1. IDS/ISP

Securitate stratificata este cheia pentru protejarea oricarei rețea de orice dimensiune, iar pentru cele mai multe companii, înseamnă implementarea ambelor sisteme de detectare a intruziunilor (IDS) și sisteme de prevenire a intruziunilor (IPS). Când vine vorba de IPS și IDS - ambele sunt necesare pentru protecție maximă împotriva traficului de produse malitioase. De fapt, furnizori sunt din ce în ce orientati spre combinarea celor două tehnologii într-un singur pachet.

Un dispozitiv IDS este pasiv, pachetele de date traversează rețeaua printr-un port de monitorizare, si în cazul în care se detectează ceva suspect IDS semnaleaza alarma. Un IDS poate detecta mai multe tipuri de trafic malitios, care ar aluneca de un firewall tipic, inclusiv atacuri de rețea împotriva serviciilor, bazate pe date de atacuri asupra aplicațiilor, atacuri bazate pe gazdă, cum ar fi datele de conectare neautorizate, si malware cum ar fi viruși, cai troieni, viermi.. Cele mai multe produse IDS folosesc mai multe metode pentru a detecta amenințări, de obicei, detectare bazată pe semnături, detectare a anomaliilor desfasurate, și analiza de protocol dinamică. Motorul IDS înregistrează incidente care sunt înregistrate de senzorii IDS într-o bază de date și generează alerte pe care le trimite la administratorul de rețea. Deoarece IDS oferă vizibilitate adânca în activitatea de rețea, acesta poate fi de asemenea utilizata pentru a ajuta la problemele punctuale cu politica de securitate a organizației, amenințările existente de documente. Plângerea principal cu IDS este numărul de alarme false.

Avantajul IPS

Un IPS are toate caracteristicile unui IDS bun, si poate opri traficul in caz de detectare a codului malitios. Spre deosebire de un IDS, IPS sta in linie cu fluxurile de trafic pe rețea si in caz de detectare a virusilor se poate opri atacul de reziliere a conexiunii la rețea, prin blocarea accesului la țintă de la contul de utilizator, adresa IP sau alt atribut asociat cu acel atacator, sau prin blocarea de orice acces la gazdă țintă, servicii , sau aplicație. În plus, un SPI poate răspunde la o amenințare detectată în alte două moduri. Se poate reconfigura alte controale de securitate, cum ar fi un firewall sau router, pentru a bloca un atac. Unele dispozitive IPS pot aplica patch-uri, chiar dacă gazda are anumite vulnerabilități. În plus, unele IPS pot elimina conținutul malware, de exemplu ștergerea unui atașament infectat de la un e-mail înainte de a transmite e-mail a utilizatorului.

De două ori protecție

Deoarece dispozitivele IDS și IPS stau în locuri diferite pe rețea, ele pot - și ar trebui - să fie utilizate concomitent. Un produs IPS instalat în perimetrul rețelei va ajuta la stoparea atacurilor Zero Day, cum ar fi viermi și viruși, chiar si cele mai noi amenințări pot fi blocate cu reglare riguroasă. Un produs IDS instalat în interiorul firewall-ul va monitoriza activitatea internă, paza împotriva amenințării din interior mereu este prezent, și să dea o mai mare vizibilitate în evenimentele de securitate, trecute și prezente. Alegerea unui produs care oferă ambele tehnologii pot fi abordarea cea mai eficientă și eficace.

Diferențierea IDS și IPS

Un IPS nu este la fel ca un IDS. Cu toate acestea, tehnologia pe care o utilizați pentru a detecta problemele de securitate într-o IDS este foarte similar cu tehnologia pe care o utilizați pentru a preveni problemele de securitate într-o IPS.

Este important să începem cu înțelegerea că IDS și IPS sunt instrumente foarte, foarte diferite. Chiar dacă acestea au o bază comună, acestea se încadrează în rețeaua în locuri diferite, au functii diferite, și de a rezolva diferite probleme.

Un IPS este cel mai bine în comparație cu un firewall. Într-un firewall tipic întreprindere, veți avea un număr de reguli: poate o sută, poate o mie. Cele mai multe dintre aceste reguli sunt reguli "pass": "permite trafic prin intermediul." Astfel, firewall-ul devine un pachet de pe sârmă și începe prin normele sale, în căutarea pentru o regulă care spune că "permite acest pachet prin." Dacă se ajunge la sfârșitul listei și nu există nici o regulă spune "permite acest pachet prin," atunci exista un "nega" regula final: ". Drop totul altceva" Astfel, în lipsa unui motiv pentru a trece de trafic firewall scade.

Și IPS este așa, dar pe dos: are reguli, poate sute, poate mii. Cele mai multe dintre aceste reguli sunt reguli "neagă": "bloca această problemă de securitate cunoscut." Când un pachet apare la IPS, IPS arata prin lista de regula de sus în jos, în căutarea pentru un motiv să renunțe la pachet. La sfârșitul listei, deși, este un implicit "trecere" regula: "permit acest pachet prin." Astfel, în lipsa unui motiv să renunțe trafic, IPS acesta trece prin.

Firewall-uri și IPS sunt dispozitive de control. Ei stau în linie între două rețele și controla traficul trece prin ele. Acest lucru înseamnă că IPS este în partea politica a casei de securitate. Se va pune în aplicare sau a pune în aplicare o politică special cu privire la ceea ce traficul nu este permis prin intermediul.

Afinitatea evident de firewall-uri și IPSes din punct de vedere topologic ne-a dus la lumea de UTM, în cazul în care un IPS este încorporat în firewall. UMTS să aveți ambele servicii de securitate (blocarea amenințărilor de securitate, care să permită traficul de bine cunoscut), într-un singur dispozitiv. Vom vorbi despre cea mai bună în compresie de IPS si firewall, firewall UTM (Unified Threat Management) mai târziu.

Principalul motiv de a avea un IPS este de a bloca atacurile cunoscute într-o rețea. Atunci când există o fereastră de timp între când un exploit este anunțată și aveți timp sau posibilitatea de a patch sistemele, un IPS este un mod excelent de a bloca rapid atacurile cunoscute, în special cele cu ajutorul unui instrument comun sau bine-cunoscut exploit.

Desigur, IPSes poate oferi alte servicii. Ca furnizori de produse căuta să se diferențieze, IPSes au devenit instrumente de limitare rata (care este, de asemenea, de ajutor în Denial de atenuare Service), instrumente de aplicare a politicii, datele scurgeri de instrumente de protecție, și comportament instrumente de detectare anomalie. În fiecare caz, totuși, funcția cheie a SPI este o funcție de control.

