Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEKTION 3
PROTOKOLLE UND PORTS

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

"License for Use" Information 2
Informationen zur Nutzungslizenz 2
Mitwirkende 4
3.1 Einführung 5
3.2Grundlegende Konzepte von Netzwerken 6
3.2.1 Bauteile 6
3.2.2 Topologien 6
3.3 TCP/IP Modell 7
3.3.1 Einführung 7
3.3.2 Schichten 7
3.3.2.1 Die Anwendungsschicht (Application): 7
3.3.2.2 Die Transportschicht (Transport): 8
3.3.2.3 Die Internetschicht (Internet): 8
3.3.2.4 Die Netzwerkzugangsschicht (Network Access): 8
3.3.3 Protokolle 8
3.3.3.1 Protokolle der Anwendungsschicht (application layer) 9
3.3.3.2 Protokolle der Transportschicht 10
3.3.3.3 Protokolle der Internetschicht 10
3.3.4 IP Adressen 10
3.3.5 Ports 13
3.3.6 Kapselung 15
3.4 Übungen 16
3.4.1 Übung 1: Netstat 16
3.4.2 Übung 2: Ports und Protokolle 17
3.4.3 Übung 3: Mein erster Server 17
Weitere Informationen 19

Mitwirkende

Gary Axten, ISECOM

La Salle URL Barcelona

Kim Truett, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Pete Herzog, ISECOM

ÜBERSETZUNG

Georg Berky

Karl Pausch

3.1 Einführung

Der Text und die Übungen in dieser Lektion versuchen ein grundsätzliches Verständnis für die derzeitig benutzten Ports und Protokolle wie auch der Bedeutung in den Betriebssystemen Windows und Linux zu geben.

Zusätzlich bekommst Du die Gelegenheit mit einer Anzahl an nützlichen Hilfsmitteln vertraut zu werden, welche Dir das richtige Verständnis der Netzwerkfähigkeiten deines Computers erlauben.

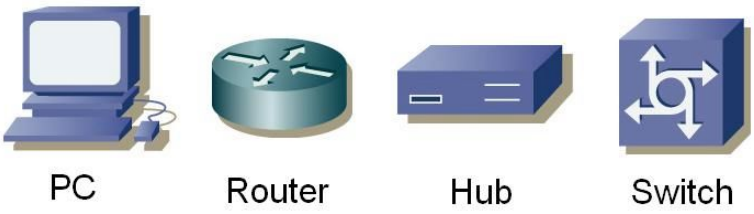
Am Ende dieser Lektion solltest Du grundsätzliches Wissen haben über:

- Konzepte von Netzwerken
- IP Adressen
- Ports und Protokolle

3.2Grundlegende Konzepte von Netzwerken

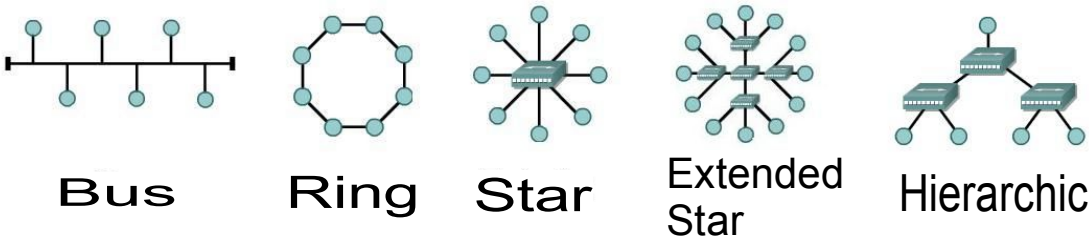
3.2.1 Bauteile

Um die Erklärung der Protokolle und Ports zu verstehen ist es nötig, dass Du mit den Symbolen, welche die häufigsten Geräte in den nachfolgenden Plänen repräsentieren, vertraut wirst. Diese sind:



3.2.2 Topologien

Mit diesen Geräten können Lokale Netzwerke (oder LANs) aufgebaut werden. In einem LAN können Computer Ressourcen gemeinsam nutzen, wie Festplatten, Drucker und Internet Verbindungen und ein Administrator kann kontrollieren wie diese Ressourcen genutzt werden. Wenn ein LAN aufgebaut wird, ist es möglich eine der folgenden Topologien zu wählen.



