UNIVERSITÀ DEGLI STUDI DI CAMERINO

FACOLTÀ DI SCIENZE E TECNOLOGIE

Corso di Laurea in Tecnologie Informatiche

Dipartimento di Matematica e Informatica

IDS/IPS ANALISI COMPARATIVA

Tesi di Laurea
In
Reti di Calcolatori

Laureando

Ercoli Andrea

Relatore

***Prof.* Fausto Marcantoni**

ANNO ACCADEMICO 2009 / 2010

Alla mia famiglia che ha sempre creduto in me

Indice

Introduzione

Negli ultimi anni il crescente sviluppo di Internet, delle tecnologie correlate ed il continuo inserimento in rete dei sistemi informatici di tutto il mondo, ha reso importante e delicato il problema della sicurezza nelle reti di calcolatori.

Basti considerare che, oltre ai sistemi commerciali della vendita di beni e servizi, sono sempre maggiori i sistemi bancari, assicurativi, di pubblica amministrazione che offrono, tramite internet, i propri servizi al cittadino.

Non basta più configurare correttamente i dispositivi hardware e software nella propria rete per stare tranquilli perché, nonostante la presenza dei già noti mezzi di difesa come Antivirus e Firewall, molti sono i tentativi di intrusione che le nostre reti, aziendali e non, possono subire.

E' stata quindi ideata un'ulteriore linea di difesa nella rilevazione degli accessi illegittimi: gli IDS e IPS, rispettivamente Intrusion Detection System e Intrusion Prevention System, o brevemente IDPS.

Questi strumenti hardware o software, sono impiegati per individuare accessi non autorizzati ai computer o alle reti locali attraverso l'analisi del traffico di rete o degli archivi delle connessioni, sulla base di regole definite a priori sfruttando database, librerie e signature (firme d'attacco) per rilevare e prevenire intrusioni.

Già ci sono moltissimi IDPS in circolazione ed è interessante osservare che la maggior parte di questi appartengono al software libero, indi open source.

Scopo di questo studio è l'analisi e il raggruppamento di tutti questi software in una tabella che rispecchi le caratteristiche di ognuno, al fine di avere un quadro generale sui vari prodotti a disposizione.

L'opera sarà articolata in due sezioni:

- **Capitolo 1:** si fornisce un'introduzione ai concetti base di Intrusion Detection e Prevention e si presenta una panoramica delle tecnologie IDPS, inclusi componenti tipici e le metodologie di rilevamento.

- **Capitolo 2:** si presenta una descrizione dettagliata di tutte le caratteristiche individuate, un Data Sheet per ogni software testato e una serie di Tabelle comparative riportanti i risultati della ricerca.

Infine descriveremo brevemente l'ambiente di test del progetto seguito da alcune conclusioni e considerazioni sul lavoro svolto.

Capitolo 1 - Principi di Rilevamento e Prevenzione delle Intrusioni

La rilevazione delle intrusioni è il processo di monitoraggio degli avvenimenti che avvengono in un computer o in una rete e l'analisi di questi per trovare segni di possibili inconvenienti quali violazioni, pericoli imminenti di violazione della sicurezza del computer o pericoli di corruzione dati.

Questi inconvenienti hanno cause multiple, come malware persone che accedono senza autorizzazione al sistema da Internet, utenti autorizzati del sistema che abusano dei propri privilegi per minare alla sicurezza, o che cercano di guadagnare più privilegi per accedere a zone non autorizzate.

Sebbene molti inconvenienti siano volutamente malintenzionati, ne esistono molti altri anche di natura accidentale, ad esempio una persona potrebbe sbagliare a scrivere l'indirizzo di un computer ed entrare erroneamente in un altro sistema senza autorizzazione.

Un Intrusion Detection System (IDS) è un software che riesce a rendere automatico il processo di rilevazione delle intrusioni cercando di distinguere le minacce reali da quelle accidentali.

Un Intrusion Prevention System (IPS) è un software che ha tutte le capacità di un Intrusion Detection System, ma può anche tentare di fermare i possibili attacchi in maniera attiva.

1.1 Uso degli IDPS

Sia IDS che IPS sono primariamente focalizzati nell'identificazione di un incidente.

Ad esempio possono individuare quando qualcuno è riuscito a compromettere il sistema sfruttando una falla di sicurezza. L'IDPS potrebbe allora riportare la notizia all'amministratore della rete o chi di dovere, permettendogli di iniziare velocemente azioni preventive per minimizzare o annullare i danni causati dall'attacco. L'IDPS può anche registrare i dati dell'attacco per permetterne il successivo studio, sia per capire le nuove modalità di attacco, sia per risalire al responsabile.

Molti di questi software possono anche identificare attività di ricognizione, che possono indicare un attacco imminente. Infatti molti strumenti di attacco, ed in particolare i malware worms, eseguono una ricognizione tramite host e port scan per identificare gli obbiettivi dell'attacco successivo. L'IDPS quindi blocca questa attività di "scanning" e notifica l'amministratore della sicurezza, che può prendere provvedimenti.

Dato che le sonde sono un'attività molto frequente su Internet, il rilevamento di queste ultime viene effettuato prima nelle reti interne protette.

In aggiunta all'identificazione e prevenzione degli inconvenienti, gli IDPS possono avere anche altri usi:

- **Identificazione problemi di sicurezza:** Se installato in una posizione idonea, l'IDPS può effettuare un controllo di qualità sui sistemi di sicurezza già presenti, come vedere se ci sono duplicati nei firewall rulesets, oppure allertare quando è presente traffico di rete che dovrebbe essere bloccato dal firewall, ma non lo è per una sua probabile configurazione errata.

- **Documentare una minaccia esistente:** Grazie alla registrazione delle informazioni riguardo le minacce rilevate, si possono capire la frequenza e le caratteristiche degli attacchi verso le risorse del sistema, cosi da poter trovare le giuste contromisure.

- **Scoraggiare gli individui dal violare la sicurezza:** Sapere che le proprie azioni sono costantemente monitorate da un IDPS potrebbe intimidire intenzioni di violazione.

Vista la sempre maggiore importanza che stanno acquisendo le informazioni e quindi il crescente impatto che hanno le intrusioni su questi sistemi, gli IDPS stanno diventando un'aggiunta necessaria ad ogni sistema di sicurezza.

1.2 Componenti

Componenti tipici:

I componenti tipici che costituiscono un IDPS sono i seguenti:

- **Sensori o Agenti:** I sensori e gli agenti sono quelli che effettivamente monitorizzano ed analizzano l'attività. Il termine sensore viene tipicamente usato per gli IDPS che osservano le reti, compresi i Network-Based, Wireless e Network Behavior Analysis, mentre il termine agente è usato per gli Host-Based IDPS.

- **Server di gestione:** Un server di gestione è un dispositivo centralizzato che riceve informazioni dai sensori o dagli agenti e li organizza. Alcuni server possono addirittura analizzare i dati in ingresso per individuare anomalie sfuggite ai sensori o agenti. Alcuni IDPS fanno a meno del server di gestione, lasciando tutto il compito agli amministratori, ma nel caso di architetture su vasta scala si opta addirittura per server di gestione multipli.

- **Server Database:** Un Database è un deposito per le informazioni registrate dagli agenti, dai sensori e dai server di gestione.

- **Console:** La console è un programma che fornisce un'interfaccia per l'utilizzatore dell'IDPS, generalmente viene installata su qualche computer di tipo Desktop o Laptop. In alcuni casi le console vengono utilizzate soltanto per motivi amministrativi come configurazione dei sensori o agenti o applicare aggiornamenti, mentre in altri casi vengono utilizzate proprio per lo scopo di monitoraggio ed analisi.

1.3 Tipi di IDPS

Ci sono vari tipi di IDPS, ma generalmente si scindono in quattro gruppi basati sul tipo di eventi che controllano e nella maniera in cui sono sviluppati:

- **Network-Based:** monitorano il traffico di rete attraverso particolari segmenti o dispositivi e analizzano le attività del protocollo di rete e di applicazione per identificare attività sospette. In genere viene posizionato al limite della rete in prossimità di firewalls, routers, VPN servers o reti wireless.

- **Wireless:** controllano il traffico wireless analizzandone il protocollo per identificare attività sospette. Non può individuare attività sospette nei protocolli dello strato di applicazione e quelli più alti dello strato di rete (es:TCP,UDP). In genere viene posizionato nel limite di copertura della wireless, o anche in zone dove ci possono essere connessioni non protette.

- **Network Behavior Analysis:** esaminano il traffico di rete per individuare minacce che ne alterano il flusso, come attacchi di tipo Destribuite Denial of Service (DDoS), alcune forme di malwere (Worms, Backdoors) e altre violazioni. I sistemi Network Behavior sono spesso sviluppati dove possono monitorare il flusso della rete interna di un'organizzazione o anche per monitorare il flusso di traffico fra la rete dell'azienda e l'esterno.

- **Host-Based:** monitorano le caratteristiche di un singolo host e gli eventi che occorrono al suo interno per individuarne attività sospette. Esempi di caratteristiche possono essere, il traffico di rete (solo

verso questo host), system logs, processi, applicazioni, accesso e modifica ai files e cambiamenti nelle configurazioni di sistema. Questi IDPS sono spesso sviluppati per host critici come server di accesso pubblico, o server che contengono informazioni delicate.

Alcune forme di IDPS sono più consolidate rispetto ad altre perché sono in uso da molto più tempo, come ad esempio i Network-Based e gli Host-Based che sono in circolazione già da più di dieci anni.
Software di tipo Network Behavior Analysis è una nuova forma, ancora poco utilizzata, nata unendo in parte prodotti per il rilevamento di DDoS attacks, ed in parte prodotti sviluppati per monitorare il flusso del traffico di reti interne.
La tecnologia Wireless invece è proprio un nuovo tipo di IDPS sviluppato in risposta alla popolarita delle wireless local area network (WLAN) e le crescenti minacce verso questo tipo di strutture.

1.4 Architettura

Gli IDPS sono stati creati per identificare ed analizzare svariati tipi di protocolli, tra cui quelli dello strato di rete, di trasporto e di applicazione e la precisione o il metodo con cui questi protocolli vengono visionati dipende dalla tipologia dell'IDPS stesso.
Proprio per questo motivo è essenziale studiare attentamente dove poter inserire il nostro dispositivo di prevenzione**.**
Avendo precedentemente illustrato i componenti e le varie tipologie di IDPS passiamo ora a descriverne l'architettura e l'ubicazione ottimale in una rete. Ovviamente dovremo muoverci in maniera differente in base al tipo e allo scopo del nostro dispositivo quindi faremo un'analisi separata delle diverse architetture.

Network-Based IDPS:
Un network-based IDPS è generalmente composto da sensori, uno o più management servers, una console e se supportato uno o più database servers.
Tutti questi dispositivi sono simili per tutti i tipi di IDPS ad eccezione dei sensori. Un sensore di un IDPS Network-Based osserva ed analizza quello che avviene in uno o più segmenti della rete. Il numero di sensori utilizzati dipende da quanto è grande la rete da analizzare, ma in ogni caso possono essere presenti solo in due formati:

- **Apparecchio fisico:** Un sensore fisico è dotato di hardware e software specializzato. L'hardware spesso è ottimizzato includendo speciali drivers per la cattura dei pacchetti o processori per assistere la fase di analisi. A volte possono essere costruiti sopra sistemi operativi già esistenti dove neanche gli amministratori non possono

avere accesso.

- **Solo Software:** Alcuni produttori vendono sensori senza apparecchi fisici come supporto. Gli amministratori devono quindi installare il software dentro host con determinati requisiti.

Locazione dei Sensori:

La scelta fondamentale nell'ubicazione dei sensori di un Network-Based è costituita dal fatto se il dispositivo sarà utilizzato come IDS o IPS. Nel primo caso dovremo soltanto analizzare i pacchetti che fluiscono nel determinato segmento di rete senza dover agire direttamente su di essi, quindi sarebbe auspicabile inserire i sensori in una zona isolata dal resto della rete dove poter monitorare il traffico in maniera passiva.

Nel secondo caso invece il dispositivo IPS dovrà essere inserito “inline” .

Per quanto riguarda l'ubicazione effettiva dei sensori nella nostra rete, in genere si ricade sempre in due scelte:

- **Inserire l'IPS fra il firewall ed il router:** In generale porre il sistema davanti al firewall ha il vantaggio di osservare tutti gli attacchi diretti alla nostra rete, con l'inconveniente che se il firewall fa anche da NAT non saremo in grado di capire la sorgente dei pacchetti che vengono dall'interno. D'altra parte l'elevata quantità di attacchi rilevati può far abituare a chi li controlla ad un esame poco accurato, rendendo più difficile l'individuazione delle vere minacce.
- **Inserire L'IPS fra il firewall e la rete interna:** Ponendo il sistema dietro al firewall avremo il vantaggio di rilevare solo gli attacchi che passano quest'ultimo generando meno carico di lavoro su chi deve effettuare i controlli. Inoltre è possibile individuare le macchine che inviano traffico sospetto ed accorgersi di attacchi provenienti dall'interno, spesso i più pericolosi. D'altra parte non si riuscirebbe ad avere una vista reale degli attacchi diretti alla rete.

Sia che i sensori siano ubicati fra il firewall e la rete esterna che fra il firewall e la rete interna, come precedentemente accennato ci sono due modi in cui questi dispositivi possono essere schierati:

- **Inline:** Un sensore viene installato inline così che il traffico di rete vi passi attraverso in maniera simile al flusso di traffico che passa attraverso al firewall, infatti alcuni sensori sono un ibrido fra firewall e IDPS. Il motivo principale di inserire un sensore inline è quello di permettergli di bloccare attivamente il traffico. I sensori ibridi spesso vengono esposti al traffico esterno collegandoli direttamente al router, quelli privi di firewall invece vengono inseriti in una zona protetta così da avere meno traffico da processare.

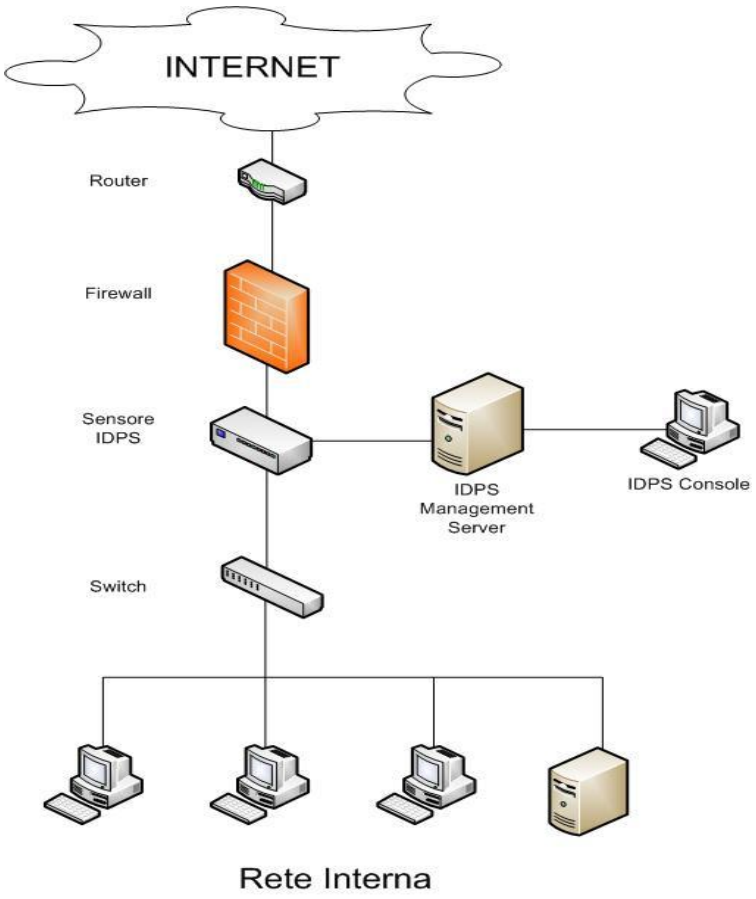


Fig.1 – Network Based IDPS Inline

- **Passivo:** Un sensore viene installato passivo cosi da poter monitorare una copia del traffico di rete, perché nessun traffico passa attraverso il sensore. Questo può essere effettuato in due modi:

    - **Spanning o Mirror port:** Molti switch hanno una spanning port, che sarebbe una porta che può vedere tutto il traffico che passa attraverso lo switch. Questo metodo è semplice e privo di costi, ma può avere delle problematiche. Se lo switch è configurato malamente la porta potrebbe non osservare tutto il traffico, inoltre in caso di grossa mole di traffico lo la spanning port potrebbe perdere dei pacchetti, infine in alcuni casi l'abilitazione di questa modalità degrada notevolmente le prestazioni.

