Tecnologie per la sicurezza e privatezza – a.a. 2012/2013 – Domande e risposte

by Salvatore Fresta

CRIMINI INFORMATICI E LORO CARATTERISTICHE

Descrivere quali sono gli effetti della introduzione delle misure di sicurezza.

Le misure di sicurezza riducono la possibilità di violazione ed i danni che questa può causare. Possono essere classificate in tre tipi:

1. **Fisiche**: salvaguardia delle risorse hardware
2. **Logiche**: salvaguardia delle informazioni logiche, permettendone l'accesso solo al personale correttamente identificato ed autorizzato.
3. **Organizzative**: definizione e suddivisione di ruoli e responsabilità tra il personale.

Discutere l'affermazione "la sicurezza ha un costo."

La sicurezza ha un costo e per tale motivo va bilanciata in rapporto all'informazione da proteggere ed al costo che un'eventuale furto o compromissione comporterebbe. Il costo non è da intendersi solo a livello monetario bensì anche a livello prestazionale. D'altronde un sistema privo di controlli di sicurezza comporterebbe costi maggiori in quanto continuamente a rischio.

Dire cosa si intende per bomba logica e cavallo di Troia.

La bomba logica è un malware che avvia le proprie funzioni al verificarsi di una condizione. Il cavallo di Troia è un malware che infetta software legittimi in modo tale che quando questi vengono eseguiti, in background (sottofondo) vengono eseguite anche operazioni non lecite con lo scopo di violare la sicurezza del sistema (ad esempio mettendo in ascolto un socket su una porta da cui ricevere comandi per il controllo remoto del sistema vittima). Il nome deriva dal fatto che un utente non si accorge del malware poiché convinto di avviare un'applicazione lecita.

Discutere brevemente le differenze tra il concetto di confidenzialità e privatezza.

La confidenzialità fa riferimento ad una qualsiasi classe di informazione mentre la privatezza solo quella riferita ai singoli individui, dando vita al concetto di **privacy**: diritto di stabilire se, come, quando e a chi l'informazione che ci riguarda può essere rilasciata.

Dire cosa si intende per confidenzialità, integrità e disponibilità delle informazioni.

Confidenzialità è il termine utilizzato per salvaguardare l'informazione dalla lettura di utenti non autorizzati. Per via della natura, si ottiene crittografando il messaggio. Assicurare integrità significa fornire un metodo tramite il quale l'utente destinatario è capace di verificare una possibile alterazione del messaggio avvenuta da utenti non autorizzati a farlo. Per disponibilità si intende la possibilità di accedere, da parte di utenti autorizzati, all'informazione in qualsiasi momento (attacchi denial of service rendono indisponibili informazioni e/o servizi, per cui utenti autorizzati non riescono ad utilizzare l'informazione che diventa indisponibile).

Descrivere le principali tipologie di crimini informatici dolosi.

I crimini dolosi sono quelli premeditati. Di seguito l'elenco dei principali crimini dolosi:

- **Sabotaggio**: operazione atta a danneggiare od impedire il funzionamento di un sistema.
- **Intrusione**: accesso non autorizzato al sistema.
- **Falsificazione dei dati**: alterazione dei dati.
- **Aggiramento**: esecuzione di software per alterare, eliminare, copiare, rendere indisponibili dati memorizzati nel sistema.
- **Ricerca fraudolenta di informazioni**: ricerca di informazioni riservate da parte di utenti non leggittimi all'interno del sistema.
- **Itercettazione**: lettura di informazioni che viaggiano su un canale non sicuro. Se l'attività comprende anche l'alterazione e l'intromissione dell'informazione alterata nel sistema, prende il nome di tampering.
- **Malware**: esecuzione di software che viola la sicurezza.

Dire cosa si intende per crimini informatici non dolosi.

Tutti quei crimini effettuati all'insaputa dell'utente. Ad esempio una macchina compromessa utilizzata come bot di una botnet.

Dire cosa si intende per intercettazione attiva e passiva di informazioni.

L'intercettazione passiva si limita alla lettura dell'informazione. Quella attiva oltre alla lettura, altera l'informazione e la reinserisce all'interno della rete.

Dire cosa si intende per intrusione fisica e logica e fornire degli esempi.

Intrusione fisica alla risorsa, come ad esempio l'accesso di persona ad un server a cui non si è autorizzati. Un'intrusione logica avviene con il software, come ad esempio lo sfruttamento di una vulnerabilità che consente di avere accesso al sistema.

Dire cosa si intende per sabotaggio fisico, logico e psicologico.

- **Fisico**: danneggiamento fisico della risorsa.
- **Logico**: modifica o distruzione di informazioni al fine di compromettere il funzionamento del sistema.
- **Psicologico**: aggiramento dell'utente.

Dire cosa si intende per falsificazione dei dati ed aggiramento.

- **Falsificazione**: alterazione dei dati prima, durante o dopo l'elaborazione.
- **Aggiramento**: esecuzione di software per alterare, eliminare, copiare, rendere indisponibili dati memorizzati nel sistema.

Dire cosa si intende per ricerca fraudolenta di informazioni fisica e logica.

- **Fisica**: la ricerca avviene in informazioni memorizzate su materiale, ad esempio fogli stampati.
- **Logica**: la ricerca avviene all'interno del sistema.

Dire cosa si intende per contromisura e fornire degli esempi di contromisure insieme con la

relativa spiegazione.

Sinonimo di difesa. Un'insieme di tecniche per ridurre le vulnerabilità. Esempio: identificazione dell'utente mediante autenticazione.

Descrivere cosa sono le misure di sicurezza logiche, fisiche ed organizzative.

- **Fisiche**: si occupano della salvaguardia delle risorse hardware.
- **Logiche**: salvaguardano le informazioni presenti nel sistema.
- **Organizzative**: definiscono ruoli e responsabilità del personale.

Nell’ambito della sicurezza informatica descrivere i concetti di vulnerabilità e minacce.

- **Vulnerabiltà**: errore o debolezza che se sfruttata mette a rischio la sicurezza.
- **Minaccia**: evento o circostanza che potrebbe causare violazioni della sicurezza.

AFFIDABILITÀ DEL SOFTWARE

Dire cosa si intende per virus ed elencare le caratteristiche principali di un virus.

Il virus è un malware capace di infettare altri software con la copia di se stesso e di propagarsi. È composto da una parte utilizzata per la duplicazione e da una contenenti le funzioni di danneggiamento o di violazione della sicurezza.

Descrivere, in base alle caratteristiche di attivazione, come possono essere classificati i virus.

Il virus può essere **transiente** se per essere avviato necessita del programma infettato o **residente** se risiede già in memoria e quindi la sua esecuzione è indipendente.

Descrivere il processo di infezione di un virus.

La propagazione virale può avvenire in molti modi: trasmissione in rete (allegati email, chat, social network, file sharing) o tramite i dispositivi removibili di mass storage (pendrive, sd, hard disk esterni)

Descrivere in che modo un virus puo ottenere il controllo.

