Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEKTION 4
DIENSTE UND VERBINDUNGEN

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Informationen zur Nutzungslizenz

Die folgenden Lektionen und Arbeitsmaterialien sind öffentlich verfügbar unter den folgenden Bedingungen seitens ISECOM:

Alle Materialien der Hacker Highschool werden für den nicht-kommerziellen Einsatz in Grund-, Haupt-, Realschulen und Gymnasien zur Verfügung gestellt, sowohl für öffentliche und private Bildungseinrichtungen, als auch für Privatunterricht zu Hause. Die Materialien dürfen in keiner Form für den Wiederverkauf reproduziert werden. Der kommerzielle Einsatz der Materialien, welche käuflich erworben werden können, in jeglicher Form von Schulstunde, Unterricht, Training, Meeting, Kongress, Vorlesung, Fortbildung, Sommer- oder Abendschulen ist ohne vorigen Erwerb einer Lizenz explizit untersagt. Um eine Lizenz zu erwerben, besuchen Sie bitte http://www.hackerhighschool.org/license.

Das Hacker Highschool (HHS) Projekt ist ein Unterrichtswerkzeug. Der Einfluss auf die Lernenden liegt beim Lehrer, nicht jedoch beim Werkzeug. Aus diesem Grund erkärt sich ISECOM nicht für Schäden verantwortlich, welche aus einem eventuellen Missbrauch der hier publizierten Informationen hervorgehen.

Das HHS Projekt ist die Arbeit einer offenen Gemeinschaft. Wir hoffen, dass die Lesenden Nutzen in unsem Projekt finden werden und bitten um Unterstützung unserer Arbeit, sei es durch den Erwerb einer Lizenz, durch eine Spende, Sponsoring oder in anderer Form.

Für das gesamte Material © ISECOM 2004

Inhalt

Mitwirkende

Chuck Truett, ISECOM

Guiomar Corral, La Salle URL Barcelona

Jaume Abella, La Salle URL Barcelona - ISECOM

Kim Truett, ISECOM

Marta Barceló, ISECOM

Pete Herzog, ISECOM

ÜBERSETZUNG

Georg Berky

Karl Pausch

4.0 Einführung

Das Ziel dieser Lektion ist es, dass Du einige grundlegende Dienste, die in Netzwerken zur Weitergabe von Informations verwendet werden, verstehst. Ebenfalls werden wir einige Methoden besprechen, wie man PCs und lokale Netze miteinander verbindet, und wie so letztendlich das Internet entsteht.

4.1 Dienste (Services)

Du hast einen Computer und weißt, dass sich darauf interessante Informationen befinden, aber so viel wird das nicht sein. Andererseits haben andere Leute, Millionen anderer Leute, ebenfalls Computer, auf denen sich wohl auch interessante Informationen befinden.

Man kann annehmen, dass diese anderen Leute auf ihren Computern wohl Informationen haben, die für Dich von Interesse sein könnten. Das einzige Problem besteht darin, wie man auf diese Informationen, die auf deren Computern sein könnten, zugreifen kann.

Die Computer selbst können leicht miteinander kommunizieren, über Ports und die verschiedenen Protokolle, die zu diesem Zweck entworfen worden sind, aber das bringt uns auch nicht wirklich weiter. Die binären Daten, die zwischen den Computern hin- und herfließen verstehen wir auch nicht einfach so. Wir benötigen eine bestimmte Interpretation dieser binären Daten, die wir von anderen Rechnern empfangen, damit wir sie verwenden können.

Die Programme, welche die Computer verwenden, um die binären Daten, die sie austauschen in eine Form zu übersetzen, die wir verstehen können, nennen wir Dienste („services"). Diese Services erlauben es uns, Webseiten anzusehen, E-Mails zu schreiben, zu chatten und uns auf viele verschiedene Arten mit anderen Computern auszutauschen.

Dein Computer, der lokale Computer („localhost"), verwendet Programme um die Informationen die er empfängt zu interpretieren. Diese Programme nennen wir „Clients". Die anderen Computer verwenden Programme um uns diese Informationen anzubieten. Diese Programme nennen wir „Server".

