NON SPEGNERE IL PC A FINE ESAME

Corso di Sistemi Operativi e Reti

Modulo Reti

Prova di laboratorio 21 Luglio 2022 - Prova 1

Durata Prova **90 minuti**

ISTRUZIONI

Lo svolgimento della prova consiste nello sviluppo e simulazione di una rete locale (Firewalling + Routing + Configurazione).

1. **Rinomina** la cartella chiamata "Cognome-Nome-Matricola" che hai trovato sul Desktop e in cui hai trovato questa traccia, sostituendo "Cognome" "Nome" e "Matricola" con i tuoi dati personali e lasciando i trattini;
2. Configura la topologia lasciando tutti i file necessari nella cartella di cui sopra.

Istruzioni per il confezionamento dei file di configurazione:

1. I domini di collisione dovranno essere elencati all'interno del file `CDs` già presente all'interno della cartella **Cognome-Nome-Matricola**.

```
## ESEMPIO DI CD ##
CD1
    network 10.0.0.0/24
    netmask 255.255.255.0
    broadcast 10.0.0.255

CD2
    network 10.0.7.0/30
    netmask 255.255.255.252
    broadcast 10.0.7.3

CDX
...

# Accorpamento RED
RED
    network 10.0.0.0/23
    netmask 255.255.254.0
    broadcast 10.0.1.255
```

2. La risposta ai quesiti deve essere scritta all'interno del file `Quesiti` situato all'interno della directory **Cognome-Nome-Matricola**. Il formato dovrà essere uguale a quello dell'esempio sottostante:

NON SPEGNERE IL PC A FINE ESAME

```
1.
2. comando -xaz
3. altroComando -x -a -z
```

3. Le rotte dell'intero progetto potranno essere specificate all'interno di un file dal nome **rotte.sh** debitamente commentato. Per semplificare, è possibile usare la notazione *networkAreaRed/22* per indicare ad esempio, il network e la maschera di una determinata area o dominio di collisione (evitando dunque di riportare l'intero indirizzo del network del dominio) e *R1[eth0]* per indicare, ad esempio, l'indirizzo ip relativo alla scheda di rete *eth0* del router *R1.* La stessa convenzione può essere utilizzata anche nelle regole di firewalling se necessario e lo si ritiene opportuno.

Si noti che per ogni risposta è riportato il numero del quesito a cui ci si riferisce. Se non si vuole dare alcuna risposta ad una determinata domanda basta scrivere il numero del quesito e lasciare in bianco la riga.
Non è consentito l'uso di alcun altro tipo di materiale (appunti, esempi, libri, calcolatrice, dati trasferiti tramite USB).

N.B. Per il superamento della prova è necessario completare correttamente **i primi 3 punti** specificati all'interno della sezione **[REQUISITI].**

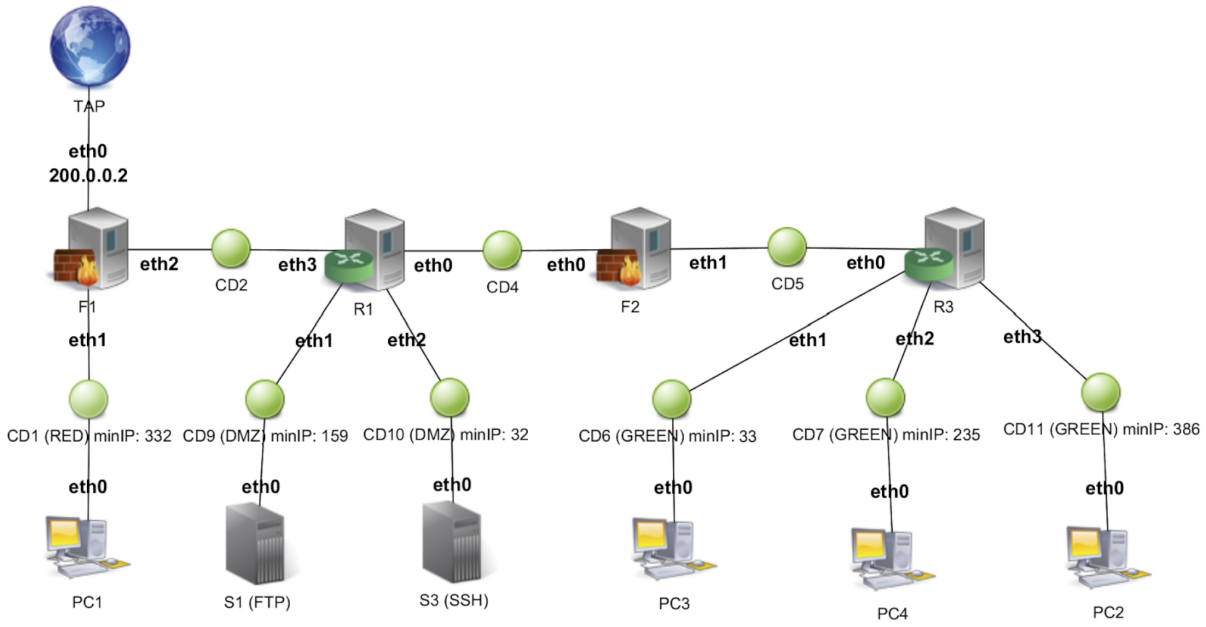
Quando finisci NON spegnere il PC.