In einer *Bus* Topologie, sind alle Computer mit einem Übertragungsmedium verbunden, und jeder Computer kann direkt mit jedem anderen kommunizieren. In der *Ring* Konfiguration ist jeder Computer mit dem folgenden verbunden und der letzte wieder mit dem ersten und jeder Computer kann direkt, nur mit den zwei benachbarten Computern kommunizieren. In der *Stern („Star")* Topologie ist kein Computer direkt mit den anderen verbunden. Stattdessen sind sie über einen zentralen Punkt miteinander verbunden und das Gerät am zentralen Punkt ist verantwortlich für die Weiterleitung von Informationen von Computer zu Computer. Sind mehrere zentrale Punkte miteinander verbunden erhält man eine *erweiterte Stern* („Extended Star") Topologie. In der Stern oder erweiterten Stern Topologie sind alle zentralen Punkte *Peers,* das heißt, jeder tauscht Informationen auf einer gleichberechtigten Basis aus. Verbindest du zwei Stern- oder erweiterte Stern-Netzwerke durch einen zentralen Punkt, der den Informationsaustausch zwischen den beiden Netzwerken regelt oder einschränkt, hast Du ein neues „hierarchisches" Netzwerk erzeugt.

3.3 TCP/IP Modell

3.3.1 Einführung

TCP/IP wurde vom DoD(Department of Defense, Verteidigungsministerium) der Vereinigten Staaten und vom DARPA (Defense Advanced Research Project Agency, eine dem Verteidigungsministerium unterstellte Forschungseinrichtung der US-Armee) in den 70er Jahren entwickelt. TCP/IP wurde als ein offener Standard gestaltet den jeder nutzen konnte, um Computer miteinander zu verbinden, und um Informationen zwischen diesen auszutauschen. Letztendlich wurde es die Basis für das Internet.

3.3.2 Schichten

Das TCP/IP Modell definiert vier völlig unabhängige Schichten in welche der Prozess der Kommunikation zwischen zwei Geräten eingeteilt wird. Die Schichten, durch welche Informationen zwischen zwei Geräten weitergegeben werden sind:

3.3.2.1 Die Anwendungsschicht (Application):

Die Anwendungsschicht ist die Schicht, die am nächsten am Benutzer ist. Sie ist dafür verantwortlich, die Daten aus der Anwendung in Informationen zu übersetzen welche über das Netzwerk versendet werden können.

Die grundsätzliche Funktionen dieser Schicht sind:

- Repräsentation
- Codierung
- Dialogkontrolle
- Anwendungsmanagement

3.3.2.2 Die Transportschicht (Transport):

Die Transportschicht baut virtuelle Verbindungen für die Übertragung von Informationen auf, hält sie aufrecht und schließt sie wieder. Sie stellt Kontrollmechanismen für den Datenfluss zur Verfügung und erlaubt das Senden von Informationen. Des Weiteren stellt Sie auch Mechanismen für die Erkennung und Korrektur von Fehlern bereit. Informationen die von der Applikationsschicht zu dieser Schicht gelangen, sind in verschieden Segmente eingeteilt. Informationen, die von der Internetschicht zur Transportschicht kommen, gelangen über Ports wieder in die Anwendungsschicht. (Details zu Ports findest du im Abschnitt 3.3.5 Ports)

Die grundsätzlichen Funktionen dieser Schicht sind:

- Zuverlässigkeit
- Flusskontrolle
- Fehlerkorrektur
- Senden von Informationen

3.3.2.3 Die Internetschicht (Internet):

Diese Schicht teilt die Segmente der Transportschicht in Pakete und sendet die Pakete über das Netzwerk welches das Internet ausmacht. Dazu nutzt es IP oder Internet Protokoll Adressen um den Ort des empfangenden Gerätes zu bestimmen. Es gewährleistet dabei keine Zuverlässigkeit für die Verbindung denn hierauf achtet schon die Transportschicht aber sie ist verantwortlich für die Wahl der besten Route zwischen dem absendenden und dem empfangenden Gerät.

