Hacker Highschool
SECURITY AWARENESS FOR TEENS

LES 3
POORTEN EN PROTOCOLLEN

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.

Informatie over de Gebruiksvoorwaarden

De lessen en werkboeken van het Hacker Highschool (HHS) project zijn beschikbaar onder de volgende door ISECOM gestelde voorwaarden:

Alle informatie uit het HHS-project mag, niet-commercieel, gebruikt worden voor en door basisschool-leerlingen en studenten van middelbaar en hoger onderwijs. Dit materiaal mag niet worden gereproduceerd voor (door-)verkoop in welke vorm dan ook. Gebruik van dit materiaal in een klas, cursus, training, kamp of andere georganiseerde vorm van kennisoverdracht waarvoor geld wordt gevraagd is expliciet verboden zonder een licentie. Om een licentie te regelen kunt u het onderdeel LICENSE bezoeken op de website van de Hacker Highschool, www.hackerhighschool.org/license.

Het HHS-project is een leermiddel en, zoals met elk leermiddel, de docent/trainer bepaalt in grote mate het effect van het leermiddel. ISECOM kan geen aansprakelijkheid aanvaarden voor de positieve of negatieve gevolgen van het gebruik van dit materiaal en de daarin opgenomen informatie.

Het HHS-project is een initiatief van de open community, en wanneer u de resultaten van onze inspanning waardevol genoeg vindt om het te gebruiken, vragen we u uw steun te betuigen door:

- de aankoop van een licentie;
- een donatie
- ons te sponsoren.

Op al het werk berust copyright van ISECOM, 2004.

Inhoudsopgave

Auteurs

Gary Axten, ISECOM

La Salle URL Barcelona

Kim Truett, ISECOM

Chuck Truett, ISECOM

Marta Barcelo, ISECOM

Pete Herzog, ISECOM

Vertaald door:

Raoul Teeuwen

3.1 Introductie

De tekst en oefeningen in deze les proberen een basisidee te geven van momenteel gebruikte poorten en protocollen en hun belang binnen een besturingssysteem, Windows en Linux.

Daarnaast krijg je de kans kennis te maken met een aantal handige hulpmiddelen die je helpen te begrijpen welke netwerk-mogelijkheden je computersysteem heeft.

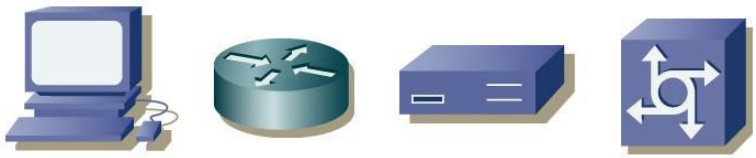
Aan het eind van de les zou je basisbegrip moeten hebben van:

- het concept van netwerken
- IP adressen
- poorten en protocollen.

3.2 Basis concepten van netwerken

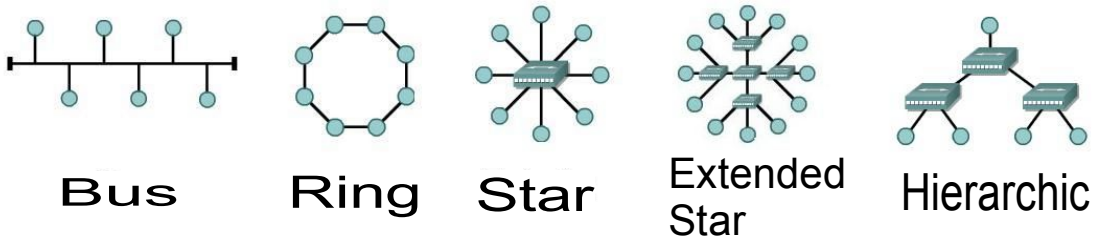
3.2.1 Apparaten

Om de uitleg over protocollen en poorten te begrijpen is het nodig dat je bekend bent met de iconen waarmee veel voorkomende apparaten worden weergegeven in schema's. Het gaat om:



