Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEZIONE 3
PORTE E PROTOCOLLI

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.

Informazioni sulla licenza d’uso

Le seguenti lezioni ed il materiale per gli esercizi (workbook) sono materiale di tipo "open" e pubblicamente disponibili, secondo i seguenti termini e condizioni di ISECOM:

Tutto il materiale inerente il progetto Hacker Highschool è fornito esclusivamente per utilizzo formativo di tipo “non-commerciale” verso gli studenti delle scuole elementari, medie e superiori ed in contesti quali istituzioni pubbliche, private e/o facenti parte di attività del tipo “doposcuola”.

Il materiale non può essere riprodotto ai fini di vendita, sotto nessuna forma ed in nessun modo.

L’erogazione di qualunque tipologia di classe, corso, formazione (anche remota) o stage tramite questo materiale a fronte del corrispondimento di tariffe o denaro è espressamente proibito, se sprovvisti di regolare licenza, ivi incluse classi di studenti appartenenti a college, università, trade-schools, campi estivi, invernali o informatici e similari.

Per comprendere le nostre condizioni di utilizzo ed acquistare una licenza per utilizzi di tipo commerciale, vi invitiamo a visitare la sezione LICENSE del sito web Hacker Highschool all’indirizzo http://www.hackerhighschool.org/license.

Il Progetto HHS è uno strumento per apprendere e, come ogni strumento di questo tipo, la chiave formativa consiste nella capacità e nell'influenza dell'istruttore, e non nello strumento formativo. ISECOM non può accettare e/o farsi carico di responsabilità per il modo in cui le informazioni qui contenute possono essere utilizzate, applicate o abusate.

Il Progetto HHS rappresenta uno sforzo di una comunità aperta: se ritenete il nostro lavoro valido ed utile, vi chiediamo di supportarci attraverso l'acquisto di una licenza, una donazione o una sponsorizzazione al progetto.

Tutto il materiale e' sotto copyright ISECOM, 2004

Indice

Hanno contribuito

Gary Axten, ISECOM

La Salle URL Barcelona

Kim Truett, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Pete Herzog, ISECOM

Per la versione in lingua italiana:

Raoul Chiesa, ISECOM

Doriano Azzena, centro CSAS del progetto Dschola IPSIA Castigliano - Asti

Sophia Danesino, centro CSAS del progetto Dschola ITIS Peano – Torino

Nadia Carpi, centro CSAS del progetto Dschola ITIS Peano – Torino

Fabrizio Sensibile, OPST&OPSA Trainer, @ Mediaservice.net Srl, Torino – ISECOM Authorized Training Partner

Claudio Prono, @ Mediaservice.net Srl, Torino – ISECOM Authorized Training Partner

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

mediaservice.net
CORPORATE SECURITY & IMAGE

LA SALLE
Enginyeria
Arquitectura
Universitat Ramon Llull

3.1 Introduzione

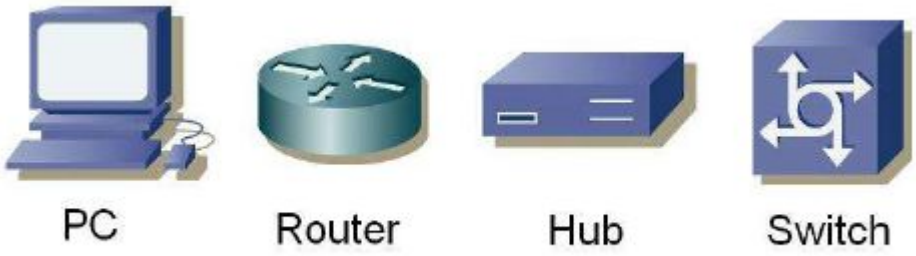
Il testo e gli esercizi di questa lezione mirano a fornire una conoscenza di base sulle porte e sui protocolli più diffusi e ad evidenziarne l'importanza nei sistemi operativi, Windows e Linux. Oltre a ciò, avrete l'opportunità di familiarizzare con un insieme di funzionalità utili che consentono di comprendere le potenzialità di rete del vostro computer. Al termine della lezione avrete una conoscenza di base su:

1. i concetti delle reti
2. gli indirizzi IP
3. le porte e i protocolli

3.2. Concetti base delle reti

3.2.1 Componenti

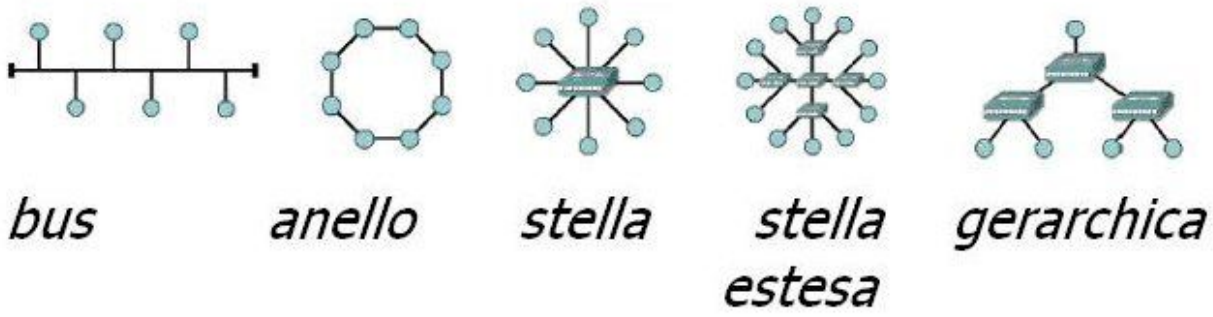
Per comprendere la trattazione reativa alle porte ed ai protocolli, è necessario familiarizzare con le icone che rappresentano i dispositivi più comuni negli schemi di rete. Essi sono:



3.2.2 Topologie

Con questi dispositivi possono essere realizzate reti locali o LAN (Local Area Network). In una LAN i computer possono condividere risorse quali dischi, stampanti e connessioni ad Internet, e un amministratore può controllare come vengono condivise tali risorse.

Quando viene realizzata una LAN è possibile scegliere una tra le seguenti topoogie fisiche:



In una topologia a bus, tutti i computer sono connessi ad un singolo mezzo trasmissivo e ogni computer può comunicare direttamente con gli altri.

Nella configurazione ad anello ogni computer è connesso al successivo e l'ultimo con il primo; ogni computer può comunicare direttamente solo con quelli a lui adiacenti.

In una topologia a stella nessuno dei computer è connesso direttamente agli altri. Al contrario essi sono connessi attraverso un punto centrale e il dispositivo centrale è responsabile di inoltrare le informazioni da un computrer ad un altro. Se più punti centrali sono connessi tra loro, si ottiene una rete a stella estesa.

In una topologia a stella o a stella estesa, tutti i punti centrali sono paritetici, cioè scambiano informazioni su basi uguali. Se, tuttavia, due reti a stella o a stella estesa vengono connesse attraverso un punto centrale che controlla o limita lo scambio di informazioni tra le due reti, si è di fronte ad una singola topologia gerarchica.

3.3. Modello TCP/IP

3.3.1 Introduzione

Il TCP/IP è stato sviluppato dal DoD (Department of Defense) degli Stati Uniti dalla DARPA (Defense Advanced Research Project Agency) negli anni 1970. Il TCP/IP è stato progettato come standard aperto utilizzabile da chiunque per connettere i computer tra loro e scambiare informazioni tra loro. E' diventato il protocollo di base di Internet.

3.3.2 Strati o Livelli

Il modello TCP/IP definisce 4 livelli totalmente indipendenti in cui dividere il proceso di comunicazione tra due dispositivi. I livelli attraverso cui transita l'informazione scambiata tra due dispositivi sono:

3.3.2.1 Applicazione

Lo strato Applicazione (Application) è il livello più vicino all'utente finale. E' il livello deputato a tradurre i dati dalle applicazioni in informazioni che possono essere inviate attraverso la rete.

