Networking

github.com/asdrubalini

December 7, 2021

1 TCP e UDP

TCP: Orientato alla connessione UDP: Non richiede una connessione

Protocollo TFTP su rete locale non poggia su TCP ma su UDP perchè la rete locale ha una bassa latenza e una bassa probabilità di errori.

Anche il protocollo DNS su rete locale usa UDP, mentre su internet usa TCP. Due server DNS tra loro non dialogano un UDP ma in TCP, sempre sulla porta 53.

Il DNS è un protocollo critico perchè i DNS di tutto il mondo devono parlarsi e scambiarsi informazioni. I regimi dittatoriali configurano i DNS presenti sul territorio in modo che non diano tutte le informazioni.

Ognuno si deve fidare delle informazioni che gli vengono rilasciate dall'altro. Ci sono delle autorità superiori che controllano chi possiede i DNS. Se si verificano delle anomalie, le autorità riescono a risalire a chi ha creato le anomalie.

Socket = IP + Porta L'header del TCP normalmente ha 20 bytes + da 0 a 32 bytes opzionali.

Sequence number = TCP tiene sotto controllo il flusso e da un ordine ai pacchetti. Acknowledgement number = chi riceve i dati comunica a chi li ha trasmessi il corretto recapito dei dati.

Bit di controllo = quali funzioni sono attive in quel pacchetto. Ad esempio, se il pacchetto è parte di un segmento fragmentato oppure no. Oppure se il pacchetto contiene oppure no un ACK number.

Window = delimitare il numero massimo di pacchetti che possono essere spediti senza ricevere un ACK.

Checksum = controllo degli errori nella trasmissione (sia header che dati)

Selective ACK = vengono reinviati solo i segmenti persi e non tutti, come è di default.

Durante la fase di connessione (3 way handshake) si settano anche alcuni parametri della comunicazione che possono essere risettati durante la connessione. Ad esempio windows size dove ci si mette d'accordo sul numero massimo di segmenti che possono essere spediti prima di ricevere l'ACK.

Se in un determinato momento ci sono tanti host che parlano con un server, il suo buffer si riempie e il server manda dei segmenti chiedendo di ridurre la finestra dei pacchetti massimi che si possono spedire ogni ACK.

I protocolli di oggi utilizzano le sliding windows e inviano un ACK ogni due segmenti che ricevono.

Le dimensioni della finestra non vengono definite in termini di segmenti ma in termini di bytes, quindi la finestra viene modificata ogni due segmenti.

Tipicamente la dimensione massima di un segmento è di 1460 bytes ma può essere modificato nel corso della connessione.

Alla fine dipende sempre dai tempi.

Guardare a casa il capitolo 15.

2 Dominio di coalisione

Dominio di coalisione è l'insieme delle linee di una LAN in cui può esserci coalisione fisica = due dispositivi che inviano dei dati insieme. Ecludendo le connessioni wireless, sulle LAN con connessioni fisiche, il dominio di coalisione è il singolo tratto che connette i PC allo switch. La coalisione viene evitata dal fatto che la tipologia di connessione è in full duplex (però essendo in full duplex non c'è comunque collisione).

Il dominio di broadcast è l'insieme dello spazio di rete raggiungibile dai pacchetti broadcast. Le reti VLAN servono a segmentare le reti in modo da ridurre i domini di broadcast. Un altro modo per segmentare una rete è quello di utilizzare un router con più interfacce e su ogni interfaccia viene suddivisa un'intera rete in sottoreti.

I router aziendali ormai non hanno più tante interfacce perchè con il meccanismo della VLAN. Normalmente un rouer aziendale non ha più di 4 interfacce. Un paio vengono usate per il collegamento ad internet. Un'interfaccia per le sottoreti interne ed eventualmente un'altra interfaccia di collegamento diretto verso le altre filiali.

Le reti VLAN danno molta flessibilità.

La virtualizzazione non ha bisogno degli switch layer 3, sono sufficienti quelli di layer 2. Per configurarlo si va sugli switch e si crea una nuova VLAN con un certo nome. Poi comincio a lavorare sulla porta o sul range di porte che voglio usare per una determinata VLAN. Ad esempio ho uno switch 24 porte, su 12 voglio avere una VLAN e sulle altre 12 un'altra. Dichiaro le due VLAN, prendo il range delle prime 12 porte e faccio il tag della prima. Poi prendo l'altro range e faccio il tag della seconda.

Esercizio: tre VLANs, un PC per ogni VLAN, un solo switch. Sulla VLAN 1 mettiamo l'indirizzo IP dello switch che fa da SVI (Switch Virtual Interface) con tre PC. Quindi la VLAN 1 non verrà mai usata per creare una VLAN. Per questo motivo di parte della VLAN 2.

Di default le porte sono impostate per non far passare le VLAN. Posso dire allo switch di far transitare tutte le VLAN su una porta.

in una delle tre vlan bisogna mettere due pc. poi bisogna aggiungere un altro pc che non appartiene a nessuna vlan così facciamo tutte le prove.

3 VLAN Giovedì 28 Ottobre 2021

Una porta può essere taggata solo con una VLAN o con tutte. Il trunk permette il passaggio di tutte le VLAN. Non permette il passaggio di comunicazioni non taggate.