Il virus può decidersi se **sovrapporsi** alle istruzioni del software infetto, impedendo il funzionamento di quest'ultimo, o se **aggiungersi** (non sovrapposto) al software infetto, modificando di fatto la dimensione del programma. Poi il controllo della macchina, una volta avviato, può avvenire in diversi modi: al **boot**, dopo l'avvio del sistema operativo, dopo l'esecuzione di un software infetto ecc..

Descrivere le principali differenze tra virus sovrapposto e virus non sovrapposto.

La differenza principale è che il virus sovrapposto non permette al software che lo ospita di funzionare correttamente mentre quello non sovrapposto potrebbe permetterlo, avviandosi come una routine che non influisce con le operazioni del software.

Descrivere cosa di intende per firma di un virus e le diverse tipologie di pattern che possono

essere considerati per la sua definizione.

La firma è una sequenza di bit statica del codice del virus che serve agli antivirus per identificarlo. Essendo una sequenza di bit, può capitare che la stessa si trovi anche in software legittimi, dando vita a falsi positivi da parte degli antivirus. Esistono diversi pattern:

- Pattern di **memorizzazione**: il virus può essere invariante, essere memorizzato sempre nelle stesse posizioni del file infetto o avere delle istruzioni sospette (come un jump come prima istruzione del file infetto).
- Pattern di **esecuzione**: il virus è in grado di effettuare diverse operazioni come diffondersi, provocare danni e nascondersi.
- Pattern di **trasmissione**: il virus è capace di trasmettersi da un sistema ad un altro.

Descrivere cosa si intende per dinamicita della firma.

È una firma variabile da infezione ad infezione.

Dire cosa si intende per virus polimorfo e fornire un semplice esempio.

È un virus che cambia forma da infezione ad infezione. Il polimorfismo si può ottenere in diversi modi, ad esempio aggiungendo in modo random istruzioni nop nel codice, che non influiscono sull'esecuzione ma sulla sequenza di bit e quindi sulla firma.

Descrivere i componenti principali di un virus crittografico.

I componenti principali sono tre: la parte crittografata, la chiave crittografica e la routine di decrittazione.

Descrivere il funzionamento di un virus boot sector.

Il virus viene avviato dal software di bootstrap, che di norma esegue queste operazioni: legge il boot sector dall'hard disk, esegue il bootstrap loader che carica il sistema operativo a cui viene passato il controllo. Il virus, se inserito nel settore di boot, viene avviato prima del sistema operativo. Sarà il virus ad avviare il bootstrap loader.

Dire cosa si intende per trapdoor ed a cosa serve.

La trapdoor è un accesso nascosto ad un modulo o ad un software, di norma utilizzato dagli sviluppatori in fase di test. Se dimenticato (a volte volutamente lasciato) nelle release e scoperto, può essere utilizzato da terzi per violare la sicurezza.

Dire cosa si intende per salami attack e fornire un esempio.

Sono una serie di piccoli attacchi che singolarmente hanno un basso impatto sulla sicurezza ma che se presi tutti insieme hanno un impatto critico. Un esempio può essere la sottrazione di piccole quantità di denaro dai trasferimenti bancari. Danno irrisorio per il singolo caso ma notevole per la mole di trasferimenti bancari che avvengono in una banca.

Descrivere le principali cause della presenza del salami attack.

Le cause principali possono essere errori di computazione ed arrotondamenti nel software.

Descrivere cosa sono i covert channel e quali sono le conseguenze della loro presenza in un sistema.

Sono dei canali di comunicazione che permettono ad un processo di trasferire informazioni che violano la sicurezza. Sono difficili da indivduare in quanto si adattano a canali legittimi e permettono a terzi di avere accesso ad informazioni non autorizzate.

Dire cosa si intende per storage channel e fornire un esempio.

Sono dei covert channel che sfruttano la presenza o l'assenza di oggetti in memoria. Per esempio si può trasmettere utilizzando il canale **file lock**: si trasmette un bit se il file è bloccato oppure no.

Dire cosa si intende per timing channel e fornire un esempio.

Sono dei covert channel che sfruttano la velocità con cui accadono certi eventi. Per esempio se il software di sistema usa il tempo computazionale offerto dalla CPU, il programma spia trasmette 1, altrimenti 0.

Descrivere la tecnica basata sull'analisi delle risorse per l'individuazione di covert channel.

Si crea una matrice M avente come le risorse come righe, i processi nelle colonne e l'azione (lettura/modifica) come cella. Dopo di che si cerca una situazione come la seguente:

M		**R**
R		**R**

e si completa con una **R**. Si analizza la matrice per verificare se ci sono trasmissioni di informazione indesiderata.

Descrivere la tecnica basata sull'analisi del codice sorgente per l'individuazione di covert channel.

Si controlla il codice per verificare assegnazioni non ovvie, come ad esempio:

if(d == 1) b = a

Definire cosa sono le stringhe di formato e come possono essere utilizzate per apportare un attacco di tipo buffer overow.

Si tratta di un particolare tipo di stringa che contiene dei parametri identificati dal simbolo % con il quale è possibile stampare o scrivere delle variabili in un formato ben preciso (%s stringa, %d numero intero decimale, %f numero a virgola mobile ecc..). Se tale parametro non viene specificato, è possibile formattare la stringa in input in modo tale da poter scrivere nello stack utilizzando il parametro %n fino a sovrascrivere le aree di memoria adiacenti.

Dire cosa si intende per buffer overow e quali effetti puo avere.

È una vulnerabilità che permette la sovrascrittura delle aree di memoria adiacenti a quella del buffer in questione. Gli effetti possono essere molteplici quali: esecuzione di codice arbitrario con i privilegi dell'applicazione vulnerabile e denial of service. Può avvenire nello stack, andando a sostituire l'indirizzo presente nel registro Instruction Pointer, o nello heap.

Dire cosa si intende per overow off-by-one e fornire un esempio.

È un buffer overflow di un byte che non permette di sovrascrivere il return address ma di sovrascrivere in parte l'indirizzo del frame precedente. Capita ad esempio quando si scrive in ciclo un array ed il contatore prosegue ancora per un'unità oltre quella della dimensione massima.

Illustrare, tramite un esempio, un overow dello stack.

```
Int main(int argc, char *argv[]) {

char frase[10];

if(argc > 1) strcpy(frase, argv[1]);

}
```

La funzione strcpy non effettua nessun controllo sulla dimensione del buffer di destinazione per cui se argv[1] contiene più di 10 byte, i byte in overflow andranno a sovrascrivere le aree di memoria adiacenti a frase. Avviene nello stack in quanto il buffer frase non viene definito dinamicamente.

Dire cosa sono le stringhe di formato ed illustrare un esempio di come l'uso improprio delle stringhe di formato possa consentire delle scritture nello stack.

Si tratta di un particolare tipo di stringa che contiene dei parametri identificati dal simbolo % con il quale è possibile stampare o scrivere delle variabili in un formato ben preciso (%s stringa, %d numero intero decimale, %f numero a virgola mobile ecc..). Se tale parametro non viene specificato, è possibile formattare la stringa in input in modo tale da poter scrivere nello stack utilizzando il parametro %n. Esempio:

```
Int main(int argc, char *argv[]) {

printf(argv[1]);

}
```

se passo come argomento “ciao%n” il numero 4 viene scritto in argv[1]. Posso passare diverse combinazioni di parametri in modo tale che il valore che andrà a sovrascrivere il return address sia corrispondende a quello dell'indirizzo di memoria dove si troverà il codice arbitrario.

