]HackingTeam[| SEAT PAGINE GIALLE SPA

Seat PG

Soluzione di Intrusion Detection sull'infrastruttura di backbone

Milano

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	18 Luglio 2005	Prima stesura
//	//	//
//	//	//

INFORMAZIONI		
Data di Emissione	18 Luglio 2005	
Versione	1.0	
Tipologia Documento	Allegato Tecnico	
Numero di Protocollo	//	
Numero Pagine	11	
Numero Allegati	0	
Descrizione Allegati	1	//
	2	//
Redatto da	Andrea Cariola Claudio Agosti	
Approvato da	Gianluca Vadruccio	

INDICE

FIGURE

1 Obiettivo

Lo scopo del progetto è quello di analizzare la tipologia di traffico esistente nell'infrastruttura del cliente ed installare una piattaforma di intrusion detection che permetta di rilevare anomalie ed eventuali attacchi alla sicurezza informatica.
Avendo ben chiari e definiti:

- il traffico che la rete interna gestisce
- l'esposizione a minacce ed il livello degli attacchi subiti
- il grado di tuning necessario
- la quantità di falsi positivi generati ed il relativo livello di allarmistica
- la gestione degli incidenti informatici necessaria
- l'efficacia e la adeguatezza di strumenti free per la detection

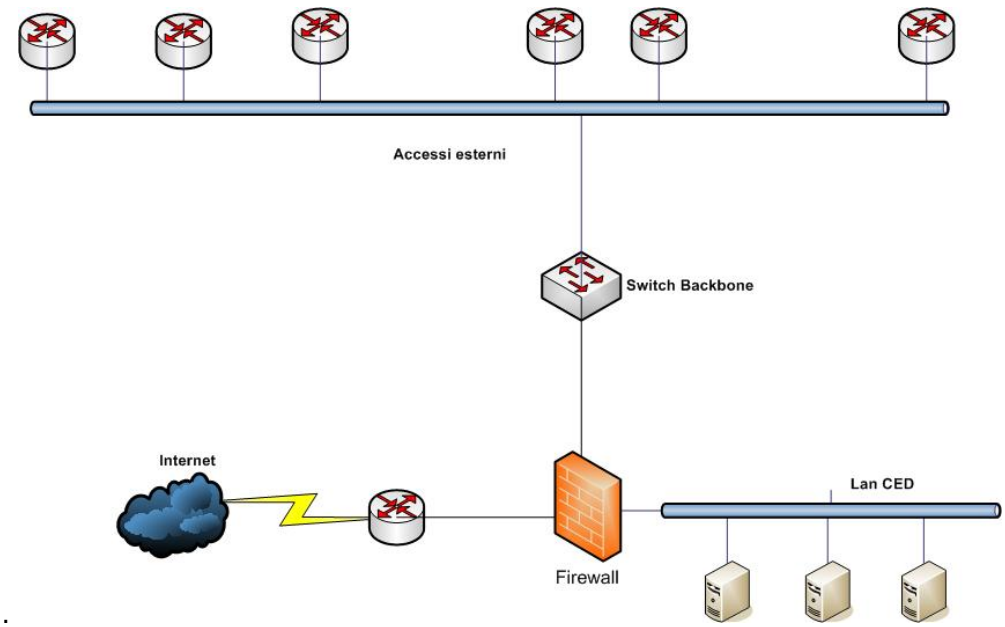
si potrà in seguito pianificare e progettare al meglio quello che sarà il Sistema Anti-Intrusione di Seat Pagine Gialle. Lo scopo principale delle attività descritte e proposte è quindi quello di analizzare e stabilire con precisione e chiarezza tutti i punti sopra elencati.

Per il corretto perseguimento dell'obiettivo, l'installazione del sistema di intrusion detection avverrà sulla rete di backbone del cliente, al fine di ottenere un'analisi di massima riguardo le minacce telematiche in transito a livello generale.
Agendo in questo modo si perderanno tutti quegli attacchi e quei protocolli che iniziano e terminano le loro attività in un ambito locale e che quindi non transitano attraverso il nodo centrale di backbone. Questa modalità di procedere è utile a limitare le attività necessarie per quella che deve essere solo una fase di scrematura iniziale di requisiti e funzionalità di intrusion detection.

Alla fine delle attività, il cliente avrà un documento che contiene la descrizione delle attività effettuate ed una dettagliata analisi dei risultati ottenuti. Saranno presenti tutti quegli elementi necessari alla corretta futura progettazione e configurazione del sistema di Intrusion Detection di Seat Pagine Gialle.