3.2.2 Topologien

Met deze apparaten kan een lokaal netwerk of LAN (Local Area Network) worden gemaakt. In een LAN kunnen computers middelen, zoals harde schijven, printers en internet verbindingen, delen. Ook kan een administrator (beheerder) bepalen hoe deze middelen gedeeld worden. Als een LAN wordt ontworpen kan men kiezen uit de volgende topologien:



BUS **RING** **STER** **BOOM** **HIERARCHISCH**

In een bus topologie zijn alle computers aangesloten aan hetzelfde transportmiddel en kan elke computer communiceren met alle andere. In de ring configuratie is elke computer verbonden met de volgende, en de laatste met de eerste, en elke computer kan alleen communiceren met zijn directe buren. In de ster topologie is geen enkele computer rechtstreeks met een andere verbonden. In plaats daarvan zijn ze verbonden met een centraal punt en het apparaat op dat centrale punt is ervoor verantwoordelijk informatie tussen de computers uit te wisselen. Wanneer meerdere centrale punten met elkaar verbonden zijn, dan spreken we van een boom topologie. In een ster- en boom-topologie zijn alle centrale punten gelijkwaardig. Wanneer je echter twee ster- of boom-netwerken met elkaar verbindt via een centraal punt waarmee de gegevensuitwisseling tussen de twee delen beheerd of beperkt wordt dan heb je een hierarchische netwerk topologie gemaakt.

3.3 TCP/IP model

3.3.1 Introductie

TCP/IP werd in de jaren '70 ontwikkeld door het Ministerie van Defensie van de Verenigde Staten (DoD, Department of Defense) en het Defensie onderzoeks-centrum DARPA (Defense Advanced Research Project Agency). TCP/IP werd ontwikkeld als een open standaard die iedereen kon gebruiken om computers met elkaar te verbinden en informatie uit te wisselen. Uiteindelijk werd het de basis van het Internet.

3.3.2 Lagen

Binnen het TCP/IP model worden vier onafhankelijke lagen onderkend om het communicatieproces tussen twee apparaten te beschrijven. De lagen waarlangs informatie tussen twee apparaten gaat zijn:

3.3.2.1 Applicatie

De applicatie-laag is de laag die het dichtst bij de gebruiker zit. Deze laag zorgt dat informatie uit applicaties wordt vertaald in informatie die via een netwerk verstuurd kan worden.

De basis functies van deze laag zijn:

- Representatie (Representation)
- Coderen (Codification)
- Sessie management (Dialog Control)
- Applicatie Management

3.3.2.2 Transport

De transport-laag bouwt virtuele verbindingen voor informatie-uitwisseling op, onderhoudt ze en verbreekt ze weer. Hij verzorgt controle-mechanismes voor data-uitwisseling en voor het detecteren en corrigeren van fouten. De informatie die vanuit de applicatie-laag aankomt wordt in stukjes (segmenten) opgedeeld. Informatie die de transport-laag bereikt vanuit de internet-laag wordt aan de applicatie-laag aangeboden via poorten. (zie paragraaf 3.3.5 Poorten voor uitleg over poorten.)

De basis-functies van deze laag zijn:

- Betrouwbaarheid (Reliability)
- Stroomregulering (Flow Control)
- Fout-herstel (Error Correction)
- Broadcasting (het gelijktijdig uitzenden van een pakket naar meerdere bestemmingen)

3.3.2.3 Internet

Deze laag deelt de segmenten uit de transport-laag op in pakketjes en zend de pakketjes over de netwerken die het Internet vormen. Het gebruikt IP, of internet protocol adressen om de lokatie te bepalen van het apparaat waar het pakketje naartoe moet. Deze laag bemoeit zich niet met de vraag of alles goed verloopt; dit wordt namelijk afgehandeld door de transport-laag. De internet-laag zorgt er wel voor dat de beste route tussen afzendend apparaat en ontvangend apparaat wordt bewandeld.

