

Die Router und Hosts dieses Szenarios sind mit einem Systemdienst zur Unterstützung des Protokolls Simple Network Management Protocol (SNMP) [28] ausgestattet. Dieses erlaubt es, aus einer standardisierten Tabelle von Werten, unterschiedliche Systemdaten aus einem entfernten Netzwerkgerät auszulesen. Mit diesem Dienst kann sowohl die Funktion der Kommandosequenzen anschaulich gemacht werden, als auch die Funktionalität weiterer Netzwerküberwachungssoftware überprüft werden. Im Programmpaket Cheops für VNUML steht hierfür zum Beispiel das Standardprogramm zum Auslesen von SNMP-Werten von entfernten Rechnern, „snmpwalk“ zur Verfügung. Des Weiteren ist im vorkonfigurierten Netzwerküberwachungsprogramm NAGIOS die Überwachung von zehn VNUML Geräten schon vordefiniert. Wird der Internet Browser „Firefox“ gestartet und die Standardanmeldung bestätigt, so öffnet sich eine Tabelle mit überwachten Geräten. Im Grundzustand sollten dort verschiedene Server der Universität Koblenz und des Labors für Rechnernetze als erreichbar markiert sein, eine Liste der dort überwachten Dienste findet sich im Anhang zum Programmpaket NAGIOS. Ohne eine laufende Simulation finden sich zehn vordefinierte VNUML Geräte in der Liste, welche erst einmal als unerreichbar markiert sind und somit rot dargestellt werden [vgl. Abb. 16].

Wird in der Cheops für VNUML GUI nun eine Simulation gestartet, so werden nach einiger Zeit die laufenden VNUML-Geräte in der Nagios-Tabelle als erreichbar angezeigt. Die Hosts werden wie bei Nagios üblich nur alle fünf Minuten überprüft - Nach bis zu zwei Intervallen sollten alle VNUML-Geräte in der NAGIOS-Ansicht zur Verfügung stehen. Wie in der Tabelle sichtbar werden alle erreichbaren VNUML-Geräte nach und nach eingetragen [vgl. Abb. 17]. Hierbei wird die Rückgabe des PING-Kommandos, welches zum Prüfen der Erreichbarkeit durch NAGIOS benutzt wird, ebenfalls ausgewertet. Sollte somit ein VNUML-Gerät zwar erreichbar, das PING-Kommando aber Auffälligkeiten, wie etwa Paketverlust aufzeigen, so wird dies entsprechend in der Nagios-Tabelle farblich sichtbar gemacht und eine entsprechende Einstufung in das Statusfeld des VNUML-Geräts eingetragen.

In einem nächsten Schritt kann nun mittels einer vordefinierten Kommandosequenz des Beispielszenarios die Auswertung über Simple Network Management Protocol, hinzugefügt werden. Dazu wird mittels der Cheops für VNUML-GUI die Kommandosequenz gestartet, was auf jedem VNUML-Gerät die Ausführung des SNMP-Agenten bewirkt.

Nach einer kurzen Wartezeit füllen sich in der NAGIOS-Tabelle die auf SNMP basierenden Felder mit Daten [vgl. Abb. 18]. Im vordefinierten Szenario geben diese Felder den Status der Netzwerkschnittstellen der VNUML-Hosts sowie die „Uptime“, also die Zeit seit dem Start des jeweiligen Geräts, der VNUML-Hosts an. Die Wartezeit resultiert aus der Abfragetechnik, welche der Nagios-Server für das Protokoll SNMP einsetzt. Es wird hier mit niedriger Priorität gearbeitet und Abfragen werden absichtlich zeitverzögert durch das Netzwerk geleitet um keine Lastspitzen zu erzeugen. Etwa vergleichbar mit der Abfrage von vorhandenen Hosts in einem Netzwerkbereich des Cheops für VNUML Programms geschieht die Verarbeitung auch hier streng sequentiell.