2 Ambiente di riferimento

L'ambiente di riferimento è schematizzato nella seguente Figura 1. Si noti che tale schema non ha alcuna pretesa di completezza, il solo scopo è di formalizzare il contesto tecnologico nel quale l'offerta è considerata valida.



.

Figura 1 - Ambiente di riferimento

Per semplificare la topologia, si è suddiviso l'ambiente in tre aree:

- Area Internet
  - L'accesso è garantito e protetto attraverso un cluster firewall che controlla e separa l'esterno dalla rete dei server e dalla rete interna.
- Area CED
  - Si tratta della rete maggiormente critica per il business del cliente ed è protetta dal cluster firewall di internet. Ospita tutti i server di produzione, tratta i dati maggiormente sensibili ed è costituita da una sottorete fisica senza altri accessi né in ingresso né in uscita.
- Area interna e di accesso
  - E' l'area maggiormente complessa. Vi sono presenti accessi dall'esterno di utenti (fissi e mobili), di fornitori, di sedi geograficamente dislocate e di tutti quei link logici

e fisici che devono garantire connettività degli utenti. Anch'essa è protetta dal cluster firewall di internet dal quale è separata dal nodo di backbone.

3 Analisi dei requisiti

Per svolgere un'analisi passiva del traffico, è necessario disporre di apparati che consentano la duplicazione del traffico verso i sistemi di intrusion detection, nonché dell'hardware per implementare il sistema IDS stesso.

Per la duplicazione del traffico, si possono utilizzare le seguenti tecnologie:

- Porta mirror: opportuna configurazione dei devices di secondo livello per consentire la duplicazione del traffico di determinate porte verso una specifica porta (alla quale sarà attestata una sonda di intrusion detection oppure un apparato di rete che funge da collector dei pacchetti).
- TAP: inserimento nel flusso da monitorare di un apparecchio in grado di spillare il traffico full duplex e contemporaneamente di consentire al normale traffico di fluire regolarmente. Tale traffico (RX e TX) confluirà ad una sonda di intrusion detection oppure ad un apparato di rete che funge da collector dei pacchetti.

In entrambi i casi, una volta duplicato il traffico, quest'ultimo potrà essere spedito direttamente al sistema di intrusion detection oppure potrà essere indirizzato verso un nodo di collector al quale confluiranno eventuali altri traffici e al quale sarà attestato il sistema di analisi e rilevamento delle intrusioni.

Per evitare qualsiasi tipo (anche minimo) di sovraccarico agli switches e per evitare problematiche legate alla sua configurazione, si consiglia di adottare la seconda tecnologia; di utilizzare quindi i dispositivi TAP per lo spillamento del traffico. Ovviamente l'apparato di spilling consente il passaggio del flusso principale in qualsiasi condizione, compresa quella di propria mancanza di alimentazione o di proprio fault.

Addentrandosi nella parte tecnologica di un sistema di rilevamento ed eventualmente prevenzione delle intrusioni, si può affermare che le componenti principali di un sistema IDS completo riguardano la protezione di tre ambienti:

- Network Protection: protezione della rete a cui è assegnato. L'attività consiste nell'analizzare il flusso dei pacchetti transitanti con l'obiettivo di rilevare eventuali attacchi informatici e di monitorare la tipologia di traffico.

- Server Protection: protezione dei server su cui è installato. L'attività consiste nell'analizzare le attività locali alla ricerca di violazioni dell'integrità o della sicurezza della macchina.
- Desktop Protection: protezione dei desktop o dei laptop su cui è installato. L'attività consiste nell'analizzare le attività locali alla ricerca di violazioni dell'integrità o della sicurezza del PC utente sia quando si trova all'interno della rete sia quando si trova all'esterno del perimetro.

Essendo l'attività descritta propedeutica alla vera e propria progettazione di un sistema di intrusion detection, la proposta tecnologica di questa fase *esplorativa* prevede l'utilizzo della componente network-based IDS.

Nel caso si abbia a che fare con limitate occupazioni di banda e numerosi segmenti di rete da monitorare, si può ricorrere ad una forma di aggregazione del traffico in maniera tale da evitare che i costi della soluzione lievitino a causa

- del numero elevato di sensori
- della complessità di gestione che si genera

Una possibilità architetturale consiste nel concentrare il traffico in uno o in pochi punti di controllo per consentire l'analisi di più segmenti di rete o in generale sorgenti di traffico ad un solo sensore IDS (o a pochi sensori IDS qualora si stia trattando con una topologia architetturale complessa).

