E-SECURITY: INTRODUZIONE SU IP E RETI

Questo tutorial è stato scritto da Gallerini Micaela (heba, heba.ry.mg@gmail.com), esso non vuole avere la presunzione di spiegare tutto fin nei minimi particolari, ma vuole essere un tramite tra gli utenti comuni e l'informatica, la sicurezza informatica, la programmazione. E' vero che esistono molti tutorial rivolti a questi argomenti, ma molti di loro sono esclusivamente scritti per utenti esperti o per esperti del settore. Ciò che mi sono riproposta è di scrivere una serie di tutorial che portino a capire l'informatica in modo semplice e poco contorto.

Gli ip

Prima di cominciare a parlare di sicurezza informatica, nonché di sicurezza sul web, è necessario capire cosa siano gli ip, il perché vengono usati, cosa sia una rete e tutto ciò che gli gira intorno.
Innanzi tutto l'IP è l'identificativo di Internet Protocol esso è scritto con una notazione, una notazione è una scrittura di numerazione in decimale dove il numero è separato dal puntino, esso identifica una macchina ed il suo proprietario, di solito costituito in questo modo:

255.255.255.0

Esistono due tipologie di tecnologie che servono l'IP, IPv4 e IPv6, il primo viene comunemente utilizzato per le reti domestiche[1] mentre il secondo è supportato (dipende dal sistema operativo che si utilizza) ancora poco per le reti domestiche anche se molti si stanno spostando verso questa tecnologia, IPv6 è utilizzato soprattutto dalle aziende molto grosse e dagli enti statali e tecnologici.
IPv4 consiste di 4 byte (32 bit) detti anche ottetti, ogni IP ha un valore in notazione decimale di 4 numeri separati da punti, quindi quattro ottetti, ogni ottetto può essere composto da numeri che vanno da 0 a 255, quindi è possibile che esistano IP che vanno da 0.0.0.0 a 255.255.255.255.
IPv6, invece, consiste in 16 byte (128 bit) e non 4 come IPv4, questo significa che può avere una molteplicità di possibili IP molto elevata rispetto a IPv4. A differenza di IPv4, IPv6 ha una composizione basilare per gli ip costituita in questo modo:

hhhh: hhhh: hhhh: hhhh: hhhh: hhhh: hhhh: hhhh

quindi, come si nota i byte sono separati dai due punti e la notazione è una notazione esadecimale e non decimale come invece negli IP classici (IPv4), quindi avrà una scrittura tipica:

E5F6: 0000: 0000: 0000: 35E2: 7E6G: T45R: 3210

IPv6 contiene nella notazione completa molti ottetti a 0[2], essi verranno tolti dalla notazione in *Shorthand* anche se rimarranno presenti nell'indirizzo di rete reale, l'ultimo ottetto (3210) può essere riscritto in una notazione *mixed* per cui si otterrà questo numero di IPv6:

E5F6: 35E2: 7E6G: T45R: 10.15.102.1

Definito questo, continuiamo a parlare di IPv4, esso è diviso in cinque categorie di settore (A,B,C,D,E), che identificano un'area di definizione particolare per cui è possibile utilizzare ogni IP. Tutti gli ip riservati alla categoria A hanno l'estremo bit[3] di sinistra in 0, gli altri bit degli ottetti potranno avere indicazione 0 o 1, la categoria B potrà avere i primi due bit a sinistra posizionati in 10 ed i restanti in zero o uno; la categoria C avrà gli estremi tre bit sinistri in 110, la categoria D avrà gli estremi quattro bit sinistri in 1110 ed infine la categoria E avrà gli estremi quattro bit sinistri in 1111. La categoria D, nella tecnologia IPv4, ha riservato quei numeri di IP al multicast[4], per cui teoricamente non si potrebbe navigare in internet, ma dovrebbero essere utilizzati solo dai nodi di ricerca.

