Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

Scrivi qui GRANDE 509 o 270

Tempo a disposizione: **60/70 minuti.** Libri e appunti chiusi.
Vietato comunicare con chiunque.
Vietato l'uso di cellulari, calcolatrici, palmari e affini.

1. Considera il seguente codice C e rispondi alle seguenti domande.

```
int main(int argc, char** argv) {
char dir[99999];
char *command;
scanf("%999999s",dir);
command=malloc(sizeof(dir)+20);
sprintf(command, "ls –l %s", dir);
system(command);
...
}
```

1.1. Descrivi i problemi di sicurezza che riscontri nel codice sopra riportato.

1.2. Se tu fossi responsabile della sicurezza dell'esecuzione di quel codice ma non puoi cambiarlo, come ti comporteresti. Rispondi nei due casi in cui l'input è **fidato** e in cui l'input è **non fidato**

Input fidato

Input non fidato

1.3. Supponi di poter cambiare il codice, che cosa suggeriresti ai programmatori per migliorarne la sicurezza?

Cognome:_____ Nome: _____ Matricola:_____

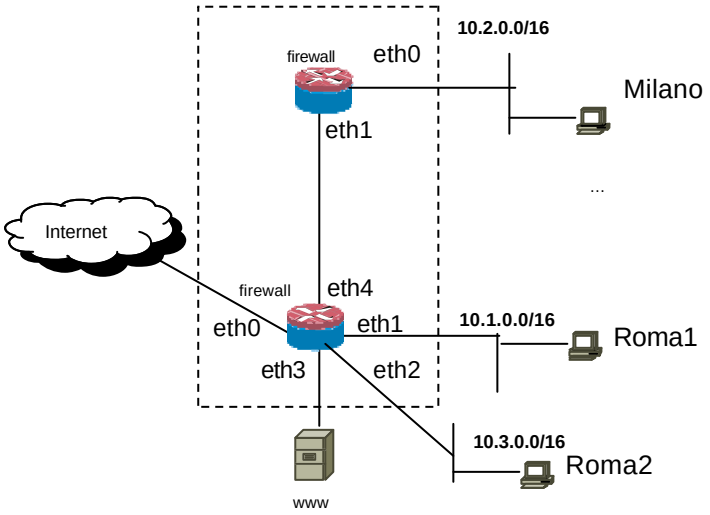
Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

2. Considera il concetto di hash crittografico

2.1. Descrivi l'attaco di tipo birthday, mostrando un esempio

2.2. Descrivi l'attacco per mezzo di rainbow table e la struttura del database utilizzato.

3. Considera la rete in figura.



Supponi che le tabelle di routing dei firewall siano correttamente configurate per assicurare la raggiungibilità completa e le configurazioni dei due firewall siano:

Milano

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

Roma

```
:FORWARD DROP
-A FORWARD -i eth1 -m state --state NEW -j ACCEPT
-A FORWARD -i eth2 –o eth0 -m state --state NEW -j ACCEPT
-A FORWARD -i eth4 –o eth3 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

3.1. Mostra un matrice di accesso del sistema dei due firewall per traffico tcp/udp. Inserisci nelle caselle "Q" per richiesta, "R" per risposta o "-" per filtrato.

A **Da**	Milano	Roma1	Roma2	www	Internet
Milano	----------				
Roma1		----------			
Roma2			----------		
www				----------	
Internet					----------

3.2. Supponi di avere un secondo ISP presso milano. Ciascuna sede usa il suo ISP per tutte le comunicazioni. Nessuna ridondanza sul fault dell'ISP. Il link tra le sedi è usato solo per le comunicazioni tra le due sedi. Descrivi la configurazione del routine e del firewalling, o problemi che riscontrati che ne impediscono la realizzazione (ignora l'esistenza di www).

Routing:

Firewalling:

3.3. Come sopra, ma Entrambe le sedi usano l'ISP di Roma se questo è disponibile, altrimenti usano l'ISP di Milano. Il link tra le sedi è utilizzato anche per l'accesso ad Internet dalla sede di Milano in situazione normale e da Roma in caso di backup. Descrivi la configurazione del routine e del firewalling, o problemi che riscontrati che ne impediscono la realizzazione (ignora l'esistenza di www).

Routine

Firewalling

4. Documento Programmatico di Sicurezza e Piano di Sicurezza.

4.1. Confronta i due documenti

	DPS	**Piano di sicurezza**
Obiettivi		
Contenuti		
Obbligatorietà		
Altro		

4.2. Descrivi, per ciascuno dei due documenti, quale è il rapporto con la normativa antiterrorismo specificando cosa i due documenti conterranno in relazione a tale normativa.

Rapporto con il DPS

Rapporto con il Piano di Sicurezza

5. Descrivi le maggiori vulnerabilità degli switch e delle reti locali.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

6. **[solo per 270]** Descrivi le proprietà della struttura dati autenticata (ADS) Merkle Hash Tree e il metodo per produrre un **certificato** della **presenza** di un elemento in tale struttura e il metodo per produrre un certificato della **assenza** di un elemento in tale struttura.

MHT

Certificazione della presenza di un elemento

Certificazione della assenza di un elemento