Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 2 settembre 2016

Nome Cognome

Numero documento

1. Descrivere il metodo ricorsivo per il calcolo dell'esponente modulare e discuterne la complessità

2a.: La tecnica nota come ARP poisoning

A) realizza un buffer overflow sul server ARP

B) realizza un buffer overflow sul firewall

C) invia una risposta ARP con indirizzi IP modificati

D) invia una risposta ARP con indirizzi MAC modificati

E) invia una risposta ARP causando un buffer overflow

2b. il Syn flooding

A) è un attacco di buffer overflow

B) è un attacco DOS che può essere utilmente abbinato ad IP spoofing

C) è un attacco DOS, non abbinabile ad IP spoofing

D) richiede una modifica del layer TCP del server

E) permette di modificare i cookie di sessione

3. Dimostrare che esistono infiniti numeri primi e discuterne le conseguenze in crittologia

4. Discutere il concetto di non disconoscibilità nella firma elettronica

5. Descrivere il concetto di DMZ, con una possibile topologia di rete, e spiegare perché è utile per la sicurezza di una rete locale