3.3.2.4 Netwerk toegang

Deze laag regelt informatie-uitwisseling met het LAN- en fysieke niveau. De laag vertaalt alle informatie van de bovenliggende lagen naar de meest basale informatie-eenheden (bits) en verstuurt het naar de juiste lokatie. Op dit niveau wordt het bestemmingsadres van de informatie bepaald door het MAC-, of media access control, adres van het geadresseerde apparaat.

3.3.3 Protocollen

Om informatie tussen twee apparaten uit te kunnen wisselen, moeten ze dezelfde taal spreken. Deze taal noemt men het protocol.

De protocollen die je tegenkomt in de applicatie-laag van het TCP/IP-model zijn:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (smtp)
- Domain Name Service (DNS)

- Trivial File Transfer Protocol (TFTP)

De protocollen van de transport-laag zijn:

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

De protocollen van het internet-laag zijn:

- Internet Protocol (IP)

Het meest gebruikte protocol in de network-toegang-laag is:

- Ethernet

De bovengenoemde protocollen en de bijbehorende poorten worden beschreven in de navolgende paragrafen.

3.3.3.1 Applicatie laag protocollen

FTP of file transfer protocol wordt gebruikt om bestanden tussen 2 apparaten uit te wisselen. FTP gebruikt TCP om een virtuele verbinding te maken voor het managen van de informatiestroom, waarna nog een verbinding wordt opgezet voor het uitwisselen van de data. Meestal worden hier de poorten 20 en 21 voor gebruikt.

HTTP of hypertext transfer protocol wordt gebruikt om informatie te vertalen in webpagina's. Deze informatie wordt op een zelfde manier verspreid als waarop e-mail wordt verspreid. De meest gebruikte poort is poort 80.

SMTP of simple mail transfer protocol is een mail service welke is gebaseerd op het FTP-model. Er wordt mail tussen twee systemen mee uitgewisseld en het zorgt voor een seintje van inkomende mail. De meest gebruikte poort voor SMTP is poort 25.

DNS of domain name service zorgt voor de koppeling tussen een domain name (domein naam) met een ip-adres. De meest gebruikte poort is poort 53.

TFTP of trivial file transfer protocol heeft dezelfde functies asl FTP maar gebruikt UDP in plaats van TCP.
(Zie Paragraaf 3.3.3.2 voor details over de verschillen tussen UDP en TCP.) Het zorgt voor meer snelheid, maar voor minder beveiliging en betrouwbaarheid. De meest gebruikte poort is poort 69.

3.3.3.2 Transport laag Protocollen

Er zijn twee protocollen die door de transportlaag gebruikt kunnen worden voor het afleveren van informatie-segmenten.

TCP of transmission control protocol zorgt voor een logische verbinding tussen de twee eindpunten binnen het netwerk. Het synchroniseert en regelt het verkeer met een manier die men "Three Way Handshake" noemt. Bij de “Three Way Handshake” stuurt het zendende apparaat als eerste een zogenaamd SYN pakketje. Het geadresseerde apparaat stuurt een bevestigingspakket, een zogenaamdSYN/ACK-pakket. Het zendende apparaat stuurt vervolgens een pakket met de naam ACK, en dat is een bevestiging (Engels: ACKnowledgement) van de bevestiging. Op dat moment

hebben de afzender en de geadresseerde vastgesteld dat er een verbinding is en dat beide apparaten er klaar voor zijn om data uit te wisselen.

UDP of user datagram protocol is een transport protocol welke niet is gebaseerd op een verbinding. Het zendende apparaat begint te zenden zonder vooraf aan de geadresseerde te vragen of hij er klaar voor is. De ontvanger moet maar kijken of hij de data kan ontvangen. Door allerlei controles achterwege te laten is UDP sneller dan TCP, maar kan het niet garanderen dat een pakketje ook wordt aangenomen door de geadresseerde.

