Sicurezza e Privatezza

Docente: Prof. Pierangela Samarati

Appello di Febbraio - 18 Febbraio 2004

Tempo a disposizione 2:30h

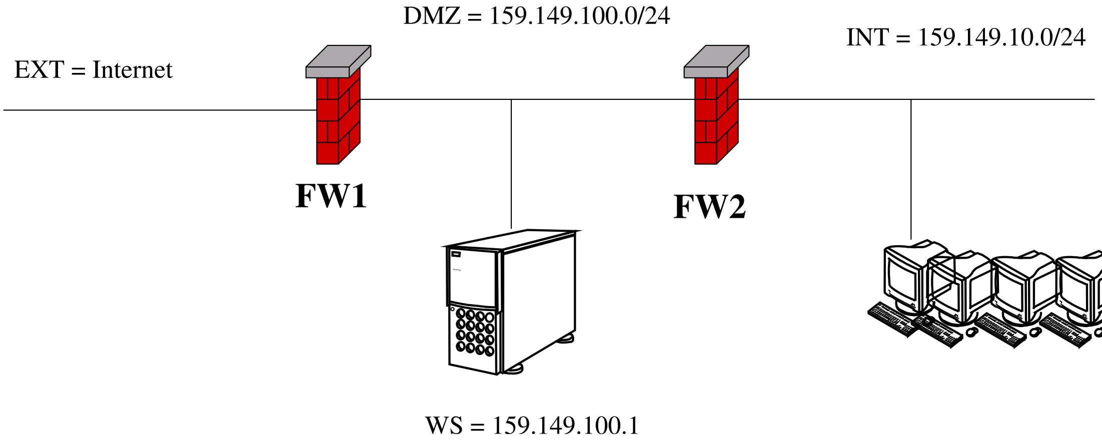
Domanda 1)
Discutere l'applicazione di politiche mandatorie alle basi di dati. In particolare si richiede di:

1. definire il modello relazione multilivello con classificazione a livello di elemento (esistono altri livelli di classificazione?);
2. descrivere in modo completo e fornire esempi relativi al problema della *poliinstanziazione*;
3. descrivere possibili tecniche che possono essere adottate per prevenire la poliinstanziazione.

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

1. Descrivere il concetto di finestra temporale di esposizione di un sistema in relazione al ciclo di vita tipico di una vulnerabilità. Da quali fattori dipende l'ampiezza di tale finestra?
2. Considerate il seguente testo: "Un annuncio relativo al SistemaXY indica che la generazione casuale del TCP ISN (Initial Sequence Number) è predicibile". Che tipo di problema di sicurezza vi fa venire in mente? Descrivetene sinteticamente le caratteristiche principali.
3. In relazione al problema della sicurezza delle password dire cosa si intende per:
   - spoofing
   - snooping
   - sniffing
   - masqueranding
4. Concetti di storage, timing e covert channel.
5. Dire cosa sono i link referenziali e i cookie.
6. A cosa serve la firma digitale e quali proprietà deve soddisfare.
7. Descrivere le differenze tra i cifrari simmetrici e asimmetrici illustrando vantaggi e svantaggi.

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.



La sottorete **DMZ** tra i due firewall ha indirizzi 159.149.100.0/24 e vi è un host con indirizzo 159.149.100.1. Tale host (indicato con **WS**) agisce da Web Server (80/tcp) e ha il servizio SSH (22/tcp) abilitato. La rete interna **INT** ha indirizzi 159.149.10.0/24. Internet puo' essere indicata con **EXT**.

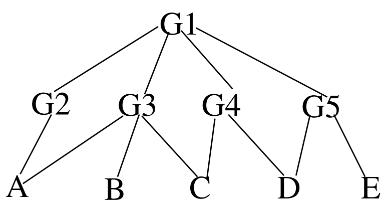
Si definisca una politica di sicurezza per autorizzare le seguenti connessioni:

1. Client da Internet devono poter accedere al Web server aziendale (**WS**) per visualizzarne le informazioni.
2. Client della rete interna INT devono potere accedere a Web server pubblici su Internet e visualizzarne le informazioni.
3. La postazione dell'amministratore di sistema con indirizzo 159.149.10.65 deve poter accedere al Web server aziendale (**WS**) via SSH per motivi di gestione. Nessun altro deve poterlo fare.
4. Ogni altra connessione, in ingresso o in uscita, 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)
Data la seguente gerarchia di gruppi e le autorizzazioni:
(G1,+,read,file1); (G3,+,read,file1); (G4,-,read,file1); (G5,-,read,file1)



Dire quali autorizzazioni si applicano ai singoli utenti secondo le politiche: *denials take precedence* (dtp); *most specific takes precedence* (mstp); *most specific along a path takes precedence* (mslptp). Si richiede di eseguire l'esercizio compilando la tabella allegata.

(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								

(MATRICOLA) (COGNOME) (NOME)

Tabella per l'Esercizio 2)

Si richiede di inserire all'interno di ogni casella il segno (o segni) delle autorizzazioni applicabili all'utente.

Utente	dtp	mstp	mslptp
A			
B			
C			
D			
E			