4.1.1. Das Web und HTTP

Beim Wort „Internet" kommt den meisten Leuten wohl zuerst das „World Wide Web" („WWW") in den Sinn. Das World Wide Web, oder auch einfach nur „das Web" genannt, ist nicht das Internet. Das Web ist eine Methode für den Informationsaustausch unter Computern, die das Internet verwenden. Das Web ist also ein Teil, eine Teilmenge, des Internet, jedoch macht es nicht das ganze Internet aus. Das Web ist der Teil des Internet, der http, das „hypertext transfer protocol" verwendet, um Informationen zwischen lokalen und entfernten („remote") Computern in Form von Webseiten („web pages") auszutauschen. Die Web Clients werden meistens als „Web Browser" oder einfach nur als „Browser" bezeichnet. Die Server nennt man „Web Server".

Was du auf dem lokalen Computer siehst, ist der Web Browser. Er empfängt über das http Protokoll Daten von einem entfernten (remote) Computer, interpretiert sie, und stellt sie in der

Form von Webseiten dar.

Das „hypertext" in „hypertext transfer protocol" beschreibt eine spezielle, nichtlineare Art, Informationen darzustellen. Normaler Text wird meistens linear gelesen: Wort 3 nach Wort 2, Satz 6 nach Satz 5 und Absatz 8 nach Absatz 7. Die Idee, die zur Erfindung von Hypertext führte, war, dass man Informationen in nichtlinearer Weise darstellen und man nicht mehr an die exakte Reihenfolge der Sätze, Absätze und Kapitel gebunden sein wollte.

Mit Hypertext kann man einzelne Wörter und Ideen verbinden – nicht nur mit den sie direkt umgebenden Wörtern zu Sätzen, sondern auch mit anderen Wörtern, Ideen und Bildern über sogenannte Hyperlinks, die zum Beispiel auf eine Erklärung des verlinkten Begriffs verweisen. Klickst Du den verlinkten Begriff an wirst Du auf eine andere Webseite mit der Erklärung weiterverbunden. Hypertext ist nicht auf das Web beschränkt. Mit den meisten guten Textverarbeitungsprogramme kannst Du Dateien im Web- oder html-(„hypertext markup language")Format auf Deinem Computer abspeichern. Diese Dateien kannst Du dann wieder in Deinem Web Browser öffnen und sie verhalten sich so, als ob Du sie gerade von einem Webserver heruntergeladen hättest. Sie sind jedoch nur auf Deiner Festplatte gespeichert.

An dieser Stelle sollte Dir der Unterschied zwischen http und html klar geworden sein: http ist das Protokoll, mit dem Du Daten übertragen kannst. Diese Daten sind im Fall des Word Wide Web meistens im html Format. Dein Browser empfängt die Daten mit Hilfe des http Protokolls. Handelt es sich um HTML Daten, so kann er sie als Webseite interpretieren und darstellen, wie Du es gewohnt bist. Bei http handelt es sich also um eine Methode Daten zu übertragen, bei html um eine Methode, Informationen als Hypertext Seiten darzustellen.

Auf deinem lokalen Rechner verwendest Du einen Browser um Webseiten anzuzeigen. Im Gegensatz zu dem, was Dir wohl Glauben gemacht worden ist, gibt es eine Menge Browser für sowohl Windows als auch Linux. Die wohl bekanntesten sind der Internet Explorer, Mozilla Firefox, Mozilla, Opera und der Netscape Navigator.

Du kannst auch Deine eigenen Webseiten erstellen. Am leichtesten geht das wahrscheinlich mit Deinem Textverarbeitungsprogramm, also OpenOffice, Microsoft Word oder WordPerfect. Mit diesen Programmen wirst Du ziemlich schnell einfache Webseiten erstellen können.

