Sicurezza e Privatezza

Docente: Prof. Pierangela Samarati

Appello di Settembre - 12 Settembre 2003

Tempo a disposizione 2:30h

Domanda 1)

Discutere il problema della integrità e descrivere un modello il cui obiettivo e salvaguardare l'integrità.

Domanda 2)

Discutere le vulnerabilità e limitazioni delle politiche discrezionali e delle politiche mandatorie.

Domanda 3)

Rispondere brevemente, ma in modo completo, alle seguenti domande.

1. Cosa si intende con EGRESS e INGRESS FILTERING? Che problemi di sicurezza tendono a limitare queste due tecniche?
2. Descrivere in sintesi le caratteristiche principali di un Trojan Horse e l'evoluzione nelle tecniche di comunicazione che questi sistemi hanno mostrato.
3. Spiegare quali sono le principali criticità per la sicurezza di una rete poste dall'uso di Wireless LAN 802.11.
4. Descrivere il concetto di funzione hash one-way ed illustrare il suo utilizzo nell'ambito delle firme digitali.
5. Dire cosa si intende per crittosistema incondizionato sicuro e computazionalmente sicuro. Fornire un esempio di entrambi i crittosistemi.
6. Descrivere le operazioni di cifratura e decifratura dell'algoritmo crittografico RSA. La sicurezza di RSA su quale problema matematico si fonda?
7. Definire la politica aperta e la politica chiusa. Indicare per quale ragione si considerano le autorizzazioni negative ed i problemi che queste portano.
8. Fare un esempio di separazione dei privilegi statico e dinamico.

Esercizio 1)
Si svolgano in maniera esaustiva i seguenti punti.

1. Supponete di avere rilevato una traccia come quella sotto riportata (la classe 159.179 rappresenta la vostra rete). Analizzatela descrivendo il tipo di traffico e le anomalie rispetto a normali connessioni TCP.

   ```
   Traccia rilevata:
   May 1 17:44:57 66.87.26.63:0 -> 159.179.0.1:21 SYN FIN
   May 1 17:44:57 66.87.26.63:0 -> 159.179.0.2:21 SYN FIN
   May 1 17:44:57 66.87.26.63:0 -> 159.179.0.3:21 SYN FIN
   May 1 17:44:57 66.87.26.63:0 -> 159.179.0.4:21 SYN FIN
   [...] seguono molti altri analoghi [...]
   May 1 17:51:49 66.87.26.63:0 -> 159.179.255.247:21 SYN FIN
   May 1 17:51:49 66.87.26.63:0 -> 159.179.255.248:21 SYN FIN
   May 1 17:51:49 66.87.26.63:0 -> 159.179.255.249:21 SYN FIN
   May 1 17:51:49 66.87.26.63:0 -> 159.179.255.250:21 SYN FIN
   [...] seguono molti altri analoghi [...]
   May 1 18:48:47 61.0.139.122:0 -> 159.179.12.36:139 SYN FIN
   May 1 18:48:42 61.0.139.122:0 -> 159.179.12.37:139 SYN FIN
   May 1 18:48:44 61.0.139.122:0 -> 159.179.12.38:139 SYN FIN
   May 1 18:48:45 61.0.139.122:0 -> 159.179.12.39:139 SYN FIN
   [...] seguono molti altri analoghi [...]
   May 1 18:53:54 61.0.139.122:0 -> 159.179.31.32:139 SYN FIN
   May 1 18:53:52 61.0.139.122:0 -> 159.179.31.19:139 SYN FIN
   May 1 18:53:53 61.0.139.122:0 -> 159.179.31.27:139 SYN FIN
   May 1 18:53:53 61.0.139.122:0 -> 159.179.31.31:139 SYN FIN
   May 1 18:53:53 61.0.139.122:0 -> 159.179.31.33:139 SYN FIN
   [...] seguono molti altri analoghi [...]
   ```

2. Descrivere le anomalie rispetto gli standard TCP/IP del traffico di rete presentato e i motivi per cui può essere generato.

3. Definire una politica di sicurezza di tipo packet filter per limitare scanning come quello precedente. In particolare volete che:

   (a) siano permesse connessioni HTTP al vostro Web server (porta 80) da qualunque indirizzo esterno (il vostro sito web deve poter essere visualizzato da chiunque);

   (b) siano permesse connessioni a server SSH (porta 22) esterni alla vostra rete ma non connessioni da client esterni a server SSH interni.

   (c) altre tipologie di connessioni vanno impedite.

   Utilizzate la tabella allegata (il numero di righe non è indicativo) e descrivete in maniera precisa ed esauriente il significato di ogni regola che avete definito e di come complessivamente esse soddisfino la politica di sicurezza richiesta.

Esercizio 2)
Si considerino i seguenti livelli di segretezza `Privato`, `Confidenziale`, `Divulgativo`, dove `Privato` $>$ `Confidenziale` $>$ `Divulgativo` e il seguente insieme di categorie {OrdinePubblico,Amministrazione}. Definire la politica mandatoria per la segretezza delle informazioni, indicando le classi di accesso, la relazione fra di esse e il reticolo risultante. Definire i flussi di informazioni permessi e dare un esempio di flusso di informazione non permesso dalla politica.

(MATRICOLA) (COGNOME) (NOME)

Tabella per l’Esercizio 1)

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								