Esempio: un'azienda dove faccio 3 VLAN per 3 reparti differenti e poi in una quarta VLAN metto dei server. I server presumibilmente dovranno comunicare con le altre tre VLAN.

Per far comunicare due VLAN serve un Router. Sul router ci sarà bisogno di una sola interfaccia fisica. Su ogni interfaccia virtualizzo una scheda di rete. Si possono creare sottointerfacce.

interface gigabitEthernet 0/0/0.1

Il protocollo da usare è speciale perchè deve trattare dei pacchetti che a livello 2 hanno un tag. Usiamo lo standard 802.1Q. Il comando da usare è encapsulation.

Ricapitolando: Una VLAN deve fare capo ad un'interfaccia virtuale del router. Entro nell'interfaccia virtuale del router e gli dico che lì arriveranno dei pacchetti taggati della VLAN.

encapsulation dot1q ¡vlan id¿

Per far comunicare la VLAN 2 con la VLAN 3 devo andare sulla stessa interfaccia ed aprire una seconda interfaccia virtuale.

show ip interface brief

Mettere in comunicazione la VLAN 2 e la VLAN 3

4 Cisco Netacad

Server autorevole su un determinato dominio è un server che ha delle informazioni in modo diretto. L'informazione può anche essere indiretta, in questo caso viene indicato che l'informazione non proviene da un server autorevole.

Record A: IPv4 Record AAAA: IPv6 Record MX: Mail server Record CNAME: alias di un record DNS

TLD: Top level domain

Per vedere i record DNS di un dispositivo $ipconfig/displaydns$

Root level domain sono gestiti a livello nazionale.

Compito: cercare il comando per inserire nella cache DNS un'associazione IP -¿ Dominio

Domando *nslookup*

Il protocollo FTP lavora con due porte, una su cui trasferisce i dati e l'altra su cui trasferisce i dati.

Il protocollo SMB serve per condividere i file.

5 Capitolo 15

Il capitolo 15 è una panoramica sulla sicurezza informatica. Gli strumenti di attacco cambiano continuamente. Chi attacca non lo fa sempre per creare un

danno alla rete che viene creata. In moltissimi casi, le aziende stesse che gestiscono le reti pagano delle persone per chiedere di attaccare le proprie reti.
Ci sono anche degli hacker che lo fanno senza permesso per poi avvisare l'azienda della falla che ha scoperto nella speranza di ricevere un compenso economico oppure un posto di lavoro.

Fasi degli attacchi di rete:

1. Si va alla ricerca di un obiettivo;
2. Ricognizione sull'obiettivo;

Il linguaggio utilizzato nella sicurezza di rete è lo stesso di quello che si usa in ambito militare.
Per sapere se ci sono delle falle ho bisogno di ottenere delle informazioni, ad esempio sull'hardware utilizzato ed il relativo produttore. Tutto ciò che viene messo in rete ed ha un sistema operativo è attaccabile.
Successivamente si stabilisce su cosa andare ad agire.
Tantissime frodi e attacchi esistono perchè non sono state seguite le policy di sicurezza ed arrivano dall'ingenuità dei dipendenti che si fanno fregare in 1000 modi possibili.
Metto un blocco all'apertura dei file allegati e se la segretaria vuole aprire un file clicco su un pulsante che gira l'allegato ad una macchina virtuale.
Anche l'assenza di policy scritte è molto importante.
L'amministratore di rete deve tenere sempre sotto controllo lo stato dei dispositivi della sua rete. Raccoglie informazioni con dei software che utilizzano come base il protocollo Simple Network Management Protocol (SNMP). Questo protocollo va a richiedere delle informazioni a tutti i dispositivi. Un protocollo di questo tipo attivo su uno switch è un grosso rischio perchè nel momento in cui qualche tipo di software non autorizzato usa lo stesso protocollo, lui risponde.

Le appliance hanno dei software specifici. Filtrano lo spam e le email sospette. I backup e la ridondanza sono molto importanti. Inoltre, spesso ogni giorno si vanno a backupare le infrastrutture e tutti i sistemi, giornalmente. Ci possono essere anche due link fisici.

La DMZ (Demilitarized Zone) è una parte di rete con meno difese rispetto al resto.

Mettere lo spazio nel file può aumentare la sicurezza. Settare la lunghezza minima

service password encryption seurity passwords min-length ¡n caratteri¿

Per mitigare gli attacchi bruteforce posso impostare un limite massimo di password.

SSH è un protocollo criptato. Supporta la crittografia di tipo RSA. Il modulus mi dice di quanti bit è lunga la chiave. Il minimo raccomandato è 1024.

cryptokey generate rsa genera-keys modulus 1024. Per collegarmi in SSH devo entrare nel command prompt e digitare il comando ssh

Un amministratore di rete dovrebbe disabilitare tutti i dispositivi maggiormente soggetti ad attacchi.

Sempre avere ridondanza dove è possibile.

CDP o Cisco Discovery Protocol: protocollo che permette di verificare quali sono gli altri dispositivi di rete direttamente collegati al router.

In moltissime aziende sono spariti i server perchè si fa quasi tutto in cloud.

VoIP: scadente IP phone: molto utilizzato

richiedono dei server interni all'azienda che gestiscono le varie linee interne ed il centralino aziendale. IP phone e VoIP di solito hanno la priorità massima.