3.3. NAGIOS-Auswertung des Beispielszenarios

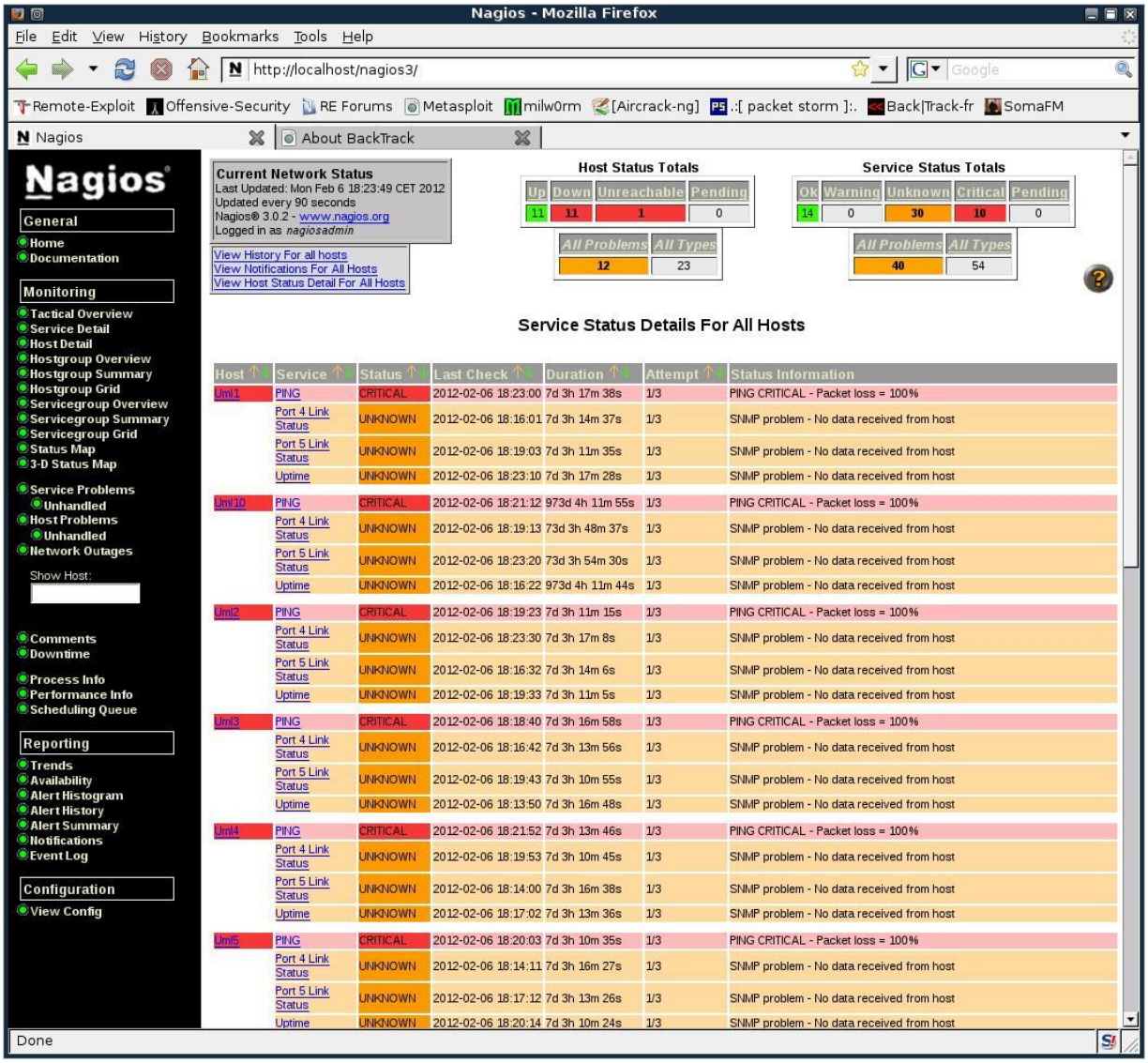


Abb. 16: Ausgabe von NAGIOS, keine VNUML-Geräte erreichbar

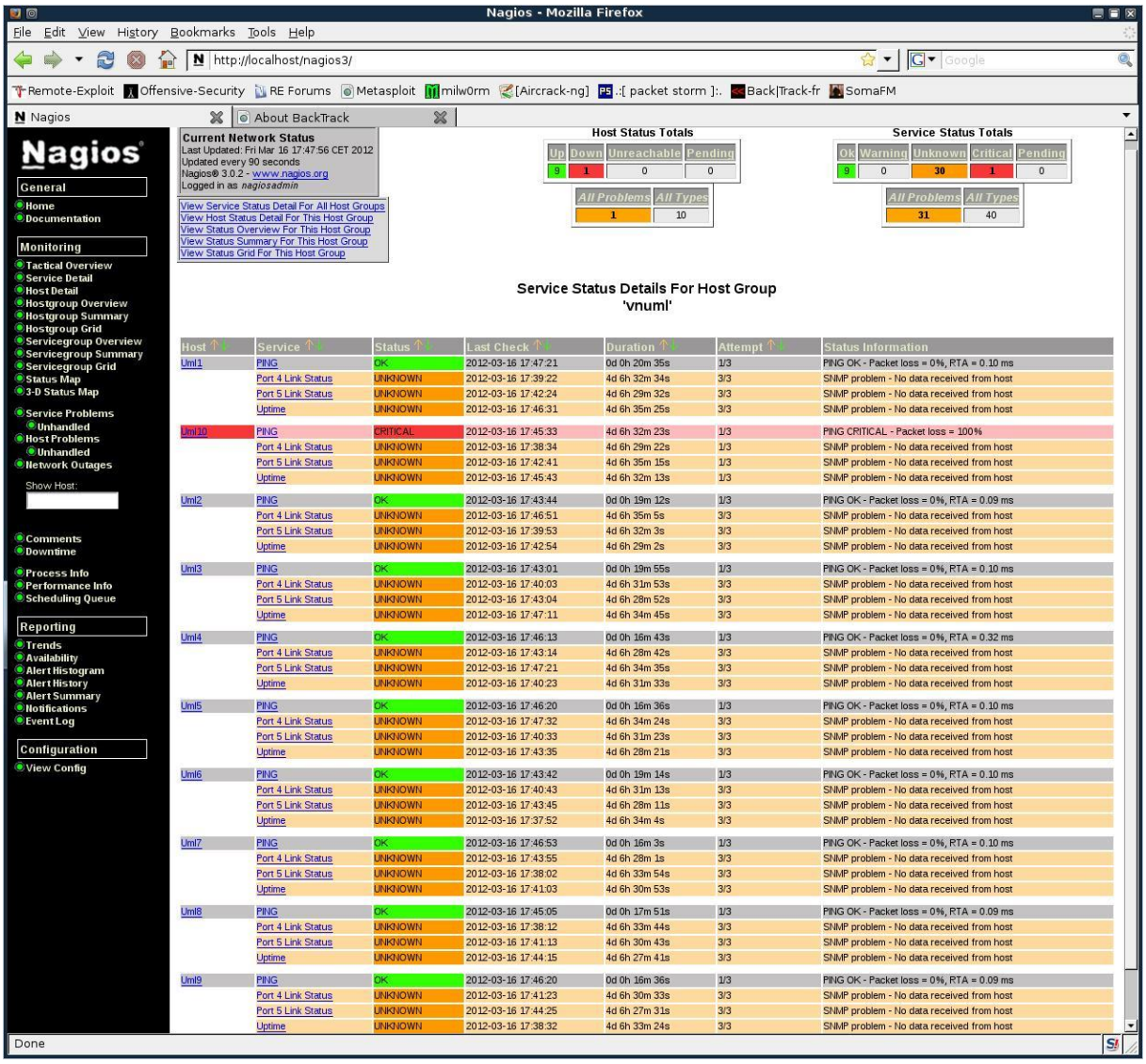


Abb. 17: Ausgabe von NAGIOS, VNUML-Geräte UML1 – UML9 erreichbar

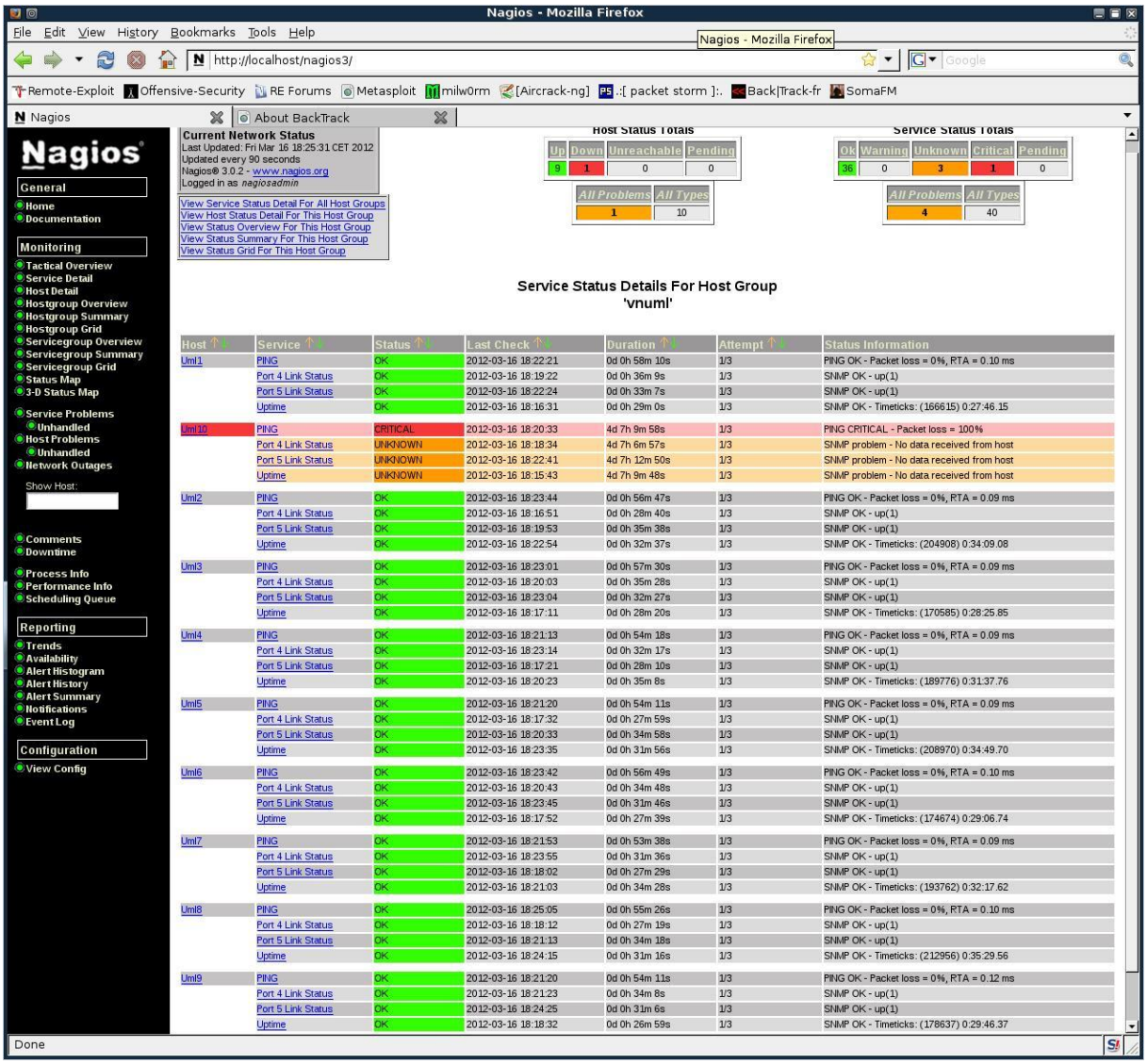


Abb. 18: Ausgabe von NAGIOS, VNUML-Geräte UML1 – UML9 mit SNMP Status „OK“

4. Linux Distribution Backtrack 4

4.1. Backtrack - ein modulares Live-System

Die Distribution Backtrack [17][18] ist als Live System ausgelegt. Hierbei wurde nicht nur die Lauffähigkeit von einer DVD berücksichtigt, sondern infolge der zunehmenden Beliebtheit und des günstigen Preises von USB-Sticks auch dieses Speichermedium.
Der USB-Stick macht es dem Benutzer möglich, seine durchgeführten Änderungen am Live-System abspeichern zu können. Die Backtrack Distribution stellt dafür zwei Möglichkeiten zur Verfügung: Erst einmal kann der Benutzer permanent auf einem Dateisystem in einer normalen Festplattenpartition arbeiten. Die Distribution bietet hierbei ein unveränderliches ROM, aus welchem Betriebssystem und Anwendungen geladen werden - jeder Schreibvorgang wird jedoch wie gewohnt auf einem Dateisystem durchgeführt. Zur Anschauung sei gesagt, dass eine Datei solange lediglich virtuell vorhanden ist, also in einer RAM-Disk vorrätig gehalten wird oder bei Nichtbenutzung nur im ROM vorliegt, bis sie verändert und geschrieben wird. Zu diesem Zeitpunkt gelangt die aktualisierte Form direkt auf den Speicher für Änderungen, also eine Festplattenpartition oder eine XFS-Datei. Wichtig ist natürlich auch, dass beim wiederholten Laden der Distribution, das Speichermedium für Änderungen immer zuerst überprüft wird, nämlich daraufhin, ob eine aktuellere Version einer zu verarbeitenden Datei vorliegt.

Bei dieser Benutzung der Distribution ist ein sehr zügiges Arbeiten gewährleistet - in der Tat ist es so, dass bis auf den Startvorgang, der die Geschwindigkeit von DVD-ROM oder USB-Stick abhängig macht, keine Geschwindigkeitseinbußen gegenüber fest installierten Systemen befürchtet werden müssen. Dies liegt auch daran, dass versucht wird, für den Zugriff benötigte Dateien möglichst geschickt im Hauptspeicher des Computers, genauer gesagt, in einer RAM-DISK, bereit zu halten.
Die zweite Speicherung von Änderungen, zu der die Backtrack Distribution in der Lage ist, ist eine auf Flexibilität optimierte Möglichkeit. Hierbei kann der Benutzer, wenn er seine Änderungen abzuspeichern wünscht, am Ende seiner Sitzung an der Backtrack Distribution durch eine manuelle Befehlseingabe die Speicherung anstoßen.
Daraufhin werden all diejenigen Inhalte der RAM-Disk, welche Änderungen erfahren haben, in ein XFS- oder EXT2-Dateisystem geschrieben.

Die Besonderheit dabei ist, dass ein XFS Dateisystem nicht notwendigerweise eine komplette Festplattenpartition einnehmen muss, sondern vielmehr als Datei in einem beliebigen darunterliegenden Dateisystem abgelegt werden kann. Es ist damit möglich, alle geänderten Dateien mit Ihren Zugriffsrechten und weiteren Attributen, innerhalb einer XFS-Datei in ein DOS/Windows Dateisystem wie FAT16 oder FAT32 abzulegen. Ein solches Dateisystem befindet sich zum Beispiel häufig auf einem verwendeten USB-Stick der auch die Backtrack Distribution trägt - es kann sich aber auch um eine im Computer verbaute Festplatte, mit dem Betriebssystem Microsoft Windows darauf, handeln. Wichtig ist lediglich, dass der Speicherort, genau wie die Partition aus der zuvor vorgestellten Speichermöglichkeit, dem Backtrack Betriebssystem schon beim Systemstart zur Verfügung steht.
Als eine Kombination der beiden vorgenannten Speicherungsarten gibt es die weitere Möglichkeit, die Daten permanent in eine XFS-Datei auf einer DOS/Windows-Partition zu schreiben. Hierbei werden Änderungen sobald sie erfolgen auf das Dateisystem übertragen.

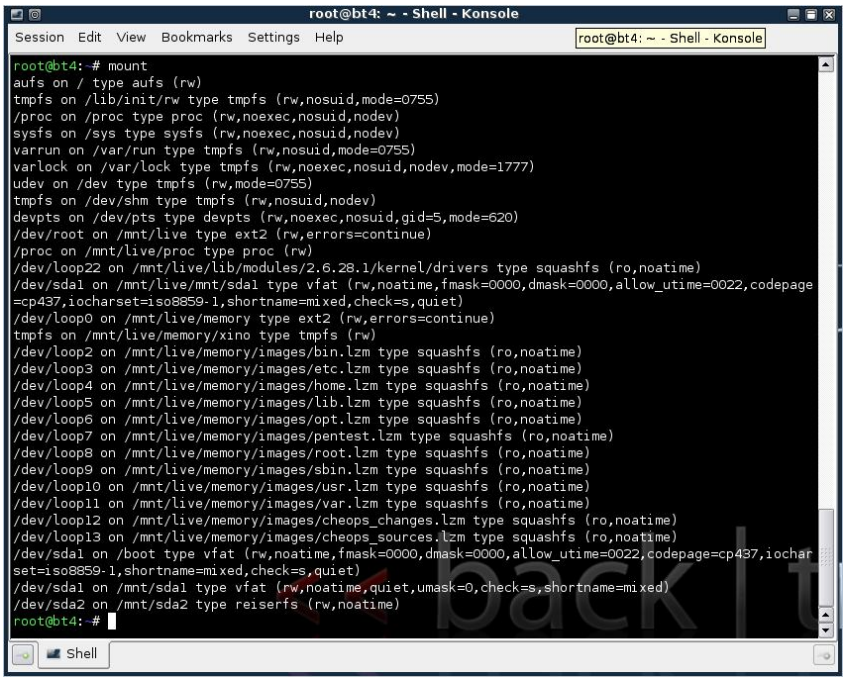


Abb. 19: eingehängte Dateisysteme der Backtrack Distribution

Die angepasste Backtrack Distribution mit Cheops für VNUML benutzt ein weiteres effizientes Mittel, das sich aus dem vorgenannten ergibt. Um eine möglichst hohe Arbeitsgeschwindigkeit zu ermöglichen - indem verhindert wird, dass die Änderungsdatei bei jedem Neustart in den Startvorgang eingebunden ist - sind alle Änderungen gegenüber der Original Backtrack Distribution in weitere LIVE Module aufgeteilt worden. Zur Erläuterung sei gesagt, dass LIVE Distributionen ihre Inhalte meist aus komprimierten Dateien laden. In mehreren solcher Archive ist auch der Inhalt, den das Cheops für VNUML-Paket bietet, abgelegt worden. Dem Benutzer steht es damit völlig frei, über die Organisation seiner Änderungen und den Umfang des gestarteten Systems zu entscheiden.

Beim Startvorgang der Backtrack Distribution mit Cheops für VNUML besteht die Auswahl zwischen dem Arbeiten ohne das Hinterlassen von Änderungen - auch hier kann aber trotzdem immer noch das Wegschreiben der Änderungen per Hand angestoßen werden - und der bequemen Aufzeichnung aller Änderungen auf einer Datei oder Partition auf einem USB Stick oder Festplatte - egal ob von einem solchen selbst oder von einer DVD gestartet wurde.
Zwischen diesen Arbeitsweisen, die schon beim Systemstart unterschieden werden, wird der Benutzer zu Beginn des Startvorgangs durch ein komfortables Startmenü zur Auswahl aufgefordert.
Auch diese Startmöglichkeiten kann der Benutzer selbst beeinflussen, da das Erstellen des Startmediums durch einfache, vom Benutzer überschaubare Schritte vorgenommen wird. Hierzu verwendet die Backtrack Distribution die Standardprogramme SYSLINUX und ISOLINUX [34].
Als Änderungsmedium kann bei Erstellung einer Backtrack Distribution auf einem Wechseldatenträger, genauso wie bei der Installation von Backtrack auf eine lokale Festplatte, jedes beliebige beschreibbare Medium ausgewählt werden. Hierbei bietet sich beim Durchführen einer Installation auf Festplatte eine eigene Partition an. Diese sollte mit dem Dateisystem EXT2 oder EXT3 initialisiert werden. Eine solche Umgebung bietet die bestmögliche Arbeitsgeschwindigkeit. Eine entsprechende Installation findet sich auf dem Dell Optiplex PC im Labor Rechnernetze der Universität Koblenz.