3.3.2.4 Die Netzwerkzugangsschicht (Network Access):

Diese Schicht ist verantwortlich für das Senden von Informationen auf der LAN Ebene, wie auch auf der physikalischen Ebene. Sie wandelt alle Informationen, die von den oberen Schichten ankommen in die einfachsten Informationen (bits) um, die ein Computer verarbeiten kann, und leitet Sie zur richtigen Stelle weiter. Auf dieser Ebene wird auch das Ziel der zu übertragenden Informationen durch die *MAC* oder „*media access control*“ Adresse des empfangenden Gerätes ermittelt.

3.3.3 Protokolle

Um Informationen zwischen zwei Geräten senden zu können müssen beide die gleiche Sprache sprechen. Diese Sprache nennt man Protokoll.

Einige Protokolle, die auf der Applikationsschicht des TCP/IP Modells auftauchen sind zum Beispiel:

- File Transport Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)

- Post Office Protocol 3 (POP3)
- Domain Name Service (DNS)
- Trivial File Transport Protocol (TFTP)

Die Protokolle der Transportschicht sind:

- Transport Control Protocol (TCP)
- User Datagram Protocol (UDP)

Die Protokolle der Internetschicht sind:

- Internet Protocol (IP)

Das Protokoll das meistens auf der Netzwerkzugriffsschicht genutzt wird ist:

- Ethernet

Die oben aufgelisteten Protokolle und die damit verbundenen Ports werden im folgenden Abschnitt erklärt.

3.3.3.1 Protokolle der Anwendungsschicht (application layer)

Das FTP oder „File Transfer Protocol“ wird zur Übertragung von Dateien zwischen zwei Geräten verwendet. Es verwendet dazu TCP um virtuelle Verbindungen zur Kontrolle der Informationen aufzubauen dann wird eine weitere Verbindung aufgebaut die zur Auslieferung der Daten benutzt wird. Die meist benutzten Ports sind 20 und 21.

HTTP oder „Hypertext Transfer Protocol“ wird zum Übersetzen von Informationen in Web Seiten genutzt. Diese Information wird in einer Art und Weise verteilt die vergleichbar mit der ist wie sie für Elektronischer Post genutzt wird. Der meist benutzte Port ist 80.

SMTP oder „Simple Mail Transfer Protocol“ ist ein elektronischer Post („mail“, „electronic mail“, „E-Mail“) Dienst der auf dem FTP Modell basiert. Es überträgt Elektronische Post zwischen zwei Systemen und stellt die Benachrichtigung über ankommende Post sicher. Der meist benutzte Port ist 25.

POP3 oder „Post Office Protocol 3“ wird dazu verwendet, E-Mail zu holen, die mit SMTP (siehe oben) verschickt worden sind. In deinem E-Mail Programm (Outlook, Mozilla Thunderbird) wirst du in den Optionen meistens zwei Einträge für Server finden. SMTP Server lässt dich Nachrichten verschicken, POP3 lässt dich Nachrichten abholen, die du dann mit deinem E-Mail Programm lesen kannst. Für beide braucht du meistens Zugangsdaten.

DNS oder Domain Name Service ist ein Mittel um einen Domainnamen mit einer IP Adresse zu verknüpfen. Mit DNS wandelt man also URLs wie http://www.isecom.org in eine IP-Adresse wie 216.92.116.13 um („DNS lookup“). Andersherum funktioniert das auch („reverse DNS lookup“). Der meist benutzte Port ist 53.

TFTP oder Trivial File Transfer Protocol hat die gleiche Funktion wie FTP aber nutzt UDP anstatt TCP. (Für Details zu den Unterschieden zwischen UDP und TCP schau Dir den Abschnitt 3.3.3.2 an). Das ergibt zwar mehr Geschwindigkeit aber dafür weniger Sicherheit und Vertrauenswürdigkeit. Der meist benutzte Port ist 69.

