Hacker Highschool

SECURITY AWARENESS FOR TEENS



LEZIONE 3
SOTTO L'INTERNET

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

ATTENZIONE

Il progetto Hacker Highschool è uno strumento di apprendimento e come tutti gli strumenti di apprendimento non è esente da pericoli. Alcune lezioni, se usate in modo improprio, possono causare danni fisici. Eventuali pericoli possono emergere anche in caso non si sia svolta una sufficiente ricerca in merito agli effetti di particolari tecnologie. Gli studenti che usano queste lezioni dovrebbero essere incoraggiati ad imparare, provare e testare. Ad ogni buon conto ISECOM non potrà essere ritenuto responsabile per un uso improprio di quanto esposto.

Le seguenti lezioni ed esercizi sono “open” e disponibili pubblicamente alle seguenti condizioni e termini stabiliti da ISECOM:

Tutti i contenuti del progetto Hacker Highschool vengono forniti per uso non-commerciale per gli studenti delle scuole elementari, scuole medie inferiori e scuole medie superiori sia per le istituzioni pubbliche che per quelle private, ammettendone l'uso per le esercitazioni a casa. Non è ammessa la riproduzione del materiale per la vendita. L'utilizzo del materiale presente in queste lezioni è consentito per i corsi di ogni tipo che prevedono il pagamento di una tassa/quota d'iscrizione o frequenza, previa acquisizione di regolare licenza. Sono soggetti a tale norma anche i corsi presso le università, campi estivi e tutto quanto sia inteso come formazione. Per acquistare una licenza è possibile visitare la sezione LICENSE della pagina web della HHS all'indirizzo web: http://www.hackerhighschool.org/licensing.html.

Il progetto Hacker Highschool rappresenta lo sforzo di una comunità “open.” Pertanto se trovi utile questo materiale vi inviatiamo a supportarci tramite l'acquisto di una licenza, attraverso una donazione o una sponsorizzazione.

Indice

Hanno contribuito

Marta Barceló, ISECOM
Pete Herzog, ISECOM
Glenn Norman, ISECOM
Chuck Truett, ISECOM
Bob Monroe, ISECOM
Kim Truett, ISECOM
Gary Axten, ISECOM
Marco Ivaldi, ISECOM
Simone Onofri, ISECOM
Greg Playle, ISECOM
Tom Thomas, ISECOM
Mario Platt
Ryan Oberto, Johannesburg South Africa

Traduttori italiani

Raoul Chiesa, ISECOM (Coordinatore Team di lavoro edizione italiana)
Matteo Benedetti, Security Brokers SCpA
Ing. Selene Giupponi, Security Brokers SCpA
Francesco Mininni, Ing. PhD., Uff. E.I.
Riccardo Trifonio, Mar.Ca. CC

Introduzione e Obiettivi

Nelle lontane profondità del passato, prima che esistesse un'internet, la comunicazione elettronica era pura materia esoterica. Ogni produttore di computer aveva la propria idea di come i computer dovessero comunicare attraverso un filo. E nessuno considerava neppure la possibilità che un computer Wang potesse comunicare con un computer Burroughs.

Il mondo è cambiato quando gli scienziati e gli studenti hanno sperimentato la gioia di utilizzare un terminale per accedere a un mainframe. Il famoso PC IBM arrivò e i primi possessori iniziarono a voler accedere a quel mainframe dal loro personal computer. Ben presto i modem iniziarono a realizzare connessioni dial-up e gli utenti a lavorare in emulatori di terminale. Il mondo della connettività si era guadagnato la fama di essere come la magia nera e gli addetti ai lavori vennero chiamati (realmente) **guru**.

Il mondo cambiò di nuovo drasticamente quando Internet, che nacque come un progetto militare, venne resa disponibile al grande pubblico. Le connessioni di rete erano sempre state locali, il che significa limitate ad un ufficio o al massimo un campus. Come avrebbero potuto parlarsi fra loro tutti questi sistemi differenti?

La risposta fu quella di “inserire” un sistema di indirizzamento universale sulle reti esistenti, un sistema che noi generalmente chiamiamo **Internet Protocol (IP)**. Raffiguralo in questa maniera: immagina che un tuo amico d'oltreoceano ti mandi un pacco. Quel pacco può viaggiare con l'aereo, il treno o l'automobile ma tu non hai bisogno di sapere l'orario dell'areo o la posizione della stazione più vicina. Il tuo pacco arriverà alla fine all'indirizzo della tua strada che è solamente l'ultima cosa che interessa. Il tuo **indirizzo IP** è proprio così: i pacchetti possono viaggiare come elettroni, segnali di luce o onde radio, ma questi sistemi non ti interessano. L'importante è il tuo indirizzo IP e l'indirizzo IP del sistema con cui stai parlando

Una cosa che, nel mondo reale, complica questo concetto è che più di una persona può vivere ad un singolo indirizzo. Nel mondo delle reti questo accade quando un server fornisce, per esempio, sia un normale servizio HTTP che un servizio sicuro HTTPS sicuro che un servizio FTP. Vedi la P alla fine o verso la fine di questi acronimi? Quelle sono sempre le abbreviazioni per **protocol,** che è un altro modo per dire “un tipo di comunicazione.”

Questa lezione ti aiuterà a capire come I protocolli e le loro porte lavorano in Windows, Linux, e OSX. Prenderai confidenza con diverse utilities (alcune delle quali sono già state introdotte nella lezione precedente) che esplorano le capacità dei tuoi sistemi di rete.

Al termine della lezione avrai una conoscenza di base relativa a:

- i concetti delle reti e come avviene la comunicazione
- gli indirizzi IP
- le porte e i protocolli

Concetti di base sulle Reti

Il punto di partenza per le reti è la rete locale (**LAN** - local area network). Le LAN permettono ai computer di condividere risorse, come stampanti e spazio disco, e agli **amministratori** di controllare quello che accede, il tutto in uno spazio fisico comune. Le sezioni seguenti descrivono i comuni dispositivi di rete e le topologie.

Dispositivi

Proseguendo nella tua carriera di hacker, avrai modo di vedere una gran quantità di diagrammi di rete. È utile riconoscere I simboli più comuni:

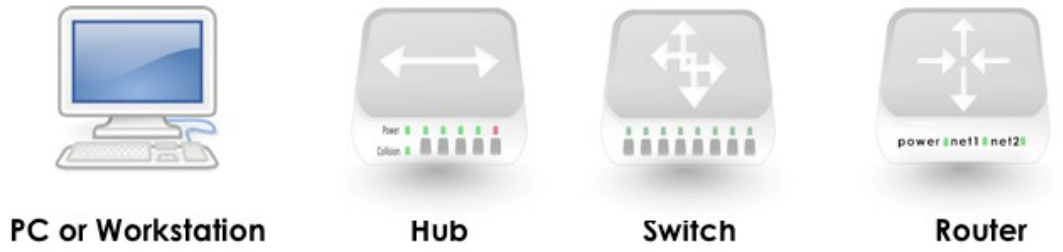


Figure 3.1: Simbologia comune di rete

Un **hub** è come un vecchio centralino: tutti sono sul medesimo filo e possono ascoltare le conversazioni degli altri. Questo può rendere una LAN “rumorosa ma veloce.”