Cum lucreaza IDS

Dacă un IPS este un instrument de control, atunci un IDS este un instrument vizibilitate. Sisteme de detectare a intruziunilor sta într-o parte a rețelei, de monitorizare a traficului de la mai multe puncte diferite, și să ofere vizibilitate în postura de securitate a rețelei. O analogie

bună este de a compara un IDS cu un analizor de protocol. Un analizor de protocol este un instrument care un inginer de rețea utilizează să se uite adânc în rețea și să vedem ce se întâmplă, în detaliu, uneori chinuitor. Un IDS este un "analizor de protocol" pentru inginer securitate. IDS se uită adânc în rețea și vede ce se întâmplă din punct de vedere al securității.

În mâinile unui analist de securitate, IDS devine o fereastră în rețea. Informațiile furnizate de IDS va contribui la securitatea și echipele de management de rețea descoperi, ca un start:

Încălcări ale politicii de securitate, cum ar fi sistemele sau utilizatorii care execută aplicații împotriva politicii

Infectii, cum ar fi virusi sau troieni care au control parțial sau complet de sisteme interne, folosindu-le să se răspândească infecția și ataca alte sisteme

Scurgere de informații, cum ar fi rularea spyware și furnizori de bustean cheie, precum și scurgerea de informații accidentală de către utilizatori valabile

Erori de configurare, cum ar fi aplicații sau sisteme cu setările de securitate incorecte sau de performanță, uciderea greșelile rețea, precum firewall-uri greșelilor în setul de reguli nu se potrivește cu politica

Clientii neautorizate și servere, inclusiv aplicații server de rețea în pericol, cum ar fi DHCP sau servicii DNS, împreună cu aplicațiile neautorizate, cum ar fi instrumente de scanare în rețea sau desktop la distanță negarantate.

Această vizibilitate crescută în postura de securitate a rețelei este ceea ce caracterizează un IDS, și care diferențiază funcția vizibilitatea unui IDS din funcția de control al unui SPI.

Desigur, din moment ce ambele IDS și IPS au cuvântul "intruziune", ca la începutul acronim lor, ați putea fi întrebați de ce nu am menționat "intruziune", ca parte a funcției fie IDS și IPS. Parțial că este, deoarece cuvântul "intruziune" este atât de vagă încât e dificil să știi ce o intruziune, este. Desigur, cineva încearcă în mod activ să pătrundă într-o rețea este un intrus. Dar este un calculator infectat, o "intruziune?" Este cineva care desfășoară recunoaștere rețea un intrus ... sau pur și simplu cineva a face cercetare? Și dacă un actor malware este în rețea în mod legitim - de exemplu, un angajat rogue - sunt legitime și nelegitime acțiuni intruziuni sau altceva?

Mai important motiv pentru care a plecat "intruziune" din descrierea atât pentru IDS și IPS este că ele nu sunt foarte bun la prinderea intruși adevărat. Un IPS va bloca atacurile cunoscute foarte bine, dar cele mai multe dintre aceste atacuri sunt fie recunoaștere rețea sau scanari automate, căutarea sau alte sisteme pentru a infecta - greu "intruziuni" în sensul clasic al cuvântului. Cel mai bun sistem de prevenire a intruziunilor, în acest caz, este firewall, care nu lasa trafic necorespunzătoare în rețea, în primul rând.

Este greșită a cuvântului "intruziune", cu referire la aceste tehnologii vizibilitate și control care a provocat o astfel de confuzie și așteptările greșite în personalul de la întreprinderile care au desfășurate fie IDS și IPS.

Da, un IDS va detecta intruziuni adevărat. Da, un IPS va bloca intruziuni adevărat. Dar aceste produse nu mai mult de atât - ele oferă un control mai mare și o mai mare vizibilitate, care este în cazul în care valoarea lor reală.

Ce despre IPSes UTM?

Combinația dintre un IPS și un firewall într-un singur sistem, cu un singur sistem de management, este atractiv. Din păcate, sisteme de management amenințarea cea mai unificate (UMTS) sunt proiectate pentru SMB implementare, un mediu în care simplitatea sistemului de management este una dintre cerințele de proiectare cele mai critice. Combinând managementul IPS cu managementul firewall-ul este o sarcină foarte dificilă. De fapt, nici un furnizor de produse a reușit să fuzioneze sistemul de management al firewall-ul web-based, cu un bun instrument de management IPS.

Nu trebuie să presupunem că un IPS încorporate într-un firewall UTM va oferi aceleași tipuri de controale și de protecție ca IPS stătătoare.

Acest lucru nu înseamnă că nu există firewall UTM mari cu IPSes încorporate, aceasta înseamnă doar că sistemele de management pentru partea IPS din aceste produse sunt destul de diferite (și de multe ori separat) din părțile firewall.

În cazul în care vânzătorul dumneavoastră potențial firewall UTM are incluse IPS și funcționalitatea firewall pe toate într-o interfață omogenă singur web, sunteți în căutarea la un produs care IPS este obtinerea instrumente de management de mâna a doua. Acest lucru poate fi bine în medii în care sunteți interesat doar de control, cum ar fi la sucursale sau în cazul în care doar un mic set de sisteme sunt protejate.

Pentru a gasi un IPS enterprise-class, combinate cu un firewall UTM, uita-te pentru produsele care sunt, în mod paradoxal, mai puțin integrate: un IPS independente și firewall independent combinate în același șasiu, de exemplu.

- Joel SNYDER

Cerințe preliminare

Pentru a obține cele mai multe din articol, ar trebui să aveți cunoștințe de bază de Snort, Linux și un sistem Linux de lucru pe care le puteți practica comenzile cuprinse în acest articol. De asemenea, ar trebui să aveți unele cunoștințe de rețea, cum ar fi TCP / IP, iptables, etc

Ce este IPS (Intrusion Prevention System)?

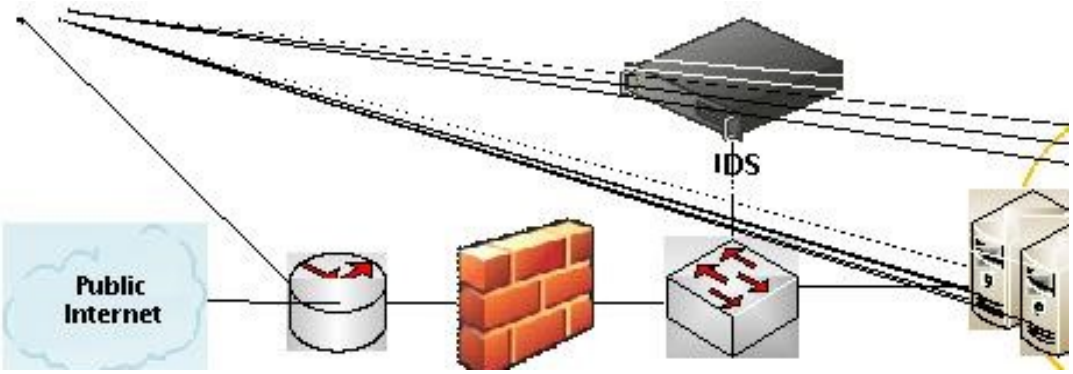
Intrusion Detection System (IDS) este un dispozitiv care monitorizeaza pachetele din rețea. IDS raportează comportamente de atac, bazate pe normele de securitate și semnăturile aplicate pe dispozitiv. Cu toate acestea IDS are anumite dezavantaje, cum ar fi de mare rata de rezultate fals pozitive, în imposibilitatea de a opri Denial of Service (DoS) atac și de intruziuni din protocoalele UDP.