Eine variable Möglichkeit der Benutzung der Cheops für VNUML-Software stellt die Installation auf einem USB-Stick dar. Das Speicherabbild [32] des Referenz-Wechseldatenträgers [29], das vom Server der AG Rechnernetze der Universität Koblenz heruntergeladen werden kann, ist wie folgt aufgebaut: Der gesamte Datenträger ist aus kompatibilitätsgründen mit dem Dateisystem FAT32 initialisiert. Im Verzeichnis „boot“ befinden sich die zum Systemstart nötigen Dateien des Pakets ISOLINUX/SYSLINUX sowie die Linux Startdateien. Im Verzeichnis „bt4“ befinden sich die relevanten Dateien für die angepasste Backtrack Installation. Es sind dies im Unterverzeichnis „base“ die Archive der Backtrack Distribution und im Unterverzeichnis „optional“ die zwei Archive für die „Cheops für VNUML-Quellen und Programmierumgebung“ und die „Cheops für VNUML-ausführbare Dateien und Einstellungen“. Es können wahlweise auch, die zu umfangreich erscheinenden Bereiche der Backtrack Distribution, in den Bereich „optional“ ausgelagert werden. Von hier werden die Archive nicht mehr automatisch geladen, sondern nur auf Anforderung beim Start eingebunden. Die Cheops für VNUML-Archive werden natürlich durch eine entsprechende Anpassung der Starteinstellungen immer automatisch gestartet. Als Beispiel wäre es möglich, den umfangreichsten Teil der Backtrack Distribution zum Thema „Penetration Testing“[6] vom automatischen Start auszuschließen. Dies dient jedoch lediglich dem Sparen von Speicherplatz.

Beim Start des vollen Funktionsumfanges der Backtrack Distribution stehen dem Anwender nach Systemstart die folgenden Kategorien von Sicherheitssoftware zur Verfügung:

Information Gathering
Network Mappings
Vulnerability identification
Penetration
Privilege Escalation
Maintaining Access
Radio Network Analysis
VoIP
Digital Forensics
Reverse Engineering
Miscellaneous

Abb. 20: Kategorien von Sicherheitssoftware und Tools im Startmenü von Backtrack 4

Es werden nun einige Tools beschrieben, die der Software Cheops für VNUML sehr nahe stehen und sich im Kontext von Netzwerkerkennung und Netzwerküberwachung als nützlich erwiesen haben.

4.1. NMAP

Ursprünglich entwickelt von Gordon „Fyodor“ Lyon in 1997 [18]. Lyon war zur Entwicklungszeit von NMAP ein Mitglied der „Hackerszene“, heute ist er sogenannter „ethical Hacker“, also jemand, der sich an die gesetzlichen Vorgaben hält und seine Fähigkeiten zur Absicherung von Rechneranlagen einsetzt. Das Programm war anfangs ein sehr kompakter Portscanner - ein Programm das eine oder mehrere IP-Adressen auf offene Ports prüft [19].

6: Oft findet sich auf entsprechenden Webseiten die Abkürzung „pentest“

Die Ports werden dann in die Klassifizierungen offen, geschlossen und verborgen eingeordnet. Ein verborgener[7] Port ist dabei als ein Port anzusehen, bei dem der angesprochene Dienst nicht sofort antwortet sondern dies erst nach einer bestimmten Art der Anfrage oder einer bestimmten Zeitdauer tut, um den Dienst im Internet vor Angriffen zu schützen.
Das Programm NMAP wurde bald um die Fähigkeit erweitert, Bereiche von IP-Adressen durchzuarbeiten und in diesen nach aktiven Geräten zu suchen. Die Schwierigkeit in dieser erst einmal trivial erscheinenden Funktion liegt darin, dass im Internet funktionale Server oft dadurch versteckt werden, dass sie auf die meisten üblichen Anfragen nicht antworten, etwa auf das Kommando PING. NMAP versucht hier signifikante Ports zu benutzen, auf denen dennoch eine Antwort erfolgt, etwa den Port 135 des Dienstes RPC.
Eine weitere Besonderheit des Programms NMAP ist eine Datenbank und Techniken zur Realisierung der Funktion OS-Fingerprinting. Hierbei werden bestimmte Ports abgefragt sowie Verbindungen aufgebaut und einige Pakete übermittelt um aus der Abfolge der Reaktionen in der entsprechend aufgebauten Datenbank nach dem Herkunftsbetriebssystem suchen zu können. Diese Datenbank schließt nicht nur die Betriebssysteme von Computern, sondern auch von Netzwerkgeräten ein, auf denen Betriebssysteme laufen, sogenannte „Appliances“.

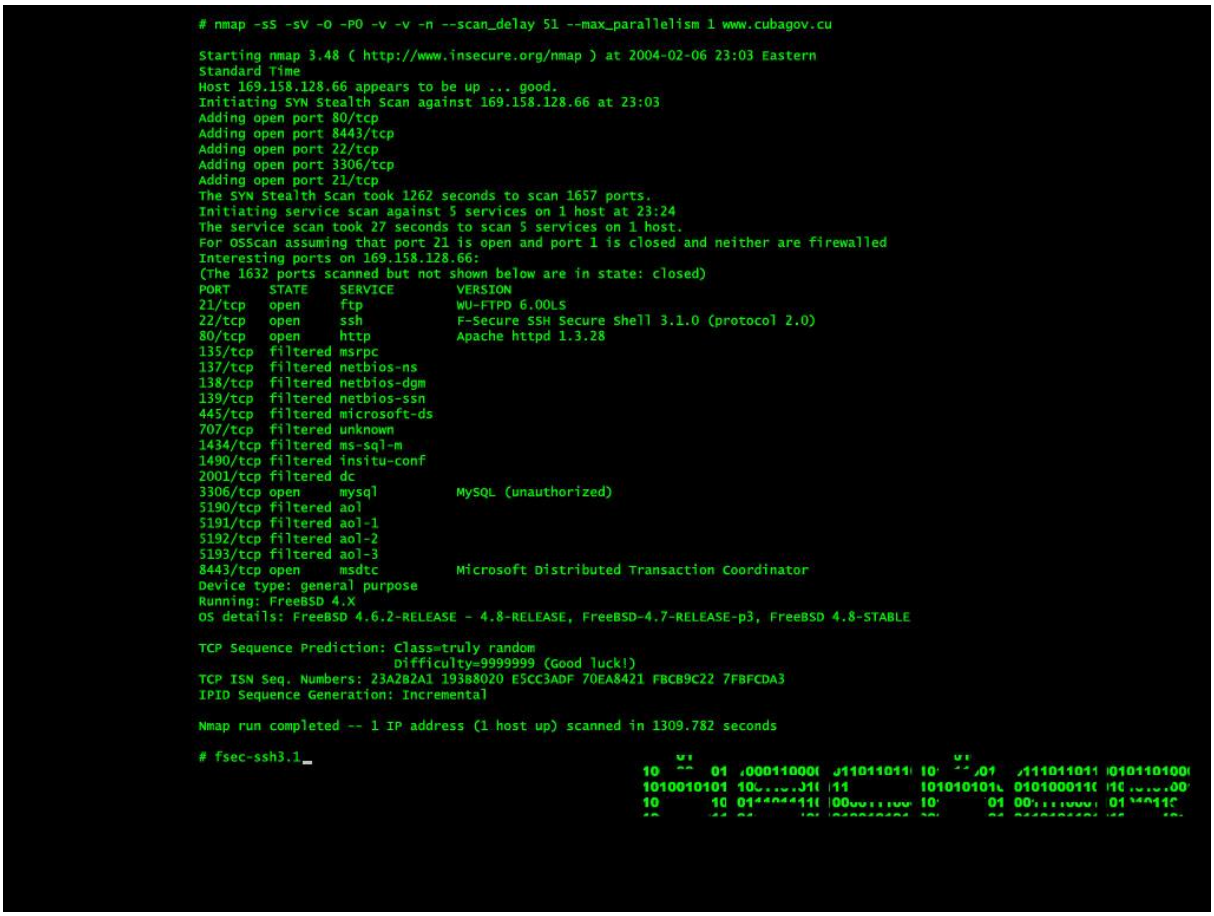


Abb. 21: sogenannte „Fan-Art“ um das Thema NMAP. Ein illustriertes Bild eines Mitglieds der Community um NMAP. Zu sehen ist der illustrierte „Portscan“ eines kubanischen Regierungsservers.

7: Gebräuchlicher ist die englische Bezeichnung „Stealthed“

4.2. WIRESHARK

Dieses Programm ist der bekannteste Vertreter der Programmgruppe der Netzwerk-Sniffer [20]. Diese Programme dienen dazu Netzwerkverkehr zu analysieren. Das Programm WIRESHARK trägt diesen Namen seit 2006 [21]. Zuvor war es als ETHEREAL bekannt, unter diesem Namen begann Gerald Combs 1997 mit der Entwicklung. WIRESHARK verwendet sogenannte Low-Level Treiber oder entsprechende Einstellungen an vorhandenen Netzwerktreibern um den gesamten Verkehr in einem Subnetz über das Interface des WIRESHARK Gastrechners einzusehen. Da die Netzwerkhardware normalerweise nur die Pakete für die eigene MAC-Adresse einer Netzwerkschnittstelle an das Betriebssystem übermittelt, wird hier der „Promiscuous Mode“ einer Netzwerkkarte genutzt, um dies zu umgehen. Gerätetreiber, die dies unterstützen, gibt es sowohl für die Betriebssysteme Linux und Microsoft Windows als auch für verdrahtete und schnurlose Netzwerke.
Das Programm WIRESHARK kann den so aufgefangenen Netzwerkverkehr aber nicht nur anzeigen oder aufzeichnen, sondern stellt Techniken zur Verfügung, um den Netzwerkverkehr effizient darzustellen und Fehler erkennen zu können. Außerdem werden statistische Funktionen angeboten.