3.3.3.3 Internet laag Protocollen

IP of internet protocol dient als universeel protocol om twee computers te laten communiceren via een netwerk. Net als UDP, is het connectionless, omdat het niet eerst een verbinding afspreekt met de ontvangende computer voordat het begint met zenden. Het is een, zoals ze zeggen, best effort service, wat betekent dat het zijn best doet te zorgen dat het werkt, maar geen garanties biedt dat het ook goed werkt. Het Internet Protocol bepaalt het formaat voor de pakket headers, inclusief de IP-adressen van het zendende en het ontvangende apparaat.

3.3.4 IP-adressen

Een domein-naam (domain name) is het web-adres zoals je dat normaal gebruikt in je web-browser. De naam is gekoppeld aan één of meer IP-adressen. Zo is de domeinnaam microsoft.com bijvoorbeeld aan bijna een dozijn IP-adressen gekoppeld. Domein-namen worden gebruikt in URLs om webpagina's te adresseren.

Een voorbeeld: in de URL http://www.pcwebopedia.com/index.html is pcwebopedia.com de domein-naam.

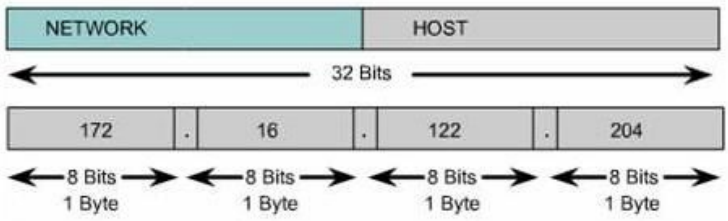
Elke domein-naam heeft een achtervoegsel (Engels: suffix) welke aangeeft tot welk hoofddomein (top level domain, TLD) het behoort.

Er zijn maar een beperkt aantal van zulke domeinen. Enkele voorbeelden:

.gov – overheidsinstellingen (Engels: Government agencies)
.edu – educatieve instellingen (Engels: Educational institutions)
.org – organisaties zonder winstoogmerk (nonprofit)
.com – commerciele bedrijven
.net – netwerk organisaties (Engels: network organizations)

Omdat het internet is gebaseerd op IP-adressen en niet op domein-namen, heeft elke web-server een Domain Name System (DNS)-server nodig om domeinnamen te vertalen naar ip-adressen.

IP-adressen worden gebruikt om verschillende computers en apparaten die op een netwerk zijn aangesloten een unieke naam te geven. Elk apparaat heeft een eigen IP-adres, om te voorkomen dat niet duidelijk is welk apparaat een pakket verzendt of moet ontvangen. Een IP-adres bestaat uit 32 bits, verdeeld in vier octets van elk 8 bits welke gescheiden zijn door een punt. Een deel van het IP-adres is het netwerk-adres, de overige bits identificeren de individuele computers op het netwerk.



Er zijn publieke en private IP-adressen. Private IP-adressen worden gebruikt binnen privé-netwerken die geen directe verbinding hebben met externe netwerken. IP-adressen binnen een privé-netwerk moeten uniek zijn binnen dat netwerk, maar computers op twee verschillende – maar niet verbonden – privé-netwerken zouden hetzelfde IP-adres kunnen hebben. De IP-adressen die door de IANA, de Internet Assigned Numbers Authority, toegestaan zijn om te gebruiken binnen/voor privé-netwerken zijn:

10.0.0.0 tot 10.255.255.255

172.16.0.0 tot 172.31.255.255

192.168.0.0. tot 192.168.255.255

IP-adressen zijn verdeeld in enkele categorien, afhankelijk van welk deel van het adres wordt gebruikt om het netwerk te identificeren.