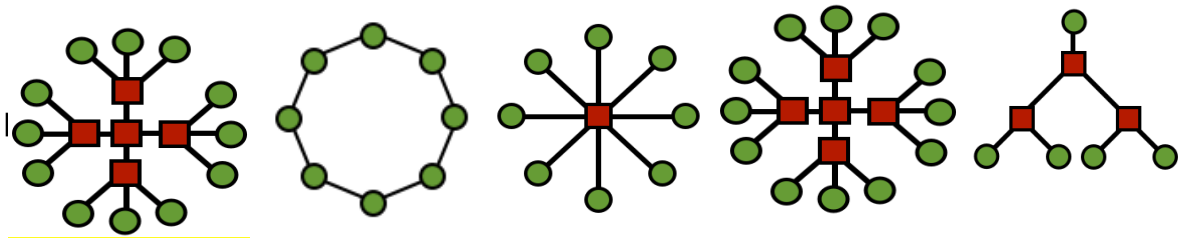
Uno **switch** è migliore: filtra il traffico così che solo i due computer che parlano fra di loro possono ascoltare la conversazione. Ma come un hub, si usa solo su una LAN.

Un **router** si posiziona fra LAN; viene usato per accedere ad altre reti e sull'internet ed inoltre usa indirizzi IP. Controlla i pacchetti che vengono mandati e decide a quale rete appartengono questi pacchetti. Se il pacchetto appartiene all'”altra” rete, indirizza il pacchetto dove deve andare, come farebbe un vigile.

Topologie

Una **topologia** è un'altra maniera di dire “la maniera in cui lo connettiamo.” Il tipo di decisioni che prendiamo a riguardo della nostra topologia può influire positivamente o negativamente sul futuro, a seconda delle tecnologie che vengono usate, dei vincoli tecnologici e fisici, dei requisiti di performance e sicurezza, della grandezza e della natura dell'organizzazione, etc.

La struttura fisica di una LAN può avere l'aspetto di una qualunque delle seguenti topologie fisiche:



Bus **Anello** **Stella** **Stella estesa** **Gerarchica**

Figure 3.2: Topologie

In una topologia a **bus**, tutti I computer sono connessi ad un singolo cavo e ogni computer può comunicare direttamente con uno qualunque degli altri. Ma la rottura di una qualsiasi parte del bus comporta l'esclusione di tutti dalla rete.

Nella configurazione ad **anello**, ciascun computer è connesso con il seguente e l'ultimo con il primo e ogni computer può comunicare direttamente con I due adiacenti.

Le topologie a bus sono raramente usate oggigiorno. Le tecnologie a ring sono spesso usate al livello interstatale, solitamente con due anelli controrotanti che inviano il traffico in direzioni opposte per garantire affidabilità e resistenza al guasti.

Nella topologia a **stella**, nessuno dei computer è direttamente connesso con gli altri, invece essi sono connessi attraverso un hub o uno switch che rilancia le informazioni da un computer all'altro.

Se diversi hub o switch sono connessi uno all'altro, si può ottenere una topologia a **stella estesa**.

In una topologia a stella o a stella estesa, tutti I punti centrali sono detti **peer**, che significa che sono essenzialmente uguali. Questa è la topologia LAN più comune oggigiorno.

Comunque, se connetti insieme due reti a stella o stella estesa usando un punto centrale che controlla o limita il traffico fra le due reti, allora avrai una topologia di rete **gerarchica**. Questa è la topologia solitamente sviluppata nelle imprese più estese.

Inizia il Gioco: Lasciare la Back Door Aperta

Nel calore del sole rovente dell'estate, Jace era felice di aiutare il dipartimento locale di polizia, dotato di aria condizionata, per sistemare la loro piccola rete. Già un bel pò prima del gran caldo, l'avevano ricompensata con biscotti, conversazione e l'opportunità di installare una backdoor. Strisciando sotto scrivanie di acciaio che non erano state spostate per decenni, Jace aveva trovato il punto più sporco dove nascondere un access-point WiFi. Lo aveva appena collegato e coperto di spazzatura e stava stendendo un rotolo di cavo Ethernet verso la borchia che aveva installato in precedenza.

Una mano pesante colpì la scrivania sopra di lei. Jace colpì il metallo e urlò"Ahi! La mia testa" poi aggiunse "sei sicuro che non vuoi che ti sistemi il server?"

Il poliziotto si schiarì la gola e cercò di assumere il tono di voce del tipico professore allampanato"Beh lo farei io, ma non sono sicuro di come la resistenza di flusso dei raggi potrebbe reggere fino all'alimentazione dei micro-canali-incrociati. Soprattutto quando la luna piena cade l'ultimo Martedì del mese."

Jace sbatteva i piedi fingendo l'irritazione di una adolescente."A quanto pare non avete problemi a raggiungere livelli quantici di sciocchezze. E quando posso avere i miei biscotti, agente Kickam?"

"Jace per piacere, chiamami Hank. Mi fai sentire vecchio quando mi chiami agente Kickam""

Lui cercò di sembrare ferito ma lei, mentre lo ascoltava, conosceva già l'ingegneria sociale. Stava veramente tentando di distrarla dai biscotti.

"Hank, mi dispiace darti la notizia, ma tu sei vecchio."

"Ahi, che dolore. Io non sono vecchio, io sono maturo", ribattè, confrontando le sue lucidissime scarpe nere da poliziotto con le Sneaker a brandelli di Jace che scomparve sotto la pesante scrivania. Poi emersero occhi castani color cannella e un viso coperto di ragnatele. Jace aveva ancora una bobina di cavo sotto un braccio. Hank l'aiutò ad alzarsi e le tolse le ragnatele dal viso e dalle spalle.

"Aiuto, la brutalità della polizia," disse Jace prendendolo in giro.

"Criminale pericoloso" rispose Hank"Dai, spiegami qual è il tuo piano diabolico", chiese l' uomo di legge peloso e muscoloso, con quello che sembrò a Jace come un tono supplichevole.

Quella sembrava una bella cosa, così lei chiese: "Sei sicuro che vuoi sapere qualcosa su questa roba di rete?" Lui annuì con entusiasmo. Jace pensò: “lecchino.”

"Va bene, quello che ho fatto è stato progettare una topografia di rete, come una mappa che mostri dove saranno posizionate tutte le attrezzature, i computer, gli hub, i jack, gli switch, i router e il firewall. Non è possibile avviare un progetto come questo senza una mappa,"disse, alzando lo sguardo verso il poliziotto."Tutto è fatto in modo che ogni nodo possa comunicare con ogni altro nodo, senza punti di interruzione. Così, per esempio, una architettura a bus non va bene perchè se uno dei nodi cade tutti fanno la stessa fine."Hank annuì così Jace continuò.

"Pensa come la rete sia questo negozio di polizia, ops, stazione di polizia, e qualcuno abbia appena portato un sospettato. Ogni poliziotto ha diritto al proprio bel turno per picchiare il ragazzo senza sottrarre tempo a qualcun'altro. Se la vittima, voglio dire sospettato, viene spostato in un'altra cella, tutti i poliziotti che hanno ancora bisogno di picchiare il tizio devono sapere dove sia andato."