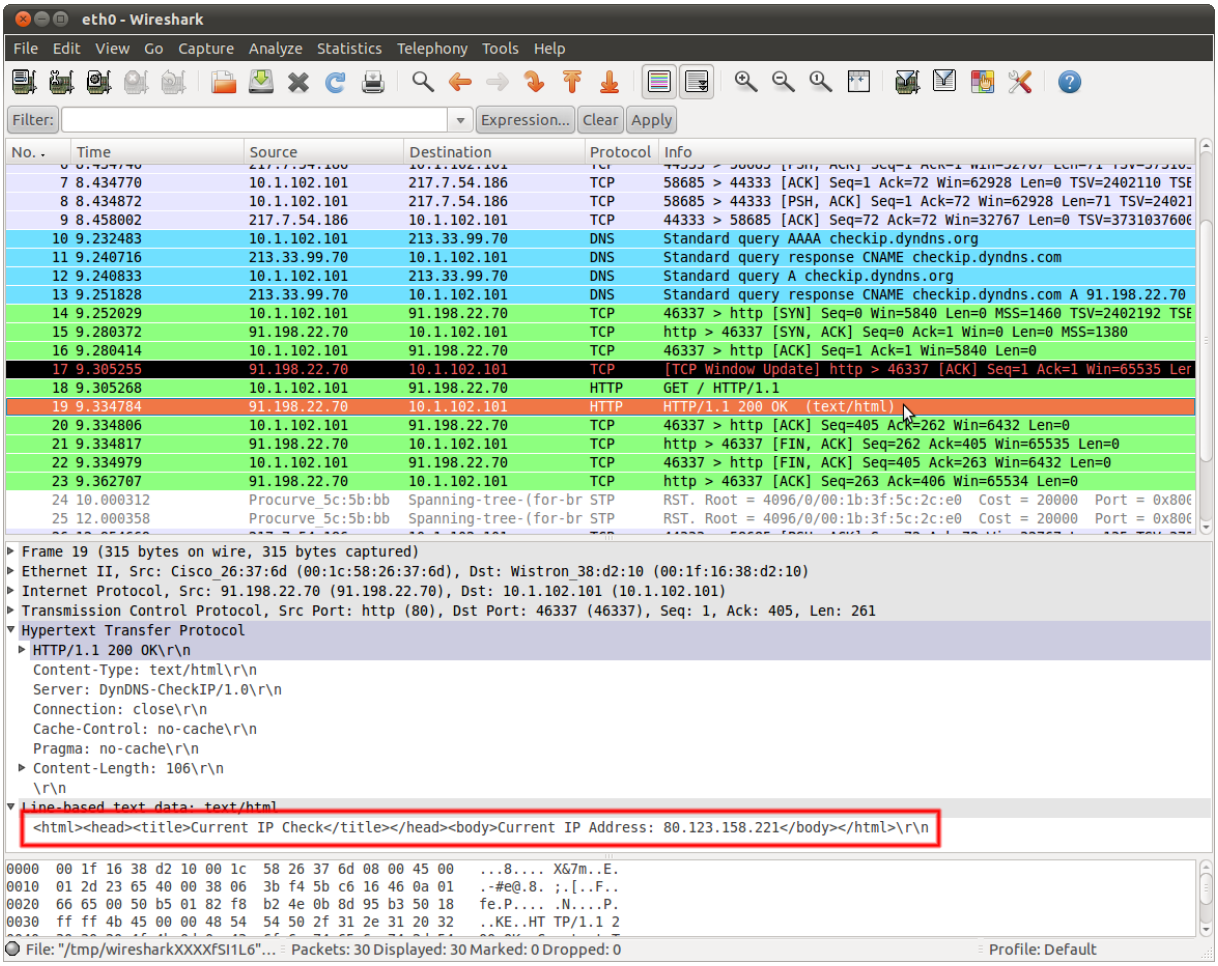


Abb. 22: Analyse eines Netzwerkverkehrs mit WIRESHARK und Filterung des Ports 80 „HTTP“. Aus einer erklärenden Seite der Firma Thomas Krenn

Um zum einen fehlerhafte Pakete in einem Netzwerkprotokoll anzeigen zu können und zum anderen Pakete, in deren Funktion für eine Rechner zu Rechner Kommunikation, richtig benennen zu können, ist es natürlich nötig, das das Programm WIRESHARK hinreichende Kenntnis über diese Protokolle hat. Die Anzahl der unterstützten Protokolle geht dabei mit den häufigen neuen Versionen von WIRESHARK stetig nach oben, die unterstützten Protokolle umfassen nicht nur auf Layer-3 aufbauende Protokolle [21], sondern auch Layer-2 Protokolle, sowohl verdrahteter als auch schnurloser Netzwerke. Etwa Protokolle zum Verbindungsaufbau von WLAN Netzen, wie auch Protokolle zur Beherrschung des Schleifenproblems in, aus Netzwerk-Switches aufgebauten, Layer-2 Netzwerken.

4.3. ETTERCAP

Grundsätzlich ist ETTERCAP zur Programmgruppe der Netzwerk-Sniffer gehörig, also ein Programm zur Analyse des Netzwerkverkehrs, aber mit entscheidenden Änderungen, die das Programm nach der gegenwärtigen Auffassung nah an die Programmgruppe der Schadprogramme heranrückt. Die erste Ausgabe des Programms ETTERCAP stammt aus dem Jahr 2001, die Entwickler sind Alberto „ALoR“ Ornaghi und Marco „NaGA“ Valerie [22]. Beide sind auch heute noch an der Entwicklung des Projekts beteiligt und werden der „Hackerszene“ zugerechnet. ETTERCAP beherrscht es durch das Fälschen von Paketen Einfluss auf Verbindungen zu nehmen. Mit dieser Technik werden etwa sogenannte „Man in the middle“-Angriffe bewerkstelligt. Hierbei werden Datenpakete zwischen zwei miteinander kommunizierenden Hosts derart verändert und den Kommunikationspartnern wieder zugesandt, dass zum einen die Existenz des Angreifers zwischen den beiden Partnern unentdeckt bleibt und zum anderen eine wie auch immer ausgeführte Manipulation an den Daten vorgenommen wird. Der erste Schritt besteht meist aus dem Ausspähen von Anmeldedaten oder Kennwörtern, später wird der laufende Verkehr durch die Manipulation von Daten derart verändert, wie es dem Angreifer zu dessen Vorteil gereicht.
ETTERCAP ist zudem in der Lage, auf den Ebenen unterhalb des Protokolls IP, Pakete zu interpretieren und zu manipulieren. So kann die Funktionsweise von Layer-2 Netzen gestört werden oder das Protokoll ARP für das Ausspähen von Daten manipuliert werden. Dieser Angriff wird auch als ARP-Spoofing bezeichnet. Hierdurch wird die korrekte Hardware-Adresse eines Kommunikationspartners bewusst gefälscht, um diesen durch einen eigenen, zum Zwecke des Dateneinbruchs existierenden Host zu ersetzen. Auf diesem kann dann die eintreffende Kommunikation des angegriffenen Hosts mit komfortablen Netzwerk-Sniffer-Programmen wie etwa WIRESHARK aufgezeichnet und ausgewertet werden. Das Programm ETTERCAP gilt als potenzielles Hacker Werkzeug, dessen Einsatz in Deutschland aufgrund des sogenannten Hackerparagraphen nur mit Kenntnis der Gesetzeslage durchgeführt werden sollte [vgl. Kapitel 4.5].

4.4. Bekannte Fehler der Backtrack Distribution

Zu beachten ist ein bekannter und nicht korrigierbarer Fehler bei Betrieb im lokalen Netz der Universität Koblenz: Verursacht durch die Sperrung des Ports 123 für den Dienst NTP kann kein üblicher NTP-Zeitserver im Internet abgefragt werden. Zwar ist der lokale Zeitserver der Universität Koblenz hier eingetragen, ein mit Stratum-3 eingestufter Zeitserver und damit ausreichend genau, leider wird dieser Server durch einen Fehler im zugrundeliegenden Ubuntu-Linux nicht von Systemstart an abgefragt. Es muss daher durch einen Rechtsklick auf die Systemuhr der Dialog „Adjust Date/Time“ geöffnet werden, anschließend muss lediglich

die automatische Synchronisierung der Systemuhr deaktiviert und anschließend wieder neu aktiviert werden. Daraufhin wird die Systemzeit korrekt mit dem Zeitserver der Universität Koblenz abgeglichen. Bei einem Betrieb außerhalb der Universität Koblenz muss hier natürlich wieder auf den voreingestellten Zeitserver der Ubuntu-Distribution oder einen anderen allgemein verfügbaren Zeitserver wie „pools.ntp.org“ umgeschwenkt werden.

4.5. Rechtliche Lage in Deutschland

Einige der Programme, die die Backtrack Distribution beinhaltet, fallen in Deutschland unter den sogenannten Hackerparagraphen, §202c StGB [23]. Dieser Paragraph sieht vor, den Besitz und Vertrieb von Programmen unter Strafe zu stellen, die dazu geeignet sind Sicherheitsmaßnahmen von IT-Einrichtungen auszuhebeln oder zu umgehen. Hierbei ist ein notwendiges Kriterium der Strafbarkeit jedoch die Absicht zu einer späteren, illegalen Nutzung. Diese wird in §202a StGB und §202b StGB genauer beschrieben.
In diesem Kontext des „Vorbereitens des Ausspähens oder Abfangens von Daten“ kommt dem „in Besitz nehmen“ geeigneter Programme oder dem Vertrieb zum späteren Zwecke des illegalen Einsatzes der Status des „Vorbereitens einer Straftat“ zu.

Zur legalen Nutzung muss dementsprechend jeder Schritt ab dem Erwerb oder kostenlosen „in Besitz nehmen“ bis zur Ausführung, etwa einer Passwortumgehung oder einer Datenaufzeichnung, lückenlos dokumentiert werden. Auch in einem geschäftlichen Umfeld, wenn es die eigene IT betrifft oder im privaten Raum, sollte jeder Audit, also die praktische Überprüfung von IT-Sicherheitseinrichtungen auf Lücken hin, immer dokumentiert werden.
Diese Regelungen betreffen den gesamten Europäischen Raum, wo durch den Rahmenbeschluss des Europarats in ETS No. 185 „Cybercrime Convention“ das Vorgehen gegen Angriffe auf Computersysteme geregelt wird.

Aus dieser Regelung sollte jeder interessierte Benutzer einer solchen Distribution, den Test derselben, immer streng auf den privaten Raum beschränken. Als Anschauungsbeispiel kann hierzu ein kompromittierbares System, etwa aufgebaut mit der Linux-Distribution „Damn Vulnerable Linux“ (DVL) [35] benutzt werden. Diese enthält eine spezielle Zusammenstellung von bekannt sicherheitsanfälligen und trotzdem oft benutzten Diensten, die in den nicht sicherheitsmodifizierten Versionen vorliegen. Hier kann ein Benutzer der Backtrack-Distribution in einem zweiten Arbeitsschritt auch gleich die vorzunehmenden Sicherheitsverbesserungen an seiner DVL-Referenzinstallation vornehmen und prüfen.

5. Network Monitoring

5.1. NAGIOS

Das Programm NAGIOS [24] ist das populärste Programm zum Network Monitoring. Es ist Open Source Software und steht unter GNU Lizenz. Das Programm war nativ zum Einsatz unter Linux entwickelt, ist jedoch mit vielen anderen Unix Varianten lauffähig.
Das Programm zeichnet sich durch die hohe Anzahl verfügbarer Erweiterungen aus, die es ermöglichen, das Programm in nahezu jeder Netzwerkumgebung einzusetzen. Ebenso ist das Programm durch die einsetzbaren Plugins besonders gut skalierbar.
Die erste Version von Nagios war 1999 verfügbar. Zu dieser Zeit hieß das Programm noch NETSAINT. Es kam jedoch zu einem Namenskonflikt mit einem anderen Projekt, dem Network Security Scanner NETSAINT, der etwa zur selben Zeit Verbreitung fand. Ethan Galstad benannte sein Programm daher um in NAGIOS. Der Name ist ein „Portmanteau“-Wort aus dem Begriff „Network“ und dem griech. Wort „Hagios“, welches heilig bedeutet. Eine weitere Lesart gibt Ethan Galstad mit der Deutung des Wortes Nagios als rekursives Akronym, wie es bei vielen unter dem Betriebssystem UNIX gebräuchlichen Programmnamen zur Tradition geworden ist. Nagios wäre demnach die Abkürzung für "Nagios Ain't Gonna Insist On Sainthood".

5.2. Grundsätzliches zur Funktion

NAGIOS steht bei vielen Linux-Distributionen direkt in deren Repository zur Verfügung. Nach der Installation wird Nagios über Einstellungsdateien konfiguriert. Dabei werden zum einen Gruppen angelegt, in denen die zu überwachenden Netzwerkgeräte anhand ihrer IP-Adressen eingetragen werden, sogenannte Host Groups und zum anderen Gruppen erstellt, mit den zu überwachenden Diensten oder Eigenschaften der Geräte, bezeichnet als Service Groups.