Questo tipo di architettura, correttamente supportata dalla tecnologia, permette, in aggiunta a quanto sopra menzionato, di avere un sistema di rilevamento delle intrusioni attivo in alta affidabilità o addirittura in bilanciamento del carico. Ad esempio, qualora il punto di controllo accentrato fosse rappresentato da un bilanciatore, si potrà configurare il sistema per garantire la spedizione del traffico su uno degli altri sistemi di monitoraggio qualora avvenisse un fault nella relativa sonda IDS.

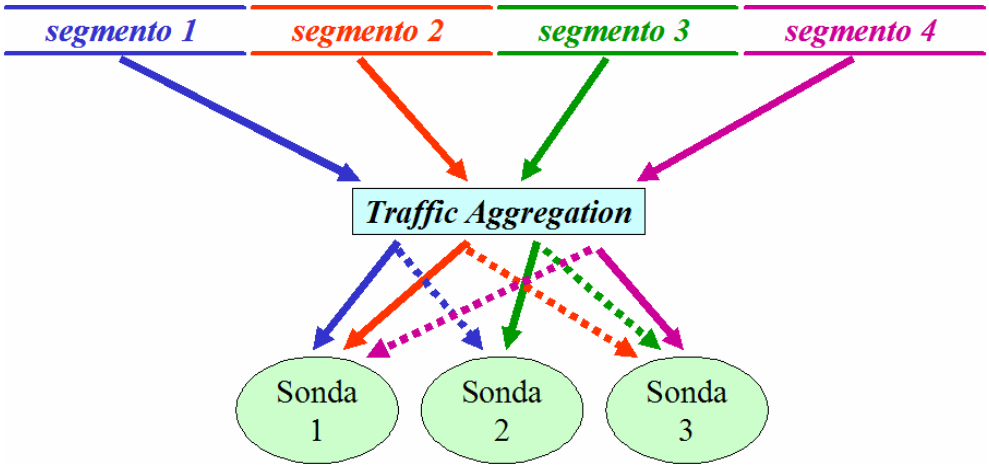


Figura 2 - Aggregazione e bilanciamento

In Figura 2, il flusso primario di ogni segmento è affidato ad un sensore specifico (freccia a linea intera); qualora un sensore dovesse avere un fault, il flusso primario non viene più controllato e a questo punto interviene il sensore di backup che si attiva e controlla relativo flusso secondario (freccia a linea tratteggiata).
L'utilizzo di un aggregatore con funzionalità di bilanciamento potrà essere evidenziato e confermato solo da una specifica richiesta o esigenza del cliente. Con le poche informazioni attualmente disponibili questo approccio non è ritenuto indispensabile, se non a fronte di una analisi approfondita prevista all'inizio delle attività.

4 Descrizione della soluzione

La soluzione proposta prevede l'installazione di una sonda SNORT di analisi che riceve il traffico. In relazione alle tecnologie di duplicazione, alla quantità di dati da analizzare e alla centralizzazione dell'infrastruttura si possono implementare delle varianti specifiche.
Le tecnologie di duplicazione del traffico devono integrarsi nell'infrastruttura dopo un'attenta analisi. Come sopra detto, principalmente se ne possono distinguere due tipologie: attive e passive.

1. Duplicatori attivi sono ad esempio switch con porte di monitoring.
2. Duplicatori passivi sono ad esempio i TAP che richiedono una configurazione più oculata delle sonde e favoriscono la decentralizzazione della soluzione sia come numero di interfacce di rete che, di conseguenza, numero di sonde.

Un utilizzo ibrido delle due modalità, consente in linea di massima di ottenere un buon compromesso in termini di risorse utilizzate (sia fisiche che logiche).
La soluzione proposta prevede l'installazione di una sonda per ogni flusso di traffico da monitorare. L'utilizzo di una modalità attiva o passiva verrà deciso a seconda del tipo di traffico e dell'hardware che gestisce il segmento di rete in questione, nell'ottica di avere l'impatto minore possibile sulla normale operatività degli apparati e offrire una soluzione modulare.

Nello schema che segue (Figura 3) viene rappresentato un esempio di implementazione con 2 sonde ed una console/database collector.