---

1 in questo caso una rete domestica è definita anche come un unico pc collegato alla rete, si definisce una rete domestica anche i pc privati utilizzati da casa
2 gli zero verranno sostituiti dalla notazione in esadecimale mano a mano che il sistema IPv6 sarà più utilizzato e quindi avrà più IP a cui far riferimento.
3 si sta parlando di sistema binario quindi costituito solo di numeri 0 o 1
4 è un protocollo internet utilizzato comunemente nelle trasmissioni radio per rendere più efficiente la diffusione dei pacchetti, esso permette l'invio di un pacchetto al solo che lo ha richiesto e non a tutti indistintamente come avviene nella classica radiodiffusione.

La categoria E è riservata alla rete locale (lan), quindi è un indirizzo di rete interna e non dovrebbe essere utilizzata per navigare in internet con ip che vanno da 255.0.0.0.0 a 255.255.255.255 (vedi figura 2).
Le categorie A, B e C hanno accesso alla rete internet tradizionale e sono gli unici autorizzati ad uscire e comunicare.
Gli IP identificati da 127.0.0.0 a 127.255.255.255 sono tipici dell'utilizzo in *loopback,* questo è un sistema che permette di inviare un pacchetto in modo diretto alla fonte a cui lo abbiamo spedito e di riceverne immediata risposta (il ping).
Gli IP riservati alle reti intranet (lan) sono: per la categoria A da 10.0.0.0 a 10.255.255.255, per la categoria B da 172.16.0.0 a 172.31.255.255, per la categoria C da 192.168.0.0 a 192.168.255.255.
Tutte le altre numerazioni possono essere utilizzate liberamente per la navigazione in internet.
Gli IPv6 hanno solo tre tipi di configurazione degli IP: *unicast, multicast e anycast*.
Gli unicast ed il messagging di multicast equivalgono allo stesso IPv4, anche se IPv6 non sostiene la radiodiffusione, ma il meccanismo del multicast ha la stessa funzione, per il multicast gli IP saranno utilizzati come "FF"(255) proprio come con IPv4.
Anycast è una variazione del multicast, mentre quest'ultimo ha la facolta di inviare il pacchetto a tutti i nodi in multicast, anycast ha la facoltà di inviare tutti i pacchetti selezionati a ttutto un nodo specificato di multicast favorendo così una velocizzazione di tutto il sistema di invio dati.
IPv6 ha solo due IP riservati, 0: 0: 0: 0: 0: 0: 0: 0 e 0: 0: 0: 0: 0: 0: 0: 1. Il primo viene riservato per evitare che i nodi possano utilizzarlo per i propri scopi (interni od esterni), quindi è un numero di esecuzione interna al nodo stesso, mentre il secondo equivale al 127.0.0.1 di IPv4 ed è quindi riservato al loopback, esso è anche scritto in questo modo:

::1

Come si può notare il protocollo IPv6 e decisamente più semplice, veloce e agevole da programmare e da gestire a livello di reti, nonché permette una più elevata possibilità di numeri di IP, esso è anche decisamente più sicuro rispetto a IPv4, questo perchè eliminando la programmazione di rete settoriale come è ora utilizzando una sottorete ed una programmazione dei workgroup per ogni nodo si velocizza anche l'esecuzione degli invii di tutti i pacchetti, sia sulla rete interna (intranet) sia su quella esterna (internet).
L'indirizzo IP è utilizzato da molti protocolli internet: TCP e UDP, i browser o client FTP, programmi di posta elettronica, eccetera eccetera.

Quindi, ogni persona ha un indirizzo IP personale, un indirizzo IP può essere *variabile* o *statico*, un indirizzo IP variabile è un indirizzo che utilizza un numero finale variabile ma compreso in un range fisso dato dal proprio isp[5].
Per esempio, un IP variabile potrebbe avere questa composizione:

da 10.15.102.1 a 10.15.102.15

come si può notare vi è una parte (quella sottolineata) che rimane invariata, mentre l'altra parte è il range che il nostro isp ci assegna, un IP variabile si modifica ogni volta che ci disconnettiamo e riconnettiamo a internet, quindi per seguire il nostro esempio di prima, la prima volta che ci colleghiamo ad internet potremmo avere come IP 10.15.102.8 e la volta successiva 10.15.102.13, o 15 o 1 o 3, eccetera eccetera.
La variabilità dell'IP è data informaticamente parlando da un programma random per cui ognuno di noi utilizza diversi numeri di IP i quali però sono ben noti al nostro isp ed egli sa perfettamente a chi