Le funzioni di questo livello sono:

- Rappresentazione
- Codifica
- Controllo del Dialogo
- Gestione Applicazione.

3.3.2.2 Trasporto

Il livello di Trasporto (Transport) stabilisce, mantiene e termina circuiti virtuali per il trasferimento delle informazioni. Fornisce meccanismi di controllo di flusso, consente il broadcasting e fornisce meccanismi per la rilevazione e correzione degli errori. L'informazione che arriva a

questo livello dal livello applicazione è divisa in segmenti diversi. L'informazione che giunge al livello di trasporto dal livello Internet è inviata al livello applicazione attraverso porte (si veda la sezione 3.3.5 Porte per dettagli sulle porte).

Le funzioni di base di questo livello sono:

- Affidabilità
- Controllo di flusso
- Correzione degli errori
- Broadcasting

3.3.2.3 Internet

Questo livello divide i segmenti del livello di trasporto in pacchetti e li invia attraverso le reti che formano Internet. Usa indirizzi IP (Internet Protocol) per determinare l'ubicazione del destinatario. Non assicura l'affidabilità della connessione, perchè è già compito del livello di trasporto, ma è responsabile di selezionare il cammino migliore tra il nodo sorgente e quello destinatario.

3.3.2.4 Accesso alla rete

Questo livello è deputato ad inviare informazioni sia al livello LAN che al livello fisico. Trasforma tutte le informazioni che giungono dai livelli superiori in informazioni elementari (bit) e le invia alla locazione corretta. A questo livello, la destinazione delle informazioni è determinata dall'indirizzo MAC (Media Access Control) del dispositivo destinatario.

3.3.3 Protocolli

Per poter inviare informazioni tra due dispositivi, entrambi devono utilizzare lo stesso linguaggio. Questo linguaggio è chiamato protocollo. I protocolli che compaiono nel livello applicazione del TCP/IP sono:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name Service (DNS)
- Trivial File Transfer Protocol (TFTP)

I protocolli del livello di trasporto sono:

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

I protocolli del livello Internet sono:

- Internet Protocol (IP)

Un protocollo frequentemente usato dal livello di accesso alla rete è:

- Ethernet

I protocolli elencati sopra e le loro porte associate verranno descritti nelle sezioni seguenti.

3.3.3.1 Protocolli del livello Applicatione

L'**FTP** o file transfer protocol è utilizzato per la trasmissione di files tra due dispositivi. Usa TCP per creare una connessione virtuale per il controllo dell'informazione, poi crea un'altra connessione utilizzata per il trasferimento dei dati. Le porte più comunemente usate sono la 20 e la 21.

HTTP o hypertext transfer protocol è utilizzato per tradurre le informazioni in pagine web. Questa informazione viene distribuita in maniera analoga a quella utilizzata dalla posta elettronica. La porta più comunemente utilizzata è la 80.

SMTP o simple mail transfer protocol è un servizio di posta basato sul modello FTP. Trasferisce posta elettronica tra due sistemi e fornisce una notifica della posta in arrivo. La porta più comunemente utilizzata è la 25.

DNS o domain name service fornisce un meccanismo per associare ad un nome di dominio un indirizzo IP. La porta più comunemente utilizzata è la 53.

TFTP o trivial file transfer protocol ha la stessa funzione di FTP ma usa UDP invece che TCP (si veda la Sezione 3.3.3.2 per i dettagli relativi alle differenze tra UDP e TCP). Questo fornisce maggior velocità, ma minore sicurezza e affidabilità. La porta più comunemente utilizzata è la 69.

3.3.3.2 Protocolli del livello Transporto

Ci sono due protocolli che possono essere usati dal livello di trasporto per consegnare segmenti di informazioni.