SERVIZI DI SICUREZZA

Spiegare il concetto di autenticazione e discutere le tre principali tecniche di autenticazione utente computer.

Autenticarsi significa identificarsi al sistema e lo si fa mediante qualcosa che potenzialmente potremmo fare/sapere solo noi. Le tre principali tecniche di autenticazione sono:

- Autenticazione basata sulla **conoscenza**: per autenticarsi si usa qualcosa che solo noi conosciamo,come una password.

– Autentizzazione basata sul **possesso**: per autenticarsi si usa qualcosa che solo noi abbiamo, come un token hardware.
– Autenticazione basata sulla **biometria**: per autenticarsi si usa qualcosa che possediamo naturalmente, come l'impronta digitale o il riconoscimento vocale.

Nell'ambito delle tecniche di autenticazione basate sul possesso, descrivere le differenza tra memory card e smart token.

La differenza sta che le memory card non hanno un processore quindi nessuna capacità computazionale per proteggere o elaborare le informazioni memorizzate, mentre lo smart token può.

Nell'ambito delle tecniche di autenticazione basate sulla conoscenza, dire cosa si intende per password grafiche.

Sono tutte quelle password sottoforma di immagini. Ad esempio la ricostruzione di un puzzle con uno schema particolare può essere utilizzato per autenticarsi.

Descrivere la tecnica di autenticazione single sign-on. Quali sono i vantaggi di questa tecnica di autenticazione rispetto ad una tecnica tradizionale basata su password?

Il problema che porta al single sign on è quello di utilizzare password diverse per ogni sistema/servizio/server. Da qui si è pensato di utilizzare un singolo server come entità atta a memorizzare la password ed un certificato di autenticazione prodotto da questo per autenticarsi presso altri server. In questo modo è possibile gestire più servizi con la stessa password.

Nell'ambito della tecnica di autenticazione SSO, dire cosa si intende per network identity.

Sono l'insieme delle informazioni dell'utente sparse tra i vari server SSO federati.

Descrivere le differenze tra autenticazione e autorizzazione.

L'autenticazione è il processo di identificazione mentre l'autorizzazione consiste nel controllo ed eventuale rilascio/negazione dei privilegi dell'utente/processo autenticato che richiede di effettuare una determinata operazione.

In relazione al problema della sicurezza delle password dire cosa si intende per:
• spoofing;
• snooping;
• sniffing;
• masqueranding.

– **Spoofing**: imitare il server legittimo con uno illegittimo al fine di rubare la password.
– **Snooping**: osservare l'utente mentre digita la password al fine di poterla memorizzare.
– **Sniffing**: lettura della password inviata su un canale non sicuro in cui ci si è messi in ascolto.
– **Masqueranding**: chiunque riesce a conoscere la password di un utente può impersonarlo.

Nell'ambito della tecnica di autenticazione basata su password, descrivere le principali regole per una buona gestione delle password.

Scegliere una password lunga almeno 8 caratteri e composta da caratteri maiuscoli, minuscoli, numerici e, se possibile, simboli. Comporla in modo tale da ricordarla, in quanto se memorizzata su qualche dispositivo o scritta su un foglio di carta, perderebbe la sua sicurezza. Cambiarla regolarmente.

Nell'ambito della tecnica di autenticazione basata su password, descrivere l'attacco denominato brute force attack.

È un attacco che prova tutte le combinazioni possibili di password fornito una lunghezza ed un dataset (set di caratteri da provare).

Nell'ambito delle tecniche di autenticazione, descrivere il meccanismo di challenge response. A quale tipo di attacco è vulnerabile il challenge response

Il client effettua richiesta di autenticazione. Il server invia una stringa casuale in chiaro che il client deve crittografare. Questo la crittografa e la invia al server. Il server la decifra e la confronta con quella originale. Se sono uguali, autentica il client. Il problema di questo sistema è che è vulnerabile ad attacchi di man in the middle.

Commentare l'affermazione "il meccanismo di autenticazione di challenge response non è vulnerabile ad attachi di tipo replay."

Non è vulnerabile ad attacchi replay perché il server genera una nuova challenge ad ogni richiesta di autenticazione.

Nell'ambito delle tecniche di autenticazione basate su caratteristiche dell'utente, descrivere il processo di autenticazione.

In questo tipo di autenticazione viene utilizzata una caratteristica univoca dell'utente, come l'impronta digitale o il timbro vocale. Gli algoritmi devono mantenere un margine di errore oltre il quale negare l'autenticazione. È un sistema che per via dei costi di implementazione non è largamente diffuso.

Nell'ambito delle tecniche di autenticazione basate su caratteristiche dell'utente, descrivere in cosa consiste la fase di enrollment.

È la fase di definizione di un template e dove vengono elaborate le informazioni ottenute dalla lettura della caratteristica biometrica.

Descrivere l'attacco Mig in the middle.

1. La nave nemica invia un challenge all'aereo.
2. L'aereo trasmette il challenge alla nave amica.
3. La nave amica aspetta l'ingresso nello spazio aereo di un mig nemico ed invia a questo il challenge
4. Il mig nemico risponde alla nave amica
5. La nave amica inoltra la risposta all'aereo amico
6. L'aereo amico la invia alla nave nemica e viene identificato da questa come amico

Nell'ambito del meccanismo di autenticazione di Apache, descrivere le differenze tra l'autenticazione di base e l'autenticazione digest.

L'autenticazione di digest, a differenza dell'autenticazione base, utilizza una funzione di hash per le password.

Dire cosa si intende per politica per il controllo dell’accesso e politica amministrativa.

La politica per il controllo dell'accesso si occupa di consentire o negare l'accesso da parte di un soggetto ad un oggetto mentre quella amministrativa si occupa di definire chi deve distribuire le autorizzazioni.

Descrivere le caratteristiche principali delle politiche discrezionarie. Perché sono politiche “discrezionarie”?

Controllano l'accesso sulla base dell'identità dell'utente che lo richiede e su un insieme di regole che stabiliscono l'accesso alle risorse. Si chiamano discrezionarie perché l'utente può trasferire, a propria discrezione, i propri privilegi ad un altro utente.

Descrivere le caratteristiche principali delle politiche mandatorie.

Impongono dei vincoli (restrizioni) al flusso di informazione. Fanno una netta distinzione tra utente e soggetto:

- **Utente**: coloui che utilizza il sistema.
- **Soggetto**: processo avviato dall'utente.

Si basano sulla definizione di classe di sicurezza (classificazione di oggetti e soggetti), intesa come un elemento di un insieme parzialmente ordinato, formata da due componenti: livello di sicurezza e categorie. Le classi di sicurezza sono relazionate da una relazione di dominanza. Queste possono essere usate da politiche che garantiscono la segretezza o l'integrità.

Descrivere le caratteristiche principali delle politiche basate sui ruoli.

