swisscom

HTW Chur
Hochschule für Technik und Wirtschaft

Fachhochschule Ostschweiz
University of Applied Sciences

Von Merens Decasper, Bruno Studer, Valentin Hitz,
R.Berther, M.Gafner, B.Cajacob, R.Lanicca

Datum 19.03.2001

Thema Praktika - Aufgabe C15

zur Kenntnis

geht an

Internet Sicherheit – Firewall und IDS

© Art by Giorgio Cavazzano

Swisscom AG
Telecom Labor
Ringstrasse 34
7000 Chur

Gratisnummer 0800 800 113
Telefon +41 81 286 37 37
Telefax +41 81 286 37 38

Standortadresse:
Ringstrasse 34
7000 Chur
E-Mail:
info@tlab.ch

Inhaltsverzeichnis

1 Kurzbeschreibung der Aufgabe

Im Rahmen dieses Praktikums lernen Sie in einem theoretischen Teil die Grundlagen zur Sicherheit im Internet kennen und erhalten eine Übersicht verfügbarer Produkte. Die erarbeiteten Kenntnisse aus dem Theorieteil werden anschliessend im praktischen Teil angewendet.

Der erste praktische Teil "Unix-Networking" soll Ihnen einen Einstieg in Unix-Netzwerkkonfiguration geben. Im folgenden Abschnitt lernen Sie das kommerzielle Firewall-Produkt " FireWall-1" kennen, welches in der Praxis vielerorts eingesetzt wird. Sie nehmen dazu einige Konfigurationen vor und testen diese jeweils aus. Für diese Aufgabe sind 4 Std. vorgesehen.

Im zweiten Praktischen Teil „Intrusion Detection Systems“ (IDS) lernen Sie ein mächtiges Programm von der Firma ISS (Internet Security Systems) kennen. Real Secure 5.0, welches momentan **das** Tool für Intrusion Detection ist. In den Aufgaben können einige Angriffe getätigt werden, um RealSecure auszutesten und kennenzulernen.

In der Nachbearbeitung haben Sie dann die Gelegenheit, einige interessante Fragen zu diskutieren. Wenn immer Sie einen Begriff nicht kennen, so schlagen Sie doch einfach im Anhang nach.

1.1 Hinweise

1.1.1 Für Besucher aus dem Internet

Dieser Arbeitsplatz ist das Resultat einer Diplomarbeit von R. Berther / M. Gafner im Herbst 1996 (Firewall). Die Diplomarbeit wurde ergänzt und erneuert durch eine Semesterarbeit von B. Cajacob / R. Lanicca mit Intrusion Detection Systems (IDS).

Die Anleitung ist abgestimmt auf die im Labor zur Verfügung stehende Infrastruktur und benützt deshalb Frames, Java und Style Sheets. Die meisten der Aufgaben lassen sich aber auf einem beliebigen UNIX Rechner durchführen wobei an einigen Stellen root Zugriff nötig ist.

1.1.2 Zur Durchführung im Labor

Für die Dürchführung des Firewall Praktikums werden die Rechner *fw* und *peru* benötigt. Der Rechner *djibouti* wird erst beim Lösen der IDS-Aufgaben eingesetzt.

Die genauen Bezeichnungen und Passwörter sind einem Beiblatt am Arbeitsplatz zu entnehmen. Falls in den Lösungen Hostnamen und IP Adressen angegeben sind gelten diese als Beispiel. Das Menu auf diesen Seiten wurde mit Jwalk version 2.2 von InterAxtion erstellt. Wenn Sie Fragen und Anregungen haben wenden Sie sich bitte an Bruno.Studer@fh-htwchur.ch oder info@tlab.ch.

2 Einleitung und Lernziele

Wenn man heute von Internet spricht, so stösst man meist auf Begriffe wie WWW, Surfen, FTP, eMail und vielleicht sogar noch auf Sicherheit im Internet. Letzteres ist für den einzelnen Privatbenutzer des Internets nicht von grosser Bedeutung. Für Anbieter kommerzieller Dienste und Industriebetriebe auf dem Internet ist Sicherheit meist von höchster Priorität. Kleinbetriebe koppeln z.B. Teilnetze der verschiedenen Filialen über das Internet oder ermöglichen Aussendienstmitarbeitern Fernsitzungen auf ihrem lokalen Rechenzentrum abzuhalten. Bei Grossbetrieben ist die Problematik ähnlich, auch sie nutzen die vielen Möglichkeiten, welche das Internet bietet. Dabei sind die nötigen Vorkehrungen zu treffen, damit firmeninterne Daten vor unerlaubtem Zugriff oder gar Zerstörung geschützt sind. Man versucht also, sich vom Internet abzuschotten, quasi eine dicke Mauer zwischen das interne Netz (Intranet) und das Internet zu stellen.

Solche Mauern nennt man "Firewall". Firewalls sind Gebilde, welche sich an die Anforderungen des jeweiligen zu schützenden Netzes anpassen lassen. Sie überwachen dann den Datenverkehr von und zum Internet.

Nach der Installation der Firewall kann man sich aber nicht darauf verlassen, dass das System für immer und ewig vor „Einbrecher“ sicher ist. Darum muss ein Tool eingesetzt werden, welches das System ständig überwacht. Ein solches Tool nennt man IDS (Intrusion Detection System). Bei uns wird Real Secure 5.0 von ISS (Internet Security Systems) eingesetzt.

Das Sicherheitssystem (Firewall+IDS) kann man sich vorstellen, wie wenn die Firewall die Türe zu einem Haus ist und das IDS die Alarmanlage. Zur Tür (Firewall) kommen nur erwünschte Teilnehmer rein. Kommt aber jemand von Fenster ins Haus muss die Alarmanlage (IDS) einspringen und die nötigen Massnahmen ergreifen.

Nach der Durchführung dieses Praktikums sollten Sie folgende Lernziele erreicht haben:

- Notwendigkeit von Sicherheit kennen
- Wichtige Sicherheitsaspekte kennen
- Ein einfaches Sicherheitskonzept erstellen können
- Das Prinzip einer Firewall kennen
- Den Unterschied zwischen Proxy/Paket-Filter kennen
- Einige Evaluationskriterien für Firewall-Systeme kennen
- Eine Firewall konfigurieren und testen können
- Das Prinzip eines IDS kennen
- Real Secure beherrschen
- Anwendungsmöglichkeiten eines IDS kennen

3 Theorie Firewall und IDS

Mit zunehmender Verbreitung des Internets wächst nicht nur die Zahl der ehrlichen Internet-Benutzer. Leider bekommen auch dunkle Gestalten einen einfacheren Zugriff zu Computer und -netzen. Darum ist es wichtig, sich mit "Sicherheit im Internet" auseinanderzusetzen. Dieses Kapitel zeigt einige wichtige Aspekte zur Sicherheit auf und motiviert zugleich, aktiv zur Sicherheit beizutragen.

Sicherheit wir oft als Oberbegriff für zwei Themengebiete verwendet:

- *Datensicherheit* = Datenintegrität und Betrieb gewährleisten
  dazu gehören Massnahmen wie Stromversorgung, Backup, Mirroring, Redundante System etc.
- *Datenschutz* = Missbrauch von Daten verhindern
  dazu gehören Massnahmen wie Firewalls, Verschlüsselung etc.

Im weiteren werden wir den Begriff Sicherheit allgemein für den Bereich Datenschutz verwenden. Datensicherheit im Sinne obiger Definition ist nicht das primäre Thema dieses Arbeitsplatzes.

Hier noch einige Beispiele die zeigen, was geschehen kann, wenn ein Netz ungenügend geschützt ist:

Elektronische Einbrüche

In New York wurden fünf Männer beschuldigt, im Juli 1992 in Computersysteme mehrerer regionaler Telefonfirmen und Grossunternehmen, Universitäten und Kreditforschungsinstituten wie TRW eingebrochen zu haben. Bei TRW sollen sie 176 Konsumentenkreditberichte gestohlen haben. Dabei zapfte die Regierung erstmals mit gerichtlicher Bewilligung Leitungen an, um Gespräche und Datenübermittlungen von Hackern festhalten zu können.

Quelle: Computerworld Schweiz, Nr. 17/93, p. 13

Pentagon-Hacker

Die britische Polizei verhaftete mit Schützenhilfe der US-Fahnder den 16-jährigen Pentagon-Hacker mit Vulgo "Datastream". Der junge Brite hat im Juli 1995 im Computer des amerikanischen Verteidigungsministeriums unter anderem geheime Mitteilungen zum amerikanisch-koreanischen Atomstreit entdeckt. Dateien zu Raketenforschung, Besoldung, Personaldaten und E-Mail wurden über Internet verbreitet. Dann jedoch lief er in eine elektronische Falle: aufgeflogen ist der Jugendliche, weil er über Nacht vergass, die Verbindung zum Pentagoncomputer abzubrechen.

Quelle: The Independent, January 3, 1995, 2766

3.1 Sicherheit

Um zu bestimmen was ein Sicherheitssystem leisten soll müssen zuerst die Anforderungen definiert werden.

3.1.1 Anforderungen

An Daten und Informatiksysteme werden allgemein folgende Anforderungen gestellt:

- *Verfügbarkeit*
- *Authentizität und Integrität*
- *Vertraulichkeit*

dazu kommt je nach Anwendung:

- Beweisbarkeit von Vorgängen
- Überwachung der Ressourcenbenützung

Verfügbarkeit

Fragestellungen:

- Wie lange kann ein Unternehmen ohne seine Daten leben?
- etc.

Die Erhöhung der Verfügbarkeit ist das Hauptziel der meisten Sicherheitsmassnahmen wie Redundante System, Backups etc.

Wie kritisch diese Grösse für ein Unternehmen ist kann sich je nach Anwendung stark unterscheiden. (Bsp. Ein Börsenmakler braucht aktuelle Daten innerhalb von Minuten für die Steuerung einer Maschine dagegen entscheiden Sekunden usw.)
Jeder Benutzer merkt üblicherweise sofort ob sein System und seine Daten verfügbar sind.

Authentizität und Integrität

Fragestellungen:

- Was geschieht wenn falsche Daten weiterverarbeitet werden?
- Was geschieht wenn auf Grund modifizierter oder gefälschter E-Mail Entscheidungen getroffen werden?
- etc.

Authentizität und Integrität wird teilweise von Sicherheitsmassnahmen wie Checksummen etc. gewährleistet. Dies Massnahmen schützen üblichweise vor Hard- und evtl. Softwarefehlern für einen Schutz gegen Angriffe muss meist aber noch mehr getan werden.

Kaum ein Benutzer macht sich Gedanken über die Authentizität und Integrität der Daten; was der Computer liefert wird meist als wahr und richtig angenommen.

Vertraulichkeit

Fragestellungen:

- Was geschieht wenn Konkurrenten Einsicht in interne Daten erhalten?
- Was geschieht wenn Entscheide zu früh publik werden?
- etc.

Zur Wahrung der Vertraulichkeit dienen Methoden wie Kryptographie und Zugangsschutz. Die meisten Benutzer sind sensibilisert für Vertraulichkeit weil sie dies auch bei nicht IT Anwendungen (z.B. Briefpost) beachteten.

3.1.2 Bedrohungen

Welche Bedrohungen sind zu erwarten? Man unterscheidet zwei Varianten:

- *Aktive Angriffe:*
    - Eindringen nichtauthorisierter Personen
    - Beeinträchtigung und Störung des Netzwerkbetriebes
    - Vortäuschen einer falschen Identität
    - Modifikation von Daten
- *Passive Angriffe:*
    - Abhören von Teilnehmer-Identitäten und Passwörtern
    - Abhören von Daten
    - Verkehrsflussanalyse

Wer sind die Angreifer:

- Mitarbeiter des eigenen Unternehmens
- Personen aus dem Konkurrenz/Wettbewerbs-Umfeld
- Hacker/Cracker aus der Computer-Untergrundszene
- professionelle Hacker/Industriespione

Je nachdem, in welchem Bereich eine Firma tätig ist, wird sie auch stärker von einer bestimmten Personengruppe besucht und leider auch attackiert. Die überwiegende Anzahl von Angriffen und Gefahren (beabsichtigt oder unbeabsichtigt) droht von den eigenen Mitarbeitern! (ca. 70%)

Aus Statistiken ist zu sehen, dass sehr viele Angriffe aus dem Internet von Universitäten und Schulen ausgehen. Vermehrt stellt man jedoch fest, dass professionelle Hacker für Industriespionage eingestellt werden.

3.1.3 Schwachstellen

Wie aber gelangen Angreifer auf fremde Systeme? Man kann die Schwachstellen in folgende Kategorien unterteilen:

- **mangelhafte Software:**
  Keine Software ist 100%ig fehlerfrei. Es ist bereits vorgekommen, dass Angreifer Softwarefehler auf entfernten Systemen ausgenutzt haben, um höher privilegierte Benutzerrechte zu erhalten.
- **schlecht konfigurierte und administrierte Systeme:** Die beste Firewall nützt nichts, wenn sie nicht richtig konfiguriert ist. In Zeitnot wird vielfach vergessen Sicherheitsmechanismen nach der Administration wieder einzuschalten oder nach dem Einbau einer neuen Komponente die Gesamtsicherheit des Systems neu zu überdenken. Daraus ergibt sich ein wichtiger Grundsatz aller Sicherheitssysteme: Die Einhaltung der Sicherheitspolitik ist **nicht** Sache der Systemadministratoren sondern sollte wo immer möglich an eine andere Stelle delegiert werden.
- **Sicherheitsprobleme der Kommunikationsprotokolle:** UDP und TCP garantieren keine sicheren Kommunikationspfade. Bei der Datenübertragung mit Hilfe von TCP/IP lässt sich nicht vorhersagen, über welche Knoten die Übertragung der Pakete erfolgt. Sitzt ein Angreifer am Terminal eines Vermittlungsknotens, so kann er die Daten, welche dort vermittelt werden, lesen.
- **Passwörter:**
  Die Wahl und Verteilung von Passwörtern hat einen grossen Einfluss auf die Sicherheit des Systems. Was nützt es, wenn jeder Benutzer das Passwort des Systemverwalters kennt oder die Passwörter so schlecht sind dass man sie mit einem Taschenrechner knacken kann?

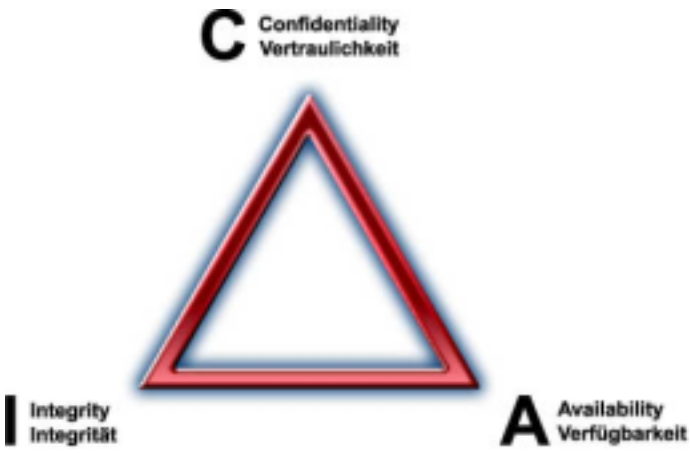


Abbildung 1 - CIA Dreieck

3.1.4 CIA Dreieck

Bei allen Bemühungen um Sicherheit darf man folgendes aber nicht vergessen: Werden Massnahmen zur Erhöhung der Vertraulichkeit eingesetzt leidet darunter die Verfügbarkeit, erhöht man die Verfügbarkeit leidet darunter die Integrität usw.
Man kann diesen Zusammenhang in einem Dreieck darstellen ("CIA" Dreieck, siehe Abbildung) mit den drei Kriterien Vertraulichkeit, Integrität und Verfügbarkeit als Eckpunkte und die Eigenschaften eines Systems oder die Anforderungen an ein System darin als Fläche eintragen.

Oder mit einem Beispiel ausgedrückt: Das sicherste System wäre ein Computer ohne Netzwerkanschluss und Stromzufuhr eingeschlossen in eine Safe: Man hätte damit fast ein Maximum an Vertraulichkeit gewonnen - wie aber kann man jetzt darauf aktuelle Daten nachführen (Integrität) und wie ermöglicht man den Zugriff für Benutzer (Verfügbarkeit)?

3.1.5 Sicherheitskonzept

Bevor man etwas absichern will, muss man wissen, wie man was vor was genau absichern will. Dieses Wie, Was und Wovor definiert man als eine Reihe von Entscheidungen in einem "Sicherheitskonzept" oder in "Sicherheitsrichtlinien". Dieses Kapitel zeigt, worauf beim Erstellen eines Sicherheitskonzepts geachtet werden muss und stellt dabei ein einfaches Gerüst zur Verfügung.

Was muss geschützt werden?

Als erstes müssen die zu schützenden Objekte identifiziert werden. Dies ist ein sehr wichtiger Teil. Wird nur eine Workstation vergessen, kann schon ein Angriff darauf ein ganzes Netz lahmlegen! Die folgende Aufstellung kann beim Erfassen der Objekte hilfreich sein [kyas96]:

- Hardware
- Software
- Daten
- Dokumentation
- Zubehör

Wovor wird geschützt?

Nach der Zusammenstellung der zu schützenden Objekte kann man sich nun überlegen, wovor die Objekte geschützt werden sollten. Grundsätzlich fragt man sich, welche Mitarbeiter welche Zugriffsrechte haben. Dazu definiert man Benutzergruppen:

- Gäste
- Aushilfen
- Mitarbeiter
- Systemadministrator
- Service-Personal
- externe Benutzer

Ein Mitarbeiter kann dabei in keiner Gruppe, einer oder mehreren Benutzergruppen angehören. Gehört er keiner Benutzergruppe an, so hat er keine Zugriffsrechte. Sind Zugriffsrechte verteilt, kann man unterscheiden, ob authorisierte oder nicht authorisierte Zugriffe erfolgen.

Wie gut wird geschützt?

Grundsätzlich unterscheidet man zwischen zwei Denkweisen:

- Alles, was nicht ausdrücklich erlaubt ist, ist verboten
- Alles, was nicht ausdrücklich verboten ist, ist erlaubt

Eine 100%ige Sicherheit wird nie erreicht [Murphy]! Man kann aber eine hohe Sicherheit erreichen, wenn die 1. Denkweise angewendet wird und einige Regeln eingehalten werden [chap95]:

- **Minimale Zugriffsrechte und Datensicht**
  Nur die zur Erfüllung einer Aufgabe absolut notwendigen Rechte dürfen vergeben werden. Dieses Prinzip verkleinert die Angriffsfläche und begrenzt den Schaden bei gezielten Attacken. Was der Mitarbeiter nicht probiert er auch nicht aus und kann damit keinen unbeabsichtigten Schaden anrichten.
- **Mehrschichtige Verteidigung:**
  Man sollte sich nie auf nur einen Schutzmechanismus verlassen. Es müssen Mechanismen eingesetzt werden, die sich gegenseitig unterstützen oder verstärken.
- **Die Passierstelle:**
  Die Passierstelle zum geschützten Bereich sollte möglichst eng sein. Zum Beispiel beim Anschluss des Firmennetzes an das Internet verwendet man darum nur eine Schnittstelle. Diese Schnittstelle kann genau überwacht werden. Werden dagegen mehrere Schnittstellen verwendet, kann man sich zuwenig auf die einzelnen konzentrieren und es geschehen schneller Fehler.
- **Das schwächste Glied:**
  Eine Kette ist nur so stark wie ihr schwächstes Glied. Dies gilt auch für ein Schutzsystem. Ein Angreifer sucht immer nach dem schwächsten Glied, um so schnell wie möglich die Mauer zu durchbrechen. Deshalb sollte man sich genau überlegen, worauf man sich bei der Überwachung besonders konzentrieren muss.
- **Zuverlässigkeit:**
  Es ist bekannt, dass jede Software Fehler hat. Es muss darauf geachtet werden, dass bei einem Softwarefehler ein Angreifer nicht plötzlich Zugang erhält, wo er sonst abgewiesen würde. Es kann sich unter Umständen auch lohnen mehrer Firewallsysteme gestaffelt hintereinander einzusetzen damit nicht beim Auftreten eines Softwarefehlers in einem System die ganze Verteidigung weg ist.
- **Umfassende Beteiligung:**
  Jeder Mitarbeiter muss mitmachen wollen und darum für die Sicherheit motiviert werden.
- **Einfachheit:**
  Die Sicherheitssysteme sollten einfach und übersichtlich gestaltet werden. Nur so ist es möglich, eine Kontrolle darüber zu haben. Bsp. Zwingt man die Benutzer dazu jede Woche ein neues 15stelliges Passwort zu verwenden werden sie es sicher irgendwo aufschreiben...

3.1.6 Sicherheitsklassen

Mit zunehmender Abhängigkeit heutiger Unternehmen von der Funktionsfähigkeit der Informationssysteme werden auch die Sicherheitsaspekte zu einem wichtigen Faktor. Um die Sicherheit von Informationssystemen auch nach objektiven Kriterien einheitlich beurteilen zu können, wurden Richtlinien geschaffen.

Der erste bedeutende Kriterienkatalog war das sogenannte "Orange Book" (TCSEC - Trusted Computer System Evaluation Criteria), welches vom amerikanischen Verteidigungsministerium herausgegeben wurde. Darauf aufbauend folgten weitere, wie aus folgender Abbildung zu sehen ist.

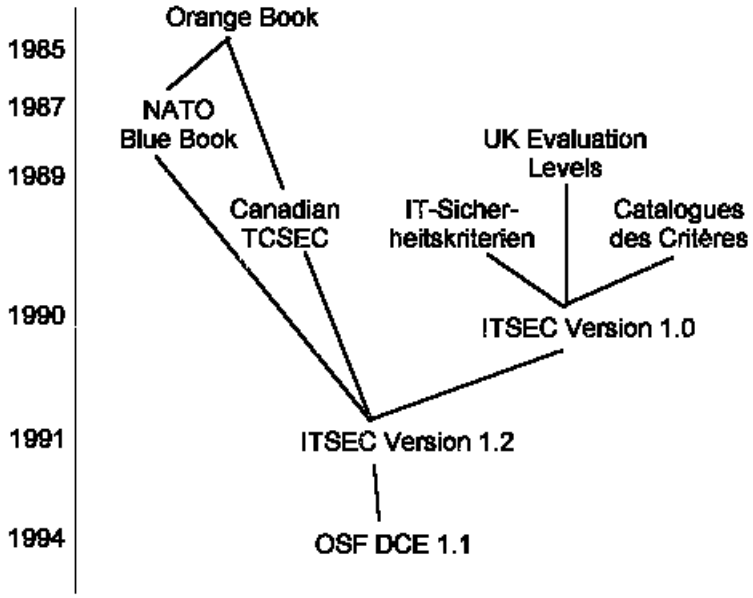


Abbildung 2 - Sicherheitsklassen

Das Orange Book

Im Orange Book werden Informationssysteme (auch IT-Systeme genannt) in die sieben Sicherheitsklassen D, C1, C2, B1, B2, B3 und A1 unterteilt.

Das Orange Book ist das "militärische" Modell von Sicherheit mit dem primären Ziel der Einhaltung der Vertraulichkeit und betrifft nur die Sicherheit eines Hosts und nicht eines Netzwerks. Das Modell umfasst immer Systeme d.h. die ganze Hard- und software inkl. aller Anschlüsse, den Ort an dem sich das System befindet und die komplette Dokumentation. Es ist deshalb nicht möglich ein Betriebssystem zu kaufen welches z.B. C2 sicher ist; Software ist allenfalls C2 zertifizierbar im Rahmen eines kompletten Systems!

In der **Klasse D** sind alle Systeme eingeordnet, welche die Anforderungen für die Klassen C bis A nicht erfüllen. Das System kann zwar sehr sicher sein, erfüllt aber mindestens eine Anforderung der anderen Klassen nicht. Die Klasse D beschreibt den geringsten Sicherheitsstandard.

Die **Klasse C** wird in die zwei Sicherheitsebenen C1 und C2 unterteilt.
C1 beschreibt die Sicherheitsmechanismen, welche normalerweise auf einem typischen Unix-System verfügbar sind. Die Benutzer müssen sich dem System gegenüber mit einem Loginnamen und einem Passwort legitimieren. Durch diese Kombination werden auch die Zugangsrechte für die Benutzer festgelegt.
C2 verlangt zusätzlich zu den Sicherheitsmechanismen von C1, dass alle oder bestimmte Operationen der einzelnen Benutzer überwacht und gespeichert werden können.