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

Afhankelijk van hoe groot elk deel is, kunnen er meer of minder apparaten binnen dat netwerk een eigen IP-adres krijgen of hoe meer unieke netwerken er te adresseren zijn. De bestaande categorien (Class) zijn:

- Class A: het eerste bit is altijd nul, dus binnen deze categorie vallen de adressen van 0.0.0.0

tot en met 126.255.255.255 (126 is als je het in bits noteert: 01111110). Noot: de adressen die beginnen met 127.x.x.x (01111111) zijn gereserveerd voor de loopback-service en de localhost.

- Class B: de eerste 2 bits van het eerste octet zijn '10', dus deze categorie omvat de adressen van 128.0.0.0 tot en met 191.255.255.255.
- Class C: de eerste 3 bits van het eerste octet zijn '110', dus deze categorie omvat de adressen van 192.0.0.0 tot en met 223.255.255.255.
- Class D: de eerste 4 bits van het eerste octet zijn '1110', dus deze categorie omvat de adressen van 224.0.0.0 tot en met 239.255.255.255. Deze adressen zijn gereserveerd voor groep multi cast implementaties.
- De overige adressen worden gebruikt voor experimenten of voor toekomstig gebruik.

Op dit moment worden de categorien niet gebruik om onderscheid te maken tussen het deel van het adres wat het netwerk identificeert en het deel dat de individuele apparaten identificeert. Daarvoor in de plaats wordt een masker, een mask, gebruikt. In het masker staat een binair '1' bit voor het deel wat het netwerk identificeert en een '0' binair bit geeft het deel aan waarmee individuele apparaten worden geidentificeerd. Om een apparaat te identificeren is het nodig zowel het IP-adres als het masker te weten:

IP: 172.16.1.20
Mask: 255.255.255.0

IP-adressen 127.x.x.x zijn gereserveerd voor de loopback of local host adressen. Ze verwijzen terug naar de lokale computer. Iedere computer heeft een local host adres van 127.0.0.1, dus dat adres kan niet gebruikt worden om andere apparaten te identificeren. Er zijn ook nog andere adressen die niet gebruikt mogen worden. Dit zijn het netwerk-adres en het broadcast
adres.
Het netwerk adres is een adres waarvan het deel dat normaal gesproken het apparaat binnen het netwerk aangeeft, allemaal nullen bevat. Dit adres kan niet worden gebruikt omdat het een netwerk identificeert, en nooit een specifiek apparaat kan identificeren.

IP: 172.16.1.0
Mask: 255.255.255.0

Het broadcast adres is een adres waarvan het deel dat normaal gesproken het apparaat binnen het netwerk aangeeft, allemaal enen bevat. Dit adres kan niet worden gebruikt om een specifiek apparaat te identificeren omdat het dit adres wordt gebruikt om informatie naar alle computers binnen dat netwerk te sturen.

IP: 172.16.1.255
Mask: 255.255.255.0

3.3.5 Poorten

Zowel TCP en UDP gebruiken poorten om informatie uit te wisselen met applicaties. Een poort is een uitbreiding van een adres, net zoals sommige huizen binnen adres door een toevoeging een eigen adres krijgen (“grote straat 42a”, “grote straat 42b” enz). Een brief waarop het adres staat zonder toevoeging, komt wel aan in de goede straat, maar zonder de toevoeging kan hij niet bij het juiste adres worden afgeleverd. Poorten werken op een soortgelijke manier. Een IP-pakket kan worden afgeleverd bij het juiste IP-adres, maar zonder de bijbehorende poort, kan niet worden bepaald welke applicatie iets met het pakketje moet doen.

Zodra de poorten zijn gedefinieerd wordt het voor de verschillende soorten informatie die naar hetzelfde IP-adres worden gestuurd mogelijk om aan de juiste applicatie aangeboden te worden. Door poorten te gebruiken wordt het voor een service die op een computer op afstand draait mogelijk te bepalen welke soort informatie een lokale client vraagt, te bepalen welk protocol gebruikt moet worden om de informatie te versturen en kunnen er verbindingen worden onderhouden met meerdere clients.