Das Problem dabei: diese einfachen Seiten sind nicht hip – hip im Sinne von Frames, Scripts und Animationen, wie Du sie von den ganzen tollen Webseiten kennst. Hip bedeutet auch, dass Du einen Haufen Geld für ein tolles Webdesign-Programm ausgeben musst. Mit solchen Programmen kannst Du viele interessante Effekte auf deinen Webseiten platzieren, aber sie sind auch um einiges komplexer und schwerer zu bedienen als die Textverarbeitungsprogramme, die Du schon kennst.

Sobald Du Deine Webseite fertig entworfen hast, brauchst Du einen Server, auf dem Du sie ablegen kannst, damit andere Leute sie ansehen können. Das nennt man „Web Hosting".

Auf dem Computer, der Deine Seiten anderen zur Verfügung stellt (sie „hostet"), muss ein Webserver Programm laufen. Natürlich ist es möglich, ein solches Programm auf Deinem eigenen Computer laufen zu lassen, aber das hat einige Nachteile. Der größte Nachteil ist wohl die Beständigkeit (Persistenz) der Informationen. Diese sind nur abrufbar, wenn der Computer mit dem Webserver angeschaltet ist, einwandfrei funktioniert und Anfragen (Verbindungen) annehmen kann. Wenn Du also den Computer in Deinem Zimmer als Webserver verwenden willst, musst Du ihn die ganze Zeit angeschaltet lassen und musst überprüfen, ob das Serverprogramm richtig funktioniert, was Hardwareprobleme, Virenbefall, Würmer und andere Attacken sowie die unvermeidlichen Fehler und Bugs im Programm mit

einschließt. Außerdem musst Du natürlich ständig mit dem Internet verbunden sein. Aus diesen Gründen lassen die meisten Leute diese ganzen Arbeiten von einem anderen machen.

Eine Webhostingfirma speichert Deine Dateien auf ihrem Computer. Ideale Firmen haben viele redundante Server, die im Falle eines Ausfalls des einen Servers auf einen anderen Server umsteigen können, und werden zudem regelmäßig durch Backups (Datensicherungen) gesichert. Sie haben ein Serviceteam, das den Server trotz Hardwareproblemen und Angriffen aus dem Netz am laufen hält. Ebenso haben sie eine große Zahl von Verbindungen zum Internet, so dass das Erstellen Deiner Webseite sowie das Hochladen auf den Server der Hostingfirma alles ist, was Du tun musst. Danach kannst du Deinen eigenen Rechner abschalten und ins Bett gehen, während Deine Webseite der ganzen Welt zur Verfügung steht.

Es gibt auch Organisationen und Firmen, die kostenloses Webhosting anbieten. Die meisten dieser Firmen finanzieren ihren Service durch Werbung. Jeder, der seine Seite bei dieser Firma hosten lässt, muss zuerst die Werbung einer anderen Firma anzeigen. Die Leute, die Deine Webseite ansehen, müssen natürlich nichts kaufen und Du musst auch nichts für das Hosting bezahlen.

4.1.2. E-Mail: POP3 und SMTP

Der zweite wohl am meisten bekannte Aspekt des Internet ist (wohl) E-Mail. Auf Deinem Computer verwendest Du einen Mail Client, der sich mit einem Mail Server verbindet. Wenn Du dir einen Mail Zugang („account“) erstellst, erhältst Du eine eindeutige Mail Adresse in der Form benutzer@domain und ein Passwort, das Du benötigst, um Deine Mails abzuholen.

Das SMTP Protokoll („simple mail transfer protocoll“) wird dazu verwendet, um Mails abzuschicken. Dafür braucht man meistens kein Passwort. Als das Protokoll erfunden wurde, mag das noch kein Problem dargestellt haben, weil das Internet eine relativ kleine Gemeinschaft von gleich denkenden Leuten war. Heute hat sich diese Tatsache aber als ziemlich fatal herausgestellt, weil sie die unerlaubte Verwendung von Mailservern und viele andere Tricks erlaubt, etwa Mail Spoofing (das Versenden von Mail unter einer falschen Absenderadresse). Glücklicherweise minimieren schon viele Mailserver dieses Risiko, indem sie einen zusätzlichen Authentifizierungsschritt vor dem Versenden der Mail einbauen, bei dem sich der Sender vor dem Verschicken der Nachricht zuerst identifizieren muss.