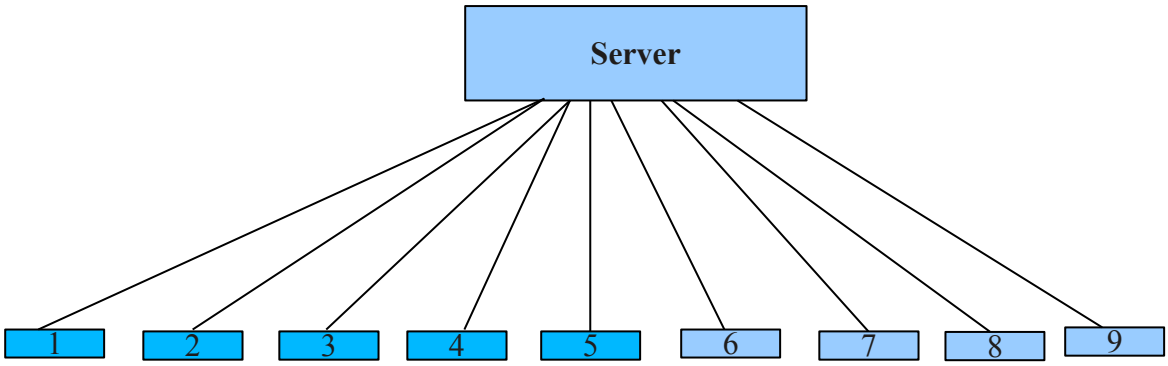
5 l'isp è l'azienda che ci fornisce la copertura internet, per esempio per l'Italia potrebbe essere Telecom, Eutelia, Wind eccetera eccetera.

corrisponde tale numero.
E' possibile anche avere un numero di IP fisso, di solito avere un numero di IP fisso ha dei costi maggiori a seconda del piano tariffario del nostro gestore di internet (isp); avere un IP fisso non comporta cambiamenti, ad ogni collegamento ad internet avremo un unico IP assegnatoci dal nostro isp, per esempio 10.15.102.30. Gli Isp utilizzano una configurazione con il server DHCP che permette di potersi connettere anche se non si ha un IP configurato sulla propria macchina riuscendo così a mettere in comunicazione la macchina privata con quella dell'isp che gli invierà il suo numero di IP corrispondente per quella sessione di collegamento.
Di solito le uniche che prediligono utilizzare un indirizzo IP statico sono le aziende che hanno diversi computers collegati al server centrale, quindi ad una rete aziendale.

Reti aziendali e reti domestiche

Una rete aziendale può avere diverse composizioni, innanzi tutto definiamo che cosa significa la parola server, server in italiano è traducibile come *servizio*[6]. La parola assume diversi significati a seconda di come è utilizzata, nel qual caso stiamo parlando di una macchina allora il server verrà identificato come macchina che serve tutte le altre collegate, il server di solito è collegato in modo permanente, mentre tutte le altre macchine si possono accendere e spegnere tranquillamente, oppure la parola viene indicata come un servizio che una macchina può avere (es. server mysql), ma di questo ne parleremo in altra sede.
Per cui come abbiamo detto, una rete aziendale può avere diverse combinazioni, può avere un server centrale e da uno a 100.000 pc collegati (v. figura 1), esistono anche reti domestiche identificabili con un server e al massimo cinque pc collegati ad esso, mentre una piccola rete aziendale consta da 6 pc collegabili al server centrale fino ad una ventina, una di medie dimensioni parte dai 21 pc collegati, e così via.