"Oh Jace, sembra che anche tu abbia bisogno di qualche buona bastonata se continui a parlare così di noi ufficiali di pace." Hank sollevò il cinturone con la fondina e tirò in dentro la pancia.

Jace scoppiò in una risata."Quindi il sospettato è un pacchetto di dati e voi poliziotti violenti siete i dispositivi di rete. E ogni dispositivo, uno switch, un router, un firewall, un altro server o qualsiasi altra cosa, ha bisogno di sapere come il pacchetto di dati viene trattato. Tipo, essere colpito con i manganelli della polizia. Penso che tu chiameresti questa cosa, fare a qualcuno uno shampoo di legno."

Hank alzò gli occhi e cercò il manganello ma non lo aveva con sè.

Ridacchiando, Jace alzò la bobina di cavo come uno scudo."Hey, ho un rotolo di cavo e non ho paura di usarlo. Metti giù la tazza di caffè e nessuno si farà male."Perdendo l'equilibrio e ridendo, Jace si lasciò cadere su Hank, che non si mosse. Wow, questo ragazzo è veramente una roccia, non potè fare a meno di pensare. La mano che lui le posò sulla spalla le ricordava ... qualcosa.

Si alzò un pò troppo in fretta, arrossendo."Quindi ci sono due tipi di dispositivi. Dispositivi intelligenti e quelli stupidi. Proprio come poliziotti." Quattro uomini in divisa che si avvicinavano, apparvero esattamente nel momento sbagliato per sentire" gli stupidi, proprio come i poliziotti."Esitando Jace continuò," I dispositivi intelligenti ricordano tutto quello che fanno. Tengono i registri delle loro attività."

"E quelli stupidi? Come i poliziotti?" chiese il Capo della Polizia.

Game Over

Il Modello TCP/IP (DoD)

TCP/IP fu sviluppato dal **DoD (Department of Defense)** degli Stati Uniti e dal **DARPA (Defense Advanced Research Project Agency)** negli anni '70. TCP/IP fu creato per essere uno standard aperto che chiunque potesse usare per connettere insieme computer e scambiare informazioni fra di essi. Ultimamente è diventato la base per l'Internet.

Generalmente la più semplice forma del modello TCP/IP è chiamata il **Modello DoD** ed è quello da dove inizieremo.

Livelli

Il semplice modello DoD definisce 4 livelli totalmente indipendenti, fra i quali si divide il processo di comunicazione fra due dispositivi. I livelli attraverso cui passa l'informazione sono:

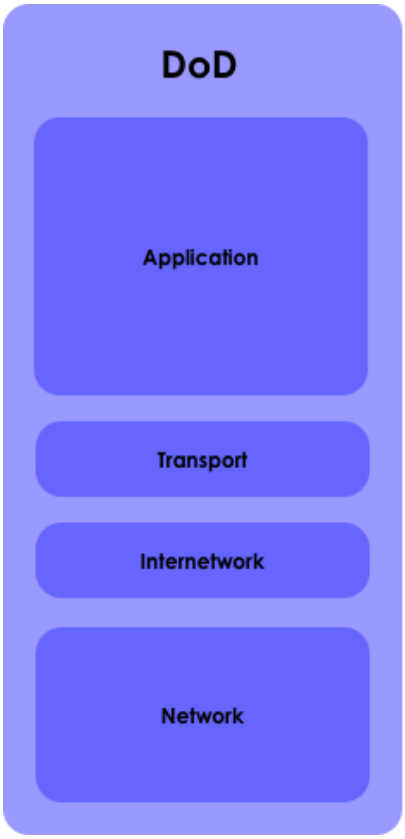


Figure 3.3: Il Modello DoD

Applicazione

Il livello applicazione è esattamente quello che probabilmente pensi che sia: il livello dove lavorano le applicazioni come Firefox, Opera, i client di posta elettronica, i siti di social network, la messaggistica istantanea e le applicazioni chat di lavoro. Sono veramente tante le applicazioni che accedono all'internet: alcune applicazioni per l'ufficio, per esempio, si connettono a raccolte online di clip art. Il livello applicazione crea il payload (contenuto) che tutti gli altri livelli trasportano. Una buona analogia è un sistema postale. L'applicazione crea il pacchetto che viene avvolto con le istruzioni su come il pacchetto dovrebbe essere usato. Poi porta il package alla stanza della posta: il Livello di Trasporto.

Trasporto

Il livello trasporto imposta le connessioni di rete che, nel mondo dell'internet, sono chiamate **sessioni.** Il protocollo principale nel livello trasporto è il **TCP (Transmission Control Protocol).** Il TCP aggiunge un altro strato all'esterno del pacchetto, con le istruzioni su quale pacchetto esso sia (ad esempio, 1 di 3), su come essere sicuri che il pacchetto giunga a destinazione e se il pacchetto sia integro.

Supponiamo che tu stia mandando via email una lettera a tua mamma. La lettera può essere leggera o pesante, ma è troppo grande per essere inviata attraverso l'internet in un unico pezzo, TCP divide quella lettera in **segmenti**, piccoli pezzi che sono numerati consecutivamente con un piccolo bit di codice di controllo di errore alla fine. Se un pacchetto si corrompe durante il transito, TCP richiede una ritrasmissione. Alla fine della ricezione, TCP rimette insieme I pezzi nell'ordine corretto e tua mamma riceverà la lettera nella sua email.

Ma non dimenticare che TCP non è l'unica alternativa possibile: anche l'**UDP** funziona a questo livello e in particolare NON crea sessioni. Invia soltanto un flusso di **datagrammi**, che sono simili ai segmenti ma l'UDP non controlla mai se tu li hai ricevuti.

A questo livello tutto il traffico, sia TCP che UDP, è assegnato a specifici **numeri di porta**.

Internetwork

Questo livello aggiunge informazioni circa gli indirizzi di origine e di destinazione e dove il **pacchetto** inizia e finisce. É come una compagnia di spedizioni che consegna I pacchi all'indirizzo corretto. Non è importante se ci sono tutti I pacchetti che lo compongono o se sono intatti; quello è compito del livello Trasporto. Il più importante protocollo a questo livello è sicuramente l'**IP (Internet Protocol)**. E questo è il livello che usano gli indirizzi IP per far si che i pacchetti arrivino nel posto giusto e con il percorso migliore.

Accesso alla Rete

Questo è il più basso livello del network fisico che usi per connetterti all'internet. Se ti stai collegando componendo un numero di telefono ci dispiace ed evidentemente stai usando una semplice connessione **PPP.** Se hai una **DSL** allora starai usando **ATM** o **Metro Ethernet**. E se hai una connessione internet via cavo stai usando una rete fisica **DOCSIS**. Non importa quale tu usi perchè TCP/IP fa in modo che tutte lavorino insieme. Il livello di accesso alla rete è composto dal cavo Ethernet e dalla **scheda di rete (NIC - network interface card)**, o dalla scheda wireless e dall'access point. Questo gestisce al livello più basso gli uno e gli zero (ovvero i bit) perchè vadano da un punto all'altro.

Nutrite la vostra mente: Osserva “Il Modello OSI”

Osserva “Il Modello OSI” alla fine di questa lezione per un punto di vista alternativo sul modello di rete.