Die **Klasse-B**-Kriterien fordern zusätzliche Mechanismen zu den Kriterien der Klasse C. Die Klasse B wird in die drei Sicherheitsebenen B1, B2 und B3 unterteilt.
In **B1** werden verschiedene Sicherheitsniveaus wie nicht vertraulich, vertraulich, geheim oder streng geheim unterschieden. Die Rechte der Besitzer und Benutzer können nur durch den Systemoperator verändert werden.
B2 verschärft die Sicherheitskriterien der Ebene B1 weiter und fordert zusätzlich:

- Zugangskontrollen zu allen Komponenten des Systems
- gesicherter Kommunikationspfad zwischen Benutzer und System
- Abschirmung gegen elektromagnetische Abstrahlung nach aussen
- Unterscheidung zwischen Operator und Systemverwalter
- Markierung aller Einrichtungen mit der jeweiligen Geheimhaltungsstufe
- Formelle Beschreibung des Sicherheitsmodells

B3 Systeme erfüllen noch höhere Kriterien und müssen in der Regel von Grund auf als solche konzipiert und entwickelt werden. Dabei sind unter anderem zusätzliche Mechanismen zur Wiederherstellung des ursprünglichen Systemzustands nach Systemfehlern zur Verfügung zu stellen. Die **Klasse-A**-Kriterien fordern keine zusätzliche Systemerweiterung. Um diese Sicherheitsklasse jedoch zu erhalten, müssen alle Bedingungen der unteren Klassen erfüllt und zusätzlich bis auf das kleinste Detail dokumentiert sein.

Der ITSEC-Kriterienkatalog

Auch in Europa wurde ein Kriterienkatalog für die Beurteilung der Sicherheit von Informationssystemen geschaffen. ITSEC (Information Technology Security Evaluation Criteria) wurde in Anlehnung an das Orange Book auch in sieben Klassen aufgeteilt , welche in der Definition auch ungefähr mit dem Orange Book übereinstimmen, wie aus folgender Tabelle zu entnehmen ist:

Tabelle 1 - Übersicht über die Sicherheitsklassen

Orange Book	ITSEC	Sicherheit
D	E0	unzureichend
C1	E1	getestet
C2	E2	methodisch getestet, Konfigurationskontrolle und kontrollierte Verteilung
B1	E3	teilanalysiert (Schaltpläne, Quellcode)
B2	E4	formales Sicherheitsmodell, Spezifikation in semi-formaler Notation
B3	E5	nachvollziehbare Abbildung von Spezifikation/Quellcode
A1	E6	Anforderungen und Grob-Spezifikation in formaler Notation, Konsistenz mit dem formalen Sicherheitsmodell nachweisen

Sicherheit im OSI-Modell

ISO hat zusammen mit IEC, JTC1 und SC21 ebenfalls eine Sicherheitsarchitektur [ISO 7498-2] entwickelt. In dieser Sicherheitsarchitektur werden verschiedene Sicherheitsdienste defininiert, welche mittels Sicherheitsmechanismen realisiert werden können. Untenstehende Abbildung zeigt die Zusammenhänge:

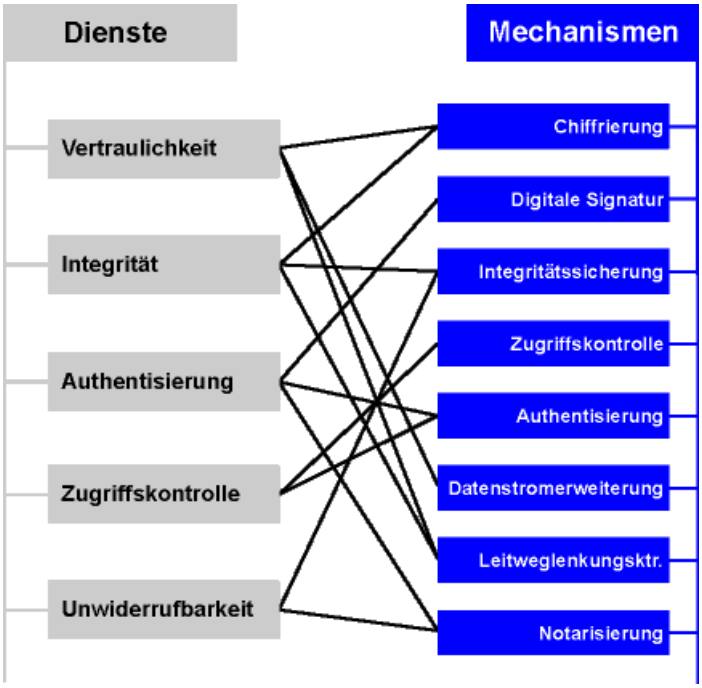


Abbildung 3 - OSI Sicherheitsarchitektur

Ein Problem ist allerdings, dass OSI die Sicherheitsarchitektur für offene Systeme definiert hat. Dies führt dazu, dass die Definition so offen ist, dass man sie genauer definieren muss, um überhaupt damit arbeiten zu können. In der Industrie werden meist sog. Subsets definiert. Diese genaueren Definitionen sind nun die Sicherheitsdienste in obiger Abbildung. Das Zusammenwirken aller Sicherheitsdienste gewährleistet schlussendlich die Gesamtsicherheit eines Systems.

3.1.7 IPng (IPv6)

An einer neuen Version des Internet Protocols (IP) wird schon längere Zeit gearbeitet. Das Internet Protocol Next Generation (IPng) oder auch IP Version 6 (IPv6) enthält neben dem um vielfaches grösseren Adressraum, den verbesserten Multicast-Adressfunktionen und der neuen Anycast-Adressen auch stark verbesserte Sicherheitsfunktionen. So wurde in IPng die Authentifizierung und die Sicherheitseinkapselung (Encapsulating Security Payload, ESP) eingebaut. [Hosen96]

Security Parameters Index

Der Security Parameters Index (SPI) wird aus der Zieladresse und einer sogenannten Security Association (Sicherheitskombination) berechnet. Die Security Association gibt unter anderem an, welcher Authentifizierungsalgorithmus und im Falle der Sicherheitseinkapselung, welcher Schlüssel für die Verschlüsselung verwendet wird.

Authentifizierung

Mit dem Authentifizierungs-Header, welcher eine Art fälschungssichere Unterschrift darstellt, wird bezeugt, dass ein IP-Paket wirklich vom richtigen Absender stammt und unterwegs nicht verfälscht wurde. Dies wird Angriffe wie IP-Spoofing verunmöglichen.
Die Schlüsselverwaltung für die Authentifizierung wird nicht in IPng integriert, damit es für unterschiedliche Schlüsselverteilungsverfahren offen bleibt. Der Zielrechner kann aber den Algorithmus und den Schlüssel immer aus der Security Association bestimmen, welche aus der eigenen Adresse und dem SPI berechnet werden kann.

Sicherheitseinkapselung

Die Sicherheitseinkapselung (ESP) ermöglicht es, entweder nur die Nutzdaten eines Datenpakets oder ein komplettes Datagramm zu verschlüsseln. Wird ein komplettes Datagramm verschlüsselt, so wird dem verschlüsselten Datagramm ein neuer, unverschlüsselter Header vorangestellt. Somit können vertrauliche Daten wie Kreditkartennummern und Geschäftsberichte sicher durch das Internet geschickt werden.

Zukunft

IPng wird in nächster Zukunft mehr und mehr anzutreffen sein. Einerseits ist das Verlangen nach einem grösseren Adressraum sehr gross und andererseit sind alle Internetbenutzer sehr an einer sicheren Datenübertragung auf dem Internet interessiert, um zum Beispiel Waren über das Internet einzukaufen und mit Kreditkarte sicher zu bezahlen. Die IETF hat die Spezifikationen von IPng als "Proposed Internet Standard" verabschiedet. Momentan wird an den Details des neuen Protokolls gefeilt. Es sind bereits Implementationen von IPng verfügbar.

3.2 Firewalls

In diesem Abschnitt lernen Sie die Grundlagen zu Internet-Firewalls kennen. So wird das Prinzip von Firewalls erklärt und aufgezeigt, wozu sie gebraucht werden. Ein Modell zeigt deren Einordnung im OSI-Referenzmodell. In einer Tabelle finden Sie eine Übersicht über die wichtigsten Begriffe, welche im Zusammenhang mit Firewalls oft gebraucht werden. Des Weiteren werden die Eigenschaften der verschiedenen Firewall-Typen und -Architekturen erläutert und zum Schluss aufgeführt, was Internet-Firewalls nicht leisten.

3.2.1 Prinzip

Eine Firewall setzt sich aus einer oder mehreren Komponenten zusammen. Sie überwacht oder beschränkt den Zugriff zwischen dem Internet und einem privaten Netz.

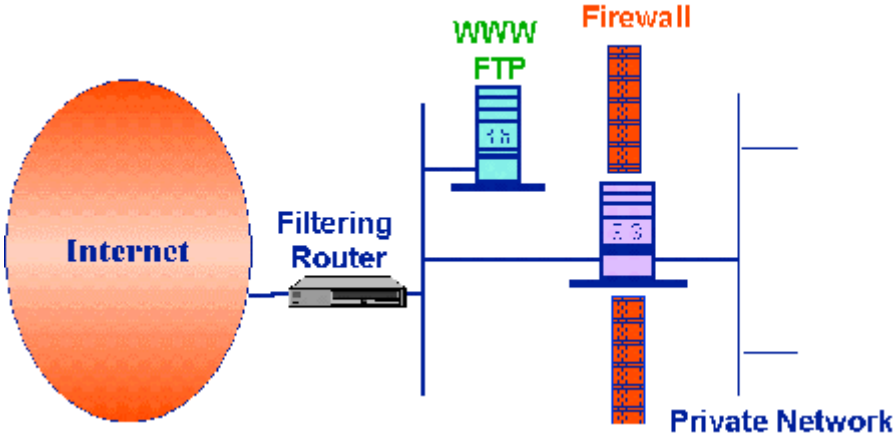


Abbildung 4 - Firewall Prinzip

Man unterscheidet im Allgemeinen zwischen Filtern (manchmal auch "Screens" genannt) und Gateways. Filter schleusen nur ausgewählte Klassen von Verkehr durch, während Gateways als Relais für bestimmte Dienste dienen, welche durch die Filter blockiert werden. So kann ein Systemadministrator einen bestimmten Dienst erlauben, solange dieser über "sein" Gateway geführt wird. Ein Gateway besteht aus einer oder mehreren Maschinen. [Ches96]

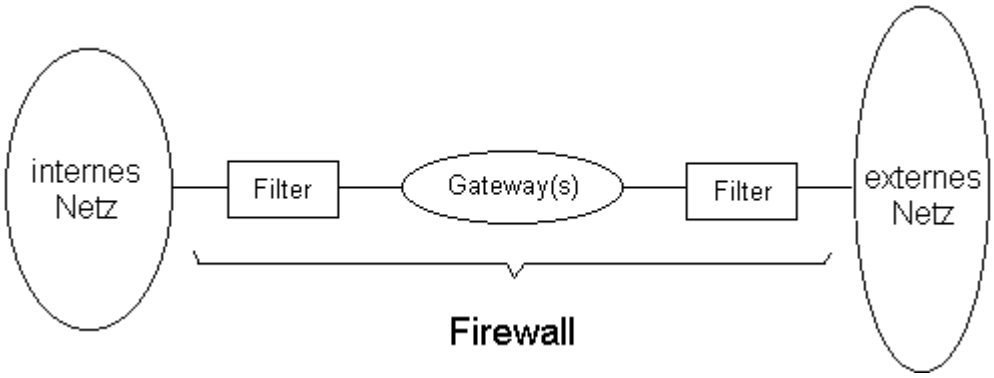


Abbildung 5 - Firewall Prinzip (2)

3.2.2 Definitionen und Begriffe

In folgender Liste sind die wichtigsten Begriffe aufgeführt, welche im Zusammenhang mit Firewalls oft verwendet werden. Hinterher finden Sie zu jedem Begriff die entsprechende Beschreibung. [Chap95]

- **Firewall**
  Eine oder mehrere Komponenten, welche zwischen einem geschützten Netz und dem Internet (oder einem anderen Netz) den Zugriff überwachen resp. beschränken.
- **Host**
  Ein eigenständiges Computersystem mit Anschluss an einem Netz (PC, Workstation, etc.).
- **Bastion-Host**
  Bastion -> Bastei, Bollwerk, Verteidigungsanlage: Besonders geschützte Computeranlage, da diese in der Regel eine wichtige Anlaufstelle für interne Benutzer und gegenüber dem Internet offen ist.
- **Dual-Homed-Host**
  Computersystem mit mindestens zwei Netzschnittstellen.
- **Dämon**
  Ein Programm, welches beim Bootvorgang oder beim Starten einer Anwendung gestartet wird und im Hintergrund aktiv bleibt. Es läuft also unsichtbar ab, deshalb der Name *Dämon* -> Geist, Spuk.
- **Proxy**
  Proxy -> Stellvertreter: System oder Prozess, welcher für Maschinen ohne Zugang eine Zugangsmöglichkeit bietet.
- **Proxy-Server**
  Ein Programm, welches stellvertretend für interne Clients mit externen Servern kommuniziert. Es stellt eine Art Verbindungspunkt für diese Kommunikation dar, denn nur so ist ein Server von einem Client erreichbar.
- **Proxy-Dienst**
  Einzelner Teil eines Proxy-Systems, welches für einen einzelnen (Internet-)Dienst benötigt wird (Bsp.: FTP-, Telnet-, HTTP-Proxy).
- **Paketfilterung**
  Prozess, welcher Pakete gemäss gegebenen Regeln passieren lässt oder sperrt. Filterung wird z.B. in lokalen Netzen von Bridges ausgeführt, um Pakete nicht mehr ins Ursprungssegment zu schicken, die als Ziel ein anderes Netzsegment haben als deren Ursprungssegment.
- **DMZ (Grenznetz)**
  DMZ: De-Militarisierte Zone. Netz, das als Schutzschicht zwischen ein geschütztes und ein externes Netz eingefügt wird.
- **Innerer Router**
  Der innere Router (manchmal auch Choke-Router genannt) schützt das interne Netz vor der DMZ (Grenznetz) und vor dem Internet. Der innere Router liegt somit zwischen dem internen Netz und der DMZ.
- **Äusserer Router**
  Der äussere Router (man chmal auch Access-Router genannt) schützt die DMZ und das interne Netz vor dem Internet. Meistens wird dieser Router vom Internet-Provider angeboten. Falls hohe Sicherheit verlangt wird, ist der äussere Router ein firmeninternes Gerät. Die Hauptaufgabe ist dann das Blockieren von Paketen mit gefälschten Ursprungsadressen. Diese Pakete behaupten, vom internen Netz zu kommen, werden aber auf dem Internet-"Port" vom Router empfangen.-> Diskrepanz.

3.2.3 Wozu braucht man Internet-Firewalls?

Ein internes Netz (Intranet) gar nicht ans Internet anzuschliessen, ist eine Möglichkeit. Eine andere ist ein Anschluss mit kontrollierbarer Sicherheit. Hier wird eine Einrichtung benötigt, die es ermöglicht, das Netz ans Internet anzuschliessen und dabei ein bestimmtes Mass an Sicherheit beizubehalten. Diesen Schutz bieten Firewalls, sofern diese gewissenhaft eingerichtet werden.

Im Allgemeinen gibt es verschiedene Modelle, ein Firmennetz zu schützen:

- *Keine Sicherheit* ist der einfachste Ansatz. Dabei werden lediglich die Sicherheitsmechanismen eingesetzt, welche ein Hersteller standardmässig bereitstellt.
- *Sicherheit durch Unsichtbarkeit* geht davon aus, dass niemand von der Existenz der bestimmten Ressource weiss.
- *Netzsicherheit*, wobei die Sicherheit beim Netzzugang gewährleistet wird. Dieses Konzept beinhaltet Firewalls, Authentifizierungsverfahren und Verschlüsselung.

- *Hostsicherheit* Könnte man davon ausgehen, dass moderne Betriebssysteme genügen Sicherheitsmechanismen beinhalten und zudem die Möglichkeit gesicherter Host-Host Kommunikation bieten müssten keine anderen Methoden eingesetzt werden. Man kann zwar einzelne Hosts sichern, verteilt damit aber die Administration und erhöht den Aufwand. Meistens wird man deshalb einen Ansatz mit gesicherten Teilnetzen verbunden über Netzsicherheitselemente als Lösung wählen.

Es gibt jedoch kein Sicherheitsmodell für alle Fälle. Jedes Modell muss der entsprechenden Netzumgebung sowie dem zu verwirklichenden Sicherheitskonzept angepasst werden. [Chap95]

3.2.4 Firewalls im OSI-Modell

Firewalls werden eingesetzt, um Systeme vor unerlaubtem Zugriff zu schützen. Ein Zugriff kann physikalisch oder logisch geschehen. Physikalisch, wenn z.B. eine Anschlussleitung angezapft wird und logisch, wenn der Zugriff z.B. softwaremässig geschieht.
Das OSI-Referenzmodell beschreibt ein Kommunikationssystem allgemein. Der Kommunikationsvorgang wird in sieben aufeinanderliegende Schichten zerlegt, wobei jede Schicht gewisse Funktionen realisiert. Diese Funktionen oder Dienste werden jeweils der nächst höheren Schicht zur Verfügung gestellt.
Die Schicht 1 ist die physikalische Schicht, welche beim physikalischen Zugriff auf das Übertragungsmedium massgeblich ist. Die verschiedenen Funktionen einer Firewall liegen in den Schichten 2 bis 7. Untenstehende Abbildung veranschaulicht die Einbettung von Firewalls ins OSI-Referenzmodell.

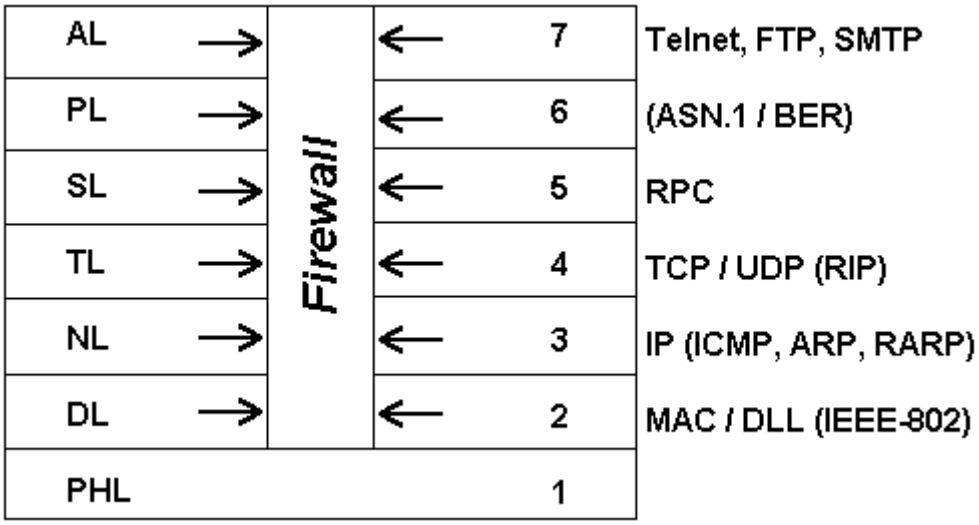


Abbildung 6 - Einbettung von Firewalls im OSI Modell

Aus der Abbildung wird ersichtlich, wo die Firewall ihren Einsatz findet. Ab Schicht 2 nämlich kontrolliert sie jeglichen Protokollverkehr zweier kommunizierender Schichten.

3.2.5 Firewall-Architekturen

[Chap95]
Dual-Homed-Host Architektur

Eine Dual-Homed-Host Architektur wird um den Dual-Homed-Host herum aufgebaut. Dieser Host wird zwischen dem internen und dem kritischen Netz (Internet) plaziert. Der Host könnte somit das Routen zwischen den beiden Netzen übernehmen, die Routingfunktion wird für den Einsatz in der Firewall-Architektur jedoch deaktiviert. Auf diese Weise werden IP-Pakete nicht direkt von einem ins andere Netz geroutet. Ein Rechner ausserhalb der Firewall und ein Rechner innerhalb der Firewall können somit nur mit dem Dual-Homed-Host kommunizieren, nicht aber direkt miteinander. Folgende Abbildung zeigt die Netzkonfiguration einer Dual-Homed-Host Architektur:

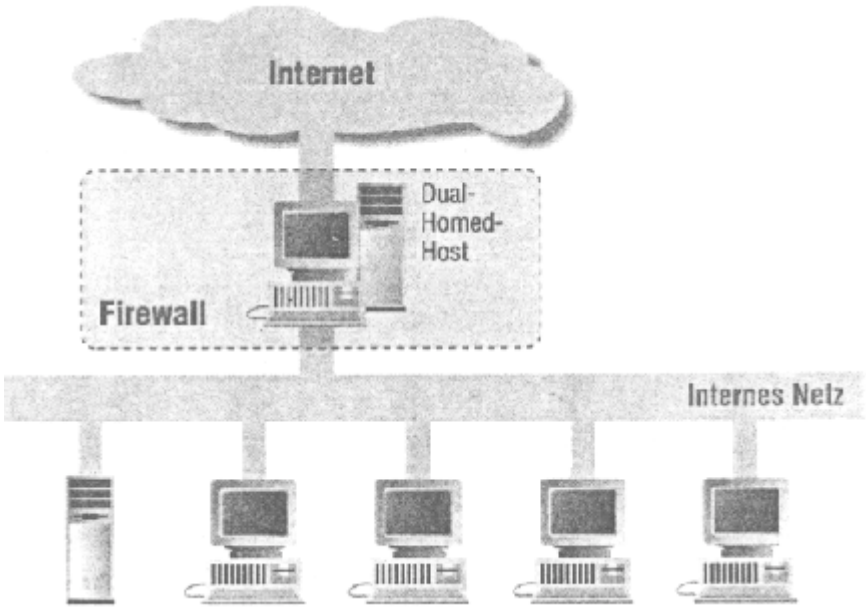


Abbildung 7 - Dual Homed Host

Architektur mit überwachtem Host (screend-host architecture)

Diese Architektur bietet Dienste über einen getrennten Router an, welcher als Paketfilter wirkt. Die Dienste werden von internen Maschinen angeboten, meist vom Bastion-Host selbst. Die Paketfilterung auf dem Überwachungsrouter wird so eingerichtet, dass aus dem Internet Verbindungen nur zum Bastion-Host aufgebaut werden können. Deshalb muss dieser auch höchste Rechnersicherheit bieten.

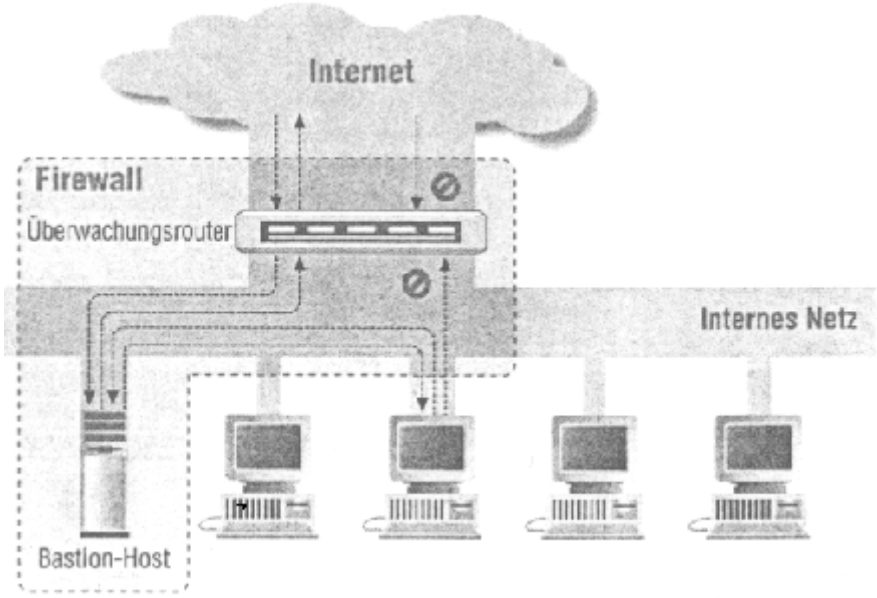


Abbildung 8 - Screened Host

Architektur mit überwachtem Teilnetz (screend-subnet architecture)

Diese Architektur wird gegenüber der Architektur mit überwachtem Host um ein Grenznetz ergänzt (Abbildung 1.4-6). D.h. zwischen dem Internet und dem internen Netz befindet sich hier das Grenznetz (auch DMZ genannt). Es können auch

mehrere Grenznetze zwischen die Aussenwelt und das interne Netz gelegt werden. Diese Massnahme ist jedoch nur sinnvoll und wirksam, wenn sich die verschiedenen Schichten auch unterscheiden. Bei der einfachsten Art dieser Architektur gibt es zwei Überwachungsrouter, die am Grenznetz angeschlossen sind. Man unterscheidet zwischen dem inneren Router und dem äusseren Router. Ein Angreifer muss also an beiden Routern vorbeikommen, um auf das interne Netz zu gelangen. Bei der Architektur mit überwachtem Host ist nur ein Router zu überwinden.