A volte per completare delle operazioni occorre avere diversi privilegi. Da qui nasce il concetto di ruolo visto come un insieme di privilegi assegnati dinamicamente. Gli utenti possono avere diversi ruoli in tempi differenti. Con questa politica le autorizzazioni vanno assegnate ai ruoli e non ai singoli utenti, cosicché tutto diventa più scalabile.

Nell’ambito delle politiche discrezionarie, descrivere i componenti di un modello di sicurezza.

Il modello di sicurezza è formato da una tripla S-O-A dove S sono i soggetti intesi come gli utenti, O sono le risorse ed A è la matrice d'accesso le cui celle individuano le azioni che un soggetto S può compiere sulla risorsa O.

Nell’ambito delle politiche per il controllo dell’accesso, descrivere le differenze tra ruolo e gruppo.

Il gruppo è un insieme statico di utenti mentre il rulo è un insieme dinamico di privilegi.

Nell’ambito del modello a matrice di accesso, descrivere i componenti dello stato di protezione.

Lo stato è formato da: tre **entità**:

1. soggetti (coloro che richiedono l'accesso alle risorse)

2. oggetti (le risorse)
3. azioni (azioni che possono essere compiute sugli oggetti).

Nell'ambito del modello a matrice di accesso, descrivere le tre tecniche di implementazione della matrice, discutendone i relativi vantaggi e svantaggi.

- **Tabelle di autorizzazione**: si memorizzano tutte le triple non nulle in una tabella. Anche qui comunque si ha uno spreco di spazio dovuto alla ridondanza delle informazioni.
- **Access Control List (ACL)**: per ogni oggetto si ha una lista di soggetti i cui record contengono le azioni che possono compiere. È vantaggiosa in quei sistemi dove l'accesso alle risorse è frequente.
- **Capability List (ticket)**: per ogni soggetto si ha una lista di oggetti i cui record contengono le azioni che possono essere compiute. Si deve far si che il soggetto non possa modificare il contenuto di tale lista. È vantaggiosa in quei sistemi dove il soggetto viene interpellato di frequente.

Nell'ambito del modello a matrice di accesso, definire un comando che consenta al proprietario di un file di concedere il diritto di esecuzione su tale file ad un altro utente del sistema.

conferExecute(owner, friend, file) dove owner è il proprietario, friend l'utente destinatario e file il file a cui si fa riferimento.

Descrivere le caratteristiche principali del modello Chinese Wall ed i suoi principali problemi.

È una politica di tipo mandatorio che applica la separazione dinamica dei privilegi per prevenire i flussi di informazione che causano un conflitto di interesse tra varie organizzazioni che operano sullo stesso contesto. Gli oggetti sono organizzati in:

- **basic object**: contengono informazioni, ognuno di un'organizzazione diversa
- **company dataset**: gruppi di oggetti della stessa organizzazione
- **classi di conflitto di interesse**: insieme di dataset in competizione

La separazione dinamica dei privilegi permette di non dare troppe agevolazioni ad un utente in modo che questo non possa abusare del sistema. Ciononostante alcuni problemi rimangono irrisolti:

- Non gestisce la storia degli accessi
- Non fornisce procedure per sanitizzare i dati
- Non garantisce l'accessibilità in quanto se tutti gli utenti volessero accedere allo stesso dataset, si bloccherebbe il sistema

Descrivere le principali debolezze delle politiche discrezionarie fornendo anche un esempio.

Applicando una serie di comandi leggittimi è possibile portare il sistema in uno stato non sicuro in relazione alla politica di sicurezza imposta. Questo problema può essere indecidibile nel caso in cui il numero di comandi che è possibile avviare siano maggiori ad 1 e se il numero di soggetti ed oggetti è illimitato. Inoltre la politica discrezionaria regolamenta solo l'accesso alla risorsa e non l'uso che ne si fa delle informazioni, pertanto è vulnerabile ad attacchi trojan horse. Ad esempio un trojan potrebbe aprire una risorsa a cui ha accesso, leggerne il contenuto, creare una nuova risorsa, copiarne all'interno il contenuto e renderlo disponibile anche a chi non ha i permessi per accedere alla risorsa originaria.

Nell’ambito delle politiche mandatorie, fornire la definizione di classi di sicurezza e di relazione di dominanza tra classi.

Una classe di sicurezza è un insieme di elementi parzialmente ordinati formato da due componenti: un livello di sicurezza, definito come un elemento di un insieme ordinato gerarchicamente, ed una categoria, definita come un sottoinsieme di un insieme di elementi non ordinati che rappresentano le classi di appartenenza e servono anche ad imporre restrizioni need to know. Le classi sono relazionate tra di loro mediante la relazione di dominanza che dice che una classe X domina la classe Y se e solo se il livello di sicurezza della classe X domina quello della classe Y e se le categorie della classe Y sono sottoinsieme delle categorie della classe X.

Nell’ambito delle politiche per il controllo dell accesso, descrivere il principio del minimo privilegio (least privilege).

Il principio del minimo privilegio dice che ad un soggetto devono essere fornite solo ed esclusivamente le autorizzazioni minime necessarie a completare il lavoro.

Nell’ambito delle politiche per il controllo dell’accesso, dire cosa si intende per politica aperta e politica chiusa.

Una politica è aperta quando, a meno di restrizioni specifiche, un soggetto è libero di fare tutto ciò che eredita mentre una politica è chiusa quando, al contrario, a meno di specifici permessi al soggetto viene negato ogni permesso.

Definire il principio di separazione dei privilegi e fornire un esempio.

Il principio dice che nessun utente dovrebbe avere abbastanza privilegi da poter abusare del sistema. La separazione può essere definita in modo **statica**, ovvero autorizzazioni assegnate in principio stando attenti a non concederne troppe, o **dinamica**, ovvero un utente decide quali privilegi scegliere ed il sistema negherà gli altri di conseguenza. Esempio:

Una transazione è composta da 4 operazioni fondamentali: fare l'ordine, spedirlo, registrare la fattura e pagare. Abbiamo 4 persone in grado di eseguirla. Posso decidere in principio chi eseguirà le operazioni, ovviamente una a testa (**separazione statica**) o far decidere ad ogni utente un'operazione a scelta (**separazione dinamica**). In ogni caso il lavoro non può essere compiuto da una persona sola.

Caratterizzare i tre meccanismi per il controllo dell’accesso: ACL, capability e tabella di autorizzazione in termini della facilità con cui è possibile eseguire le seguenti operazioni:
• data una richiesta di accesso, determinare se la richiesta è permessa oppure no;
• aggiunta di una autorizzazione per un nuovo soggetto;
• cancellazione di una autorizzazione per un soggetto;
• creazione di un nuovo oggetto su cui tutti i soggetti per default hanno il privilegio di lettura;
• cancellazione di un oggetto.

- 1: più semplice nella tabella di autorizzazione.
- 2: più semplice nella capability
- 3: più semplice nella tabella di autorizzazione
- 4: più semplice nella ACL
- 5: più semplice nella ACL

Nell’ambito delle politiche per il controllo dell’accesso che supportano sia autorizzazioni

positive sia autorizzazioni negative, dire cosa si intende per inconsistenza e non completezza. Si richiede inoltre di discutere come possono essere risolti tali problemi.