Il **TCP** o transmission control protocol stabilisce una connessione logica tra i punti finali della rete. Sincronizza e regola il traffico con un meccanismo noto come "Three Way Handshake". Nel "Three Way Handshake" il sistema sorgente invia un pacchetto iniziale noto come SYN al sistema destinatario. Il sistema destinatario invia un pacchetto di conferma detto SYN/ACK (acknowledge). Infine il dispositivo sorgente invia un pacchetto chiamato ACK, che è una conferma della conferma. A questo punto, entrambi i dispositivi sorgente e destinatario hanno stabilito che esiste una connessione tra loro, ed entrambi sono pronti a inviare e ricevere dati.

UDP o user datagram protocol è un protocollo di trasporto non basato su una connessione. In questo caso il sistema sorgente invia i pacchetti senza avvisare il destinatario del loro invio. E' quindi delegata al dispositivo destinatario l'accettazione o meno dei pacchetti.

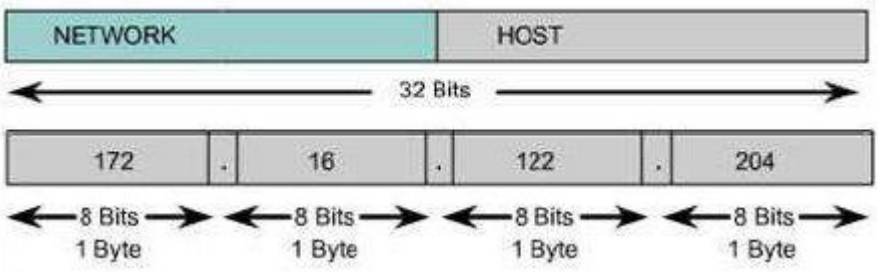
Di conseguenza, UDP è più veloce di TCP, ma non può garantire che un pacchetto sarà accettato.

3.3.3.3 Protocolli del livello Internet

IP o Internet Protocol è un protocollo universale che consente a due computer di comunicare attraverso qualunque rete in qualunque momento. Come UDP, è senza connessione, poichè non stabilisce una connessione con il computer remoto. Al contrario è ciò che si può definire il miglior servizio possibile, nel senso che fa tutto il possibile per assicurare il corretto funzionamento, ma non garantisce l'affidabilità. Il protocollo Internet determina il formato delle intestazioni dei pacchetti, incluso l'indirizzo IP dei sistemi sorgente e destinazione.

3.3.4 Indirizzi IP

Gli indirizzi IP sono gli identificatori utilizzati per distinguere i dispositivi che sono connessi ad una rete. Ogni dispositivo deve avere un indirizzo IP differente, così non ci sono problemi di errata identificazione all'interno della rete. Un indirizzo IP consiste in 32 bit divisi in 4 ottetti separati da punti. Parte dell'indirizzo IP identifica la rete e il resto dell'indirizzo IP identifica il singolo computer all'interno della rete.



Esistono sia indirizzi IP privati che pubblici. Gli indirizzi IP privati sono usati da reti private che non hanno connessioni con le reti esterne. Gli indirizzi IP all'interno di una rete privata non devono essere duplicati, mentre computer presenti su due reti private diverse – ma non connesse – possono avere IP duplicati. Gli indirizzi IP che sono stati definiti dalla IANA, Internet Assigned Numbers Authority, come disponibili per reti private sono:

da 10.0.0.0 fino a 10.255.255.255

da 172.16.0.0 fino a 172.31.255.255

da 192.168.0.0. fino a 192.168.255.255

Gli indirizzi IP sono suddivisi in classi in base alla porzione dell'indirizzo che viene utilizzata per identificare la rete e a quella utilizzata per identificare il singolo computer.

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

A seconda della dimensione assegnata ad ogni parte, possono essere definiti più dispositivi all'interno della rete o possono essere definite più reti. Le classi esistenti sono:

- **Classe A**: il primo bit è sempre zero, di conseguenza la classe comprende gli indirizzi compresi tra 0.0.0.0 e 126.255.255.255. Nota: gli indirizzi del tipo 127.x.x.x sono riservati per i servizi di loopback o localhost.