Protocolli

Finalmente ora sei connesso all'Internet. Questo sembra sufficientemente semplice ma considera la situazione reale in cui ti trovi: sei impegnato in una innocente ed importante ricerca sull'Internet, mentre il tuo caro fratello o sorella sta perdendo tempo guardando un film in streaming. Perchè questi due flussi di traffico non vengono mischiati? Come li distingue la rete?

La risposta è nei **protocolli,** che sono come dei linguaggi che parlano i differenti tipi di traffico. Il traffico Web usa un protocollo, I trasferimenti di file un altro e l'email un altro ancora. Come tutte le cose digitali I protocolli non usano nomi reali sul livello network; usano indirizzi IP e **numeri di porte**.

Protocolli del livello Applicazione

FTP o F*ile Transfer Protocol è usato per la* trasmissione di file fra due dispostivi. Usa una porta per inviare i dati e un'altra porta per mandare segnali di controllo (“Ho ricevuto il file! Grazie!”). Le porte più comunemente usate sono la 20 e la 21 (TCP).

HTTP o *Hyper-Text Transfer Protocol è usato per le pagine* web. Questo traffico solitamente usa la porta 80. **HTTPS** è una variante sicura che cifra il traffico di rete, solitamente su TCP porta 443.

SMTP o S*imple Mail Transfer Protocol è il* protocollo che invia le email. La sua porta TCP è la 25.

DNS o *Domain Name Service* è la maniera in cui un dominio del tipo ISECOM.org viene associato a un indirizzo IP come 216.92.116.13. Usa la porta 53 (UDP).

Protocolli di livello Trasporto

TCP e **UDP** sono i due protocolli principali usati dal livello trasporto per trasferire dati.

TCP o Transmission Control Protocol *stabilisce una connessione logica* (una **sessione**) fra due computer su una rete. Attiva questa connessione usando l'handshake a tre vie.

1.Quando il mio computer vuole collegarsi al tuo, manda un pacchetto **SYN**, che sta semplicemente dicendo “Sincronizziamo gli orologi così possiamo scambiare traffico con marcatori temporali.”

2.Il tuo computer (se accetterà la connessione) risponde con un pacchetto di riconoscimento **SYN/ACK**.

3.Il mio computer chiude la procedura con un pacchetto **ACK** e noi siamo connessi.

Ma questo accade solo con il TCP. L'**UDP (User Datagram Protocol)** invece è un protocollo di trasporto che non si cura se hai una connessione. É come una manichetta antincendio: se prendi il flusso lo prendi, altrimenti niente. Questo rende l'UDP molto veloce, così è utile per molte cose come lo streaming vocale e video, nel quale perdere un singolo pacchetto non importa granchè o nei giochi online, dove perdere un singolo frame non importa (dipende da che parte della pallottola stai).

Protocolli del livello Internet

IP o Internet Protocol serve come un protocollo universale per permettere a due computer qualunque di comunicare attraverso una qualunque rete in qualunque momento. É come il corriere postale che consegna la posta; tutto quello che fa è portare I pacchetti al loro indirizzo di destinazione.

Internet Control and Management Protocol (ICMP)

ICMP è il protocollo che I dispositivi di rete e gli amministratori di rete usano per risolvere I problemi e manutenere la rete. Include cose come il **ping** (Packet InterNet Groper) e comandi similari che testano la rete e riferiscono gli errori. Poiché qualcuno ha usato cose come ping floods per far cadere computer e reti, molti sistemi limitano l'ICMP ad una risposta per secondo.

Per riassumere, porte e protocolli si fondono in questo modo:

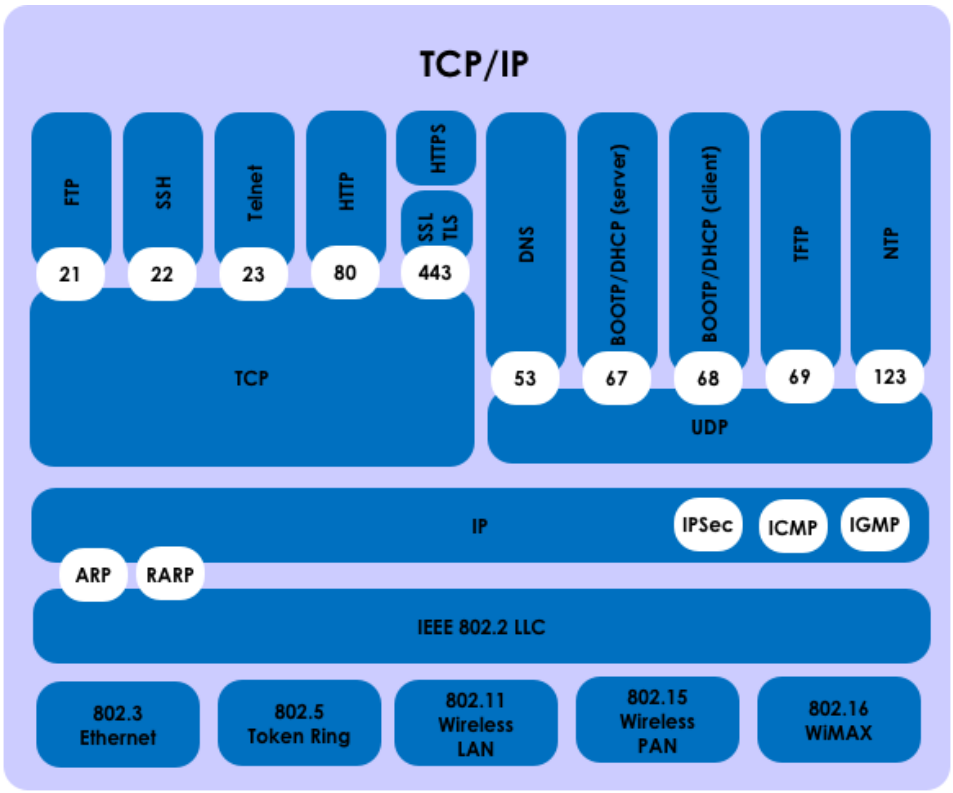


Figure 3.4: Lo stack TCP/IP

Indirizzi IPv4

I nomi a dominio sono fatti apposta per gli umani, perché siamo capaci di ricordare nomi come ISECOM.org. Ma le reti non li capiscono affatto; queste capiscono solo indirizzi IP numerici. Così quando tu chiedi di accedere a ISECOM.org, il tuo computer fa una veloce ricerca usando il **DNS (Domain Name Service)** per trovare il corrispondente indirizzo IP.

Gli indirizzi IP sono come gli indirizzi stradali. Se tu vuoi ricevere la posta devi averne uno. L'indirizzo **IPv4** consiste di 32 bit che sono dividi in 4 **otteti** da 8-bit, separati da punti. Questo significa che ci sono 2^{32} (o 4,294,967,296) indirizzi unici sull'internet, sotto IPv4. Parte dell'indirizzo IP identifica la rete e il rimanente dell'indirizzo IP identifica il singolo computer sulla rete. Pensa a queste parti come alla porzione di indirizzo relativa alla nazione/città (network)e alla porzione di indirizzo della via (host).