Wichtig ist, dass Dir klar wird, dass E-Mail kein geeignetes Mittel zum versenden von vertraulichen Informationen darstellt. Die meisten POP3 Clients und Server fordern, dass die Zugangsdaten unverschlüsselt (!) zum Mailserver geschickt werden. Das bedeutet natürlich nicht, dass jeder, der eine Mail von dir bekommt, auch Dein Passwort lesen kann, aber jemand mit genug Wissen und den richtigen Werkzeugen kann bei unverschlüsselter Kommunikation relativ leicht Deine Zugangsdaten „sniffen“ (mitlesen, „schnüffeln“). In Lektion 9 - „E-Mail Sicherheit“ lernen wir, wie wir E-Mail sicherer machen können.

4.1.3. IRC

IRC oder „internet relay chat“ ist der Ort, an dem die unregulierte und liberale Natur des Internet wohl am stärksten zum Ausdruck kommt. Im IRC bekommt jeder, der meint, etwas zu

sagen zu haben, die Gelegenheit das auch zu tun.

Vielleicht bist du schon mit den Chatrooms einiger Online Dienste vertraut. IRC ist in etwa das Gleiche wie ein Chatroom, aber ohne Regeln, ohne Standards und meistens gibt es auch keine Anstandsdamen und Moralapostel. In einem IRC Channel kannst du genau das finden, was du schon immer gesucht hast - oder etwas von dessen Existenz du lieber nie gewusst hättest.

Alle Regeln, die für Chatrooms gelten, sind auch auf IRC Channels anwendbar. Sage keinem Deinen wahren Namen, deine Telefonnummer, deine Adresse oder Kreditkartennummer, aber habe Spaß.

Übungen:

Finde drei IRC Channels, die sich mit Computersicherheit beschäftigen. Wie kannst du an der Diskussion dort teilnehmen? Wie kannst du eine private Unterhaltung mit einem anderen Teilnehmer führen?

Kann man über IRC Dateien übertragen? Wenn ja, wie? Würdest du das immer so machen wollen? Warum? Warum nicht?

4.1.4. FTP

FTP steht für „file transfer protocol“. Wie der Name schon andeutet, kann man mittels FTP, Dateien von einem entfernten (remote) Computer zu einem lokalen übertragen und andersherum. Es ist zwar möglich, private Dateien mit dem FTP Protokoll zu übertragen, meistens jedoch wird es in öffentlichen, sogenannten anonymen FTP Servern dazu verwendet, Zugriff auf eine Menge von Dateien zu ermöglichen, was sich „anonymous ftp“ nennt.

Früher war anonymous ftp die gebräuchliche Methode, mit der die meisten Computerbenutzer Dateien über das Internet austauschten. Viele anonymous ftp Server werden zwar dazu verwendet, um illegal Dateien auszutauschen, welche dann oftmals von Viren infiziert sind, aber es gibt auch viele solcher FTP Server, die legal Dateien und Programme zum Herunterladen („download“) anbieten. Server, die anonymous ftp anbieten, lassen sich auf verschiedenen Wegen finden, etwa mit Suchmaschinen.

Die meisten anonymous FTP Server erlauben es heute, dass man mit einem Webbrowser auf die Dateien, die sie anbieten, zugreifen kann.

Übungen:

Sowohl Windows als auch Linux (kommen) besitzen einen einfachen FTP Client für die Kommandozeile. Öffne ein DOS-Fenster oder ein Terminal und gib folgendes ein:

ftp

Am FTP Prompt der folgendermaßen aussehen kann „ftp>“ kannst du help eingeben, um dir eine Liste der verfügbaren Befehle anzeigen zu lassen.

ftp> help

Commands may be abbreviated. Commands are:

!	delete	literal	prompt	send
?	debug	ls	put	status
append	dir	mdelete	pwd	trace
ascii	disconnect	mdir	quit	type
bell	get	mget	quote	user
binary	glob	mkdir	recv	verbose
bye	hash	mls	remotehelp	
cd	help	mput	rename	

close lcd open rmdir

Einige wichtige Befehle sind:

```
ftp> open DomainName
```
Verbindet dich mit dem FTP Server DomainName

```
ftp> dir
ftp> ls
```
Diese zeigen dir den Inhalt des Verzeichnises auf dem entfernten (remote) Computer an.

```
ftp> cd NeuesVerzeichnis
```
Wechelt in das Verzeichins NeuesVerzeichnis

```
ftp> get Dateiname
```
Lädt die Datei Dateiname herunter

```
ftp> mget Datei1 Datei2 Datei3
```
Lädt die Dateien Datei1, Datei2 und Datei3 herunter

```
ftp> close
```
Beendet die aktuelle Verbindung zum FTP Server.

```
ftp> quit
```
Beendet den FTP Client.

Um uns mit einem anonymous FTP Server zu verbinden, brauchen wir unseren FTP Client:

```
ftp
```

Anschließend verwenden wir open, um uns mit dem gewünschten Server zu verbinden:

```
ftp> open Servername
```

Damit verbinden wir uns mit Servername. Sobald die Verbindung besteht, wird sich der entfernte (remote) FTP Server bei deinem Client etwa so melden:

```
Connected to anon.server.
220 ProFTPD Server (Welcome . . . )
User (anon.server:(none)):
```

Bei den meisten FTP Servern brauchen wir den Benutzernamen anonymous. Hast du diesen Benutzernamen eingegeben, wir dir der Server bestätigen, dass er anonymous FTP akzeptiert, etwa folgendermaßen:

```
331 Anonymous login ok, send your complete email address as your password.
Password:
```

In den meisten Fällen wir der FTP Server die angegebene E-Mail Adresse nicht überprüfen und dich auch nicht davon abhalten, seine Dienste zu nutzen, selbst wenn Du eine E-Mail Adresse verwendet hast, die nicht existiert. Allerdings gilt solches Verhalten als Verletzung der Etiquette und damit als ziemlich unfreundlich. Nachdem du die E-Mail Adresse als Passwort eingegeben hast, wird dich der Server etwa so begrüßen:

```
230-
Welcome to ftp.anon.server, the public ftp server of anon.server. We
hope you find what you're looking for.
If you have any problems or questions, please send email to
ftpadmin@anon.server
Thanks!
230 Anonymous access granted, restrictions apply.
```

Ab jetzt kannst du die Befehle dir, ls, cd und get verwenden, um Dateien vom entfernten (remote) Computer herunterzuladen.

Versuche anhand dieser Beispiele eine Datei von einem anonymous FTP Server herunterzuladen. Suche mit einer Suchmaschine nach einem Server, der „Alice im Wunderland“ hat, und lade dann die Datei mit deinem FTP Programm für die Kommandozeile – nicht mit deinem Browser – herunter.

4.1.5. Telnet und SSH

Mit Telnet kannst Du Befehle für einen entfernten Computer an Deinem lokalen Computer eingeben. Dieser überträgt die Befehle an den entfernten Computer der sie ausführt. Die Ausgabe des Befehls wird dann wieder an Deinen lokalen Computer übertragen. So kannst Du über Telnet an einem entfernten Computer so arbeiten als wenn Du direkt an der Tastatur dieses Rechners sitzen würdest.

SSH oder „secure shell“ ist ein sicherer Ersatz für Telnet, denn Telnet ist nicht verschlüsselt.

Sowohl Linux als auch Windows haben einen Telnet Client, den du mit folgendem Befehl in einer Shell oder im DOS-Fenster aufrufen kannst:

telnet

Um auf einen Telnet Server zugreifen zu können, brauchst du einen Account bestehend aus einem Benutzernamen und einem Passwort, den der Administrator für dich erstellen muss, weil es für seinen Computer ziemlich gefährlich sein kann, wenn du eine Menge von Befehlen ausführen kannst, die der Sicherheit seines Servers erheblich schaden könnten.

