Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 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 – 20 settembre 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 – 20 settembre 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 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

2. Discuti brevemente i principi di progettazione "minimalità dei diritti" e "usabilità". Tra loro c'è una sinergia o un antagonismo? Spiega.

minimalità dei diritti

usabilità

sinergia o antagonismo? Spiega.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2018 – 4 CFU (la tesina vale 2 CFU)

3. Chiavi simmetriche

3.1. Quali sono i motivi per cui è consigliabile cambiare una chiave simmetrica anche se non è stata rivelata ad alcuno.

3.2. Se volessimo generare una nuova chiave simmetrica casualmente, che precauzioni dovremmo prendere nella scelta del generatore di numeri pseudo-casuali e nel suo utilizzo?

3.3. Che cosa significa key-rollover? fornisci un esempio di come si possa fare key rollover.

key-rollover.

esempio

4. Attacchi DDoS e contromisure.

4.1. Syn-flood. Che tipo di traffico viene inviato sulla rete? Perché tale traffico è un problema per il ricevente?

descrizione del traffico

effetti sul ricevente

4.2. Syn-proxy. Come agiscono? che vantaggio abbiamo ad adottarli?

come agiscono

vantaggi

4.3. Descrivi la contromisura nota come Syn-cookies.

5. Bitcoin, transazioni, UTXO.

5.1. Descrivi la struttura di una transazione, cosa sono gli UTXO e da dove vengono i fee per i miners legati a quella transazione.

struttura e UTXO

fee

5.2. Quando una transazione *spende* dei bitcoin cosa fornisce per provare che chi ha creato la transazione è il proprietario dei bitcoin? Spiega.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2018 – 4 CFU (la tesina vale 2 CFU)

6. Gli attacchi al login possono essere classificati in on-line (in cui il prompt di login è accessibile via rete) e off-line (in cui il database utenti/password è disponibile in locale all'attaccante con gli hash delle password). Compila la seguente tabella.

	On-line	Off-line
Che contromisure suggerisci per i due tipi di attacchi?		
Quali sono secondo te le criticità o difficoltà principali per l'attaccante?		
Quali sono secondo te le criticità o difficoltà principali per chi deve mitigare il rischio di un tale tipo di attacchi?		