Intrusion Prevention System (IPS), pe de altă parte, are nu numai capacitatea de IDS, dar, de asemenea, poate scădea pachete malware și sesiuni de strânsă legătură, în scopul de a opri atacurile viitoare. IPS-ar putea realiza în timp real Interzicerea de pârghie desfășurarea în linie în topologia rețelei. Acesta analizează tot traficul de rețea care trece prin sistem si ia măsuri pentru pachete suspecte imediat.

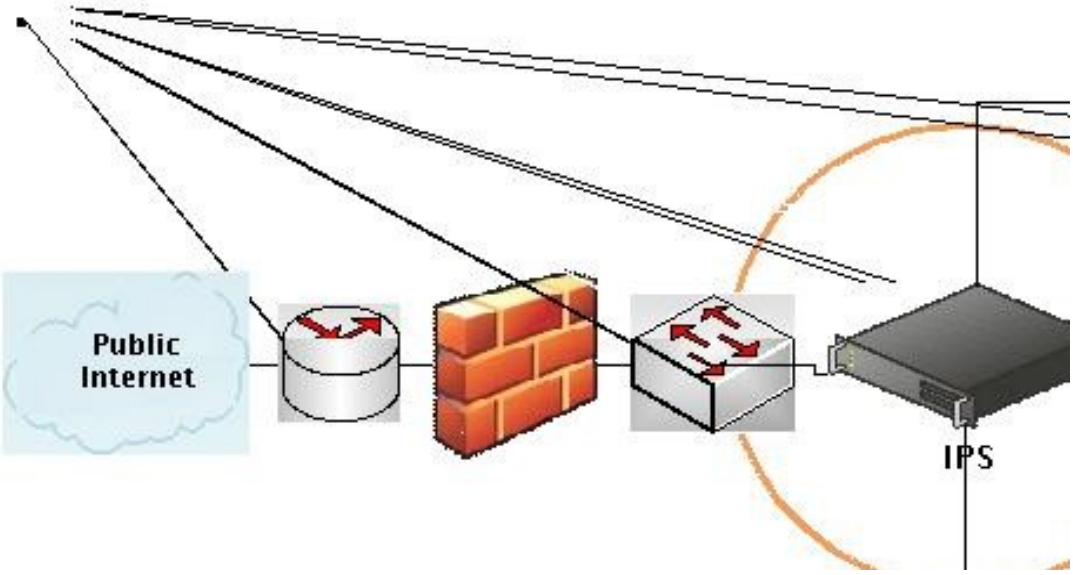
Metoda de implementare de rețea de IDS și IPS

Având în vedere diferențele dintre IDS și IPS, desfășurarea acestor două sisteme este proiectat în funcție de caracteristicile lor.

IDS, de obicei, joacă rolul de monitorizare. IDS trebuie să fie capabil de a mirosi de trafic care interesează IDS în timp ce nu compromite transfer rețeaua globală. Următoarea figură ilustrează modul tipic de implementarea unui dispozitiv IDS la o rețea.



Pe de altă parte, IPS trebuie să ia măsuri imediate pentru pachete suspecte.Implementare trebuie să activezi IPS sa se uite la fiecare pachet și să se ocupe cu pachete suspecte în timp real. Face de obicei tot traficul trece printr-IPS ar putea realiza cerința de desfășurare. Aceasta este așa-numita implementare în linie.



Snort pe Linux pentru a acționa ca un IPS

În general Snort este un software sofisticat IDS, care monitorizează traficul de rețea pentru a detecta și analiza comportamentul ataca în conformitate cu reguli predefinite. Snort trimite alerte la administratorul de rețea în timp ce sunt detectate atacuri sau activități de rețea anormale. Totuși, funcția de sistem este limitat la monitorizarea pasiv petrecere. Acțiunea de protecție trebuie să se bazeze pe răspunsul administratorului.

Deși Snort este frecvent utilizat ca un IDS, acesta are unele capabilități îmbunătățite ar putea face într-un SPI. Acest articol ilustrează în special modul în care Snort poate acționa ca un dispozitiv de IPS.

Prin utilizarea următoarele setări, Snort devine o IPS să ia măsuri imediate pentru Trafic suspecte.

- Metoda de instalare de rețea

- În-linie de implementare: implementarea inline permite Snort să se uite la fiecare pachet și să se ocupe cu pachete suspecte direct

- Configurație avansată rețea
- iptables
- Snort modul de configurare
- Modul in-line
- Snort de Acțiuni statului
- picătură / respinge / sdrop

IDS/IPS (Windows, Linux etc.)

Intrusion Detection System (IDS) şi Intrusion Prevention System(IPS o varianta mai specială a IDS) – un dispozitiv sau o aplicaţie folosit(ă) pentru a inspecta întregul trafic dintr-o reţea şi de a trimite mesaje de alertă utilizatorului sau administratorului sistemului cu privire la încercări neautorizate de acces. Principalele metode de monitorizare sunt cele bazate pe semnături şi cele bazate pe anomalii. Funcţie de metodele folosite IDS-ul poate rămâne la stadiul de a alerta utilizatori sau poate fi programat să blocheze automat traficul sau chiar programat să răspundă într-un anumit fel.

