

# Vorschlag Diplomarbeit

Maik Kündig, Michael Güntensperger

4. Februar 2003

## 1 Persönliche Angaben

<b>Teammitglied:</b>	1	2
<b>Klasse:</b>	T-00	T-00
<b>Name:</b>	Kündig	Güntensperger
<b>Vorname:</b>	Maik	Michael
<b>Adresse:</b>	Egglerstrasse 15 8117 Fällanden	Triemlistrasse 29 8047 Zürich
<b>Tel. Privat:</b>	01 / 825 22 58	01 / 400 58 00
<b>Natel Privat:</b>	079 / 609 75 39	079 / 244 58 91
<b>e-Mail Privat:</b>	<a href="mailto:maik@maik.li">maik@maik.li</a> X	<a href="mailto:michael.g@bluewin.ch">michael.g@bluewin.ch</a>
<b>Arbeitgeber:</b>	definitive systems ltd. 8152 Glattbrugg	UBS AG Zürich
<b>Tel. Geschäft:</b>	01 / 809 67 36	01 / 234 49 96
<b>Natel Geschäft:</b>	keines	079 / 244 58 91
<b>e-Mail Geschäft:</b>	<a href="mailto:mkuendig@definitive.ch">mkuendig@definitive.ch</a>	<a href="mailto:michael.guentensperger@ubs.com">michael.guentensperger@ubs.com</a> X

## 2 Titel der Arbeit

FireWallCD mit OpenBSD

## 3 Konkrete Aufgabenstellung

### 3.1 Ausgangslage

Der PacketFilter von OpenBSD genießt ein hohes ansehen. Leider ist noch keine Version verfügbar die ab CD booten kann. Dies erhöht die Sicherheit der Firewall insofern, da nicht auf das Dateisystem geschrieben werden kann. Desweiteren ist eine Firewall ab CD schneller *installiert* und konfiguriert.

Da der PacketFilter von OpenBSD, vor kurzer Zeit komplett neu implementiert wurde, sind ausführliche Dokumentationen dazu, nur in den *man Pages*, im Quellcode sowie in den Archiven von Maillisten erhältlich. Ein Ziel der Arbeit, soll es auch sein: eine aktuelle deutsche Dokumentation des PacketFilters zu erstellen.

### 3.2 Anforderungen

Anhand der Dokumentation und mit Hilfe der von uns geschriebenen Scripten, kann ein Benutzer mit Unix-Kenntnissen, sich einfach und weitgehend automatisiert, eine aktuelle CD erstellen. Und mit der erstellten CD eine Firewall aufsetzen. Daraus ergeben sich die beiden folgenden Teilbereiche:

1. Scripte um ein Isoimage der CD aus den CVS Quellen von OpenBSD zu erstellen.
2. Anleitung zum erstellen eines Isoimages, sowie eine ausführliche Dokumentation des PacketFilters.

**Erstellen der CD** Die zum erstellen der CD benötigten Scripte müssen folgende Schritte ausführen:

- aktuellen Quellcode über CVS beziehen
- Kernel erstellen

- komplettes Betriebssystem neu übersetzen
- 2.8 MByte Bootimage für die CD erstellen
- Dateisystem für die CD erstellen
- rc Dateien für das booten von CD anpassen
- /var und /tmp in einer Ramdisk mounten
- Dokumentation aus den tex Quellen übersetzen
- Isoimage der CD erstellen
- Image von /etc, für eine 1.44 MByte Diskette erstellen

Bei genügend Zeit, sollen noch konfigurations Scripte erstellt werden, die es ermöglichen die wichtigsten Einstellungen der Firewall interaktiv vorzunehmen.

**Dokumentation** Die Dokumentation beinhaltet neben dem Pflichtenheft noch eine Anleitung zum erstellen der CD, sowie eine ausführliche Beschreibung der Konfigurations-Möglichkeiten des PacketFilters. Dazu muss die Dokumentation folgende Punkte enthalten:

- Dokumentation zu den Scripten zum erstellen der CD und Anwendung anhand von Beispielen aufzeigen
- Anleitung zum ersten Starten und erstellen der Konfiguration
- Beispiel Konfigurationen
  - einfaches NAT
  - FireWall mit internem Netz und DMZ
  - eine komplexe Konfiguration
- Dokumentation zum PacketFilter
  - FilterRegeln
    - \* block/pass
    - \* in/out
    - \* tcp, udp, icmp
    - \* quick
    - \* routing Optionen
    - \* Verbindungs-Status
    - \* ISN (initial sequence number) modulation
    - \* antispoofing
  - NAT/BINAT
  - weiterleiten von Ports
  - Bandbreiten für Dienste und User regulieren
  - Macros
  - Packet Normalisierung
  - Bridge als FireWall
  - Log Möglichkeiten
  - Syntax
  - Optionen
  - Auswerten der Log-Dateien, senden der Log-Dateien an einen zweiten Rechner
  - Das empfangen von *SPAM-Mails* so lange wie möglich verzögern

### 3.3 Rahmenbedingungen

Der gesamte Quellcode von OpenBSD ist frei unter der BSD Lizenz verfügbar. Und kann somit frei für alles verwendet werden. Die Arbeit soll auch wieder unter die BSD Lizenz fallen, so dass sie eine Grundlage für weitere Arbeiten in dieser Richtung bilden kann.