- **Non completezza**: assenza di un'autorizzazione per un determinato elemento. Si risolve adottando una politica di default.
- **Inconsistenza**: presenza contemporanea di un'autorizzazione positiva ed una negativa per lo stesso elemento. Esistono delle politiche di risoluzione per questi problemi.

Nell'ambito delle politiche mandatorie per la protezione dell'integrità, spiegare i principi no read down e no write up.

- **No read down**: un soggetto può leggere solo oggetti le cui classi di integrità dominano quelle delle soggetto.
- **No write up**: un soggetto può scrivere solo oggetti di cui domina le classi di integrità.

Nell'ambito delle politiche mandatorie per la protezione della sicurezza, spiegare i principi no read up e no write down.

- **No read up**: un soggetto può leggere solo oggetti di cui domina le classi di sicurezza.
- **No write down**: un soggetto può scrivere solo oggetti le cui classi di sicurezza dominano quelle delle soggetto.

Nell'ambito del modello di Bell e LaPadula, definire quando uno stato si dice sicuro.

Uno stato si dice sicuro quando sono soddisfatte le proprietà **simple security propery** e ***property**, che formalizzano rispettivamente il principio di no read up e no write down.

Descrivere le principali limitazioni delle politiche mandatorie per la segretezza.

- **Non esiste la declassazione** delle risorse dopo un certo periodo di tempo
- Non si tiene in considerazione il fatto che **un processo può produrre dati meno sensibili di quelli a cui accede**
- La **determinazione delle classi** di accesso non è sempre facile e immediata
- Sono **vulnerabili ai covert channel** poiché non offrono sistemi per individuarli o contrastarli

Nell'ambito del modello di Biba, descrivere la politica low-water mark per oggetti. Questa politica garantisce l'integrità delle informazioni?

Nel modello base di Biba, gli utenti potrebbero accedere ad informazioni riservate per via del principio no read down. Il problema si risolve con la politica lower-water mark per soggetti: i soggetti possono leggere qualsiasi oggetto ma subito dopo il loro livello viene declassato a quello inferiore dei due, ovvero al glb dei due. Se tale politica viene applicata agli oggetti causa una violazione dell'integrità.

Nell'ambito del modello di Biba, descrivere la politica low-water mark per soggetti ed i principali problemi di tale politica.

I soggetti possono leggere qualsiasi oggetto ma subito dopo il loro livello viene declassato a quello inferiore dei due, ovvero al glb dei due. Il problema è che l'ordine delle operazioni influenza il risultato, non esiste infatti la proprietà commutativa nel glb.

Nell’ambito delle politiche amministrative, descrivere la politica di amministrazione centralizzata e cooperativa.

In quella centralizzata un unico amministratore definisce le autorizzazioni mentre in quella cooperativa esiste un pool di amministratori

Nell’ambito delle politiche per la risoluzione dei conflitti, spiegare le politiche most specific takes precedence e most specific along a path takes precedence. Si richiede inoltre di fornire un esempio che illustri il funzionamento di queste due politiche.

- **Most specific takes precedence**: vince l'autorizzazione più specifica in assoluto per un certo elemento
- **Most specific along a path takes precedence**: si prendono in considerazione le autorizzazioni più specifiche su ogni percorso (se ne esiste più di uno, se no è analoga alla Most specific takes precedence).

Spiegare i concetti di politiche di sicurezza e meccanismi per il controllo dell’accesso. Perché è utile una loro separazione?

La politica è un'insieme di regole per realizzare la sicurezza del sistema mentre i meccanismi sono le loro implementazioni. La separazione tra i due permette di concentrarsi su uno degli aspetti ed implementare anche diverse politche.

Nell’ambito dei meccanismi di sicurezza, descrivere quali proprietà deve soddisfare il reference monitor.

- Nessuno deve poterlo modificare
- Non dev'essere bypassabile
- Va memorizzato su una parte sicura del sistema operativo
- Deve avere dimensioni limitate
- Deve essere resistente ai covert channel

Discutere le principali politiche per la risoluzione dei conflitti che possono essere adottate nei sistemi ibridi (un sistema ibrido è un sistema nel quale sono presenti sia autorizzazioni positive sia autorizzazioni negative).

- **Denial takes sprecedence**: le autorizzazioni negative vincono sulle positive
- **Permission takes precedence**: le autorizzazioni positive vincono sulle negative
- **Most specific takes precedence**: vince l'autorizzazione più specifica in assoluto per un certo elemento
- **Most specific along a path takes precedence**: ssi prendono in considerazione le autorizzazioni più specifiche su ogni percorso (se ne esiste più di uno, se no è analoga alla Most specific takes precedence).

Descrivere la differenza tra politica per il controllo dell’accesso e modello per il controllo dell’accesso.

La politica è una definizione di regole mentre il modello descrive formalmente le specifiche e l'esecuzione del controllo dell'accesso e serve per passare dalla politica ai meccanismi.

Nell’ambito del controllo dell’accesso, descrivere la differenza tra utente e soggetto.

L'utente è colui che usa il sistema mentre il soggetto è il processo avviato dall'utente che andrà ad utilizzare una determinata risorsa.

Spiegare i due principi detti rispettivamente separazione dei privilegi e minimo privilegio.

- Separazione dei privilegi: nessun utente deve avere un numero di privilegi tale da poter abusare del sistema.
- Principio del minimo privilegio: ad un utente devono essere assegnati solo quei privilegi strettamente necessari a completare il lavoro.

Descrivere i quattro componenti principali del modello ANSI RBAC.

1. **Core RBAC**: gli utenti sono assegnati a ruoli da cui acquisiscono privilegi.
2. **Gerarchia dei ruoli**: generali o limitate
3. **Separazione statica dei privilegi**
4. **Separazione dinamica dei privilegi**

Nell’ambito del meccanismo di controllo dell’accesso di Apache, descrivere il processo di valutazione delle direttive contenute nei file .htaccess.

Data una richiesta di accesso ad un file, la valutazione del file htaccess parte dalla root del server discendendo il percorso valutando, ad ogni sottodirectory, tutte la configurazioni di autorizzazione.

Nell’ambito del meccanismo di controllo dell’accesso di Linux, descrivere il significato di setuid e setgid ed a cosa servono.

- **Setuid**: l'UID del processo che esegue un file è uguale a quello del proprietario del file.
- **Setgid**: analogo al setuid ma per il GID (id del gruppo).

Nell’ambito del meccanismo di controllo dell’accesso di Windows, descrivere i componenti principali del descrittore di sicurezza.

I principali componenti sono:

- SID del proprietario dell'oggetto
- SID del gruppo primario dell'oggetto
- DACL
- SACL

Descrivere le caratteristiche principali del modello di sicurezza di JDK 1.2.

La caratteristica principale è che permette di rispettare il principio del minimo privilegio.

Descrivere le caratteristiche principali dei sistemi per il controllo delle intrusioni di tipo anomaly detection.