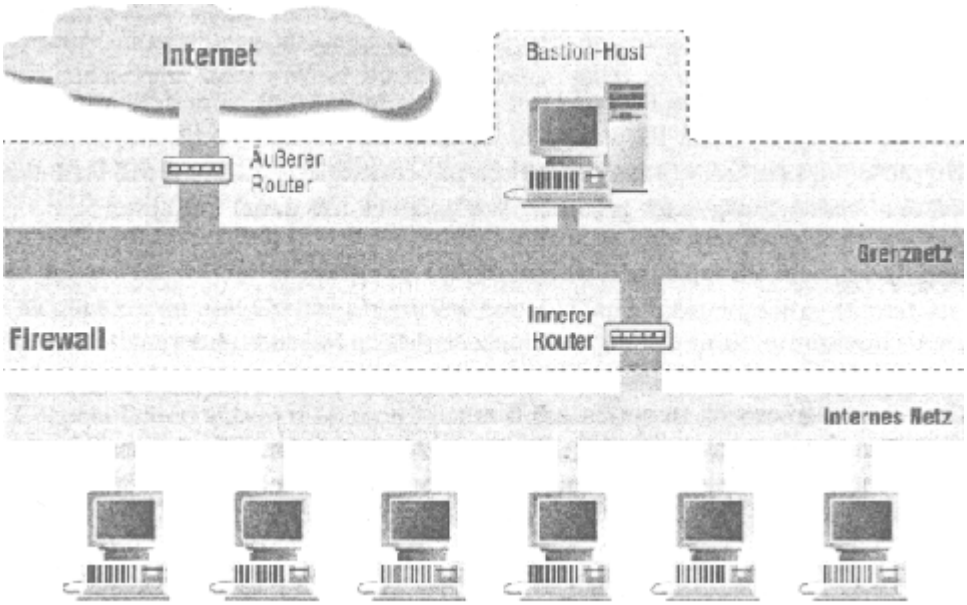


Abbildung 9 - Screened Subnet

3.2.6 Paketfilterung

Eine Firewall-Konfiguration besteht meist aus mehreren Komponenten: ein oder mehrere Filter sowie ein oder mehrere Gateways (siehe Abschnitt Prinzip). Paketfilterung ist eine billige Möglichkeit, Gateways zu schützen. Sie kann mit einem Router, welcher entsprechende Mechanismen unterstützt oder mit spezieller Software realisiert werden. Für die Paketfilterung eignen sich "normale" Router, da auf diesen die nötigen Mechanismen meist schon standardmässig implementiert sind. Zudem braucht man für den Anschluss ans Internet meistens sowieso einen Router. [Chap95]

Wozu braucht man Paketfilterung?

Mit Paketfilterung kann der Datentransfer gesteuert, zugelassen oder unterbunden werden. Dazu werden folgende Kriterien verwendet:

- Quelladresse, von der die Daten (angeblich) stammen
- Zieladresse, zu der die Daten gelangen sollen
- verwendete Sitzungs- und Anwendungsprotokolle

Die Daten selbst werden meist nicht ausgewertet. So lassen sich Filterregeln definieren, welche z.B. folgende Bedingungen erfüllen:

- Weise jeden Versuch ab, eine Telnet-Verbindung von aussen aufzubauen.
- Ermögliche jedem, uns mit E-Mail (SMTP) erreichen zu können.

Diese Regeln lassen sich relativ einfach realisieren. Schwieriger wird es wenn man mehrfache Kombinationen von Regeln ausdrücken will welche sogar voneinander abhängig sein können. Sinvollerweise setzt man dann ein entsprechendes Konfigurationswerkzeug (z.B. vom Routerhersteller) ein.

Folgendes Beispiel ist mit Paketfilterung jedoch nicht realisierbar, da ein Paketfilter keine Benutzer identifizieren kann:

- Ein bestimmter Benutzer kann sich von aussen mittels Telnet anmelden, alle anderen nicht.

Gewisse Schutzmechanismen lassen sich nur durch Router mit Paketfilterung realisieren. Dazu kommt, dass sich der Router dabei an einer bestimmten Stelle im Netz befinden muss. So ist es beispielsweise sinnvoll, alle Pakete mit interner Quelladresse abzuweisen. Dadurch können Pakete eines Angreifers, welcher als Quelladresse eine interne Adresse angegeben hat, leicht erkannt und eliminiert werden. Der Router alleine weiss nämlich, an welcher physikalischen Netzschnittstelle das externe Netz (z.B. Internet) bzw. das interne Netz angeschlossen ist.

Vorteile der Paketfilterung

- *Einfacher Schutz für ein ganzes Netz durch einen einzigen Überwachungsrouter:*
  Ein geschickt plazierter Router kann ein ganzes Netz schützen, wenn dieser als einziger Zugang zum Internet wirkt. Dabei ist die Netzsicherheit unabhängig von der Grösse des Netzes.
- *Einfache Handhabung resp. Transparenz für Anwender:*
  Für den Einsatz eines Paketfilters sind keine Software-Anpassungen und Konfigurationen auf den Client-Rechnern nötig. Eine spezielle Schulung der Anwender und eine etwaige Anmeldeprozedur fallen auch weg. Der Paketfilter "erscheint" dem Anwender transparent, so nimmt er diesen höchstens im Falle eine kritischen Prozedur wahr.
- *Standardmässige Implementation der Filtermechanismen:*
  In den meisten Hard- und Software-Routern ist die Funktionalität der Paketfilterung bereits standardmässig enthalten. So lässt sich ein bereits im Betrieb stehender Router problemlos zu einem Paketfilter "erweitern".

Nachteile der Paketfilterung

- Die meisten Implementationen von Paketfiltern weisen die folgenden Nachteile auf:
- Paketfilterregeln sind meist schwer formulierbar.
- Paketfilterregeln sind oft nur mühsam zu testen.
- Paketfilterfunktionen sind unvollständig und erschweren oder verunmöglichen oft die Realisierung von bestimmten Filtern.
- Ein fehlerhaftes Paketfilterungsprogramm kann Pakete passieren lassen, welche es hätte sperren müssen.
- *Paketfilterung ist nicht für alle Protokolle geeignet:*
  Die r-Befehle von BSD-UNIX sowie NFS und NIS/YP sind sicherheitskritische Protokolle, welche mit Paketfilterung nicht sicher genug abgefangen werden können.
- *Aktionen, welche normale Router mit gegebener Information nicht ausführen können:*
  Pakete geben Auskunft über ihren Ursprungsrechner. Von welchem Benutzer das Paket kommt, lässt sich jedoch nicht ausfindig machen. Weiter ist der verwendete Port ersichtlich, aber nicht die Anwendung, zu welcher das Paket gehört. Somit lässt sich ein bestimmter Dienst nur über dessen Portnummer kontrollieren. Und diese Portbelegung kann wiederum manipuliert werden.

Protokollierung

Wie bei allen Überwachungsaktivitäten werden auch bei der Paketfilterung Ereignisse protokolliert. Was wie zu protokollieren ist, entscheidet der Systemadministrator selbst. So kann er z.B. nur die potentiell "bösartigen" oder alle Pakete protokollieren. Hier gilt es ein vernünftiges Mass zu finden. Anhand der Protokolle ist es z.B. möglich, sich einen Überblick über eingehende oder abgehende Verbindungen zu verschaffen.

Antwort auf ICMP-Fehlermeldungen

ICMP (Internet Control Message Protocol) dient dazu, Hosts günstigere Routen zu einem Ziel bekanntzugeben, über Routing-Probleme zu informieren oder Verbindungen bei Problemen im Netz abzubrechen [Ches96].
Es stehen folgende zwei Gruppen von ICMP-Fehlermeldungen zur Auswahl:

- Das Ziel ist nicht erreichbar: "host unreachable" oder "network unreachable".
- Das Ziel ist aus administrativen Gründen nicht erreichbar: "host administratively unreachable" oder "network administratively unreachable".

Es gibt mehrere Punkte, die zu beachten sind bei der Entscheidung, ob der Überwachungs-Router ICMP-Fehlermeldungen zurückgibt oder nicht:

- Welche Meldungen werden zurückgeschickt?
- Ist der Zusatzaufwand akzeptabel, welcher beim Versenden der Fehlermeldungen entsteht?
- Erhalten Angreifer durch die Fehlermeldungen zu viele Informationen über Ihr System?

Wo werden Paketfilter plaziert?

Grundsätzlich sollte die Paketfilterung überall dort eingesetzt werden, wo es möglich ist. Die mögliche Anzahl Stellen im Netz hängt aber von der gewählten Firewall-Architektur ab. Bei der Architektur mit überwachtem Host und der Architektur mit überwachtem Teilnetz liegt die Lösung auf der Hand, da sowieso nur ein Router vorhanden ist. Sobald jedoch mehrere Router vorhanden sind, kann die Paketfilterung auch auf mehreren Routern vorgenommen werden. Es empfiehlt sich, die Paketfilterung an möglichst vielen Orten zu nutzen. Damit findet das Prinzip der minimalen Zugriffsrechte Anwendung: alles was nicht explizit erlaubt ist, ist verboten.

3.2.7 Proxy-Systeme

Proxy steht für Stellvertreter. Rechner mit Zugriffsmöglichkeiten dienen als Stellvertreter (Proxies) für Maschinen ohne Zugang, für die sie die gewünschten Aufgaben erledigen [Chap95]. Will ein interner Rechner z.B. Verbindung mit einem Rechner im Internet aufnehmen, nimmt er, der Proxy-Client, Kontakt mit dem Proxy-Server auf. Der Client wendet sich also nicht direkt an den "echten" Rechner, sondern kommuniziert über den Proxy-Server mit diesem. Für den Benutzer ist nicht zu unterscheiden, ob er es mit dem "echten" Server oder dem Proxy-Server zu tun hat. Umgekehrt nimmt der "echte" Server an, er arbeite mit dem Benutzer direkt, obwohl für ihn nur der Proxy-Server sichtbar ist. Damit Proxy-Systeme effektiv arbeiten, sind sie in Kombination mit Verfahren einzusetzen, welche den Netzverkehr zwischen den Clients und den eigentlichen Servern auf IP-Ebene einschränken. Ansonsten ist es möglich, den Proxy-Server zu umgehen. [Chap95]

Wozu braucht man Proxy-Dienste?

Proxy-Dienste werden eingesetzt, um vielen Benutzern den Zugriff auf das Internet zu ermöglichen und gleichzeitig ein bestimmtes Mass an Sicherheit beizubehalten. Der Benutzer erhält nur Zugriff mit Diensten (resp. Protokollen), für die auf dem Gateway entsprechende Proxies installiert sind.
Ein Proxy-System agiert somit als Kontrollstelle, da es nur jene Funktionen zulässt, welche in den installierten Proxy-Diensten realisiert sind. Ein Proxy-Prozess läuft völlig im Hintergrund ab, sodass die Verbindung ins Internet für den Benutzer scheinbar transparent ist. Daraus ergibt sich die einfachste Handhabung von Benutzerseite her.

Vorteile von Proxy-Diensten

- *Bieten Benutzern "direkten" Zugriff auf Internet-Dienste:*
  Proxy-Dienste gestatten Benutzern, von ihren eigenen Systemen aus auf Internet-Dienste zuzugreifen. Sie vermitteln den Benutzern den Eindruck, direkt mit den Internet-Diensten zu kommunizieren, obwohl im Hintergrund einige Prozesse ablaufen.
- *Bieten effektive Möglichkeiten zur Protokollierung:*
  Proxy-Server kennen die zu "vertretenden" Protokolle. Dadurch kann z.B. ein FTP-Proxy-Server nur die abgesetzten Kommandos protokollieren anstelle der gesamten Daten. Die Aufzeichnungen werden somit nicht so umfangreich und bleiben meist recht übersichtlich.

Nachteile von Proxy-Diensten

- *Software nicht immer leicht zu finden:*
  Es ist oft ein Problem, stabile Software für neue oder spezielle Dienste zu besorgen. Zudem vergeht meist viel Zeit, bis für einen neu eingeführten Dienst ein entsprechender Proxy-Server verfügbar ist.
- *Unter Umständen für jeden Dienst eigener Server nötig:*
  Es sind jedoch einige Produkte erhältlich, bei welchen mehrere Server integriert sind.
- *Clients und/oder Prozeduren müssen abgeändert werden:*
  Jede Änderung hat gewisse Nachteile. So lassen sich entsprechende Anweisungen auf einmal nicht mehr wie gewohnt verwenden und es wird eine zusätzliche Fehlerquelle geschaffen.
- *Proxies nicht für alle Dienste möglich:*
  Es gibt Dienste wie *talk*, welche komplizierte und verwickelte Interaktionen aufweisen. Für solche Dienste wird es wahrscheinlich nie einen Proxy-Dienst geben.
- *Kein Schutz vor Schwächen im Protokoll:*
  Proxy-Dienste überwachen oder ersetzen sicherheitskritische Protokolloperationen. Bei manchen Protokollen ist es aber sehr schwierig, diese kritischen Operationen ausfindig zu machen und diese zu überwachen. Dabei darf die Funktionsfähigkeit nicht eingeschränkt werden. X11 beispielsweise besitzt zahlreiche unsichere Operationen.

Wie funktionieren Proxies?

Die Funktionsweise eines Proxys ist vom Dienst abhängig. Manche Dienste funktionieren mit den Standardservern, bei anderen wird eine Anpassung der Clients oder Server nötig. Auf der Client-Seite unterscheidet man zwischen angepasster Client-Software und modifiziertem Verfahren für die Benutzer. Bei ersterer Alternative muss der Quellcode zur Verfügung stehen, ansonsten lassen sich keine Änderungen an den Clients anbringen. Beim modifizierten Verfahren kann der Benutzer die Standard-Client-Software verwenden, da der Proxy-Server in diesem Fall mit diesen zusammenarbeitet. Bei der Vorgehensweise jedoch wird vom Benutzer ein spezielles Vorgehen verlangt.

Verschiedene Arten von Proxy-Servern

Application-Level-Proxy

Application-Level-Proxy-Server kennen den Dienst und dessen Protokoll, für welchen sie eingesetzt werden. Sie werden meist in Verbindung mit modifizierten Verfahren verwendet, da sie zusätzlich benötigte Informationen mit Kenntnis des Anwendungsprotokolls oder aus den Benutzerdaten beziehen können (z.B. Zieladresse des "echten" Servers). Sie interpretieren also das Protokoll des entsprechenden Dienstes.

Circuit-Level-Proxy

Circuit-Level-Proxy-Server interpretieren das Anwendungsprotokoll nicht. Sie benötigen vom Benutzer also zusätzliche Informationen zum Verbindungsaufbau und verwenden dazu angepasste Clients. Im Allgemeinen fungiert ein Circuit-Level-Proxy-Server quasi als Vermittlungsstelle für die entsprechenden Protokolle.

Intelligente Proxy-Server

Intelligente Proxy-Server verfügen über zusätzliche Funktionalität. Beispiel: Ein HTTP-Proxy-Server hält Daten in einem Cache, um Anfragen nach denselben Daten nicht erneut ins Internet leiten zu müssen.

3.2.8 Authentifikation

Authentifikation kann als *Beweisen der eigenen Identität* umschrieben werden. In diesem Abschnitt wird auf die Benutzer- und die Host-Host-Authentifikation eingegangen. [Ches96]

Benutzerauthentifikation

Passworte

Die Authentifikation mittels Passwort fällt in die Kategorie "Wissen". Sie hat den Vorteil, dass dazu keine besonderen Ausrüstungen gebraucht werden. Dass Wissen aber verraten oder mitgehört werden kann, ist ein Nachteil. Passworte zählen daher auch nicht zu den starken Authentifikations-Mechanismen.

Einmal-Passworte

Die Einmal-Passwort-Authentifikation verwendet, wie der Name es schon sagt, nur einmal das gleiche Passwort. Dies bewirkt eine effektive Verteidigung gegenüber Mithören oder Verrat. Es gibt verschiedene Einmal-Passwort-Verfahren. Beispielsweise das Verfahren mit einer Streichliste oder jenes, welches einen Taschenauthentifikator verwendet. Beim ersteren ist der Benutzer im Besitze einer Liste von Passwörtern, welche er der Reihe nach anwendet. Nach Gebrauch wird das eben verwendete Passwort gestrichen. Für die nächste Sitzung ist dann das folgende Passwort zu gebrauchen.
Authentifikation mittels Taschenauthentifikator beruht auf einer internen Uhr und einem geheimen Schlüssel. Die aktuelle Zeit und der geheime Schlüssel werden durch eine Funktion miteinander verknüpft. Das Resultat dieser Verknüpfung dient dem Benutzer als Passwort, das sich von Minute zu Minute jeweils ändert. Der Host nimmt nun die Authentifikation anhand seiner eigenen Uhr und einer Kopie des geheimen Schlüssles vor. Stimmt das Resultat mit der Eingabe des Benutzers überein, so erhält dieser Zugang zum System.

Es gibt noch weiter Verfahren zur Authentifikation. An dieser Stelle sei jedoch auf [Ches96] verwiesen.

Smart Cards - "Intelligente" Chipkarten

Chipkarten oder Smart Cards sind heute weitverbreitet. Sie verfügen meist über eine CPU, einen I/O-Kanal und einige Kilobytes ROM. Die Verwendung von Chipkarten ist sehr einfach und in der Öffentlichkeit oft angewandt. Chipkarten fallen in die Kategorie "Gegenstände" und werden mit der PIN um "Wissen" ergänzt. Ein Angreifer benötigt in diesem Fall wie beim Verfahren mit Einmal-Passwörtern die PIN (Persönliche Identifikationsnummer) oder Benutzerkennung sowie das entsprechende Gerät (Chipkarte oder Taschenauthentifikator), um einen Benutzer zu verkörpern.

Biometrik

Diese Methode verwendet benutzerspezifische Eigenschaften, um eine Authentifikation durchzuführen. Übliche Biometriken sind: Fingerabdruck, Stimmuster oder Unterschrift. Der Vorteil von Biometriken ist, dass diese nicht verloren oder gestohlen werden können. Ein Nachteil dieses Verfahrens ist jedoch, dass spezielle Hardware benötigt wird. Bei der Erkennung von Biometriken sind Grenzen gesetzt. So wird ein Benutzer niemals zwei 100%ig übereinstimmende Unterschriften produzieren können. Dies verlangt nach Toleranzen bei der Erkennung. Und, würden Sie einem Benutzer ein Login auf Ihrem System erlauben, der (nur) zu 85% dieser bestimmte Benutzer ist?

Host-Host-Authentifikation

Datennetz-basierte Authentifikation

Die überwiegende Form der Hos-Host-Authentifikation verlässt sich (noch) auf das Netz. Das Netz transportiert die Identität des Benutzers und verlässt sich zudem auf die Sicherheit im Netz. Bei der Datennetz-basierten Authentifikation gibt es zwei Varianten: adressbasiert und namensbasiert. Die adressbasierte Variante verlässt sich auf die numerische IP-Adresse. Die namensbasierte Variante überprüft nebst der Adresse auch noch den damit verknüpften Namen. Dies eröffnet einem Angreifer jedoch die Möglichkeit, einen Mechanismus, der IP-Adresse in Host-Namen umsetzt, zu unterwandern.

Kryptografische Verfahren

Kryptografische Verfahren werden in symmetrische und asymmetrische Verfahren unterteilt. Symmetrische Verfahren verwenden zur Verschlüsselung und Entschlüsselung jeweils an beiden Seiten (Sender und Empfänger) den gleichen geheimen Schlüssel. D.h. beide, Sender und Empfänger, müssen den geheimen Schlüssel kennen. Eines der bekanntesten symmetrischen Verfahren ist DES (Data Encryption Standard). Asymmetrische Verfahren verwenden zur Verschlüsselung und Entschlüsselung jeweils verschiedene Schlüssel. Dabei ist einer dieser Schlüssel öffentlich (bekannt) und der andere geheim. Die Verschlüsselung erfolgt mit dem öffentlichen Schlüssel. Die Entschlüsselung wird mit Hilfe des geheimen Schlüssels ermöglicht, d.h. nur der berechtigte Empfänger kann die Daten richtig entschlüsseln. Ein bekanntes asymmetrisches Chiffrierverfahren ist RSA (von Rivest, Shamir und Adleman).

Eine Anwendung, die sehr oft für die Verschlüsselung von E-Mail verwendet wird, ist PGP (Pretty Good Privacy).

3.2.9 PGP - Pretty Good Privacy

[iX9/96] PGP ist ein Verschlüsselungsverfahren von Phillip Zimmermann. PGP ist ein Public-Key-Verfahren, das mit zwei Schlüsseln arbeitet: einem öffentlichen und einem privaten. Beide Schlüssel werden einmal gemeinsam generiert. Das Verfahren bietet folgende Möglichkeiten:

- Eine Nachricht wird so codiert, dass nur ein Empfänger, dessen Public Key man selbst besitzt, sie lesen kann.
- Es wird sichergestellt, dass eine Nachricht von einem bekannten Adressat stammt. Dazu muss der eigene Public Key dem Mail-Verteiler vorher bekanntgegeben worden sein.
- Durch die Verschlüsselung der Nachricht beim Absender wird eine mögliche Änderung auf dem Weg vom Absender zum Empfänger ausgeschlossen. Eine entsprechende Modifikation am chiffrierten Text würde das Programm sofort anzeigen.

Der öffentliche Schlüssel kann also als Adresse oder Telefonnummer angesehen werden. Dabei kann der Inhalt einer Nachricht verschiedenen Formats sein: nur Text, Grafik oder Programme.

Beispiel einer digitalen Unterschrift mit PGP


```
-----BEGIN PGP SIGNATURE-----
Version: 2.6.3i
Charset: latin1

iQCVAgUBMP41DbCfd7bM70R9AQFOjQQAgjP7RkaLaDFeh0iHBKYH0iKqo+xAEMre
/4QizPhGRlUTCqaATg5bz72Gn2MGrCNFJ2LeFoDE5LDHsF3TWYd12Hp2ZTrLpLXD
cm9iCUJJRKO6aGuQRY27sJQiy00N04G691PniuFAh9oMuQeh/SakhqRYjWD8v7kC
zTXqqt4uhbc=
=JVWt
-----END PGP SIGNATURE-----
```

3.2.10 Was Firewalls nicht leisten

Firewalls sind ein starkes Werkzeug zum Schutz von Datennetzen. Dennoch bieten sie nur Schutz mit beschränkten Möglichkeiten. Es ist also auch wichtig zu wissen, was Firewalls nicht leisten resp. wo ihre Grenzen liegen. Wenn Sie von den üblichen Netzwerkschichten (Schichten 2-4) ausgehen, dann stellt die Firewall einen guten Schutz dar. Adressfälschung oder verbotene Dienste können relativ problemlos erkannt werden. Falls eine Attacke jedoch auf höherer Ebene ansetzt, muss die Firewall deren Paketinhalt durchsuchen. Es lohnt sich z.B., zu überlegen, ob der kritische X11-Dienst nicht besser von Anfang an zu sperren ist.

Ein bekanntes Beispiel ist auch *sendmail*. Beim Interpretieren des Inhalts von bestimmten Mail-Headern liess es sich manchmal zu übelgesinnten Aktionen verleiteten. Es verdeutlicht also gut, dass in Fällen, wo der Programmcode einer Anwendung schon fehlerhaft und unsicher ist, auch die beste Firewall als nutzlos erscheint. Selbst wenn alle bekannten Schlupflöcher gestopft sind, können durch neue Anwendungen oder Dienste bereits wieder neue Schlupflöcher entstanden sein, die man noch gar nicht kennt! [Ches96]

3.3 Firewall - Produkte

Dieses Kapitel gibt eine Übersicht über einige auf dem Internet bekannten Firewall-Produkte.

