

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

Sicurezza dei sistemi informatici e delle reti – 17 luglio 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 – 17 luglio 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 – 17 luglio 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.

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

Sicurezza dei sistemi informatici e delle reti – 17 luglio 2019 – 4 CFU (la tesina vale 2 CFU)

**1. SQL injection.**

**1.1.** Spiega brevemente in cosa consiste una vulnerabilità di tipo SQL injection e fai un esempio mostrando anche una architettura di un sistema che può essere vulnerabile a SQL injection.

spiegazione SQL injection

esempio con architettura

**1.2.** Supponi di voler fare un vulnerability assessment su una form di un sito web. Come procedi per verificare l'esistenza di vulnerabilità SQL injection?

**1.3.** Cosa bisogna inserire nel codice per evitare che un sito sia vulnerabile a SQL injection?

**2. Controllo di accesso in UNIX.**

**2.1.** EUID vs. UID.

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

Sicurezza dei sistemi informatici e delle reti – 17 luglio 2019 – 4 CFU (la tesina vale 2 CFU)

2.2. Cosa distingue i processi *privilegiati* in UNIX? ad esempio quelli di root (ma non solo).

2.3. Set-user-id bit, cosa è e quando si usa?

2.4. Elenca tre cose che un processo privilegiato può fare che un normale processo non può fare.

3. Discuti brevemente i principi di progettazione “isolamento” e “semplicità”. Tra loro c’è una sinergia o un antagonismo? Spiega.

isolamento

semplicità

sinergia o antagonismo? Spiega.

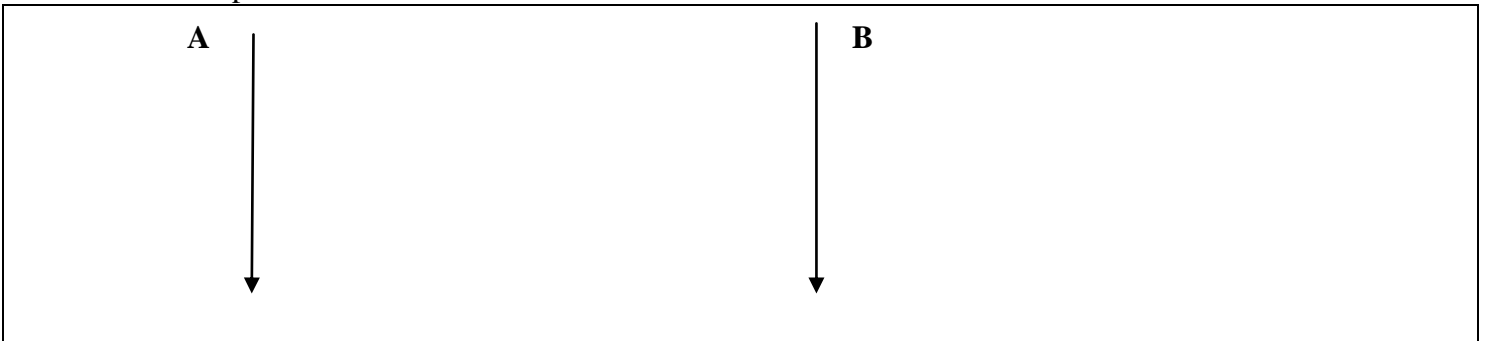


Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

Sicurezza dei sistemi informatici e delle reti – 17 luglio 2019 – 4 CFU (la tesina vale 2 CFU)

5.2. Supponi che la polizia debba intercettare una comunicazione tra A e B effettuata con un protocollo dotato di PFS e che la magistratura abbia fornito alla polizia i segreti a lungo termine (cioè le chiavi private) di A e B. Come procede?

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



6. Smart contracts.

6.1. Nel contesto di Bitcoin, descrivi i concetti di *locking e unlocking script*, le loro possibilità e i loro limiti.

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

Sicurezza dei sistemi informatici e delle reti – 17 luglio 2019 – 4 CFU (la tesina vale 2 CFU)

**6.2.** Nel contesto di Ethereum, descrivi il concetto di *account*, i tipi account, il loro ruolo in rapporto agli smart contract.

**6.3.** Descrivi il ciclo di vita di uno smart contract in Ethereum.



**Cognome:** \_\_\_\_\_ **Nome:** \_\_\_\_\_ **Matricola:** \_\_\_\_\_

**Sicurezza dei sistemi informatici e delle reti – 17 luglio 2019 – 4 CFU (la tesina vale 2 CFU)**