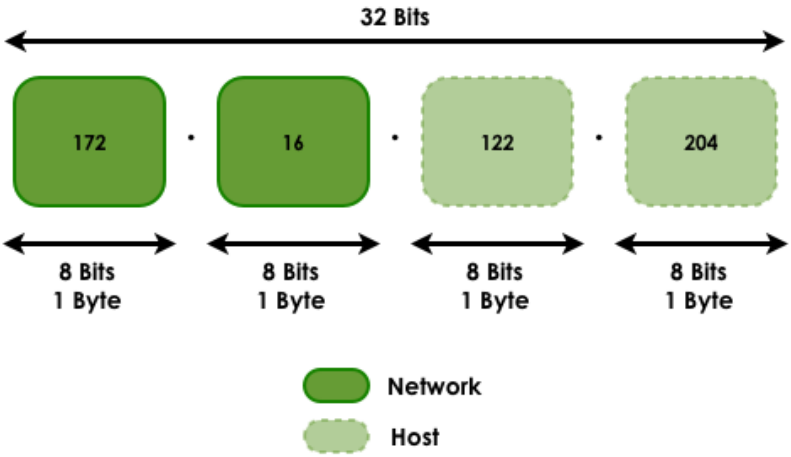


Figure 3.5: Numeri di rete e ID computer

Ritornando all'analogia del servizio postale: IP è il camion delle consegne che porta il pacchetto all'ufficio postale corretto TCP è il rivestimento esterno con la lista di quanti pacchetti vi siano in una spedizione e quale di questi esso sia (ad esempio il numero 3 di 65). Gli indirizzi di livello-host sono l'abitazione precisa (il computer) alla quale il pacchetto è destinato.

Ci sono **indirizzi IP** pubblici e **privati (non routabili)**. Gli indirizzi privati sono usati da per reti private; i router non permettono l'accesso di questi indirizzi all'internet.

Gli indirizzi IP presenti all'interno di una rete privata non dovrebbero essere duplicati all'interno di quella rete, ma computer su due reti private differenti – ma non interconnesse – possono avere gli stessi indirizzi IP. Gli indirizzi IP che sono stati definiti dalla IANA, l'Autorità per l'Assegnazione dei Numeri Internet, per essere usati per le reti private (vedi la RFC 1918) sono:

10.0.0.0 fino a 10.255.255.255	(Classe A)
172.16.0.0 fino a 172.31.255.255	(Classe B)
192.168.0.0. fino a 192.168.255.255	(Classe C)

Classi

Gli indirizzi IP sono divisi in classi basate su quale porzione dell'indirizzo è usata per identificare la rete e quale porzione è usata per identificare I singoli computer.

A seconda della dimensione assegnata ad ogni parte, ci saranno più dispositivi presenti all'interno della rete o più reti saranno ammesse. Le classi esistenti sono:

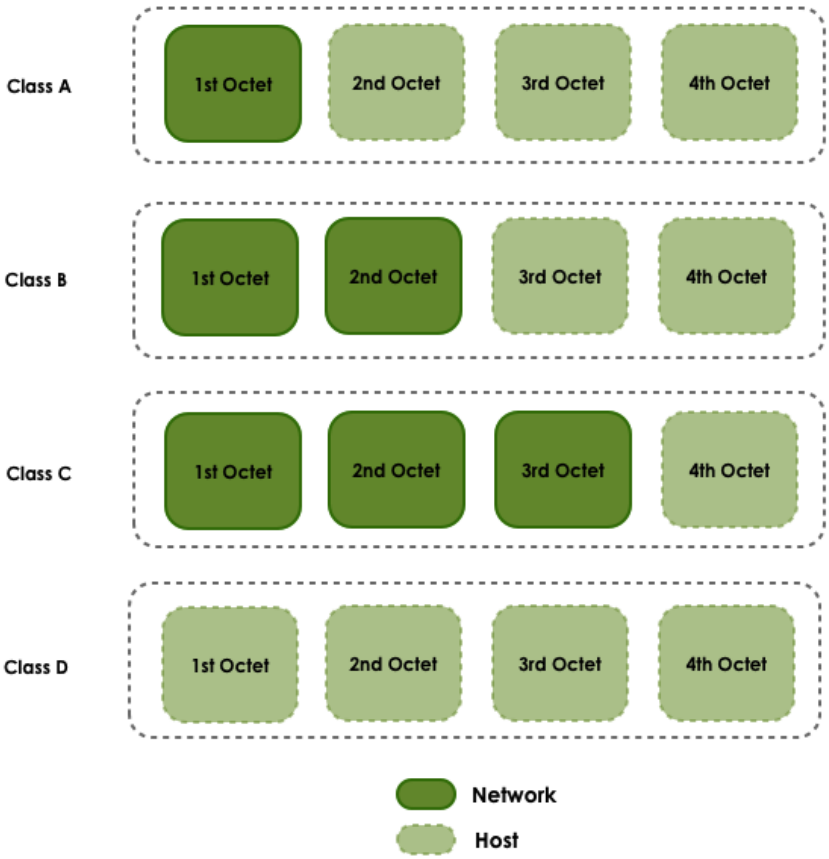


Figure 3.5: Divisioni per classi di IP

Classe A: Il primo bit è sempre zero, così questa classe include gli indirizzi fra 0.0.0.0 (che, per convenzione, non è mai usato) e 126.255.255.255. Attenzione: gli indirizzi di 127.x.x.x sono riservati per servizi di loopback o localhost (vedi sotto).

Classe B: I primi due bit del primo ottetto sono '10', così questa classe include gli indirizzi fra 128.0.0.0 e 191.255.255.255.

Classe C: I primi tre bit del primo ottetto sono '110', così questa classe include gli indirizzi tra 192.0.0.0 e 223.255.255.255.

Classe D: I primi quattro bit del primo ottetto sono '1110', così questa classe include gli indirizzi fra 224.0.0.0 e 239.255.255.255. Questi indirizzi sono riservati per implementazioni di gruppi multicast.

I rimanenti indirizzi sono usati per sperimentazioni o per possibili future allocazioni.

La **maschera (o maschera di rete)** è usata per marcare queste differenze di classe. Ragionando in binario, un bit '1' mostra la parte contenente l'identificativo di rete e un bit '0' rappresenta la parte che identifica il computer. Le maschere di rete di default per le prime tre classi sono:

255.0.0.0 (Classe A)

255.255.0.0 (Classe B)

255.255.255.0 (Classe C)

Questo è piuttosto semplice, poiché le reti che usano le classi di default maschereranno un ottetto se sono di Classe A, due ottetti per la Classe B e tre ottetti per la Classe C. L'uso delle classi di default è comodo – ma non tutti lo fanno.

Tutto questo significa che per identificare un computer, hai bisogno di un indirizzo IP e di una maschera di rete:

IP: 172.16.1.20
Maschera: 255.255.255.0

Indirizzi Loopback

Gli indirizzi IP da 127.0.0.1 fino a 127.255.255.254 sono riservati per essere usati come **loopback** o indirizzi locali, che significa che essi indirizzano la comunicazione nuovamente verso il computer locale. Ogni computer ha un indirizzo localhost 127.0.0.1, perciò quell'indirizzo non può essere usato per identificare altri computer.