Een voorbeeld: als een lokale computer probeert verbinding te maken met de website www.osstmm.org, waarvan het IP-adres 62.80.122.203 is, met een web-server die draait op poort 80, dan zou de lokale computer verbinding maken met de computer-op-afstand gebruikmakend van het socket adres: **62.80.122.203:80**

Om voor een bepaald niveau van standaardisatie te zorgen bij de meest gebruikte poorten heeft IANA bepaald dat de poorten 0 tot 1024 moeten worden gebruikt for de algemene services.
De overige poorten – tot en met 65535 – worden gebruikt naar behoefte of voor speciale services.

De meest gebruikte poorten – zoals vastgesteld door de IANA – staan hieronder vermeld:

Poort Toewijzingen		
Decimalen	**Sleutelwoorden**	**Omschrijving**
0		Gereserveerd
04/01/05		Niet vastgesteld (Engels: not assigned)
5	rje	Remote Job Entry
7	echo	Echo
9	discard	Discard
11	systat	Active Users
13	daytime	Daytime
15	netstat	Who is Up of 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

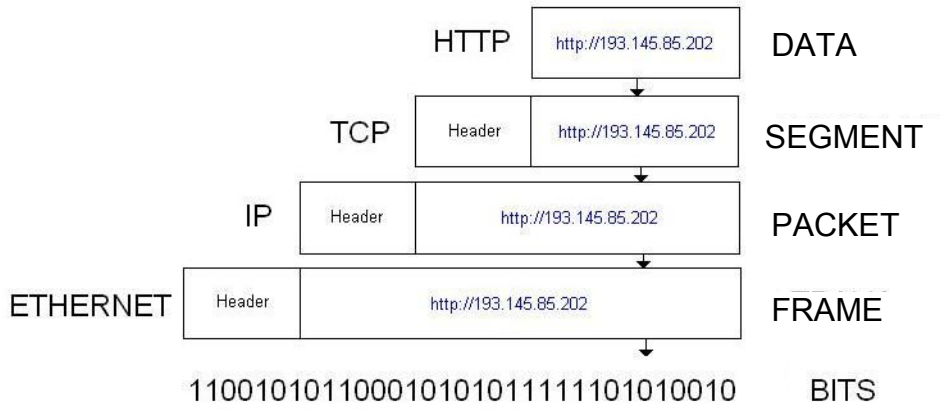
Poort Toewijzingen		
80	www-http	World Wide Web HTTP
95	supdup	SUPDUP
101	hostname	NIC Host Name Server
102	iso-tsap	ISO-TSAP Class 0
110	pop3 P	ost Office Protocol - Version 3
113	auth	Authentication Service
117	uucp-path	UUCP Path Service
119	nntp	Network News Transfer Protocol
123	ntp	Network Time 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

Op http://www.isecom.info/oprp treft u meer gedetailleerde informatie over poorten.

3.3.6 Encapsulatie (Engels: encapsulation)

Wanneer een stuk informatie – bijvoorbeeld een e-mail bericht – van de ene computer naar de andere wordt gestuurd, ondergaat hij enkele keren een omzetting. De applicatie-laag maakt de data, die daarna aan de transport-laag wordt overhandigd. De transportlaag neemt de informatie en voegt er een header aan toe. De header bevat informatie, zoals het IP-adres van de afzender en de geadresseerde, zodat vaststaat wat er moet gebeuren om het pakketje af te leveren. De volgende laag voegt er nog een header aan toe, enzovoorts. Deze herhalende procedure staat bekend als encapsulatie.

Elke laag na de eerste beschouwt de informatie van de vorige laag als data en 'doet er een envelop omheen'/pakt het in, totdat je aankomt bij de laatste laag waar de daadwerkelijke verzending plaatsvindt. De volgende figuur laat grafisch zien wat encapsulatie is:



Wanneer de zo ingepakte informatie aankomt op zijn bestemming, moet het daar weer worden uitgepakt.

Elke laag haalt de informatie uit het pakketje die het krijgt van de vorige laag, en negeert daarbij de header die er door de vorige laag aan is toegevoegd.

