Introduzione

Return

Indice

Introduzione alla Sicurezza dell'Informazione

Morris Internet Worm

Primo Worm su Internet, 1988, lanciato da un lab del MIT.

Colpiva sistemi UNIX sfruttando delle vulnerabilità di alcuni software.

Il tipo di attacco ricate nella categoria DOS (Denial of Service). Si manifesta perchè il worm si auto-reinstallava nello stesso pc più volte.

Tipi di attacchi informatici

Spoofing

consiste nel fingersi qualcun altro. Il più comune è **IP Spoofing** in cui si falsifica il *Source Address* di un pacchetto IP.

DOS (Denial of Service)

Il DOS consiste nel negare l'accesso ad un servizio. Può essere causato con **SYN flood** inondando di pacchetti SYN un server facendo riservare spazio in memoria per ogni connessione.

Hijacking

Dirottare il traffico da un host A ad un host B su un terzo host C. **Man in the middle**

Codice maligno o Trojan

Un trojan è un programma che si presenta come un software legittimo ma in realtà contiene codice maligno mettendo a rischio i dati di un sistema. Non si autoreplica a differenza dei virus.

Accesso non autorizzato

L'accesso non autorizzato è un attacco in cui un utente riesce ad accedere a dati o sistemi per cui non ha i permessi. Può essere causato da una vulnerabilità del sistema o da credenziali rubate.

Port scanning/probing

Per scoprire quali porte soono aperte e quali servizi sono in ascolto su di esse per permettere un attacco.

Virus e Worm

Programmi maligni che infettano sistemi operativi. I virus si attaccano a un file mentre i worm sono programmi indipendenti.

Data sniffing

Ascolto di un canale catturando informazioni scambiate tra host.

Definizioni base

Confidenzialità

Mira a garantire che, nello scambio di informazioni fra un mittente e un destinatario, un terzo soggetto non possa venire a conoscenza del contenuto di tali risorse.

[[01.DatiSicuri]]

Caratteristica di un dato che non ha subito modifiche nel contenuto (intenzionali o accidentali)

Disponibilità

Prevenire la non accessibilità delle informazioni ai legittimi utilizzatori

Quando miriamo a proteggere delle informazioni, siamo interessati a garantire il rispetto di una o più delle suddette caratteristiche. Vogliamo essere certi dell'identita con cui interagiamo quindi definiamo meccanismi di **autenticazione**. Il **non ripudio** di un'informazione è un altro requisito che potremmo desiderare.

Progettare per la sicurezza

Rispondiamo alle seguenti domande:

- Quanto valgono le informazioni?
- Come possiamo quantificare il rischio di un attacco?
- Come possiamo quantificare il danno subito con la perdita di informazioni?
- Quanto costa proteggere le informazioni?

Per garantire i requisiti di sicurezza si utilizzano **servizi di sicurezza**. Questi utilizzando uno o più **meccanismi di sicurezza**.

Gestione della Sicurezza Informatica

Definizioni di base

La stesura di un **piano di sicurezza** tiene conto di misure **tecnologiche, organizzativi** e **normative**.

Analisi del contesto

Rilevazione e documentazione del sistema informativo: individuano i flussi informativi, quali processi vengoono utilizzati e quali requisiti di sicurezza sono richiesti.

Analisi del contesto normativo e legislativo vigente.

Analisi del sistema informatico

Censimento delle risorse hardware e software al dine di individuare i punti deboli e le responsabilità di gestione di ogni componente. Censimento di dati e archivi che prevede lo stiduio dei contesti operativi delle risorse, requisiti e politiche di backup.

Analisi e valutazione dei rischi

Vulnerabilità della azienda. Si raggruppano i dati in DATA ASSET. Ogni tipo di vulnerabilità può dare luogo ad un attacco.

Per ogni tipo di vulnerabilità si deve determinare il costo del danno.

Individuazione e valutazione delle contromisure

Si valutano le contromisure per le vulnerabilità trovae.

Formulazione del piano di sicurezza

Il piano di sicurezza è un documento che contiene le informazioni necessarie per la gestione della sicurezza informatica. Deve essere redatto in modo chiaro e comprensibile, in modo da poter essere utilizzato come guida per la gestione della sicurezza.