3.3.3.2 Protokolle der Transportschicht

Es gibt zwei Protokolle die von der Transportschicht zur Auslieferung von Informationssegmenten genutzt werden können.

TCP oder Transmission Control Protocol erstellt eine logische Verbindung zwischen den Endpunkten eines Netzwerks. Es synchronisiert und reguliert den Verkehr mit etwas das bekannt ist als „Three Way Handshake", „Drei Wege Händeschütteln". Beim „Three Way Handshake" sendet das abgehende Gerät ein Anfangspaket das SYN genannt wird zum empfangenden Gerät. Das empfangende Gerät sendet daraufhin ein Antwortpaket das SYN/ACK genannt wird. Dann sendet das abgehende Gerät ein sogenanntes ACK Paket das eine Antwort auf die Antwort ist. An diesem Punkt haben beide Geräte, das abgehende sowie das empfangende, festgestellt das die Verbindung zwischen beiden Geräten zum Empfang und Versand der Daten sowohl hin als auch zurück zu jedem bereit ist.

UDP oder User Datagram Protcol ist ein Transportprotokoll welches nicht auf einer Verbindung basiert. In diesem Fall sendet das abgehende Gerät Pakete an den Empfänger ohne das Gerät des Empfängers zu warnen das es diese annehmen soll. Es liegt dann am empfangenden Gerät zu entscheiden ob die Pakete akzeptiert werden oder nicht. Das Resultat ist, dass UDP schneller ist als TCP, aber im Gegenzug ohne die Sicherheit das ein Paket akzeptiert wird oder gar ankommt.

3.3.3.3 Protokolle der Internetschicht

IP oder Internet Protokoll dient als ein universelles Protokoll das jeglichen zwei Computer zu jeder Zeit erlaubt über jedes Netzwerk zu kommunizieren. Wie UDP ist es verbindungslos da es keine Verbindung mit einem entfernten Computer herstellt. Stattdessen ist es etwas das bekannt ist als best effort (es gibt sich die größte Mühe) Dienst, das heißt es wird alles tun was möglich ist um sicherzustellen das es korrekt arbeitet, aber die Zuverlässigkeit ist eben nicht garantiert. Das Internet Protokoll legt das Format für die Paket Header fest, eingeschlossen die IP Adressen von beiden, dem abgehenden und dem empfangendem Gerät.

3.3.4 IP Adressen

Der Domänenname ist der Name der Web Adresse den Du normal in Deinen Web Browser tippst. Dieser Name identifiziert eine oder mehrere IP Adressen. Domänennamen werden in URLs (Web Adresse) benutzt um eine spezielle Web Seite zu identifizieren.

Zum Beispiel ist in der URL http://www.pcwebopedia.com/index.html pcwebopedia.com der Domänenname.

Jeder Domänenname hat einen Suffix (Endsilbe) welche anzeigt zu welcher Top Level Domain (TLD) er gehört. Es gibt nur eine begrenzte Anzahl an solchen Domänen.

.gov – Regierungsstellen der USA

.edu – Bildungseinrichtungen der USA

.org – Organisationen

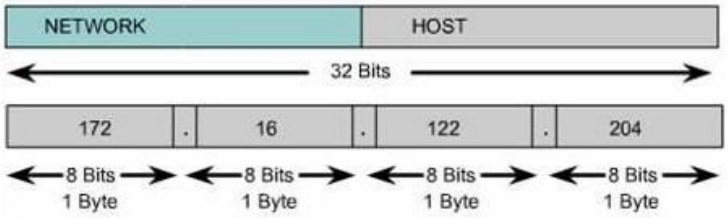
.com – kommerzielle Unternehmen

.net – Netzwerk Organisationen

.de – deutsche Webseiten

Weil das Internet auf IP Adressen basiert und nicht auf Domänennamen, benötigt jeder Web Server einen Domain Name System (DNS) Server um Domänennamen in IP Adressen übersetzen zu können.