Gli IDS basati su anomaly detection verificano le intrusioni facendo riferimento ad un modello di uso normale del sistema. Tutto ciò che si discosta da tale modello viene preso in considerazione. Questo permette di riuscire ad indentificare attacchi non noti ma per via della natura è alto anche il rischio di falsi allarmi. Inoltre è tutt'altro che banale riuscire a formare un modello di uso normale del sistema.

Descrivere le caratteristiche principali dei sistemi per il controllo delle intrusioni di tipo misuse detection.

Gli IDS basati su misuse detection utilizzano un database di signature per verificare un tentativo di intrusione. Se tali signature sono molto precise, aumenta il rischio di falsi negativi mentre se sono troppo generiche aumenta quello di falsi positivi.

Descrivere sinteticamente a cosa serve un NIDS (Network Intrusion Detection System).

Un Network IDS serve ad identificare un tentativo di intrusione analizzando i dati che viaggiano in rete.

Nell'ambito dei sistemi per il controllo delle intrusioni, si descrivano i sistemi host-based e networkbased.

- **Hostbased IDS**: sono quegli IDS la cui analisi avviene nel sistema stesso, ad esempio mediante la lettura dei file di log di sistema, calcolo del checksum di alcuni file critici ecc.. quindi limitano il raggio d'azione al sistema stesso.
- **Network-based IDS**: sono quegli IDS la cui analisi avviene sul flusso di informazioni che passa in rete, ad esempio analizzando il traffico. Il loro raggio d'azione è esteso alla rete che controllano.

Nell'ambito dei sistemi per il controllo delle intrusioni, dire cosa si intende per falsi positivi e falsi negativi.

- **Falsi positivi**: operazioni legittime identificate come allarmi.
- **Falsi negativi**: attacchi non rilevati.

Nell'ambito dei servizi di audit per l'analisi delle procedure si descriva:
• le aree di intervento in cui opera;
• cosa comporta l'analisi dei rischi;
• in cosa consista la fase di preparazione.

Le aree di intervento sono:

- **Sicurezza organizzativa**: verifica delle responsabilità e delle politiche aziendali.
- **Sicurezza logica e fisica**: valutazione della protezione da accessi non autorizzati, da eventi di natura umana o ambientale, dell'infrastruttura di rete, di client e server.
- **Sicurezza delle applicazioni**: verifica delle protezioni per i sistemi applicativi contro rischi di tipo intrinseco e implementativi.

L'analisi del rischio comporta:

- Valutazione della probabilità che si verifichi un determinato rischio
- Meccanismi atti a contenere i rischi
- Determinazione delle contromisure
- Sviluppo delle contromisure
- Determinazione della gravità di ogni singolo rischio e assegnamento delle contromisure

La fase di preparazione consiste nel stabilire a che livello tra host, server, firewall o rete si applicherà l'audit. Dopo di che occorre scegliere i tool di audit e selezionare il personale adatto.

Nell'ambito delle tecniche di audit per l'analisi degli eventi, si descrivano i componenti di un audit log

I componenti sono:

- Il soggetto che richiede l'accesso
- L'oggetto a cui si accede
- L'operazione richiesta
- Il tempo in cui è stata effettuata la richiesta
- La locazione da dove la richiesta proviene
- La risposta del sistema del controllo dell'accesso
- La quantità di risorse impiegate dal sistema
- L'esito dell'operazione

SICUREZZA NELLE RETI

Descrivere le caratteristiche principali degli attacchi di tipo interruzione ed intercettazione.

Ciò che caratterizza l'attacco di interruzione è il rendere inutilizzabile un servizio o una risorsa, mentre la caratteristica di un attacco di intercettazione è la possibilità di avere accesso ad informazioni riservate che passano attraverso un canale non sicuro.

Descrivere le caratteristiche principali degli attacchi di tipo modifica e produzione.

La caratteristica di un attacco di modifica è la possibilità di poter alterare l'informazione mentre la caratteristica di quello di produzione è la possibilità di poter introdurre nel sistema dei componenti nuovi.

Descrivere gli attacchi spoofing e sniffing.

Per spoofing si intende l'attacco atto a falsificare l'identità di uno degli interlocutori di una comunicazione mentre per sniffing si intende l'attacco atto ad intercettare la comunicazione tra due o più interlocutori in un canale non sicuro.

Descrivere in cosa consiste l'attacco file spoofing e fornire un esempio.

Un attacco di file spoofing consiste nel falsificare l'estensione di un file. Ad esempio utilizzare la doppia estenzione nei sistemi Microsoft i quali di default la nascondono. Esempio: immagine.jpg.exe, vista solitamente come immagine.jpg nei sistemi Microsoft.

Dire cosa si intende per TCP session hijacking.

Si intende l'attacco che mira a dirottare una connessione TPC intercettando e calcolando il prossimo Serial Number della comunicazione. L'interlocutore attaccato sarà disconnesso e l'attaccante prenderà il suo posto.

Nell'ambito degli attacchi a protocolli di rete, descrivere in maniera chiara e sintetica in cosa

consiste un attacco di tipo Denial-of-Service (DoS). Quali sono le differenze tra DoS e DDoS (Distributed Denial-of-Service)?

Un attacco DoS consiste nell'impedire l'utilizzo di un servizio o di una risorsa, solitamente mediante un sovraccarico o lo sfruttamento di una vulnerabilità che ne consegue il crash. Le differenza tra DoS e DDoS è che quest'ultimo è distribuito tra più macchine, ovvero ci sono diverse macchine infettate, denominate bot, controllate da una macchina, denominata master, le quali inonderanno di richieste un determinato server specificato dal master.

Descrivere gli attacchi SYN flooding e smurf attack.

- L'attacco SYN flooding consiste nell'avviare il 3-way handshake TCP con l'invio di tantissimi pacchetti con il flag SYN attivo, facendo allocare al server tanti slot di comunicazione fino ad esaurirli e non accettare più connessioni da client legittimi.
- Lo smurf attack consiste nello spoofare l'indirizzo IP di una macchina in LAN, inviare in broadcast un pacchetto ICMP e far si che le risposte intasino la macchina vittima al fine di renderla inutilizzabile.

Spiegare in sintesi l'attacco cross-site scripting e quali contromisure possono essere adottate.

È un attacco ad applicazioni web che consiste nella possibilità di iniettare in una variabile del codice html e javascript. Questo permette di alterare non solo la grafica della pagina ed il suo contenuto (solo visuale, non nel server in quanto è un attacco lato client) ma di accedere anche a contenuti come i cookie con la possibilità di stolen della sessione. Per evitare questo attacco non bisogna accettare codice html come input o effettuare il giusto escaping.

Spiegare in sintesi l'attacco SQL injection e quali contromisure possono essere adottate.

È un attacco il cui scopo è l'esecuzione di codice SQL arbitrario. Le contromisure sono sostanzialmente due, ovvero effettuare un parsing dell'input numerico ed escaping di apici e doppi apici per input stringa.

Descrivere gli attori principali del protocollo Kerberos.

Gli attori principali sono il protocollo AS, TGS, Client e Server.

Descrivere il flusso dei messaggi che vengono scambiati tra i vari attori del sistema nel caso in cui si utilizzi Kerberos versione 4 per l'autenticazione.