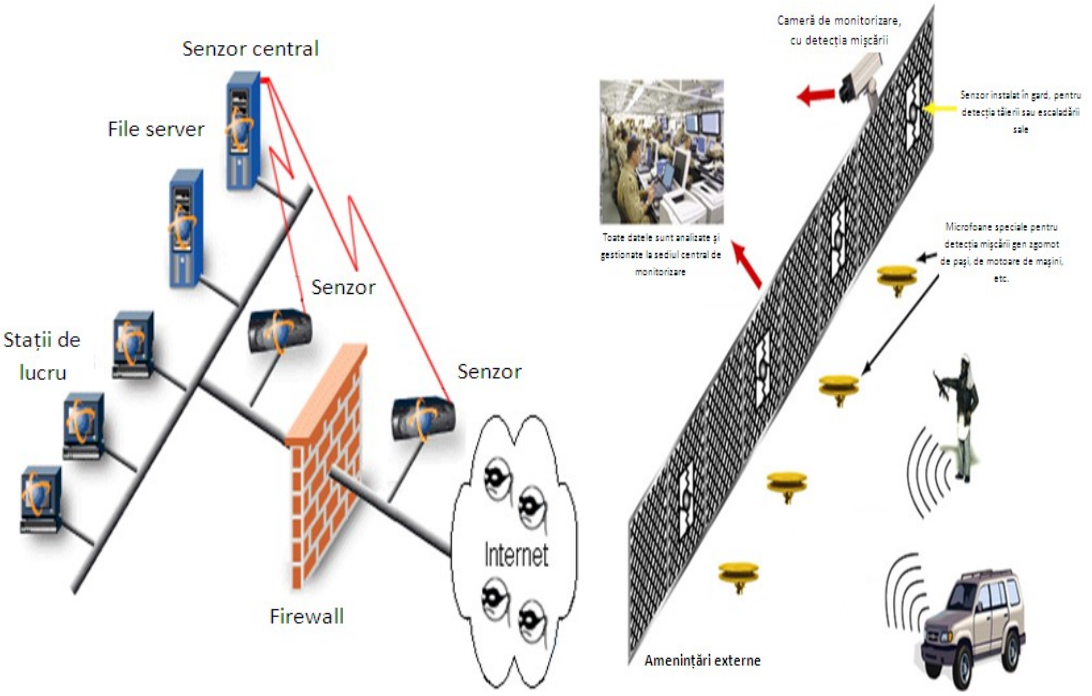


Fig. 1.1 IDS la nivel software şi hardware (în patea dreptă se observă avantajele folosirii sistmelor de tip IPS pentru protecţia unor instituţii speciale cum ar fi baze militare, închisori, etc.)

Intrusion Detection System (IDS)

Este din ce in ce mai important, pentru personalul ce asigura securitatea retelei sa apere resursele companiei, nu doar pasiv, prin utilizarea de firewall-uri, retele virtuale private (VPN), tehnici de criptare sau orice alte "trucuri pe care le au in maneca", dar si prin implementarea unor dispozitive ce supravegheaza proactiv reteaua. Aceasta este momentul in care intra in actiune Intrusion Detection System (IDS) – sistemele de detectare a intruziunii.

In general, intruziune este atunci cand cineva incearca sa patrunda abuziv sau exploateaza o slabiciune a sistemului dumneavoastra pentru a avea acces neautorizat la o resursa. Mai precis, politica de securitate a companiei dumneavoastra defineste ceea ce constituie o intruziune.

Intrusion Detection System este utilizat pentru a detecta comportamente malitioase care incearca sa se furisese in retea si sa compromita securitatea unui sistem informatic. Acestea includ atacurile asupra retelelor ce gazduiesc servicii si aplicatii vulnerabile, atacurile asupra unui anumit sistem/host, cum ar fi conectari neautorizate si acces la fisiere sensibile, precum si malware (virusi, cai troieni si viermi). Odata intrat in retea/sistem, virusul poate dormita saptamani intregi inainte de a-si indeplini misiunea. Pentru a fi eficient IDS-ul trebuie sa-si actualizeze baza de date cu semnaturi, dar pentru ca cracker-ii sunt intr-o continua cautare, compania nu este niciodata complet imuna.

Trebuie mentionat ca sunt doua tipuri de intrusi: interni si externi.

Desi majoritatea tentativelor de intruziune, apar din interior organizatiei sau sunt facute de catre intrusi interni, cele mai frecvente masuri de securitate sunt implementate pentru a proteja interiorul retelei de lumea exterioara. Intrusii externi sunt deseori denumiti crackers.

Este clara necesitatea unui mecanism care sa poate detecta continuu ambele tipuri de intruziuni. IDS-urile sunt solutii eficiente pentru ambele tipuri de atacuri. Aceste sisteme ruleaza permanent in retea, notificand personalul responsabil cu securitatea retelei, atunci cand detecteaza o tentativa pe care o considera suspecta. IDS-ul are doua componente principale si anume: senzori IDS si management IDS.

Senzorii IDS pot fi atat software cat si hardware si sunt utilizati pentru a colecta si analiza traficul din retea. Acesti senzori sunt disponibili in doua variante, pentru retea si pentru calculator (host).

1. Senzorul IDS pentru host/gazda este o aplicatie agent care ruleaza pe un server cu un minim de incarcare pentru a monitorizara sistemul de operare.

2. Senzor IDS pentru retea poate fi incorporat intr-un dispozitiv de retea, poate fi dispozitiv independent sau poate fi un modul de monitorizare a traficului din retea.

Componenta de management IDS, asigura colectarea avertizarilor si realizeaza configurarea si implementarea serviciilor pe senzori IDS din retea.

In lista de instrumente ce supravegheaza proactiv traficul din retea se regaseste atat NBA (Network Behavior Analysis – analizeaza comportamentul intr-o retea), cat si IPS (Intrusion-prevention systems – sistem de prevenire a intruziunii).

Pentru inceput sa facem o comparatie intre cele trei instrumente IDS, NBA si IPS

NBA este un instrument ce are capacitatea de a identifica anumite modele de trafic care nu sunt considerate normale in traficul de zi cu zi din retea. Pur si simplu, aceasta este o incercare a industriei din domeniu de a identifica nereguli in retea dincolo de pragul simplu al setarilor pentru trafic excesiv. Unul dintre cele mai raspandite modele de trafic anormal ce reprezinta o amenintare la adresa securitatii retelei este modelul cunoscut ca atac DdoS (Distributed Denial of Service). Acest tip de atac este o mare amenintare la adresa securitatii furnizorilor de servicii de Internet precum si pentru infrastructurile mari de retea. Distributed Denial of Service (DDoS) – acest atac foloseste atacuri DoS pornite de mai multe host-uri. Prima

data atacatorul compromite host-urile vulnerabile, folosind diferite instrumente si tehnici, apoi urmeaza atacul real DDoS pe o anumita tinta folosind intreg grupul de host-uri compromise.

IPS-urile sunt dispozitive instalate in retea destinate detectarii si blocarii unei mari varietati de atacuri. Unele studii din domeniul cercetarii arata ca aceste IPS-uri sunt folosite pentru detectarea intruziunii si pentru monitorizarea pasiva a traficului.

Cu alte cuvinte orice echipament IPS poate fi folosit ca si echipament IDS.

