

Cognome: _____ Nome: _____ Matricola: _____

Cybersecurity – 8 luglio 2022 – 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:** _____

Cybersecurity – 8 luglio 2022 – 4 CFU (la tesina vale 2 CFU)

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

Cognome: _____ Nome: _____ Matricola: _____

Cybersecurity – 8 luglio 2022 – 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. Analisi dei rischi

1.1. Considera la pianificazione della sicurezza, ed in particolare la fase di analisi del rischio. Che documento produce questa fase? Descrivilo. Perché l'analisi del rischio è importante? In che rapporto è questa fase con la parte di progetto di contromisure?

Output dell'analisi del rischio
Importanza
Rapporto con le contromisure

1.2. Considera il piano impatto-frequenza (alle volte anche detto impatto-probabilità) del singolo evento avverso legato ad un rischio. Usa tale schema per descrivere, a parole e graficamente, tutti i vari casi che si pongono circa il trattamento dei rischi.

--

Cognome: _____ Nome: _____ Matricola: _____

Cybersecurity – 8 luglio 2022 – 4 CFU (la tesina vale 2 CFU)

2. Network Intrusion Detection Systems (NIDS).

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

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

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

3. Hash crittografici.

3.1. Descrivi brevemente cosa è un hash crittografico e in dettaglio la sua proprietà di non invertibilità.

breve descrizione

proprietà di non invertibilità

Cognome: _____ Nome: _____ Matricola: _____

Cybersecurity – 8 luglio 2022 – 4 CFU (la tesina vale 2 CFU)

3.2. Descrivi la tecnica nota come rainbow tables per attaccare la proprietà di non invertibilità.

4. **Sicurezza del codice: persistent cross site scripting (XSS).** Considera una architettura a tre livelli composta dai seguenti elementi architettureali: client web, application server, database. Descrivi l'attacco persistent XSS mostrando le elaborazioni fatte da ciascun elemento architettureale e descrivendo i suoi dati di input e di output durante l'attacco. Metti in luce gli aspetti critici per la sicurezza. Cerca di spiegare alcuni dettagli tecnici che pensi siano rilevanti. Se pensi sia utile, puoi fare ulteriori ipotesi sull'architettura ma rendile esplicite nelle risposte.

Cognome: _____ Nome: _____ Matricola: _____

Cybersecurity – 8 luglio 2022 – 4 CFU (la tesina vale 2 CFU)

5. Protocolli AAA.

5.1. A che serve un protocollo AAA? Rispondi in astratto (gli esempi sono richiesti nel prossimo punto).

5.2. Per ciascuna “A” fornisci una esempio di una realizzazione tecnologica o commenta un aspetto tecnologico rilevante.

- A.....
Esempio o aspetto tecnologico.

- A.....
Esempio o aspetto tecnologico.

- A.....
Esempio o aspetto tecnologico.

6. Blockchain e consenso.

6.1. Spiega il concetto di consenso in astratto ed il suo ruolo nell’ambito di una qualsiasi blockchain.

Cognome: _____ Nome: _____ Matricola: _____

Cybersecurity – 8 luglio 2022 – 4 CFU (la tesina vale 2 CFU)

6.2. Spiega come funziona il consenso di Bitcoin, cioè il cosiddetto proof-of-work.

6.3. Spiega l'attacco Eclipse.