Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 29 gennaio 2019 – 4 CFU (la tesina vale 2 CFU)

SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 29 gennaio 2019 – 4 CFU (la tesina vale 2 CFU)

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 29 gennaio 2019 – 4 CFU (la tesina vale 2 CFU)

SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME

Tempo a disposizione: 60 minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di smartphone/watch, calcolatrici e affini.

1. Sicurezza del codice.

Considera il seguente codice C che devi considerare essere eseguito con input non fidato in ambiente Unix.

```
int main(int argc, char** argv) {
  char cmd[1000];
  strcpy(cmd, "cp sorgente/");
  strcat(cmd, argv[1]);
  strcat(cmd, " destinazione/");
  strcat(cmd, argv[1]);
  system(cmd);
}
```

1.1. Elenca le vulnerabilità che pensi siano presenti in questo codice con una breve descrizione del problema.

1.2. Suggerisci delle modifiche al codice per risolvere le vulnerabilità.

2. AAA.

2.1. Per ciascuna A: scrivi il nome per esteso, descrivi brevemente il significato e descrivi una realizzazione tecnologica o un aspetto tecnologico rilevante.

- A…..
Descrizione:

Aspetto tecnologico:

- A……
Descrizione:

Aspetto tecnologico:

- A….
Descrizione:

Aspetto tecnologico:

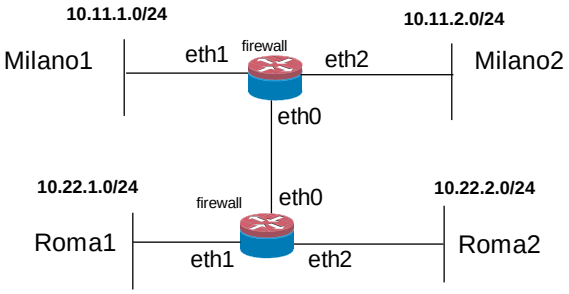
Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 29 gennaio 2019 – 4 CFU (la tesina vale 2 CFU)

2.2. Mostra un diagramma di flusso che esprima come i vari elementi del modello AAA entrano in gioco nel tempo.

3. Networking.

Considera la rete in figura con le configurazioni dei firewall date sotto. Non vi sono nat ed il routing è configurato correttamente.



Roma

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

Milano

```
:FORWARD DROP
-A FORWARD –i eth0 –s 10.22.2.0/24 –m state --state NEW –j ACCEPT
-A FORWARD –m state --state ESTABLISHED –j ACCEPT
```

3.1. Esprimi la policy realizzata dal sistema dei due firewall, con le configurazioni mostrate, compilando la matrice di accesso corrispondente (supponi un comportamento non malevolo degli utenti). Inserisci Q se passa il primo pacchetto (Query), R se passano solo i pacchetti successivi al primo (Response).

A Da	Roma1	Roma2	Milano1	Milano2
Roma1	-----			
Roma2		-----		
Milano1			-----	
Milano 2				-----

3.2. Supponi che nella rete vi siano utenti malevoli. Date le configurazione di sopra, vedi un modo per aggirare almeno una parte della policy? Descrivi la vulnerabilità e fornisci una soluzione.

vulnerabilità

soluzione

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 29 gennaio 2019 – 4 CFU (la tesina vale 2 CFU)

4. Hash crittografici.

4.1. Descrivi cosa è un hash crittografico e le sue proprietà tipiche.

breve descrizione

lista delle proprietà con una breve descrizione

4.2. Descrivi la tecnica nota come rainbow tables.

5. Strutture dati autenticate.

5.1. Descrivi la struttura di un Merkle Hash Tree.

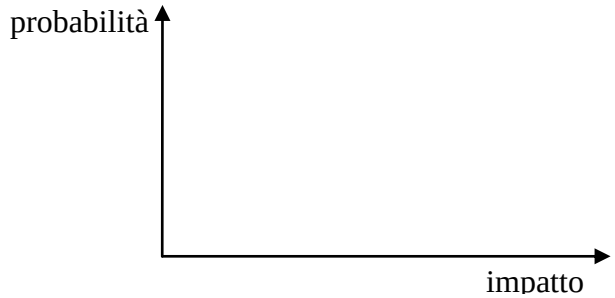
5.2. La struttura Markle Hash Tree è progettata per contenere dati il cui ordine è dato dal dato stesso, essendo una variante di un albero di ricerca. Supponi di voler autenticare il contenuto dei settori di una partizione di un disco mantenendo l'ordine che questi hanno sul disco. Suggerisci una modo di usare i MHT per questo scopo.

6. Metodologie.

6.1. Descrivi brevemente i modi in cui si può trattare un **rischio** illustrando come ciascuno di essi si "muove" (o "non si muove") in uno schema sul piano impatto-probabilità.

descrizione

schema



6.2. Descrivi cosa è un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e di cosa tratta lo standard ISO 27001.

Definizione SGSI

ISO27001