### 3.4 Motivation für die Arbeit

**Maik Kündig** Ich selber betreue Firewalls unter OpenBSD in meinem Heimnetz sowie im Geschäft. Dabei hätte ich schön öfters ein CD-Version gebrauchen können um schnell eine Firewall auf einem Rechner installieren zu können, ohne eine schon existierende Installation auf dem Rechner zu löschen.

Ich selber profitiere viel von OpenBSD und seinem PacketFilter, ich setze diese privat und auch beruflich ein. Ich denke, dass ich mit diesem Projekt und der Dokumentation etwas zurückgeben kann. Und um mein Wissen über: Unix Programmierung, erstellen von bootbaren CD's, Packetfiltern, Unix und TCP/IP zu erweitern.

**Michael Güntensperger** Die Wichtigkeit der Sicherheit in der IT wird immer von grösserer Bedeutung. So werden Firmen und Private auch in Zukunft mit dem Thema IT-Security konfrontiert. Das Resultat der Arbeit dient zur schnellen Installation einer Firewall auf einem beliebigen Rechner, der Sicherheit im Privat- wie auch Geschäftsbereich verschafft.

Meine Motivation für diese Aufgabe liegt darin, etwas sinnvolles zu erarbeiten, dass sich auf die schulischen Fächer bezieht. Es wird ein umfangreicher Unterrichtsstoff integriert und theoretisch erlerntes umgesetzt. Mit dieser Arbeit wird ein viel Verwendbares Instrument geschaffen, dass von vielen Leuten benutzt und geschätzt werden soll. Ich freu mich jetzt schon auf das fertig gestellte Produkt aus dieser Arbeit. Diese Arbeit hilft zudem, für einen möglichen internen Wechsel in die IT-Security.

## 4 Aufwandschätzung

Arbeit:	Aufwand [h]:	Starttermin:	Endtermin:
Entwicklungsumgebung einrichten:	5	1.3.2003	1.3.2003
Vorabklärungen:	50	2.3.2003	15.4.2003
Dokumentationen sammeln und auswerten:	30	1.4.2003	1.5.2003
Scripte zum erstellen der CD:	15	1.4.2003	1.8.2003
Erstellen eines CD Prototypen:	40	1.4.2003	1.6.2003
Pflichtenheft:	15	1.4.2003	1.7.2003
Beispiel Konfigurationen:	20	1.5.2003	1.7.2003
Tests definieren:	15	1.5.2003	1.7.2003
Testen:	30	1.5.2003	Abgabe
Dokumentation:	100	1.5.2003	Abgabe
Konfiguration Scripte:	20	1.7.2003	Abgabe
Dokumentation Final:	5	15.7.2003	Abgabe
<b>Total:</b>	<b>345</b>		

## 5 Eingesetzte Mittel

- Quellcode von OpenBSD
- Shell- und Perl- Scripte
- Makefiles
- *mkhybrid* zum erstellen des Isoimages
- CVS
- L<sup>A</sup>T<sub>E</sub>X

## 6 Vorschlag Betreuung

Als Betreuer, haben wir einen Lehrer der TSU gefunden: **Sherin Ibrahim**, hat uns bereits zugesagt, da er selber auch Interesse an den Resultaten der Diplomarbeit hat.

Wir würden uns freuen die Arbeit mit Sherin Ibrahim als Betreuer durchzuführen. Würden aber auch einen anderen Betreuer akzeptieren.

## 7 Ersatzvorschlag

Erstellen eines *Honeypots*, mit Hilfe frei erhältlicher Software. Es sollen alle Schritte zum erstellen eines Honeypots dokumentiert werden, sowie einige Honeypots über mehre Wochen betrieben werden. Alle Aktivitäten auf dem Rechner sollen in einer Datenbank gesammelt werden. Mit den gesammelten Daten soll eine detaillierte Auswertung vorgenommen werden. Mit dem Ziel: Informationen über die häufigsten Angriffs-Arten, Zeiten bis verschiedene Betriebssystem *gehackt* werden usw. zusammenzutragen und graphisch darzustellen.