NAGIOS beherrscht verschiedene Möglichkeiten, um entfernte Netzwerkgeräte zu überwachen. In diesem Funktionsumfang liegt einer, wenn nicht der Hauptvorteil des Programms NAGIOS begründet. Die zu überwachenden Netzwerkgeräte und Ihre Dienste lassen sich so mit einer, der Situation angepassten, Abfragemethode ansprechen und dies mit einer, der Art der Erreichbarkeit entsprechenden, Zugriffsmethode.
Im Folgenden sollen die Abfragemöglichkeiten, im Hinblick auf Ihre Fähigkeiten, in Bezug auf die Eigenschaften des abzufragenden Dienstes und der Zugriffsmöglichkeit auf das entfernte Gerät, in Bezug auf die speziellen Eigenschaften des verwendeten Netzwerks, dargestellt werden.
Die Software NAGIOS ist nicht zuletzt deswegen so verbreitet, weil sie als sehr universell einsetzbar bezeichnet werden darf. NAGIOS ist dafür ausgelegt, mit drei unterschiedlichen Methoden, Daten von anderen Netzwerkgeräten abfragen und Ergebnisse empfangen zu können. Dies sind erst einmal das verbreitete Protokoll SNMP, welches die meisten festverdrahteten Netzwerkgeräte implementieren sollten. Für Computersysteme stehen zusätzlich die Erweiterungen NRPE und NSCA zur Verfügung.

5.2. Das NAGIOS Plugin-System

NRPE stellt für NAGIOS ein Plugin dar, welches es dem Nagios System ermöglicht, eine Anfrage zum Auslesen von Systemparametern eines bestimmten Netzwerkgerätes abzusetzen. Die NRPE Infrastruktur sendet die Anfrage anschließend mit SSL-Verschlüsselung an das Zielsystem. Dort wird die Anfrage von einem NRPE Agenten, der auf jedem kontrollierten Zielsystem vorhanden sein muss, abgewickelt. Dieser Agent besitzt auf dem Zielsystem die nötigen Berechtigungen um die gewünschten Parameter auslesen zu können. Der NRPE Agent kann hierzu sowohl Skripte als auch Programme zur Ausführung bringen.
Die erzielten Ergebnisse werden dann zeitnah vom NRPE Agenten wieder an das anfragende Kontrollsystem zurückgesendet. Auch die Sendung in Rückrichtung wird über einen gesicherten Kanal vorgenommen.
NSCA stellt im Gegensatz hierzu eine Methode dar, bei der die Informationserzeugenden Instanzen im Netzwerk ohne dazu aufgefordert werden zu müssen - sondern aufgrund eines zeitgesteuerten Ablaufplans - ihre Werte an das Nagios Kontrollsystem absetzen. Die Informationserhebung und Informationsübermittlung erfolgt dabei nach einem im Client abzulegenden Zeitplan. Dem Nagiossystem steht ein Plugin zur Seite, welches auf eingehende Informationssendungen wartet, diese annimmt und dem Nagiossystem die gewonnenen Daten zur Verfügung stellt.

Die verschiedenen Informationen, die das Nagiossystem so über das Netzwerk sammelt, können optional mit Hilfe eines weiteren Plugins, „ndoutils“, in einer „mysql“ Datenbank gespeichert werden. Dies ermöglicht sowohl eine zeitversetzte Analyse der Daten, als auch die spätere Kontrolle von besonderen Zuständen oder Vorfällen und deren genaue zeitliche Abfolge.

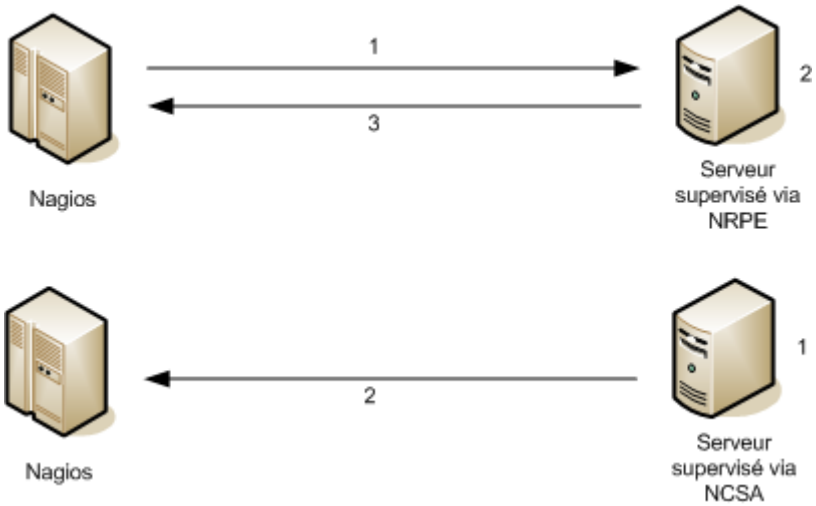


Abb. 23: Schema der Signalverarbeitung bei den Methoden NRPE und NSCA

Die Stärke des NAGIOS-Systems besteht in der leichten Erweiterbarkeit durch Plugins und des reichhaltigen Vorhandenseins derselben. Erst durch Plugins wird das NAGIOS-System zu dem universell einsetzbaren Werkzeug das es ist.

Die Plugins teilen sich in offizielle Plugins, welche sich von der NAGIOS Webseite beziehen lassen und inoffizielle Plugins, die auf weiteren Community-Webseiten angeboten werden. Diese Plugins können dann entweder auf Client-Seite eingesetzt werden, etwa zum Auslesen von Umgebungswerten oder zum generellen Auslesen von ad hoc nicht unterstützten Platt-

formen oder sie dienen auf Serverseite zur weiteren Speicherung oder Verarbeitung der ausgelesenen Daten.
Hier sei angemerkt, dass jedoch gerade dieses Plugin-System auch zur Schwachstelle des Programmsystems NAGIOS gehört. Der Ärger der unterstützenden Community entbrennt hierbei zumeist über dem sich zu langsam entwickelnden „Core Plugin System“, nämlich dem Teil der offiziellen Plugins, die eng mit der NAGIOS-Engine an sich verzahnt sind und gänzlich von einer kleinen Entwicklergruppe um Ethan Galstad weiterentwickelt werden. Von der Community wird immer wieder bemängelt, dass diese „Core Plugins“ und die Schnittstellen der NAGIOS Engine, weit hinter der Dynamik der inoffiziellen Community-Plugins zurückbleiben und so ein schnelles Voranschreiten der Entwicklung einschränken. Als Folge dieser Verstimmungen spalteten sich im Mai 2009 mehrere Mitglieder der Nagios Community ab und begannen die Entwicklung eines NAGIOS-„Fork“ mit Namen ICINGA [25]. „Fork“ steht hierbei für die Abspaltung und Parallelentwicklung eines Software Projekts. In diesem „Fork“ wurde als wichtigster Unterschied zum Ur-NAGIOS eine API zur Entwicklung von Plugins implementiert. Wenngleich dieses Projekt internationale Unterstützung erfährt, scheint hier jedoch aus aktueller Sicht ein kommerzieller Faktor die ausschlaggebende treibende Kraft für die Abspaltung gewesen zu sein. Die den Kernentwicklern von ICINGA nahestehende Firma vermarktet, ähnlich wie die von NAGIOS-Gründer Ethan Galstad gegründete Firma, Mehrwertdienste und Supportdienstleistungen in Zusammenhang mit den Softwaresystemen ICINGA und NAGIOS.

5.3. Die Konfiguration von NAGIOS

Das Konfigurationsparadigma von NAGIOS ist leider nicht einheitlich, sondern im Laufe der Entwicklung erst so angepasst worden, dass NAGIOS in die Lage versetzt wurde, auch in großen Computernetzwerken eingesetzt werden zu können. Im ersten Konfigurationskonzept von NAGIOS ist für jeden zu überwachendem Host eine Konfigurationsdatei vorgesehen, die seine zu überwachenden Eigenschaften festlegt. Später wurde über dieses Konzept eine Objektorientierung gelegt, die es möglich machte, Eigenschaften für eine Klasse von Hosts festzulegen und diese dann auf beliebig viele Hosts zu vererben. In einem weiteren Entwicklungsschritt wurden Templates definiert, die verschiedene Host-Klassendefinitionen zur Verfügung stellen.
Es sei auch angemerkt, dass es mit Hilfe von Plugins möglich ist, durch eine automatisierte Netzwerkerkundung entfernte Hosts zu finden, in eine Konfiguration einzufügen und dann mit Hilfe eines geeigneten Templates abzufragen. Ein solches Template würde typischerweise diejenigen Werte eines Hosts abfragen, die keine weitere Installation von Überwachungsprogrammen, etwa eines NRPE-Agenten, auf einem entfernten Host erfordern. Zu nennen wäre hier konkret die Eigenschaft, ob der Host zu einem bestimmten Zeitpunkt erreichbar ist - ein sogenannter „Alive“-Check mittels ICMP Echo Request- und Echo Reply-Funktionalität - und wie viele Millisekunden die Antwort auf den ICMP-Echo Request benötigt.
Im realen Umfeld wird diese Funktionen aber weniger von Interesse sein, da es zur schnellen Übersicht über ein unbekanntes Netzwerk durch vollautomatische oder automatisierte Erkundung leichter zu installierende und bedienende Tools gibt. Daher wird solch ein Plugin dort vielmehr als „Gimmick“ anzusehen sein.

Die übliche Konfigurationsmethode von NAGIOS ist dementsprechend die manuelle Festlegung der zu überwachenden Hosts – dies können natürlich auch alle anderen existierenden

Netzwerkgeräte sein, sofern Nagios ein geeignetes Plugin bietet, um von diesen eine für das Monitoring interessante Kenngröße zu überwachen.
In einem typischen Anwendungsfall wird für jede Gruppe von Netzwerkgeräten eine eigene Klasse definiert, um zu beschreiben, was es in dieser Gruppe zu überwachen gilt. Dabei wird gleich implizit behandelt, über welche Möglichkeiten der Überwachung das entsprechende Gerät verfügt. Die bei einer solchen Definition zur Anwendung kommenden NAGIOS Schlüsselwörter sind „Hosts“ – zur Definition der Gerätenamen oder IP-Adressen und „Services“ - zur Definition der zu überwachenden Dienste. Welche Dienste hier zur Verfügung stehen, hängt natürlich von den Möglichkeiten des entsprechenden Gerätes ab. Ein Switch oder eine Appliance wird dabei wegen der meist proprietären Betriebssystemsoftware meist nur über das, auf fast jedem dieser Geräte, implementierte SNMP Protokoll überwachbar sein. Auf einer Workstation oder einem Server steht zusätzlich die Möglichkeit zur Verfügung, einen der zuvor beschriebenen Nagios Agenten zur Anwendung zu bringen. Mit einem solchen wird es möglich, auch andere Eigenschaften eines Computers, wie Auslastung, Speicherplatz oder auch interne Fehlermeldungen sowie den Status von RAID-Systemen auszulesen.
Hier entfernt sich das Programmsystem NAGIOS zwar vom Network Monitoring, jedoch muss festgestellt werden, dass ein fehlerfreier interner Zustand eines Servers, der eine funktionale Rolle in einem Netzwerk einnimmt, natürlich wichtige Aussagen über die Funktionsfähigkeit und Belastbarkeit dieses im Netzwerk angebotenen Dienstes liefert.