IP Adressen sind die Kennungen die dazu benutzt werden um zwischen Computern und anderen Geräten zu unterscheiden welche mit dem Netzwerk verbunden sind. Jedes Gerät muss dazu ein unterschiedliche IP Adresse haben, damit keine Probleme mit einer irrtümlichen Identifizierung innerhalb des Netzwerks auftauchen. IP Adressen sind zusammengesetzt aus 32 bits, die in vier 8 bit Octets unterteilt und durch Punkte getrennt sind. Ein Teil der IP Adresse identifiziert das Netzwerk und der Rest der IP Adresse identifiziert den individuellen Computer im Netzwerk.



Es gibt sowohl öffentliche wie auch private IP Adressen. Private IP Adressen werden für private Netzwerke genutzt die keine Verbindung zu außenstehenden Netzwerken haben. IP Adressen in einem privaten Netzwerk sollten innerhalb dieses Netzwerks nicht kopiert werden, aber Computer in zwei verschiedenen, nicht miteinander verbundenen, privaten Netzwerken können gleiche IP Adressen haben. Die IP Adressen, die durch das IANA die „Internet Assigned Numbers Authority“ vorgegeben wurden und für private Netzwerke genutzt werden können sind:

10.0.0.0 bis 10.255.255.255

172.16.0.0 bis 172.31.255.255

192.168.0.0 bis 192.168.255.255

IP Adressen sind eingeteilt in Klassen die darauf basieren welcher Teil der Adresse benutzt wird um das Netzwerk zu identifizieren und welcher Teil dazu genutzt wird um die einzelnen Computer zu identifizieren.

Abhängig von der Größe die jedem Teil zugesprochen wird, sind mehr Geräte im Netzwerk oder mehrere Netzwerke erlaubt. Die vorhandenen Klassen sind:

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Klasse A: Das erste bit ist immer Null, daher beinhaltet diese Klasse die Adressen zwischen 0.0.0.0 und 126.255.255.255. Hinweis: die Adressen von 127.x.x.x sind reserviert für die Dienste loopback oder localhost.

Klasse B: Die ersten zwei bits des ersten Octet sind '10', daher beinhaltet diese Klasse die Adressen zwischen 128.0.0.0 und 191.255.255.255.

Klasse C: Die ersten drei bits des ersten Octet sind '110', daher beinhaltet diese Klasse die Adressen zwischen 192.0.0.0 und 223.255.255.255.

Klasse D: Die ersten vier bits des ersten Octet sind '1110', daher beinhaltet diese Klasse die Adressen zwischen 224.0.0.0 und 239.255.255.255. Diese Adressen sind reserviert für Gruppen Multicast Implementierungen.

Die restlichen Adressen werden für experimentelle Zwecke oder für mögliche zukünftige Belegungen genutzt.

Derzeit werden die Klassen nicht dazu genutzt zwischen dem Teil der Adresse der das Netzwerk identifiziert und dem Teil der das einzelne Gerät identifiziert zu unterscheiden. Stattdessen wird eine Maske genutzt. In der Maske stellt ein bit mit dem Wert '1' den Teil dar der die Netzwerk Identifikation beinhaltet, und der Wert '0' stellt den Teil dar, der das einzelne Gerät identifiziert. Um nun ein Gerät zu identifizieren, ist es nötig, als Zusatz zur IP Adresse eine Netzwerk Maske („netmask“) zu bestimmen.

IP: 172.16.1.20
Mask: 255.255.255.0

Die IP Adressen 127.x.x.x sind für die Nutzung als loopback oder local host Adressen reserviert, das heißt, sie weisen direkt wieder auf den lokalen Computer zurück. Jeder Computer hat die lokale Host Adresse 127.0.0.1 darum kann diese Adresse nicht zur Identifizierung von verschiedenen Geräten benutzt werden. Es gibt noch andere Adressen die nicht benutzt werden können. Das sind die Netzwerk Adresse und die Broadcast Adresse.