Ci sono anche altri indirizzi che non possono essere usati. Questi sono gli **indirizzi di rete** e gli **indirizzi di broadcast**.

Indirizzi di rete

L'indirizzo di rete è fondamentalmente la parte rete di un indirizzo IP **con zeri dove dovrebbe essere la parte host**. Questo indirizzo non può essere dato ad un computer perché identifica l'intera rete, non un computer solo.

IP: 172.16.1.**0**
Maschera: 255.255.255.0

Indirizzi Broadcast

L'indirizzo broadcast è fondamentalmente la parte rete di un indirizzo IP, **con tanti uno dove dovrebbe essere la parte host**. Questo indirizzo non può essere usato per identificare uno specifico computer perché è l'indirizzo che ascoltano tutti I computer (logicamente quello è il significato di trasmettere: tutti ascoltano).

IP: 172.16.1.**255**
Maschera: 255.255.255.0

Porte

Sia TCP che UDP usano **porte** per scambiare informazioni con le applicazioni. Una porta è un'estensione di un indirizzo, come aggiungere un appartamento o numero di stanza a un indirizzo stradale. Una lettera con l'indirizzo della via arriverà all'edificio corretto ma senza il numero dell'appartamento non sarà inserita nella giusta cassetta.

Le porte operano nella medesima maniera. Un pacchetto può essere inviato all'indirizzo IP corretto ma senza la porta associata non c'è possibilità di determinare quale applicazione dovrebbe operare sul pacchetto. Anche un numero di porta è un numero a 16 bit che significa che può avere valori decimali fra 0 e 65535 (2 elevato alla 16).

Un altro sistema per capire questo concetto potrebbe essere: ogni computer è un ufficio postale. Ogni applicazione ha la sua casella postale; due applicazioni non devono condividere la stessa casella postale. Il numero di porta è il numero della cassetta postale.

I numeri di porta rendono possibile avere molti flussi di informazione operanti su un indirizzo IP, dove ciascun flusso è inviato all'applicazione appropriata. Il numero di porta permette a un servizio operante su un computer remoto di conoscere che genere di informazione sta richiedendo un client locale e quale protocollo è usato per inviare quelle informazioni, mantenendo tutti le comunicazioni simultanee con una quantità di client diversi.

Per esempio, se un computer locale tenta di connettersi al sito www.osstmm.org, il cui indirizzo IP è 62.80.122.203, con un webserver che opera sulla porta 80, il computer locale dovrebbe connettersi al computer remoto usando l'**indirizzo socket**:

62.80.122.203:80

Per assicurare un livello di standardizzazione fra le porte più comunemente usate, IANA ha stabilito che le porte dalla 0 alla 1024 sono usate per servizi comuni, **privilegiati** o **conosciuti.** Le porte rimanenti – fino a 65535 – sono usate per allocazioni dinamiche o servizi particolari.

Le porte più comunemente usate (ben-conosciute) – secondo l'assegnazione **IANA** – sono elencate qui:

Assegnazione delle porte		
Numero	**Parola chiave**	**Descrizione**
5	rje	Remote Job Entry - Voce lavoro remoto
0		Reserved - Riservato
1-4		Unassigned - Non assegnato
7	echo	Echo
9	discard	Discard - Scartare
11	systat	Active Users - Utenti attivi
13	daytime	Daytime - Ora del giorno
15	netstat	Who is Up or NETSTAT - Chi è up
17	qotd	Quote of the Day - Citazione del giorno
19	chargen	Character Generator - Generatore di caratteri
20	ftp-data	File Transfer [Default Data] - Dati di trasferimento di file
21	ftp	File Transfer [Control] - Controllo del trasferimento di file
22	ssh	SSH Remote Login Protocol - Protocollo di login remoto
23	telnet	Telnet
25	smtp	Simple Mail Transfer - Semplice trasferimento di posta
37	time	Time - Tempo
39	rlp	Resource Location Protocol - Location protocol risorsa
42	nameserver	Host Name Server - Nome host del server
43	nicname	Who Is - Chi è
53	domain	Domain Name Server - Server del nome di dominio
67	bootps	Bootstrap Protocol Server - Server del protocollo bootstrap
68	bootpc	Bootstrap Protocol Client - Client per il protocollo bootstrap
69	tftp	Trivial File Transfer – Banale trasferimento del file

Assegnazione delle porte		
Numero	**Parola chiave**	**Descrizione**
70	gopher	Gopher
75		any private dial out service - Qualsiasi servizio di chiamate in uscita privata
77		any private RJE service - Qualsiasi servizio privato RJE
79	finger	Finger
80	www-http	World Wide Web HTTP -
95	supdup	SUPDUP
101	hostname	NIC Host Name Server – NIC nome host del server
102	iso-tsap	ISO-TSAP Class 0
110	pop3	Post Office Protocol Version 3 - Post Office Protocol versione 3
113	auth	Authentication Service - Servizio di autenticazione
117	uucp-path	UUCP Path Service - UUCP Percorso Servizi
119	nntp	Network News Transfer Protocol - Protocollo di rete di trasferimento di notizie
123	ntp	Network Time Protocol - Protocollo del tempo di rete
137	netbios-ns	NETBIOS Name Service – NETBIOS nome del servizio
138	netbios-dgm	NETBIOS Datagram Service – NETBIOS servizion di datagram
139	netbios-ssn	NETBIOS Session Service – NETBIOS servizio di sessione
140-159		Unassigned - Non assegnato
160-223		Reserved - riservato

Incapsulamento

Quando una parte di informazione – una mail ad esempio – è mandata da un computer ad un altro, è soggetta ad una serie di trasformazioni. Il livello applicazione genera I dati che poi sono trasferiti al livello trasporto.

Il livello trasporto prende questa informazione, la suddivide in segmenti e aggiunge un'intestazione a ciascuno, che contiene le porte, il numero univoco del segmento e altre informazioni sulla sessione.