1. Il client si autentica con AS
2. AS invia al client una chiave di sessione ed un ticket
3. Il client invia al TGS le informazioni ottenute
4. Il TGS autentica il client ed invia un ticket di servizio
5. Il client utilizza tale ticket per poter comunicare con il server

Descrivere le funzionalità di una PKI (Public Key Infrastructure).

Una PKI consente lo scambio di chiavi pubbliche.

Descrivere il meccanismo di revoca dei certificati digitali basato su CRL (Certificate Revocation List).

È una lista di certificati revocati, firmati dalle CA, che devono essere controllati prima di utilizzare un certificato digitale.

Descrivere cosa sono i certificati digitali e che funzione svolge una certification authority.

Sono dei documenti elettronici che, mediante la firma di una Certification Authority, attestano la chiave pubblica allegata ad una determinata entità. La Certification Authority è un ente esterno fidato che firma i certificati digitali. Tale firma può sempre essere verificata dal client mediante la chiave pubblica rilasciata dalla stessa.

Descrivere le caratteristiche principali dei firewall di tipo static packet filtering.

È un tipo di firewall che analizza i pacchetti in modo isolato, ovvero senza tener conto della storia della connessione. Utilizza una ACL, ovvero una lista di regole letta dall'alto verso il basso che regolamentano le azioni per i pacchetti con delle specifiche condizioni. Se nessuna delle regole corrisponde al pacchetto in analisi, si applica la policy ti default che può essere default deny o default allow.

Dire a cosa serve un firewall.

Serve a decidere quale traffico può attraversare i confini di una rete.

Descrivere le differenze tra i firewall static packet filtering e dynamic packet filter.

Il dyamic packet filter, a differenza dello static, può lavorare a più livelli. Ad esempio può lavorare contemporaneamente a livello applicativo e transport.

Nell'ambito dei firewall a livello applicativo, descrivere le caratteristiche principali dei circuit firewall.

Descrivere le principali minacce alla sicurezza delle e-mail.

Tutti i campi dell'header mail possonoe essere alterati per cui l'informazione presente nell'intestazione non può essere ritenuta attendibile al 100%. Inoltre i protocolli standard, SMTP e POP, non utilizzano crittografia quindi le informazioni viaggiano in chiaro e, in un canale non sicuro, sono soggette a sniffing ed alterazioni.

Descrivere il processo di autenticazione di PGP.

Calcolo l'hash del messaggio e lo cifro con la chiave privata. Compatto tutto e invio messaggio e firma al destinatario. Quest'ultimo, con la mia chiave pubblica, dopo aver scompattato, decifra la firma, calcola l'hash del messaggio ricevuto e lo confronta con quello decifrato. Se sono uguali è stata garantita integrità ed autenticità.

Descrivere il processo di segretezza di PGP.

Il mittente genera un numero casuale di 128 bit utilizzato solo per questo messaggio e lo utilizza come chiave di sessione. Il messaggio viene poi cifrato con un algorimo **simmetrico** utilizzando questa chiave di sessione. La chiave viene poi cifrata utilizzando la chiave pubblica del destinatario e viene inviata, insieme al messaggio cifrato, al destinatario. Quest'ultimo decifra la chiave di sessione che utilizza per decifrare il messaggio.

Descrivere il processo di segretezza ed autenticazione di PGP.

È una combinazione dei due precedenti. Il messaggio e la firma vengono compattati e cifrati con un algoritmo simmetrico utilizzando la chiave di sessione. Quest'ultima viene cifrata con la chiave pubblica del destinatario e viene inviata a quest'ultimo insieme al messaggio. Il destinarario decifra la chiave di sessione, decifra il messaggio, decifra la firma utilizzando la chiave pubblica del mittente, calcola l'hash del messaggio e lo confronta con quello della firma. Se sono uguali è stata ottenuta integrità (checksum valido), autenticazione (in quanto solo il mittente può avere la chiave privata usata per cifrare il checksum) e segretezza (fornita dalla cifratura del messaggio con la chiave di sessione).

Nell'ambito del protocollo PGP, dire cosa si intende per key ring.

Le chiavi utilizzate da PGP devono essere memorizzate in modo che il loro utilizzo sia efficace. PGP offre all'utente una struttura di nome key ring formata da due strutture dati:

- **Private key ring**: contiene la coppia chiave pubblica/privata dell'utente. La chiave privata viene cifrata con una password nota all'utente.
- **Public key ring**: contiene le chiavi pubbliche delle persone note all'utente

Descrivere l'architettura del protocollo SSL.

L'architettura di SSL è formata dai seguenti 4 protocolli:

- **Protocollo record**: trasporta dati SSL tra diversi peer e fornisce a livelli superiori gli stessi servizi di TCP con in più i servizi di sicurezza
- **Protocollo handshake**: gestisce i parametri di sicurezza, autenticazione e derivazione di chiavi
- **Protocollo change chiper**: segnala la fine dell'handshake
- **Protocollo alert**: gestisce gli errori

Descrivere il processo di handshake del protocollo SSL.

Il client invia al server una lista di algoritmi conosciuti ed un numero RA generato casualmente. Il server risponde con l'algoritmo da utilizzare, il proprio certificato digitale, un numero RB generato casualmente ed un session id.

Opzionalmente il server può richiedere l'autenticazione del client. Se così fosse il client invia al server il proprio certificato digitale, una stringa univoca tra client e server, una chiave (PMS) crittata con la chiave pubblica del server ed infine l'hash dei messaggi precedenti crittato con una chiave (master session) generata dai valori di RA, RB e PMS, che significa la fine dell'handshake.

Il server finirà l'handshake inviando anch'esso l'hash dei messaggi precedenti crittato con la master session.

Descrivere a cosa serve il protocollo AH ed ESP di IPSec.

Il protocollo AH serve per verificare l'identità delle parti, evitare attacchi di replay e per verificare l'integrità mediante una funzione di checksum. Il protocollo ESP si occupa della confidenzialità.

Descrivere a cosa servono i numeri di sequenza del protocollo IPSec.

Servono ad evitare attacchi di replay.

Descrivere cosa rappresenta una relazione di associazione del protocollo IPSec.

Serve per lo scambio delle chiavi, per accordarsi sul tipo di algoritmo crittografico da utilizzare.

GESTIONE DELLA SICUREZZA DI INFORMAZIONI

Definire cos'è ed in cosa consiste un piano di contingenza.

È un piano realizzato per far fronte ad eventi che possono bloccare il sistema a differenza delle misure di sicurezza adottate ed ha come scopo quello di riprendere il normale funzionamento del sistema con costi minimi.

Nell'ambito della sicurezza delle informazioni, elencare e descrivere le sei caratteristiche note come le sei p

1. **Progettazione**: si occupa di pianificare le strategie da adottare in ogni sistema. Ha come scopo principale quello di fornire diversi piani per far fronte a diversi eventi.
2. **Politiche**: sono quelle linee guida che regolamentano il comportamento di un'organizzazione che può avere impatto sulla sicurezza.
3. **Programmazione**: lo sviluppo di contromisure sia logiche che fisiche.
4. **Protezione**: non tutte le risorse necessitano dello stesso grado di sicurezza per cui occorre identificarlo e decidere come comportarsi per ciascuna risorsa.
5. **Persone**: non bisogna sottovalutare il personale aziendale. Oltre alla verifica dei gradi e delle responsabilità occorre controllare anche il rapporto con il personale aziendale e con l'azienda stessa al fine di evitare fughe di informazioni sensibili.
6. **Project managment**: è una disciplina il cui obiettivo è controllare le risorse utilizzate nel progetto, misurare i progressi ed eventualmente aggiustare il processo.