Die Netzwerk Adresse ist eine Adresse in der der der Geräteteil der Adresse nur aus Nullen besteht. Diese Adresse kann nicht benutzt werden weil sie ein Netzwerk identifiziert und kann deshalb niemals ein bestimmtes Gerät identifizieren.

IP: 172.16.1.0
Mask: 255.255.255.0

Die Broadcast Adresse ist eine Adresse in welcher der Teil der Adresse der normalerweise das Gerät identifiziert nur aus Einsen besteht. Diese Adresse kann nicht dazu benutzt werden um ein bestimmtes Gerät zu identifizieren da die Adresse dazu benutzt wird um Informationen an alle Computer zu senden die zum angegebenen Netzwerk gehören.

IP: 172.16.1.255
Mask: 255.255.255.0

3.3.5 Ports

Sowohl TCP als auch UDP nutzen Ports, um Informationen zwischen Anwendungen auszutauschen. Ein Port ist eine Erweiterung einer Adresse, vergleichbar etwa mit dem Hinzufügen einer Wohnungs- oder Raum Nummer zur Adresse. Ein Brief mit einer Adresse wird am korrekten Gebäude ankommen, aber ohne die Wohnungsnummer wird er nicht zum korrekten Empfänger gelangen. Ports arbeiten auf die gleiche Art und Weise. Ein Paket kann an die korrekte IP Adresse ausgeliefert werden aber ohne den zugehörigen Port ist es unmöglich zu ermitteln welche Anwendung für das Paket handeln soll.

Sobald die Ports definiert sind, ist es für die verschiedenen Arten von Informationen, die zu einer IP Adresse gesendet wurden, möglich, an die dementsprechende Anwendung weitergegeben zu werden. Durch die Nutzung von Ports kann ein laufender Dienst auf einem entfernten Computer ermitteln, welche Art von Information ein lokaler Rechner anfordert, welches Protokoll dazu benötigt wird, um die Informationen zu senden, und er kann gleichzeitig die Kommunikation mit anderen, verschiedenen Rechnern aufrechterhalten.

Wenn zum Beispiel ein lokaler Computer versucht, sich mit der Webseite www.osstmm.org zu verbinden, deren IP Adresse 62.80.122.203 ist, und auf deren Computer ein Web Server auf Port 80 läuft, dann wird der lokale Computer sich zum entfernten Computer über folgende Socket Adresse verbinden:

62.80.122.203:80

Um ein gewisses Niveau der Standardisierung bezüglich den meistgenutzten Ports Aufrechtzuhalten hat die IANA die Nummerierung von 0 bis 1024 für allgemein benutzte Ports eingeführt. Die restlichen Ports – aufsteigend bis 65535 – werden für die dynamische Belegung oder spezielle Dienste genutzt.

Die gebräuchlichsten Ports – wie von der IANA vergeben – sind nachfolgend aufgelistet:

Port Assignments		
Decimals	**Keywords**	**Description**
0		Reserved
1-4		Unassigned
5	rje	Remote Job Entry
7	echo	Echo
9	discard	Discard
11	systat	Active Users
13	daytime	Daytime
15	netstat	Who is Up or NETSTAT
17	qotd	Quote of the Day
19	chargen	Character Generator
20	ftp-data	File Transfer [Default Data]
21	ftp	File Transfer [Control]
22	ssh	SSH Remote Login Protocol
23	telnet	Telnet
25	smtp	Simple Mail Transfer
37	time	Time
39	rlp	Resource Location Protocol
42	nameserver	Host Name Server
43	nicname	Who Is
53	domain	Domain Name Server
67	bootps	Bootstrap Protocol Server
68	bootpc	Bootstrap Protocol Client
69	tftp	Trivial File Transfer
70	gopher	Gopher
75		any private dial out service
77		any private RJE service
79	finger	Finger