    - **Network Tap:** Un network tap è una connessione diretta fra il sensore e il link fisico della rete. Il tap fornisce al sensore una copia di tutto il traffico di rete nel link. Il problema di questo mezzo è che per essere installato o in caso di malfunzionamenti deve mandare la rete “down”.

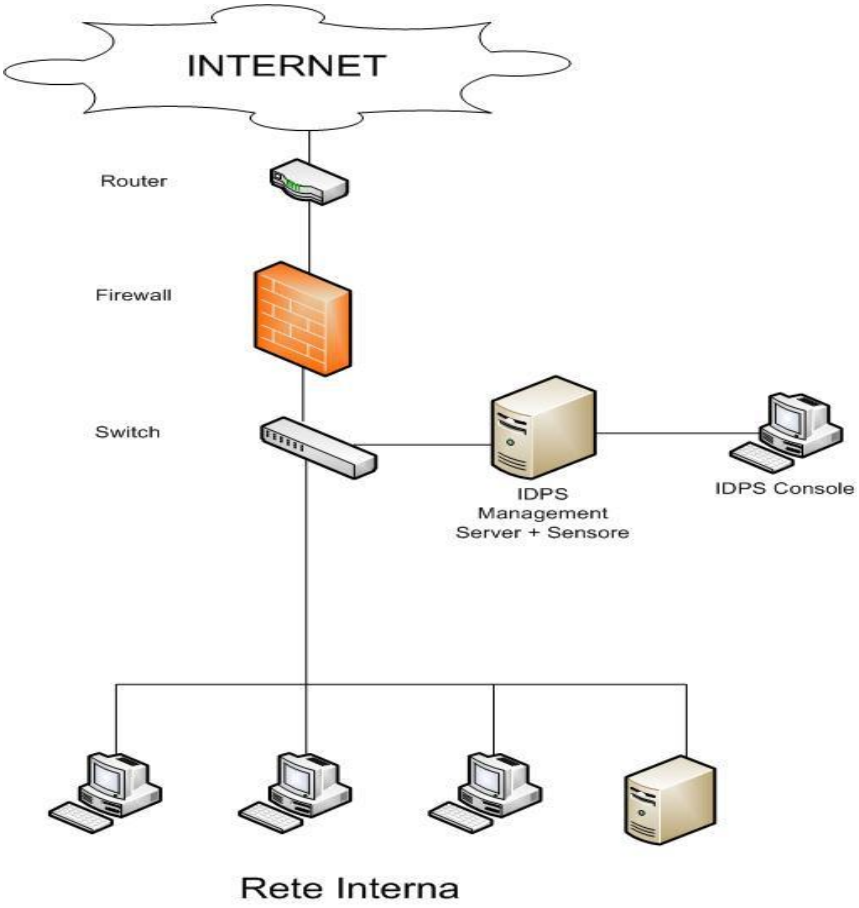


Fig.2 – Network Based IDPS Passivo

Network Behavior Analysis IDPS:

NBA hanno tipicamente soltanto sensori e consoles, alcuni prodotti forniscono anche un management server a volte chiamato analyzer. Nella maggior parte dei casi i sensori NBA sono apparecchi fisici. Alcuni hanno un funzionamento simile a quello dei Network-Based, altri invece non monitorizzano direttamente la rete, ma si basano sulle informazioni del flusso di traffico fornitegli dai routers o da altri dispositivi. Il flusso si riferisce a particolari sessioni di comunicazione fra hosts; dati particolarmente rilevanti possono essere:

- Indirizzi IP sorgente e destinazione
- Porte sorgente e destinazione TCP o UDP o codici ICMP
- Numero di bytes e pacchetti trasmessi nella sessione

- L'ora dell'inizio e della fine della sessione

Locazione dei Sensori:

La maggior parte degli NBA possono essere collegati soltanto in maniera passiva alla rete usando gli stessi metodi del Network-Based, quindi è opportuno inserire i sensori in locazioni chiave come nei punti di divisione di più sottoreti

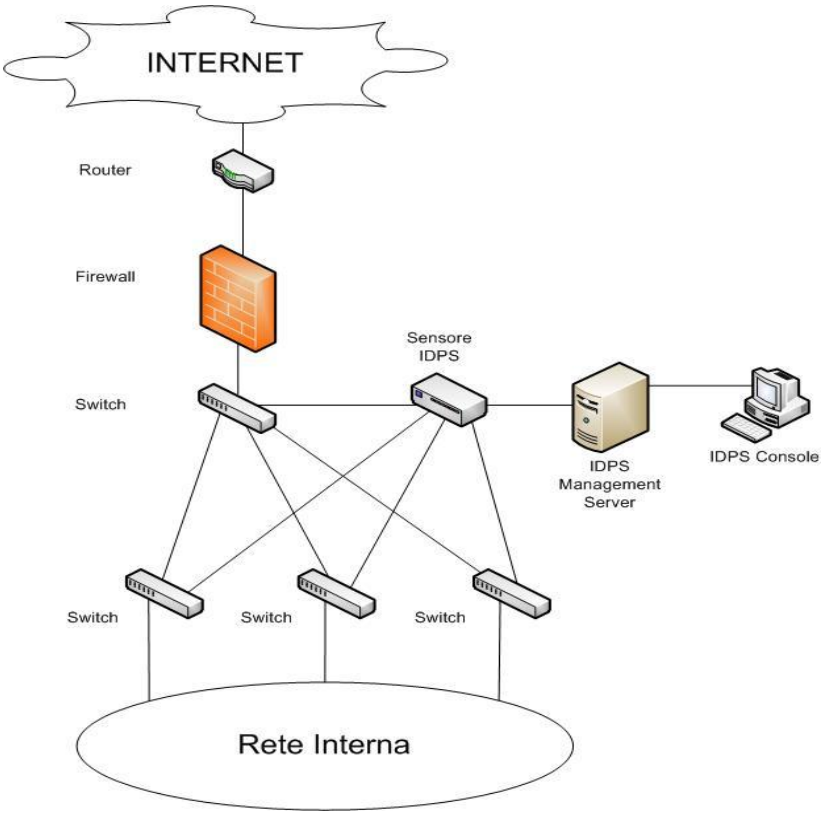


Fig.3 – Network Behavior Analysis IDPS

Host-Based IDPS:

Gli host-based IDPS hanno un software di rilevamento conosciuto come agents installato negli host di interesse. Ogni agents osserva le attività nel singolo host e se le funzionalità di prevenzione sono attivate, possono attivare azioni reattive.Gli agents trasmettono i dati raccolti al management server che può utilizzare un database server per immagazzinarli. La console è utilizzata per la gestione ed il monitoraggio.

Ogni agente è tipicamente creato per proteggere uno dei seguenti

dispositivi:

- **Un Server:** Oltre al monitoraggio del sistema operativo l'agent può analizzare anche alcune applicazioni comuni.
- **Un Client host:** Anche in questo caso l'agent monitora il sistema operativo e alcune delle più comuni applicazioni (e-mail clients, Web browsers).
- **Un Servizio:** Alcuni agents sono creati per monitorare delle applicazioni che forniscono servizi come Web server o Database server. Questi vengono anche chiamati Appliance-Based agents.

Locazione dei sensori:

L'architettura di rete per gli Host Based IDPS è la più semplice in quanto gli agents sono installati su host già esistenti nell'organizzazione di rete e i vari componenti comunicano attraverso quest'ultima invece di essere installati in reti separate appositamente per la gestione. Gli appliance-based agents vengono posizionati inline avanti all'host che stanno proteggendo.

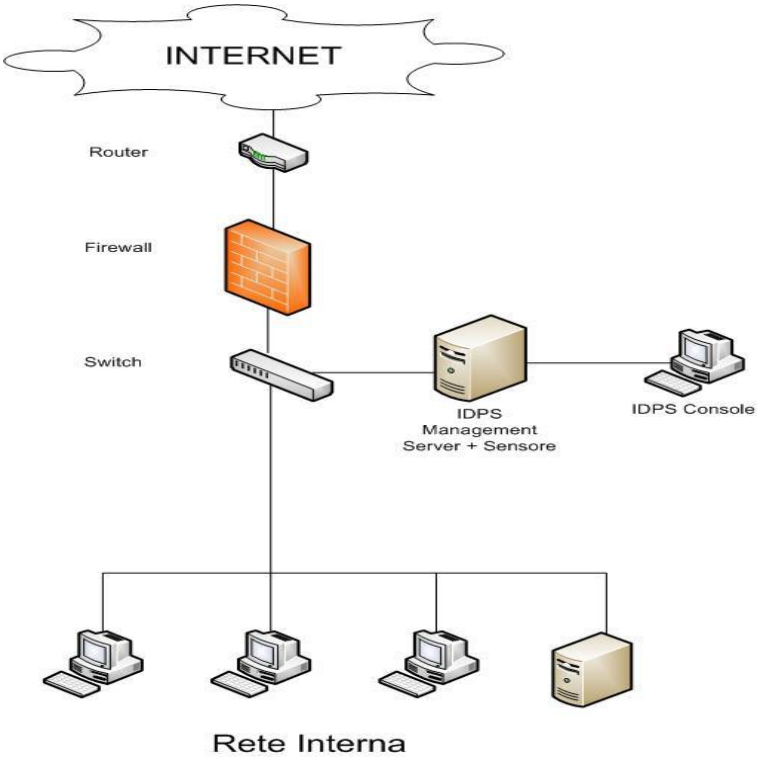


Fig.4 – Host Based IDPS

1.5 Funzioni chiave di un IDPS

Ci sono vari tipi di IDPS differenziati principalmente dai tipi di eventi che sono in grado di riconoscere e dalle metodologie che usano per identificare le anomalie.
In aggiunta all'analisi e al monitoraggio degli eventi per identificare quelli indesiderati, tipicamente tutti i tipi di IDPS eseguono le seguenti funzioni:

- **Registrano informazioni relative agli eventi osservati:** Le informazioni sono generalmente salvate in locale, ma possono anche essere spedite su sistemi separati.

- **Notificare gli amministratori sull'osservazione di eventi importanti:** Queste notifiche, in genere chiamate “alert”, avvengono tramite svariati metodi: e-mail, pagine, messaggi nell'user interface dell'IDPS se presente, Simple Network Management Protocol (SNMP) traps, messaggi di tipo syslog, e anche script o programmi definiti dall'utente. La notifica in genere presenta solo informazioni basilari sull'evento , l'amministratore quindi deve accedere all'IDPS per saperne di più.

- **Produrre rapporti:** I rapporti o in genere detti “report”, riassumono gli eventi monitorati, o producono dettagli di particolari situazioni d'interesse.

Alcuni IDPS sono anche in grado di cambiare il proprio profilo di sicurezza quando sono individuate nuove minacce. Per esempio un IDPS potrebbe collezionare informazioni più dettagliate durante una sessione, dopo aver individuata un'attività malevola nella stessa.

Le tecnologie IPS si differenziano in questi ambiti dagli IDS da una caratteristica: i primi possono rispondere ad una minaccia cercando di fermarla.
Anche in questo caso ci sono molteplici tecniche di prevenzione, ma in generale possiamo dividerle nei seguenti gruppi:

- **L'IPS ferma l'attacco stesso:** Esempi di come può farlo sono i seguenti:
  - Terminare la connessione o la sessione dell'utente che sta effettuando l'attacco.
  - Bloccare l'accesso all'obiettivo dall'account, indirizzo IP o altri attributi dell'intruso.
  - Bloccare tutti gli accessi all'host, servizio, applicazione o altre risorse bersaglio per una durata prestabilita in genere misurata in minuti ore o raramente giorni.

- **L'IPS cambia le condizioni di sicurezza:** L'IPS può cambiare la configurazione di altri dispositivi di sicurezza per bloccare l'attacco.
  Un esempio potrebbe essere quello di riconfigurare un dispositivo della rete
  (es router, firewall, switch ecc..) per bloccare l'accesso dell'attacco.

- **L'IPS cambia il contenuto dell'attacco:** Alcuni IPS possono sostituire o rimuovere parti maligne di un attacco per renderle innocue. Un esempio semplice può essere che l'IPS rimuova un allegato infetto da un'e-mail, e permetta l'e-mail pulita di raggiungere il destinatario, funzione che è normalmente demandata ad un sistema Antivirus.

Nonostante tutte le caratteristiche descritte, gli IDPS non riescono comunque a fare un rilevamento completamente accurato.

Infatti quando una attività benigna viene erroneamente identificata come malevola, ci troveremo in una situazione di “false positive”.

Invece quando un IDPS fallisce e non identifica una minaccia, avremo una situazione di “false negative”.

Sfortunatamente non è possibile eliminare del tutto queste due situazioni e nella maggior parte dei casi ridurne una vuol dire far crescere la probabilità dell'altra.

Molte organizzazioni scelgono comunque di diminuire i false negative al costo di far crescere i false positive, che vuol dire aumentare il rilevamento di attacchi al costo di aumentare risorse di analisi per identificare i veri false positive.

Questo fenomeno di manipolazione delle configurazioni dell'IDPS per aumentare la sua accuratezza prende il nome di “tuning”.

1.6 Metodologie comuni di rilevazione

Gli IDPS usano diverse metodologie di rilevamento e tra le più usate troviamo:

- Signature-Based
- Anomaly-Based
- Stateful Protocol Analysis

Esse possono essere utilizzate in maniera separata, o integrate fra loro per fornire una rilevazione più ampia ed accurata.

Signature-Based Detection:

Una signature è un pattern che corrisponde ad una minaccia conosciuta.
La Signature-Based Detection si basa sulla comparazione di queste signature con gli eventi osservati per identificare possibili minacce. Esempi di signature possono essere:

- Una connessione telnet tenta di entrare con username “root”, che è una violazione di sicurezza di un'organizzazione.
- Un'e-mail con un oggetto e un allegato che combaciano con forme di malware conosciuti.
- Un log in entrata di un sistema operativo con status code di 645, che significa che l'auditing dell'host è stato disabilitato.

Signature Based Detection è veramente efficace nel rilevare le minacce conosciute, ma ampiamente inefficace quando si tratta di rilevare in anticipo le minacce ancora sconosciute o malware che hanno subito anche solo una piccola variante.
Ad ogni modo il Signature-Based è il modo più semplice di rilevazione perché si limita a comparare l'unità corrente, sia essa un pacchetto o un log, con una lista di signature, tramite la comparazione con regole atte a

descrivere le attività malevole conosciute.