Echipamentele IPS in general lucreaza impreuna cu sistemele NBA si IDS. Cand este detectat un atac de catre IDS sau NBA, sistemul IPS poate sterge pachetele respective, permitand totusi ca restul traficului sa treaca.

Un sistem NBA poate fi considerat un pic mai putin proactiv decat cel IDS si, in general, se axeaza pe traficul intern. Poate fi de asemenea implementat si peste o anumita conexiune si sa inspecteze pachete exact ca un IDS. Spuneam mai putin proactiv deoarece NBA incearca sa recunoasca problemele care sunt deja in curs de desfasurare (de exemplu, scanarea retelei sau atacurilor DDOS, care sunt in curs de desfasurare). Incearca sa identifice amenintarile ce nu au fost identificate de IDS sau de software-ul antivirus. Deoarece sistemul NBA este orientat spre identificarea simptomelor sau a comportamentelor actualizarea motorului de analiza se face mai rar comparativ cu sistemele IDS.

IDS Software:

Snort IDS (under binaries);

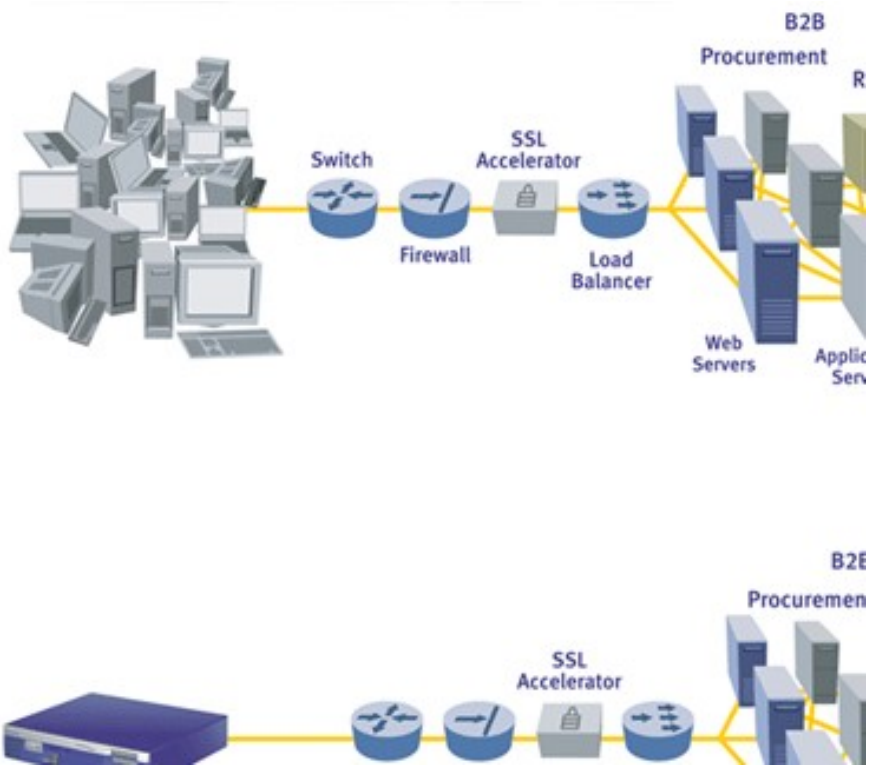
WinPcap (for packet capturing);

LiTe Sniffer (network traffic monitor);

IDScenter (Snort front end)

IDS/IPS

IDS - Sisteme de detectie ale intruziunilor



Un sistem de detectie al intruziunilor - IDS (Intrusion Detection System) reprezinta un echipament (sau o aplicatie) care monitorizeaza activitatile retelei si/sau sistemului cautand activitati malitioase sau violari ale politicilor.

Detectia intruziunilor este procesul de monitorizare a evenimentelor care au loc intr-un sistem sau o retea de calculatoare si analiza lor pentru a detecta posibile incidente care sunt violari sau amenitari iminente de violare a politicilor de securitate, a politicilor de utilizare acceptate sau a practicilor standard de securitate. Prevenirea intruziunilor este procesul prin care se desfasoara detectia intruziunilor si incercarea de inlaturare a posibilelor incidente detectate. Sistemele de detectie si prevenire ale intruziunilor - IDPS (Intrusion Detection-Prevention Systems) au ca scop principal identificarea posibilelor

incidente, inregistrarea informatiilor despre ele, incercarea de inlaturare a incidentelor si raportarea catre administratorii de securitate. In plus, organizatiile pot folosi IDPS-urile si pentru alte scopuri: identificarea problemelor legate de politicile de securitate, documentarea amenintarilor existente si descurajarea indivizilor in a incalca politicile de securitate.

1.2. Tipuri de IDS-uri

1.2.1. Network-based si host-based

Sistem de detectie al intruziunilor de tip network-based

Intr-un sistem de detectie al intruziunilor de tip network-based - Network-based Intrusion Detection System (NIDS) - senzorii sunt localizati in puncte critice ale retelei care este monitorizata, de cele mai multe ori la marginea retelei sau in DMZ (demilitarized zone). Senzorii capteaza tot traficul din retea si analizeaza continutul fiecarui pachet cautand urme de trafic malitios.
Un NIDS reprezinta o platforma independenta care identifica intruziunile prin examinarea traficului din retea si monitorizeaza mai multe statii. NIDS-urile pot vizualiza traficul din retea prin conectarea lor la un hub sau la un echipament switch configurat cu port mirroring.

Sistem de detectie al intruziunilor de tip host-based

Intr-un sistem de detectie al intruziunilor de tip host-based - Host-based Intrusion Detection System (HIDS) - senzorul consta, de obicei, intr-un agent software care monitorizeaza toata activitatea ce se desfasoara pe statia pe care este instalat, incluzand aici sistemul de fisiere, kernel-ul si chiar aplicatii in unele cazuri.
Un HIDS reprezinta un agent care ruleaza local pe statie si care identifica intruziunile analizand activitatile sistemului, aplicatiile, modificarile sistemului de fisiere si alte activitati ale statiei.