- **Classe B**: i primi due bit del primo ottetto sono '10', di conseguenza la classe comprende gli indirizzi compresi tra 128.0.0.0 e 191.255.255.255.

- **Classe C**: i primi tre bit del primo ottetto sono '110', di conseguenza la classe comprende gli indirizzi compresi tra 192.0.0.0 e 223.255.255.255

- **Classe D**: i primi 4 bit del primo ottetto sono '1110', di conseguenza questa classe comprende gli indirizzi compresi tra 224.0.0.0 e 239.255.255.255. Questi indirizzi sono riservati per implementazioni di multicast di gruppo.

- Gli indirizzi restanti sono usati per sperimentazioni o per usi futuri.

E' necessario un meccanismo per distinguere tra la parte dell'indirizzo usata per identificare la rete e la parte usata per identificare il singolo dispositivo. Per questo viene usata una maschera di bit. Nella maschera la parte costituita da bit '1' rappresenta la parte contenente l'identificativo della rete e quella costituita da '0' la parte che identifica il singolo dispositivo. Quindi per identificare un dispositivo oltre all'indirizzo IP è necessario specificare una maschera di rete (network mask):

IP: 172.16.1.20
Mask: 255.255.255.0

Gli indirizzi IP 127.x.x.x sono riservati per essere usati come loopback o indirizzi del sistema locale, essi cioè si riferiscono direttamente al computer locale. Ogni computer ha un indirizzo locale 127.0.0.1, quindi quell'indirizzo non può essere usato per identificare dispositivi diversi. Ci sono anche altri indirizzi che non possono essere usati. Questi sono l'indirizzo di rete (network address) e quello di broadcast.

L'indirizzo di rete è un indirizzo in cui la parte che normalmente identifica il dispositivo è tutti zero. Questo indirizzo non può essere usato, perchè identifica una rete e non può mai essere usato per identificare un dispositivo specifico.

IP: 172.16.1.0
Mask: 255.255.255.0

L'indirizzo di broadcast è un indirizzo in cui la parte dell'indirizzo che normalmente identifica il dispositivo è tutto 1. Questo indirizzo non può essere usato per identificare un dispositivo specifico, perchè è usato per inviare informazioni a tutti i computer che appartengono ad una rete specifica.

IP: 172.16.1.255
Mask: 255.255.255.0

3.3.5 Porte

Sia TCP che UDP utilizzano porte per scambiare informazioni con applicazioni. Una porta è un'estensione di un indirizzo, esattamente come quando si aggiunge il numero di un appartamento ad un indirizzo. Una lettera con un indirizzo arriverà all'edificio corretto, ma senza il numero dell'appartamento non verrà consegnata al destinatario corretto. Le porte lavorano in modo simile. Un pacchetto può essere consegnato all'indirizzo IP corretto, ma senza la porta associata non vi è modo di determinare quale applicazione dovrebbe agire sul pacchetto.

Una volta definite le porte i tipi diversi di informazioni inviate ad un indirizzo IP possono essere inviate all'applicazione appropriata. Utilizzando le porte un servizio in esecuzione su un computer remoto può determinare che tipo di informazione sia richiesta dal client locale, può determinare il protocollo richiesto per inviare quell'informazione e mantenere comunicazioni simultaneee con un numero di client diversi.

Ad esempio, se un computer locale cercasse di connettersi al sito web www.osstmm.org, il cui indirizzo IP è 62.80.122.203, con un server web in esecuzione sulla porta 80, il computer locale si connetterebbe a quello remoto utilizzando l'indirizzo (socket address):

62.80.122.203:80

Per mantenere un livello di standardizzazione tra le porte più comunemente usate, la IANA ha stabilito che le porte numerate da 0 a 1024 sono usate per servizi comuni. Le porte rimanenti -fino a 65535 – sono usate per allocazioni dinamiche o servizi particolari. Le porte più comunemente utilizzate – come assegnate da IANA – sono elencate nella tabella seguente.