Tra le limitazioni di questo metodo inoltre troviamo la ristretta cognizione di molti protocolli di rete e di applicazione, che lo rende incapace di capire lo stato di comunicazioni troppo complesse e l'impossibilità di ricordare le richieste precedenti, mentre si sta elaborando quella corrente che quindi limita il rilevamento di attacchi che comprendono eventi multipli se nessuno di questi contiene una chiara indicazione di minaccia. Le firme in genere sono fornite dai produttori via web, ma sono sempre più diffusi IDPS che sono compatibili con firme di altri software, siano essi altri IDPS, Antivirus o altro.

Anomaly-Based Detection:

Anomaly-Based Detection è un metodo che compara definizioni che descrivono quali attività sono normali rispetto agli eventi osservati, per identificare qualche anomalia o deviazione.

Un IDPS che usa l'Anomaly-Based Detection possiede dei profili che rappresentano il normale comportamento di vari soggetti quali utenti, hosts, connessioni di rete o applicazioni. Questi profili sono sviluppati per monitorare le caratteristiche di un'attività tipica durante un certo periodo di tempo.

Per esempio, un profilo per una rete può visualizzare quelle attività Web che occupano in media il 13% di banda o superiore durante un normale giorno lavorativo.

L'IDPS quindi usa metodi statici per comparare le caratteristiche dell'attività corrente con una soglia relativa al profilo associato, come nel caso del Web che occupa più banda di quella aspettata.

I profili possono essere sviluppati in base a svariati attributi per ogni comportamento, come il numero di e-mail spedite da un utente, il numero di login falliti per entrare su un host o la percentuale di processore usato in un

certo periodo di tempo.
I profili possono essere sia dinamici che statici, un profilo statico non cambia finché l'IDPS non ne crea uno nuovo e lo sostituisce, mentre un profilo dinamico cambia man mano che eventi nuovi vengono osservati.
Dato che sistemi e reti cambiano spesso nel tempo, anche i normali comportamenti cambiano con esse, e quindi un profilo statico deve essere periodicamente rigenerato.
I profili dinamici non hanno questo problema, ma sono più suscettibili ai tentativi di evasione da parte degli attacchi.
Il beneficio maggiore dell'Anomaly-Based Detection è che può essere veramente efficiente nell'identificare anticipatamente minacce sconosciute.
Ci sono anche alcuni problemi ad usare questo metodo come quello di aggiungere inavvertitamente comportamenti malevoli nel profilo e la difficoltà di creare un profilo accurato perché il comportamento del computer spesso è molto complesso.
Oltre a questo c'è da dire che metodi Anomaly-Based producono molti falsi positivi per via delle normali azioni non dannose che però deviano significativamente da quelle descritte sul profilo, specialmente in ambienti dinamici.
Un ultimo importante problema risiede nel fatto che spesso è difficile per l'analista determinare perché un particolare alert è stato generato e capire se si tratta di false positive, per via della complessità degli eventi e dall'elevato numero di essi che potrebbe aver sollevato la notifica.

Stateful Protocol Analysis:

Il metodo Stateful Protocol Analysis confronta profili predeterminati, costruiti sulla base del normale comportamento di un protocollo per ogni suo stato, rispetto all'evento osservato per rilevare deviazioni.
Diversamente dall'Anomaly-Based, che usa profili host o di rete, Stateful Protocol Analysis conta su profili universali sviluppati dal venditore, che

specificano come i particolari protocolli vanno o non vanno usati.
La parola “Stateful” ci fa intuire che l'IDPS è capace di capire e rintracciare i protocolli dello strato di rete, di trasporto e di applicazione; per esempio se un utente inizia una sessione di File Transfer Protocol (FTP), essa inizialmente è in stato non autenticato. Un utente non autenticato dovrebbe essere capace di utilizzare solo pochi comandi come vedere le informazioni di “help” o fornire username e password.
Una parte importante per capire uno stato è riuscire ad accoppiare le richieste con le relative risposte, quindi nel caso dell'FTP se arriva una richiesta di autenticazione, l'IDPS può determinare se è andata a buon fine cercando nello status code della relativa risposta. A questo punto l'utente è autenticato e si può prevedere che utilizzi qualsiasi comando fra la dozzina di quelli disponibili, azione che sarebbe stata considerata sospetta se quest'ultimo fosse in stato non autenticato.
Lo Stateful Protocol Analysis può anche identificare una sequenza di comandi inaspettata, come digitare un comando ripetutamente, o digitare un comando senza aver avviato prima il comando a cui è correlato.
Un'altra caratteristica di questo metodo è che per i protocolli che effettuano autenticazione, è possibile tenere traccia dell'elemento autenticante usata per ogni sessione, e registrarlo qualora effettui azioni sospette.
La parte di “Protocol Analysis” effettuata invece richiede dei ragionamenti per controllare i comandi come la lunghezza minima e massima dell'argomento.
Il principale problema dello Stateful Protocol Analysis è il grande utilizzo di risorse per via della complessità dell'analisi e il grosso dispendio dovuto alla ricerca di ogni stato nel caso di multisessione.
Un altro problema serio è che questo metodo non può rilevare attacchi che non violano le caratteristiche di un comportamento generale accettabile per un protocollo, come usare molte azioni benigne ad alta frequenza per generare un Denial of Service.

1.7 Metodi di sicurezza

Molti IDPS possono fornire una grande varietà di metodi di sicurezza, i più comuni sono: information gathering, logging, detection e prevenction.

Information Gathering:

Alcuni IDPS offrono capacità di raccolta informazioni, come reperire dati su di un host o una rete sulla quale si sta osservando un'attività. Esempi includono identificare il sistema operativo e le applicazioni aperte dall'host ed identificare le caratteristiche generali della rete.

Capacità di logging:

Gli IDPS generalmente forniscono un vasto registro di dati, comunemente detto "log", correlato agli eventi individuati. Questi dati possono essere usati per verificare la validità degli alert o investigare sugli inconvenienti che avvengono in rete.

I campi dei dati comunemente usati includono la data e l'ora, il tipo di evento, il livello di importanza, e le azioni di prevenzione utilizzate, se ce ne sono.

Alcuni specifici tipi di IDPS inoltre registrano altri campi, come i Network-Based che eseguono la cattura dei packet o gli Host-Based che registrano gli User ID.

Generalmente gli IDPS permettono di immagazzinare i registri localmente e spedire copie dei log a server centralizzati, per permettere l'integrità e la disponibilità dei dati anche in situazioni critiche.

Per far fronte a problemi di sincronia si è stabilito che gli IDPS debbano sincronizzare il proprio orologio usando il Network Time Protocol (NTP) o attraverso frequenti controlli manuali per far si che l'ora sia sempre accurata.

Capacità di rilevamento:

Gli IDPS generalmente offrono diverse ed ampie capacità di rilevamento, molti di essi addirittura utilizzano una combinazione fra più tecniche per ottenere maggiore flessibilità ed accuratezza.
Le organizzazioni quindi dovrebbero considerare attentamente la varietà di aggiustamenti e caratterizzazioni che possono offrire un IDPS.
Alcuni esempi possono essere:

- **Soglie:** Una soglia è un valore che può essere impostato come limite tra un comportamento normale ed uno anomalo. In genere specificano un livello massimo accettabile come un numero connessioni fallite in sessanta secondi o il numero massimo caratteri per il nome di un file. Le soglie vengono usate specialmente dagli Anomaly-Based Detection e Stateful Protocol Analysis.

- **Blacklists e Whitelists:** Una Blacklist è una lista di entità, come host, porte TCP o UDP, applicazioni, usernames, url, nomi di files o estenzioni di files etichettate a priori come malevole. Sono utilizzate generalmente per permettere all'IDPS di riconoscere e bloccare immediatamente attività altamente dannose, ed anche per assegnare una maggiore priorità agli alert che combaciano con quelli descritti nella Blacklist. Al contrario una Whitelist è una lista di entità conosciute come benevole e vengono spesso usate per ridurre i falsi positivi. Blacklist e Whitelist vengono spesso usate dai Signature-Based e Stateful Protocol Analysis.

- **Impostazioni degli Alert:** Molti IDPS permettono all'amministratore di personalizzare ogni tipo di alert. Ad esempio:

- Abilitarlo o disabilitarlo
- Impostare il livello di priorità
- Specificare quale informazione dovrebbe essere registrata e quale metodo di notifica dovrebbe essere utilizzato.
- Specificare quale mezzo di prevenzione dovrebbe essere utilizzato.

Alcuni prodotti possono anche sopprimere gli alert se ne vengono generati troppi in un piccolo intervallo di tempo ed ignorare il traffico proveniente da quell'attacco, per evitare di esserne sovraccaricato.

Capacità di prevenzione:

Gli IPS offrono svariati metodi di prevenzione che variano da software a software. Essi in genere permettono agli amministratori di specificare il mezzo di prevenzione per ogni tipo di alert ed alcuni permettono di abilitare la modalità simulazione che invece di far agire l'IPS, notifica quando l'azione preventiva sarebbe stata svolta. Questo aiuta gli amministratori a scegliere la giusta configurazione del software, così da ridurre inavvertitamente il rischio di bloccare attività benevole.
Ovviamente i mezzi utilizzati per fermare un attacco per un IPS che lavora su una rete e un IPS che lavora su un host sono profondamente differenti.

Network Based: I Network-based IPS offrono parecchi metodi di prevenzione in base a come i sensori vengono installati:

- **Solo Passivo**
  - **Chiusura della connessione TCP:** Un sensore passivo può tentare di chiudere una sessione TCP spedendo pacchetti TCP reset; a volte questo metodo viene chiamato *session sniping*.

Il sensore in questo caso farà credere ad ogni terminale che l'altro sta tentando di chiudere la connessione. Lo scopo viene raggiunto se uno dei due terminali chiude la connessione prima che l'attacco abbia successo, ma sfortunatamente a volte il tempo di analisi e identificazione dell'evento è troppo lungo per poter spedire i pacchetti prontamente. Questa tecnica è ormai poco utilizzata perché non permette di prevenire attacchi portati da altri tipi di pacchetti come UDP o ICMP.

- **Solo Inline**
  - **Effettuare tecniche di Firewalling:** Molti IPS inline offrono capacità di Firewall che effettuano operazioni di *drop* o *reject* sulle attività sospette.
  - **Manipolare l'utilizzo di Banda:** Se un protocollo viene utilizzato in appropriatamente, come nel caso degli attacchi DoS o distribuzione di malware, gli IDPS possono limitare la percentuale di banda che il dato protocollo può usare, cosi da evitare un impatto negativo sulle altre risorse.
  - **Alterare contenuto Malevolo:** Come menzionato in precedenza, alcuni IPS inline possono curare parte di un pacchetto sostituendo la zona malevola con un contenuto innocuo e mandarlo a destinazione.

- **Sia Passivo che Inline**
  - **Riconfigurare altri dispositivi di Sicurezza:** Molti dispositivi IPS possono ordinare a dispositivi di sicurezza come firewall, routers o switch di riconfigurarsi per bloccare un'attività o instradarla da qualche altra parte. Questa tecnica

è utile solo per il traffico di rete che può essere differenziato tramite le caratteristiche dell'header del pacchetto tipicamente riconosciute dai dispositivi di sicurezza, come indirizzi IP e numeri di porta.

- **Eseguire programmi o script:** Alcuni IPS possono eseguire uno specifico script o programma dettato dall'amministratore quando si verificano particolari situazioni. In questo modo il dispositivo di prevenzione si potrà comportare esattamente come l'amministratore desidera, infatti si usano programmi o script quando l'IPS non fornisce l'azione di prevenzione che si vuole.

Host-Based: Negli host-based le tecniche di prevenzione delle intrusioni variano in base allo scopo ed al tipo di tecnica utilizzata per la rilevazione, di seguito vedremo i mezzi di prevenzione in base al metodo utilizzato:

- **Analisi del Codice:** L'IPS può prevenire l'esecuzione del codice inclusi malware e applicazioni non autorizzate. Alcuni possono anche fermare applicazioni di rete dall'invocare shells, mezzo che potrebbe essere utilizzato per effettuare alcuni tipi di attacchi. Se ben progettata la tecnica di analisi del codice può essere particolarmente efficace in particolar modo per fermare preventivamente attacchi sconosciuti.

- **Analisi del Traffico di Rete:** Questo metodo può fermare l'elaborazione del traffico di rete in entrata o di quello in uscita da un determinato host. Può essere usato per fermare attacchi diretti agli strati di rete, di trasporto e di applicazione oppure l'utilizzo non autorizzato di applicazioni e protocolli.

- **Filtraggio del Traffico di Rete:** In questo caso l'IPS si comporta come un firewall e può fermare accessi non autorizzati e violazioni di policy. Questo metodo è efficace solo contro attività identificabili dall'indirizzo IP e porte TCP, UDP o tipologie di ICMP.

- **Monitoraggio Filesystem:** L'IPS può prevenire l'accesso, la modifica, la sostituzione o l'eliminazione dei files che potrebbe fermare l'installazione di malware, inclusi Trojan e rootkit, o altri attacchi che coinvolgono un inopportuno accesso ai files.

Altri metodi di rilevamento come analisi dei log, controllo della configurazione di rete e controllo dell'integrità dei files, generalmente non prevedono azioni di prevenzione perché questi eventi vengono identificati soltanto dopo essere accaduti.

1.8 Gestione e Aggiornamenti

La maggior parte degli IDPS offrono gli stessi strumenti di gestione e aggiornamento, di seguito esamineremo ed approfondiremo quelli più comuni.

Strumenti di gestione:

Quasi tutti gli IDPS sono programmati per essere utilizzati e gestiti tramite un'interfaccia grafica o GUI (Graphical User Interface), conosciuta come console.
La console generalmente permette agli amministratori di configurare ed aggiornare i sensori o i management servers, così come permette di controllare il loro stato.
Gli amministratori possono anche gestire gli account utente, personalizzare reports o attivare svariate altre funzioni.
Gli utenti hanno accesso a funzioni più limitate, ma possono comunque vedere ed analizzare i dati o i reports generati.
Molti IDPS permettono di creare diversi account per ogni tipologia di utente, concedendo ad ognuno solo i privilegi adatti al ruolo del proprietario. Questo viene realizzato visualizzando diversi menu ed opzioni in base al ruolo dell'account autenticato. Alcuni prodotti addirittura possono regolare l'accesso ai componenti, come ad esempio su quali sensori o agents determinati utenti possono effettuare operazioni, cosi da poter dividere grandi aree da controllare, in unità logiche ognuna descritta da uno scopo preciso.

Un altro strumento di controllo presente in tutti gli IDPS è l'interfaccia a linea di comando o CLI (Command-Line Interface). Diversamente dalla GUI, che in genere viene usata da remoto, le CLI sono usate per la gestione

in locale dei componenti. A volte le interfacce a linea di comando possono essere raggiunte anche in remoto tramite una connessione criptata stabilita tramite Secure Shell (SSH) o altri metodi.
Le consoles sono più semplici da utilizzare delle CLI e spesso hanno anche più funzioni da poter utilizzare.

Operazioni di Manutenzione:

Un amministratore dovrebbe mantenere la struttura IDPS eseguendo alcune operazioni base:

- Monitorando i componenti stessi per verificarne l'operatività
- Verificando periodicamente che l'IDPS funzioni propriamente (es: gestire i giusti eventi, sollevare alerts quando ci sono movimenti sospetti ecc..)
- Effettuare regolari accertamenti di vulnerabilità
- Tenersi informato dai rivenditori dei problemi relativi al prodotto
- Tenersi informati sugli aggiornamenti cercando di testarli prima di applicarli al sistema.