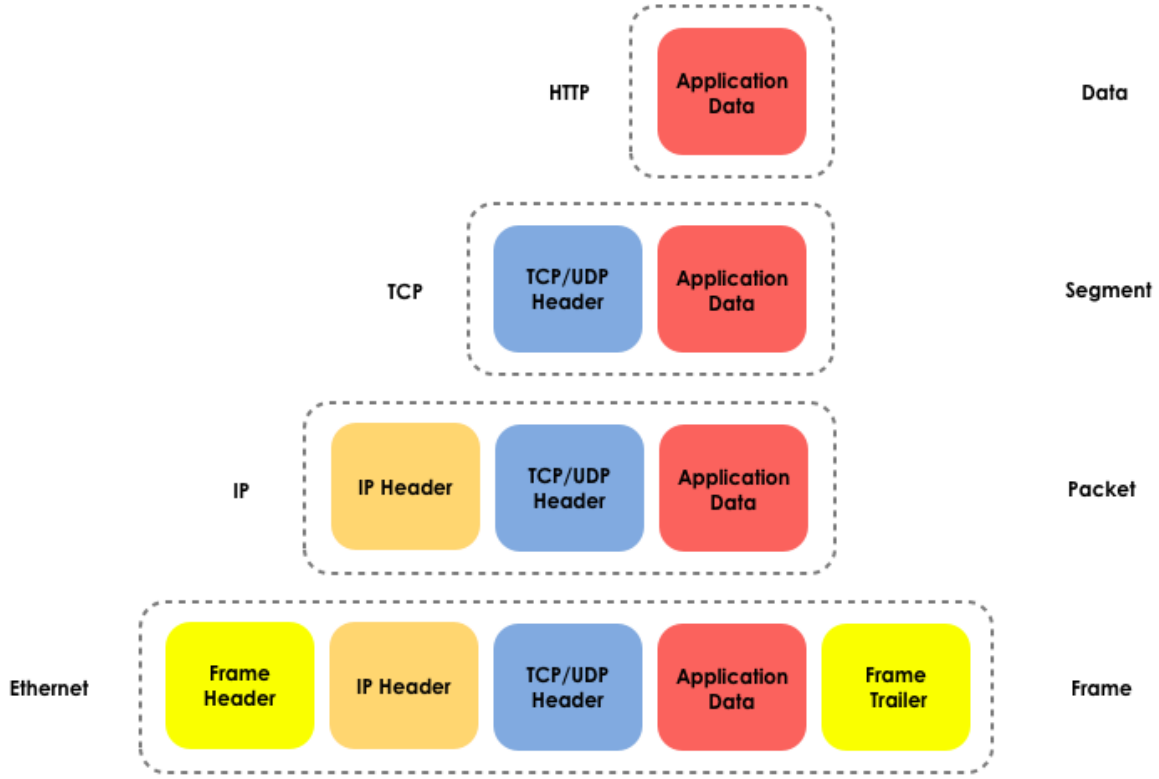
Poi il segmento viene passato al livello Network dove viena aggiunta un'altra intestazione contenente gli indirizzi IP di origine e ulteriori meta--informazioni.

Il livello successivo, che nella maggioranza delle reti locali è fornito da Ethernet, aggiunge ancora un'altra intestazione e così via. Questa procedura è conosciuta come **incapsulamento.**

Ciascun livello dopo il primo crea i suoi dati come un incapsulamento del precedente livello di dati, finchè si arriva al livello finale nel quale avviene la reale trasmissione. L'incapsulamento è rappresentato così:

Figure 3.6: Incapsulamento

Quando l' informazione incapsulata arriva alla sua destinazione, questa deve essere de-incapsulata. Poiché ciascuno livello passa l'informazione al livello successivo della pila, questo rimuove l'informazione contenuta nell'intestazione inserita dal livello precedente.



Il bit finale di informazione in questo grande schema di indirizzamento è l'assolutamente unico indirizzo della scheda di rete (NIC) del computer: l'**indirizzo Media Access Controller (MAC)**. Questo indirizzo è solitamente visualizzato come sei numeri **esadecimali** a due- caratteri, separati da due-punti o hyphen (trattini). É l'indirizzo fisico della scheda di rete e supponendo che non possa essere cambiato (veramente ci sono sistemi per cambiarlo, ma esattamente come lo vedremo un'altra volta). Un indirizzo MC si presenta così:

00-15-00-06-E6-BF

Esercizi

3.1. Usando i comandi che hai imparato nelle Lezioni 1 e 2, individua il tuo indirizzo IP, la maschera di rete, l'indirizzo del DNS e l'indirizzo MAC. Confrontali con quelli dei tuoi compagni. Cosa sembra simile e cosa è differente? Usando lo schema dell'indirizzo IP della rete che stai usando, si tratta di una rete pubblica o privata?

3.2. netstat

Il comando **netstat** ti fornisce le caratteristiche della tua rete: a chi sei connesso, da quanto la connessione è stata stabilita e così via. In Linux, Windows o OSX puoi aprire un'interfaccia a riga di comando e digitare:

```
netstat
```

Nella finestra a riga di comando, vedrai una lista delle connessioni stabilite. Se vuoi vedere le connessioni in una forma numerica, digita:

```
netstat -n
```

Per vedere le connessioni e le porte attive (in ascolto, aperte), digita:

```
netstat -an
```

Per vedere un elenco delle altre opzioni, digita:

```
netstat -h
```

Nell'output di netstat, osserva le colonne che elencano gli indirizzi IP locali e remoti e le porte che stanno usando:

```
Proto Recv-Q Send-Q  Local Address        Foreign Address     (state)
tcp4    0      0  192.168.2.136.1043   66.220.149.94.443    ESTABLISHED
```

Le porte sono i numeri che seguono l'indirizzo IP regolare; possono essere separate da punti o due punti. Perché le porte usate dall'indirizzo remoto sono differenti dalle porte usate dall'indirizzo locale?

Apri diverse finestre del browser o schede su siti diversi, poi lancia di nuovo netstat.

Se ci sono diverse schede aperte, come fa a sapere il browser quale informazione va a quale scheda?

Perché accade che quando un browser web viene usato nessuna porta di ascolto è specificata?

Che protocolli vengono usati?

Cosa accade quando un protocollo viene usato in più di una istanza?

3.3.Il mio primo server

Per effettuare questo esercizio devi avere il programma **netcat (nc)**. BackTrack lo include di default, come fa OSX, ma puoi scaricare l'eseguibile per vari sistemi operativi..

1.In una finestra a riga di comando, digita:

```
nc -h
```

Questo mostra le opzioni che sono disponibili in netcat.

Per crare un semplice server, In Linux o Windows digita:

```
nc -l -p 1234
```

o in OSX digita:

```
nc -l 1234
```

hai appena avviato un server che ascolta la porta 1234.

2.Apri una seconda finestra a riga di comando e digita:

```
netstat –a
```

Questo dovrebbe verificare che c'è un nuovo servizio che ascolta sulla porta 1234.

Per comunicare con un server, devi avere un client. In una seconda finestra a riga di comando digita:

```
nc localhost 1234
```

Questo comando crea una connessione con il server che sta ascoltando sulla porta 1234. Ora, qualunque cosa venga scritta in ciascuna delle due finestre a riga di comando aperte, può essere vista nell'altra finestra.

Considera le implicazioni. Qualcuno come potrebbe abusare di questa possibilità per ottenere il controllo della tua macchina?

Netcat manda tutto il suo traffico in chiaro. Esiste un'alternativa sicura?

3.Ferma il tuo server tornando alla prima finestra a riga di comando e digita Control-C.

4.Ora crea un semplice file di testo chiamato *test* contenente il testo, “Benvenuto nel mio server!”

Una volta che hai fatto questo, osserva il comando seguente e spiegalo all'istruttore: Cosa esegue ogni parte? Quindi nella tua prima finestra a riga di comando , digita:

```
nc -l -p 1234 < test
```

Dall'altra finestra a riga di comando, connettiti al server digitando:

```
nc localhost 1234
```

Quando il client si connette al server, dovresti vedere l' output del file *test*.

Quale protocollo è stato usato per connettersi al server?

Netcat ti permette di cambiarlo? Se si, come?

