Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 14 luglio 2017

Nome Cognome

Numero documento

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

2a. Nel contesto della “Blockchain”:

1. In ogni momento una sola blockchain è valida
2. In ogni momento sono valide più blockchain che condividono una sottocatena iniziale
3. La blockchain è resa valida dalla firma di una terza parte fidata
4. La blockchain è resa valida da un voto di maggioranza sulla rete peer to peer
5. La blockchain è resa valida da un MAC (message authentication code)

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

1. È normalmente realizzato in una configurazione con load-balancing
2. È normalmente realizzato in una configurazione con DNS round-robin
3. È normalmente realizzato in una configurazione con fail-over
4. È un firewall application-aware
5. 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