

LA SOLUZIONE

www.unmondodisoluzioni.it



E*MAZE
ipLegion



ipLegion è la soluzione in grado di identificare i servizi di vulnerabilità in una rete (computer ed apparecchiature di rete) attraverso una serie di simulazioni di attacco controllate e pianificate; ipLegion genera inoltre dettagliati rapporti riguardo i problemi riscontrati che comprendono le indicazioni per risolverli.

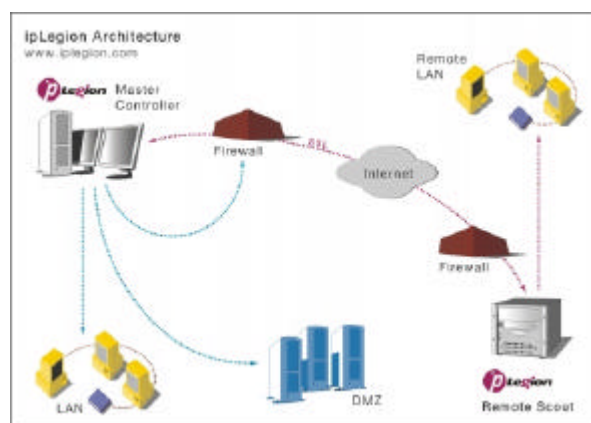
ipLegion è in grado di analizzare i sistemi operativi ed i servizi disponibili su rete IP e di testare le vulnerabilità presenti sulla apparecchiature connesse quali Server, Router, Firewall, Switch. La tecnologia ipLegion è ottimizzata per la piattaforma Sun.

PRINCIPALI CARATTERISTICHE

I punti chiave che rendono la soluzione peculiare possono essere così riassunti:

- **Multilingue:** interfaccia web multilingue. Linguaggi attualmente supportati: Italiano, Inglese, Tedesco e Spagnolo.
- **Scheduling:** è possibile fissare una scansione con predeterminate preferenze per effettuare test in specifiche date o a intervalli regolari senza alcun ulteriore intervento.
- **Security Checks:** ipLegion è basato su un insieme di test specifici per ogni vulnerabilità, aggiornato in tempo reale.
- **On-Demand Scanning:** il sistema può lanciare automaticamente un test ogni volta che un nuovo security check viene inserito nel database.
- **Scansioni di Reti:** è possibile testare intere sottoreti (gruppi di IP) o un singolo IP. Le sottoreti possono essere condivise con altri utenti o con altri gruppi di utenti
- **Moduli Scout:** gli Scout possono essere facilmente posizionati nelle reti IP per eseguire le scansioni dall'interno.
- **Sicurezza:** la connessione è protetta da HTTPS e da chiavi a 2048 bit
- **Licensing:** per scansione, per IP e ibrido.
- **Report:** i report completi o brevi sono disponibili in formato PDF e HTML.
- **Sviluppo di Security Check Ad Hoc:** l'insieme dei test già esistenti può essere integrato con

security check personalizzati per soddisfare esigenze particolari.



ipLegion presenta un'architettura che include i seguenti moduli tecnologici: Web Server, Database, Scout, Master Controller.

VANTAGGI DELLA SOLUZIONE

- **Amministrazione:** ipLegion è multiutente e permette più accessi contemporanei. ipLegion prevede una gestione gerarchica delle utenze che permette di creare utenti con differenti livelli di privilegi. La possibilità di riunire i singoli IP in più gruppi può essere usata per condividere la visibilità delle sottoreti così create. Ogni utente può essere abilitato a compiere determinate azioni su determinati gruppi.
- **Report:** I risultati possono essere organizzati e visualizzati secondo Host, Porta e Vulnerabilità. I report offrono un'analisi dei sistemi target anche tramite report differenziali che comparano i risultati rilevati con quelli memorizzati nello storico. Si può accedere al database tramite interfaccia SQL per estrarre ogni informazione rilevante da poter integrare con altri sistemi. Il motore ipLegion non richiede alcun intervento manuale di revisione dei dati, quindi i risultati di una scansione possono essere consultati non appena il test è finito. I report sono disponibili con 2 diversi livelli di dettaglio in formato PDF e HTML. E' stata implementata anche una semplice visione dell'intera rete analizzata.