Nutri la mente: Il Modello OSI

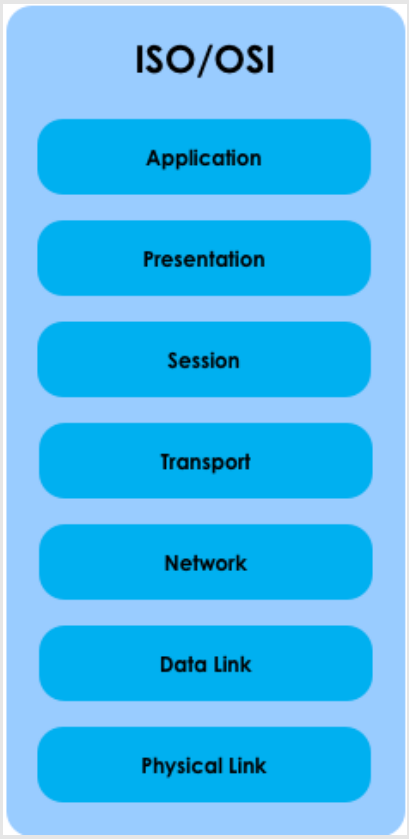


Figure 3.7: Il Modello ISO/OSI

Il **modello OSI** sviluppato negli anni '80 (circa dieci anni dopo il Modello TCP/IP) dalla **ISO**, l'Organizzazione per gli Standard Internazionali. OSI è l'acronimo di **Open Systems Interconnection**, e fu un tentativo di standardizzare l'architettura di rete che proveniva da un'organizzazione che non era minimamente interessata allo sviluppo della rete.

Il Modello OSI è un modello a livelli con un una manciata di semplici regole. Le funzioni simili sono raggruppate insieme nel medesimo livello e (per favore non dimenticarlo) ogni livello è servito dal livello **sottostante** e serve il livello **soprastante**.

Questo modello a livelli è una buona idea perché finché ciascuno livello (in teoria) esegue la propria comunicazione, i nuovi sviluppi in un livello qualsiasi non danneggiano nessuno degli altri livelli. Questa caratteristica spiega da sola lo sviluppo di internet che abbiamo avuto dal 2000, con nuove applicazioni e servizi che comparivano quasi ogni giorno.

Oltre alle due regole di questo modello OSI di cui abbiamo già discusso (le funzioni simili sono raggruppate e ogni livello è servito dal livello sottostante e serve il livello soprastante) questo standard ha una regola stringente in più . Ogni livello, coinvolto da un computer in una connessione, comunica direttamente con lo stesso livello sull'altro computer. Questo significa che quando tu digiti www.google.com sul tuo browser, c'è una interazione diretta fra l'interfaccia livello 7 del tuo computer (il tuo browser web) e I web server di Google (anche in quel caso interfaccia di livello 7), e lo stesso può essere detto per ogni livello.

Definiamo prima cosa sono i livelli del modello OSI e i loro rispettivi compiti.

Livello Applicazione	É responsabile della diretta interazione fra applicazioni e l'interfaccia utente dell'applicazione per esempio l'uso di un browser web come IE o Firefox.
Livello Presentazione	Garantisce che le informazioni siano scambiate in una maniera comprensibile da entrambe le parti. Nei servizi che usano una forma di cifratura questa avviene al livello presentazione.
Livello Sessione	Controlla il dialogo fra due computer. Fondamentalmente attiva, gestisce e termina tutte le connessioni che avvengono tra I computer.
Livello Trasporto	Fornisce il trasferimento trasparente di informazioni fra computer, garantendo servizi affidabili di trasferimento di dati al livello soprastante Questo significa che è responsabile dell'assemblaggio dei dati in porzioni più piccole che possono essere trasportate in maniera affidabile su una rete dati. Se un pacchetto viene perso o non è ricevuto è compito del livello trasporto assicurarsi che quel singolo pacchetto sia ritrasmesso e quindi riassemblato nell'ordine corretto.
Livello Network	Questo livello è responsabile della parte di indirizzamento della connessione. Non solo assicurandosi che ogni indirizzo sia unico sulla rete ma anche accertandosi che qualunque percorso sia disponibile (sia esso ottimale o meno), si possa sempre consegnare l'informazione dove necessita e che la nostra informazione sarà inviata da un passaggio all'altro finché non raggiunga la destinazione finale.
Livello Data Link	Il livello data link fu progettato con lo scopo di assicurare che il livello fisico fosse in grado correggere gli errori che possono accadere e per operare con diversi mezzi di comunicazione. Praticamente esso prepara (incapsula) l'informazione così che possa essere trasmessa su qualunque mezzo fisico sia necessario (onde radio, cavo di fibra ottica, rame).
Livello Fisico	Questo livello definisce le specifiche fisiche del dispositivo e cosa necessiti essere fatto perché le informazioni siano trasmesse sul mezzo selezionato. Per una connessione WiFi, questo è un segnale radio; per una connessione in fibra è un segnale luminoso che viene inviato; o per una connessione sul rame è un segnale elettronico sul filo che viene inviato.

Questi sette livelli comprendono ogni cosa si renda necessaria per una comunicazione affidabile fra computer.

Ecco il confronto fra I differenti modelli di cui abbiamo parlato:

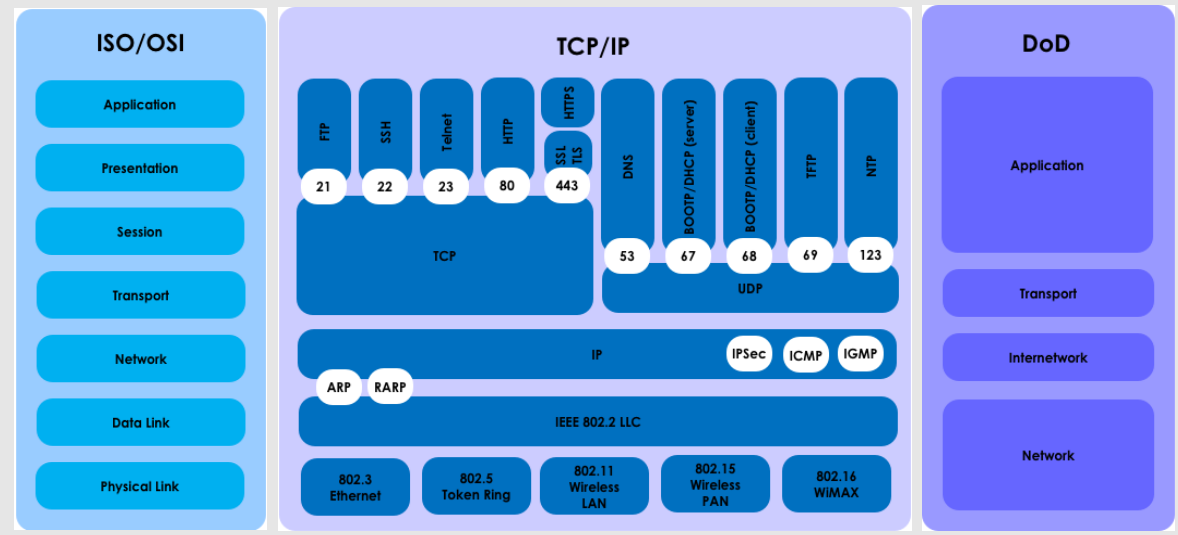


Figure 3.8: Comparazione dei modelli di rete

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM