

Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 12 giugno 2017

Nome

Cognome

1. Descrivere il concetto di DDOS (distributed denial of service)

2a. Per effettuare un'analisi del rischio secondo la metodologia OWASP, si utilizza la formula:

- A) Probabilità = $f(\text{gravità del rischio, vulnerabilità})$
- B) Gravità del rischio = $f(\text{probabilità, impatto})$
- C) Probabilità = $f(\text{agente della minaccia, impatto})$
- D) Impatto = $f(\text{impatto tecnologico, probabilità})$
- E) Gravità del rischio = $f(\text{impatto tecnologico, impatto di business})$

2b. In una VPN "tunnel"

- A) è tutto cifrato, tranne il MAC address
- B) l'indirizzo IP del solo terminatore sorgente è cifrato
- C) gli indirizzi IP di entrambi i terminatori sono cifrati
- D) il reale indirizzo IP sorgente è cifrato
- E) il reale indirizzo IP sorgente è in chiaro

3. Definire e illustrare graficamente il concetto di "Merkle Tree"

4. Spiegare il "bit s" nel controllo di accesso ai sistemi Unix, e perché può essere pericoloso in presenza di vulnerabilità di un eseguibile

5. Algoritmo iterativo per calcolare in modo efficiente l'esponente modulare e sua complessità