Acquisire ed Applicare gli Aggiornamenti

Esistono due tipi di aggiornamenti: software update e signature update.
Il primo corregge bugs nel software o aggiunge nuove funzioni, mentre il secondo aggiunge nuove minacce rintracciabili o migliora la percezione di quelle già conosciute (es: riduzione dei falsi positivi).
Per alcuni IDPS il signature update causa alterazioni o sostituzioni del codice del programma, quindi sono una sorta di software update, in altri casi le signature sono contenute in file separati dal codice, cosi l'update è solo l'aggiornamento di questi dati.
Il software update può includere alcuni o tutti i componenti dell'IDPS ,

come sensori, agents, management servers e consoles. Nel caso dei sensori e management server nella maggior parte dei casi l'aggiornamento avviene sostituendo il CD o il software esistente e riavviando l'applicazione, infatti molti IDPS vengono avviati direttamente da CD cosi che non sia necessaria nessuna installazione.
Altri componenti, come gli agents, richiedono che l'aggiornamento venga fatto o manualmente dall'amministratore in ogni host, o automaticamente generalmente tramite un software di gestione dell'IDPS.
Per reperire il software e il signature update la via più comune è quella di scaricarli direttamente dal sito Web del venditore, ma spesso anche nell'interfaccia del software si possono trovare funzioni per scaricare ed applicare gli aggiornamenti.
Una volta acquisiti gli amministratori dovrebbero controllarne l'integrità prima di applicarli, perché i files potrebbero essere stati inavvertitamente o intenzionalmente alterati o sostituiti.
I metodi di verifica dipendono dal formato dell'aggiornamento:

- **Files scaricati da un sito Web o un sito FTP:** L'amministratore dovrebbe comparare il checksum fornito dal venditore con quello del file ricevuto.

- **Aggiornamento scaricato automaticamente tramite l'interfaccia IDPS:** In genere l'interfaccia effettua un controllo di integrità del o dei files.

- **Supporto Removibile (Cd, DvD, ecc...):** Se il venditore non fornisce un servizio di verifica, sarebbe opportuno contattare il venditore per avere informazioni a riguardo. L'amministratore potrebbe prendere anche in considerazione l'idea di effettuare una scansione sul dispositivo per verificare la presenza di maleware.

Tipicamente gli IDPS sono progettati così che software e signature update non interferiscano sulle configurazioni presenti, ma è bene che gli amministratori effettuino un back up di queste ultime periodicamente cosi da non perderle inavvertitamente.

Gli amministratori dovrebbero testare il software e i signature updates prima di applicarli, ad eccezione di casi d'emergenza (es: una signature può identificare una nuova minaccia che sta danneggiando il sistema); a questo scopo spesso viene consigliato di avere un sensore o agent usato solamente per i test.

1.9 Firewall e IDPS

I Firewalls filtrano il traffico basato su caratteristiche TCP/IP come gli indirizzi IP, numeri di porta o protocolli utilizzati a livello di trasporto oppure possono bloccare connessioni effettuate da un'attività non autorizzata come port scanning o malware.
Essendo due elementi indispensabili per la sicurezza di una rete è indispensabile che Firewall e IDPS operino insieme per perseguire degli scopi comuni come i seguenti:

- Alcuni Firewalls spesso effettuano il network address translation (NAT), che è il processo di mappatura degli indirizzi da una rete ad un'altra. In particolar modo il NAT è utilizzato per mappare indirizzi privati di una rete interna con un indirizzo pubblico collegato alla rete esterna. Spesso gli indirizzi e le mappature NAT sono registrati dal firewall e queste informazioni possono essere utilizzate dall'IDPS.

- Se un IDPS non può fermare una minaccia proveniente dalla rete come network service worm o denial of service, può invece riconfigurare il Firewall per poterli bloccare.

- L'IDPS può analizzare direttamente i log del firewall per poter avere una migliore visione di quello che accade nella rete esterna o prendere informazioni sulle minacce incombenti.

- I dati forniti dal Firewall possono essere presi come risorse dati per

un IDPS di tipo Network Behavior Analysis.

Nel caso degli IDS la configurazione è semplice, difatti essi possono analizzare il traffico di rete indipendentemente dalla locazione del Firewall con implicazioni descritte in precedenza. Per quanto riguarda l'analisi dei log, alcuni IDS forniscono funzioni proprie, mentre altri devono avvalersi di Addon esterni tipo Snorter (http://shweps.free.fr/wiki/wakka.php?wiki=SnorTer).

In ognuno dei due casi sarà comunque necessario configurare il dispositivo facendo le opportune considerazioni in base al tipo di Firewall da utilizzare.

Per gli IPS la questione è un po' più complessa, infatti essi devono prelevare i pacchetti provenienti dal Firewall per poterli analizzare.

La maggior parte degli IDPS fornisce un'opzione per poter usare questa funzionalità ed ognuno di essi si avvale di librerie già ampiamente diffuse nell'ambito della cattura dei pacchetti, che sia "libipq" utilizzato da Snort (http://www.snort.org) o "libpicap" utilizzato da Suricata (https://awstats.openinfosecfoundation.org).

Se le librerie fornite dagli IDPS non ci sono utili, sul web si possono trovare dei tools appositi per l'interfacciamento di questi ultimi con i Firewalls.

Una tecnica comunemente utilizzata è quella di far comunicare i due dispositivi tramite connessione SSH, più precisamente il tool in questione permette di prelevare gli host malevoli inseriti nel database dell'IDPS ed inserirli nella tabella dei blocchi che caratterizza ogni Firewall.

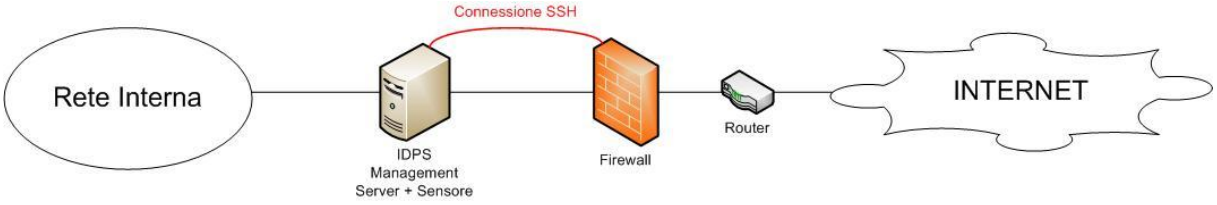


Fig.5 – Interfacciamento IDPS-Firewall

Capitolo 2 - Analisi Comparativa

Nel presente capitolo ci si occuperà in primis della presentazione delle tecnologie campionate attraverso lo schema del data sheet così da fornire subito una panoramica del lavoro svolto.
In secondo luogo si avrà premura di analizzare le caratteristiche degli IDPS che in precedenza erano stati succintamente descritti.
Il capitolo si concluderà poi con delle tabelle riassuntive finalizzate a presentare al lettore i risultati dell'analisi.

2.1 Data Sheets

Al fine di dare al lettore una panoramica delle tecnologie IDPS testate nelle pagine seguenti, attraverso i "data sheet", verranno fornite le prime indicazioni sui prodotti che poi, ovviamente, verranno trattati successivamente nel dettaglio.
Ogni Data Sheet è strutturato in tre parti:

1. Una breve introduzione del prodotto
2. Descrizione delle caratteristiche che lo distinguono
3. Se presenti, i requisiti hardware necessari

2.1.1 Snort

Snort è un Network Intrusion Detection e Prevenction System sviluppato da Sourcefire (http://sourcefire.com) che combina i benefici dei metodi signature, protocol e anomaly-based inspection per analizzare e proteggere la rete. Snort è senza dubbio la tecnologia IDS/IPS più sviluppata e utilizzata tanto da diventare standard de facto per gli IPS.

CARATTERISTICHE:

Applicazioni: Snort può essere utilizzato in quattro diverse maniere:

- Packet Sniffer
- Packet Logger
- Intrusion Detection System
- Intrusion Prevention System

Sicurezza: Snort è capace di effettuare analisi del traffico e packet logging in tempo reale sulla rete. Effettua protocol analysis, content searching/matching e rileva una grande quantità di attacchi e sonde, come buffer overflows, port scans, attacchi CGI e tentativi di violare il sistema.

Logging: Snort offre diverse maniere per immagazzinare dati che comprendono il formato unified2, syslog, pcap o la possibilità di utilizzare un database.

Addons: Sono sempre più numerosi gli Addons e i Plugins disponibili per Snort aggiungendo nuove funzionalità o migliori strumenti di gestione al prodotto.

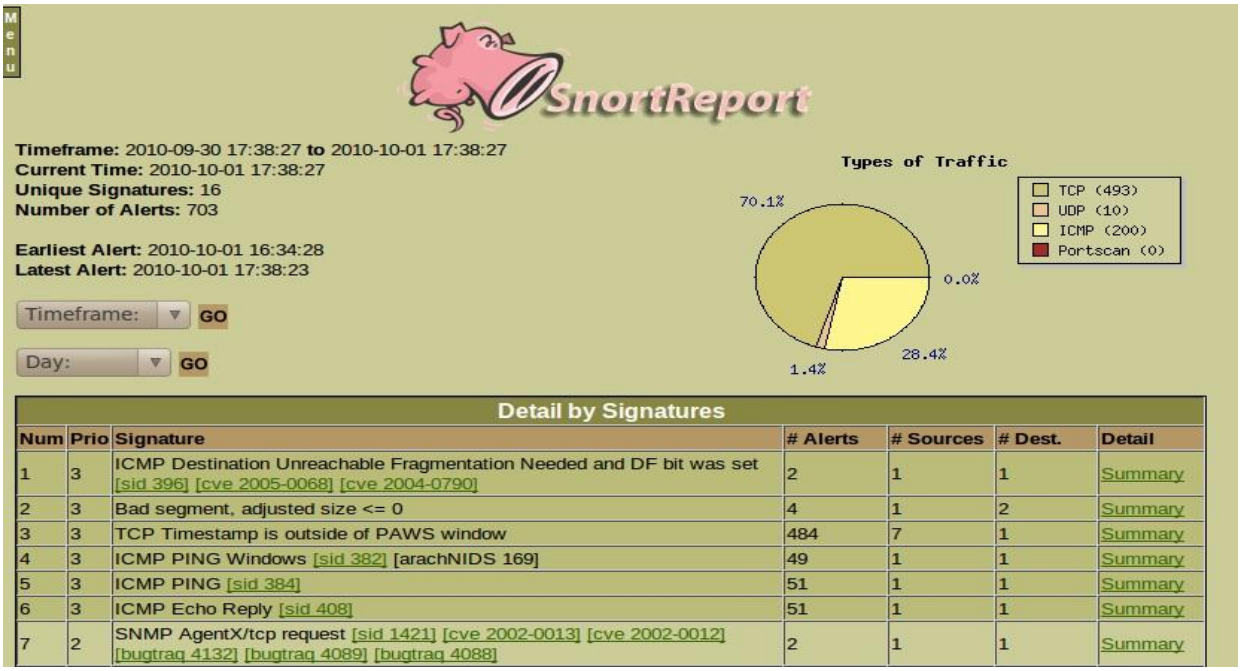
Supporto del Sourcefire Vulnerability Research Team™ (VRT): il Sourcefire Vulnerability Research Team™ (VRT) è un gruppo di esperti della sicurezza nelle reti che si occupa di scoprire i nuovi mezzi di Hacking e di minacce alla vulnerabilità.

Regole: Ci sono due tipi di regole reperibili per Snort:

- **Community Rules:** che si riferiscono a tutte quelle regole presentate dalla comunità open source. Queste regole sono reperibili gratuitamente da tutti gli utenti Snort e sono governate dal GPL.
- **Sourcefire VRT Certified Rules:** si riferiscono alle regole sviluppate, testate e approvate dal Sourcefire VRT Vulnerability Research Team (VRT) tramite un'iscrizione a pagamento.

Le community rules sono gratuitamente distribuite dal sito di Snort. Mentre le regole Sourcefire VRT Certified si possono ricevere nei seguenti modi:

- Gli utenti iscritti ricevono le regole in tempo reale rispetto a quando sono rilasciate da Sourcefire, 30 giorni prima degli utenti registrati.
- Gli utenti registrati possono reperire le regole quando sono pubblicate.
- Gli utenti non registrati avranno soltanto le regole statiche che escono con ogni release di Snort.



Num	Prio	Signature	# Alerts	# Sources	# Dest.	Detail
1	3	ICMP Destination Unreachable Fragmentation Needed and DF bit was set [sid 396] [cve 2005-0068] [cve 2004-0790]	2	1	1	Summary
2	3	Bad segment, adjusted size <= 0	4	1	2	Summary
3	3	TCP Timestamp is outside of PAWS window	484	7	1	Summary
4	3	ICMP PING Windows [sid 382] [arachNIDS 169]	49	1	1	Summary
5	3	ICMP PING [sid 384]	51	1	1	Summary
6	3	ICMP Echo Reply [sid 408]	51	1	1	Summary
7	2	SNMP AgentX/tcp request [sid 1421] [cve 2002-0013] [cve 2002-0012] [bugtraq 4132] [bugtraq 4089] [bugtraq 4088]	2	1	1	Summary

2.1.2 EasyIDS

EasyIDS (http://www.skynet-solutions.net/easyids) è un Sistema Operativo creato per installare un Intrusion Detection System basato su Snort in modo facile e con una minima conoscenza di Linux.
Oltre a Snort, EasyIDS fornisce molti dei più famosi Addons e funzioni aggiuntive già configurati e pronti all'uso.

CARATTERISTICHE:

Costruito su un Sistema Operativo sicuro e stabile: EasyIDS è costruito sopra CentOS, una distribuzione Linux fornita da RedHat (http://www.it.redhat.com) sicura e stabile con una vasta community di supporto.

