NON SPEGNERE IL PC A FINE ESAME

Corso di Sistemi Operativi e Reti

Modulo Reti

Prova di laboratorio 30 Gennaio 2023

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].**

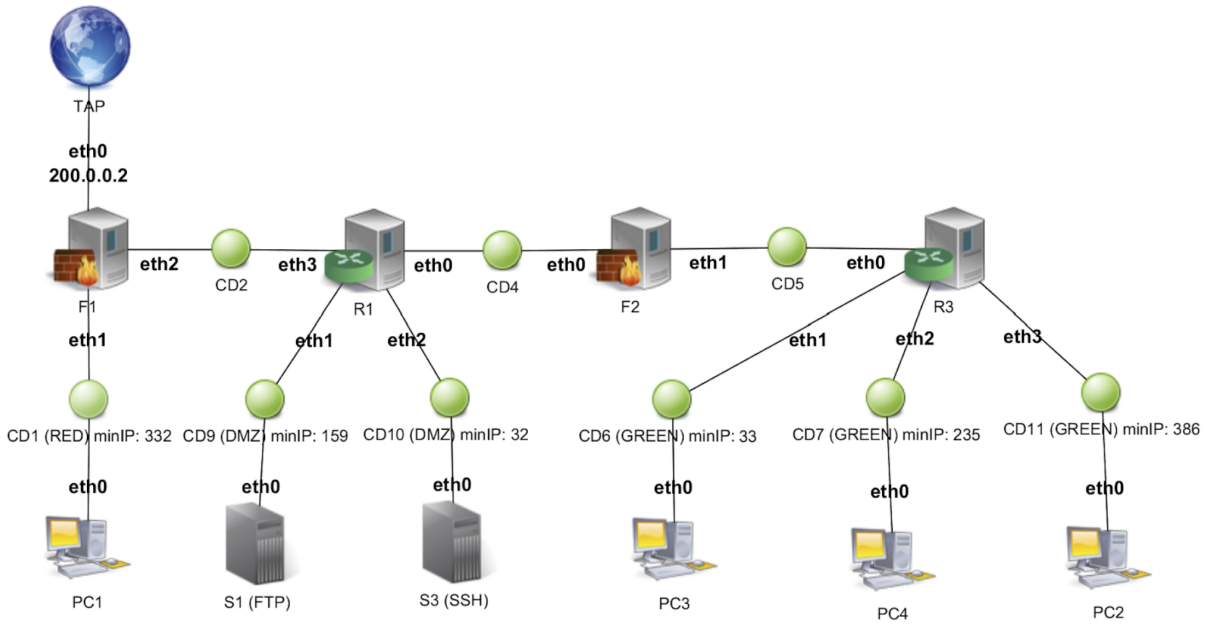
Quando finisci NON spegnere il PC.

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 DMZ e l'area RED. L'area DMZ potrà effettuare nuove richieste ping (echo-request) e l'area RED potrà rispondere alle richieste pervenute da DMZ (echo-reply).

NON SPEGNERE IL PC A FINE ESAME

c. **(2pt)** Il firewall F2 mette a disposizione un servizio web sulla porta 8080. 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 **443**, il pacchetto dovrà essere rediretto in **S1** sulla nuova porta **4443**.
      2. Se il pacchetto arriva in input sulla scheda di rete *eth0* di **F1** e la sua porta destinazione è la **25**, il pacchetto dovrà essere rediretto in **S3** sulla nuova porta **25**.

   i. Si scriva una regola per mascherare l'indirizzo ip sorgente di tutte le connessioni provenienti dall'interno della rete con l'indirizzo ip del firewall F1 su *eth0*.

5. **(1pt)** Scrivere il comando usato per ricavare il percorso seguito dai pacchetti sulla rete.
6. **(1pt)** Scrivere il comando per aprire un server in ascolto sulla porta 1234 sul computer locale.
7. **(1pt)** Creare uno script **tap.sh** che consente le connessioni internet in una topologia GNS3.

ESERCIZIO 2 (8 pt)

Si scriva uno script, in linguaggio Python o Perl che, ricevuto tra argomenti un file contenente una lista di MAC address, verifichi se per ognuno di essi è presente una entry all'interno della sua arp table.

Per ogni mac address trovato all'interno della arp table, lo script deve ricavare l'indirizzo ip ad esso associato e controllare se vi è almeno una connessione instaurata tra il localhost (127.0.0.1) e l'indirizzo ip in questione.

Lo script stamperà per ogni indirizzo IP trovato, il numero di connessioni instaurate con il localhost.

Se esistono più di 5 connessioni per uno stesso IP, lo script eseguirà una opportuna regola di firewall al fine di bloccare tutte le future connessioni tcp in entrata da quello specifico indirizzo ip.

Esempio:

1. ***File in input (mac_address.txt)***

```
8c:de:e5:20:5a:01
2b:28:6d:45:46:b9
8c:ee:77:ba:2e:63
8f:b7:7a:68:a9:3e
99:79:1a:f1:77:05
```

2. ***Esecuzione dello script***

```
python3 script.py mac_address.txt
```

3. ***Output***

```
IP address      # connections
10.0.1.4   2
10.0.2.3   4
10.0.1.1   7
```

(N.B.: A questo punto lo script avrà bloccato tutte le connessioni tcp in entrata da parte dell'indirizzo ip 10.0.1.1)

È parte integrante dello script conoscere i comandi e le opzioni utili a ricavare le informazioni relative agli indirizzi ip associati ad un mac address nella macchina locale e al numero di connessioni instaurate tra 2 hosts.

NON SPEGNERE IL PC A FINE ESAME