Telnet wurde früher dazu verwendet, dass Administratoren von ihrem Computer aus ihre Server steuern und warten können. Heute wird Telnet in den meisten Fällen durch SSH ersetzt.

Telnet kann auch dazu verwendet werden, eine Menge anderer interessanter Dinge zu machen, wie etwa E-Mails zu senden und zu empfangen. Telnet ist jedoch eine der kompliziertesten Methoden, um diese Aufgabe zu erledigen. Telnet kann zu einer Menge illegaler Dinge missbraucht werden, aber es gibt auch viele berechtigte Einsatzgebiete. Bei einem sehr vollen Postfach und einer langsamen Internetanbindung kann es beispielsweise nützlich sein, dass Du deine Mails mit telnet überprüfst, zum Beispiel Dir nur die ersten Zeilen anzeigen lässt und dann die Mails löscht, die du nicht brauchst, ohne die ganze große Nachricht herunterladen zu müssen.

4.1.6. DNS

Wenn Du einen Freund anrufen willst, brauchst du die richtige Telefonnummer. Wenn du dich mit einem Computer verbinden willst, ist das genauso. Du erinnerst dich sicher an die IP-Adresse, die Computer in einem Netzwerk haben, was wir Dir in einer der vorigen Lektionen erklärt haben.

Da es sich bei IP-Adressen um Zahlen handelt, ist es relativ leicht für einen Computer, damit umzugehen. Für Menschen ist das nicht so leicht. Wir verwenden lieber Domänen (domain) Namen, mit denen wir leichter umgehen können. Wollen wir uns beispielweise mit der Hacker Highschool Homepage verbinden, geben wir 'www.hackerhighschool.org' in die Adressleiste unseres Browsers ein. Um eine Verbindung über das Netzwerk herstellen zu können, braucht der Webbrowser – wie jedes andere Programm auch – aber eine IP-Adresse. Aus diesem Grund muss dein Computer irgendwie den Domänen (domain) Namen in eine IP-Adresse umwandeln können. Gäbe es nur wenige hundert oder tausend Computer im Internet, könnte man alle Zuordungen in einer einfachen Tabelle speichern. Angesichts der Millionen von Domänen (domain) Namen und IP-Adressen im Internet und sich ständig ändernder Daten, reicht eine einfache Tabelle nicht mehr aus.

Aus diesem Grund gibt es DNS („domain name service“), um Domänen (domain) Namen in IP-Adressen zu übersetzen. Wenn du www.domainname.com in deinem Webbrowser eingibst, fragt dieser zuerst beim DNS Server deiner Internetfirma nach der IP-Adresse für diese Domäne (domain). Ist diese in der Datenbank des DNS Servers, liefert er sie an deinen Webbrowser zurück, andernfalls fragt er beim nächsthöheren Server in der Hierarchie nach, um letztendlich entweder die korrekte IP-Adresse oder die Tatsache, dass die Domäne nicht existiert zurückgeliefert wird.

Übungen:

Mehr über DNS:

Öffne ein DOS Fenster oder eine Shell und finde heraus, welche IP-Adresse dein Computer hat. Wie hast du das herausgefunden?

Welche IP-Adresse hat der DNS Server deines Internetanbieters (provider)? Wie hast du das herausgefunden? Welche Befehle hast du verwendet?

Sende eine ping-Anfrage and www.isecom.org. Erhältst du eine positive Anwort? Welche IP-Adresse beantwortet den ping?

Kannst du deinen Computer dazu bringen, einen anderen DNS Server zu verwenden? Wenn

ja, lass ihn einen anderen verwenden und sende erneut eine ping-Anfrage an www.isecom.org. Erhältst du die selbe Antwort wie davor? Warum?

4.1.7. DHCP

DHCP („dynamic host configuration protocol“) ermöglicht die dynamische Zuweisung von IP-Adressen in einem Netzwerk. Einem Netzwerk wird eine Anzahl (Menge) von IP-Adressen zugewiesen, aus der dann jeweils eine vergeben wird, sobald ein Computer dem Netzwerk beitritt. Wenn er das Netz wieder verlässt, wird seine Adresse wieder frei für die Benutzung durch einen anderen Rechner.