3.3.1 Kommerzielle Firewall-Produkte

Produkt	Firma	Typ
Actane Controller	Actane	Proxy
ANS Interlock	ANS	Proxy
BorderWare Firewall	Borderware	Proxy
Firewall-1	Checkpoint	Packet-Filter
AltaVista Firewall	DEC	Packet-Filter
Gauntlet Firewall	Trusted Information Systems	Proxy
GFX Internet Firewall	GFX	Proxy & Packet-Filter
IBM Firewall	IBM	Proxy
SecureIT	Milkyway Systems	Proxy
Raptor Firewall	AXENT	Proxy
NetGate Firewall	SmallWorks	Packet-Filter
SunScreen	Sun	Packet-Filter

Neuere Produkte findet man auch bei Yahoo!

3.3.2 Freeware Firewall-Toolkits

Name	Beschreibung
tcpwrapper	Protokollierung und Filterung
portmapper	Protokollierung und Filterung
Socks	Proxy
TIS FWTK	Proxy

3.4 Intrusion Detection Syteme (IDS)

Selbst das beste Sicherheitssytem kann nicht mit letzter Sicherheit ausschliessen, dass es jemanden gelingt, sich unerlaubt Zutritt in das zu schützende Computersystem zu verschaffen. Damit ein erfolgreicher Angriff möglichst schnell erkannt werden kann wurden Intrusion Detection Systeme (IDS) entwickelt.

Solche Systeme sind in der Lage mögliche Systemeinbrüche durch Überwachen einer Vielzahl von Netzaktivitäten (Verkehrslast, Aktivitäten an bestimmten Ports, ...) zu erkennen.

3.4.1 Hauptaufgaben des IDS

Das Ziel der Intrusion Detection-Systeme ist die Erkennung von Sicherheitsverletzungen und eine angemessene, schnelle Reaktion darauf. Hauptaufgaben des IDS sind:

- Missbrauchserkennung auf der Netzwerkebene

  Erkennung von Angriffen (Denial of Service, SYN-Flooding, PING-Flooding, Pre Attack Probe (Information über Netzwerke, Angriffe über Portscan-Verfahren), Angriffe über World Wide Web Dienste (Aktive X, Java,..))

- Rechnersystemen- basierte Angriffserkennung

  Alle wichtigen Audit-Dateien auf dem System werden überwacht und ausgewertet. Bei Erkennung von Angriffen werden Alarme ausgelöst.

- Erkennung von Anomalien

  Erkennung von untypischen System- und Benutzerverhalten.

- Intrusion Response

  Bei Angriffen können verschiedene Gegenmassnahmen (z.B Alarme über E-Mail, SMS, Unterbrechung der Verbindung, Protokollierung des Angriffs) eingeleitet werden.

- Ereignismeldungen

  Alle Ereignismeldungen können nach verschiedenen Prioritäten (High, Medium, Low) zugeordnet und angezeigt werden.

- Protokolierung / Berichterstattung

  Es werden Log-Dateien geführt und nach verschiedenen Kriterien ausgewertet (grafische Auswertung).

3.4.2 Möglichkeiten der Signaturerkennung

Um Angriffe erkennen zu können, muss man wissen wonach man suchen muss. Angreifer setzen häufig bestimmte Techniken ein, um Angriffe vorzubereiten. Diese Angriffe erfolgen nach bestimmten Mustern. Kennt man das Muster, Signatur genannt, des Angriffs ist eine Erkennung (Detection) des Angriffs möglich. Einige typische Auswirkungen, die einen Angriff kennzeichnen und deutliche Signaturen hinterlassen, sollen hier als Beispiele kurz vorgestellt werden. Viele dieser Signaturen können nur als Anzeichen für einen Angriff gewertet werden, wenn sie gehäuft oder in ungewöhnlichem Zusammenhang auftreten (ein Einlogversuch mit falschem Passwort ist sicher kein Angriff, bei mehreren hundert Versuchen, ist es eindeutig einer). In den folgenden Unterkapiteln werden einige der häufigsten Angriffsarten beschrieben.

3.4.2.1 TCP-Portscan

Ein TCP-Portscan ermöglicht es festzustellen, welche TCP-basierten Dienste ein Zielrechner anbietet. Ein TCP-Verbindungsaufbau geschieht normalerweise in drei Schritten:

1. Angreifer sendet SYN an zu testenden Port des Zielrechners
2. Zielsystem antwortet mit SYN/ACK
3. Angreifer sendet ACK an Zielsystem

Nun ist eine aktive Verbindung aufgebaut, die vom Zielsystem normalerweise protokolliert werden sollte, so dass sie leicht entdeckt werden kann. Verzichtet der Angreifer auf den dritten Schritt, weiss er trotzdem, dass dieser Dienst existiert. Der versuchte Verbindungsaufbau wird jedoch häufig nicht in die Log-Dateien übertragen. Programme wie Tcplog sind allerdings in der Lage, auch fehlgeschlagene Verbindungsaufbauten zu protokollieren. Werden häufige (fehlgeschlagene) Verbindungsaufbauten in relativ kurzer Zeit beobachtet, ist dies ein sicheres Zeichen für einen Angriff. Es gibt allerdings auch Portscans, die von Tcplog nicht erkannt werden.

3.4.2.2 UDP-Portscan

UDP ist ein verbindungsloses Protokoll und besitzt demnach keine Verbindungsaufbauprozedur, die Informationen über angebotene Dienste geben kann. Schickt der Angreifer jedoch UDP-Anfragen an einen inaktiven UDP-Port, so antwortet der Zielrechner mit "ICMP Port unreachable", so dass der Angreifer von den inaktiven auf die aktiven Ports schliessen kann. Die Vielzahl der Anfragen kann einem IDS als Signatur dienen.

3.4.2.3 Finger- und r-Dienste

Diese und einige weitere Dienste können Informationen über die Benutzer eines Systems liefern, die eventuell für einen Angriff genutzt werden können. Werden diese Dienste auffällig häufig benutzt, deutet dies auf einen bevorstehenden Angriff hin.

3.4.2.4 IP mit falschen Parametern

Diese Angriffsart wird häufig benutzt, um den Betrieb eines Rechners zu stören (Denial of Service). Die IP-Pakete sind allerdings an ihren falschen Parametern zu erkennen, so dass sie als eindeutige Signatur für einen Angriff dienen können. Beispielsweise stürzen viele Rechner aufgrund einer fehlerhaften Implementierung ab, wenn die Quell- und die Zieladresse sowie Quell- und Zielport übereinstimmen.

3.4.2.5 Überflutung

Dieser Angriff basiert darauf, einen Rechner oder Dienst dadurch auszuschalten, dass man ihn mit Daten "überflutet". Sendet man beispielsweise E-Mail in grossen Mengen an einen Rechner, so wird das Spool-Verzeichnis überlaufen und kann keine weiteren Daten entgegennehmen. Bei einigen Implementierungen kann es auch zu einem Totalabsturz des Rechners kommen. Diese Angriffsart funktioniert auch mit einigen anderen Diensten, als Indiz kann einem IDS der gehäufte Bedarf an Resourcen dienen.

Ist die Quelladresse eines SYN-Pakets (das normalerweise dem Verbindungsaufbau dient) unerreichbar, weil sie gefälscht ist, wird trotzdem Arbeitsspeicher für die gewünschte Verbindung reserviert. Wird die Anfrage in schneller Folge wiederholt, bindet der Angriff im Rechner zuviel Betriebsmittel und kann seine normalen Aufgaben nicht mehr im vollen Umfang bewältigen.

3.4.2.6 ICMP-Echo-Request

Ein ICMP-Echo-Request (ping) dient normalerweise dazu, die Erreichbarkeit bestimmter Rechner zu überprüfen. Übersteigen diese ICMP-Pakete eine bestimmte in der Spezifikation vorgesehene Maximalgrösse können sie aufgrund einer falschen Implementierung den Zielrechner zum Absturz bringen. Die ICMP-Echo-Request-Pakete können durch ein IDS analysiert werden, so dass auch dieser Angriff automatisch erkannt werden kann.

Mit ICMP-Echo-Requests ist es leicht möglich, die Netzinfrastruktur des Opfers zu untersuchen, indem man alle Netzadressen, die in dem Zielnetz vorkommen können, anspricht. Ping-Pakete an alle vorhandene und sogar an nicht vorhandene Rechner sind ein starkes Indiz für die Vorbereitung eines Angriffs.

3.4.2.7 Einkapselung/Tunneln

Fast jedes Transportprotokoll lässt es zu, dass in seinem Datenfeld bestimmte Daten untergebracht werden, die auf der Empfängerseite interpretiert werden können. So kann beispielsweise SMB über IP übertragen (getunnelt) werden. Natürlich kann auch IP in IP eingekapselt und so getunnelt werden. Firewalls überprüfen häufig die in Datenfeldern stehenden

Informationen nicht. Bestimmte getunnelte Protokolle können jedoch durch Überwachung des Netzverkehrs aufgedeckt werden.

3.4.2.8 WWW-Spoofing

Der Betreiber eines WWW-Servers hat die Möglichkeit, als Angreifer dem Opfer ein Dokument mit ausschliesslich gefälschten URLs zuzuspielen. Der Benutzer kann diesen Angriff leicht entdecken, indem er die Statusanzeige des Browsers beobachtet. Auch ist es notwendig, dass der Benutzer die WWW-Seiten des Angreifers anwählt. Als Signatur können die für diesen Angriff notwendigen verlängerten URLs leicht von einer IDS entdeckt werden.

3.4.3 Vor- und Nachteile der Signaturerkennung

Vorteile der Signaturerkennung sind:

- Häufig werden Angriffe auf Basis von Angriffsskripten durchgeführt, aus denen sich leicht Signaturen ableiten lassen, so dass eine hohe Entdeckungswahrscheinlichkeit gegeben ist.
- Stehen die Signaturen zur Verfügung, ist der Aufwand zur Installation und Wartung gering.

Nachteile sind:

- Der Erfolg hängt unmittelbar von der Güte der Signaturdatenbank ab. Existiert für einen Angriff keine Signatur, wird er nicht erkannt.
- Eine Anpassung der Signaturdatenbank an lokale Gegebenheiten oder eine Definition neuer Signaturen ist meist sehr aufwendig. Aufgrund der speziellen Anpassung sind Signaturdatenbanken nur beschränkt Portabel.
- Die Signatur muss regelmässig an neu entdeckte Angriffssignaturen angepasst werden (ähnlich dem Vorgehen bei einem Virenscanner). Die neuen Angriffssignaturen sollten vom Hersteller zur Verfügung gestellt werden.

3.4.4 DoS-Attacken und DDoS-Attacken

Seit den Anfängen des Internets existieren sie, die sog. "Denial-of-Service" (DoS) Angriffe, deren Ziel ist es, die Verfügbarkeit bestimmter Rechner und/oder Dienste einzuschränken. Meist wird bei dieser Form von Angriffen über das Internet versucht, durch das Ausnutzen von Schwachstellen in Betriebssystemen, Programmen und Diensten bzw. das Ausnutzen grundsätzlicher Entwurfsschwächen der verwendeten Netzwerkprotokolle, die angegriffenen Systeme zum Absturz zu bringen, oder derartig zu überlasten, dass diese Systeme ihre eigentliche Funktionalität nicht mehr erbringen können. Reine DoS-Angriffe haben also nicht das Ziel, vertrauliche Daten zu stehlen oder Benutzer-Authentisierungs-Mechanismen zu umgehen, sondern Diensteanbieter lahm zu legen.

3.4.4.1 DoS-Attacken

Als Denial-of-Service bezeichnet man Attacken, bei welchem ein Benutzer soviel Systemresourcen belegt, dass für die anderen Benutzer keine Ressourcen mehr zur Verfügung stehen. Dadurch kann ein Server oder eventuell nur ein Dienst, der auf dem Server läuft, empfindlich beeinträchtigt werden. Die Ressourcen können Prozesse, Plattenplatz oder die Auslastung der CPU sein. Es gibt zwei Arten von DoS-Attacken:

- Die erste zielt darauf ab, das System unbrauchbar zu machen. Das kann zum Einen durch einen herbeigeführten Disk-Crash oder zum Anderen durch Löschung wichtiger Kommandos erreicht werden.
- Die zweite Art überlastet irgendeine Ressource im System, um so den anderen Benutzern die Verwendung dieser Ressource unmöglich zu machen.

3.4.4.2 DDoS-Attacken

Ein neuer Trend in Denial-of-Service Angriffen wird seit Mitte 1999 beobachet und hat Anfang 2000 bei Angriffen auf Firmen, wie Yahoo, Buy.com, eBay, Amazon, Datek, ETrade und CNN für weltweites Aufsehen gesorgt.

Bei einem Distributed Denial of Service-Angriff wird im Vergleich zu einem Denial-of-Service-Angriff , wie der Name schon sagt, nicht nur von einem einzelnen Rechner attackiert, sondern von einer grossen Anzahl unterschiedlicher Systeme.

Diese grossflächig verteilten Angreifer attackieren, zentral koordiniert, einzelne Systeme oder Netzwerke. Die Anzahl der an einem Angriff beteiligter Systeme wurde bereits beobachtet. Da die an einem Angriff beteiligte Rechner oft über grosse Teile des Internets verteilt sind, spricht man deshalb von einem sogenannten „Distributed Denial-of-Service“ (DDoS) Angriff. Momentan sind unzählige solcher Tools unter Namen, wie „Trible Flood Network“, „Stacheldraht“, „trinoo“, „Shaft“ oder „MStream“ im Internet aufgetaucht.

3.4.5 Real Secure von ISS

Im Praktikum wird das RealSecure 5.0 von der Firma ISS (Internet Security Systems) als IDS eingesetzt um die verschiedenen Angriffe zu erkennen. Es folgen einige Erklärungen über diese Software.

Ähnlich einer Sicherheitskamera am Eingang eines Gebäudes bietet RealSecure ein Schutzsystem, um statische Sicherheitstechnologien, wie Firewalls, zu ergänzen und so die Unternehmensnetze der Anwender über alle Geräte und Netzschichten hinweg vor Eindringlingen zu schützen. Dabei überwacht RealSecure alle am Netz angeschlossene Geräte, ohne die Leistung des Netzes negativ zu beeinflussen.

- Umfassende Datenbank zur Erkennung von Angriffsversuchen

Dank der umfangreichen Kenntnisse von ISS über Sicherheitslücken und der einzigartigen Digital-FingerPrint-Technologie analysiert RealSecure im Hintergrund unbemerkt das Netzwerk mit hoher Geschwindigkeit und sucht nach verdächtigen Aktivitäten. Um diese zu erkennen verfügt RealSecure über eine grosse Datenbank an Angriffs-Signaturen.

- Unterstützung verschiedener Netz-Topologien

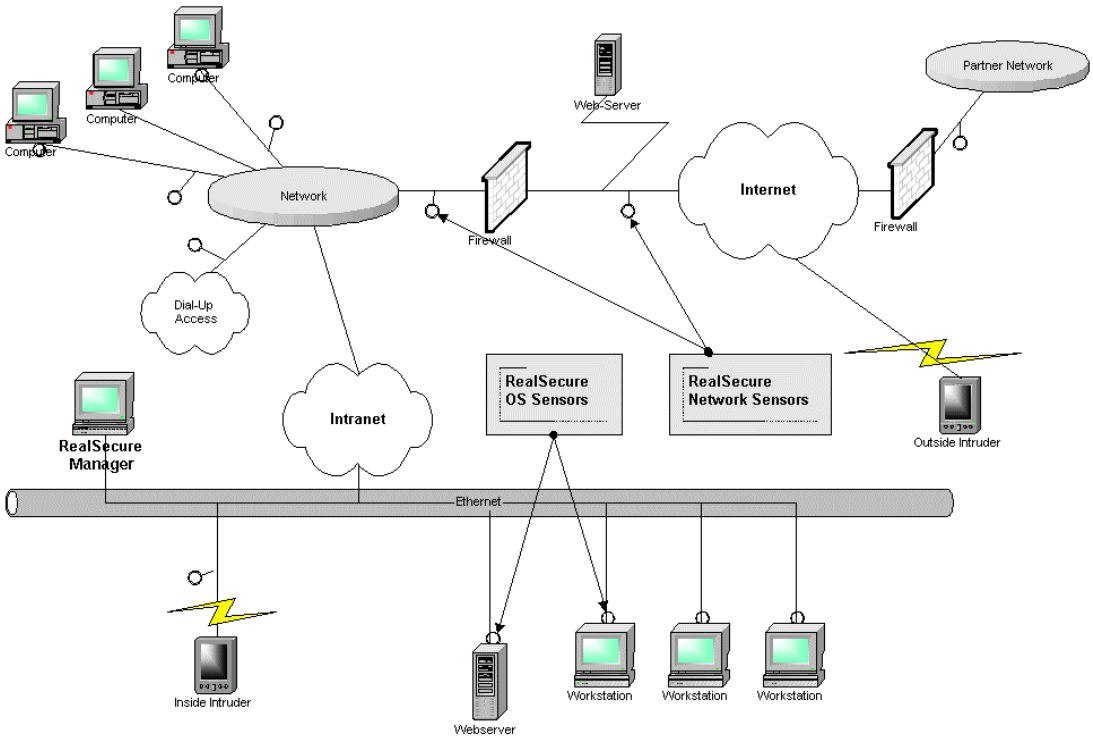
RealSecure analysiert kundenspezifische Netze. Dabei überwacht das System eine grosse Zahl an potentiellen Angriffspunkten. Hierzu zählt auch die Unterstützung von Fast Ethernet und Token Ring. Dank des einzigartigen Digital-FingerPrints-Verfahrens untersucht RealSecure viele Pakete pro Sekunde und ist gleichzeitig in der Lage nach hunderten von Angriffsmustern zu suchen. Eine Aufgabe, die mit der steigenden Übertragungsgeschwindigkeit in den Netzen immer komplexer wird.

- Umfangreiche Gegenmassnahmen

RealSecure verfügt über einen grossen Umfang an Gegenmassnahmen gegen unbefugte Netzbesucher. Das System überwacht hierzu die interne Datenübertragung sowie den Datenverkehr von aussen, der durch Firewall-Tunnels in das Netz kommt. Auf verdächtige Aktivitäten reagiert RealSecure sofort und schneidet die Session für eine spätere, genaue Überprüfung mit. Gleichzeitig alarmiert das System den Netzadministrator oder trennt automatisch die Verbindung. Zur Analyse oder als Beweis für einen kriminellen Einbruchsversuch können die aufgezeichneten Sessions später erneut abgespielt werden.

Zusätzlich bietet RealSecure neue, benutzerdefinierte Reaktionsmöglichkeiten, so dass Security-Administratoren mehr Kontrolle über ihre Netze haben. Auf diese Weise können sie sofort und mit aller Macht auf Einbruchsversuche reagieren. Diese Möglichkeit ist der erste Schritt in Richtung selbstheilender Netze und gibt den Anwendern den umfassendensten Schutz für ihre Netze.

3.4.6 Beispielaufbau mit Real Secure



3.5 IDS - Produkte

Dieses Kapitel gibt eine Übersicht über einige auf dem Internet bekannten IDS-Produkte.

3.5.1 Kommerzielle Auditing-Produkte

Name	Beschreibung
eTrust	Netzwerk Analyzer (Windows)
EnGarde T-Sight	Netzwerk Analyzer (Windows)
ICEcap Security Suite von Network ICE	Netzwerk Analyzer, Host- und Netzwerkbasierend (Windows)
NetRanger von Cisco	Netzwerk basierendes IDS mit Sensor und Director (Unix)
Dragon Intrusion Detection von NSW	Netzwerk basierendes IDS mit Sensor, Squire und Server (Unix)
Centrax 2.3 von CyberSafe	Hostbasiert, Netzwerk, Netzwerkknoten intrusion detection (Unix+Win)
Intruder Alert 3.0 und NetProwler	Netzwerk basierendes IDS mit Interface, Agent, Manager (Unix+Win)
Real Secure 5.0 von ISS	Netzwerk basierendes IDS mit Console und Sensor (Unix+Win)
CyberCop Monitor Network Associates	Hostbasierende IDS (Unix+Windows)

3.5.2 Freeware Auditing-Toolkits

TAMU	Schwachstellenanalyse
COPS	Schwachstellenanalyse
SATAN	Netzschwachstellenanalyse
Crack	Passwort-Cracker

4 Vorbereitung

4.1 Theorieteil

- Lesen Sie den Theorieteil
- Lesen Sie die beiden Dokumente 'Site Security Handbook' und 'Users Security Handbook' im Anhang
- Lösen Sie die Aufgaben

4.2 Sicherheitskonzept

Stellen Sie sich vor, Ihr Auftraggeber möchte einen Internetanschluss einrichten. Er beauftragt Sie ein Sicherheitskonzept für die Firma zu erstellen und einzuführen.
Versuchen Sie auf Grund der unter 4.1 gelesenen Informationen ein Sicherheitskonzept für die Ausgangssituation unter 4.2.1 zu formulieren.
Sie werden während der Durchführung einen Teil dieses Konzeptes implementieren.

4.2.1 Ausgangssituation

Ihr Auftraggeber ist ein kleines Ingenieurbüro welches hauptsächlich Teile für den Automobilbau entwickelt. Es werden folgende Informatikmittel verwendet:

- 30 Arbeitsplätze:
  10 x UNIX Workstation mit Solaris
  20 x PC mit Windows NT
- 3 Server:
  1 x Novell Netware als Dateiserver
  1 x Windows NT für Administration und Buchhaltung
  1 x Solaris mit Entwicklungsdaten, Plänen und der Produktedatenbank
- 4 Heimarbeitsplätze (verbunden über Dial-Up Zugänge)

Neu eingeführt wird:

- E-Mail für alle
- Web Zugriff für alle
- FTP Zugang für den Dateiaustausch mit Partnern
- Ein Webserver auf welchem ein Auszug aus der Produktedatenbank präsentiert wird
- Telnet Zugang auf die Produktedatenbank für Partner

4.2.2 Erwartetes Resultat

Beantworten Sie für das Management dieser Firma die folgenden Fragen: (max. 1 Seite A4)

- Welche Bedrohungen erwarten Sie?
- Welche Massnahmen wollen Sie treffen?
- Was benötigen Sie neu an Ressourcen (Hard- Software und Personal)?
- Kosten/Nutzen bzw. Argumente für die Einführung?
- Welche Einschränkungen sind für die Benutzer/Abläufe zu erwarten?
- Ist das Firmennetz nach der Installation der Firewall absolut sicher? Was könnte ein IDS bewirken?
- Überlegen Sie sich auf welche Art die Firewall und das IDS zusammenarbeiten können?

Stellen Sie als Vorbereitung für die Durchführung zusätzlich die Funktionen der Firewall graphisch dar.

Tips:

- Da sich dieses Praktikum mit Firewalls beschäftigt, sollten Sie auch eine vorsehen...
- Sie müssen nicht jedes technische Detail lösen, sondern Ihre Lösung nur grob skizzieren

5 Durchführung

5.1 Einleitung

Sie werden bei der Durchführung mit UNIX arbeiten. Deshalb hier zur Repetition noch eine Übersicht über Unix-Kommandos im Vergleich zu DOS-Befehlen:

Vergleich DOS- und Unix-Kommandos

Unix	DOS	Beschreibung
cd	cd	Verzeichnis wechseln
chgrp	-	Dateigruppe wechseln
chmod	-	Zugriffsrechte ändern
chown	-	Dateibesitzer ändern
cp	copy	Datei kopieren
env	set	Umgebungsvariablen anzeigen
find	dir [datei] /s	Datei suchen
grep	-	Suchen nach Wörtern in einer Datei
kill	-	Prozess beenden
ls	dir	Verzeichnis anzeigen
man	help	Hilfe zu Kommandos
mkdir	md	Verzeichnis anlegen
more	type	Textdateien anzeigen
mv	move	Dateien und Verzeichnisse verschieben
rm	del	Dateien und Verzeichnisse löschen
rmdir	deltree	Verzeichnisse löschen
setenv	set	Umgebungsvariablen setzen
vi	edit	Texteditor aufrufen

Hinweise

UNIX ist CaSe sEnSiTiV

Wissen Sie einmal nicht, welche Parameter ein Kommando benötigt oder welche Optionen möglich sind, so geben Sie

man [Kommando]

ein. *man* ist die Online-Hilfe von Unix. Übrigens - *man* gibt auch Auskunft über verschiedene Konfigurationsdateien wie hosts, networks, inetd.conf etc..