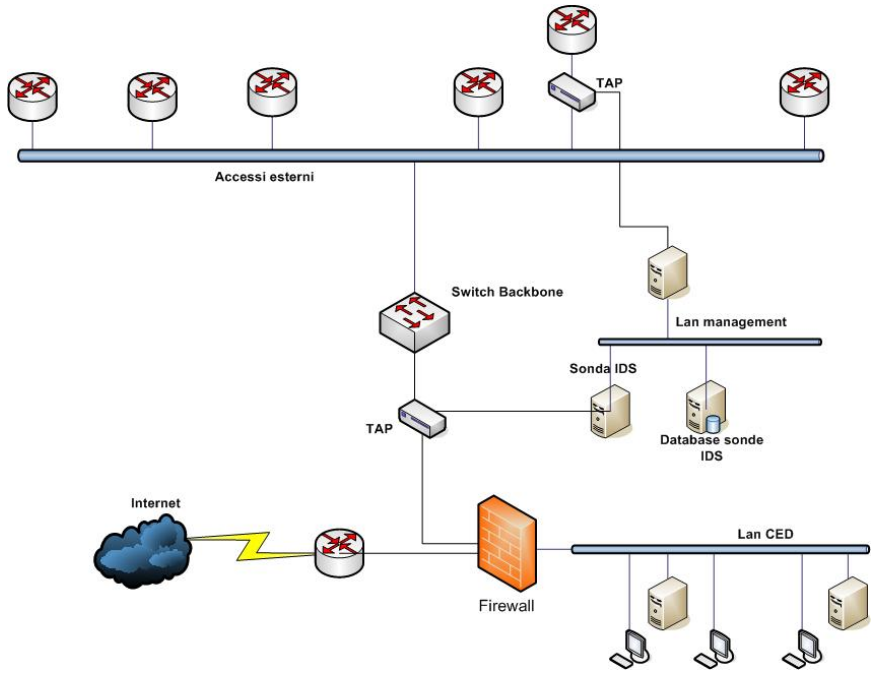


Figura 3 - Soluzione con TAP

Eventuali varianti potranno essere le seguenti:

- una sonda ids potrà essere attestata non ad un TAP ma ad una porta di monitoring
- una sonda potrà essere attestata direttamente al nodo di backbone (con limitazioni legate alla quantità di traffico)
- tutto il traffico, proveniente sia da TAP che da porte monitoring, potrà essere convogliato in un unico switch con attestata/e (in port monitoring) una o più sonde ids a seconda del traffico

La corretta architettura potrà essere definita e confermata solo

- **dopo una valutazione attenta degli obiettivi e dei requisiti**
- **dopo una precisa e dettagliata analisi della topologia di rete fisica e logica**
- **dopo una fase iniziale di analisi del traffico**
- **dopo una corretta progettazione del sistema di rilevamento**

5 Metodologia

La metodologia che sarà seguita per il delivery dell'intero progetto è dettagliata nella seguente figura:

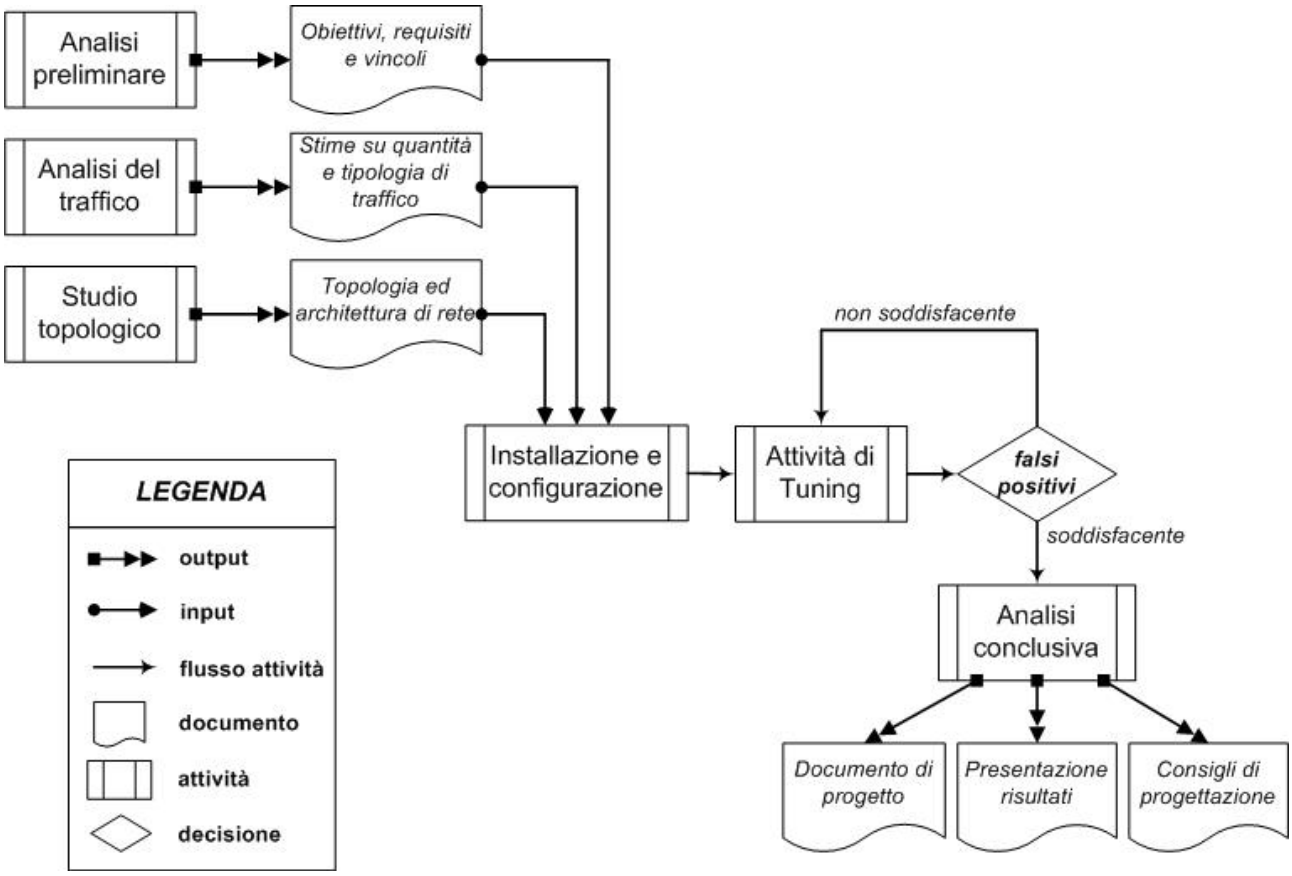


Figura 4 - Flusso di attività operative

Per la corretta impostazione ed implementazione di questo progetto si ritiene importante una fase iniziale in cui verrà posizionato un network sniffer, nello stesso punto (o negli stessi punti) dove poi sarà posizionata la sonda IDS; questo sistema registrerà il traffico dei segmenti di rete prescelti per 2/3 giorni.

Successivamente il traffico catturato sarà oggetto, presso la nostra sede, di analisi comparativa tra un sistema Snort ed altri prodotti di intrusion detection allo scopo di determinare la differente segnalazione di attacchi sul traffico del cliente. In questo modo si potranno eliminare in buona parte i falsi positivi e quindi già in fase di startup presso il cliente partire con una più significativa reportistica del sistema IDS Snort.

Contemporaneamente saranno definiti e convalidati gli obiettivi che il cliente intende perseguire con il progetto e si procederà inoltre alla analisi della topologia di rete logica e fisica esistente. L'insieme dei risultati ottenuti dalle fasi appena descritte consentirà di pianificare ed eseguire al meglio la successiva fase di installazione, configurazione e tuning di base del sistema Snort di intrusion detection network-based.

La fase di tuning della sonda Snort sarà effettuata sia subito dopo l'installazione sia ad intervalli di circa 10 giorni per 3/4 volte successive a seconda delle necessità rilevate in corso d'opera.

Al termine dell'intero progetto verrà rilasciato un documento finale composto da tutti i deliverables elencati in figura.

6 Macro attività

A livello tecnico, le fasi del progetto saranno le seguenti:

- Creazione di una soluzione modulare per le sonde e la gestione degli eventi
- Studio dell'infrastruttura oggetto del monitoring
- Presentazione dello schema di rete risultante dalle attività svolte in questo progetto
- Introduzione delle sonde e del sistema di analisi dei log con minimo impatto sull'infrastruttura
- Osservazione dell'andamento dell'attività svolta dalle sonde, processo di tuning di base ed eventuale processo di tuning incrementale successivo
- Presentazione di un documento contenente i risultati delle attività di analisi del traffico svolta dalle sonde durante il monitoring