Vor allem in sehr großen Netzwerken ist dieser Dienst extrem nützlich, da der Administrator nicht mehr jedem Computer von Hand eine eigene feste (statische) IP-Adresse zuweisen muss. Stattdessen wird ein DHCP Server verwendet. Wenn ein neuer Computer sich mit dem Netzwerk verbindet, ist das erste was er tut, eine IP-Adresse vom DHCP Server anzufordern. Sobald ihm vom DHCP Server eine Adresse zugewiesen worden ist, kann er wie die anderen Teilnehmer des Netzes, auf die zur Verfügung stehenden Dienste zugreifen.

4.2 Verbindungen (Connections)

Die meisten Computer verbinden sich mittels eines Modems mit dem Internet. Ein Modem („modulator-demodulator“) wandelt die digitalen Signale eines Computers in Signale um, die über die weitverbreiteten Telefonleitungen verschickt werden können. Die Geschwindigkeit eines Modems wird in baud oder bits pro Sekunde gemessen. Höhere Baudraten sind natürlich besser, da die Datenübertragung dadurch schneller ist, aber es gibt immer noch einige Szenarien, für welche ein 20 Jahre altes 300 baud Modem ausreicht, etwa eine telnet-Verbindung zu einem MUD („multi user dungeon“) - vorausgesetzt du tippst nicht besonders schnell. Andere Szenarien, etwa Video Streaming holen aber oft das letzte, sogar aus den schnellen DSL- oder Kabelmodems heraus.

4.2.1. Internet Dienstanbieter (ISPs)

Wir können nicht einfach das Internet anrufen, sondern brauchen Zugang zu einem Server, der uns mit dem Internet verbindet. Dieser Server macht die ganze schwere Arbeit für uns, etwa 24 Stunden am Tag angeschaltet und online zu sein. Solche Server werden von einem Internet Dienstanbieter oder ISP („internet service provider“) betrieben.

Ein ISP ist immer mit dem Internet verbunden und auf seinen Servern laufen die Dienste, die du nutzen willst. Solche Dienste könntest du selbst auch anbieten, etwa deinen eigenen Mailserver, aber wie oben beschrieben, ist das ziemlich unpraktisch oder sogar unangenehm, weil Dein Computer immer angeschaltet sein müsste, nur um 24 Stunden am Tag auf eine kleine Verbindung oder Anfrage zu warten. ISPs erledigen diese Arbeit für alle ihre Kunden. Ihre Mail Server haben die ganze Zeit Arbeit, und warten nicht nur auf einzelne Anfragen. Zusätzlich sind ISPs über Hochgeschwindigkeits- (highspeed) Leitungen mit NAPs („network access points“), Zugangspunkten zum Internet, verbunden, welche wiederum durch Ultra-Hochgeschwindigkeits- (highspeed) Leitungen, den sogenannten „backbones“ untereinander verbunden sind. Das ganze nennt sich dann Internet.

4.2.2. Plain old telephone service – Zugang per Telefon

POTS oder „plain old telephone service“ ist immer noch die am weitesten verbreitete Methode, um sich mit dem Internet zu verbinden. Ihr größter Nachteil ist die langsame Geschwindigkeit, aber in vielen Fällen macht die große Verfügbarkeit diesen Nachteil wieder wett. Die meisten landesweiten ISPs haben lokale Einwahlnummern, und fast jeder hat eine Telefonleitung zuhause. Theoretisch könnest du dich mit einem akustischen Modem, einem sogenannten „Akkustikkoppler“, und einer handvoll Wechselgeld in einer Telefonzelle mit dem Internet verbinden. Ob du das auch willst, ist die andere Frage.

POTS ist ziemlich langsam. Die schnellstem Modems behaupten, dass sie 56'600 baud schnell sind. Im Kleingedruckten erklären sie dann, dass das eine Lüge ist. Die Spannungsbegrenzung beschränkt die Downloadgeschwindigkeit auf etwa 53'000 baud. Zudem ist die tatsächlich erreichte Geschwindigkeit meistens um einiges niedriger und lässt sich nicht mit DSL- oder Kabelmodems vergleichen.