5.2 Unix-Networking

In diesem Abschnitt lernen Sie die Unix-Netzkonfiguration kennen. Dabei verwenden Sie einige TCP/IP-Tools, um sich einen Überblick über die zur Netzkonfiguration benötigten Dateien zu verschaffen. Es wird zusätzlich jeweils die Funktion der Datei und deren sicherheitsrelevanten Aspekte beschrieben. Zum Abschluss dieses Abschnitts werden Sie eine vorbereitete (!) *passwd*-Datei mit Hilfe eines Passwort-Crackprogramms "analysieren".

Führen Sie an dieser Stelle folgenden Befehl aus, um das System in einen definierten Zustand zu setzen: **cleanup**

5.2.1 Das Verzeichnis /etc

Im Verzeichnis */etc* (und seinen Unterverzeichnissen) befinden sich Konfigurationsdateien für die Programme des Root-Filesystems sowie rechnerspezifische Konfigurationsdateien für andere Distributionen. Alle Dateien in diesem Verzeichnis sind ASCII-Dateien und können mit einem normalen Editor wie z.B. *vi* bearbeitet werden. Aus Sicherheitsgründen sollte nur der Administrator (**root**) schreibend auf diese Dateien Zugriff haben.

Je nach System stehen verschiedene Tools zur Verfügung um diese Dateien zu bearbeiten und Konsistenz zwischen ihnen zu gewähren.

Allgemeine Konfigurationsdateien

/etc/group

In dieser Datei sind die Benutzergruppen und ihre Mitglieder festgehalten. Jede Zeile entspricht einem Datensatz welcher folgendermassen aufgebaut ist:

```
groupname:password:  gid:user-list
```

mit:

- groupname = Der Name der Gruppe
- password = Passwort für die Gruppe
- gid = Numerische Gruppennummer (üblicherweise kleiner 60000)
- user-list = Usernamen aus /etc/password der Mitglieder (durch Komma getrennt)

Sinn der Gruppenbildung ist es, den Benutzern einen kontrollierten Zugriff auf bestimmte Teile des Systems (z.B. Drucker, News, Diskettenlaufwerk etc.) zu geben. Es stellt somit einen systeminternen Sicherheitsmechanismus dar.

/etc/passwd

Die Datei *passwd* ist die Benutzerdatenbank des Systems. Hier werden die Namen, die Benutzernummern und das *home*-Verzeichnis der Anwender gespeichert:

```
uname:pwd:uid:gid:gcos-field:home-dir:login-shell
```

mit:

- uname = Der login Name des Benutzers
- pwd = dieses Feld ist leer, die eigentlichen Passworte sind in *shadow* verschlüsselt abgelegt
- uid = Numerische Benutzernummer
- gid = Numerische Gruppennummer (der Standardgruppe)
- gcos-field = Vollständiger Name des Benutzers
- home-dir = Homeverzeichnis des Benutzers
- login-shell = Die Shell welche nach dem Login gestartet wird.

Die Passworte waren früher üblicherweise verschlüsselt an der zweiten Stelle der *passwd* Datei eingetragen. Da diese Datei aber für alle User lesbar sein muss ist es für jeden Benutzer des Systems einfach eine solche Datei als Eingabe einem Passwort Crack Programm zu füttern und die Passworte herauszufinden.
Moderne UNIX Implementationen verwenden deshalb diesen "Shadowing" Mechanismus mit zwei Dateien. Die separate Datei ist für Systembenutzer im Gegensatz zu *passwd* nicht direkt lesbar.

/etc/syslog.conf

syslog.conf ist die Konfigurationsdatei zum entsprechenden Dämon syslogd. syslogd wird meist beim Booten gestartet und zeichnet alle Systemaktivitäten auf. Darunter fallen z.B. Debugging-, Info-, Warning-, Error- und weitere Meldungen. syslog.conf wird dazu gebraucht, festzulegen, wo syslogd seine Loginformationen ablegen soll. Sie enthält demnach folgende Einträge:

Art der Meldung; Ablageort(Pfad und Dateiname)

Bei der Art der Meldung unterscheidet man verschiedene Dringlichkeitsstufen. Schauen Sie sich hierzu die Möglichkeiten an mit:

```
man syslogd oder
man -s4 syslog.conf
```

Wichtige Netz-Konfigurationsdateien

/etc/ethers

ethers kann die MAC-Adressen (48Bit Ethernet Adresse) aller Rechner an einem lokalen Netz enthalten. Sie wird von Programmen wie rarpd verwendet um eine Zuweisung zwischen **IP-Adresse - Hostname - MAC Adresse** zu ermöglichen und z.B. Diskless Clients beim Start mit einer IP Adresse und Hostnamen auszustatten. Die Einträge setzen sich folgendermassen zusammen:

```
MAC-Adresse Rechnername
```

/etc/hosts

In der Datei hosts werden die (noch) vier Byte langen IP-Adressen den verbalen Namen der Netzwerkrechner zugeordnet. Die Einträge bestehen aus den IP-Adressen der Hosts am Anfang der Zeile und den Namen der Rechner. Wir mit einem anderen Namenssystem (DNS oder NIS) gearbeitet ist diese Datei häufig bis auf den Eintrag des eigenen Hosts leer.

Eine Ergänzung zu hosts ist die Datei hosts.equiv. die eine Liste von vertrauenswürdigen Maschinen enthält. Mit einem Eintrag in dieser Datei wird eine Kombination von Benutzer und System dem Zielsystem vertrauenswürdig gemacht. Danach kann dieses vertrauenswürdige System mittels r-Befehlen eine Verbindung zu dieser Maschine aufzubauen, ohne dass dabei ein Passwort abgefragt wird.

Ein Hauptziel eines jeden Angreifers ist die Datei hosts.equiv. Wenn es ihm gelingt, in der Datei einen Eintrag zu deponieren, dann steht ihm, sofern der Systemadministrator es nicht vorher merkt, immer eine Hintertüre offen. Die Information über existierende Hosts aus der Datei hosts liefert dem Angreifer neue mögliche Angriffsziele.

/etc/inetd.conf

inetd.conf ist die Konfigurationsdatei zum inet-daemon (inetd). inetd lauscht auf den TCP/IP-Ports auf ankommende Verbindungsanforderungen. Bei einer Verbindungsanforderung aktiviert er den entsprechenden Server.
Angreifer sind sehr an der Datei interessiert, da sie ihnen angreifbare Dienste auflistet. Zur Protokollierung der inet-Aktivitäten ist ein TCP-Wrapper sehr gut geeignet.

/etc/netmasks

In der Datei netmasks sind alle vom System benötigten Subnetzmasken eingetragen. Mit Hilfe der Einträge kann die Maschine feststellen, in welches Subnetz das empfangene Paket zu senden ist. Das entspricht einer Routing-Funktion, die nur auf Maschinen mit mehreren Netzwerkschnittstellen nötig wird.
Die Datei stellt keine (bekannten) sicherheitsrelevanten Funktionen dar.

/etc/networks

Die Datei networks teilt Netznamen IP-Adressen zu. Sie ist mit der Datei hosts zu vergleichen.
Ein Angreifer erhält mit dieser Datei "nur" Informationen über die Netztopologie.

/etc/services

Die Datei services enthält eine Zuordnung von Portnummern zu Diensten. Die Einträge haben folgendes Format:

```
Dienstname Portnummer Protokoll Alias
```

Wenn die Portnummer und das Protokoll zusammen angegeben werden, sind die Angaben mit einem Schrägstrich (/) getrennt.
Ein Angreifer kann sich durch Verlegen eines Standardports auf einen höheren, nichtpriviligierten Port (1023) eine Einschlupf schaffen. Dazu muss er jedoch **root**-Zugriff haben.
Diese Datei steht im Zusammenhang mit inetd.conf. Der Dienstname in /etc/services wird in inetd.conf wieder benutzt um die Eigenschaften für den jeweiligen Dienst zu bestimmen.

5.2.2 Wichtige TCP/IP-Werkzeuge

In folgenden Abschnitten werden verschiedene TCP/IP-Werkzeuge beschrieben. Dabei wird kurz deren Funktion erläutert. Wenn Sie jedoch zu einem Werkzeug detailliertere Angaben wünschen, dann verwenden Sie dazu das Online-Handbuch. Sie geben dazu einfach **`man`** ***`Ausdruck`*** an. Das System zeigt Ihnen darauf eine detaillierte Beschreibung der Funktion und aller möglichen Optionen des entsprechenden Werkzeugs.

arp

arp wird dazu verwendet, anhand einer IP-Adresse die entsprechende MAC-Adresse zu ermitteln. Als Parameter wird die IP-Adresse des gewünschten Systems angegeben. Die MAC-Adresse wird vom Schicht-2-Protokoll zur Adressierung des Zielsystems benötigt. Mit *arp* lassen sich aber auch Modifikationen am aktuellen ARP Cache durchführen. Mit arp -a kann der gesamte aktuelle Cache ausgegeben werden.

finger

Mit *finger* lassen sich Informationen wie Login-Name, richtiger Name, Terminal-Name, Bereitschaftszeit, Loginzeit und Standort der aktiven Benutzer eines Systems anzeigen. Mit verschiedenen Optionen kann ein bestimmtes Ausgabeformat der Informationen erzeugt werden.

ifconfig

ifconfig wird für die Konfiguration der Netzwerkschnittstelle eingesetzt. Dazu gehört das Festlegen der Netmask, der Broadcast-Adresse, der IP-Adresse und eine Angabe, ob die Schnittstelle aktiv ist oder nicht. Normalerweise wird *ifconfig* beim Systemstart ausgeführt. Man kann aber auch während dem Betrieb Änderungen an den aktuellen Einstellungen vornehmen.

netstat

netstat zeigt verschiedene netzwerkbezogene Informationen in verschiedenen Formaten abhängig von den Optionen an. Sie können damit Routingtabellen, die Speicherauslastung innerhalb des Netzwerks, eine Protokollstatistik usw. anzeigen lassen.

ping

Der Name *ping* stammt von einem Sonarsystem, bei welchem ein Ping als Tonimpuls ausgesendet wird. *ping* arbeitet mit dem gleichen Prinzip, verwendet aber anstelle Tonsignals jedoch das ICMP-Element *ECHO_REQUEST*. Die angesprochene (oder besser "angepingte") Maschine antwortet auf jedes empfangene Paket mit einem ICMP-*ECHO_REPLY*. Die anfragende Maschine erhält dann die Meldung `host is alive`. Sollte die Maschine nicht erreichbar sein, wird nach einem *Timeout no answer from host* eine Fehlermeldung ausgegeben. Die Standardeinstellung des Timeouts ist 20 Sekunden. Wenn *ping* standardmässig aufgerufen wird, d.h. ohne eine Option anzugeben, dann muss es mit Ctrl+C beendigt werden. *ping* verfügt über zahlreiche Optionen. An dieser Stelle sei auf das Online-Handbuch verwiesen.

traceroute

traceroute steht für "verfolge Route" und liefert alle Teilstrecken zwischen Quellsystem und Zielsystem, die ein Paket auf seinem Weg durchwandert. Dabei verwendet es das *time-to-live*-Feld im IP-Paket, um eine allfällige *ICMPTIME_EXCEEDED*-Meldung bei entsprechenden Gateways auf dem Weg zum Ziel zu ermöglichen. *traceroute* sendet so lange Pakete aus, bis entweder die maximale Anzahl an Pakten erreicht ist oder der entfernte Rechner mit der Meldung *ICMP PORT UNREACHABLE* antwortet. Somit versucht es, den Weg ausfindig zu machen, den ein IP-Paket voraussichtlich einschlagen wird, um zum entsprechenden Host zu gelangen.

5.2.3 Aufgaben zu UNIX Networking

Aufgabe 1

Suchen Sie die folgenden Angaben über die WS und den PC zusammen:

- Hostname
- IP Adresse(n) und zugehörige Netzmaske(n)
- Schnittstelle(n) und deren MAC Adresse(n)

Skizzieren Sie mit diesen Angaben den Aufbau des Praktikumsplatzes mit Angabe der Schnittstellen, Adressen und Netzmasken. Wir werden im folgenden die PC-WS Verbindung als "intern" und alles andere als "extern" betrachten.

Aufgabe 2

Was ist ein Dämon? Wie können Sie einen aktiven Dämonen auf der WS finden?

Aufgabe 3

Welche Netzwerk Verbindungen sind auf der WS aktiv?

Aufgabe 4

Stellen Sie vom PC aus mit *telnet* eine Verbindung zur WS her.

- Was geschieht beim Verbindungsaufbau in Bezug auf *inetd*?
- Welcher Dämon muss aktiv sein, damit die Verbindung überhaupt aufgebaut werden kann?
- Welcher Dämon wird zusätzlich noch benötigt?
- Wo befindet sich die ausführbare Datei des Dämons?

Wie funktioniert dasselbe bei einer *FTP*-Sitzung? Bauen Sie vom PC aus eine *ftp* Verbindung auf und übertragen Sie danach zusätzlich noch Daten.

Aufgabe 5

- Welche Benutzer sind auf der WS eingeloggt?
- Welche Benutzer sind auf dem Rechner "arosa" eingeloggt und wie lange ist dieser schon unbenutzt?

Zum Abschluss des Teils Unix-Networking versuchen Sie in folgender Aufgabe, eine vorbereitete *passwd*-Datei mit einem *Crack-Tool* zu entschlüsseln. Das Crack Tool verwendet ein Wörterbuch. Mal sehen, welche Passwörter die Datei enthält!

Aufgabe 6

Der Durchlauf eines Crackprogrammes dauert meist einige Stunden und ist deshalb bereits vorbereitet: Geben Sie crack_report ein. Damit erhalten Sie eine Ausgabe mit der originalen Passwortdatei, dem Resultat des Programmes *john* und den Ergebnissen des Programmes *Crack*. Bei John wurde nur ein kleines Dictionary verwendet, dafür aber einige intelligente Permutationen und Crack ein etwas grösseres Wörterbuch welches auch die deutsche Sprache unmfasst. Sie können die Funktionsweise der beiden Programme in der Dokumentation nachlesen: Für *John* unter ~fw/praktikum/john/doc/* und für *crack* unter /opt/c50a/doc .

5.3 Firewall-1

In diesem Teil des Praktikums lernen Sie die *FireWall-1* kennen.

Danach nehmen Sie einige Einstellungen zur Konfiguration der Firewall vor und installieren die Regeln, die zur Realisierung Ihres Sicherheitskonzepts nötig sind auf der WS.

Führen Sie an dieser Stelle folgenden Befehl aus, damit FireWall-1 anschliessend problemlos funktioniert:

prepare.solstice

5.3.1 Einführung

In folgenden zwei Aufgaben starten Sie Solstice FireWall-1 und verschaffen sich kurz einen Überblick über die grafische Benutzeroberfläche der Solstice FireWall-1.

Aufgabe 7

Schauen Sie sich zuerst den Status des Systems an. Führen Sie dazu in einem *Command Tool* den Befehl **`fw stat`** aus. Die Firewall sollte durch das script *prepare.solstice* bereits gestartet sein. Die Statusmeldung sollte etwa folgendermassen aussehen:

```
HOST    POLICY    DATE
fw      sample    8Dec98  8:55:12 :  [>le1 ] [<le1 ]
```

Sollte dies nicht der Fall sein, müssen Sie die Firewall noch starten. Geben Sie dazu **`FWstart`** ein. Und kontrollieren Sie mit **`fw stat`** den Zustand. Sie können die Firewall jederzeit wieder stoppen indem Sie in einem *Command Tool* folgenden Befehl ausführen: **`FWstop`**.

Nun können Sie das Konfigurationstool starten (**`Rechte Maustaste : Programs : Solstice FireWall-1`**). Es erscheinen folgende Hauptfenster:

- Network Objekt Manager
- Users Manager
- Rule Base Editor

- System Status View
- Services Manager (muss mittels Checkbox angezeigt werden).

Die einzelnen Fenster lassen sich über eine Checkbox im *Rule Base Editor* ein- und ausblenden.

Nehmen Sie sich einige Minuten Zeit, um sich mit der Benutzeroberfläche von *Solstice FireWall-1* vertraut zu machen. Schauen Sie sich die verschiedenen Menus und Menupunkte an.

5.3.2 Konfiguration der Firewall

Um die Firewall aufzubauen, sollten Sie folgende Reihenfolge einhalten:

- Definieren der Netzwerkobjekte
- Definieren von Gruppen/Benutzer
- Definieren von (speziellen) Diensten
- Definieren und Installieren von Sicherheitsregeln.

Für eine detaillierte Beschreibung schlagen Sie bitte im Solstice FireWall-1 Administrator's Guide [solst96] nach.

Definition von Netzwerkobjekten

Als erstes müssen alle Netzkomponenten, die zur Firewallkonfiguration gehören und eine sicherheitsrelevante Funktion ausführen, als Netzobjekte definiert werden. *Solstice FireWall-1* kennt folgende Objekte:

- Host
- Gateway
- Router
- Switch
- Blackbox
- Network
- Domain
- Logical
- Group.

Die Eigenschaften eines Netzwerkobjektes müssen festgelegt sein, bevor es im Sicherheitskonzept (security policy) verwendet wird. Öffnen Sie die Datei *sample.W*, falls diese nicht schon geöffnet ist (**`File : Load : sample.W`**).

Aufgabe 8

Definieren Sie die Netzwerkobjekte welche Sie in Ihrem Konzept vorgesehen haben. Verwenden Sie die richtigen Typen und geben Sie die entsprechenden Adressen ein.

Definition von Gruppen und Benutzern

Mit *FireWall-1* ist es möglich, benutzer- oder gruppenspezifische Privilegien zu vergeben.

Aufgabe 9

- Richten Sie eine Gruppe ein.
- Definieren Sie mindestens einen Benutzer **fwuser** welcher dieser Gruppe angehört Zur Authentifikation verwenden Sie das S/Key Verfahren.

Definition und Installation von Sicherheitsregeln

Bevor Sie damit beginnen, Ihre Objekte in Regeln zu verwenden, speichern Sie Ihre Eingaben in der Datei *sample.W* (**`File:Save As...`**).

Im Folgenden werden Sie Ihr Sicherheitskonzept mittels *FireWall-1* umsetzen. Das Vorgehen sowie einige wichtige Aspekte bei der Definition und Installation von Regeln sind im Administrator's Guide [solst96] im Kapitel 9 ausführlich beschrieben. Lesen Sie deshalb zuerst dieses Kapitel und beginnen Sie danach mit der Aufgabe.

Aufgabe 10

- Realisieren Sie Ihr vorbereitetes Sicherheitskonzept mit Hilfe von Regeln. Benutzen Sie dazu die bereits definierten Objekte.

- Überprüfen Sie nun ihr Sicherheitskonzept mit **`Policy:Verify...`** auf Konsistenz. Es erscheint ein Fenster mit *Security Policy Verified*. Bestätigen Sie mit **`Confirm.`** (Sollte das Sicherheitskonzept Inkonsistenzen aufweisen, erhalten Sie entsprechende Meldungen.)
- Installieren Sie nun Ihre Policy mit **`Policy:Install...`** Bestätigen Sie mit Apply und zweimal OK. Beachten Sie bei der Installation die Statusmeldungen: `Loading Security Policy sample on all.all@fw`
  `Loading Security Policy on localhost (fw) succeed`
  Done.
- Sie müssen diese Installation nach jeder nachträglichen Änderung erneut ausführen.

Definition von Diensten

Solstice FireWall-1 bietet die Möglichkeit, Netzzugriffe nicht nur anhand der Quell- und Ziel-Adresse einer Kommunikationsverbindung zu überwachen, sondern auch anhand des angeforderten Dienstes (service request). Die Dienstprotokolle können in folgende Kategorien eingeteilt werden: TCP, UDP, RPC, ICMP (und Other).

Aufgabe 11

- Verschaffen Sie sich einen Überblick über die vordefinierten Dienste. Sehen Sie sich im Speziellen die Einstellungen von *Telnet*, *FTP* und *HTTP* an.
- Führen Sie *ssh* als neuen Dienst ein und fügen Sie eine neue Regel ein damit Sie vom PC aus mit *ssh* auf die WS zugreifen können.
- Testen Sie diese Konfiguration und verwenden Sie den *Log Viewer*, um Ihre Aktivitäten auf der Firewall zu beobachten. Überlegen Sie sich dabei, welche Bedeutung eine Meldung haben könnte und ob die Firewall gemäss Ihren Einstellungen richtig reagiert. (Zum Test: **`telnet fw 22`**)

Kontrolleigenschaften

In diesem Abschnitt erhalten Sie einen Einblick in die verschiedenen Kategorien der Kontrolleigenschaften. Dabei werden einige Parameter von bestimmten Kategorien näher betrachtet. *Solstice FireWall-1* kennt folgende Kategorien:

- *Security Policy* (Sicherheitkonzept)
- *Logging and Alerting*
- *Names Resolving*
- *Routers*
- Authentication.

Im Solstice FireWall-1 Administrator's Guide [solst96] im Kapitel 5 finden Sie eine ausführliche Zusammenstellung der Kategorien, Parameter und Wertebereiche.

Aufgabe 12

Verschaffen Sie sich einen Überblick über die fünf Kategorien. Beantworten Sie dann die anschliessenden Fragen. Die Antworten auf diese Fragen finden Sie im Administrator's Guide [solst96].

Security Policy

- Welchen Parameter müssen Sie setzen, wenn Ihr Sicherheitskonzept von mehreren verteilten Maschinen realisiert wird? Warum?
- Wie können Sie FTP-Sitzungen erlauben, obwohl Sie alle hohen Ports gesperrt haben? Wie funktioniert das?

Logging and Alerting

- Wie können Sie sich die anfallenden Alarmmeldungen via Mail zukommen lassen? Testen Sie Ihre Lösung gleich aus, indem Sie den entsprechenden Parameter modifizieren. Setzen Sie diesen nach Beendigung des Versuchs bitte wieder zurück in die Ausgangslage.
- Wie lassen sich Alarmmeldungen erfassen, die durch Source-Routing-IP-Pakete erzeugt werden?

Names Resolving

- Studieren Sie die möglichen Nachschlage-Prioritäten (Lookup Priorities) anhand des Administrator's Guide, Kapitel 5 [solst96].
- Warum müssen diese Eigenschaften überhaupt einstellbar sein?

Authentifikation

Solstice FireWall-1 erlaubt das Definieren authentifizierter Zugänge für Benutzer und Clients. Sie überprüfen nun in folgender Aufgabe Ihre Einstellungen des Benutzers **fwuser**, dem Sie zur Authentifikation das S/Key-Schema eingerichtet haben.

Aufgabe 13

- Richten Sie auf der WS eine Regel für den Zugriff mit *telnet* und *user authentication* ein.
- Bauen Sie vom PC eine Telnet-Verbindung zur WS auf.
- Sie müssen nun die entsprechende S/Key challenge beantworten; suchen Sie die entsprechende Zeile im vorher generierten file (/tmp/passwd.list) und geben Sie das Passwort ein (A B S T Ä N D E beachten).
- Sie haben sich nun gegenüber der Firewall erfolgreich authentifiziert und können jetzt den gewünschten Zielhost angeben.
- Damit Sie nicht jedesmal den ganzen Schlüssel eintippen müssen können Sie das Program *winkey* verwenden. Dieses errechnet aus dem Benutzernamen, der challenge Nummer und dem geheimen Passwort (bei der Generierung verwendet) den gültigen Passwortstring aus und Sie können ihn mit Copy/Paste einfügen. Warum geht das? Wo liegt der Vorteil gegenüber einem "normalen" Username/Passwort System?

5.3.3 Adressübersetzung

Die Adressübersetzung wird benötigt, um interne IP-Adressen gegen aussen zu schützen oder gültig zu machen. Letzterer Fall ist notwendig, um internen Hosts, denen keine offiziell gültige IP-Adressen vergeben wurden, trotzdem Zugriff zum Internet zu ermöglichen. Der Zugriff erfolgt dann über einen Proxy-Server, welcher im Internet mit einer gültigen IP-Adresse erscheint. Alle internen Hosts erscheinen somit ebenfalls mit der einheitlichen Proxy-Adresse.

Solstice FireWall-1 verfügt über ein umfassendes Adress-Übersetzungssystem. Sie finden ausführliche Angaben im Administrator's Guide, Kapitel 8 [solst96].

5.3.4 Statistik: Statusanzeige und Logfiles

Wichtige Werkzeuge von *Solstice FireWall-1* sind der *System View* und der *Log Viewer*. Letzteren haben Sie in den Aufgaben schon kennengelernt. Er dient zur Darstellung aller gesammelten Log-Daten. Die *System View* liefert eine Übersicht über die von der Firewall überwachten Systeme und deren Status. Dazu können Sie eine beliebige Regel-Datenbank, welche gerade im Rule Base Editor geladen ist, auf einem beliebigen System installieren.

