

Cognome: _____ **Nome:** _____ **Matricola:** _____

Sicurezza dei sistemi informatici e delle reti – 18 luglio 2012

Usa questa pagina per la brutta, staccala, non consegnarla.

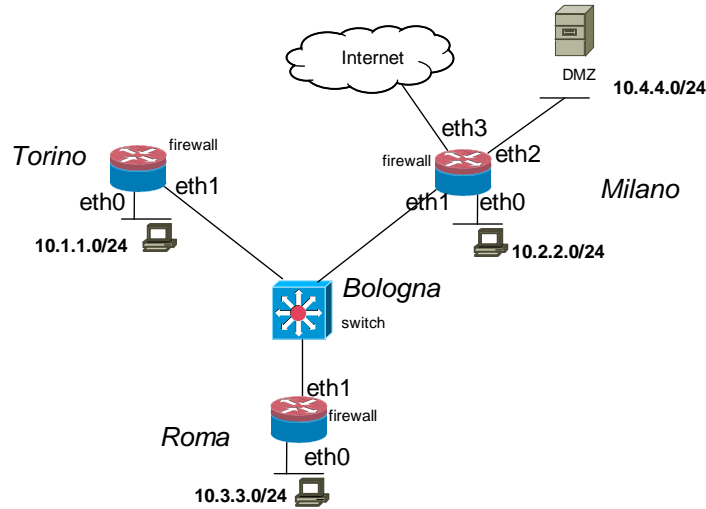
Cognome: _____ **Nome:** _____ **Matricola:** _____

Sicurezza dei sistemi informatici e delle reti – 18 luglio 2012

Usa questa pagina per la brutta, staccala, non consegnarla.

Sicurezza dei sistemi informatici e delle reti – 18 luglio 2012

2. Considera la rete in figura



I firewall delle sedi di Roma, Torino e Milano sono collegate tra loro tramite uno switch a Bologna. Le configurazioni dei firewall sono le seguenti. Il firewall di Milano fa anche NAT rispetto a Internet.

Roma

```
:FORWARD DROP
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -m state --state NEW -j ACCEPT
-A FORWARD -i eth1 -s 10.4.4.0/24 -m state --state NEW -j ACCEPT
```

Torino

```
:FORWARD DROP
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -m state --state NEW -j ACCEPT
-A FORWARD -i eth1 -s 10.4.4.0/24 -m state --state NEW -j ACCEPT
```

Milano

```
:FORWARD DROP
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -o eth2 -m state --state NEW -j ACCEPT
-A FORWARD -o eth1 -s 10.4.4.0/24 -m state --state NEW -j ACCEPT
-A FORWARD -i eth0 -o eth4 -m state --state NEW -j ACCEPT
```

2.1. Compila la seguente matrice di accesso per la rete inserendo Q: Richiesta, R: Risposta. Ignora eventuali problemi relativi allo spoofing.

da	a	Pc Roma	Pc Torino	Pc Milano	DMZ	Internet
Pc Roma						
Pc Torino						
Pc Milano						
DMZ						
Internet						

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 18 luglio 2012

2.2. Descrivi i problemi di spoofing che trovi nelle configurazioni date, specificando anche da quali sorgenti possono venire gli attacchi e verso quali destinazioni possono essere inviati con successo.

2.3. Dai una soluzione che prevenga i problemi di spoofing trovati al punto 2.2 e scrivi esplicitamente le configurazioni da aggiungere ai router di Roma Milano e Torino.

3. Rispondi alle seguenti domande sulla sicurezza dei sistemi unix.

3.1. Set UID bit: a cosa serve, come funziona e che rischi di sicurezza comporta?

A che cosa serve

come funziona

che rischi di sicurezza comporta

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 18 luglio 2012

3.2. Permessi “search” per le directory: come viene rappresentato dai filesystem e che ruolo ha nell’algoritmo di controllo di accesso di un sistema unix?

<p>rappresentazione</p> <p>ruolo nell’algoritmo di controllo di accesso.</p>

4. Public Key Infrastructure

4.1. Descrivi il motivo per avere certificati che siano validi per un limitato arco temporale. Chi ha l'onere di verificare la validità del certificato?

<p>Motivazione</p> <p>Chi verifica</p>

4.2. Descrivi il motivo per avere certificati che siano revocabili. Come avviene la revoca? Chi verifica se un certificato è stato revocato?

<p>Motivazione</p> <p>Procedura di revoca</p> <p>Chi verifica</p>

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 18 luglio 2012

4.3. Descrivi il motivo per avere certificati che non siano usabili per firmare altri certificati. Chi attua tale verifica?

Motivazione
Chi verifica

4.4. Certificati self-signed. Qual è la valenza di sicurezza di tali certificati? Motiva la risposta.

--

5. Pianificazione della sicurezza

5.1. Supponi di dover far capire al tuo capo (che non si occupa di sicurezza) il valore di un certo piano di sicurezza già redatto. Elenca brevemente gli aspetti che metteresti in risalto per metterlo in grado di decidere se eseguire il piano o no.

--

5.2. Quali sono secondo te delle buone pratiche per progettare le contromisure e per pianificare il loro acquisto/deployment?

--

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 18 luglio 2012

6. [solo per 270] Considera un database A in locale, di una sola tabella con molti record, aggiornato di frequente (ad sempio con insert e delete di interi record), e un backup remoto B collocato su un server non fidato presso un cloud provider. B è aggiornato in sincronia con A ma non viene mai letto se non in caso di disaster recovery.

6.1. Poiché B è non fidato potrebbe essere manomesso. Vorremmo mantenere un hash H in locale dell'intero database A in modo da rilevare eventuali manomissioni di B. Descrivi un modo per fare questo badando all'efficienza dell'operazione di aggiornamento.

Descrizione della soluzione proposta per mantenere H

Complessità computazionale dell'aggiornamento del db (es. insert di un record) comprendente il ricalcolo di H

6.2. Supponi che in caso di disaster recovery si rilevi che l'hash di B non sia pari ad H. Secondo la tua soluzione è possibile distinguere parti manomesse da parti integre? Spiega.