Soweit so gut. POTS ist sicher nicht dazu geeignet, Raubkopien von Filmen herunterzuladen. Erstens ist es unmoralisch und illegal. Zweitens würde es deine Telefonleitung bis spät in die Nacht oder sogar bis zum nächsten Abend belegen. Für nette E-Mails an deine Oma reicht es aber auf jeden Fall. Wenn du telnet verwendest, kannst du sogar mit einem alten DOS Computer aus dem Keller MUD spielen.

4.2.3. DSL

DSL („digital subscriber line“) dient dazu, große Mengen an Daten über die schon vorhandenen POTS-Telefonleitungen zu verschicken. Der größte Vorteil gegenüber POTS ist dabei die um einiges höhere Geschwindigkeit. In einigen Ländern (leider tanzt Deutschland 'mal wieder aus der Reihe) hat man mit DSL sogar eine permanente Verbindung ins Internet. Zusätzlich wird durch DSL die Telefonleitung nicht belegt. Der Hauptnachteil von DSL ist, dass es nur in der Nähe von Zugangspunkten verfügbar ist. Wohnt man zu weit weg: Pech gehabt.

Übungen:

Suche mit einer Suchmaschine nach Firmen, die DSL anbieten. Welche anderen Dienste, bieten diese Firmen noch an (Telefon, Fernsehen, ...)?

4.2.4. Kabelmodems

Kabelmodems verwenden nicht die normalen Telefonleitungen zur Verbindung mit dem Internet, sondern gebrauchen fiberoptische „Lichtsignale“ Leitungen um digitale Signale über das Kabel zu übertragen. Wie DSL bieten Kabelmodems (meistens) eine permanente Verbindung ins Internet und sind größtenteils schneller als DSL.

Kabelmodems haben zwei grundlegende Nachteile. Der erste ist, dass man sich die Kabelleitungen mit seinen Nachbarn teilen muss, und damit die Geschwindigkeit abnimmt, sobald einer der Nachbarn die Leitung mitverwendet. Der zweite Nachteil ist, dass Kabelzugänge nur an Orten verfügbar sind, wo die Firmen bereits die dazu nötigen fiberoptischen Kabel verlegt haben.

Übungen:

Suche mit einer Suchmaschine nach Firmen, die einen Kabelzugang anbieten. Welche anderen Dienste bieten diese Firmen noch an?

Weite Informationen:

How E-mail Works: http://computer.howstuffworks.com/email.htm
An IRC FAQ: http://www.irchelp.org/irchelp/new2irc.html
A Basic FTP FAQ (old, but extensive): http://www.faqs.org/faqs/ftp-list/faq/
Another FTP FAQ (also old): http://www.ibiblio.org/pub/Linux/docs/faqs/FTP-FAQ
An Overview of SMTP (with a link to RFC 821, which details the protocol):
http://www.freesoft.org/CIE/Topics/94.htm
And a complementary Overview of POP3 (with a link to RFC 1725):
http://www.freesoft.org/CIE/Topics/95.htm
An Overview of Telnet: http://www.dmine.com/bbscorner/telover.htm
Retrieving Mail with Telnet:
http://wiki.linuxquestions.org/wiki/Retrieving_mail_manually_using_telnet
SSH a more secure alternative to Telnet: http://www.openssh.com/
Basic DNS Information:
http://hotwired.lycos.com/webmonkey/webmonkey/geektalk/97/03/index4a.html
More Detailed DNS Information:
http://www.microsoft.com/technet/itsolutions/network/deploy/confeat/domain.mspx
A collection of DNS commands, tests and lookups: http://www.dnsstuff.com/
A detailed DHCP FAQ: http://www.dhcp-handbook.com/dhcp_faq.html
A long article on DCHP, with information on NAT and routers:
http://hotwired.lycos.com/webmonkey/00/39/index3a.html?tw=backend
An Overview of Cable Modems: http://electronics.howstuffworks.com/cable-modem.htm