



Università degli Studi di Verona, Dipartimento di Informatica
Programmazione di Rete, A.A. 2014/2015
Appello d'esame del 18 Febbraio 2016

- L'esame consiste di due parti; ciascuna parte è composta da un esercizio e alcune domande.
- Lo studente svolga Parte I e Parte II su fogli distinti per permetterne la correzione in parallelo.
- Su ciascun foglio scrivere **nome, cognome** e **numero di matricola** (non è obbligatorio consegnare la brutta copia)
- I risultati verranno pubblicati sugli avvisi della pagina del corso **Martedì 23 Febbraio dopo le 19:00**
- La correzione dei temi d'esame può essere visionata durante la registrazione o il ricevimento docenti
- **Orali** (facoltativi a meno di una richiesta esplicita dei docenti) e **registrazioni** si terranno **Mercoledì 24 Febbraio alle 10:00 in Aula G**

I Parte

Esercizio 1 (8 punti)

Implementare un servizio semplificato di web proxy. Il client si collega al proxy sulla porta 8000, gli comunica un URL, riceve la corrispondente pagina web (solo HTML) e stampa a video il contenuto HTML. Il proxy deve gestire molti client contemporaneamente. Si discuta:

1. la scelta del protocollo di livello trasporto nella comunicazione tra i client e il web proxy;
2. il possibile ruolo di un tale proxy ai fini della sicurezza dei client che ne fanno uso.

Domande (2 punti ciascuna)

Si risponda in maniera sintetica e concisa (poche frasi per risposta sono sufficienti) alle seguenti domande:

1. Cos'è un URL? Qual è la sua sintassi?
2. Quali vulnerabilità presentano gli switch per quanto riguarda la sicurezza?
3. Qual è il principio di funzionamento della fibra ottica?

II Parte

Esercizio 3 (7 punti)

Un dipartimento di un'Università disposto su un singolo piano ospita gli studi sia dei docenti strutturati (circa 20), che dei docenti esterni (circa 10). Il dipartimento è collegato agli altri dipartimenti con un router, che rappresenta il router di default per la rete di dipartimento. Per motivi organizzativi, il traffico generato dai docenti strutturati non deve poter essere catturato a livello 2 dai calcolatori dei docenti esterni. Tuttavia, i vari calcolatori devono essere in grado di comunicare tra loro a livello IP.

Per lo scenario sopra descritto si mostrino

1. Lo schema della rete, indicando gli apparati usati con il loro numero di porte, e gli indirizzi assegnati ai due gruppi di docenti (la scelta è arbitraria e funzionale al secondo punto; non serve scrivere nessun comando per gli apparati di rete);
2. Per il router di default, i comandi necessari per permettere ai due gruppi di docenti di comunicare tra di loro.

Domande (4 punti ciascuna)

Si risponda, elaborando quanto più possibile, alle seguenti domande:

1. Si descriva lo schema di crittografia a chiave **asimmetrica** e come esso viene utilizzato nella comunicazione tra due entità.
2. Si descriva il funzionamento del Message Authentication Code (MAC) per l'autenticazione di un messaggio (non è necessario garantire la confidenzialità dei dati).
3. Un sistema di rilevamento delle intrusioni (IDS, Intrusion Detection System) si può basare su diversi modelli: rilevamento della anomalie, oppure rilevamento di uso malevolo, oppure rilevamento in base a specifiche. Si spieghi il principio di funzionamento di uno tra questi modelli, anche attraverso esempi.