Rilevazione passiva di sonde e tentativi di intrusione: Snort esegue analisi su protocolli e può scoprire passivamente svariati tentativi di attacco come sonde, buffer overflows, backdoors e attacchi Web**.**

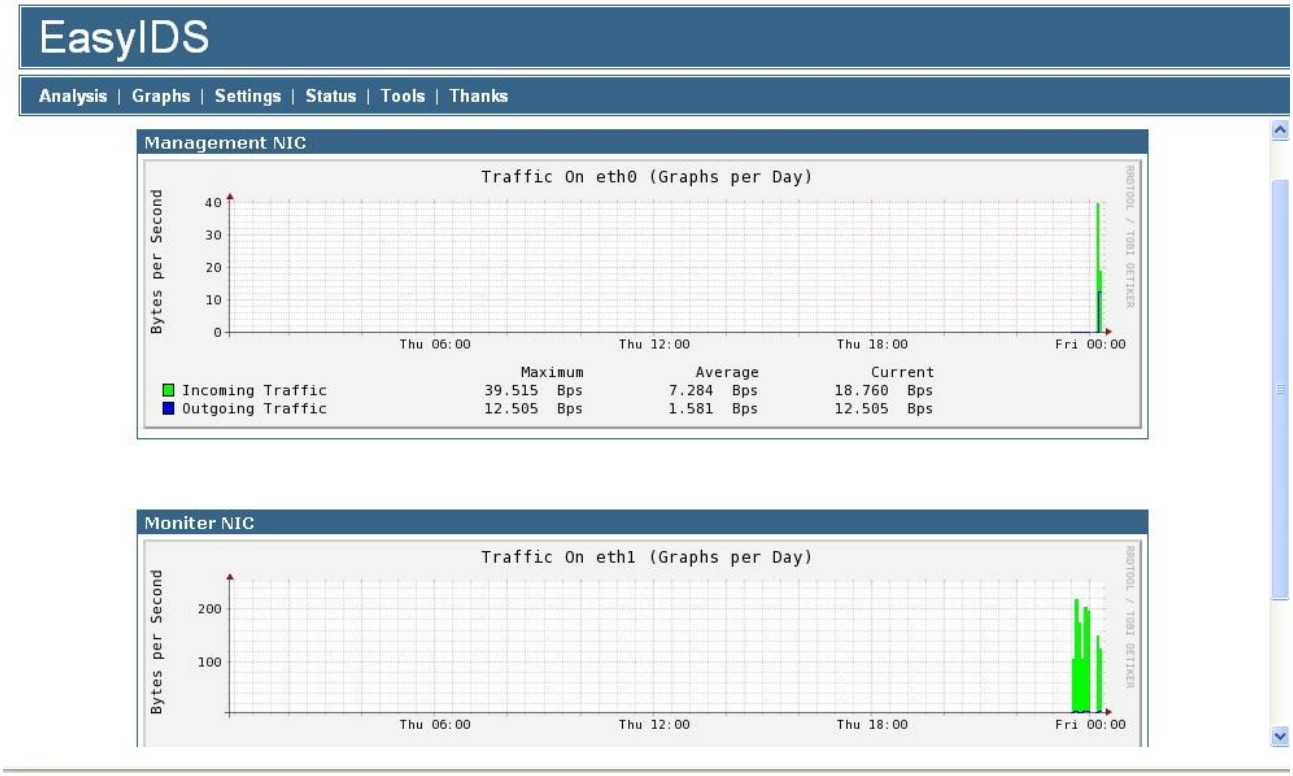
Analisi delle intrusioni via Web: EasyIDS usa l'Addon BASE (http://base.secureideas.net) che è per definizione un Basic Analysis and Security Engine, un'interfaccia Web che fornisce una rappresentazione visual dei dati e permette l'analisi di possibili intrusion che Snort ha individuate nella rete

Analisi del traffico di rete via Web: Ntop (http://www.ntop.org/news.php) è una sonda di rete che fornisce una rappresentazione visuale dell'utilizzo di banda e dell'analisi dei protocolli utilizzati dal traffico di rete.

Aggiornamento automatico delle regole: Le regole di Snort vengono aggiornate automaticamente ogni giorno. EasyIDS può essere configurato anche per poter utilizzare e aggiornare le regole ufficiali con licenza VRT.

Notifica Alert via E-Mail: Tramite lo script SnortNotify (http://www.780inc.com/snortnotify) è possibile configurare la funzione di prelevare determinati alert in base alla priorità dal Database e inviarli via E-Mail all'amministratore.

Grafici delle performance: Tramite lo script pearl PMGraph (http://www.aptivate.org/Projects.BMOTools.pmGraph.html) è possibile visualizzare svariati grafici come: pacchetti droppati, Alerts per secondo, Sessioni aperte, statistiche CPU o altro.



REQUISITI HARDWARE:

RAM	384MB minimo
Hard Disk	È necessario un Hard Disc SCSI, SATA, SAS o IDE (8GB minimo)
CD-Rom	Richiesto CD-Rom IDE, SCSI o USB solo per l'installazione
Schede di Rete	Sono supportate le più comuni schede di rete
Monitor / Tastiera	Richiesti per l'installazione e gestione tramite CLI
Altro	È necessario avere uno Switch con la funzione di mettere una porta in Mirror

2.1.3 Endian

Endian UTM (Unified Threat Management) (www.endian.com/it) tramite la sua applicazione software offre la possibilità di trasformare qualsiasi PC in una vera e propria "security appliance" con la stessa tecnologia dell'hardware fornito dai già predisposti dispositivi Endian UTM Hardware.
Endian è in grado di proteggere in modo completo e sicuro l'intera rete tramite i vari servizi integrati come il firewall, VPN, anti-virus, anti-spam, filtraggio contenuto e-mail ottimizzati per ridurre al minimo i tempi ed i costi di gestione della rete.

CARATTERISTICHE:

Sicurezza della rete: Funzionalità di Firewall, Sistema di Prevenzione delle Intrusioni e Antivirus integrate. Endian include il già noto sistema IDS/IPS Snort integrato direttamente nel Firewall come Intrusion Prevention System.
Attualmente le regole non possono essere aggiunte tramite web, ma soltanto scritte da chi ha conoscenze appropriate. Altre caratteristiche sono:

- Traffic Shaping
- Supporto VoIP/SIP
- Portscan Detection
- DoS e Ddos Protection
- SYN/ICMP Flood Protection

- Anti-spoofing Protection

Sicurezza Web:

- Proxy HTTP e FTP
- ClamAV Anti-Virus
- Blacklist
- Analisi e Filtraggio dei contenuti

Sicurezza Mail

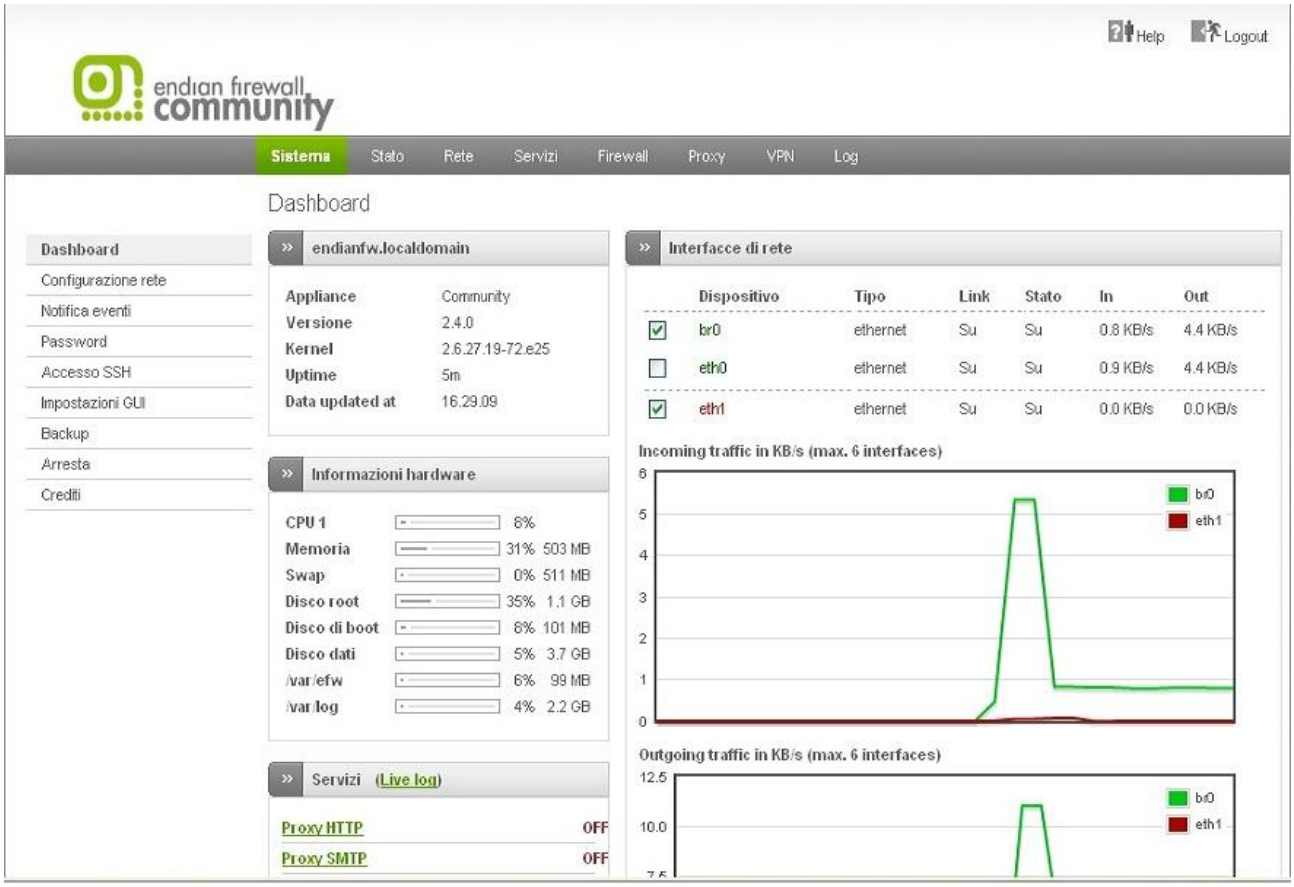
Logging e Reports: Endian UTM software offre svariati metodi di visualizzazione dei Log:

- Live Log Viewer
- Report dettagliati sugli accessi Web degli Utenti
- Statistiche sulla rete, sul sistema e sulle performance
- Syslog locale o remoto

Updates: Gli Updates delle firme antivirus, Blacklist o altro possono essere effettuate direttamente tramite Interfaccia Web.

Management: Le operazioni di gestione possono essere effettuate tramite:

- Accesso tramite Secure Remote SSH
- Console a linea di Comando
- Intuitiva Interfaccia Web di amministrazione



REQUISITI HARDWARE:

CPU	Intel x86 compatibile (500MHz minimo, 1GHz raccomandato)
Multi-Processore	Supporto Multi-Processor Symmetric
RAM	256MB minimo (512 consigliato)
Hard Disk	È necessario un Hard Disc SCSI, SATA, SAS o IDE (4GB minimo)
Software RAID	Per il software RAID1 è richiesto un Hard Disk dello stesso tipo
CD-Rom	Richiesto CD-Rom IDE, SCSI o USB solo per l'installazione
Schede di Rete	Sono supportate le più comuni schede di rete
Monitor / Tastiera	Richiesti esclusivamente per l'installazione
Sistema Operativo	Endian UTM comprende un sistema operativo basato su Linux e ottimizzato per la sicurezza.

2.1.4 Vyatta

Vyatta (http://www.vyatta.com)porta innovazione ed affidabilità nel ramo dell'industria tramite il suo Sistema Operativo per proteggere reti che siano di uffici o di internet service providers. Vyatta ha diviso il software assegnato alla rete dal proprio hardware cosi da permettere agli utenti di approfittare dei vantaggi di costo e di performance di standard-x86 hardware o di dispositivi virtuali.
Vyatta sviluppa e distribuisce tre distinti pacchetti del proprio software:

- **Vyatta Core:** Open source, liberamente scaricabile, offre servizi basilari di Vyatta e non è previsto nessun servizio di supporto del prodotto. Fra i servizi forniti ci sono supporto di routing, firewall, IPS basato su Snort configurato con regole della versione gratuita e accesso limitato alle configurazioni, filtraggio URL, servizio di QoS e supporto IPv6.

- **Vyatta Subscription Edition:** Open source proprietario, provvisto di un kit di caratteristiche esclusive, Addon commerciali e supporto tecnico. Fra i servizi forniti troviamo Supporto Wireless, VPN Client Manager e Accesso Remoto alle API

- **Vyatta Plus:** Servizi migliori e più performanti della precedente edizione: VyattaGuard Web Filter e Snort VRT service che integra

l’utilizzo delle regole utilizzate dalle Industrie e usate dai professionisti della sicurezza Web.

CARATTERISTICHE:

Connettività di Rete: Nel cuore di Vyatta c’è un complesso sistema di routing che supporta pienamente i protocolli IPv4 e IPv6, 802.11 wireless e una grande varietà di protocolli Ethernet.

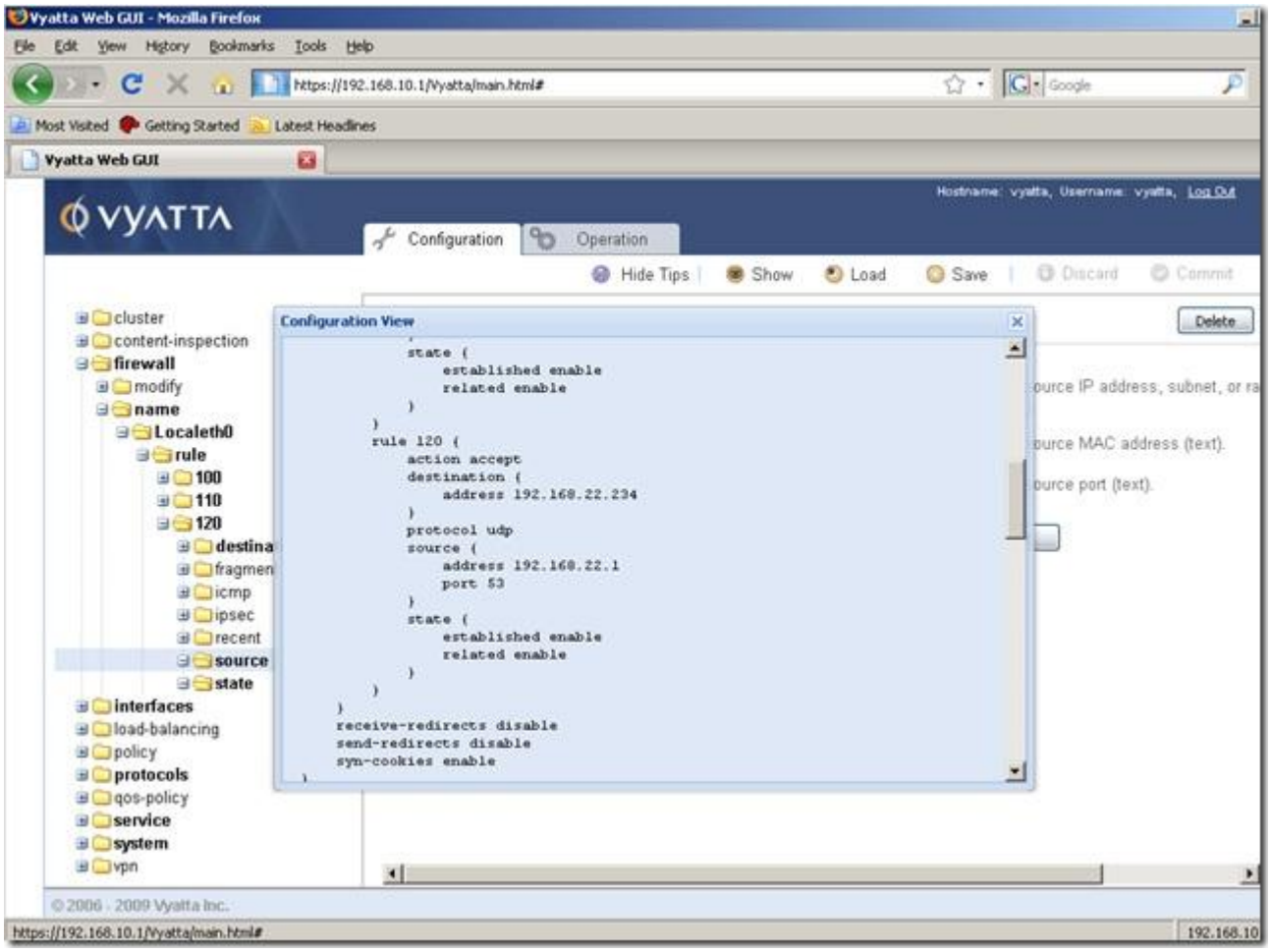
Firewall Protection: Vyatta firewall fornisce servizi di IPv4/IPv6 stateful packet inspection per intercettare e analizzare le attività di rete.

Protezione dalle minacce: Vyatta offre un ulteriore livello di protezione grazie all’integrazione del Web filtering e dell’aiuto dell’Intrusion Prevention System.

