NON SPEGNERE IL PC A FINE ESAME

Corso di Sistemi Operativi e Reti

Modulo Reti

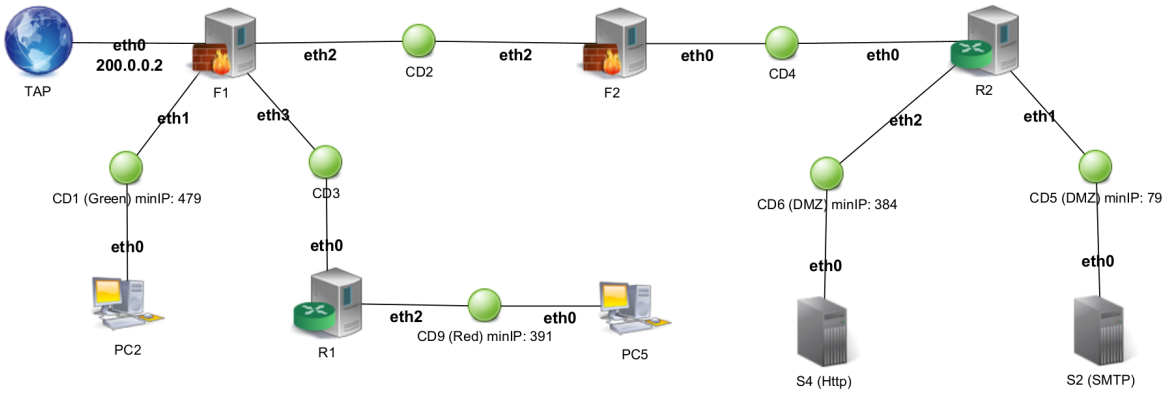
Prova di laboratorio GIUGNO 2021 - Turno 1

Durata Prova **60 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. Per ogni macchina da configurare, il corrispondente file `interfaces` dovrà essere salvato nella cartella già presente dell'host corrispondente.

NON SPEGNERE IL PC A FINE ESAME

2. 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
```

Si noti che i domini di collisione (CD1, CD2, CDX) devono essere listati in ordine crescente per nome del dominio e non per indirizzo IP

3. 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:

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

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

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. **(4pt)** 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. **(7pt)** Successivamente applicare le seguenti regole di firewalling **(default policy DROP):**
    a. **(1pt)** L'area GREEN può aprire comunicazioni verso tutti
    b. **(1pt)** L'area RED può aprire nuove comunicazioni solo verso internet
    c. **(2pt)** L'area DMZ può ricevere nuove comunicazioni solo da Internet e da Green
    d. **(3pt)** Tutti i server interni alle aree DMZ devono essere raggiungibili dall'esterno tramite l'indirizzo IP pubblico del firewall più esterno
5. **(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)
6. **(1pt)** Scrivere il comando usato per ricavare il percorso seguito dai pacchetti sulla rete
7. **(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.

NON SPEGNERE IL PC A FINE ESAME

ESERCIZIO 2 (8 pt)

Si scriva uno script, in linguaggio Python o Perl, che verifichi se all'interno del file /var/log/auth.log esistono almeno 5 tentativi di accesso tramite servizio ssh consecutivi non autorizzati da parte di un determinato indirizzo IP. In caso affermativo, si scriva una opportuna regola di firewall per bloccare le richieste di accesso al servizio ssh da parte dell'indirizzo IP trovato.

Un esempio di riga del file /var/log/auth.log in cui si evidenzia un tentativo di accesso non autorizzato, è il seguente:
Jun 7 12:04:08 pcname sshd[117968]: Failed password for root from 39.97.235.83 port 55884 ssh2

NON SPEGNERE IL PC A FINE ESAME