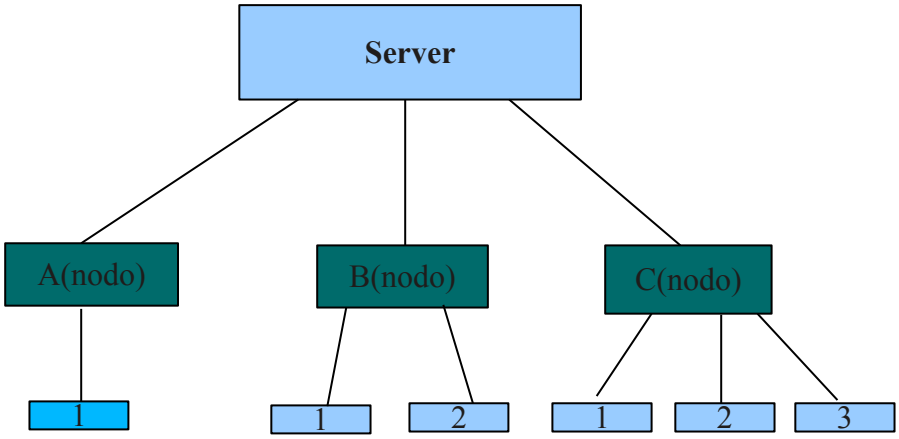
Figura 1.



Un'altra possibilità è trovare una rete aziendale composta da un server centrale, una seconda sottorete, quindi alcuni pc collegati al server primario, creando così un nodo, ed infine altri pc collegati a questi ultimi (vedi figura 2), ogni rete e sottorete ha un ip identificativo che identifica un pc in una certa posizione della rete aziendale ed il suo utilizzatore, il proprietario è l'azienda naturalmente.

Figura 2.

6 vedi l'articolo “Server questi sconosciuti” pubblicato da Pc-facile.com a questo indirizzo (http://www.pc-facile.com/news/server_questi_sconosciuti/)



Gli IP di una rete aziendale hanno un ip pubblico che serve per la navigazione in internet e un ip privato che si utilizza sulla sottorete, ritornando alle tre categorie A, B e C. La prima categoria avrà una gamma di ip che andrà da 0.0.0.0 a 127.255.255.255, per cui l'ip dell'host avrà una composizione che prenderà l'ultimo ottetto, quindi sarà 255.0.0.0; per la categoria B l'indirizzo di rete sarà compreso tra 128.0.0.0 e 191.255.255.255 e la rete interna prenderà gli ultimi due ottetti ed avremo quindi un ip pari a 255.255.0.0; per la categoria C si avrà un range che andrà da 192.0.0.0 e 223.255.255.255 che acquisirà come ip di rete gli ultimi tre ottetti avendo così un ip pari a 255.255.255.0.
Di solito l'IP della netmask (letteralmente mascherina di rete) sarà 255.255.255.255 e sarà quella che permetterà ai vari host (127.0.0.1 o 255.0.0.0) di comunicare con l'intera rete e la rete con internet una volta programmato il firewall.
Come si può notare dalle figure, avere una sottorete e dei nodi con dei workgroups ben definiti velocizza il lavoro del firewall e rende tutta la rete molto più sicura, poiché rende difficoltose tutte le operazioni di hacking dei servizi di rete (per es. il trasferimento di zona dei DNS o il ping di broadcast).

Di solito le sottoreti utilizzano una metodologia di CIDR (Classes of InterDomain), esso utilizza una combinazione tra l'IP e la relativa netmask collegata alla rete, utilizzando uno schema simile:

xxx.xxx.xxx.xxx/n

dove n corrisponde al numero di estrema sinistra in binario equivalenti a 1 della net mask, per esempio, se la net maskfosse 255.255.254.0 la n sarebbe uguale a 23.
La notazione in CIDR può essere adottata solamente su reti che permettono tale tecnologia, anche se a volte può anche essere utilizzato per internet e non solo su intranet, solo che la numerazione di n consentita è più bassa rispetto a quella della sottorete. Classe A solo fino a 8, Calsse B fino a 16 e calsse C fino a 24.