Gestione del traffico: Vyatta fornisce una grande varietà di meccanismi di accodamento relativi al QoS che possono essere applicati al traffico in entrata e in uscita o dare priorità a specifiche applicazioni.

Monitoraggio e Report: Vyatta presenta una visione completa delle informazioni di log e diagnostica che possono essere visionate tramite strumenti standard come SNMP, Netflow, Wireshark e Syslog.

Amministrazione: Vyatta può essere gestito tramite un’interfaccia a linea di comando o attraverso web-based GUI da sistemi esterni tramite una connessione SSH.



REQUISITI HARDWARE:

Multi-Processore	Supporto Multi-Processor
RAM	512MB minimo (1GB consigliato)
Hard Disk	È necessario un Hard Disc SCSI, SATA, SAS o IDE (2GB minimo)
Software RAID	Per il software RAID1 è richiesto un Hard Disk dello stesso tipo
CD-Rom	Richiesto CD-Rom IDE, SCSI o USB solo per l'installazione
Schede di Rete	Sono supportate le più comuni schede di rete
Monitor / Tastiera	Richiesti per l'installazione o se si decide di agire sulla CLI locale

2.1.5 Snorby

Snorby Snorby (http://snorby.org) è un nuovo moderno front-end basato su Snort. I concetti fondamentali su cui è stato costruito Snorby sono semplicità e potenza con l'obiettivo di creare un'applicazione open source, gratis, altamente competitiva per il monitoraggio sia di reti private che di quelle di grandi imprese.

CARATTERISTICHE:

Reports: Snorby gestisce i report esportandoli in formati standard conosciuti e indicizza eventi per una ricerca più veloce. Attualmente i formati di "export" conosciuti sono XML, CSV, e PDF.

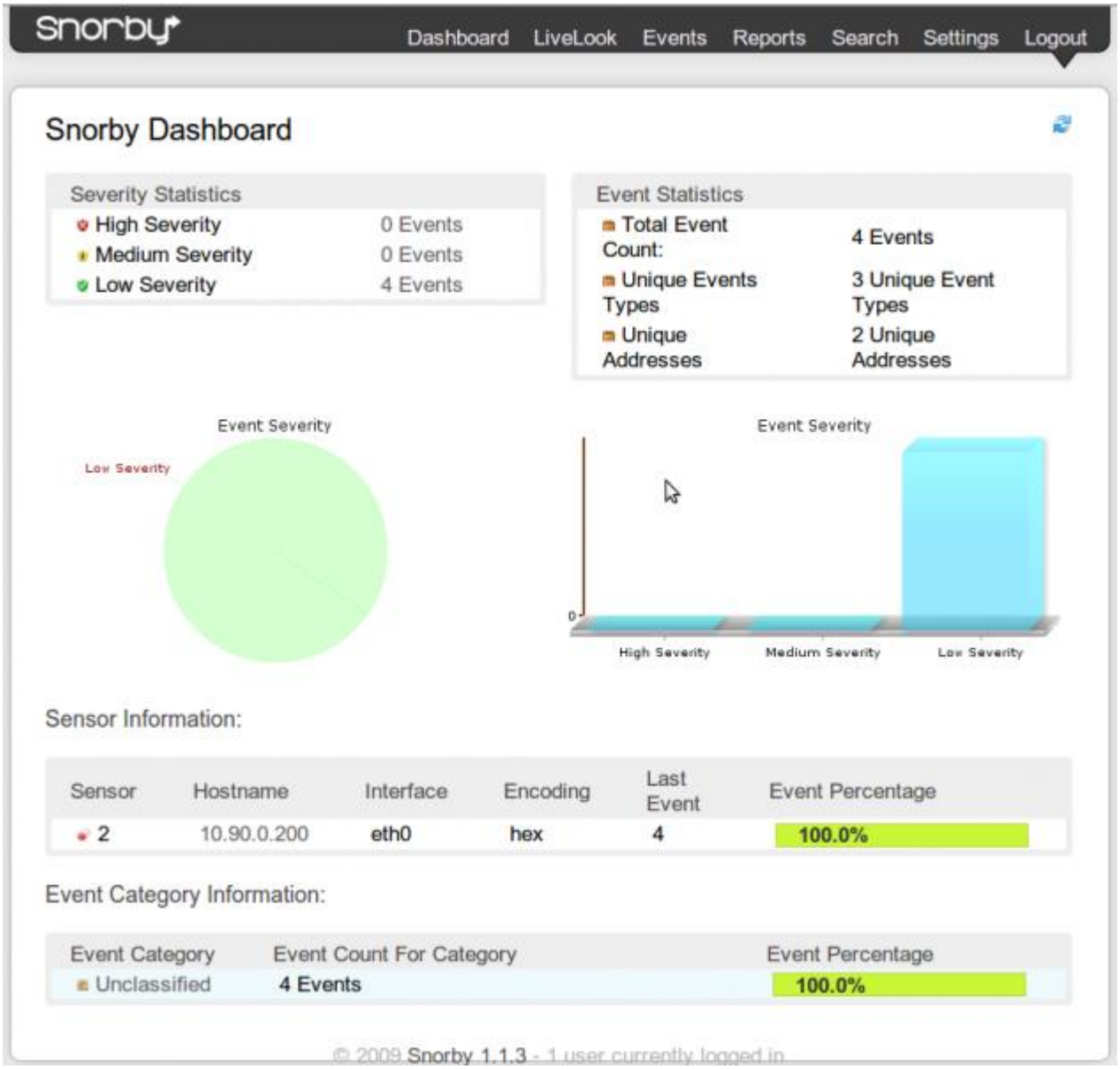
Supporto: Snorby è stato creato per supportare fino a 50 sensori e 100 alerts al minuto.

Classificazione: Snorby classifica i reports in giornalieri, settimanali e mensili cosi da poter avere sempre una buona visione e documentazione degli ultimi.

Collaborazione: Su Snorby ogni evento può essere descritto tramite note e commenti cosi ché rimanga intuitiva l'analisi per eventuali colleghi.

Organizzazione: Snorby ha un'ottima capacità di organizzazione, archiviazione e ricerca dati, così da rendere impossibile la perdita accidentale dei suddetti.

Teammates: Questa funzione è utile per sistemi distribuiti e permette di aggiungere informazioni per contattare altre persone e da l'opportunità di



REQUISITI HARDWARE:

RAM	256MB minimo
Hard Disk	È necessario un Hard Disc SCSI, SATA, SAS o IDE (4GB minimo)
CD-Rom	Richiesto CD-Rom IDE, SCSI o USB solo per l'installazione
Schede di Rete	Sono supportate le più comuni schede di rete
Monitor / Tastiera	Richiesti per l'installazione e gestione tramite CLI

2.1.6 Untangle

Untangle (http://www.untangle.com) è una piattaforma che contiene diverse applicazioni per la gestione e sicurezza della rete, il tutto unificato intorno ad una GUI , database e sistemi di report comuni.
Untangle permette di controllare le attività che decrementano la produttività della rete, come spam o inappropriati utilizzi del web, consente di accedere ovunque da remoto e protegge l'ambiente da minacce provenienti dall'esterno come virus, spyware, botnet e pushing.

CARATTERISTICHE:

Applicazioni: Il prodotto fornisce di per se diverse applicazioni sia free che a pagamento:

Gratuite:

- Web Filter
- Virus Blocker
- Spam Blocker
- Attack Blocker (Dos, DDos)
- Spyware Blocker
- Firewall
- QoS
- Intrusion Prevention

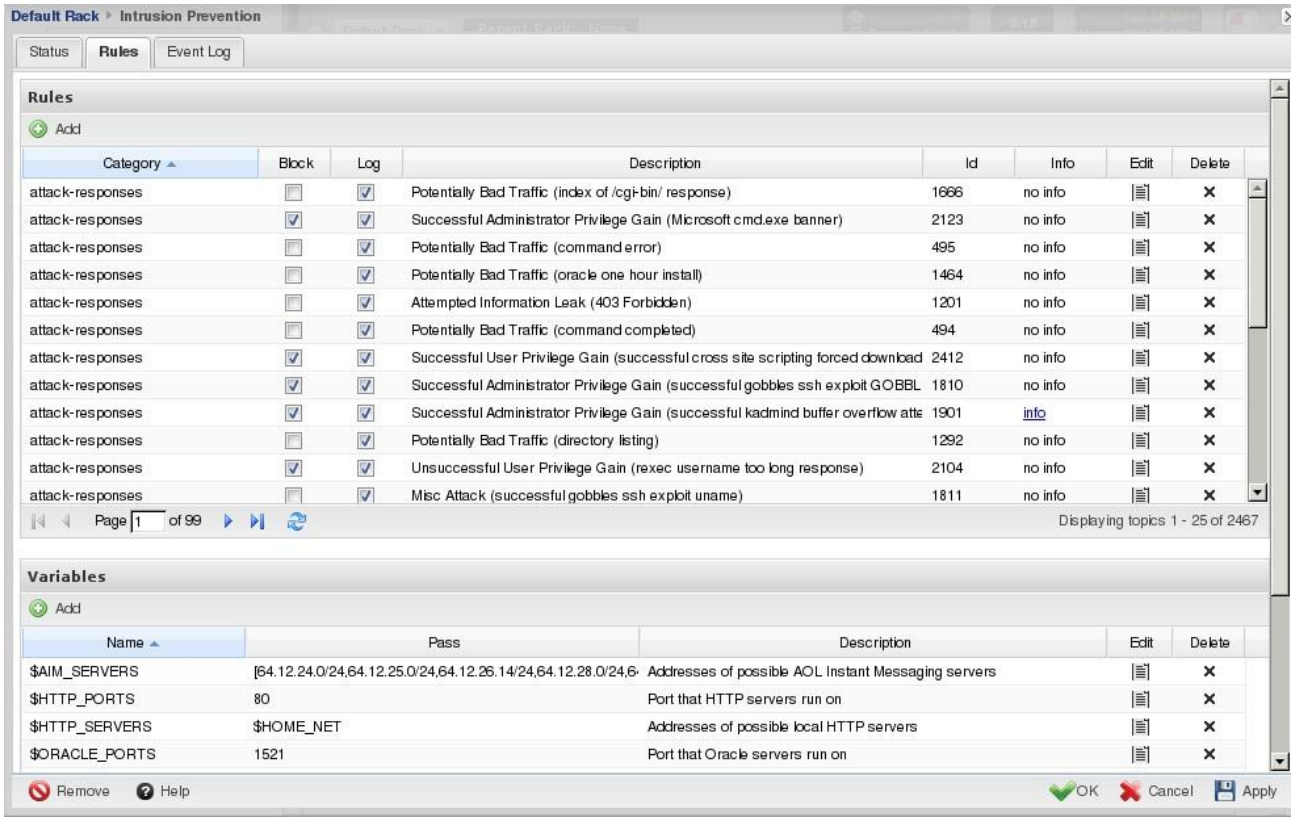
Pagamento:

- Supporto live
- eSoft web filter
- Kaspersky Antivirus
- Spam Booster
- WAN balancer
- WAN failover
- Policy Management

Intrusion Prevention System: Il sistema di prevenzione delle intrusioni è pre-configurato e modificato opportunamente per Untangle. Esso non offre grandi opportunità di modifica, si possono solo aggiungere le proprie regole o modificare quelle esistenti.
La tecnica utilizzata per rintracciare anomalie è quella del signature detection, e le signatures sono quelle di Snort che vengono aggiornate automaticamente da Untangle.

Scalabile: Untangle è una piattaforma software. Se una nuova applicazione viene sviluppata è possibile attivarla immediatamente nel server, senza necessità di comprare nuovo hardware per la rete.

Sviluppo: Untangle software può essere installato in un qualsiasi server Intel compatibile, oppure offre una selezione di servers pre-installati che hanno solo bisogno di essere collegati alla rete.



REQUISITI HARDWARE:

CPU	Intel/AMD compatibile (1GHz minimo)
RAM	512MB minimo (1GB consigliato)
Hard Disk	È necessario un Hard Disc SCSI, SATA, SAS o IDE (20GB minimo)
CD-Rom	Richiesto CD-Rom IDE, SCSI o USB solo per l'installazione
Schede di Rete	Sono supportate le più comuni schede di rete
Monitor / Tastiera	Richiesti per l'installazione e la gestione del sistema
Note	I requisiti minimi possono variare dal numero di applicazioni presenti sul server.

2.1.7 Bro

Bro 

(http://www.bro-ids.org) è un Network Intrusion Detection System open source, che monitorizza passivamente il traffico di rete in cerca di attività sospette. Individua le intrusioni attraverso un'attività di "parsing" del traffico di rete per estrarne le semantiche del livello di applicazione ed eseguire analisi "event-oriented" che comparano l'attività con patterns considerati dannosi. L'analisi include il rilevamento di attacchi specifici, grazie alle Signatures, e di attività sospette.
Bro utilizza un linguaggio personalizzato utilizzato sia come centro per gestire le operazioni, sia come supporto per fermare nuovi attacchi rinvenuti. Infatti se Bro identifica qualche cosa di interessante, può essere istruito a generare un log, un alert verso l'operatore o eseguire un comando sul sistema operativo.

CARATTERISTICHE:

Network Based: Bro è un IDS network-based, quindi raccoglie, filtra e analizza traffico che passa in uno specifico link della rete. Un monitor singolo, opportunamente piazzato in un punto chiave può controllare il traffico entrante e uscente dell'intera rete.

Ampia analisi a livello applicazione: Una delle più importanti caratteristiche di Bro è che include un dettagliato analizzatore "parser-

driven" di molti dei più popolari protocolli del livello di applicazione. L'output di queste operazioni sono una serie di eventi che descrivono in dettaglio l'attività osservata tramite termini semanticamente di alto livello. Questi di per sé non costituiscono un alert, ma sono l'input di altri processi scritti in Bro's custom scripting language.

Custom Scripting Language: Gli script Bro sono programmi scritti in "Bro language". Essi contengono le regole che descrivono quale tipo di attività sono considerate dannose e decidono quale misure adottare per ogni evento.

Policy Scripts inclusi: Bro è fornito di un ricco set di policy scripts progettati per rilevare gli attacchi più comuni cercando di limitare il numero di falsi positivi.

Signature Matching Facility: Bro ha incorporato un facility per il signature matching che osserva in modo specifico il contenuto del traffico. Queste signatures sono espresse come regular expressions piuttosto che fixed strings comunemente utilizzate dagli altri IDPS. Grazie a questo Bro non si limita a esaminare il contenuto del traffico, ma capisce il contesto delle signature riducendo un gran numero di falsi positivi.

Analisi del traffico di rete: Bro non si limita alle signature, infatti può anche analizzare protocolli, connessioni, transazioni, grosse quantità di dati e altre caratteristiche di rete.

Rilevamento seguito da Azione: Gli script di Bro possono generare output files che registano le attività osservate, incluse quelle non soggette ad attacchi. Essi possono essere generati nel formato syslog, oppure gli script possono mandare e-mail o terminare connessioni esistenti. Ovviamente essendo un IDS le azioni disponibili sono limitate.

Compatibilità con Snort: Tramite lo strumento snort2bro è possibile convertire le signatures di Snort in signature compatibili con Bro.

REQUISITI HARDWARE:

CPU	Intel/AMD compatibile (1GHz minimo, 2GHz o più consigliati)
RAM	1GB minimo (2-3GB consigliati)
Hard Disk	È necessario un Hard Disc SCSI, SATA, SAS o IDE (10GB minimo, 50GB consigliati)
CD-Rom	Richiesto CD-Rom IDE, SCSI o USB solo per l'installazione
Schede di Rete	Sono supportate le più comuni schede di rete
Monitor / Tastiera	Richiesti per l'installazione e la gestione del sistema

.