Zu diesem Abschnitt sind keine Aufgaben vorgesehen, da Sie zumindest den *Log Viewer* bereits in einigen Aufgaben eingesetzt haben. Interessierte finden ausführliche Angaben im Administrator's Guide, Kapitel 11 [solst96].

5.4 IDS Intrusion Detection System

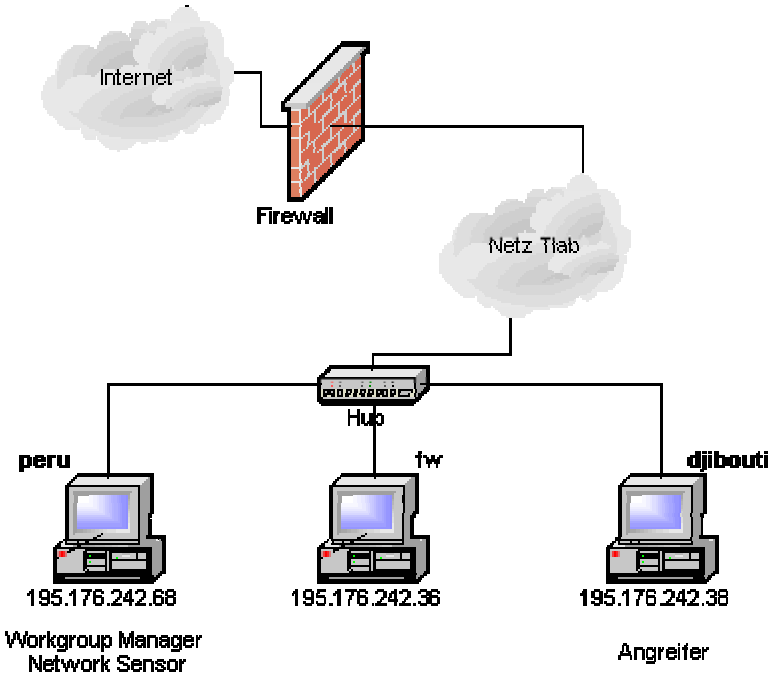
Um mit Real Secure 5.0 besser zurecht zu kommen, wird als erstes ein einfacher Angriff mittels PingFlood Schritt für Schritt durchgespielt. Um den PingFlood zu erkennen und auf dem Bildschirm darzustellen, müssen einige Einstellungen getätigt werden. Wie und wo diese gemacht werden sollen die Screenshots mit den dazugehörigen Bemerkungen erklären.

5.4.1 PingFlood

Aufgabe 14

Um RealSecure schnell und einfach kennenzulernen, ist diese Aufgabe Schritt für Schritt dokumentiert. Hier soll die IDS Software RealSecure einen *PingFlood* erkennen und einen Alarm auf dem Workgroup Manager auslösen.

Aufbau:



Von dem Rechner *djibouti* wird ein PingFlood mit dem Programm *ShadowScan* auf den Rechner *fw* gestartet.

1. Den Rechner *peru* vorbereiten:

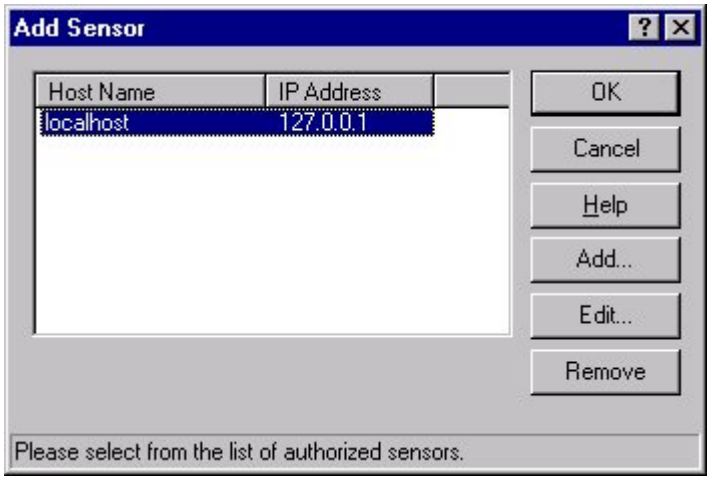
Da dieser Rechner zwei Netzwerkkarten hat, muss man ihm zuerst sagen, mit welcher Netzwerkkarte er nun arbeiten soll. Starten Sie dazu das Batch *useDefault.bat*, welches sich auf dem Desktop befindet.

2. Starten von RealSecure:

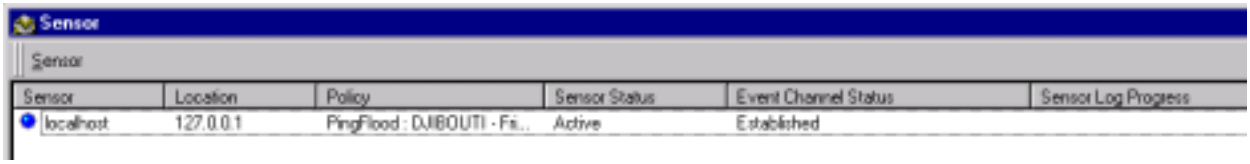
Bei dieser Aufgabe befindet sich der Netzwerk Sensor auf dem gleichen Rechner wie der Workgroup Manager und dieser heisst *peru*. Starten Sie den Workgroup Manager (Start->Programs->RealSecure->RealSecure 5.0).
Der Workgroup Manager besteht aus der Menü Leiste, drei Alarm Fenster (Low-, Medium-, High Priority), ein Sensor Fenster in welchem alle überwachenden Sensoren angezeigt werden und schliesslich das Activity Tree Fenster. In diesem Fenster werden alle Rechner aufgeführt, welche von einem der Sensoren entdeckt worden sind.

3. Sensor überwachen:

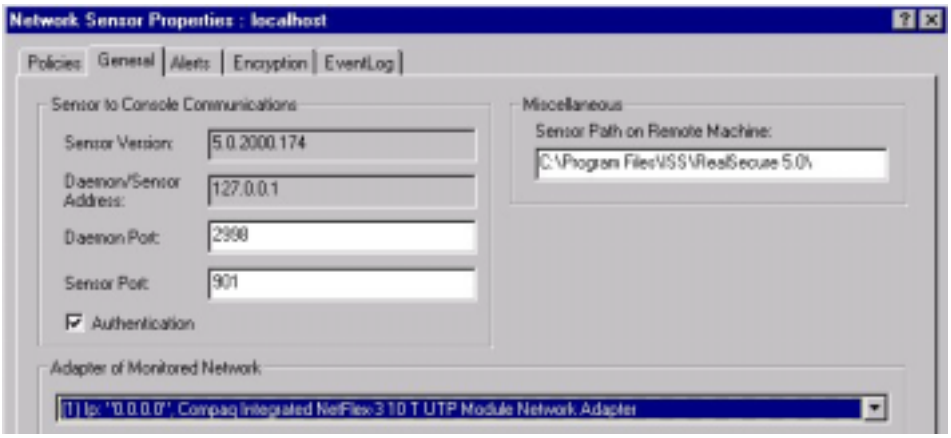
Als erstes wählen wir den Sensor aus, den wir überwachen wollen. Dazu drücken wir im Sensor Fenster *Sensor* und anschliessend *Monitor Sensor* aus. Es erscheint dieses Fenster:



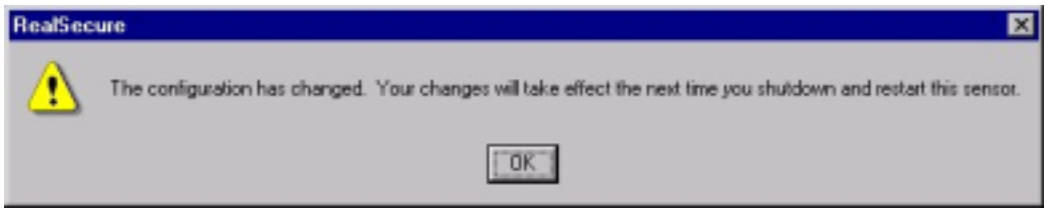
Da sich ja der Sensor und der Workgroup Manager nicht immer auf dem gleichen Rechner befinden, können hier mit Add... zusätzliche Sensoren eingerichtet werden. Wir wählen hier *localhost* mit der IP-Adresse *127.0.0.1*. Der Sensor wird gestartet. Dies wird mit der blau markierten Meldung im Sensor Fenster angezeigt.
Achtung! Man kann einen Sensor mit mehreren Workgroup Managern gleichzeitig überwachen. Jedoch nur einer kann den Sensor kontrollieren, nämlich der *master controller*! (Sensor Fenster Sensor->Set console as master controller). Um die folgenden Einstellungen machen zu können, müssen Sie Master sein. Falls dies nicht so ist, starten Sie beim Rechner *djibouti* den Workgroup Manager, fügen den gleichen Netzwerk Sensor hinzu (195.176.242.68) und deaktivieren dort diese Option. Jetzt können Sie wieder zum Rechner *peru* wechseln und dort die Option einschalten.



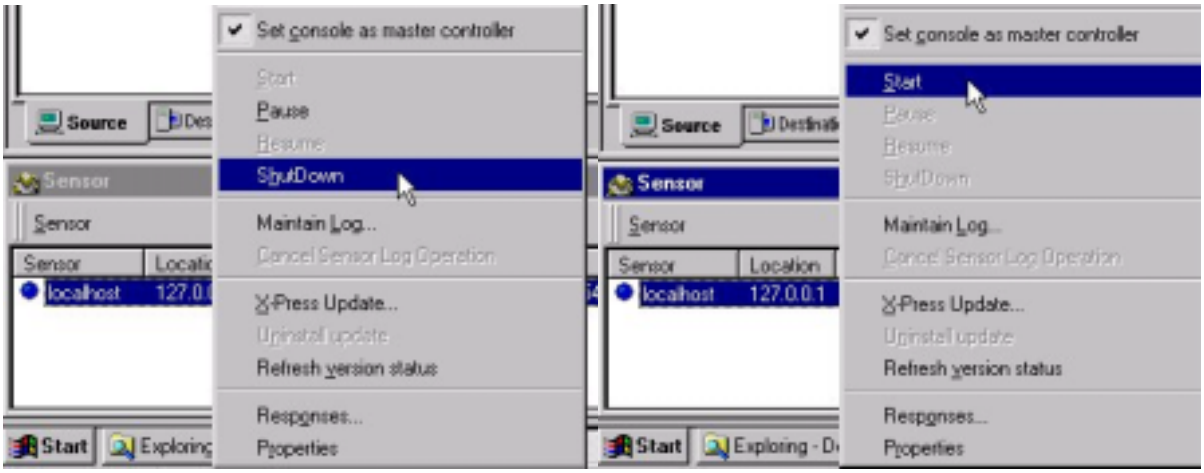
Nun müssen Sie noch überprüfen, ob der Netzwerk Sensor auch auf der richtigen Netzwerkkarte „hört". Dazu klicken Sie auf *Sensor* und wählen *Properties* aus. Im Register *General* kann nun die gewünschte Schnittstelle ausgewählt werden:



Wählen Sie nun als Adapter of Monitored Network die interne Netzwerkkarte NetFlex-3. Bei einem Wechsel von einer Netzwerkkarte auf eine andere muss der Sensor neu gestartet werden. In diesem Fall erscheint folgende Meldung:

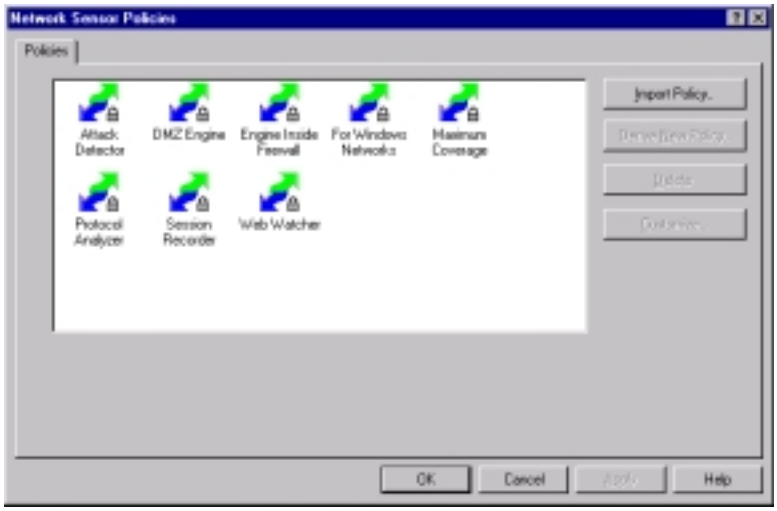


Stoppen Sie den Sensor und starten Sie ihn neu!



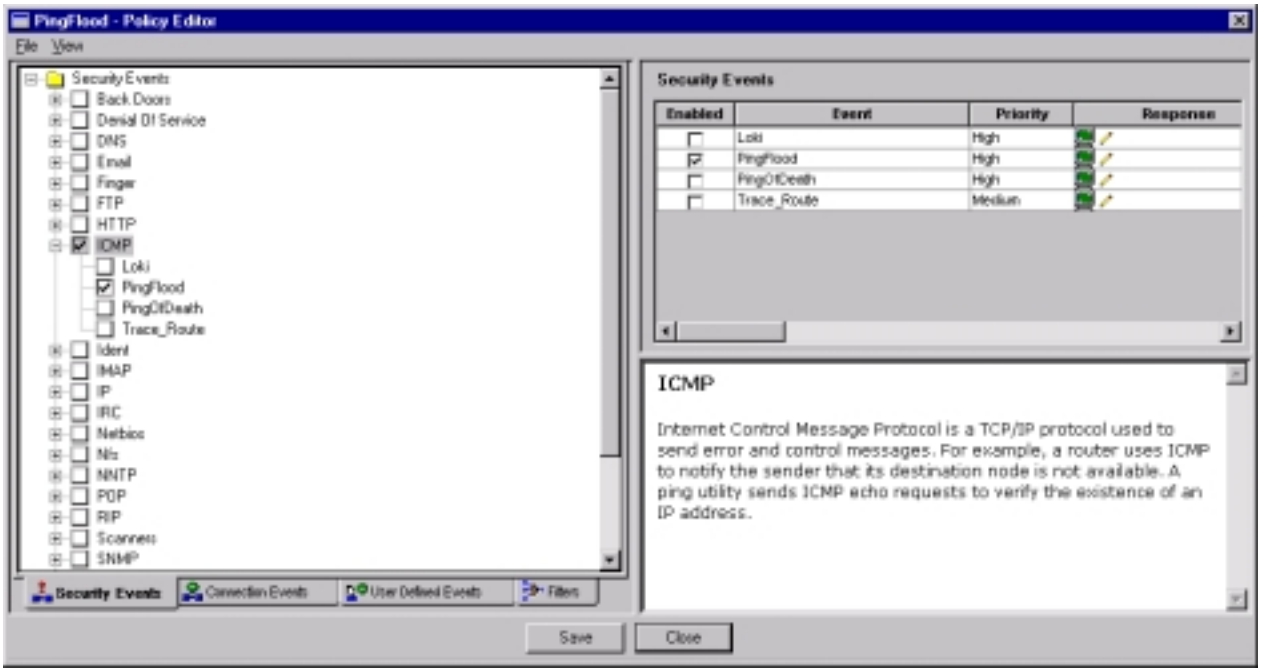
4. Policies einstellen:

Jeden Sensor kann man mit sogenannten Policies einrichten. Das heisst, der Sensor hört nur auf bestimmte Signaturen und kann, sofern diese auftreten, darauf reagieren. Wir werden nun eine solche Policy erstellen. Starten Sie den Policies Editor *(Menü Leiste View->Network Sensor Policies...).* Sie sollten nun folgendes Fenster vor sich haben:

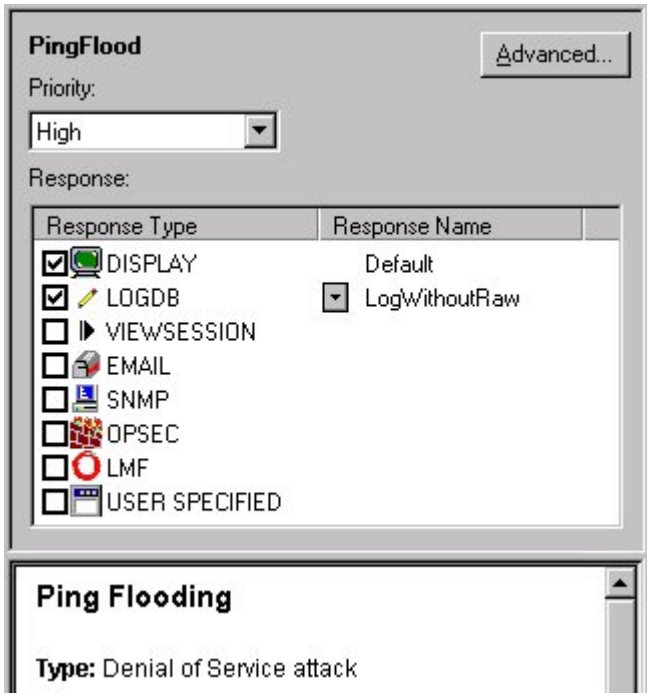


Es gibt bereits neun vordefinierte Policies. Jede dieser Policies sind speziell für einen Netzwerkbereich definiert worden. Wir wollen jedoch eine solche Policy eigenhändig erstellen. Dazu klicken Sie eine bestehende Policy an und drücken anschliessend den *Derive New Policy..* Button. Geben Sie dieser neuen Policy einen Namen (z.B. PingFlood). Nun passen wir diese neu erstellte Policy an, indem Sie die Policy anklicken und den *Customize...* Button betätigen.

Deaktivieren Sie nun alles bis auf den Eintrag *PingFlood*:



Wenn Sie den Eintrag PingFlood anklicken erscheint auf der rechten Seite dieses Fenster:

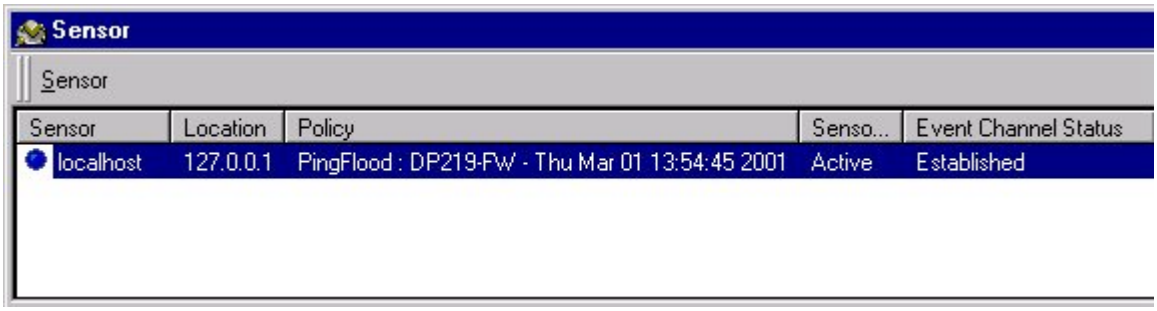


Unter *Priority* kann man den Angriff einstufen. Bei *Response* wird die Reaktion bestimmt, die die Software machen soll, wenn eine PingFlood Attacke erkannt wird. Und schliesslich im untersten Fensterteil erfährt man kurz, was das für ein Angriff ist und wie man darauf reagieren kann.
Wir wählen nur Display und LOGDB aus. Das bedeutet, dass bei einem PingFlood Angriff eine Warnmeldung auf dem Bildschirm erscheint und zwar im High Priority Fenster. Zusätzlich wird in einem Logfile der Angriff protokolliert.
Speichern Sie nun die Policy ab und schliessen Sie das Fenster.

5. Policy auf dem Sensor aktivieren:

Jetzt muss die neu definierte Policy *PingFlood* dem Sensor zugewiesen werden. Dies geschieht so, indem man den Sensor markiert, die *rechte Maustaste* drückt und *Properties* auswählt. Im neuen Fenster markieren Sie die gewünschte Policy und mittels *Apply to Sensor* Button wird diese dem Sensor zugewiesen. Das folgende Fenster sollte dann erscheinen:

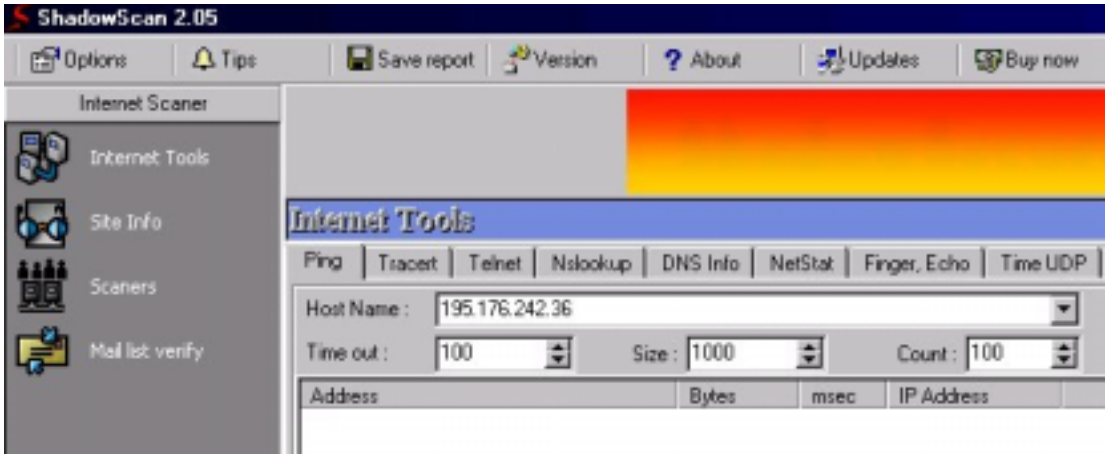
Nun sollte auch im Sensor Fenster diese Policy erkennbar sein:



Jetzt sind in den Alarm Fenster wahrscheinlich einige Meldungen erschienen, welche standardmässig gemacht werden. Diese Meldungen bestätigen, welche Einstellungen gemacht wurden.
Durch Clear All Events können diese Meldungen gelöscht werden, weil diese jetzt nicht mehr benötigt werden und auch verwirren.

6. ShadowScan

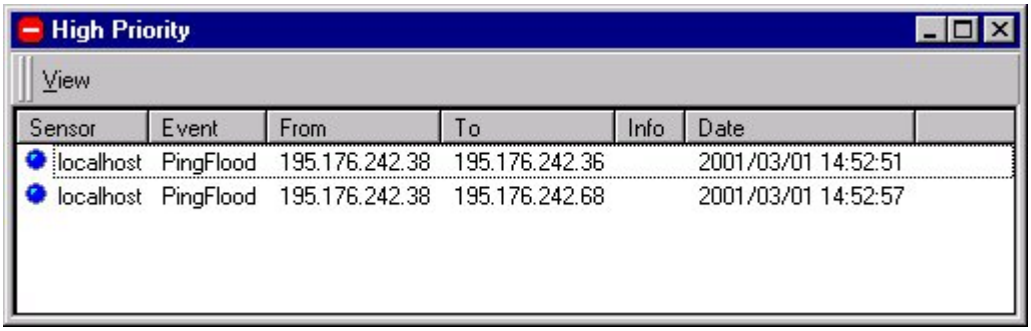
Nun starten Sie ShadowScan auf dem Rechner *djibouti* (Start->Programs->ShadowScan->ShadowScan). Dieses Programm ist ein sehr vielfälltiges Tool. Für diese Aufgabe benützen Sie die Funktion *Ping* (Internet Scaner->Internet Tools->Ping):



Starten Sie nun die Attacke auf den Rechner *fw* (195.176.242.36). Machen Sie zusätzlich einen Angriff direkt auf den Neztwerk Sensor (195.176.242.68).

7. Resultate:

RealSecure gibt den erkannten Angriff im High Priority Fenster an. Es wird die Start- und Zieladresse angezeigt. Dazu noch Angaben über Datum und Zeit des Angriffes.



Überprüfen Sie nun die Log-Dateien. Sychronisieren Sie dazu zuerst die Workgroup Manager Datenbank mit den Sensor Logs. Das geht so:

RealSecure erstellt automatisch aus der Datenbank Kurzberichte. Drücken Sie dazu das Icon wie auf dem folgenden Bild:

Nun haben Sie die Auswahl zwischen verschieden sortierten Berichten. Wählen Sie einen aus und schauen Sie diesen an. Prüfen Sie, ob alle Ping's aufgezeichnet worden sind.
Die RealSecure Datenbank ist übrigens eine Microsoft Access Datenbank. Diese befindet sich im Verzeichnis *c:\program files\iss\realsecure 5.0* und heisst *rsntclientlog.mdb.* Schauen Sie sich auch diese Datei einmal an!

