Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 19 febbraio 2013

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 19 febbraio 2013

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

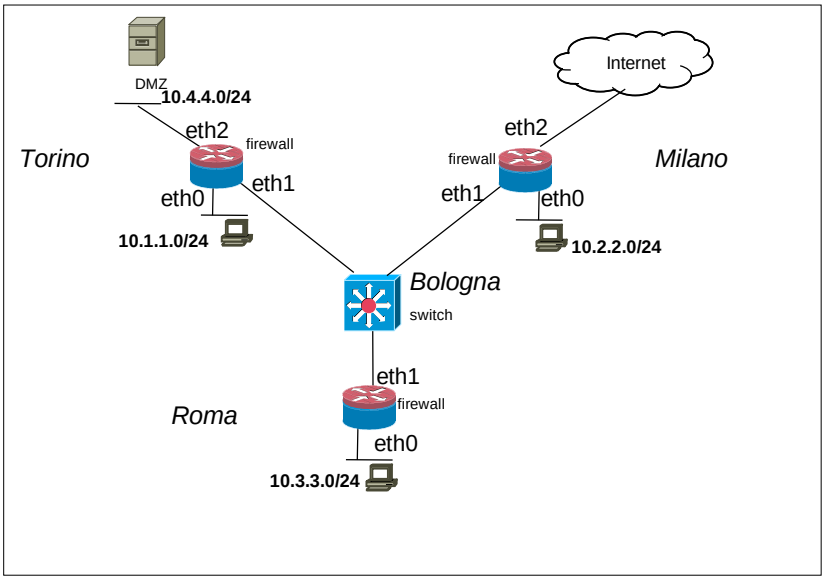
Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 19 febbraio 2013

Tempo a disposizione: 60 (5 cfu) o 70 (6 cfu) minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di cellulari, calcolatrici, palmari e affini.

1. Sicurezza delle reti.

Considera la rete in figura



I firewall delle sedi di Roma, Torino e Milano sono collegati tra loro tramite uno switch a Bologna.

Il firewall di Milano fa anche NAT rispetto a Internet.

La configurazione per **tutti** i firewall è la seguente.

Roma, Torino, Milano

```
:FORWARD DROP
-A FORWARD -m state –state
     RELATED,ESTABLISHED -j ACCEPT
-A FORWARD –i eth0 -m state --state NEW -j ACCEPT
```

1.1. Quali utenti tra quelli di Roma Milano e Torino possono accedere ad Internet? Perchè gli altri non ci riescono? Cosa puoi dire della DMZ?

1.2. Sugerisci delle modifiche alle configurazioni per far sì che (1) gli utenti di Roma e Milano possano accedere ad Internet ma quelli di Torino no, (2) gli utenti di Torino e Roma possano accedere alla DMZ ma quelli di Milano no.

1.3. La configurazione che hai suggerito è vulnerabile a spoofing? In caso affermativo, suggerisci delle contromisure sottofoma di modifiche di configurazione.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 19 febbraio 2013

2. **Sicurezza del codice**. Considera il seguente codice C in cui la funzione quotedCopy() fa la copia di una stringa aggiungendo delle backslash prima di dei caratteri backquote « ` ».

```
void quotedCopy(char* from, char* to) { ... }

int main(int argc, char** argv) {
      char inpt[1001], quotedInpt[1003];
      char *command;
      scanf("%1000s",inpt);
      quotedCopy(inpt, quotedInpt);
      command=malloc(sizeof(quotedInpt)+20);
      sprintf(command, "ls -l %s", quotedInpt);
      system(command);
}
```

2.1. Sottolinea le righe di codice che secondo te introducono una vulnerabilità e descrivi i relativi problemi di sicurezza.

2.2. Se tu potessi cambiare il codice come risolveresti i problemi riscontrati?

3. **Sicurezza delle Public Key Infrustructure (PKI).**

3.1. I certificati delle CA sono diversi dagli altri. Spiega le motivazioni di tale approccio e che verifiche deve fare un browser in quest'ambito.

3.2. Validità del certificato. Perché è necessario avere tale vincolo in un certificato? Come si deve comportare un browser in quest'ambito?

3.3. Cosa succede se una chiave privata viene erroneamente pubblicata? Descrivi rischi e contromisure previste.

4. Principi di progettazione

4.1. Descrivi brevemente il principio del confinamento

4.2. Descrivi brevemente il principio del minimo privilegio

4.3. Elenca **tre** meccanismi a te noti nell'ambito dei sistemi operativi (ad esempio nell'ambito dei sistemi unix o windows), che sono preposti ad attuare politiche di confinamento e/o restrizione di privilegio.

4.4. Il principio del minimo privilegio in unix è molto complesso da attuare a livello di processo, cioè come vincoli imposti alle system call che il processo può invocare. Mostra **due** esempi di politiche difficili da supportare in unix.

5. **Perfect forward secrecy.** Descrivi.

6. **[solo per 270]** Considera i rischi legati all'adozione di un **database** in cloud pubblica rispetto alle seguenti coordinate di sicurezza: confidenzialità, integrità, disponibilità. Per ciascuna di esse descrivi brevemente, rischio, una contromisura ed eventuali limiti di applicabilità della contromisura indicata.

6.1. Confidenzialità.

Rischio

Contromisura

Limiti

6.2. Integrità.

Rischio

Contromisura

Limiti

6.3. Disponibilità.

Rischio

Contromisura

Limiti