Sicurezza e Privatezza

Docente: Prof. Pierangela Samarati

Appello di Luglio - 4 Luglio 2003

Tempo a disposizione 2:00h

Domanda 1)
Descrivere dettagliatamente il funzionamento del crittosistema DES (non è richiesta la presentazione delle tabelle di permutazione, espansione e delle s-box). Descrivere le varianti del DES viste a lezione (DES doppio e triplo DES) e dire perché sono state introdotte. Si richiede inoltre di illustrare l'attacco meet in the middle applicato al doppio DES.

Domanda 2)
Spiegare il concetto di autenticazione e discutere le principali tecniche di autenticazione conosciute.

Domanda 3)
Rispondere in modo breve ma completo alle seguenti domande:

1. Cosa si intende con IP Spoofing? Quali contromisure si possono adottare per limitarne l'impiego?
2. Descrivere in sintesi le caratteristiche principali di un Trojan Horse.
3. Spiegare in sintesi quali conseguenze per la sicurezza può implicare una erronea validazione dei dati di input di una applicazione Web.
4. Che differenza c'è tra chiave privata e chiave pubblica?
5. Cosa sono i cifrari affini? A che tipo di attacchi sono vulnerabili?
6. Cosa si intende per crittosistema ibrido?
7. Nell ambito delle politiche per il controllo dell accesso, caratterizzare il principio del minimo privilegio (least privilege) e spiegare la differenza fra gruppi e ruoli.
8. Dire cosa sono i link referenziali e i cookie.

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 66.87.26.63:21 -> 159.179.0.1:21 SYN
May 1 17:44:57 66.87.26.63:21 -> 159.179.0.2:21 SYN
May 1 17:44:57 66.87.26.63:21 -> 159.179.0.3:21 SYN
May 1 17:44:57 66.87.26.63:21 -> 159.179.0.4:21 SYN
[...] seguono molti altri analoghi [...]
May 1 17:51:49 66.87.26.63:21 -> 159.179.255.247:21 SYN
May 1 17:51:49 66.87.26.63:21 -> 159.179.255.248:21 SYN
May 1 17:51:49 66.87.26.63:21 -> 159.179.255.249:21 SYN
May 1 17:51:49 66.87.26.63:21 -> 159.179.255.250:21 SYN
[...] seguono molti altri analoghi [...]
May 1 18:48:47 61.0.139.122:1332 -> 159.179.12.36:139 SYN
May 1 18:48:42 61.0.139.122:1333 -> 159.179.12.37:139 SYN
May 1 18:48:44 61.0.139.122:1334 -> 159.179.12.38:139 SYN
May 1 18:48:45 61.0.139.122:1335 -> 159.179.12.39:139 SYN
[...] seguono molti altri analoghi [...]
May 1 18:53:54 61.0.139.122:3625 -> 159.179.31.32:139 SYN
May 1 18:53:52 61.0.139.122:3602 -> 159.179.31.19:139 SYN
May 1 18:53:53 61.0.139.122:3616 -> 159.179.31.27:139 SYN
May 1 18:53:53 61.0.139.122:3622 -> 159.179.31.31:139 SYN
May 1 18:53:53 61.0.139.122:3627 -> 159.179.31.33:139 SYN
[...] seguono molti altri analoghi [...]
```

2. Descrivere i motivi per cui può essere eseguita una tale attività di scanning. Descrivete inoltre le caratteristiche di almeno una ulteriore tecnica di scanning di vostra conoscenza.
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 al vostro server SSH (porta 22) solo dalla sottorete esterna 80.23.16 appartenente ad una vostra sede decentrata;
   (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)
Data la seguente relazione multilivello

Nome	λ_N	**Cognome**	λ_C	**Dip**	λ_D	**Stipendio**	λ_S
Anna	S	Bianchi	S	Ammin	U	100K	U
Gianni	S	Verdi	S	Ricerca	S	100K	U
Gianni	S	Verdi	S	Sviluppo	TS	100K	U
Gianni	U	Verdi	U	Ammin	U	100K	U
Anna	S	Bianchi	S	Ricerca	S	200K	S
Dario	U	Gialli	U	Ammin	U	150K	U
Dario	U	Gialli	U	Ricerca	S	150K	U
Anna	TS	Bianchi	TS	Ricerca	S	200K	S
Gianni	S	Verdi	TS	Dept5	TS	300K	TS
Dario	U	Gialli	U	Sviluppo	S	100K	S

Indicare se soddisfa i due assiomi base per le basi di dati multilivello o indicare tutte le violazioni a questi.

(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								