1.2.2. Sisteme pasive si sisteme active

Intr-un sistem pasiv, senzorul sistemului de detectie al intruziunilor (IDS) detecteaza o potentiala bresa de securitate, inregistreaza informatia si alerteaza administratorul folosind o metoda specifica (mesaje in consola, alerte, etc.). Intr-un sistem reactiv, cunoscut sub denumirea de Sistem de Prevenire al Intruziunilor - Intrusion Prevention System (IPS), IPS-ul raspunde activitatii suspicioase prin terminarea conexiunii sau prin reprogramarea firewall-ului de a bloca traficul de retea provenind de la sursa malitioasa suspectata. Aceasta se poate intampla automat sau la comanda unui operator.
Desi ambele se refera la securitatea unei retele, si uneori notiunile pot fi confundate, un IDS difera de un firewall deoarece firewall-ul urmareste semne ale intruziunilor pentru a le impiedica sa se intample. Un IDS evalueaza o posibila intruziune o data ce a avut loc si semnaleaza o alerta. Un sistem care termina conexiunea ca metoda de raspuns este un IPS si poate fi privit uneori ca o forma de firewall la nivel de aplicatie.
Termenul IDPS - Sistem de Detectie si Prevenire al intruziunilor se refera la sisteme de securitate hibride care atat detecteaza intruziunile cat si incearca sa le previna.

1.2.3. IDS-uri bazate pe anomalii si IDS-uri bazate pe semnaturi

Sistemele de detectie ale intruziunilor folosesc cel putin una dintre cele doua tehnici de detectie: anomalii statice si/sau semnaturi.
IDS bazat pe anomalii statice - Un astfel de IDS stabileste o valoare initiala de performanta bazata pe evaluari ale traficului normal din retea. Dupa efectuarea acestui pas initial, IDS-ul va raporta traficul curent din retea la valoarea initiala stabilita pentru a stabili daca se incadreaza in limitele normale. Daca traficul din retea depaseste limitele normale va fi generata o alarma. **IDS bazat pe semnaturi** - Un astfel de IDS examineaza traficul din retea cautand modele

de atac preconfigurate si predeterminate cunoscute sub numele de semnaturi. Multe atacuri astazi au semnaturi diferite. Pentru a putea face fata amenintarilor o colectie de astfel de semnaturi trebuie actualizata in permanenta.

1.3. Limitari si tehnici de evitare ale IDS-urilor

Capabilitatile unui IDS pot fi limitate de:

- **Zgomot** - Zgomotul poate afecta in mod sever eficacitatea unui IDS. Pachete gresite, generate de defectiuni ale software-urilor, date DNS alterate si pachete locale care au scapat pot crea o rata foarte crescuta de alarme false.
- **Prea putine atacuri** - Nu este neobisnuit ca numarul de atacuri reale sa fie mult sub rata de alarme false. Atacurile reale pot fi atat de mult sub rata de alarme false incat sunt de obicei ignorate de catre IDS.
- **Actualizarea semnaturilor** - Multe atacuri sunt indreptate catre versiuni specifice de software. Pentru a putea face fata amenintarilor este nevoie de o colectie de semnaturi actualizata in mod constant. O colectie de semnaturi care nu este actualizata poate lasa IDS-ul vulnerabil la strategii noi de atac.

Tehnici de evitare a IDS-urilor:

- fragmentarea si trimiterea de pachete mici - o tehnica de baza care presupune fragmentarea informatiei in mai multe pachete mai mici pentru a face imposibila reconstruirea sesiunii la IDS
- fragmente care se suprapun - tehnica ce presupune crearea de pachete cu numere ale secventei TCP care se suprapun incercand astfel sa se exploateze faptul ca sistemele de operare trateaza diferit aceasta suprapunere: unele vor lua in considerare datele mai noi, altele datele mai vechi
- violari de protocol - violari deliberate ale protocoalelor TCP sau IP in asa fel incat statia tinta sa manevreze diferit pachetele decat IDS-ul
- inserarea de trafic in IDS - un atacator poate trimite pachete care sa ajunga doar la IDS nu si la statia tinta rezultand astfel o serie de alarme false
- atacuri de tip DoS - un atacator poate evita un IDS prin efectuarea unui atac de tip DoS asupra lui care sa ii consume resursele sau care sa genereze un numar foarte mare de alarme false reusind astfel sa ascunda atacul real

1.4.Exemple de IDS-uri

Mai jos sunt prezentate o serie de Sisteme de Detectie ale Intruziunilor :

- **OSSEC** - http://www.ossec.net/
- **Prelude Hybrid IDS** - http://www.prelude-technologies.com/en/welcome/index.html
- **Snort** - http://www.snort.org/
- **Suricata** -https://redmine.openinfosecfoundation.org/projects/show/suricata

Daca doriti mai multe informatii despre Sistemele de Detectie ale Intruziunilor puteti consulta una dintre adresele de mai jos:

- Intrusion Detection Systems de la Open Directory Project
- Guide to Intrusion Detection and Prevention Systems(IDPS) NIST SP 800-94, 02/2007
- Intrusion Detection/Prevention Systems classification tree

2. IPS - Sisteme de prevenire a intruziunilor

2.1. Introducere

Un Sistem de Prevenire al Intruziunilor - Intrusion Prevention System (IPS) - reprezinta un echipament de securitate al retelei care monitorizeaza activitatile retelei si/sau sistemelor si

poate reactiona, in timp real, sa blocheze sau sa previna unele activitati malitioase. Tehnologia prevenirii intruziunilor este vazuta de catre unii ca o extensie a tehnologiei de detectie a intruziunilor, deoarece un IPS trebuie sa fie in acelasi timp si un foarte bun IDS pentru a asigura o rata scazuta de alarme false.
Un IPS este, in mod obisnuit, conceput pentru a opera complet invizibil in retea. Produsele IPS nu au de obicei o adresa IP din reteaua protejata dar pot raspunde in mod direct oricarui tip de trafic prin diverse metode (terminarea conexiunilor, renuntarea la pachete, generarea de alerte, etc.)
Desi unele IPS-uri au abilitatea de a implementa reguli de firewall aceasta este de obicei o functie aditionala si nu una din functiile de baza ale produsului. Mai mult, tehnologia IPS ofera o mai buna monitorizare a operatiilor unei retele furnizand informatii despre statiile active, incercarile de autentificare esuate, continut necorespunzator si alte functii ale nivelelor retea si aplicatie.

2.2. Diferente fata de IDS-uri

IPS-urile au unele avantaje fata de IDS-uri. Unul dintre acestea se refera la faptul ca IPS-urile sunt proiectate sa fie implementate in-line astfel incat tot traficul sa treaca prin ele si sa poata preveni atacurile in timp real. In plus, multe dintre solutiile IPS au capabilitatea sa decodifice protocoalele de nivel aplicatie (HTTP, FTP, SMTP) oferind astfel o mai buna monitorizare. Totusi atunci cand se doreste implementarea unui IPS de tip network-based trebuie sa se ia in considerare faptul ca daca prin respectivul segment de retea circula trafic criptat majoritatea produselor nu pot sa inspecteze astfel de trafic.
Un alt avantaj major ar fi faptul ca unele dintre IPS-uri au posibilitatea de a corecta unele dintre metodele de evitare ale IDS-urilor(atacuri de tip DoS, inserarea de trafic).