Dipendenze societarie degli IP

Come si è detto l'IP deve essere unico per ogni persona/pc, per ovviare a questo è necessario che un'unica organizzazione se ne occupi e che gestisca tutto il traffico di internet. Originariamente questo compito era stato assegnato dal governo USA a IANA (Internet Assigned Numbers Authority, http://www.iana.org), nel 1998 nacque un'associazione la ICANN (Internet Corporation for Assigned Names and Numbers, http://www.icann.org) formata da organizzazioni commerciali, tecniche, accademiche e di utenti che si occupa dell'assegnazione dei DNS, degli indirizzi IP e dei parametri di protocollo e i numeri di porta. Per il momento IANA ha ancora una buona parte di tutto il lavoro di gestione delle reti internet internazionali, ma con il tempo tutto il loro lavoro dovrebbe passare a ICANN.
Dall'organismo centrale ICANN si strutturano altri organismi con specifiche competenze, esiste quindi un collegio dei direttori che sovrintende tutti i lavori escluso quello dei dipendenti ICANN, esso coordina GAC (Comitato consultivo dei governi nazionali); ALAC (comitato consultivo per la sicurezza "at large"); SSAC (comintato consultivo per la sicurezza e la stabilità e per i sistemi server primari); un gruppo di collegamento tecnico; l'ASO (Address Supporting Organization, http://www.aso.icann.org) esso si occupa di vigilare sulle politiche di indirizzamento degli IP e assegna i blocchi di indirizzi IP ai RIR[7] (Regional Internet Registries) che assegnerà gli IP alle varie arie geografiche[8]; GNSO (http://www.iana.org/gtld/gtld.htm)coordina l'assegnamento dei nomi di dominio di primo livello (gTLD, Generic Top-Level Domains) come .com, .fi, .de eccetera ecceetera; CCNSO è invece l'ente che vigila sulle politiche per i nomi di dominionazionali (ccTLD, Country-Code Top-Level Domains, http://www.iana.org/cctld/cctld-whois.htm).
Il server DNS (Domain Name Server) è un protocollo che utilizza sia gli indirizzi ip sia la nominazione (Name) per il riconoscimento di un nodo, perchè però questo metodo funzioni perfettamente il nome utilizzato dovrà essere unico in tutto il mondo.
Il DNS utilizza un sistema gerarchico per la propria organizzazione, esistono domini di primo livello, come possono essere i .com, .edu, .it, .fi, .de, e via di seguito, quindi un indirizzo internet definito in:

www.rosaventi.com

sarà un dominio di primo livello, esistono poi anche dei sottodomini, identificabili in questo modo

www.rosaventi.indirizzi.com[9]

i sottodomini sono comunque regolati ed amministrati dal gestore del primo dominio.
Esso utilizza un sistema distribuito ed ha una rubrica di tutti gli indirizzi registrati ed i relativi nomi dei proprietari, anche se tali rubriche non sono gestite da una sola macchina.
Il DNS richiede degli indirizzi IP statici e non dinamici che risiedano in modo fisso sul server dei risolutori (resolvers).
Per cui ogni sito avrà sia un corrispondente alfabetico sia un suo corrispondente IP fisso che verrà

7 ogni gruppo geografico ha un gruppo di numerazione particolare che può utilizzare e non può utilizzarne altri all'infuori. Per esempio, in Italia è possibile trovare IP che hanno numerazione 82.xxx.xxx.xxx (Tiscali), 80.xxx.xxx.xxx (TelecomItalia), 62.xxx.xxx.xxx (Eutelia) ed altri ancora, ma non 10.xxx.xxx.xxx. o 13.xxx.xxx.xxx, questo perchè all'Italia è stata assegnata un gruppo di Ip che vengono assegnati dall'autorità competente, appunto il RIR ad ogni Isp, ogni Isp ha una numerazione particolare come si è visto, il 10.xxx.xxx.xxx di solito sono appartenenti al gruppo ARIN (USA, Canada e caraibi).

8 AfriNIC (http://www.afrinic.net) corrispondente all'Africa, APNIC (http://www.apnic.net) corrispondente all'Asia e al Pcacifico, ARIN (http://www.arin.net) corrispondente all'America del Nord ed a parte dei Caraibi, LACNIC (http://www.lacnic.net) corrispondente all'America latina e parte dei Caraibi, RIPE NCC (http://www.ripe.net) Europa, parte dell'Asia, Medio Oriente.

9 è un indirizzo fittizio, non esistono sotto indirizzi per il sito rosaventi.com

registrato sui server dei rispettivi RIR.