Sicurezza e Privatezza

Docente: Prof. Pierangela Samarati

Appello di Aprile - 1 Aprile 2004

Tempo a disposizione 2:30h

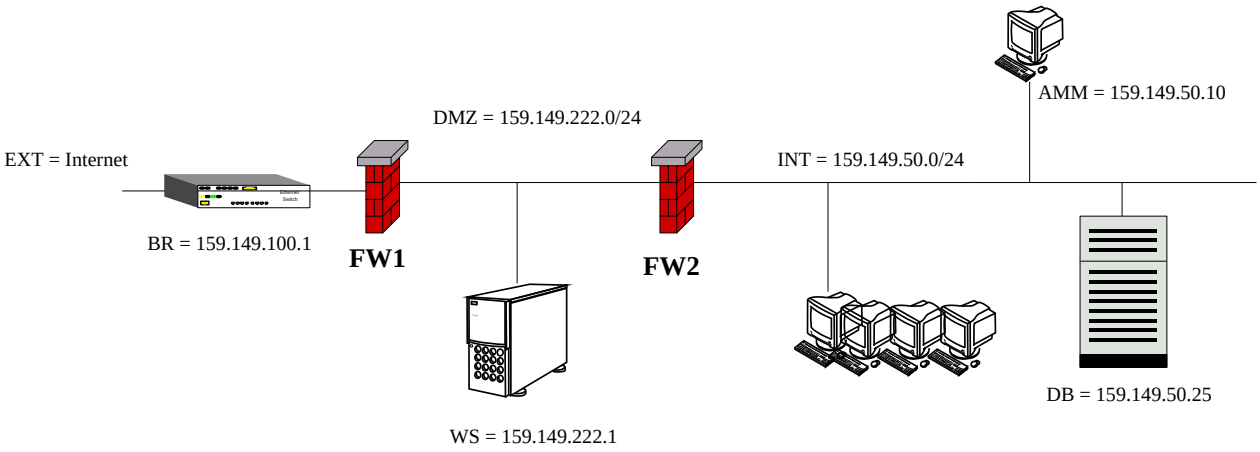
Domanda 1)
Definire il concetto di *politiche di sicurezza* evidenziando le differenza tra quelle per il controllo dell'accesso e per l'amministrazione. Si richiede inoltre di descrivere le politiche DAC, MAC e RABC descrivendo, per le MAC e DAC, un esempio di modello.

Domanda 2)
Rispondere brevemente, ma in modo completo, alle seguenti domande.

1. Descrivete sinteticamente in cosa consiste una vulnerabilità di tipo buffer overflow.
2. Descrivete le caratteristiche e gli effetti di un ACK scan.
3. Descrivere in che modo le tecniche crittografiche sono in grado di garantire i seguenti servizi di sicurezza:
   (a) riservatezza
   (b) integrità e autenticazione
   (c) non ripudiabilità
4. Dire cosa si intende per cifrari a sostituzione monoalfabetici, polialfabetici e cifrari a trasposizione.
5. Nell'ambito del cifrario RSA illustrare perché fattorizzare efficientemente è equivalente a forzare efficientemente RSA. È vero anche il viceversa?
6. Dire cosa si intende per Cavallo di Troia ed illustrare un esempio.
7. Nell'ambito della politica chinese wall, illustrare gli assiomi *simple security rule* e **-property*.

Esercizio 1)

Una rete aziendale è protetta da due firewall (FW1 e FW2) in cascata di tipo static packet filter avente ognuno due interfacce di rete.



Internet può essere indicata con **EXT**. Esternamente a FW1 vi è un Border Router (indicato con **BR**) con indirizzo 159.149.100.1 con il servizio SSH (22/tcp) abilitato. La sottorete **DMZ** tra i due firewall ha indirizzi 159.149.222.0/24. In questa sottorete vi è un Web Server (indicato con **WS**) con indirizzo 159.149.222.1 con il servizio HTTP (80/tcp) abilitato. La rete interna **INT** ha indirizzi 159.149.50.0/24. Nella rete interna vi sono un numero di postazioni di lavoro e server generici. Tra questi identifichiamo una postazione di amministrazione (indicata con **AMM**) avente indirizzo 159.149.50.10 e un Database Server (indicato con **DB**) avente indirizzo 159.149.50.25. Il Database Server **DB** ha il servizio SQLnet (1521/tcp) attivo.

Si definiscano le politiche di sicurezza di FW1 e FW2 per autorizzare le seguenti connessioni:

1. Client da Internet devono poter accedere alle pagine del Web Server aziendale (**WS**).
2. Client generici della rete interna INT devono potere accedere a Web server pubblici su Internet.
3. La postazione dell'amministratore di sistema **AMM** deve poter accedere al Border Router (**BR**) via SSH per motivi di gestione. Nessun altro deve poterlo fare.
4. il Web Server **WS**, attraverso suoi script, deve poter accedere al Database Server **DB** via SQLnet.
5. Ogni altra connessione, in ingresso o in uscita, sia per FW1 che per FW2, non esplicitamente prevista dai punti precedenti deve essere impedita (scrivere regole).

NOTA1: Utilizzate le tabelle allegate (il numero di righe non è indicativo)
NOTA2: Oltre alla compilazione della tabella è obbligatorio descrivere in maniera precisa il significato di OGNI regola definita in tabella (il significato del valore assegnato all'ACK, in particolare).

Esercizio 2)
Si considerino le seguente operazioni di GRANT, dove ciascuna operazione è preceduta dal tempo in cui è richiesta e dall'utente che la ha richiesta.
10, Alice: GRANT Select ON Impiegati TO Bob WITH GRANT OPTION
15, Alice: GRANT Select ON Impiegati TO Carol WITH GRANT OPTION
20, Carol: GRANT Select ON Impiegati TO Bob
30, Carol: GRANT Select ON Impiegati TO Dave WITH GRANT OPTION
40, Bob: GRANT Select ON Impiegati TO Elen WITH GRANT OPTION
50, Dave: GRANT Select ON Impiegati TO Elen
60, Dave: GRANT Select ON Impiegati TO Frank WITH GRANT OPTION
70, Alice: GRANT Select ON Impiegati TO Dave WITH GRANT OPTION

si richiede di:

1. costruire il corrispondente grafo delle dipendenze;

2. costruire il grafo delle dipendenze che si ottiene dopo aver eseguite le seguenti operazioni di REVOKE con cascata:
   18, Alice REVOKE Select ON Impiegati FROM Bob
   45, Carol REVOKE Select ON Impiegati FROM Dave
   nei casi in cui (1) l'operazione di revoca tenga conto dei tempi e (2) l'operazione di revoca non tenga conto dei tempi;

3. con riferimento ai casi (1) e (2) del punto precedente, specificare in quali istanti di tempo (a) Bob può eseguire una operazione di Select sulla relazione Impiegati e l'operazione "GRANT Select ON Impiegati TO Gary" WITH GRANT OPTION; (b) Dave può eseguire l'operazione "GRANT Select ON Impiegati TO Gary"

(MATRICOLA) (COGNOME) (NOME)

Tabelle per l’Esercizio 1)

Regole FW1

Num.	Direzione	Azione	Prot.	Ind. IP Sorgente	Porta Sorgente	Ind. IP Destin.	Porta Destin.	Flag ACK
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

Regole FW2

Num.	Direzione	Azione	Prot.	Ind. IP Sorgente	Porta Sorgente	Ind. IP Destin.	Porta Destin.	Flag ACK
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								