2.3. Tipuri de IPS-uri

2.3.1. Host-based

Un Sistem de Prevenire al Intruziunilor este de tip host-based (HIPS) atunci cand aplicatia de prevenire a intruziunilor se afla pe adresa IP specifica sistemului protejat, de obicei o singura statie. HIPS complementeaza metodele antivirus traditionale bazate pe semnaturi deoarece nu necesita o actualizare continua pentru a putea raspunde atacurilor. Deoarece codul daunator trebuie sa modifice sistemul sau alte componente software care se afla pe masina in cauza un HIPS va observa aceste modificari si va incerca sa previna aceasta actiune sau sa anunte utilizatorul pentru permisiune.
Dezavantajul major al unui astfel de produs consta in folosirea extensiva a resurselor statiei pe care se afla.

2.3.2. Network-based

Un Sistem de Prevenire al Intruziunilor este de tip network-based (NIPS) atunci cand aplicatia/echipamentul de prevenire al intruziunilor se afla la o alta adresa IP decat statia pe care o monitorizeaza. NIPS sunt platforme hardware/software care analizeaza, detecteaza si raporteaza evenimente legate de securitatea unei retele/segment de retea de calculatoare.

2.3.3. Diferente intre IPS-uri de tip host-based si network-based

- HIPS-urile pot lucra atat cu date criptate cat si cu date necriptate deoarece analiza se face dupa ce datele au fost decriptate de catre statie
- NIPS-urile nu folosesc din memoria si procesorul statiilor care le protejeaza ci dispun de propria memorie si propriul procesor
- NIPS-urile se afla in punctele critice ale retelei si tot traficul depinde de buna lor functionare, fapt ce poate constitui un dezavantaj atunci cand echipamentul este nefunctional

- NIPS-urile pot detecta evenimente distribuite in retea (evenimente de prioritate joasa dar care afecteaza mai multe statii din retea) si pot reactiona in timp ce HIPS-urile au la dispozitie doar datele de pe masina pe care functioneaza pentru a putea lua o decizie

Mai jos sunt prezentate o serie de Sisteme de Prevenire ale Intruziunilor :

- **Snort** -http://www.snort.org/
- **Suricata**-https://redmine.openinfosecfoundation.org/projects/show/suricata
- **Winpooch** -http://sourceforge.net/projects/winpooch/

IDS/IPS

IDS (IntrusionDetectionSystem)

Un sistem de detectare a intruziunilor (IDS) monitorizează traficul din rețea pentru activități suspecte și alerteaza sistemul sau administratorul de rețea. În unele cazuri, IDS pot răspunde, de asemenea, la traficul anormal sau rău intenționat prin luarea de măsuri, cum ar fi blocarea de utilizator sau adresa IP a sursei ce a accesat rețeaua.

IDS vin au o mare varietate de forma și se apropie de obiectivul de a detecta traficul suspect în moduri diferite. Există IDS bazată pe retea (NIDS) și IDS bazata pe hostul sistemului (HIDS). Există IDS care detecteaza dupa căutarea de semnături specifice cunoscute la fel ca si software-ul antivirus și există IDS care detecteaza intruziunile bazandu-se pe compararea tiparele de trafic de o bază inițială și caută anomalii. Există IDS care monitorizează pur și simplu și de alertă și sunt IDS care efectuează o acțiune sau măsuri ca răspuns la o amenințare detectată.

NIDS

Network Intrusion Detection Systems sunt plasate într-un punct(e) strategice pentru a monitoriza traficul de intrarea si iesire de la toate dispozitivele din rețea. În mod ideal, ar scana tot traficul de intrare și de ieșire, însă acest lucru ar putea crea un blocaj care ar putea afecta viteza de ansamblu a rețelei.

HIDS

Host Intrusion Detection Systems ruleaza pe gazde individuale sau dispozitive din rețea. HIDS monitorizează pachetele de intrare și de ieșire din aparat și va alerta utilizatorul sau administratorul in caz ca o activitate suspecta este detectată

Bazat pe semnatura

Un IDS bazat pe semnătura va monitoriza pachetele de rețea și le va compara cu o baza de date de semnături sau cu niste atribute de amenințări malware cunoscute. Acest lucru este similar cu modul in care software-ul antivirus detecteaza malware. Problema este in cazul in care amenintarea este insa ea nu e in baza de date, atunci ea nu va fi detectata.

Bazat pe anomalie

Un IDS care se bazează anomalie va monitoriza traficul în rețea și il va compara cu o bază stabilita. Linia de bază va identifica ceea ce este "normal" pentru rețea, adica: ce fel de lățime de bandă este utilizat în general, ce protocoale sunt folosite, ce porturi si dispozitive sunt conectare în general, iar atunci este detectat de trafic anormal se va alerta administratorul sau utilizatorul.

IDS pasive

Un IDS pasiv pur și simplu detectează și alerteaza. Când este detectat trafic suspect sau rău intenționat o alertă este generata și trimisa administratorului sau utilizatorului, care trebuie sa ia măsuri pentru a bloca activitatea sau să răspundă într-un fel.

IDS reactive

Un IDS reactive nu doar va detecta traficul suspect sau rău intenționat și va alerta administratorul, dar va lua măsuri proactive predefinite pentru a răspunde amenințării. De

obicei acest lucru înseamnă blocarea traficului și mai departe orice rețea de la adresa IP sursă sau utilizator.

IPS(Intrusion prevention systems)

IPS sunt dispozitive de securitate de rețea, care monitorizează activitățile de sistem de rețea și / sau pentru activitatea malware. Principalele funcții ale IPS sunt de a identifica activitatea de malware, a face un loga informațiilor despre această activitate, încercarea de a bloca / opri, și raportare.

IPS intruziunilor sunt considerate extensii ale IDS, deoarece ambele monitorizeaza traficul de rețea si contin un sistem de activități in caz ca a fost detectat o actiune malware. Principalele diferențe sunt: spre deosebire de IDS, IPS sunt plasate în linie și sunt capabili de a preveni / bloca intruziunile care sunt detectate în mod activ. Mai precis, IPS poate efectua astfel de acțiuni ca trimiterea de alarma, stergerea pachetelor malware, resetarea conexiunii și / sau blocarea traficului de la adresa IP. Un IPS poate corecta, de asemenea, prin CRC erorile, defragmenteaza fluxurile de pachete, pentru a preveni problemele de secventiere a TCP, și sterge transportul nedorit și opțiuni din layer-ul de rețea.