Sie sind nun am Ende der Aufgabe 1 angelangt!

Bemerkung:
Es kann sein, dass nicht alle Attacken auf dem Display angezeigt werden. Zwischen zwei genau gleichen Attacken (gleiche Quelle/Ziel, sowie gleiche Art) muss eine gewisse Zeitspanne liegen, erst dann wird diese Attacke auf dem Bildschirm angezeigt. Bei den Logfiles ist dies nicht so, dort werden alle einzelnen Ping's aufgelistet.

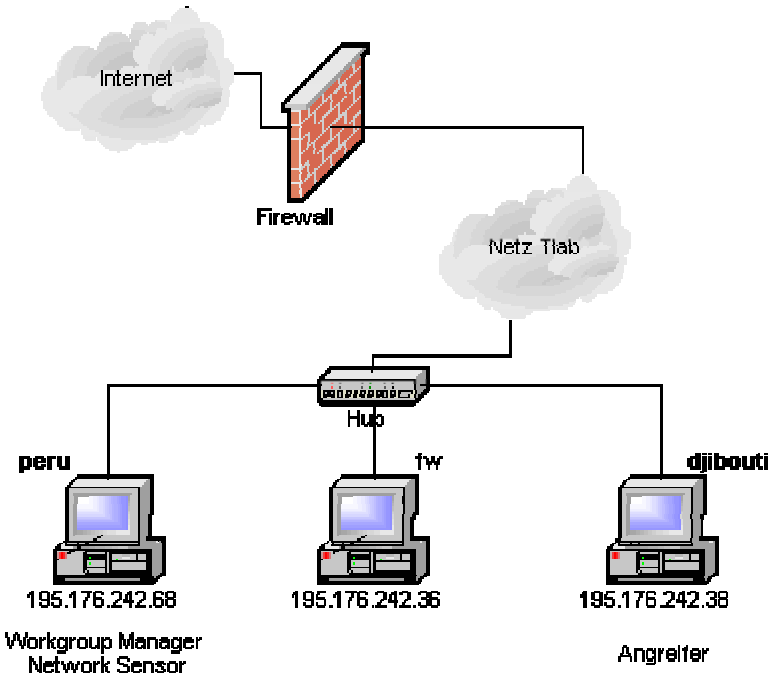
a) Konnten Sie alles wie beschrieben nachvollziehen?
Wenn nein, schreiben Sie die Unterschiede auf!

5.4.2 Portscan

Aufgabe 15

Sie kennen nun die Hauptfunktionen von RealSecure und können diese bei dieser Aufgabe vertiefen.

Aufbau:



Von dem Rechner *djibouti* wird mittels ShadowScan ein Portscan des Rechners *fw* gemacht. Der Netzwerk Sensor soll nun diese Aktion erkennen und mittels dem DOS Befehl `net send` dem Administrator eine Meldung übermitteln! Da wir nicht einen zusätzlichen Rechner aufstellen müssen, schicken wir die Meldung an den Rechner *djibouti* zurück.

1. Damit dem Angreifer eine Meldung übermittelt werden kann, muss dies zuerst bei RealSecure eingerichtet werden. Dies können Sie unter der Menüleiste *View->Global Responses...->User Specified* und anschliessend *Derive New* einstellen. Als *Command* nehmen Sie *c:\winnt\system32\net.exe* und als Arguments *send djibouti* plus eine Meldung nach Ihrer Wahl (Was ist sinnvoll dem Adminstrator bei diesem Angriff mitzuteilen?).
2. Jetzt müssen Sie diese globale Einstellung noch dem Sensor mitteilen und zwar im Sensor Fenster *Sensor->Responses...* Dort muss der *Replace with Global Responses* Button gedrückt werden.
3. Erstellen Sie nun die nötige Policy für einen Portscan. Dabei soll bei einem Angriff eine Meldung auf dem Bildschirm erscheinen und die soeben erstellte neue Aktion muss ausgeführt werden (Response Type: Display und User Specified). Weisen Sie diese Police den Sensor zu.
4. Führen Sie einen Portscan durch.

a) Wie haben Sie das mit dem Befehl *net* realisiert?

Command: c:\winnt\system32\net.exe

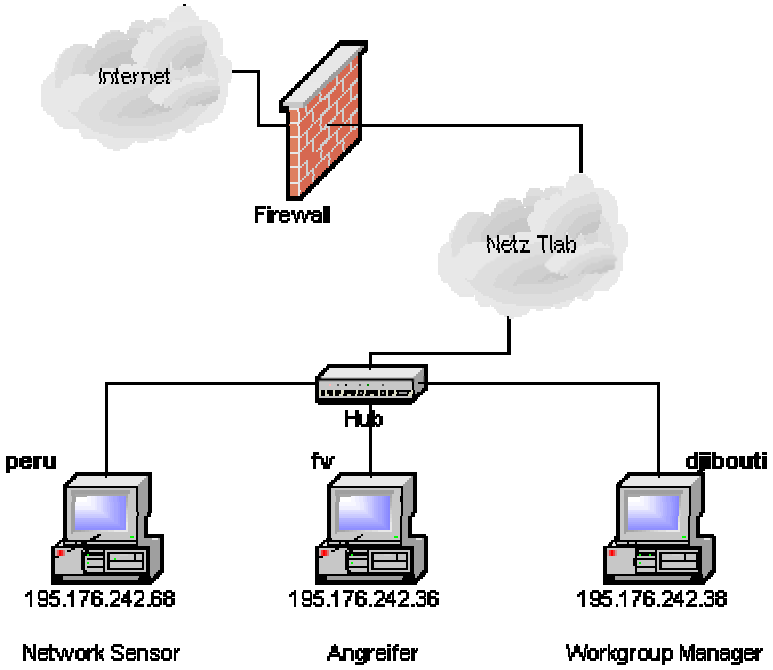
Arguments: send djibouti .....

5.4.3 IP- und Portscan

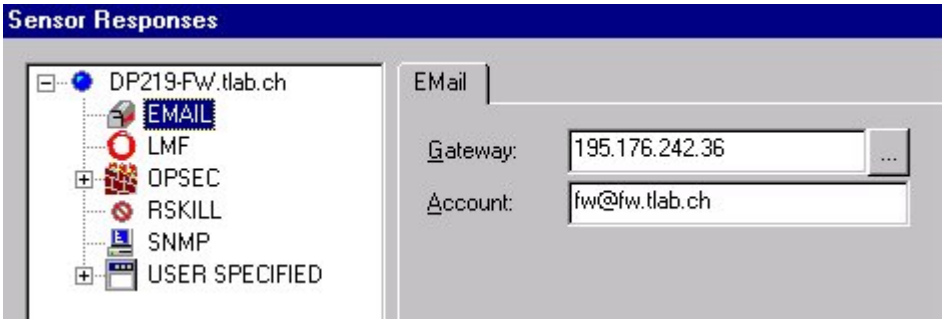
Aufgabe 16

Das Ziel dieser Aufgabe besteht darin, einen weiteren Portscanner kennenzulernen und mittels RealSecure aufzuspüren. Wir verwenden den Portscanner *nmap*, welches ein sehr mächtiges Tool ist. Ausserdem starten wir den Workgroup Manager diesmal auf einem anderen Rechner, als was sich der Network Sensor befindet und es soll ein E-Mail an den Administrator gesand werden, sobald ein Angriff erkannt wird.

Aufbau:



1. Deaktivieren Sie auf dem Rechner peru die Option *Master Controller* (Sensor Fenster: Sensor->Set Console as master controller).
2. Starten Sie den *Workgroup Manager* (Start->Programs->RealSecure->RealSecure 5.0) auf dem Rechner *djibouti* und überwachen Sie den *Network Sensor* mit der IP 195.176.242.68 (peru).
3. Überprüfen Sie bitte die E-Mail Einstellungen (Rechner djibouti). Sensor Fenster *Sensor->Sensor Responses* und dann bei *EMAIL*:



4. Erstellen Sie nun eine Policy auf dem Rechner *djibouti* für einen Portscan. Als *Response Type* wählen Sie *Display* und *EMAIL*. Aktivieren Sie diese Policy.
5. Starten Sie den Rechner *fw* (Benutzer: fw / Password: manager).
6. Lernen Sie das Programm *nmap* kennen indem Sie in der Eingabeaufforderung `man nmap` eingeben.
7. Machen Sie nun einen Portscan mit *nmap* zuerst der IP 195.176.242.68 und anschliessend der IP 195.176.24.38. Falls Sie Root-Rechte benötigen, geben Sie einfach `sudo nmap ....` ein.

8. Sobald RealSecure den Angriff bemerkt hat, können Sie überprüfen, ob auch das mit dem E-Mail geklappt hat. Geben Sie dazu in der Aufgabeeinforderung mail ein. Mit `Enter` können Sie nun durch die E-Mails "zappen", mit d kann das angezeigte Mail gelöscht werden.

a) Mit welchem Befehl haben sie den Portscan durchgeführt?

b) Erkannte RealSecure den Portscan sofort?

c) Was steht in dem Mail drin?

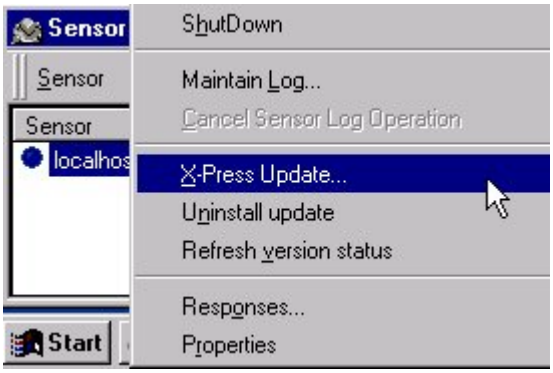
Bitte löschen Sie alle Mails auf dem Rechner *fw*, sobald Sie mit dieser Aufgabe fertig sind.

5.4.4 Update von Real Secure

Aufgabe 17

Mittels der Funktion X-Press Update kann man die RealSecure Software sehr einfach updaten, sowie die neuesten Signaturen installieren. Was ja sehr wichtig ist, weil laufend neue Angriffsprogramme zur Verfügung stehen und das Netz bedrohen.

Lernen Sie die Funktion *X-Press Update* kennen und laden Sie die erhältlichen Updates sowie Signaturen von der ISS Homepage (https://www.iss.net/update/RealSecure) herunter. Dabei gibt es mehrere Möglichkeiten von Updates. Testen Sie alle Funktionen von X-Press! Folgen Sie dabei den Anweisungen.



Die Update-Funktion kann man starten, indem auf einem Senor die rechte Maustaste gedrückt und anschliessend *X-Press Update...* ausgewählt wird.

Bemerkung:
Dabei kommt es vor, das Sie nach einem Update die Überwachung unterbrechen müssen, indem Sie den Sensor anhalten und dann wieder neu starten. Falls es immer noch nicht funktioniert, beenden Sie die Überwachung und starten Sie danach die Überwachung nochmal.
Sind mehrere Sensoren im Einsatz muss für jeden Sensor das Update durchgeführt werden! Dies können wir in diesem Praktikum nicht testen, weil unsere Lizenz nur für einen Sensor bestimmt ist.
Diese neuen Signaturen können Sie nun bei den Policies anschauen (Sensor Fenster:Sensor->Properties , öffnen einer Policy und dann im Register X-Press Updates).

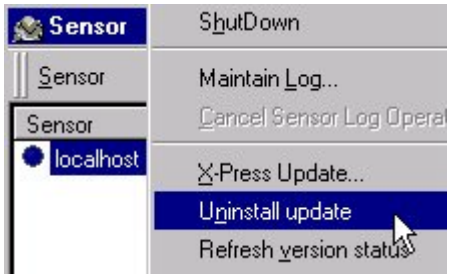
a) Was für Arten von X-Press Updates gibt es und was bewirken Sie?

b) Schreibe Sie ein paar neue Signaturen auf!

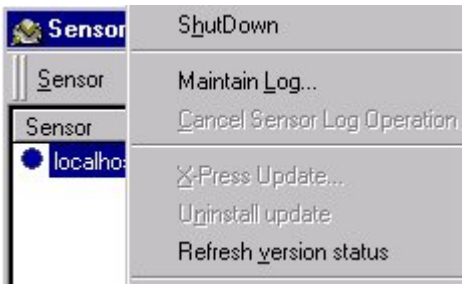
-
-
-
-
-

c) Informieren Sie sich über diese Signaturen! (Falls Sie genug Zeit haben)
Was kann man darüber sagen? Wie gross ist das Sicherheitsrisiko?

Sie haben nun die Update-Funktion von RealSecure kennengelernt. Um den nächsten Praktikumsabsolventen das gleiche Erfolgserlebnis zu garantieren, müssen Sie nun alle Updates wieder deinstallieren!!! Die Deinstallation starten Sie folgendermassen:



Wiederholen Sie diese Prozedur solange bis die Funktion *Uninstall update* nicht mehr anklickbar ist!



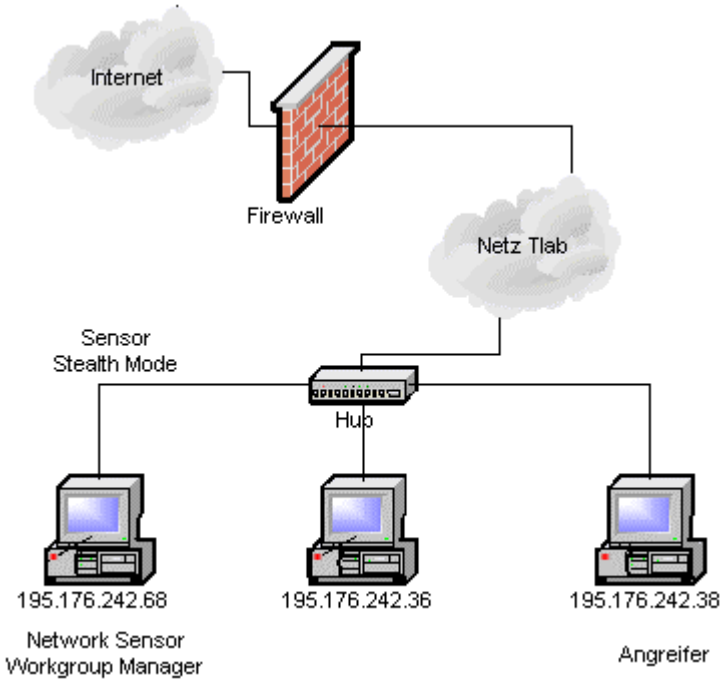
Die Nächsten werden es Ihnen danken!

5.4.5 Stealth Configuration

Aufgabe 18

Im realen Einsatz will man nicht, das der Netzwerk Sensor von einem Angreifer aus sichtbar ist. Damit dieser nicht zuerst den Sensor ausschalten kann (wie auch immer) und anschliessend das restliche Netzwerk ungestört durchforscht. Dafür gibt es den sogenannten *Stealth Mode.* Dabei wir die logische Schnittstelle deaktiviert und so ist die Schnittstelle von aussen nicht mehr sichtbar. Um aber trotzdem mit dem Workgroup Manager kommunizieren zu können, benötigt der Netzwerk Sensor eine zweite Netzwerkkarte oder der Workgroup Manager befindet sich auf dem gleichen Rechner wie der Netzwerk Sensor.

Aufbau:



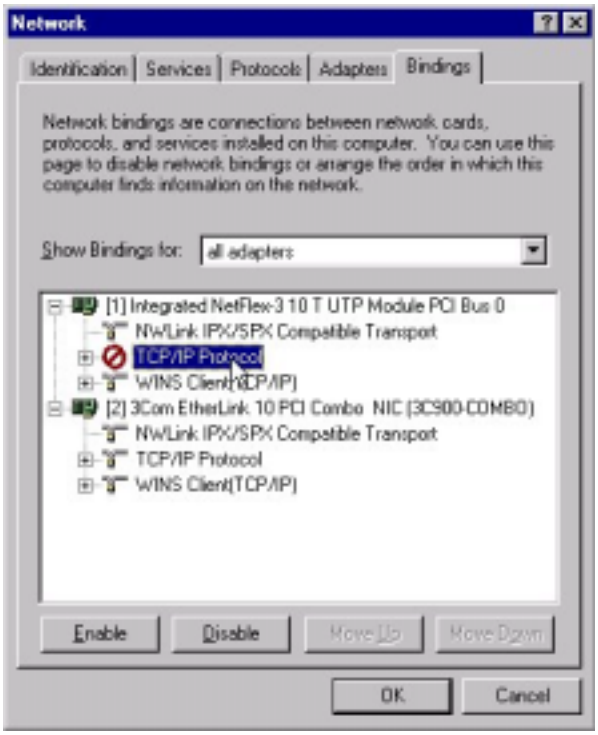
1. Normaler Modus:
   Als erstens starten Sie den Workgroup Manager auf dem Rechner peru und überwachen den Netzwerk Sensor lokal (IP 127.0.0.1). Wählen Sie unter dem Sensor *Properties -> General* die interne Netzwerkkarte aus und als Policy nehmen Sie die vordefinierte Policy *Attacke Detector*.
2. Nun benützen Sie das Tool ShadowScan um die IP-Adresse 195.176.242.68 auszuspionieren (Portscan, NetBiosscan,..)

a) Was haben Sie über die IP-Adresse herausgefunden? (Ausdrucken oder Aufschreiben)

b) Konnte RealSecure den Angriff erkennen?

3. Stealth Modus:
   Deaktivieren Sie bei der integrierten Netzwerkkarte des Rechners *PERU* das logische TCP/IP Interface. Öffnen Sie dazu unter *Start->Settings->Control Panel* die *Network* Einstellungen. Im Register *Bindings* wählen Sie *Show Bindings for all adapters* aus. Nun deaktivieren Sie das TCP/IP Protokoll für die Interne Netzwerkkarte. Alles andere nicht verändern!!!

   Es sollte so aussehen:



   Sobald Sie *OK* klicken, werden Sie aufgefordert den Rechner neu zu starten, um die neuen Einstellungen zu aktivieren. Vergessen Sie nicht, nach dem Starten das Batchfile *useDefault.bat* auszuführen!
4. Überwachen Sie wieder den Netzwerk Sensor und wiederholen Sie die Angriffe mit ShadowScan auf den Rechner peru. Zusätzlich machen Sie einen Angriff auf den Rechner fw.

c) Was können Sie jetzt mit ShadowScan herausfinden?
Vergleichen Sie die Ergebnisse mit den Auswertungen vom a)

d) Konnte RealSecure alle Angriffe erkennen? Begründung!

e) Zeichnen Sie einen sinnvollen Einsatz des Stealth Modes auf!

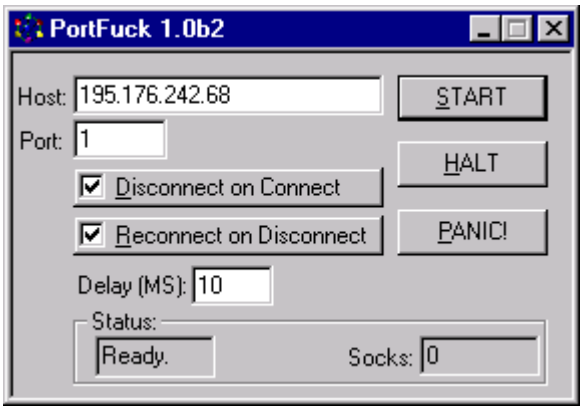
Nachdem Sie diesen Aufbau ausgiebig getestet haben, müssen Sie wieder die logische Schnittstelle aktivieren und Rechner neu starten!

5.4.6 Überlastung des Prozessors

Aufgabe 19

Untersuchen Sie die Auslastung des Prozessors der Rechner *fw* und *peru*, während die Rechner mit einem besonderen Tool (Portfuck) angegriffen werden.

Beschreibung Portfuck:
Ein kleines Programm, aber mit grosser Wirkung. Das Programm nervt den angewählten Rechner mit Connect und Disconnect Meldungen. Der angegriffene Rechner wird mit Anfragen überflutet und kommt nicht mehr nach diese zu verarbeiten. Der Rechner wird blockiert und muss heruntergefahren werden. Bei uns wird dies nicht der Fall sein, weil der Angriff nur von einem Rechner kommt.



Mit *Halt* kann der Vorgang angehalten werden und die Verbindungen werden kontinuierlich abgebaut. Der *Panic* Button bewirkt, dass die Verbindungen sofort abgebaut werden. Mit dem Delay wird die Verzögerung angegeben, welche zwischen den Abfragen gewartet wird. *Socks* ist die Angabe wieviel Ports offen sind.
Tip: Delay nicht unter 10ms wählen, sonst wird der eigene Rechner so ausgelastet, dass Sie nicht einmal den Panik Button drücken können. In diesem Fall muss Portfuck mit dem Task Manager beendet werden.

1. Aktivieren Sie die vordefinierte Policy *Attack Detector* auf dem Sensor und überwachen Sie ihn.
2. Tätigen Sie einen Angriff von *djibouti* auf *peru*, schauen Sie sich die Auslastung des Prozessors im Task Manager des angegriffenen Rechners an. Das Programm finden Sie unter *Start->Programs->RealSecure->PortFuck*.
3. Machen Sie einen Angriff von *djibouti* auf *fw*, schauen Sie sich die Auslastung des Prozessors im Performance Meter der *fw* an.
4. Gleichzeitig zu Aufgabe 3 soll noch ein Portfuck von *peru* auf *fw* getätigt werden.

a) Hat Real Secure den Angriff erkannt?

b) Was für Pakete werden für den Angriff verwendet?

c) Von welcher IP kommt der Angriff?

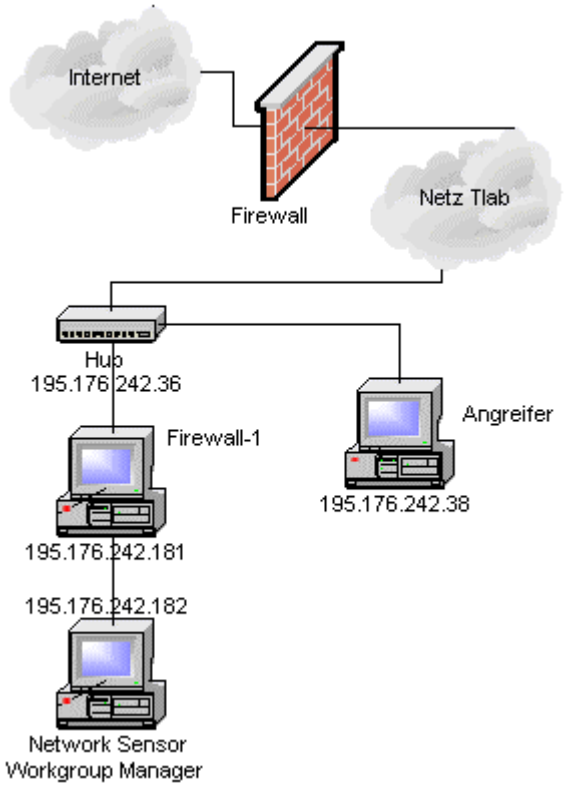
d) Wie hoch war die jeweilige Prozessorauslastung?

5.4.7 Zusammenarbeit von IDS und Firewall

Aufgabe 20

Damit bei einem Angriff eine Gegenmassnahme eingeleitet werden kann, muss die IDS Software mit der Firewall zusammenarbeiten. OPSEC™ (Open Platform for Security) ist eine Allianz, die Interoperabilität mit FireWall-1™ gewährleistet. RealSecure besitzt ein solches OPSEC™ Zertifikat.
RealSecure kann somit bei einem Angriff die Firewall-1 so umkonfigurieren, dass der Angriff sofort abgeblockt wird.
Wir wollen nun in dieser Aufgabe diese Funktion kennenlernen und austesten.