2.1.8 OpenIDS

OpenIDS OPENIDS (http://www.prowling.nu) è una distribuzione basata su OpenBSD e Snort. Con il passare del tempo questo prodotto si è evoluto da una soluzione prettamente IDS ad una più completa soluzione Network Security Monitoring. OpenIDS infatti offre flessibilità e gli strumenti giusti per aiutare nel monitoraggio della rete.

CARATTERISTICHE:

Sicurezza: Strutturato su Snort IDS, OpenIDS offre tutte le potenzialità del prodotto per quanto riguarda l'intrusion detection, compreso il supporto per le regole commerciali con licenza VRT e quelle prodotte da EmergingThreat (http://www.emergingthreats.net). OpenIDS si occuperà di aggiornarle ogni notte.

Analisi: Tramite BASE è possibile avere una migliore rappresentazione degli alerts tramite grafici, statistiche, o analisi in dettaglio, grazie ad un'interfaccia web.

Profile Search: Profile Search permette di analizzare in profondità un grande quantitativo di risorse dati estrapolando le informazioni più importanti, in base a cosa stiamo utilizzando nel sistema (BASE, P0f, Pads, GeoIP).

Statistiche del sistema o dei sensori: Su OpenIDS è possibile visualizzare statistiche sui vari sensori di tutti i sistemi connessi e dei processi più importanti.

Perfomn-graph: Perfmon-graph ci permette di visualizzare grafici di tutti i sistemi connessi, avremo informazioni come l'utilizzo della CPU, Mbit per secondo e dei pacchetti scartati.

Threat report: Fornisce un'ulteriore aiuto alla gestione dei report. Contiene infatti una visualizzazione globale di ogni mese, e se alert vengono cancellati da BASE, Threat report ne terrà conto, rimovendo quindi i falsi positivi dal report finale.

Netflow: OpenIDS genera netflows dai sensori, che verranno visualizzati nell'apposita sezione. C'è possibilità di manipolarli tramite nfdump, un'applicazione eseguibile da shell.

P0F: P0F è uno strumento passivo per effettuare operazioni di fingerprinting. È possibile effettuare una ricerca su singoli IP o su tutti i sistemi operativi rintracciati.

PADS: PADS sta per Passive Asset Detection System, ed è una ulteriore risorsa per l'analisi e la rilevazione di attività malevole che usa la tecnica signature-based.

2.1.9 Suricata

Suricata è un Next Generation Intrusion Detection e Prevention System open source. Questo prodotto non è stato ideato per rimpiazzare o emulare gli strumenti già esistenti, ma per portare nuove idee e tecnologie nel campo della sicurezza di rete.

Oltre al cuore del software Suricata si avvale di una libreria, HTP Library, personalizzata utilizzata come parser e normalizer http.

Il prodotto come la suddetta libreria sono sviluppati da OISF (http://www.openinfosecfoundation.org) un'organizzazione non a scopo di lucro fondata allo scopo di ampliare e migliorare questo progetto.

CARATTERISTICHE:

Sicurezza: Suricata è un IDPS che utilizza le tecniche di Signature e Protocol based inspection tramite regole sviluppate esternamente, per monitorare il traffico di rete e informare l'amministratore quando avviene qualche cosa di sospetto.

I protocolli riconosciuti non si soffermano ai classici IP, TCP, UDP e ICMP, ma si estendono a HTTP, TLS, FTP e SMB.

Se utilizzato come IPS ci sono vari metodi per catturare i pacchetti: NFQueue, IPFRing, lo standard LibPcap e IPFW per i sistemi FreeBSD.

Performance: Suricata supporta il multithread offrendo velocità e maggiore efficienza nell'analisi del traffico di rete. Oltre all'accelerazione hardware (limiti permettendo) il prodotto è stato creato per sfruttare al meglio la crescente potenza offerta dalle ultime CPU multi-core.
Oltre al multithread c'è un supporto sperimentale per CUDA se si utilizza una Nvidia GPU, ma non è ancora pienamente utilizzabile.

Multipiattaforma: Suricata è stato ideato per integrarsi nelle maggiori piattaforme esistenti:

- CentOS5
- Debian/Ubuntu
- Fedora Core
- FreeBSD8
- MacOS
- Windows

Rules: Un gran numero di rulesets compatibili sono scaricabili dal sito di Emerging Threats. In alternativa si possono trasferire le regole di Snort perché Suricata ne riconosce la sintassi, quindi è possibile trasferire anche le proprie regole personalizzate.

Output: I soli formati supportati per archiviare eventi sono Syslog e Unified2 format. Grazie a questo è possibile utilizzare Addons o altri strumenti utili come Barnyard2 (http://www.securixlive.com/barnyard2), BASE o Squil (http://sguil.sourceforge.net).

2.1.10 Ossec

Ossec (http://www.ossec.net) è un Host-Based Intrusion Detection System, scalabile e multipiattaforma. Possiede un potente motore di analisi e correlazione che può effettuare analisi dei log, file integrity checking, Windows registry monitoring, scovare intrusioni non autorizzate, rootkit detection, real-time alerting e active response.
Ossec è multipiattaforma e supporta la maggior parte dei sistemi operativi, come Linux, OpenBSD, MacOS, Solaris e Windows.

CARATTERISTICHE:

Architettura: Ossec è costituito da più di un dispositivo, possiede un Manager centrale che monitorizza tutto e riceve informazioni da agents (sensori), syslog e databases.

- **Manager:** Il manager è la parte centrale di Ossec e contiene i databases dei file integrity checking , dei logs e degli eventi. Contiene anche tutte le regole, i decoder e le configurazioni cosi da rendere più facile l'amministrazione di agents multipli.
- **Agent:** L'agent è un piccolo programma installato nei sistemi che si desidera monitorare. Esso raccoglie informazioni e le spedisce al Manager per l'analisi. Sono progettati per utilizzare veramente poche risorse quindi non influenzano le prestazioni del sistema.
- **Agentless:** Per i sistemi in cui non si possono installare agents, Ossec permette operazioni di file integrity monitoring . Alcuni

esempi possono essere firewalls, routers o anche particolari sistemi Unix.

Sicurezza: Ossec offre svariate funzionalità nell'ambito della sicurezza:

- Analisi dei log e correlazioni:
  - Regole flessibili basate su XML
  - Time Based Alerting
  - Libreria contenente molte regole già integrata
- Integrity Checking
- Root Kit detection

Active Response: Ossec permette di intervenire immediatamente sulla minaccia con vari metodi:

- Disabilitare il servizio per un determinato intervallo di tempo (espresso in minuti)
- Blacklists
- Firewall-Drop: uno script che permette di comunicare universalmente con i firewall delle più comuni distribuzioni Unix/Linux

Firewalls, Switch e Routers: Ossec può ricevere ed analizzare eventi Syslog da una grande varietà di firewalls, switch e routers che supportano questa tecnologia.

Supporto: Ossec è un software Open Source che conta migliaia di download al mese, ed è sempre più utilizzato da altri IPS, Università, Imprese o centri di archiviazione dati come soluzione principale. Questo comporta una crescente community e un vasto supporto. Se si necessita di aiuto più specifico, Trend Micro, la compagnia dietro questo progetto offre anche l'opzione di un supporto professionale e specifico.

2.1.11 Aide

AIDE (Advanced Intrusion Detection Environment)  (http://www.cs.tut.fi/~rammer/aide.html) è un Host-Based IDS con funzionalità di File Integrity Checker.

CARATTERISTICHE:

AIDE costruisce un database contenente tutti i file specificati nel file di configurazione.

Il database immagazzina vari attributi dei files quali: permessi, numero inode, utente, gruppo, grandezza del file, mtime e ctime, atime, numero dei link e nome dei link. Oltre a questo crea un codice checksum o hash crittografato per ogni file usando uno o più combinazioni dei seguenti algoritmi: sha1, sha256, sha512, md5, rmd160 e tiger.

Generalmente un amministratore crea un database AIDE in un sistema prima che sia collegato alla rete. Infatti il primo database sarà una rappresentazione del sistema nel suo stato originale e un mezzo con cui verranno misurati gli update e i cambiamenti futuri.

Il database dovrebbe contenere file di sistema, librerie, header files e tutti quei dati che si presume rimangano gli stessi per un lungo periodo di tempo, e non i files usati frequentemente dagli utenti.

Per i motivi descritti sopra è necessario che il database e tutti i files di configurazione vengano situati in una zona sicura come un dispositivo a

sola lettura.

Aide supporta molte delle piattaforme Unix-based quali:

- Solaris
- Linux 2.x
- FreeBSD
- Unixware
- BSDi 4.1
- OpenBSD
- AIX 4.2
- TRU64 4.0x
- HP-UX 11i

Grazie alla sua semplicità Aide è un ottimo mezzo di prevenzione sia per minacce provenienti dall'interno, sia per quelle esterne.

2.1.12 Samhain

Samhain 

(http://www.la-samhna.de/samhain/index.html) è un Host-Based Intrusion Detection System che fornisce funzioni di file integrity checking e analisi dei log. Questo prodotto è un'applicazione open source multipiattaforma creato per monitorare diversi host con differenti sistemi operativi, garantendo funzioni logging e gestione centralizzati o anche utilizzabile come applicazione stand-alone per un singolo host.

CARATTERISTICHE:

Gestione Centralizzata: Uno dei punti di forza di Samhain è la capacità di monitorare e gestire l'intero sistema da una locazione centrale. A questo scopo diverse componenti sono necessarie:

- **Samhain File/Host integrity checker:** questo è l'agent che risiede negli host monitorati, è stato creato per essere eseguito come deamon per evitare warnings ripetitivi perché il deamon tiene una memoria dei cambiamenti nei files.

- **Yule log server:** Yule colleziona log dei reports dai vari client su host remoto o locale, tiene traccia dello stato dei clients e gli permette di scaricare baseline databases e configuration files a livello runtime (se contenuti nel server).

- **Database relazionale:** Dove vengono immagazzinati tutti i log

- **Web based console – Beltaine:** Beltaine è un'applicazione PHP che consente di visualizzare i log, aggiornare i database, gestire i client, tutto in modo semplice grazie ad un'interfaccia grafica intuitiva.

- **Log facility:** ogni facility può essere abilitata o disabilitata individualmente. Esse comprendono:

    - Central log server: i messaggi vengono inviati tramite connessione TCP criptata, quindi i clients devono autenticarsi al server.
    - Syslog: i reports vengono inviati tramite sistema Syslog
    - E-mail: gli alert vengono inviati via e-mail all'amministratore
    - Programma esterno: è possibile integrare un programma esterno per aggiungere nuove funzionalità.

- **Risposta Attiva:** Samhain può eseguire programmi esterni verso eventi definiti dall'utente, comuni tecniche di risposta attiva sono il riavvio della macchina o la riconfigurazione del firewall.

- **Multipiattaforma:** Samhain supporta tutti i sistemi POSIX (Unix, Linux, Cygwin) o sistemi Windows che ne permettono l'emulazione.

2.2 Caratteristiche Individuate

In questa sezione si esamineranno in dettaglio tutte le caratteristiche individuate testando i vari prodotti. Essendo innumerevoli, per fare maggiore chiarezza, sono state raggruppate in base alla propria funzione:

- **Caratteristiche generali:** Queste rappresentano le caratteristiche che possono essere trovate su tutti gli IDPS indipendentemente dal tipo o dalla funzione.

- **Caratteristiche Host-Based:** sono quelle inerenti agli IDPS di tipo Host-Based.

- **Caratteristiche Network-Based:** quelle inerenti agli IDPS di tipo Network-Based. Essendo più complessi rispetto agli Host-Based è stato necessario fare un'ulteriore suddivisione:
    - **Caratteristiche Generali:** sono quelle comuni a tutti gli IDPS di tipo Network-Based.
    - **Protocolli analizzati:** in questa sede vengono riportati tutti i portocolli che gli IDPS effettuanti Stateful Protocol Analysis possono riconoscere e quindi analizzare.
    - **Minacce riconosciute:** Qui vengono riportate tutte le minacce che i vari prodotti possono rilevare.
    - **Formato dei log di output:** Indica tutti i formati supportati per i log di output.

Sfortunatamente non sono stato in grado di testare gli IDPS di tipo Wireless e Network Behavior Analysis in quanto si tratta di tecnologie giovani ancora poco diffuse e prive di soluzioni OpenSource.

Caratteristiche Generali

Ids / Ips: Ovviamente queste due sono le caratteristiche che costituiscono il cuore della tecnologia di rilevazione e prevenzione delle intrusioni. Un prodotto può avere sia caratteristiche di prevenzione che di rilevazione o essere utilizzato soltanto come strumento passivo che avverte quando accade qualche cosa di sospetto

Multipiattaforma: Questa caratteristica riguarda i prodotti o le componenti prettamente software e rappresenta la possibilità di installare questi ultimi in un gran numero di diversi Sistemi. Ormai i prodotti IDPS supportano praticamente qualsiasi tipo di sistema operativo, ma stanno crescendo anche quelli prodotti su supporti hardware appositi.

Multi-Threading: Il multi-threadng è una caratteristica nuova nell'ambito degli IDS.
Esso indica la possibilità di eseguire più thread da parte del processore, nel nostro caso specifico si può dividere in più thread la fase di elaborazione del pacchetto, rendendo il sistema più veloce. Nella maggior parte dei casi questa tecnica è implementata anche su sistemi multi-processore, e permette all'IDPS di sfruttare al massimo le potenzialità delle CPU.

Interfaccia Grafica: Oltre alla CLI molti IDPS possono supportare un'interfaccia grafica per una più semplice gestione e visualizzazione dei dati. Ormai è sempre più affermato l'utilizzo di interfacce web per svolgere questo compito che supportano i più noti browser.

Database Interno: Questa caratteristica indica se nel prodotto è presente un database interno o c'è bisogno di ricorrere a supporti esterni. Nella

maggior parte dei casi la presenza di questa caratteristica esclude l'utilizzo di altre tipologie di database.

Caratteristiche Host-Based

Buffer Overflow: Un buffer overflow è una vulnerabilità di sicurezza che può colpire un software. Consiste nel fatto che tale programma non controlla in anticipo la lunghezza dei dati in arrivo, ma si limita a scrivere il loro valore in un buffer di lunghezza prestabilita, confidando che l'utente non immetta più dati di quanto esso possa contenere.

System-Call monitoring: La System-Call monitoring è una tecnica per rilevare e controllare applicazioni o processi compromessi monitorando le chiamate di sistema effettuate, infatti l'agente conosce a priori quali chiamate un'applicazione dovrebbe effettuare quindi riesce facilmente a scovare comportamenti anomali.

File Integrity Check: Il file integrity check consiste nel controllare che i file di sistema o file di interesse non siano corrotti. Questo avviene attraverso l'uso di algoritmi per la verifica dell'integrità o autenticità dei files, ma richiede due copie dello stesso file. Un approccio più utilizzato è quello di memorizzare solo i checksums dei files per una futura comparazione.

File access attempts: Con file access attempts si indicà la possibilità per un agent di monitorare i tentativi di accesso ai files critici e fermare quelli sospetti.

Rootkit detection: Il rootkit è un programma software creato per avere il controllo completo sul sistema senza bisogno di autorizzazione da parte di utente o amministratore. Recentemente alcuni virus informatici si sono avvantaggiati della possibilità di agire come rootkit all'interno del sistema operativo permettendogli di non essere rintracciabili da strumenti di amministrazione e controllo.
I rootkit vengono utilizzati come supporto a una vasta gamma di malware: backdoor, trojan e spyware.