Ein Beispiel zur Verdeutlichung: Wenn die Hauptfunktionalität eines lokalen Netzwerks in der Erbringung eines WWW Dienstes für das Internet besteht und der betreffende Server eine ständige Auslastung von 75% erfährt, so sollte dieser Server aufgrund seines inneren Zustands, auch wenn er den Dienst zu erbringen in der Lage ist, trotzdem nicht als „grün“ für „vollkommen in Ordnung“, sondern viel mehr als „gelb“, nämlich genauere Kontrolle nötig, markiert werden.

Dieses Beispiel zeigt, dass die Nutzung von Netzwerküberwachungswerkzeugen in der Praxis sehr oft über die reine Aufzeichnung von Netzwerkzuständen hinaus geht. Dies liegt zum einen daran, dass die Netzwerküberwachungswerkzeuge die Abfragemöglichkeiten für eine vielseitige Nutzung meist schon mitbringen und aufgrund deren modularen Aufbaus die Diversifikation bei den Plugins sehr schnell voranschreitet, zum anderen ist es meist die Netzwerküberwachung, die in vielen Unternehmungen, die Einführung einer Monitoring Software nötig macht und andere Bereiche, in denen Überwachung von Software oder Hardware vorteilhaft ist, nutzen dann die schon vorhandene Infrastruktur. Als Beispiel hierfür zu nennen, ist etwa die Überwachung von Füllständen von Druckern oder Kopierern per SNMP, welches standardmäßig in nahezu allen Netzwerkdruckern implementiert ist. Auch genannt werden kann hier die Überwachung der Verfügbarkeit von Serverdiensten oder Rechnern die für Zugangskontrolle oder Zeitnahme in Büroräumen zuständig sind.

Ein weiteres inzwischen verbreitetes und als Standard anzusehendes Einsatzgebiet von Network Monitoring Software liegt in der Auswertung von Umgebungsparametern. Meist in Form einer Einsteckkarte, die mit externen Sensoren verbunden ist oder über vorhandene externe Anschlüsse, werden hierbei bestimmte physikalische Messwerte der Serverumgebung ermittelt und anhand der bei NAGIOS üblichen Kenngrößen für „Normal“, „Warnung“, „Fehler“ eingestuft und ausgegeben. Üblicherweise werden Umgebungstemperatur und Luftfeuchtigkeit überwacht.
Ein letztes Beispiel für die Inanspruchnahme des Network Monitoring System NAGIOS zur Überwachung von Gegebenheiten, die nicht primär Netzwerkeigenschaften sind, ist die Kon-

trolle der Stromversorgung. Auch diese sollte bei jedem Rechenzentrum oder auch einfach beim Betrieb eines Serverraums zum Standard gehören. Als Anmerkung sei gesagt, dass die Überwachung des Netzstroms meist von proprietärer Software übernommen wird, die hierzu ihre eigene Datenhaltung betreibt. Es sind jedoch Plugins verfügbar, um dies zum Beispiel zusätzlich und in der Praxis dann meist parallel auch in der eigenen Nagios-Umgebung zu protokollieren und zur Anzeige zu bringen.

Im hier vorgestellten Programmsystem wird NAGIOS zum Einsatz gebracht, um die Konfiguration vorzustellen, sowie um einen schnellen Überblick über die erstellte VNUML-Simulation zu erhalten. Um dies umzusetzen wird eine immer vorhandene Eigenschaft der VNUML-simulierten Netze benutzt, nämlich die sogenannte Management-Schnittstelle jedes VNUML-Hosts. Diese liegen in dem schon vor Erstellung einer Simulation bekannten Management-Netzwerk. Anhand einer einfachen Regelung, die vorsieht, dass für jeden VNUML-Host drei IP-Adressen zur Verfügung stehen, lässt sich einfach hochzählen, auf welche IP-Adresse die jeweilige Management-Schnittstelle eines Hosts fällt. Aufgrund dieser Eigenschaft wurden in der implementierten NAGIOS-Überwachung bereits die Management-Schnittstellen von zehn VNUML-Hosts vordefiniert.
Um dem geneigten Benutzer darüber hinaus die Funktion von Netzwerk-Überwachungsprogrammen näher zu bringen und um den Einsatz zum Zwecke der Lehre am Labor für Rechnernetze der Universität Koblenz zu ermöglichen, werden weiterhin verschiedene Server des Rechenzentrums der Universität sowie Server des Labors für Rechnernetze überwacht.
Hierbei wurden der Aufgabe des Servers entsprechende, zu überwachende Dienste ausgewählt. Es sind dies in tabellarischer Form:

Host	Port	Protokoll	Funktion
Deliver	25	SMTP	Email senden an Server, Emailverkehr zwischen Servern
Harvey	22	SSH	Secure Shell mit verschlüsselter Datenübertragung
Mail	143	IMAP4	Netzwerkdateisystem zum Zugriff auf Email-Ordner
	110	POP3	Email-Abruf für Clients von Email-Servern
Newshost	119	NNTP	Abrufen von News aus Newsgroup-Ordnern
Ns1	53	DNS	Namensauflösung
Ns2	53	DNS	Namensauflösung
Openldap	636	LDAP	Abfrage und Änderung in Verzeichnisdiensten
Printhost	631	CUPS	Senden von Druckaufträgen, Statusabfrage der Drucker
Rnetserver	80	HTTP	Abruf von Webseiten, hier: Gitorious Web Interface
	5222	JABBER	Instant Messenger Server
Vrn	80	HTTP	Web-Interface zur Verwaltung des KVM-QEMU
Winroute	22	SSH	Secure Shell mit verschlüsselter Datenübertragung
Www	80	HTTP	Webseiten der Universität Koblenz-Landau

Abb. 24: Überwachte Server der Universität Koblenz und deren funktionale Ports, vordefiniert im NAGIOS-System des Cheops für VNUML Programmpakets.

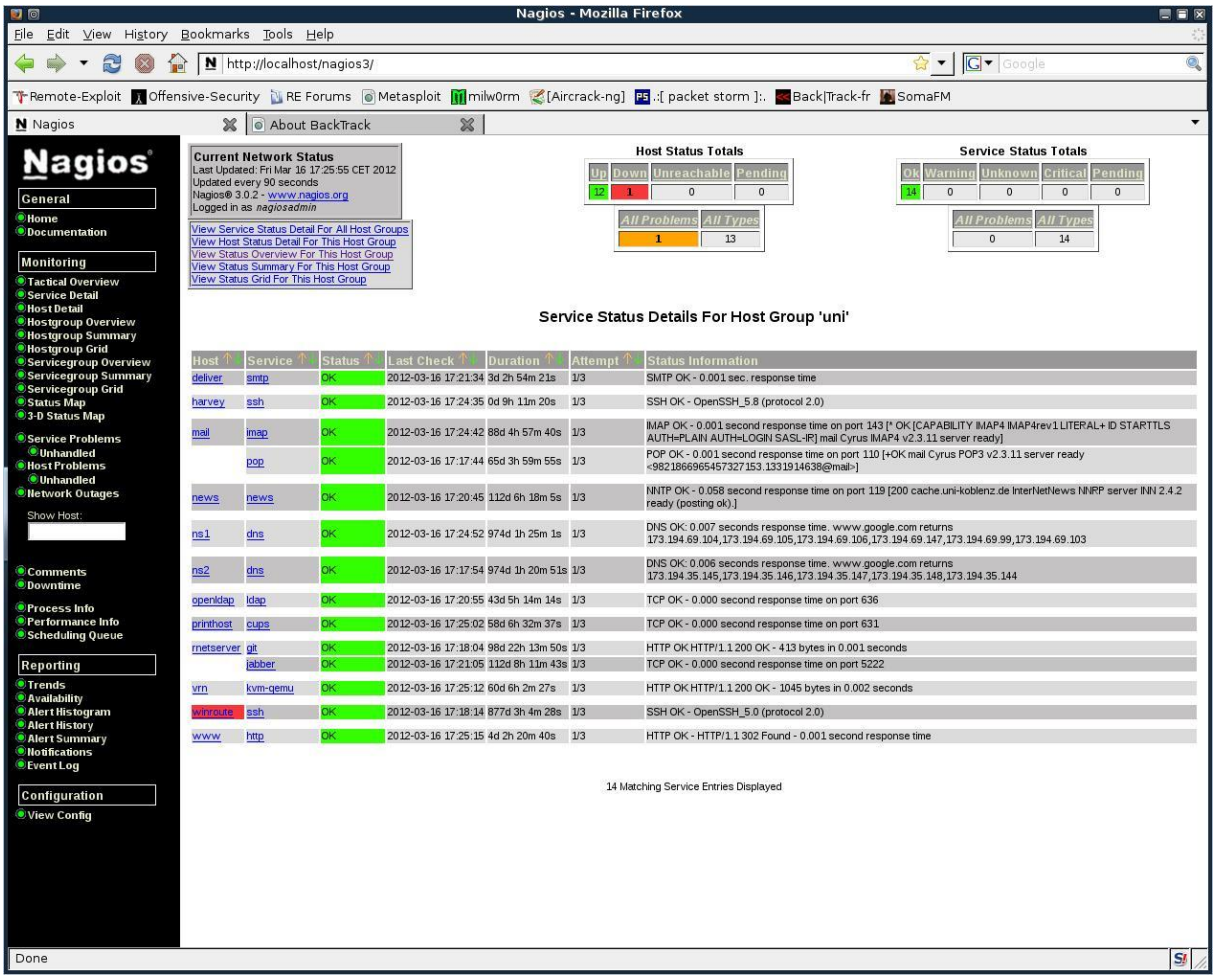


Abb. 25: Ausgabe der Überwachung der in Abbildung 23 angegebenen Server. Das Feld „Status Information“ liefert jeweils weitere Details der gemessenen Werte.

6. SNMP Monitoring und die Software CACTI

Das Simple Network Monitoring Protocol (SNMP) [28] ist ein standardisiertes Netzwerkprotokoll um verschiedenste Geräte per Netzwerk zu überwachen. Es ist das am weitesten verbreitete Protokoll mit dieser Funktion und wird in nahezu allen Netzwerkkomponenten mit verschiedenem Umfang implementiert.

Im Grundkonzept sieht SNMP sowohl das Auslesen von Parametern, welche in einer standardisierten Reihenfolge und Wertebereichen festgelegt sind, die Benachrichtigung von Fehlerzuständen und deren Fehlermeldungen, als auch das Setzen von Parametern im Netzwerkgerät, vor. In der Realität wird die Funktion, Einstellungen über SNMP zu setzen, jedoch meist nicht angeboten. Dies bieten die großen Geräteanbieter meist in proprietären Protokollen für ihre eigenen Monitoring-Lösungen wie etwa Tivoli der Firma IBM, Openview der Firma Hewlett Packard oder Ciscoworks der Firma Cisco an.

Weitere Gründe für die wenig genutzte Möglichkeit, Geräte über SNMP steuerbar zu machen, sind die meist fehlende Authentifizierung nach der SNMP Version 2, beziehungsweise die nach heutigem Maßstäben nicht mehr zureichende Festigkeit der Verschlüsselung.

Es gibt seit langem eine ganze Reihe von Werkzeugen, um die sogenannte Management Information Base (MIB) eines Gerätes auszulesen. Hierin befinden sich in definierter Reihenfolge bestimmte auslesbare Parameter des Gerätes. Um ein Gerät wirklich überwachen zu können ist es nötig, die ausgelesene Information in Echtzeit zu Überwachungszwecken anzuzeigen oder die Werte zu speichern und zu Überwachungszwecken abrufbar zu archivieren.

Um dies praktikabel umzusetzen entstanden mehrere, heute sehr weit verbreitete Web-Applikationen, die sowohl die Anzeige aktueller Daten, als auch die Speicherung und ausgewertete Anzeige von Daten aus einem gewählten Zeitraum, zu liefern imstande sind.