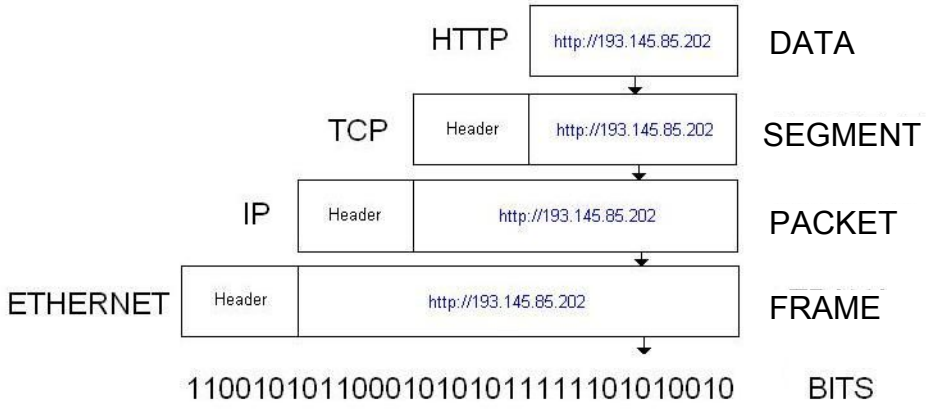
Port Assignments		
Decimals	**Keywords**	**Description**
80	www-http	World Wide Web HTTP
95	supdup	SUPDUP
101	hostname	NIC Host Name Server
102	iso-tsap	ISO-TSAP Class 0
110	pop3	Post Office Protocol - Version 3
113	auth	Authentication Service
117	uucp-path	UUCP Path Service
119	nntp	Network News Transfer Protocol
123	ntp	Network Time Protocol
137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS Datagram Service
139	netbios-ssn	NETBIOS Session Service
140-159		Unassigned
160-223		Reserved

Du kannst auf der Web Seite: *http://www.isecom.org/oprp* noch detailliertere Informationen zu Ports finden.

3.3.6 Kapselung

Wenn ein Stück Information – zum Beispiel eine E-Mail – von einem Computer zu einem anderen geschickt wird, ist diese Gegenstand einer Serie von Umbildungen. Die Anwendungsschicht erzeugt die Daten welche dann zur Transportschicht gesendet werden. Die Transportschicht nimmt diese Informationen und fügt einen Header an. Dieser Header beinhaltet Informationen wie die IP Adresse des abgehenden und des empfangenden Computers, welches erklärt was mit den Daten getan werden muss damit es am gewünschten Ziel ankommt. Die nächste Schicht fügt ebenfalls einen Header hinzu, und so geht es auch mit den anderen Schichten weiter. Diese sich selbst aufrufende Prozedur ist auch bekannt als Verkapselung.

Jede Schicht nach der ersten verkapselt ihre Daten mit den Daten der vorhergehenden Schicht, bis man bei der letzten Schicht angekommen ist, in welcher dann die letztendliche (physikalische) Übertragung passiert. Das nachfolgende Schaubild erklärt die Verkapselung in grafischer Form:



Wenn die verkapselten Informationen an Ihrem Ziel ankommen, müssen Sie dort entkapselt werden. Weil jede Schicht Informationen von der vorhergehenden mit bekommt werden die nicht benötigten Informationen welche von der vorhergehenden Schicht in den Header geschrieben wurden entfernt.

3.4 Übungen

3.4.1 Übung 1: Netstat

Der netstat Befehl zeigt Dir den Zustand der Ports auf einem Computer. Damit Du es ausführen kannst musst Du ein MS-DOS Fenster öffnen und folgendes eingeben:

netstat

In dem MS-DOS Fenster wirst Du dann eine Liste der festgestellten Verbindungen sehen. Wenn Du die Verbindungen in numerischer Form sehen möchtest gibst Du folgendes ein:

netstat - n

Um alle Verbindungen und aktive Ports anzuzeigen, gibst Du ein:

netstat -an

Wenn du sehen willst, was es noch für Optionen für netstat gibt, gib ein:

netstat -h

Wenn du den netstat-Output ansiehst, findest du in der zweiten und dritten Spalte die lokale und die „remote“ IP-Adresse der aktiven Ports, also die deines Computers und die des Computers, mit dem du verbunden bist. Warum unterscheiden sich die remote Ports von denen auf deinem Computer?