3.4 Oefeningen

3.4.1 Oefening 1: Netstat

Netstat
Het Netstat commando kun je gebruiken om de status van de poorten op een computer te bekijken. Om het te gebruiken moet je een MS-DOS window openen en tikken:

netstat

In het MS-DOS window krijg je nu een lijst met verbindingen te zien. Wanneer je de verbindingen in numeriek formaat wil tonen, tik je:

netstat - n

Om de verbindingen en de actieve poorten te zien, tik je:

netstat - an

Om een lijst met nog meer opties te zien, tik je:

netstat - h

In de door Netstat getoonde informatie zie je in kolom twee en drie het IP-adres van de lokale computer en de computer-op-afstand zoals die worden gebruikt door de actieve poorten. Waarom zijn de adressen van de poorten-op-afstand anders dan de lokale adressen?
Open nu de volgende pagina:

http://193.145.85.202

keer dan terug naar de MS-DOS prompt en voer Netstat opnieuw uit. Welke nieuwe verbinding (of verbindingen) verschijnen nu?
Open nu een nieuwe webbrowser en ga naar de volgende pagina:

http://193.145.85.203

Keer terug naar de MS-DOS prompt en voer Netstat uit:

DATA
SEGMENT
PAKKET
FRAME
- Waarom komt het HTTP-protocol in meerdere regels voor?
- Welke verschillen zie je tussen die regels?
- Als er meerdere webbrowsers open zijn, hoe weet de computer dan welke informatie naar welke browser moet?

3.4.2 Oefening 2: Poorten en Protocollen

In deze les leerde je dat poorten worden gebruikt om onderscheid te maken tussen services.
Waarom hoef je bij het gebruik van een webbrowser geen poortnummer te gebruiken?
Welke protocollen worden gebruikt?
Is het mogelijk dat één protocol meerdere keren in gebruik is?

3.4.3 Oefening 3: Mijn Eerste Server

Om deze oefening te doen moet je het Netcat programma hebben. Wanneer je het niet hebt kun je het downloaden van de volgende pagina:

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

Zodra je Netcat geinstalleerd hebt, kun je een MS-DOS window openen. Ga naar de directory (map) waar je Netcat geinstalleerd hebt en tik:

nc - h

Dit laat de opties zien die je met Netcat kunt gebruiken. Om een simpele server te maken tik je:

nc - l - p 1234

Als dat commando is uitgevoerd wordt poort 1234 geopend en zijn inkomende verbindingen toegestaan.

Open een tweede MS-DOS window en tik:

netstat – a

Je zou nu moeten zien dat er een nieuwe service luistert op poort 1234. Sluit dit MS-DOS window.

Om te kunnen stellen dat er een server is geimplementeerd, moet je een client-verbinding tot stand brengen.

Open een MS-DOS window en tik:

nc localhost 1234

Met dit commando wordt een verbinding gemaakt met de server die luistert op poort 1234. Alles wat nu in één van de twee MS-DOS windows wordt getikt, is ook te zien in de ander!

Maak een bestand met de naam 'test' wat de tekst "Welkom bij de server van de Hacker Highschool!" bevat.

Tik nu in een MS-DOS window:

nc - l - p 1234 > test

Vanuit een ander MS-DOS window maak je nu een verbinding met de server door te tikken:

nc localhost 1234

Zodra de client een verbinding krijgt met de server zou je de inhoud van het bestand 'test' te zien moeten krijgen.

Om de service te stoppen ga je naar het MS-DOS window waarin hij draait en druk je CTRL-C.

Welk protocol is gebruikt om verbinding te maken met de server?

Staat Netcat je toe om dit te veranderen? Zo ja, hoe?

Verder lezen

Meer informatie over poorten en protocollen vind je ondermeer op de volgende links:

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

Port Number references:

http://www.iana.org/assignments/port-numbers

http://www.isecom.info/oprp