Fast alle dieser langfristig am Markt befindlichen Programme, teilweise über 10 Jahre, nutzen im Hintergrund eine Open Source Software mit der Bezeichnung RRDTOOL[8] [26]. Diese Programmsammlung erlaubt das Anlegen von sich zyklisch wieder überschreibenden Datendateien und Hilfsmittel zu deren grafischer Auswertung.

Programme die dieses Programmpaket nutzen sind etwa MRTG, PRTG, MUNIN und CACTI. Das Programm CACTI soll hier näher beleuchtet werden. Es benutzt neben der Informationserhebung über SNMP-Abfragen auch die Ausführung von Shell-Skripten oder PERL [27] Programmen auf dem zu überwachenden Gerät soweit dieses ein geeignetes Betriebssystem ausführt. Die Daten legt CACTI in einer modernen MySQL-Datenbank ab.

8: RRD steht für Round Robin Database

Die Konfiguration von CACTI erfolgt über Einstellungsdateien, ähnlich dem schon vorgestellten Programm NAGIOS. In CACTI können diese komfortabel über Web-Formulare zusammengestellt werden. Hierbei werden zuerst die abzufragenden Geräte anhand ihrer IP-Adressen registriert, für jedes Gerät können dann weitere Eigenschaften festgelegt werden, etwa die Häufigkeit des Abrufs oder die implementierte Abrufmethode. Natürlich können auch die abzurufenden Parameter festgelegt werden.

Genau wie das Programmpaket NAGIOS implementiert auch CACTI in seinen neuen Versionen ein Plugin System, welches sowohl weitere Abfragearten für entfernte Systeme, wie auch die Möglichkeit zur Abfrage von Umgebungsparametern zur Verfügung stellt.

Eine wichtige neue Eigenschaft, die erst im Plugin-System für CACTI verfügbar wurde, ist die Festlegung von kritischen Wertebereichen in denen das CACTI-System für das betreffende Gerät einen Warnzustand auslöst um daraufhin eine vorher festgelegte Warnungs- oder Benachrichtigungsfunktion ausführen zu können. Dies kann wie beim System NAGIOS sowohl eine Warnmeldung per Email oder per Instant Messenger sein.

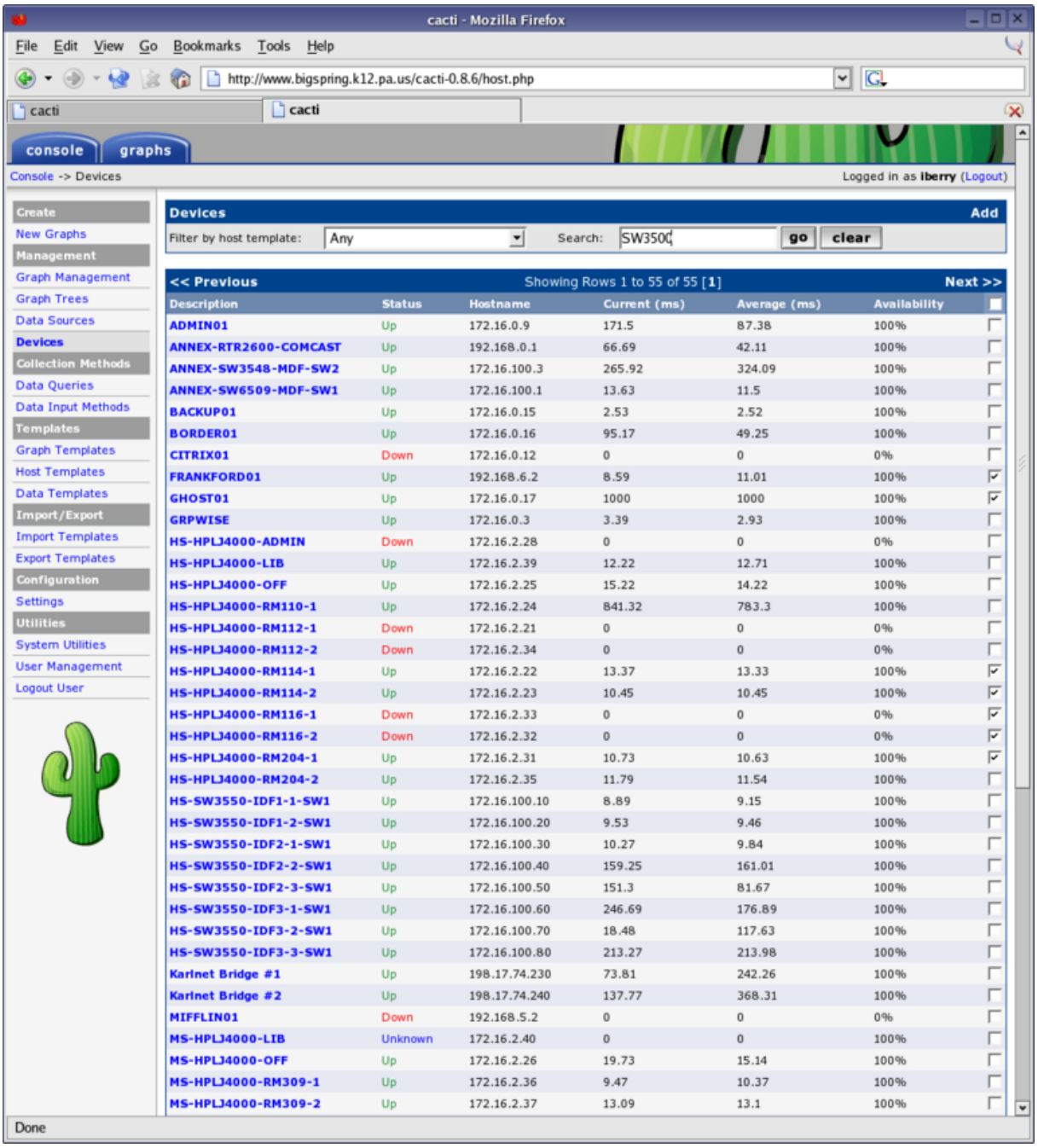


Abb. 26: CACTI-Auswertung von Zugangsgeräten, Servern und Peripherie vom Pittsburgh Supercomputing Center aus deren CACTI Howto.

7. Das RRDTOOL und die Software MRTG

Eine weitere Anwendung zur Netzwerküberwachung, die zwar inzwischen in Ihrem Funktionsumfang von anderen Systemen überholt wurde und auch ein bekanntes Nachfolgeprojekt besitzt, ist die von Tobias Oetiker et al. entwickelte Software Multi Router Traffic Grapher (MRTG) [30].

Diese Software wird heute noch manchmal als kompakte Lösung zur Speicherung und grafischen Aufbereitung von Netzwerkverkehrsdaten benutzt. Ihre Verbreitung fand sie schon in den 90er Jahren. In den meisten Projekten wird die Software nur modular benutzt, durch die zu geringe Leistungsfähigkeit, hat sich ein Nachfolgeprojekt gebildet, welches das Original inzwischen im Funktionsumfang deutlich überholt und in vielen Projekten ersetzt hat. Dies ist die Software RRDTOOL, die ebenfalls von einer Community um Tobias Oetiker entwickelt wurde. Wie die Software MRTG wird auch RRDTOOL in vielen Projekten eingesetzt um Daten, wie etwa Netzwerkverkehrsdaten, in einem Umlaufsystem abzulegen[9]. Dabei werden nach einem festzulegenden System ausgehend von Zeit oder Volumen, die Daten nach bestimmten Kenngrößen überschrieben, so dass sich die insgesamt zu speichernde Datenmenge ab einem bestimmten Zeitpunkt oder einer bestimmten Menge nicht mehr vergrößert.

Die Software RRDTOOL wird zum Beispiel im zuvor beschriebenen Softwaresystem CACTI verwendet.

Eine bekannte Abspaltung des MRTG ist ein System mit kommerziellem Hintergrund, PRTG der Firma Paessler. Diese bot zu Beginn ihrer Tätigkeit einen kostenpflichtigen Support für Ihr System an - vergleichbar mit der Supportfirma zum System NAGIOS - inzwischen wurde der Code jedoch neu implementiert und steht nunmehr nicht mehr unter Open Source. Dieses System soll hier genannt werden, da es eines der wenigen ist, das ebenfalls Möglichkeiten zur automatischen Erkennung der Netzwerkgeräte anbietet. Ansonsten bietet es weitere „Gimmicks“, die zwar im originalen MRTG nicht vorhanden sind, aber sehr wohl im großen Plugin-Angebot von NAGIOS zu finden sind. Als Beispiel sei hier ein Überwachungsapplet für Smartphones erwähnt. Seine Konkurrenten sieht Paessler selbst jedoch mehr in den kommerziellen Systemen der großen Hersteller, wie HP Openview, IBM Tivoli oder Cisco Ciscoworks.

Als Beispiel für eine MRTG-Überwachung soll die im nachfolgenden dargestellte Ausgabe des Internet-Knotenpunktes DECIX dienen. Sie zeigt den Internetverkehr in den MRTG Standardansichten: „Täglich“, „Wöchentlich“, „Monatlich“, „Jährlich“ den der Knotenpunkt DECIX, aktuell zum Zeitpunkt dieser Arbeit, für das Autonome System des RLP-NET, also des Dienstleistungsnetzes der Behörden und Einrichtungen des Landes Rheinland-Pfalz, an das auch die Universität Koblenz angeschlossen ist, aufgezeichnet hat.

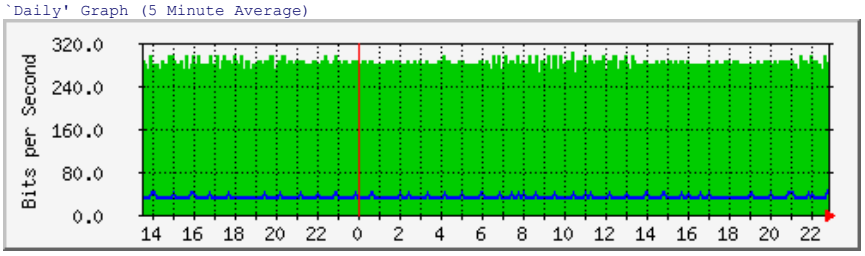
9: daher der Name RRDTOOL – Round Robin Data, meist übersetzt mit Umlaufdaten

MAC traffic for g-decix-1.rlp-net.net (AS2857)

Peer Name: g-decix-1.rlp-net.net
IP address: 80.81.192.8
Mac address: 000b.45a8.65c0
Peer AS: 2857

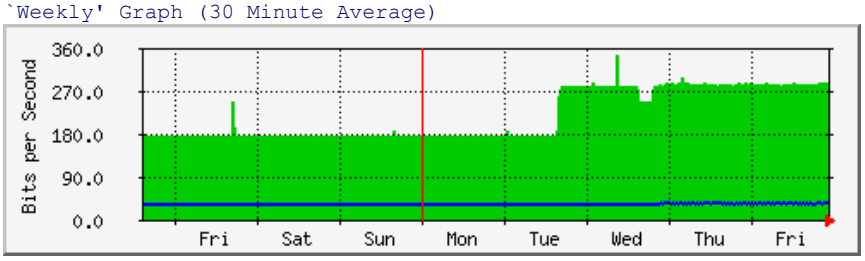
The statistics were last updated **Friday, 16 March 2012 at 22:48,**
at which time **'peer1.fra4.ix.f'** had been up for **270 days, 1:31:37.**

`Daily' Graph (5 Minute Average)