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

Port Assignments		
Decimals	**Keywords**	**Description**
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
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

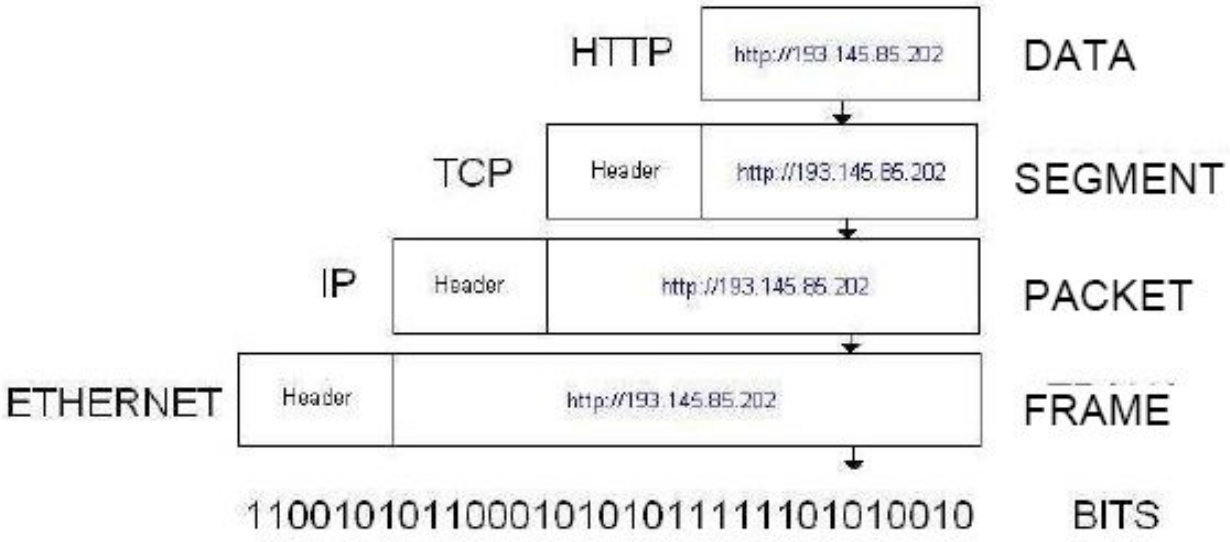
Per ulteriori dettagli sulle porte si veda la pagina web:

http://www.isecom.info/cgilocal/protocoldb/browse.dsp

3.3.6 Incapsulamento

Quando un'informazione – un messaggio e-mail ad esempio – viene inviato da un computer ad un altro, è soggetto ad una serie di trasformazioni. Il livello applicazione genera i dati che vengono inviati al livello di trasporto. Il livello di trasporto prende queste informazioni e vi aggiunge un'intestazione. L'intestazione consiste in informazioni quali l'indirizzo IP dei computer sorgente e destinatario, che specifica cosa debba essere fatto ai dati per inviarli alla corretta destinazione. Il livello successivo aggiunge un'altra intestazione e così via. Questa procedura ricorsiva è nota come incapsulamento.

Ogni livello dopo il primo incapsula i dati del livello precedente fino a che si arriva al livello finale in cui viene effettuata la reale trasmissione dei dati. La figura seguente mostra in forma grafica l'incapsulamento:



Quando l'informazione incapsulata giunge alla sua destinazione deve essere deincapsulata. Come ogni livello riceve informazioni da quello precedente, questo rimuove le informazioni non necessarie contenute nell'intestazione costruita dal livello precedente.