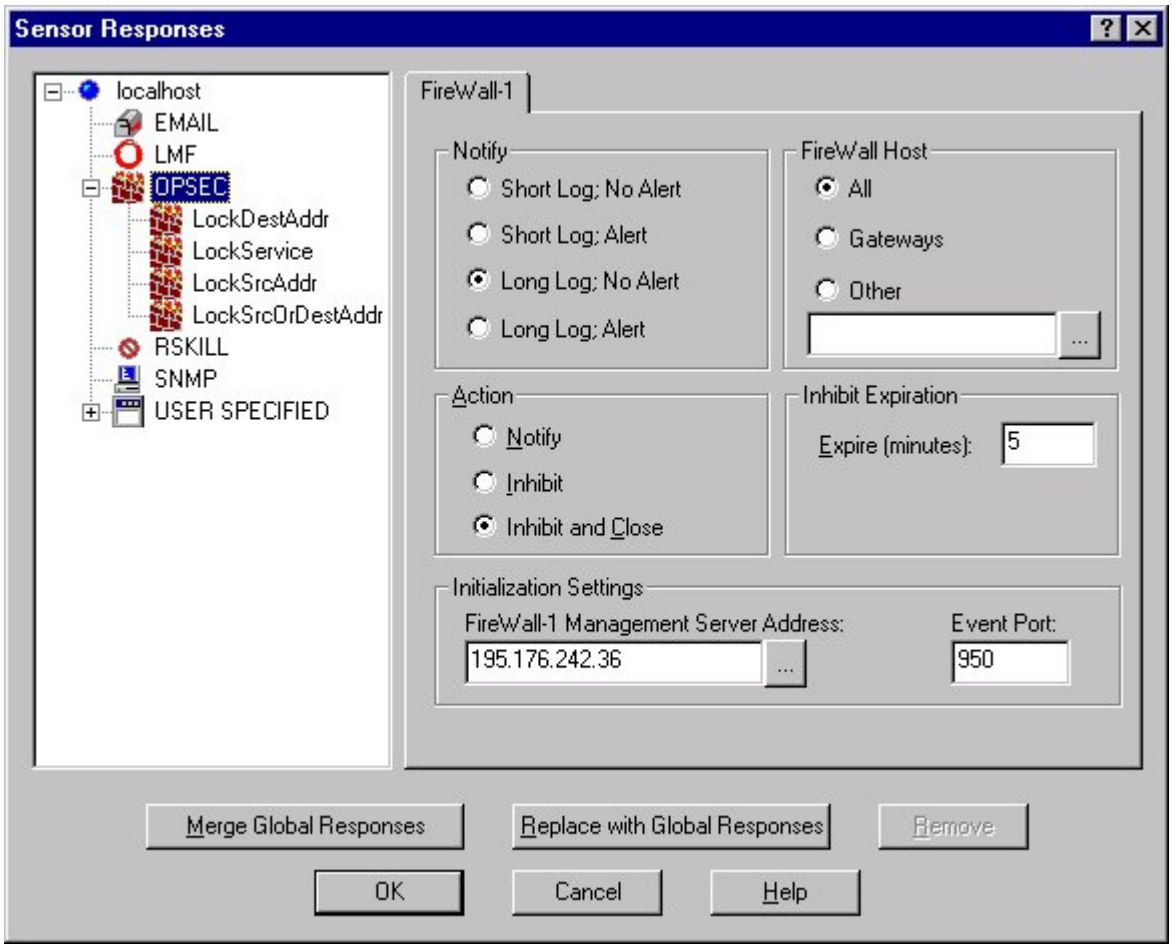
Aufbau:



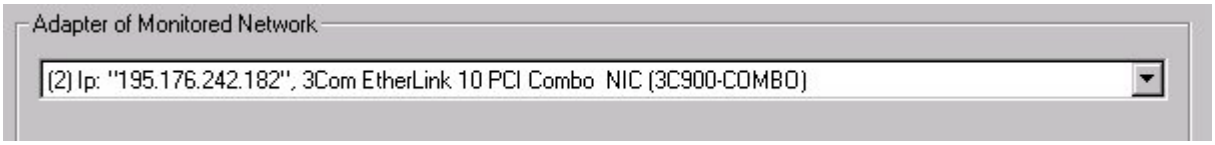
1. Um diesen Aufbau zu erreichen, muss das Batch *useFirewall.bat* auf dem Rechner *peru* ausgeführt werden. Als nächstes richten Sie die Firewall-1 so ein, dass der Rechner einwandfrei mit dem Internet kommunizieren kann.
2. Starten Sie den Rechner *fw.*
3. Bringen Sie die Firewall-1 wieder in den Grundzustand. Geben Sie dazu folgende Befehle ein:
   `cleanup`
   `prepare.solstice`
4. Starten Sie das GUI der Firewall *(rechte Maustaste->Programs->Firewall-1 GUI).*
5. Erstellen Sie die unten aufgeführte Regel:

6. Installieren Sie die Regel *(Police->Install->Apply).*

7. Überprüfen Sie die Sensor Einstellung von RealSecure (Sensor Fenster: Sensor->Responses). Sie sollte so aussehen:



8. Ausserdem schauen Sie, ob die richtige Netzwerkkarte überwacht wird. Stellen Sie diesen Adpater ein: *(Sensor->Properties->General)*

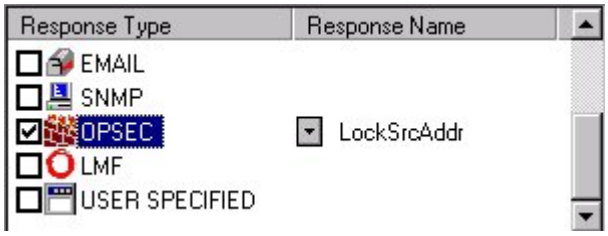


9. Erstellen Sie eine Police für die Erkennung eines Portscan's und als Response Type wählen Sie **nur** *Display!* Aktivieren Sie diese Police auf dem Sensor.

10. Starten Sie ShadowScan auf dem Rechner *djibouti* und führen einen Portscan der IP 195.176.242.182 durch*!*

a) Was für Resultate liefert Ihnen ShadowScan:

11. Nun erweitern Sie die Police mit dem Response Type *OPSEC* und wählen dort als Response Name *LockSrcAddr*. Das heisst, bei einem Portscan wird die Angreifer-IP gesperrt. Und zwar für eine Zeitdauer von 5 Minuten (gemäss Sensor Einstellungen)



12. Wiederholen Sie jetzt den Portscan zwei mal, anschliessend warten Sie mindestens 5 Minuten und machen dann wieder einen Portscan.

b) Wie sehen jetzt die ShadowScan Resultate aus?

1.PortScan:

2.PortScan:

c) Was stellen Sie fest?

d) Warum mussten Sie den Portscan zweimal wiederholen?

e) Wie sieht es nach den 5 Minuten aus?

6 Aufräumen des System

Nehmen Sie sich am Schluss noch ein paar Minuten Zeit, um die Rechner aufzuräumen! Befolgen Sie dazu folgende Anweisung:

6.1 Windows Rechner (peru <u>und</u> djibouti):

1. Unter *View->Global Responses...* löschen Sie alle Einträge bei *USER SPECIFIED.*

2. Unter *View->Network Sensor Policies* löschen Sie alle von Ihnen gemachten Policies!

3. Datenbasis löschen:
   Menüleiste: *File->Synchronize All Logs*
   Menüleiste*: File->Maintain Database...* und dann den *Clear Database* Button drücken.

4. Sensor Fenster: *Sensor->Responses* und dann *Replace with Global Responses Button* betätigen.

5. Setzen Sie den Rechner peru als Master Controller (Sensor Fenster: *Sensor->Set console as master controller).*

6.2 Unix Rechner

1. Mails löschen:
   `mail` eingeben und die Taste d soviel mal drücken, bis Sie wieder auf der Eingabeaufforderung sind.

2. Firewall aufräumen:
   `cleanup` eingeben.

Besten Dank.

7 Nachbearbeitung

7.1 Aufgaben

Aufgabe 19

- Vervollständigen Sie Ihre Unterlagen aus der Vorbereitung mit den Erkenntnissen die Sie jetzt während der Durchführung gewonnen haben.
- Würde die Softwarelösung Firewall-1 genügen um Ihre Kriterien zu erfüllen?
- Versuchen Sie abzuschätzen welcher Zeitaufwand für die Administration Ihrer Lösung nötig wäre.
- Ist eine Fernwartung der Firewall möglich?

Zugriffe auf die Firewall können protokolliert und in einem Logfile gespeichert werden. Welche Zugriffe würden Sie protokollieren? Was geschieht mit den Protokollen? Wie werden sie ausgewertet? Wo werden sie gespeichert (auf dem Firewall-Rechner oder auf einem Management-Rechner)?

8 Anhang

8.1 Firewall-Lexikon

A

Address Spoofing
Verwendung von falschen (Absender-) Adressen in IP-Packeten zur Vortäuschung eines falschen Ursprungs.

Application Proxy
An application that forwards application traffic through a firewall. Proxies tend to be specific to the protocol they are designed to forward, and may provide increased access control or audit.

arp
arp wird dazu verwendet, anhand einer IP-Adresse die entsprechende MAC-Adresse zu ermitteln. Als Parameter wird die IP-Adresse des gewünschten Systems angegeben. Die MAC-Adresse wird vom Schicht-2-Protokoll zur Adressierung des Zielsystems benötigt. Mit *arp* lassen sich aber auch Modifikationen an der ARP-Datei durchführen. So kann mit `arp -d hostname` der Eintrag einer Maschine aus der ARP-Datei gelöscht werden.

B

Bastion Host
A host system that is a "strong point" in the network's security perimeter. Bastion hosts should be configured to be particularly resistant to attack. In a host-based firewall, the bastion host is the platform on which the firewall software is run. Bastion hosts are also referred to as "gateway hosts".

C

D

Dämon
Ein Programm, welches beim Bootvorgang oder beim Starten einer Anwendung gestartet wird und im Hintergrund aktiv bleibt. Es läuft also unsichtbar ab, deshalb der Name *Dämon* -> Geist, Spuk.

DMZ (Grenznetz)
De-Militarisierte Zone. Netz, das als Schutzschicht zwischen ein geschütztes und ein externes Netz eingefügt wird.

Dual-Homed Gateway oder Dual-Homed Host
A firewall consisting of a bastion host with 2 network interfaces, one of which is connected to the protected network, the other of which is connected to the Internet. IP traffic forwarding is usually disabled, restricting all traffic between the two networks to whatever passes through some kind of application proxy.

E

/etc
Im Verzeichnis */etc* befinden sich Konfigurationsdateien für die Programme des Root-Filesystems sowie rechnerspezifische Konfigurationsdateien für andere Distributionen. Alle Dateien in diesem Verzeichnis sind ASCII-Dateien und können mit einem normalen Editor wie z.B. *vi* bearbeitet werden. Aus Sicherheitsgründen sollte nur **root** schreibend auf diese Dateien Zugriff haben.

/etc/ethers
ethers enthält MAC-Adressen aller Rechner an einem lokalen Netz. Sie wird vom *rarpd* dämon verwendet.

F

finger
Mit *finger* lassen sich Informationen wie Login-Name, richtiger Name, Terminal-Name, Bereitschaftszeit, Loginzeit und Standort der aktiven Benutzer eines Systems anzeigen. Mit verschiedenen Optionen kann ein bestimmtes Ausgabeformat der Informationen erzeugt werden.

Firewall
A firewall is any one of several ways of protecting one network from another untrusted network. The actual mechanism

whereby this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blokking traffic, while others emphasize permitting traffic.

G

/etc/group
In dieser Datei sind die Benutzergruppen und ihre Mitglieder festgehalten. Sinn der Gruppenbildung ist es, den Benutzern einen kontrollierten Zugriff auf bestimmte Teile des Systems (z.B. Drucker, News, Diskettenlaufwerk etc.) zu geben. Es stellt somit einen systeminternen Sicherheitsmechanismus dar. Für Angreifer können diese Informationen interessant sein.

H

Host
Ein eigenständiges Computersystem mit Anschluss an einem Netz (PC, Workstation, etc.).

/etc/hosts
In der Datei *hosts* werden die (noch) vier Byte langen IP-Adressen den verbalen Namen der Netzwerkrechner zugeordnet. Die Einträge bestehen aus den IP-Adressen der Hosts am Anfang der Zeile und den Namen der Rechner.

Host-based Firewall
A firewall where the security is implemented in software running on a general-purpose computer of some sort. Security in host-based firewalls is generally at the application level, rather than at network level.

I

ifconfig (Interface Konfiguration)
ifconfig wird für die Konfiguration der Netzwerkschnittstelle eingesetzt. Dazu gehört das Festlegen der Netmask, der Broadcat-Adresse, der IP-Adresse und eine Angabe, ob die Schnittstelle aktiv ist oder nicht. Normalerweise wird *ifconfig* beim Systemstart ausgeführt. Man kann aber auch während dem Betrieb Änderungen an den aktuellen Einstellungen vornehmen.

/etc/inetd.conf
inetd.conf ist die Konfigurationsdatei zum inet-dämon (*inetd*). *inetd* lauscht auf den IP-Ports auf ankommende Verbindungsanforderungen. Bei einer Verbindungsanforderung aktiviert er den entsprechenden Server.

J

K

L

M

MAC-Adresse, arp:
siehe arp

mount:
mount ist ein Unix-Kommando. Mit mount kann eine zusätzliche Festplatten-Partition in ein Verzeichnis eingebunden werden. In Unix kann man dann von Verzeichnis zu Verzeichnis und dabei von einer Platte auf die anderen wechseln. Man kann auch freigegebene Verzeichnisse von anderen Hosts über das Netzwerk 'mounten'.

N

/etc/netmasks
In der Datei *netmasks* sind alle vom System benötigten Subnetzmasken eingetragen. Mit Hilfe der Einträge kann die Maschine feststellen, in welches Subnetz das empfangene Paket zu senden ist.

netstat
netstat zeigt verschiedene netzwerkbezogene Informationen in verschiedenen Formaten abhängig von den Optionen an. Sie können damit Routingtabellen, die Speicherauslastung innerhalb des Netzwerks, eine Protokollstatistik usw. anzeigen lassen.

/etc/networks
Die Datei *networks* teilt Netznamen IP-Adressen zu. Sie ist mit der Datei *hosts* zu vergleichen.

O

P

Paketfilterung:
Prozess, welcher Pakete gemäss gegebenen Regeln passieren lässt oder sperrt. Filterung wird z.B. in lokalen Netzen von Bridges ausgeführt, um Pakete nicht mehr ins Ursprungssegment zu schicken, die als Ziel ein anderes Netzsegment haben als deren Ursprungssegment.

/etc/passwd
Die Datei *passwd* ist die Benutzerdatenbank des Systems. Hier werden die Namen, die Benutzernummern und das *home*-Verzeichnis der Anwender gespeichert. Zudem sind in der "normalen" *passwd*-Datei auch die verschlüsselten Passwörter enthalten.

ping
Der Name *Ping* stammt von einem Sonarsystem, bei welchem ein Ping als Tonimpuls ausgesendet wird. *ping* arbeitet mit dem gleichen Prinzip, verwendet anstelle des Tonsignals jedoch das ICMP-Element *ECHO_REQUEST*. Die angesprochene (oder besser "angepingte") Maschine anwortet auf jedes empfangene Paket mit einem ICMP-*ECHO_REPLY*. Die anfragende Maschine erhält dann die Meldung host is alive. Sollte die Maschine nicht erreichbar sein, wird nach einem *Timeout no answer from host* eine Fehlermeldung ausgegeben. Die Standardeinstellung des Timeouts ist 20 Sekunden.

Port
Ein Port ist ein Kommunikationsendpunkt eines Systemes. Wenn ein System mit einem anderen eine Kommunikationsverbindung aufbauen will, so muss es die Port-Nummer des Kommunikationspartners kennen. D.h. der passive Empfänger muss auf dem bestimmten Port auf die Anforderung zum Verbindungsaufbau warten. Es ist dabei möglich, dass gleichzeitig mehrere Anwendungen den gleichen Dienst (z.B. *Telnet*) benützen. Dazu werden die Verbindungen mit je einem Tupel "IP-Adresse und Port-Nummer" vom Sender und Empfänger zusammen als gemeinsamer Kommunikationsendpunkt, auch Socket genannt, unterschieden. Den gebräuchlichsten Diensten sind ihre Port-Nummern "fest" zugewiesen.

Proxy
Proxy -> Stellvertreter: System oder Prozess, welcher für Maschinen ohne Zugang eine Zugangsmöglichkeit bietet.

Proxy-Dienst
Einzelner Teil eines Proxy-Systems, welches für einen einzelnen (Internet-)Dienst benötigt wird (Bsp.: *FTP*-, *Telnet*-, *HTTP*-Proxy).

Proxy-Server
Ein Programm, welches stellvertretend für interne Clients mit externen Servern kommuniziert. Es stellt eine Art Verbindungspunkt für diese Kommunikation dar, denn nur so ist ein Server von einem Client erreichbar.

Q

R

Router, äusserer
Der äussere Router (manchmal auch Access-Router genannt) schützt die DMZ und das interne Netz vor dem Internet. Meistens wird dieser Router vom Internet-Provider angeboten. Falls hohe Sicherheit verlangt wird, ist der äussere Router ein firmeninternes Gerät. Die Hauptaufgabe ist dann das Blockieren von Paketen mit gefälschten Ursprungsadressen. Diese Pakete behaupten, vom internen Netz zu kommen, werden aber auf dem Internet-"Port" vom Router empfangen.-> Diskrepanz.

Router-based Firewall
A firewall where the security is implemented using screening routers as the primary means of protecting the network.

Router, Innerer
Der innere Router (manchmal auch Choke-Router genannt) schützt das interne Netz vor der DMZ (Grenznetz) und vor dem Internet. Der innere Router liegt somit zwischen dem internen Netz und der DMZ.

S

Screened Subnet
A firewall architecture in which a "sand box" or "demilitarized zone" network is set up between the protected network and

the Internet, with traffic between the protected network and the Internet blocked. Conceptually, this is similar to a dual-homed gateway, except that an entire network, rather than a single host is reachable from the outside.

Screening Router
A router that is used to implement part of the security of a firewall by configuring it to selectively permit or deny traffic at a network level.

/etc/services
Die Datei *services* enthält eine Liste der Dienste, die auf dem entsprechenden Rechner bekannt sind.

Socket
siehe port.

Spoofing
Siehe unter Address Spoofing.
Source Routing:
Beim Source Routing legen die Endsysteme den für ein Paket einzuschlagenden Weg (Route) fest. Dabei wird vom Quellsystem zuerst ein Suchrahmen (discovery frame) versandt, der nach dem Standort des Zielsystems fragt. Der Suchrahmen wird von allen Brücken und Routern kopiert und weitergeleitet. Auf dem Rückweg vom Zielsystem zum Quellsystem fügt jede Brücke und jeder Router seine Adresse in das Antwortpaket ein, sodass dieses bei der Ankunft beim Quellsystem den gesamten zurückgelegten Weg beinhaltet. Jetzt kann das Quellsystem aus den Antwortpaketen dasjenige auswählen, das den kürzesten Weg beschreibt. Der Algorithmus findet so auf alle Fälle den besten Weg, doch durch das Aussenden des discovery-Rahmens erfährt das Kommunikationsnetz eine Rahmenexplosion.

/etc/syslog.conf
syslog.conf ist die Konfigurationsdatei zum entsprechenden Dämon *syslogd*. *syslogd* wird meist beim Booten gestartet und zeichnet alle Systemaktivitäten auf. Darunter fallen z.B. Debugging-, Info-, Warning-, Error- und weitere Meldungen. *syslog.conf* wird dazu gebraucht, festzulegen, wo *syslogd* seine Loginformationen ablegen soll.

T

traceroute
traceroute steht für "verfolge Route" und liefert alle Teilstrecken zwischen Quellsystem und Zielsystem, die ein Paket auf seinem Weg durchwandert. Dabei verwendet es das *time-to-live*-Feld im IP-Paket, um eine allfällige *ICMPTIME_EXCEEDED*-Meldung bei entsprechenden Gateways auf dem Weg zum Ziel zu ermöglichen. *traceroute* sendet so lange Pakete aus, bis entweder die maximale Anzahl an Pakten erreicht ist oder der entfernte Rechner mit der Meldung "*ICMP PORT UNREACHABLE*" antwortet. Somit versucht es, den Weg ausfindig zu machen, den ein IP-Paket voraussichtlich einschlagen wird, um zum entsprechenden Host zu gelangen.

U

V

vi
ein bekannter und beliebter Texteditor in Unix-Systemen.

W

X

Y

Z

8.2 Literaturverzeichnis

[RFC2196]

Site Security Handbook, September 1997
Erhältlich hier in ASCII oder PDF oder in jedem RFC Archiv

[USHdraft]

Users' Security Handbook, draft-ietf-ssh-users-10.txt, October 1998
Erhältlich hier in ASCII oder PDF

[Hosen96]

Hosenfeld, Friedhelm: "Next Generation, Internet-Protokoll Version 6", in Computertechnik, 11(1996), 380-390.

[Ches96]

Cheswick, William R. / Bellovin, Steven M.: "Firewalls und Sicherheit im Internet", ISBN 3-89319-875-x, Addison-Wesley, 1996.

[iX9/96]

Klemm, Andreas / Köhntopp, Marit / Schmitz, Ulrich / Simons, Peter / Wollert, Hagen: "PGP-Anwendungen unter Unix und Windows: Sicherheitsfenster", iX - MULTIUSER MULTITASKING MAGAZIN, September 1996.

[Kyas96]

Kyas, Othmar: "Sicherheit im Internet: Risikoanalyse - Strategien - Firewalls", ISBN 3-89238-149-6, DATACOM-Buchverlag, 1996.

[Meuser96a]

Meuser, Peter: "PC-LANs sicher mit dem Internet verbinden, Firewall-Komponenten auf Intel-Basis", in LANLine, 6(1996), 176-185.

[Meuser96b]

Meuser, Peter: "Checkpoint Firewall-1 mit neuen Features, Schnell und sicher", in LANLine, 6(1996), 186-189.

[Pohl96]

Pohlmann, Norbert: "Abgeschottet, Verschlüsselung in Corporate Networks", in Gateway, 7(1996), 26-34.

[Rütsche96]

Rütsche, Erich, Dr.: "Keine Angst vor Internet-Hackern dank Firewall", in Kommunikation, 1-2(1996), 19-20.

[Solst96]

Sun Microsystems: "Solstice FireWall-1, Administrator's Guide for Solaris, Release 2.1", Revision A, August 1996.

[Uebel96]

Uebelacker, Hubert, Dr. / Kurz, Michaela: "Globale Lösungen statt Einzelbausteine, Sicherheitsarchitektur im Unternehmen", in LANLine, 6(1996), 166-174.

[Badach95]

Badach, Anatol / Hoffmann, Erwin / Knauer, Olaf: "High Speed Internetworking: Grundlagen und Konzepte für den Einsatz von FDDI und ATM", ISBN 3-89319-713-3, Addison-Wesley, 1995.

[Chap95]

Chapman, D.B. / Zwicky, E.J.: "Building Internet Firewalls", O'Reilly & Associates, Inc., 1995.

[SiKa95]

Siyan, Karajit / Hare, Chris: "Internet Firewalls & Netzwerksicherheit", Verlag SAMS, 1995.

[Wilde95]

Wilde, Michael: "Schutzmassnahme, Firewalls im Internet", in Gateway, 5(1995), 20-24.

[Farmer93]

Farmer, Dan: "Improving the Security of Your Site by Breaking Into it", ?.

[Tanen92]

Tanenbaum, Andrew S.: "Computer-Netzwerke", ISBN 3-925328-79-3, Wolfram's Verlag, 1992.

[NWSEC95]

Kaufman, Perlman, Spencier: "Network Security", ISBN 0-13-061466-1, Prentice-Hall Verlag, 1995.

8.3 Links

8.3.1 Organisationen

- NCSA National Computer Security Association [http://www.ncsa.com/]
- CERT/CC Computer Emergency Response Team / Coordination Center [http://www.cert.org/]
- COAST Purdue University [http://www.cs.purdue.edu/coast]
- CIAC Computer Incident Advisory Capability [http://ciac.llnl.gov]
- IPSEC Internet Protocol Security (für IPng) [http://www.ietf.org/html.charters/ipsec-charter.html]

8.3.2 Andere

- Yahoo! Computer and Security [http://www.yahoo.com]
- CCI Competence Center Informatik, Internet Firewalls [http://www.cci.de/cci/its/fw-inf03.htm]
- Computer Underground Society [http://underground.org/]
- Packet Filtering in Firewalls [http://www.willamette.edu/~dlabar/firewall.html]
- PHRACK Magazine [http://www.fc.net/phrack.html]
- ShadowScan [http://www.rsh.keiv.ua]
- NMAP [http://www.nmap.org]
- ISS [http://www.iss.net]

8.4 Tabellenverzeichnis

8.5 Abbildungsverzeichnis