SALVA SPESSO il tuo lavoro

NON SPEGNERE IL PC A FINE ESAME

ESERCIZIO 1 (22 punti)

Si ha a disposizione una rete di **`classe A`** (10.0.0.0/8). Si deve progettare/simulare una rete locale seguendo le specifiche riportate nella figura sottostante.



REQUISITI:

REQUISITI:

1. **(4pt)** È necessario accorpare i domini di collisione contigui della stessa tipologia (Green, Red o DMZ)
2. **(4pt)** È richiesto di minimizzare il più possibile lo spreco di indirizzi IP (**annotare sul foglio, per ogni dominio di collisione, gli indirizzi network, maschera e broadcast**)
3. **(3pt)** È necessario, in una prima fase, che tutta la rete sia completamente connessa e funzionante e che tutti gli host siano in grado di comunicare con tutti gli altri hosts (Es. I PC in CD1 devono poter raggiungere e pingare i PC di CD6 e viceversa)
4. **(8pt)** Successivamente applicare le seguenti regole di firewalling **(default policy DROP):**
    a. **(1pt)** L'area GREEN può aprire comunicazioni verso tutti; l'area RED può aprire nuove comunicazioni verso INTERNET e DMZ; l'area DMZ può ricevere nuove comunicazioni da tutti
    b. **(2pt)** Si abiliti l'uso di `icmp` tra l'area GREEN e l'area RED. L'area GREEN potrà effettuare nuove richieste ping (echo-request) mentre l'area RED potrà solo rispondere alle richieste pervenute (echo-reply).

NON SPEGNERE IL PC A FINE ESAME

c. **(2pt)** Il firewall F2 mette a disposizione un servizio web sulla porta 443. Tale servizio deve essere accessibile da INTERNET, e quindi dall'esterno della rete locale. Si scrivano le opportune regole di firewall a tal fine.
d. **(3pt)** Natting:
    i. Si crei una regola che effettui il port forwarding dei seguenti pacchetti:
        1. Se il pacchetto arriva in input sulla scheda di rete *eth0* di **F1** e la sua porta destinazione è la **1234**, il pacchetto dovrà essere rediretto in **S1** sulla nuova porta **2222**.
        2. Se il pacchetto arriva in input sulla scheda di rete *eth0* di **F1** e la sua porta destinazione è la **8052**, il pacchetto dovrà essere rediretto in **S3** sulla nuova porta **22**.
    ii. Si scriva una regola per mascherare l'indirizzo ip sorgente di tutte le connessioni provenienti dall'interno della rete e dirette verso internet come nuovo indirizzo ip sorgente quello della scheda di rete *eth0* di **F1**

5. **(1pt)** Scrivere di seguito il comando per visualizzare lo stato delle connessioni instaurate sul computer locale. Specificare inoltre i parametri per filtrare TUTTE le connessioni di tipo TCP, UDP.
6. **(1pt)** Scrivere di seguito il comando per catturare i pacchetti ***icmp*** che passano attraverso un host
7. **(1pt)** Aggiungere una static entry nella tabella arp (si usi come IP: 10.0.0.2 e come MAC ADDRESS: 00:0c:29:c0:94:bf)

ESERCIZIO 2 (8 pt)

Si scriva uno script, in linguaggio Python o Perl, che esegua il comando iptables con le corrette opzioni e riporti in output il numero di pacchetti droppati per ogni singola catena e il numero totale di pacchetti droppati dal firewall. Inoltre, se il numero di pacchetti **accettati** dalla catena dal nome "internetRed" è maggiore di 10, si esegui il comando adatto ad eliminare tutte le regole della sola catena "internetDMZ".
Hint: per eliminare tutte le regole da una singola e specifica catena, si può utilizzare lo stesso comando usato per rimuovere tutte le regole del firewall specificando di seguito il nome della catena.

Esempio:

Chain INPUT (policy DROP 81 packets, 12431 bytes)

```
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   10     0 internetRED  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 43 packets, 5845 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain internetRED(1 references)
 pkts bytes target     prot opt in     out     source               destination
    4     0 ACCEPT     tcp  --  *      *       35.87.125.36         0.0.0.0/0           tcp dpt:80
    3     0 ACCEPT     udp  --  *      *       192.168.1.150        0.0.0.0/0           udp dpt:53
    3     0 DROP       tcp  --  *      *       192.168.1.107        0.0.0.0/0           tcp dpt:8080
```

Nell'esempio mostrato sopra, il numero di pacchetti **accettati** dalla catena internetRED è minore di 10, quindi lo script stamperà in output solo il numero di pacchetti droppati dalle catene INPUT, OUTPUT e FORWARD e il relativo totale:

```
Pacchetti Droppati:
INPUT:              81
FORWARD:            0
OUTPUT:             43
internetRED:        3
--------------------------------
TOTALE:      127
```