Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 9 febbraio 2018 – 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 – 9 febbraio 2018 – 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 – 9 febbraio 2018 – 4 CFU (la tesina vale 2 CFU)

SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME

Tempo a disposizione: 50 minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di smartphone/watch, calcolatrici e affini.

1. Spiega brevemente in cosa consiste l'attacco cross-site scripting persistente e fai un esempio.

spiega

esempio

2. Discuti brevemente i principi di progettazione "isolamento" e "mediazione completa". Tra loro c'è una sinergia o un antagonismo? Spiega.

isolamento

mediazione completa

sinergia o antagonismo? Spiega.

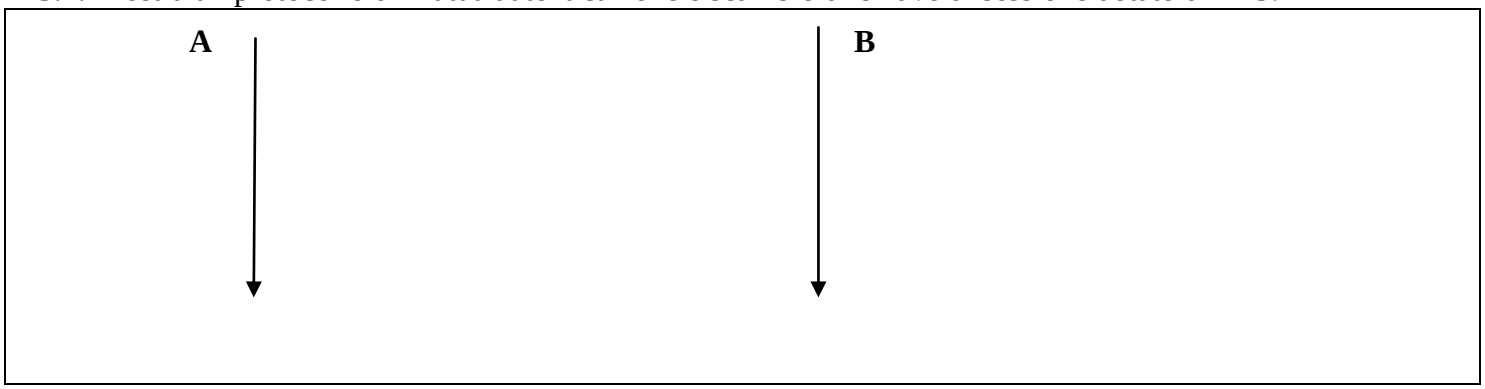
3. Perfect forward secrecy (PFS).

3.1. Cosa garantisce un protocollo dotato di PFS che un normale protocollo non garantisce?

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 9 febbraio 2018 – 4 CFU (la tesina vale 2 CFU)

3.2. Mostra un protocollo di mutua autenticazione e scambio di chiave di sessione dotato di PFS.



4. Network Intrusion Detection Systems (NIDS).

4.1. Elenca i componenti principali di un NIDS descrivendo brevemente ciascuno di essi.

4.2. Descrivi brevemente le problematiche di scalabilità di un NIDS e le tipologie di traffico più critiche.

4.3. Falsi positivi e falsi negativi: descrivi brevemente cosa sono e che problemi comportano.

5. Considera la tecnologia blockchain che è alla base di bitcoin. Rispondi alle seguenti domande sull'algoritmo di consenso noto come "proof of work".

5.1. Cosa deve riuscire a fare un nodo per aggiungere un blocco alla blockchain

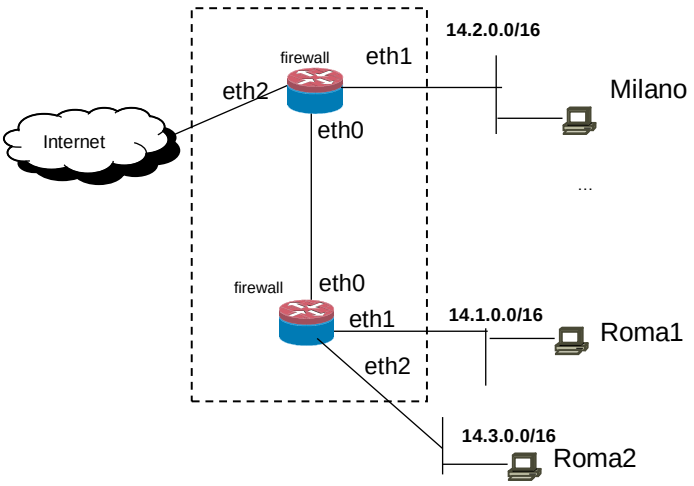
Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 9 febbraio 2018 – 4 CFU (la tesina vale 2 CFU)

5.2. Da che cosa si capisce che un certo nodo della rete è d'accordo circa un certo stato della blockchain?

5.3. Se un attaccante ha più del 50% della potenza di calcolo della rete, che attacco (o attacchi) può instaurare?

6. Considera la rete in figura. Non vi sono nat ed il routing è configurato correttamente. La policy di sicurezza, secondo cui il traffico tra le sedi è filtrato, è espressa dalla matrice di accesso mostrata. Fornisci una configurazione per i firewall di Roma e Milano per realizzare la policy preferibilmente usando la sintassi di netfilter.



A / **Da**	Roma1	Roma2	Milano	Internet
Roma1	-----		Q	
Roma2		-----		Q
Milano	R		-----	
Internet		R		-----

Roma

Milano