3.4. Esercizi

Esercizio 1: Netstat

Netstat

Il comando Netstat consente di vedere lo stato delle porte su un computer. Per eseguirlo dovete aprire una finestra MS-DOS e digitare:

netstat

Nella finestra MS-DOS veranno elenate le connessioni stabilite. Se volete vedere le connessioni in forma numerica:

netstat - n

Per visualizzare le connessioni e le porte attive:

netstat - an

Per visualizzare una lista di altre opzioni:

netstat - h

Nell'output di Netstat la seconda e terza colonna visualizzano l'indirizzo IP locale e remoto utilizzato dalle porte attive. Perchè gli indirizzi delle porte remote sono diversi da quelli locali?

Successivamente, utilizzando un browser web, aprite questa pagina web:

http://193.145.85.202

poi ritornate al prompt MS-DOS ed eseguite Netstat nuovamente. Quale connessione (o connessioni) nuova compare?

Aprite un altro browser e andate a questa pagina web:

http://193.145.85.203

Ritornate al prompt MS-DOS ed eseguite Netstat:

- perchè il protocollo HTTP appare in varie linee?
- che differenza c'è tra ognuna di esse?
- se ci sono più browser web attivi, come può il computer sapere che informazione va ad ognuno?

Esercizio 2: Porte e protocolli

In questa lezione avete imparato che le porte sono usate per distinguere i servizi. Perchè quando viene usato un browser web non è specificata nessuna porta?

Che protocolli sono usati?

E' possibile che un protocollo sia usato in più di un'istanza?

Esercizio 3: Il mio primo server

Per eseguire questo esercizio, dovete avere il programma Netcat. Se non lo avete potete effettuarne il download dalla pagina:
http://www.atstake.com/research/tools/network_utilities/
Una volta installato Netcat, aprite una finestra MS-DOS. Posizionatevi sulla directory Netcat e digitate:
nc - h
Questo visualizza le opzioni disponibili in Netcat. Per creare un semplice server digitate:
nc - l - p 1234
Quando viene eseguito questo comando, la porta 1234 viene aperta e sono consentite nuove connessioni . Aprite una seconda finestra MS-DOS e digitate:
netstat – a
Questo dovrebbe verificare che ci sia un nuovo servizio in ascolto sulla porta 1234. Chiudete la finestra MSDOS.
Per essere in grado di affermare che un server sia stato implementato, dovete stabilire un'associazione con un client. Aprite una finestra MS-DOS e digitate:
nc localhost 1234
Con questo comando, viene stabilita una connessione con il server che è in ascolto sulla porta 1234. Ora qualunque cosa venga scritta in qualunque delle due finestre MS-DOS può essere vista sull'altra finestra.
Create un file chiamato 'test', che contiene il testo, "Benvenuti sul server della Hacker Highschool!". In una finestra MS-DOS digitate:
nc - l - p 1234 > test
Da un'altra finestra MS-DOS connettetevi al server digitando:
nc localhost 1234
Quando il client si connette al server, dovreste vedere l'output del file 'test'.
Per chiudere il servizio, andate nella finestra MS-DOS in cui è in esecuzione e digitate *CTRL-C*.
Che protocollo è stato usato per la connessione al server?
Netcat vi consente di fare ciò? Se sì come?

Approfondimenti

Potete trovare ulteriori informazioni sulle porte e sui protocolli esaminando i seguenti 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

Riferimenti sui numeri di porta:

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

http://www.isecom.info/cgi-local/protocoldb/browse.dsp

Glossario

Topologia: struttura dei collegamenti tra i dispositivi che formano una rete

TCP/IP: standard aperto utilizzabile da chiunque per connettere i computer tra loro e scambiare informazioni tra loro. E' il protocollo di base di Internet.

Protocollo: regole comuni per lo scambio di informazioni tra due livelli paritetici.

Indirizzi IP: identificatori utilizzati per distinguere i dispositivi che sono connessi ad una rete.

Classi di indirizzi: classificazione degli indirizzi IP in base alla porzione dell'indirizzo che viene utilizzata per identificare la rete e a quella utilizzata per identificare il singolo computer.

Porta: estensione di un indirizzo che consente di determinare quale applicazione deve agire sul pacchetto.