Università degli Studi di Verona, Dipartimento di Informatica

Programmazione di Rete, A.A. 2014/2015

Appello d'esame del …

- 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 ***Giorno/Mese e orario***
- 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 ***Giorno/Mese, orario e luogo***

I Parte

Esercizio 1 (8 punti)

Un server implementa un servizio di bacheca elettronica, dove gli utenti appartenenti ad un gruppo possono scrivere dei messaggi e tali messaggi vengono visualizzati dagli altri utenti del gruppo. Per motivi tecnologici, il server non dispone del servizio di PUSH, e i client non possono stare connessi tutto il tempo al server, ma si connetteranno periodicamente per controllare se ci sono nuovi messaggi da scaricare. Il ritardo nel ricevere i messaggi non è un parametro di prestazioni importante. Nell fase di invio dei messaggi, invece, l'utente che ha creato il messaggio deve essere sicuro che il messaggio sia arrivato sul server.

Dati questi requisiti si chiede di:

1. Scrivere il codice in Java lato client e lato server per implementare l'invio dei messaggi sulla bacheca elettronica, giustificando le scelte fatte.
2. Scrivere il codice in Java lato client e lato server per implementare la ricezione dei messaggi presenti sulla bacheca elettronica, giustificando le scelte fatte.

Domande (2 punti ciascuna)

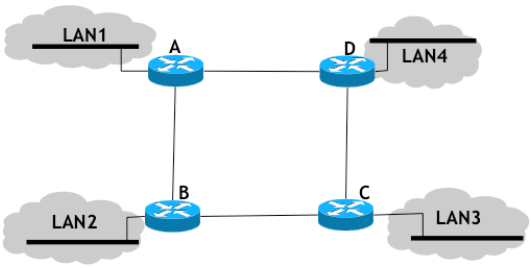
Si risponda in maniera sintetica e concisa (poche frasi per risposta sono sufficienti) alle seguenti domande:

1. Che cos'è e a cosa server un application server (o application container o web container)?
2. Cosa si può notare in Wireshark quando i pacchetti appartengono ad una connessione sicura (ad es. HTTPS o SSH)?
3. A cosa serve e come funziona l'algoritmo/protocollo spanning tree?

II Parte

Esercizio 3 (7 punti)

Una rete privata è formata da 4 router come mostrato in figura. Ciascun router si interfaccia verso una rete con indirizzo 192.168.x.0/24, dove x= 1,2,3,4, mentre i blocchi 192.168.255.y/30 dove y = 252, 248, 244 e 240 vengono usati per i collegamenti tra i router.



Si mostrino

1. Gli assegnamenti dei vari indirizzi alle reti, inclusi i collegamenti;
2. Per uno dei router, i comandi necessari per assegnare gli indirizzi alle diverse interfacce e per abilitare il routing con il protocollo RIP.

Domande (4 punti ciascuna)

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

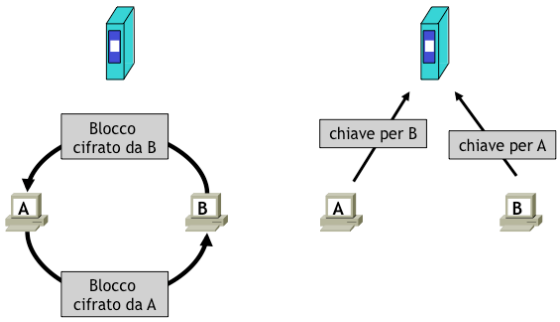
1. Si dia una breve spiegazione di ciascuno dei tre principali obiettivi della sicurezza (confidenzialità, integrità, disponibilità), anche con l'aiuto di esempi che mostrino come tali proprietà possano essere compromesse.
2. Si descrivano gli elementi che costituiscono il processo crittografico e, nel caso di crittografia a chiave simmetrica, si mostri un esempio di un semplice sistema crittografico.
3. Si mostri uno dei possibili modi in cui può essere garantita l'autenticità di un messaggio.

Programmazione di Rete, A.A. 2014/2015
Appello d'esame del …

- 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 ***Giorno/Mese e orario***
- 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 ***Giorno/Mese, orario e luogo***

I Parte

Esercizio 1 (8 punti)



Si consideri un'applicazione di scambio di file tra utenti, dove i file sono suddivisi in blocchi di uguale dimensione. Dato un file, ciascun utente possiede un sottoinsieme di blocchi e desidera ottenere gli altri blocchi dagli altri utenti per completare il file. L'applicazione cerca di imporre uno schema di condivisione equo delle risorse; in particolare, si vuole assicurare che se l'utente A manda un blocco all'utente B anche l'utente B manderà un blocco all'utente A. Per fare questo, A cifra il blocco con una chiave generata a caso e B farà lo stesso con un'altra chiave. A e B poi si scambieranno i blocchi e, in un secondo momento, si scambieranno le chiavi per decifrarli. Lo scambio delle chiavi deve essere sincrono, ovvero A deve essere certo di ricevere la chiave da B nel momento in cui invia la propria chiave. Per far questo, A e B si appoggiano ad un server per la fase di scambio di chiavi.

Dati questi requisiti si chiede di implementare la porzione di codice relativa allo scambio di chiavi, sia lato server che lato client, giustificando le scelte implementative (il server deve gestire sempre coppie di utenti che si devono scambiare le rispettive chiavi).

Domande (2 punti ciascuna)

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

1. Che cos'è e a cosa serve il protocollo SOAP?
2. In Wireshark, che differenza c'è tra filtro di cattura e filtro di visualizzazione?
3. Che differenza c'è tra UTP dritto e incrociato? Che ruoli hanno questi tipi di cavo?

II Parte

Esercizio 2 (7 punti)

Un'università ha organizzato la propria rete in Dipartimenti; ciascun Dipartimento fornisce prese di rete per i docenti afferenti al Dipartimento, per il personale dell'amministrazione e per i laboratori didattici. Gli amministratori di rete intendono tenere separati questi tre gruppi di utenti, ciascuno dei quali avrà al più 100 postazioni. I dipartimenti comunicano tra di loro con una rete IP la cui connettività è fornita da un ISP locale.

Si mostrino:

1. Lo schema della rete di un Dipartimento, con gli apparati usati (la scelta sul numero di porte di ciascun apparato è lasciata allo studente, l'importante e che il numero totale di porte sia sufficiente per rispondere alle esigenze di ciascun Dipartimento);
2. Le operazioni da eseguire sugli apparati per garantire la separazione tra i diversi gruppi di utenti.

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 attraverso quali meccanismi vengono controllati gli accessi alle risorse di un sistema (ad esempio, file, directory, programmi), dopo che l'utente si è correttamente autenticato.
3. L'architettura di IDS (Intrusion Detection System) è formata da tre elementi principali: Agente, Direttore e Notificatore. Si descrivano i principali compiti di tali elementi.