LA SOLUZIONE

- **Scansioni:** ipLegion effettua un'approfondita scansione di tutte le porte e protocolli sugli host target, analizzando le porte aperte ed i servizi trovati per simulare automaticamente una sequenza di attacco. Un target host può essere un computer o un'apparecchiatura di rete (con protocollo TCP/IP). Ogni scansione è controllata da un'interfaccia grafica che mostra lo stato di avanzamento del test.
- **Fix;** Le informazioni relative ai rimedi per i problemi evidenziati dai test sono incluse nei report insieme a riferimenti a documenti esterni, advisory, informazioni ufficiali dei vendor, patch, agli identificativi CVE delle vulnerabilità trovate e a dettagliate informazioni per verificare manualmente l'esistenza delle vulnerabilità. Queste informazioni possono essere usate per eliminare i problemi ed evitare il loro illecito sfruttamento.
- **Preferenze:** Gli utenti possono definire insieme di IP per organizzare il lavoro di scansione in aree (dipartimenti, tipi di host, ecc.). Possono essere definiti degli insiemi di regole con le quali i test devono essere effettuati (numero delle porte coinvolte, tipo di servizi, ecc.) specificando le singole vulnerabilità da cercare o le famiglie di test di proprio interesse o il livello di rischio dei problemi. L'uso di test di tipo "DoS" può essere selezionato secondo necessità. Gli utenti possono scegliere il linguaggio dell'interfaccia e il fuso orario di riferimento

Scout permette così ad ipLegion di coprire reti di qualsiasi complessità e topologia.

LA SOLUZIONE ED IL MERCATO

A causa dell'utilizzo sempre più diffuso di reti informatiche e della accresciuta dipendenza di molte aziende da queste reti, le questioni associate alla sicurezza hanno assunto un'importanza fondamentale. Un vulnerability assessment aiuta un'organizzazione a comprendere a quali rischi sia esposta la sua infrastruttura di rete e offre misure correttive da adottare per creare un ambiente operativo a prova di intrusione.

A CHI SI RIVOLGE LA SOLUZIONE

Una soluzione di vulnerability assessment consente l'erogazione di un servizio che contribuisce ad ottenere e a mantenere la lealtà della propria clientela, permette inoltre di rispettare i requisiti finanziari ed assicurativi, a proteggere la propria organizzazione da implicazioni legali, a prevenire accessi non autorizzati e attacchi di tipo denial of service, a creare gateway sicuri per l'accesso alle informazioni, a mettere alla prova le proprie contromisure di sicurezza, proteggendo così i propri redditi.

I MODULI TECNOLOGICI

Web Server: Per accedere e utilizzare ipLegion viene usato un web server. E' possibile così collegarsi al sistema da qualsiasi workstation con un Internet Browser. Tutte le attività sono gestite attraverso quest'unica interfaccia. I dati sono protetti da una connessione HTTPS.

Database: E' il database relazionale sul quale si appoggia il sistema. Memorizza le caratteristiche degli account, le preferenze e i dati raccolti dagli utenti, le vulnerabilità, le informazioni per risolvere i problemi ed i report. Il database funziona tramite chiamate SQL ed è interfacciabile tramite ODBC.

Scout: E' il modulo di scansione di ipLegion. E' in contatto con il Master Controller e ne attua le richieste di scansione. La connessione tra Master Controller e Scout è protetta tramite il protocollo SSL/TLS. Può essere usato anche in presenza di un Proxy Server.

Master Controller: E' il cuore del sistema che si occupa dell'interfacciamento al database, gestisce le comunicazioni con gli Scout e distribuisce nella misura stabilita le scansioni tra gli Scout: La scalabilità degli

Per Maggiori informazioni:

www.unmondodisoluzioni.it

www.icos.it

www.ipLegion.it

www.emaze.it

www.springfirm.it

www.01net.it/wip/icos/

