

Corso reti 2k7

linuxludus

Lezione 4, porte & servizi

Giuseppe Marocchio (LAN)
io@giuseppe-marocchio.com

Client-server

nelle reti di computer la comunicazione tra due calcolatori è possibile mediante l'architettura client-server. Su un calcolatore sarà "in ascolto" un programma chiamato server. Chi vuole accedere a quella risorsa è chiamato cliente



Porta?

una “porta” è per definizione un passaggio per entrare in una determinata stanza. nel nostro caso una porta è da vedersi come l'indirizzo logico di dove un determinato “servizio è in ascolto” le porte in un calcolatore moderno sono identificate da un numero compreso tra 0 e 65535

Tipo di protocollo.

Esistono due metodi per accedere a una risorsa. il TCP e l'UDP. il primo garantisce l'affidabilità della comunicazione. il secondo no, tuttavia UDP è più snello rispetto al fratello.



TCP

il protocollo TCP si basa sull'instaurazione di una "connessione" mediante uno scambio di pacchetti iniziali il cui fine è instaurare un canale affidabile. Questo meccanismo è detto HandShaking (Stretta di mano)

Upd

Il protocollo UDP si basa su pacchetti generalmente più snelli. Non comprende nessun meccanismo di HandShaking, pertanto non si ha mai la certezza se i dati inviati siano arrivati a destinazione o meno.

Comunicazione

Per stabilire una comunicazione con un calcolatore via rete è pertanto necessario conoscere:

Indirizzo IP, Protocollo, Porta

Protocolli Applicativi

il protocollo applicativo è il protocollo con cui i due calcolatori si scambiano messaggi dopo aver instaurato con successo una connessione.

IP: 10.10.10.10

PROTO: TCP

PORTA: 80

Appl: HTTP

Firewall?

Un firewall è un programma o una parte del sistema operativo che è in grado di identificare e filtrare quello che passa tra lui e la rete.

analizzeremo ora il firewall di linux!

Linux firewall

Il firewall di linux si chiama iptables. Lavora mediante “tabelle” contenenti le regole. queste tabelle vengono lette dall'alto al basso. Quando una regola viene “matchata” viene eseguita l'azione relativa.



Linux firewall (2)

Analizzeremo oggi le 2 tabelle basilari.
la tabella INPUT e la tabella OUTPUT.

la prima si riferisce a tutto il traffico che va direttamente al nostro PC la seconda serve a filtrare il traffico in uscita.

Linux firewall (3)

Qualche comando..

iptables -L

elenca la lista delle regole

nc -l -p <porta>

simula un server TCP

nmap -v ip

elenca le porte aperte su un PC

telnet <ip> <porta>

connette a un determinato ip su una porta

Una semplice regola

```
iptables -A INPUT -p tcp --dport 80 -j  
DROP
```

questa regola d'esempio, dice al firewall di rigettare tutto quello che arriva sulla porta 80 da qualunque indirizzo sorgente!

Obbiettivi di una regola

Gli obbiettivi di una regola sono quelli che si specificano dopo il -j essi possono essere **DROP** (rifiuta) **REJECT** (rifiuta in maniera “diversa”) **ACCEPT** (Accetta)

Esistono altri Target che vedremo la prossima serata.

Laboratorio

Configuriamo due macchine virtuali come

PC1-----PC2

su pc1 proviamo a simulare un servizio su una porta via TCP e proviamo la connessione da PC2.

Laboratorio (2)

Provate ora a filtrare la connessione mediante il comando iptables e testare cosa succede, uno spunto potrebbe essere sniffare cosa succede con tcpdump



All'opera

Proviamo ?



Domande ?

