Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 14 luglio 2017

Nome Cognome

1. Descrivere il ciclo Plan-Do-Check-Act secondo lo standard ISO-27001

2a. Nel contesto della "Blockchain":

A) In ogni momento una sola blockchain è valida

B) In ogni momento sono valide più blockchain che condividono una sottocatena iniziale

C) La blockchain è resa valida dalla firma di una terza parte fidata

D) La blockchain è resa valida da un voto di maggioranza sulla rete peer to peer

E) La blockchain è resa valida da un MAC (message authentication code)

2b. Un firewall con HA (High Availability):

A) È normalmente realizzato in una configurazione con load-balancing

B) È normalmente realizzato in una configurazione con DNS round-robin

C) È normalmente realizzato in una configurazione con fail-over

D) È un firewall application-aware

E) È un firewall di tipo packet-filter che evita la perdita di pacchetti

3. Definire il metodo di scambio di chiavi di Diffie-Hellman

4. Discutere, nel metodo di scambio di chiavi di Diffie-Hellman come descritto nella domanda 3, la complessità computazionale di ciascun passo

5. Descrivere il protocollo ESP (encapsulating security payload) nelle reti private virtuali IPSEC