Als nächstes öffne in einem Webbrowser die folgende Seite:

http://193.145.85.202

Anschließend öffne dein DOS-Fenster erneut und rufe netstat auf. Welche neuen Verbindungen sind aufgetaucht?

Öffne noch einen Webbrowser und rufe folgende Seite auf:

http://193.145.85.203

Gehe ins DOS-Fenster zurück und starte wiederum netstat.

– Warum taucht http in mehreren Zeilen auf?

– Worin besteht der Unterschied zwischen den Zeilen?

– Wenn mehrere Browser auf deinem Computer gleichzeitig laufen, wie weiß dein Rechner, welcher Browser welche Informationen erhält?

3.4.2 Übung 2: Ports und Protokolle

In dieser Lektion hast du gelernt, dass Ports benötigt werden, um zwischen Diensten („services“) zu unterscheiden.

Wie kommt es, dass du keinen Port angeben musst, wenn du deinen Webbrowser verwendest?

Ist es möglich, dass ein Protokoll in mehr als einer Instanz verwendet wird?

3.4.3 Übung 3: Mein erster Server

Für diese Übung benötigst du das Programm netcat. Wenn du es noch nicht hast, kannst du es hier herunterladen:

http://www.atstake.com/research/tools/network_utilities/

Wenn du netcat installiert hast, öffne ein DOS-Fenster und wechsle in das netcat Verzeichnis (das Verzeichnis, wohin du netcat installiert hast). Gib dort ein:

nc -h

Dies zeigt Dir die verfügbaren Optionen von netcat an. Um einen einfachen Server zu starten gib ein:

netcat -l -p 1234

Wenn das Programm ausgeführt wird, wird Port 1234 geöffnet und eingehende Verbindungen zu diesem Port erlaubt. Öffne ein zweites DOS Fenster und gib ein:

netstat -a

Dies sollte dir jetzt anzeigen, dass ein neuer Dienst auf Port 1234 hört. Schließe dieses DOS Fenster wieder.

Um wirklich sichergehen zu können, dass der Server korrekt funktioniert, muss sich ein Client, also ein Programm, das den Dienst eines Servers in Anspruch nehmen kann, mit dem Server eine Verbindung herstellen. Öffne ein neues DOS Fenster, wechsle ins netcat Verzeichnis und gib ein:

nc localhost 1234

Mit diesem Befehl erstellst du eine Verbindung zum Service auf deinem lokalen („localhost“) Rechner, der auf Port 1234 hört. Wenn du jetzt in diesem Fenster Text eintippst, wirst du sehen, dass dieser auch im Serverfenster erscheint.

Schließe jetzt alle DOS-Fenster und öffne ein neues, wo du ins netcat Verzeichnis wechselst. Erstelle dort eine Datei mit dem Namen test, die den Text „Willkommen auf dem Hackerhighschool Testserver“ enthält. Anschließend gib ein:

netstat -l -p 1234 < test

Wenn du dich jetzt in einem anderen DOS-Fenster mit netcat mit diesem Port verbindest, solltest du den Inhalt der Datei test sehen. Um netcat zu beenden, drücke in seinem DOS Fenster Strg-C.

Welches Protokoll wurde verwendet, als du dich mit dem netstat Server verbunden hast?

Kann man dieses Protokoll ändern? Wenn ja, wie?

Weitere Informationen

http://www.oreilly.com/catalog/fire2/chapter/ch13.html
http://www.oreilly.com/catalog/puis3/chapter/ch11.pdf
http://www.oreilly.com/catalog/ipv6ess/chapter/ch02.pdf
http://info.acm.org/crossroads/xrds1-1/tcpjmy.html
http://www.garykessler.net/library/tcpip.html
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm
http://www.redbooks.ibm.com/redbooks/GG243376.html

Referenzen zu den Portnummern:
http://www.iana.org/assignments/port-numbers
http://www.isecom.info/cgi-local/protocoldb/browse.dsp