Nell'ambito del processo di sicurezza, dire quale è l'obiettivo della fase di asset identification.

L'obiettivo di questa fase è identificare le risorse da proteggere.

Descrivere il ciclo di vita della gestione del rischio (risk assessment).

1. Identificare le aree di rischio
2. Valutare il rischio
3. Sviluppare ed applicare un piano per la gestione del rischio
4. Rivalutare il rischio

Descrivere le principali strategie di riduzione del rischio.

Un rischio si riduce **evitandolo**, cambiando ed esempio i requisiti di sicurezza, **trasferendolo**, ad esempio subordinando un'altra organizzazione, o **assumendolo**, quindi prepararsi ad affrontare eventuali costi.

Nell'ambito della procedura di risk assessment, definire i parametri risk likelihood e risk impact

- **Risk Lilelihood**: calcola la probabilità che una minaccia si concretizzi in un attacco.
- **Risk Impact**: calcola il costo dell'attacco, sia in termini economici che in perdite.

Descrivere come viene calcolato il risk leverage.

Viene calcolato come segue:

(risk exposure prima della strategia – risk exposure dopo la strategia) / costo risk exposure

Descrivere le diverse tecniche per la valutazione del risk likelihood.

La probabilità può essere calcolata con il metodo classico, il che richiede un modello che non sempre è possibile avere, tramite frequenza relativa, quindi basata su osservazioni, o per via del giudizio di un analista esperto che restituisce un risultato basandosi su un sistema simile.

Nell'ambito del piano di contigenza, definire gli obiettivi del piano di risposta agli incidenti.

L'obiettivo dell'incident response è quello di diminuire l'impatto.

Nell'ambito del piano di contigenza, definire gli obiettivi del piano di business continuity.

L'obiettivo è quello di rendere disponibili le funzioni critiche anche se su un sistema alternativo.

Descrive cosa sono i Common Criteria e perché sono stati introdotti.

Sono una serie di criteri di valutazione della sicurezza in ambito internazionale. Sono stati introdotti perché quelli più antichi non riuscivano più a soddisfare le esigenze di valutazione in ambito internazionale.

Nell'ambito dei Common Criteria, definire i concetti di protection profile e security target.

- **Protection Profile**: insieme di obiettivi e requisiti di sicurezza associabili a generiche categorie di sistemi o prodotti che soddisfano le necessità di sicurezza degli utenti.
- **Security Target**: insieme di requisiti e specifiche di sicurezza associabili ad un sistema o prodotto specifico che è oggetto di valutazione.

Definire le quattro fasi del modello PDCA.

1. **Plan**: Pianificazione del sistema di gestione
2. **Do**: Implementazione del sistema di gestione
3. **Check**: Verifica del sistema di gestione
4. **Act**: Manutenzione e miglioramento del sistema di gestione

Descrivere a cosa serve lo standard BS 7799.

Serve ad **identificare i protocolli più appropriati** al fine di garantire la sicurezza di un sistema.

PRIVATEZZA: TECNOLOGIA E LEGISLAZIONE

Descrivere gli scopi principali dei sistemi per la protezione della privatezza.

Gli scopi principali sono la fornitura di meccanismi che:

- rilasciano informazioni impedendo la possibilità di individuare informazioni su specifiche entità
- limitino la possibilità di acquisire informazioni sensibili
- proteggano dal data linkage, ovvero la possibilità di ricostruire informazioni sull'entità acquisendo informazioni da fonti differenti

Discutere l'affermazione "la privatezza è una problematica multidisciplinare."

Significa che per garantire la privatezza non bisogna solo soffermarsi sull'aspetto tecnologico ma anche su quello legale ed economico.

Nell'ambito delle applicazioni Web, descrivere il processo di raccolta di informazione e perché tale processo pu`o provocare violazioni alla privatezza degli utenti.

Ogni gestore di sito web ricava informazioni sull'utente, sia forniti da egli stesso (mediante i form ad esempio) che inviati dal client (informazioni inviate dal browser). Molte di queste informazioni forniscono specifiche sull'entità della persona e se non protette opportunatamente possono portare alla violazione della privatezza.

Descrivere il funzionamento di un anonymizer e per quali scopi lo si usa.

Non è altro che un proxy e si usa per rendere anonima una navigazione. Il problema è che bisogna fidarsi del gestore del proxy, per cui il problema non viene risolto.

Dire cosa sono i link referenziali e perché possono violare la privatezza degli utenti.

Ogni volta che si passa da un sito all'altro mediante il click su un link, al sito destinazione viene comunicata l'ultima URL del sito originario mediante il campo REFERER del pacchetto HTTP. Se la URL contiene informazioni sensibili (ad esempio: sito.com?name=alice&cartacredito=8287483929), avviene una violazione della privatezza. In qualche modo avviene lo stesso in quanto il sito destinazione, all'insaputa dell'utente, viene a conoscenza del fatto che questo abbia visitato il sito X.

Dire cosa sono i cookie e come possono essere usati per violare la privatezza degli utenti.

Sono delle stringhe di testo inviate dal server al client e poi inviate nuovamente dal client al server quando questo rivisita il sito del server. Risultano dannosi se possono essere letti da siti diversi

Dire cosa sono i web bug e gli spyware.

I web bug sono delle immagini invisibili ad occhio nudo che vengono inserite maliziosamente all'interno di siti al fine di catturare le informazioni inviate dal browser tramite il pacchetto HTTP.

Gli spyware sono altri software il cui scopo è quello di catturare informazioni sull'utente all'insaputa di questo.

Descrivere le principali direttive Europee in materia di privatezza.

Direttiva 95/46: tutela le persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione dei dati.

Direttiva 97/66: trattamento dei dati personali e tutela della vita privata nel settore delle telecomunicazioni.

Queste due direttive introducono il concetto di consenso dell'interessato e la facoltà di decidere di non comparire sull'elenco telefonico e di mantenere l'anonimità nelle chiamate.

Direttiva 2002/58: trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche.

Quest'ultima direttiva garantisce la libertà di circolazione dei dati personali all'interno della CE e vieta qualsiasi forma di intercettazione delle comunicazioni e dei relativi dati, salvo espresso consenso degli interessati o autorizzazione legale.

Descrivere cosa stabilisce l'Art. 8 della carta dei diritti fondamentali dell'UE di Nizza

L'articolo 8 della Carta dei diritti fondamentali dell'UE di Nizza rappresenta l'evoluzione della tutela della privacy a livello internazionale, riconoscendo il diritto di protezione dei dati personali, la lealtà del trattamento, il consenso dell'interessato, l'accessibilità della persona interessata ai propri dati, ribadendo che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.