Log Analysis: L'analisi dei log nell'ambito dell'intrusion detection è il processo o le tecniche usate per individuare attacchi su un dispositivo specifico usando i propri log come fonte primaria d'informazione.

Risposta Attiva: La risposta attiva è una caratteristica molto importante in quanto permette di agire tempestivamente sulla minaccia, le tecniche utilizzate sono quelle descritte precedentemente, ma ogni HIDPS ha un propria gamma di azioni utilizzabili.

Caratteristiche Network-Based
Generali

Traffic Shaping: Per traffic shaping si intende l'insieme di operazioni di controllo sul traffico di rete, finalizzate a ottimizzare o garantire le prestazioni di trasmissione, ridurre o controllare i tempi di latenza e sfruttare al meglio la banda disponibile tramite l'accodamento e il ritardo dei pacchetti che soddisfano determinati criteri.
Il meccanismo determina, sulla base delle condizioni del traffico, della priorità assegnata al pacchetto e ai limiti di banda prestabiliti se il pacchetto

può essere trasmesso o deve essere accodato per la successiva trasmissione.

Addons: La possibilità di applicare estensioni o meno al nostro pacchetto IDPS è una delle caratteristiche più interessanti, per via del fatto che i diversi addons possono migliorare di gran lunga l'utilizzo del prodotto aggiungendo nuove funzionalità, quindi rendendolo flessibile a nuove opportunità di applicazione.

Firewall-Ibrido: questa caratteristica riguarda soprattutto i dispositivi IPS, infatti si è discusso a lungo di come inserire questi due elementi nella rete. Un IPS/firewall-ibrido offre sicuramente un'alternativa alle tipiche configurazioni e permette di trascurare i problemi di interfacciamento e comunicazione fra i due.

Costi: Nonostante tutti i prodotti verificati siano Open Source e liberamente scaricabili, quasi tutte le implementazioni offrono uno o più servizi a pagamento che comprendono:

- Regole addizionali
- Funzionalità aggiuntive
- Supporto tecnico
- Pacchetto hardware

In genere tutti i servizi vengono offerti tramite iscrizione a pagamento annuale o mensile.

Protocolli Riconosciuti

HTTP: L'hypertext transfer protocol è usato come principale sistema di trasmissione di informazioni sul web avvalendosi del protocollo TCP.

FTP: Il file transfer protocol è un protocollo per la trasmissione dati tra host in maniera efficiente ed affidabile.

IMAP: L'internet message access protocol è un protocollo di comunicazione di ricezione e-mail inventato come alternativa più moderna all'utilissimo POP.

POP3: Il post office protocol è un protocollo che permette, mediante autenticazione, l'accesso ad un account di posta elettronica presente nel relativo host per scaricare e-mail.

SNMP: Simple Network Management Protocol è un protocollo che opera a livello 7 del modello OSI, esso consente la gestione e supervisione di apparati collegati in una rete, rispetto tutti quegli aspetti che richiedono azioni di tipo amministrativo.

Telnet: L'obiettivo di telnet è fornire supporto per le comunicazioni, è solitamente utilizzato per fornire all'utente sessioni di login remoto di tipo riga di comando fra hosts su internet.

SSH: Secure SHell è un protocollo una sessione remota codificata ad interfaccia a riga di comando con un altro host. L'interfaccia è simile a quella di telnet, ma l'intera comunicazione avviene in maniera cifrata, è per questo che SSH è diventato uno standard di fatto nella comunicazione fra

dispositivi di rete.

RTP: Il real time protocol è un protocollo che lavora a livello applicazione per servizi in tempo reale in internet come l'interattività e l'audio.

TCP: Il transmission control protocol è progettato per utilizzare i servizi forniti dal protocollo IP, per costruire un canale di comunicazione affidabile fra due processi applicativi.

UDP: L'user datagram protocol è un protocollo di trasporto a pacchetto usato in combinazione con IP. A differenza del TCP è un protocollo di tipo connectionless, inoltre non gestisce il riordinamento dei pacchetti, ma può contare su una maggiore velocità a discapito dell'affidabilità.

SMB: server message block è utilizzato principalmente per condividere files, stampanti, porte seriali e comunicazioni di varia natura tra diversi nodi di una rete. Esso include anche un meccanismo di comunicazione fra processi autenticata.

SSL: Secure Sockets Layer è un protocollo crittografico che permette una connessione sicura ed integrità dati su reti TCP/IP cifrando la comunicazione dalla sorgente alla destinazione a livello di trasporto.

IP: L'internet protocol è il protocollo su cui si basa Internet, più precisamente è nato per interconnettere reti di natura diversa di interconnessione di reti, pertanto spesso è implementato sopra altri protocolli come Ethernet o ATM.
La versione correntemente usata è detta IPv4, ma è presente anche la più recente IPv6 nata dall'esigenza di gestire meglio il crescente numero di dispositivi collegati ad internet.

ICMP: L'internet control message protocol è un protocollo di servizio che si preoccupa di trasmettere informazioni riguardanti malfunzionamenti, informazioni di controllo o messaggi tra vari componenti di una rete.
ICMP è incapsulato direttamente in IP e non è quindi garantita la consegna a destinazione dei pacchetti.

ARP: L'address resolution protocol fornisce la "mappatura" tra l'indirizzo IP a 32bit e il suo MAC address, l'indirizzo fisico a 48 bit.

Minacce Riconosciute

Backdoor: Le backdoor sono porte che rimangono sempre aperte, spesso in modo non rintracciabile, e consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema.

Botnet: Una botte è una rete di computer collegati ad Internet controllati da un'unica entità, il botmaster. Ciò può essere causato da falle nella sicurezza o mancanza di attenzione di utenti o dell'amministratore del sistema, per cui i computer vengono infettati da virus o trojan quali consentono ai loro creatori di controllare il sistema, per scagliare attacchi distribuiti.

DoS e DDoS: è la sigla di Denial of Service letteralmente negazione di servizio. Questo tipo di attacco cerca di portare il funzionamento di un sistema che fornisce un servizio al limite delle prestazioni fino a renderlo non più in grado di operare.
Il DDoS (Distributed Denial of Service) è una variante di tale approccio, realizzato utilizzando numerose macchine attaccanti (botnet), cosi da rendere difficilmente individuabile l'autore dell'azione malevola.

Exploit: exploit è un termine usato per identificare codice che, sfruttando una vulnerabilità, porta all'acquisizione di privilegi di amministratore su un sistema.

Spam: lo spamming è l'attività di invio di grandi quantità di messaggi indesiderati (generalmente commerciali) e può essere messo in atto attraverso qualunque media, anche se attualmente il mezzo più utilizzato sono le e-mail.

Policy Violation: Con policy violation si intendono tutte quelle azioni atte a forzare o ignorare le regole di un sistema, come accesso a files o zone protette e acquisizione di diritti non consentiti in un sistema.

Port Scanning: è una tecnica utilizzata per raccogliere informazioni su un computer connesso ad una rete stabilendo quali porte siano in ascolto.
Consente inoltre di inviare richieste di connessione al bersaglio elaborando risposte per stabilire quali servizi di rete siano attivi.
Il port scanning di per se non è dannoso per il sistema, ma può essere utilizzato per preparare attacchi mirati alla sicurezza.

Spyware: è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso, trasmettendole a qualcuno che li utilizzerà per trarne profitto (in genere pubblicità).

Worm: è una particolare tipologia di malware in grado di auto replicarsi. È simile ad un virus, ma non necessita di legarsi ad altri eseguibili per diffondersi

2.3 Tabelle Riassuntive

IDS/IPS Caratteristiche Generali

Prodotto	Host-Based	Network-Based	Wireless	Network-Behavior	IDS	IPS	Multipiattaforma	Multi-Threading	Interfaccia Grafica	Database Interno	Lingua
Snort	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	
EasyIDS	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓	
Endian	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	
Vyatta	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	
Snorby	✗	✓	✗	✗	✓	✗	✓	✓	✓	✗	
Untangle	✗	✓	✗	✗	✓	✓	✗	✗	✓	✓	
Bro	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	
OpenIDS	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓	
Suricata	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗	
Ossec	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗	
Aide	✓	✗	✗	✗	✓	✗	✓	✗	✗	✓	
Samhain	✓	✗	✗	✗	✓	✓	✓	✗	✓	✓	

Caratteristiche Host-Based

Prodotto	Risposta attiva	Signature-Based	Anomaly-Based	Buffer Overflow	System-Call	File Integrity Check	File Access Attempt	Log Analysis	Rootkit
Ossec	✓	✓	✓	✓	✓	✓	✓	✓	✓
Aide	✗	✗	✗	✗	✗	✓	✗	✗	✗
Samhain	✓	✓	✗	✓	✓	✓	✓	✓	✓

Caratteristiche Network-Based: Generali

Prodotto	Signature-Based	Protocol Analysis	Anomaly-Based	Traffic Shaping	Addons	Firewall-Ibrido	Costi
Snort	✓	✓	✓	✗	✓	✗	Regole VRT
EasyIDS	✓	✓	✓	✗	✗	✗	-
Endian	✓	✗	✗	✓	✗	✓	Pacchetti Hardware
Vyatta	✓	✗	✗	✓	✗	✓	Subscription Edition / Plus Edition
Snorby	✓	✓	✓	✗	✗	✗	Regole VRT
Untangle	✓	✗	✗	✓	✓	✗	Servizi Aggiuntivi / Pacchetti Hardware
Bro	✓	✓	✗	✗	✓	✗	-
OpenIDS	✓	✓	✓	✗	✗	✗	-
Suricata	✓	✓	✓	✗	✓	✗	-

Caratteristiche Network-Based: Protocolli Riconosciuti

Prodotto	HTTP	IP	TCP	UDP	ICMP	FTP	ARP	SSH
Snort	✓	✓	✓	✓	✓	✓	✓	✓
EasyIDS	✓	✓	✓	✓	✓	✓	✓	✓
Bro	✓	✓	✓	✓	✓	✓	✓	✓
OpenIDS	✓	✓	✓	✓	✓	✓	✓	✓
Snorby	✓	✓	✓	✓	✓	✓	✓	✓
Suricata	✓	✓	✓	✓	✓	✓	✗	✗

Prodotto	SSL	RPC	SMB	Smtp	POP3	FtpTelnet	IMAP
Snort	✓	✓	✓	✓	✓	✓	✓
EasyIDS	✓	✓	✓	✓	✓	✓	✓
Bro	✓	✗	✗	✓	✓	✗	✓
OpeniIDS	✓	✓	✓	✓	✓	✓	✓
Snorby	✓	✓	✓	✓	✓	✓	✓
Suricata	✗	✓	✗	✗	✓	✓	✓

Caratteristiche Network-Based: Minacce riconosciute

Prodotto	Backdoor	Buffer Overflow	Botnet	Dos	DDos	Exploit	Spam	Policy Violation	Scanning	Spyware	Worms
Snort	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
EasyIDS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Endian	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Vyatta	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Snorby	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Untangle	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bro	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓
OpenIDS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Suricata	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓

Caratteristiche Network-Based: Formato Log Output

Prodotto	Syslog	Unified	Unified2	Tcpdump Pcap	Fast Log	Database
Snort	✓	✗	✓	✓	✓	✓
EasyIDS	✗	✗	✗	✗	✗	✓
Endian	✗	✗	✗	✗	✗	✓
Vyatta	✗	✗	✗	✗	✗	✓
Snorby	✓	✗	✗	✓	✓	✓
Untangle	✗	✗	✗	✗	✗	✓
Bro	✗	✗	✗	✗	✗	✓
OpenIDS	✗	✗	✗	✗	✗	✓
Suricata	✗	✓	✓	✗	✓	✓

Conclusioni

La comparazione degli IDS/IPS è argomento ancora dibattuto a livello teorico, infatti le diverse implementazioni a cui sono destinati e la possibilità di integrazione in altri dispositivi per la sicurezza rendono difficile raggrupparne le caratteristiche a livello astratto.

All'attuale stato della tecnologia si può affermare che gli IDS/IPS per quanto riguarda alle funzionalità principali, e nello specifico il rilevamento e la prevenzione delle minacce, non presentano sostanziali differenze. La ragione di tale indifferenziazione risiede essenzialmente nell'interoperabilità di questi. Ovviamente, ogni prodotto ha i propri elementi caratteristici.

Per quanto riguarda la tipologia Network-Based, Snort rimane, a mio avviso, il miglior IDPS in circolazione data la grande flessibilità e accessibilità, lo dimostra il fatto che un'ampia gamma di IDPS lo utilizzano come motore di rilevazione e prevenzione.

Parlando degli Host-Based reputo Ossec il migliore, poiché riesce ad integrare ed estendere tutte le funzionalità che gli altri Host-Based IDPS si limitano a svolgere in maniera singolare; è per questo che risulta già ampiamente conosciuto ed affermato nel suo campo.

Bibliografia

Axelsson S., “The Base-Rate Fallacy and the Difficulty of Intrusion Detection”, 2000, http://www.raid-symposium.org/raid99/PAPERS/Axelsson.pdf

Julisch K., “Dealing with False Positives in Intrusion Detection”, 2000 http://www.raid-symposium.org/raid2000/Materials/Abstracts/50/Julisch_foils_RAID2000.pdf

Lippmann R., Fried D., Graf I., Haines J., Kendall K., McClung D., Weber D., Webster S., Wyschogrod D., Cunningham R., Zissman M., “Evaluating Intrusion Detection Systems”, 2000, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.110.4112

McHugh J., “Testing Intrusion Detection Systems”, 2000, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.85.1132

Patwardhan A., Parker J., Joshi A., “Secure Routing and Intrusion Detection in Ad Hoc Networks”, 2005, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.96.3735

Piccardi S., “Introduzione agli Intrusion Detection System”, 2004, http://svn.truelite.it/documenti/ids.pdf

Wack J., Tracy M., Souppaya M., “Guideline on Network Security Testing”, 2003, http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf

Scarfone K., Mell P., “Guide to Intrusion Detection and Prevention Systems”, 2007, http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Guaglione V., “Due IDS gratuiti ed Open Source”, 2007, http://sicurezza.html.it

Guaglione V., “IDS I sistemi per il rilevamento delle intrusioni”, 2007, http://sicurezza.html.it

Barberini N., “Spyware e IPS”, http://www.windoweb.it

Grand A., “Intrusion Detection and Prevention Systems”, 2008, http://www.scribd.com/doc/2096981/Intrusion-Detection-and-Prevention-Systems

Brox A., “Signature-Based or Anomaly-Based Intrusion Detection: The Practice and Pitfalls”, 2002, http://www.scmagazineus.com/signature-based-or-anomaly-based-intrusion-detection-the-practice-and-pitfalls/article/30471/

Ptacek T., Newsham T., “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection”, 1998, http://insecure.org/stf/secnet_ids/secnet_ids.html

http://shweps.free.fr/wiki/wakka.php?wiki=SnorTer

http://sourcefire.com

http://www.it.redhat.com

http://www.securixlive.com/barnyard2

http://sguil.sourceforge.net

http://base.secureideas.net

http://www.ntop.org/news.php

http://www.aptivate.org/Projects.BMOTools.pmGraph.html

http://www.780inc.com/snortnotify

http://www.emergingthreats.net

http://www.snort.org

http://www.skynet-solutions.net/easyids

http://www.endian.com/it

http://www.vyatta.com

http://snorby.org

http://www.untangle.com

http://www.bro-ids.org

http://www.prowling.nu

http://www.openinfosecfoundation.org

http://www.ossec.net

http://www.cs.tut.fi/~rammer/aide.html

http://www.la-samhna.de/samhain