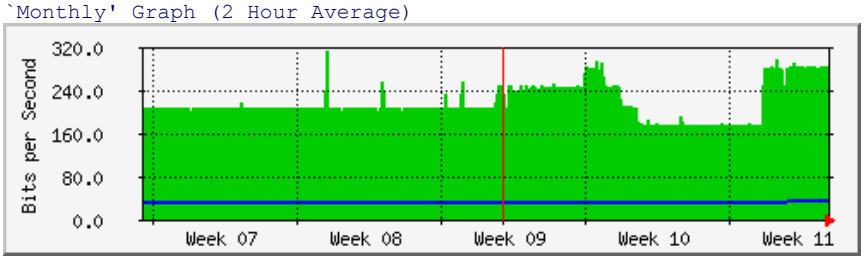
	Max	Average	Current
In	304.0 bps (0.0%)	280.0 bps (0.0%)	280.0 bps (0.0%)
Out	40.0 bps (0.0%)	32.0 bps (0.0%)	40.0 bps (0.0%)

`Weekly' Graph (30 Minute Average)



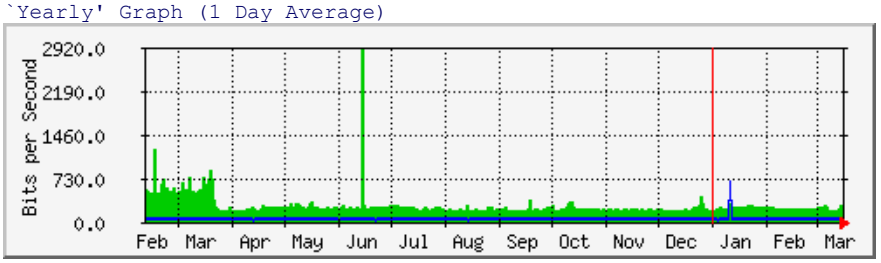
	Max	Average	Current
In	344.0 bps (0.0%)	216.0 bps (0.0%)	288.0 bps (0.0%)
Out	32.0 bps (0.0%)	32.0 bps (0.0%)	32.0 bps (0.0%)

`Monthly' Graph (2 Hour Average)



	Max	Average	Current
In	312.0 bps (0.0%)	216.0 bps (0.0%)	288.0 bps (0.0%)
Out	32.0 bps (0.0%)	32.0 bps (0.0%)	32.0 bps (0.0%)

`Yearly' Graph (1 Day Average)



	Max	Average	Current
	2888.0 bps (0.0%)	264.0 bps (0.0%)	280.0 bps (0.0%)
	648.0 bps (0.0%)	32.0 bps (0.0%)	32.0 bps (0.0%)

GREEN ### Incoming Traffic in Bits per Second
BLUE ### Outgoing Traffic in Bits per Second

2.14.7
Tobias Oetiker <tobi@oetiker.ch>
and Dave Rand <dlr@bungi.com>

Abb. 27: MRTG Ausgabe der DECIX Statistik über das Peering mit dem Autonomen System RLP-NET.

8. Fazit

Das in dieser Arbeit erstellte Programmpaket, Cheops für VNUML, versetzt den Benutzer in die Lage, durch Aktionen in einer grafischen Benutzeroberfläche (GUI), alle nötigen Schritte zu unternehmen, um die Simulation eines Netzwerks mit der Simulationssoftware Virtual Network User Mode Linux (VNUML) zu unternehmen. Der Benutzer kann dabei sowohl auf die schriftliche Erstellung von VNUML-Topologiedateien in XML, als auch auf den manuellen Programmaufruf verzichten. Die GUI übernimmt darüber hinaus nicht nur die Erstellung eigener Netzwerktopologien zum Zwecke der Simulation, sondern verbindet eine erstellte Simulation auch mit benachbarten physikalischen Netzwerken.
Hierzu nutzt das Programm Funktionen, die die Ursprungssoftware besonders vor anderen Netzwerküberwachungsprogrammen ausgezeichnet hat. In einer Erhebung wurden auch andere Softwaresysteme aus dem Bereich Netzwerküberwachung betrachtet und kurz vorgestellt.
Der bekannteste Vertreter dieser Softwaregattung, das Programm NAGIOS, wird verwendet, um die mit Cheops für VNUML durchgeführten Simulationen überprüfen zu können.
Das Programm ist eingebettet in die Linux-Distribution Backtrack, die weitere Software beinhaltet, die sich zur Analyse einer Netzwerksimulation eignen. Auch auf diese wurde eingegangen.
Der Anwender erhält mit dieser Arbeit eine Anleitung, die ihm die Fähigkeit vermittelt, das Programmsystem Cheops für VNUML bei eigenen Simulationsprojekten anzuwenden. Die Zielgruppe, an die sich das Programm richtet, sind hierbei Studenten, die das Programm zur Erstellung von rudimentären Netzwerken benutzen können. Ein zusätzlicher Effekt liegt im anschaulichen Begreifen von Netzbereichen, denn jeder erzeugte Host wird automatisch an das korrekte Subnetz angezeichnet. Werden Fehler beim Bestimmen der Adressen eines Subnetzes gemacht, so sind diese schnell ersichtlich und können korrigiert werden, noch bevor die erstellte und womöglich fehlerhafte Topologie durch VNUML simuliert wird.
Das Programm Cheops für VNUML ist ebenfalls geeignet, um als Hilfsmittel bei aufwendigen Simulationen benutzt zu werden. So ist es auch als Werkzeug im Labor der AG Rechnernetze einsetzbar. Hier sind besonders die Möglichkeiten zu nennen, beliebig komplexe VNUML-Topologiedateien zu laden und sie vor der Simulation in der GUI in Augenschein zu nehmen und auf Fehler zu überprüfen, beziehungsweise die Fähigkeit, eine Simulation mit wenigen Mausklicks an ein externes, physikalisches Netzwerk anzubinden, etwa das bestehende experimentelle Netzwerk von OpenWRT Routern.

Abbildungen und Tabellen

Weiterführende Literatur und Quellen

[1] VNUML in der Deutschen Wikipedia
Stand: 20.03.2012
http://de.wikipedia.org/wiki/VNUML

[2] VNUML an am Institut für Telekommunikationswesen der Polytechnischen Universität Madrid, Spanien
Stand: 20.03.2012
http://neweb.dit.upm.es/vnumlwiki/index.php/Main_Page

[3] User Mode Linux, Projektseite auf Sourceforge
Stand: 20.03.2012
http://user-mode-linux.sourceforge.net/

[4] VNUML Startseite der Arbeitsgruppe Rechnernetze der Universität Koblenz
Stand: 20.03.2012
http://www.uni-koblenz.de/~vnuml

[5] Folien zur Vorlesung Intra Domain Routing an der Universität Berkeley
Stand: 20.03.2012
http://walrandpc.eecs.berkeley.edu/intradomain.pdf

[6] Projektseite zum Routing Algorithmus RMTI an der Universität Koblenz
Stand: 20.03.2012
http://userp.uni-koblenz.de/~vnuml/rmti/

[7] RIPv2 RFC 2453, in der Sammlung der Internet Engineering Task Force
Stand: 20.03.2012
http://tools.ietf.org/html/rfc2453

[8] Das Count to infinity Problem in Distanzvektor Routing Algorithmen
James F. Kurose, Keith W. Ross: Computernetzwerke: Der Top-Down-Ansatz, Pearson Studium, 4. aktualisierte Auflage (1. September 2008), S. 425

[9] Cheops Version 0.61 in der Hilfesammlung der Distribution Ubuntu.
http://manpages.ubuntu.com/manpages/hardy/man8/cheops.8.html

[10] Im Sinne des englischen Begriffs „mission statement“, vgl. Tim Barry
Stand: 20.03.2012
http://articles.bplans.com/writing-a-business-plan/mantra-mission-statement-or-vision/249

[11] Cheops-NG auf der Projektseite bei Sourceforge
Stand: 20.03.2012
http://cheops-ng.sourceforge.net/index.php

[12] Kurzbeschreibung zu Netzwerk Socket in der englischen Wikipedia
Stand: 20.03.2012
http://en.wikipedia.org/wiki/Network_socket

[13] Sammlung der reservierten Adressbereiche in der englischen Wikipedia
Stand: 20.03.2012
http://en.wikipedia.org/wiki/Reserved_IP_addresses

[14] RAW Socket Programmierung und Einsatzfelder, Studienarbeit André Volk, 2008
http://kola.opus.hbz-nrw.de/volltexte/2008/316/pdf/studienarbeit_oneside.pdf
Stand: 20.03.2012

[15] Absichern eines nicht besonders geschützten TCP/IP Stack, aus Microsoft MSDN
Stand: 20.03.2012
http://msdn.microsoft.com/de-de/library/ff648853.aspx

[16] Offizielle Webseite der Backtrack Distribution
Stand: 20.03.2012.
http://www.backtrack-linux.org/

[17] Backtrack Eintrag in der deutschen Wikipedia mit vielen weiterführenden Links
Stand: 20.03.2012
http://de.wikipedia.org/wiki/BackTrack

[18] Abschnitt über Historie und Zukunft auf der Webseite des NMAP Projektes
Stand: 20.03.2012
http://nmap.org/book/history-future.html

[19] Zusammenfassung zum Thema Portscanner auf der deutschen Wikipedia-Seite
Stand: 20.03.2012
http://de.wikipedia.org/wiki/Portscanner

[20] Zusammenfassung über Netzwerk-Sniffer auf der deutschen Wikipedia-Seite
Stand: 20.03.2012
http://de.wikipedia.org/wiki/Sniffer

[21] Zusammenfassung zum OSI-Modell auf der deutschen Wikipedia-Seite
Stand: 20.03.2012
http://de.wikipedia.org/wiki/OSI-Modell

[22] Heimseite des ETTERCAP Projekts auf Sourceforge
Stand: 20.03.2012
http://ettercap.sourceforge.net/index.php

[23] Zusammenfassung und Wortlaut des Hacker-Paragraphen auf der deutschen Wikipedia-Seite
Stand: 20.03.2012
http://de.wikipedia.org/wiki/Hackerparagraf

[24] Offizielle Projektseite von NAGIOS, die Firma des Entwicklers bietet hier kostenpflichtigen Support und weitere Mehrwertdienste an
Stand: 20.03.2012
http://www.nagios.org/

[25] Offizielle Projektseite des NAGIOS-Fork ICINGA
Stand: 20.03.2012
https://www.icinga.org/

[26] Projektseite von RRDTOOL
Stand: 20.03.2012
http://oss.oetiker.ch/rrdtool/

[27] Projektseite von PERL
Stand: 20.03.2012
http://www.perl.org/

[28] SNMP in der englischen Wikipedia
Stand: 20.03.2012
http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

[29] Herunterladbares Image für USB-Sticks: Cheops für VNUML
Stand: 20.03.2012
http://agrn.uni-koblenz.de/projects/vnumlcheops

[30] Offizielle Projektseite von MRTG
Stand: 20.03.2012
http://oss.oetiker.ch/mrtg/

[31] Zusammenfassung und weiterführende Links zu VDE-Switches auf der Wikipedia-Seite der AG Rechnernetze der Universität Koblenz
Stand: 20.03.2012
http://agrn.uni-koblenz.de/wiki/index.php/Virtual_Distributed_Ethernet_Switch

[32] Zusammenfassung zum Thema Speicherabbild in der deutschen Wikipedia, im allgemeinen Sprachgebrauch wird oft der englische Begriff Image verwendet.
Stand: 20.03.2012
http://de.wikipedia.org/wiki/Speicherabbild

[33] Linux-Manpage zu Cheops 0.61 aus der Archivsammlung auf pwet.fr
Stand: 20.03.2012
http://pwet.fr/man/linux/administration_systeme/cheops

[34] SYSLINUX in der deutschen Wikipedia
Stand: 20.03.2012
http://de.wikipedia.org/wiki/SYSLINUX

[35] Damn Vulnerable Linux (DVL) in der deutschen Wikipedia
Stand: 20.03.2012
http://de.wikipedia.org/wiki/Damn_Vulnerable_Linux