

Esperti nella gestione dei sistemi informativi e tecnologie informatiche

Analisi del rischio e sicurezza delle attività

Valutazione finale

Regole per lo svolgimento della prova: E' consentito l'uso di dispense cartacee, della rete Internet e di appunti presi a lezione. Il compito deve essere svolto singolarmente (avete gli appunti e le dispense a cui fare riferimento).

Tempo per lo svolgimento della prova: 1,5 ore.

1) Dare la definizione di sicurezza informatica

La Sicurezza informatica è quella branca dell'informatica che si occupa della salvaguardia dei sistemi informatici da potenziali rischi e/o violazioni dei dati.

Si divide in sicurezza attiva e sicurezza passiva. La prima ha il compito di rendere i dati intrinsecamente sicuri mentre la seconda si occupa della difesa dei dati da accessi non autorizzati.

Sono due attività complementari.

2) Cos'è un attacco di tipo Denial of Service? Cosa si potrebbe fare per contrastarlo?

Il Denial of Service è un tipo di attacco pensato per rendere non disponibile un servizio o un server su Internet.

L'attaccante invia un lungo stream di pacchetti di attacco al target: sommergendo il target, annullando la capacità del target di reagire al sovraccarico.

Lo scopo è quello di fare in modo che i sistemi non riescano più a servire i clienti.

Per limitare questo tipo di attacchi si potrebbe impostare un firewall in maniera appropriata e contattare il provider degli attaccanti.

3) Quale di questi non è un sistema di autenticazione biometrico?

- Riconoscimento dell'impronta digitale
- Scansione dell'iride
- Access Token
- Riconoscimento della geometria facciale

4) Quale di questi personaggi è più pericoloso per la sicurezza di un sistema informativo?

- White Hat Hacker
- Black Hat Hacker
- Script Kiddie

5) Dare la definizione di Social Engineering (Ingegneria Sociale) e spiegare come contrastare il fenomeno.

Il Social Engineering consiste nell'ingannare un impiegato per ottenere informazioni o compiere un'azione che riduce la sicurezza del sistema o danneggia il sistema stesso.

Alcuni esempi possono essere: chiedere una password spacciandosi per uno che ha il diritto di conoscerla o chiedere di inviare un file contenente delle password.

Alcune tecniche di protezione possono includere training ed educazione e rinforzo attraverso sanzioni (punizioni).

6) Come risolvo il problema delle intercettazioni e degli attacchi Man In The Middle?

- Adotto un sistema di crittografia simmetrica
- Adotto un sistema di crittografia a chiave pubblica
- Utilizzo un sistema di verifica dell'identità

7) Cosa sono gli Intrusion Detection System (IDS) e i Firewall? Come possono essere impiegati?

Un IDS è come un campanello di allarme: avverte l'amministratore se riscontra un possibile attacco nascosto nei pacchetti in arrivo.

L'amministratore può prendere dei provvedimenti in modo da rendere inutili i vari tentativi di attacco. Un IDS controlla tutti i pacchetti in arrivo o in partenza ma non compie azioni sui pacchetti, seppur memorizzandoli per ulteriori analisi.

I firewall sono particolari computer progettati per tenere i messaggi dell'attaccante fuori della LAN e permettere ai messaggi di utenti autorizzati di passare all'interno di questa.

Esaminano ogni pacchetto in arrivo o in partenza: se viene riconosciuta la signature di messaggi ritenuti pericolosi eliminano il messaggio altrimenti lo immettono nella LAN.

Il dropping dei pacchetti nei firewall viene effettuato solo se si è avuta la violazione di specifiche regole. Anche negli IDS c'è l'identificazione dei pacchetti, ma sulla base di semplici sospetti, e che, quindi non possono essere eliminati arbitrariamente.

Possono essere utilizzati contemporaneamente per innalzare il livello di sicurezza nel sistema.

8) Quanti livelli prevede il protocollo di trasmissione TCP/IP?

- 7 livelli
- 5 livelli
- 4 livelli

9) Quali di queste caratteristiche non possono essere associate al sistema di crittografia a chiave pubblica RSA?

- E' sicuro se utilizza numeri primi molto elevati
- E' basato su metodi matematici
- E' molto veloce
- Non devo trasferire nessuna chiave privata

10) Quale password è in grado di resistere più a lungo ad un attacco a dizionario?

- ciao001
- <0mPu7&r
- password
- qu35710n4r10