Clasificari:

- IPS bazate pe retea (NIPS): monitorizeaza intreaga retea prin analiza activitatii protocoalelor.
- IPS Wireless (WIPS): monitorizeaza o retea fara fir prin analiza protocoalelor respective.
- Analiza comportamentului de retea (NBA): examinează traficul de rețea pentru a identifica amenințările care generează fluxuri de trafic neobișnuite, cum ar fi DDoS atacuri, anumite forme de malware și de încălcări ale politicii.
- IPS bazate pe host (HIPS): un pachet de software-ul instalat, care monitorizează o singură gazdă pentru activitate suspectă, analizeaza evenimentele care au loc în această gazdă.

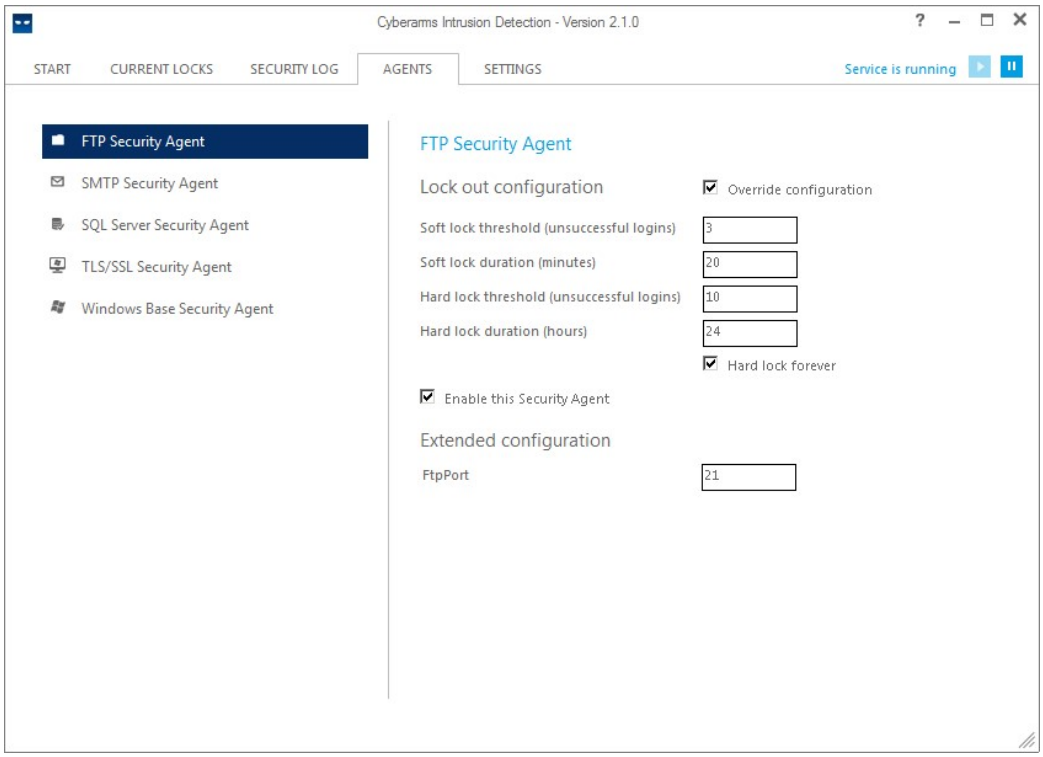
IPS ca si IDS are metodele de detectare bazate pe semnatura si bazate pe anomalie

Cyberarms Intrusion Detection

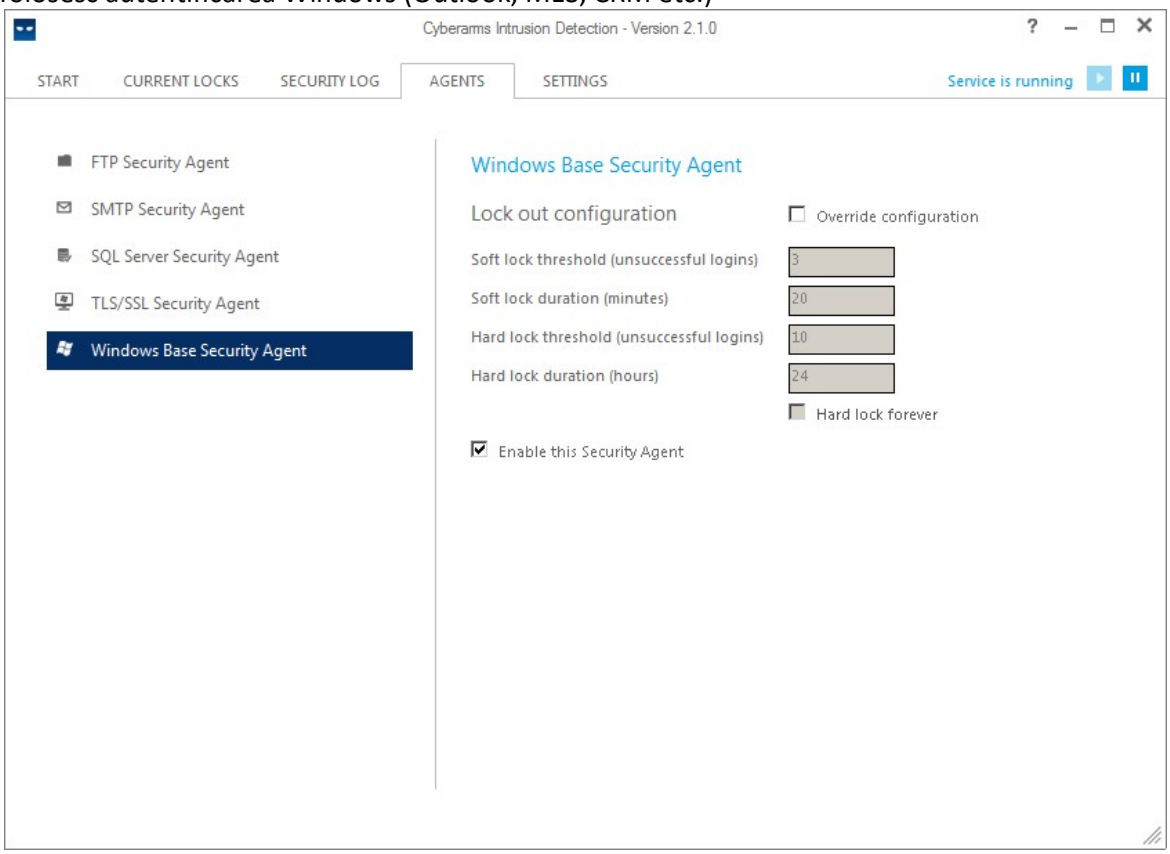
Cyberarms Intrusion Detection este un soft shareware care protejeaza SO Windows de atacuri brute force si incercari de intruziune.

Componente:

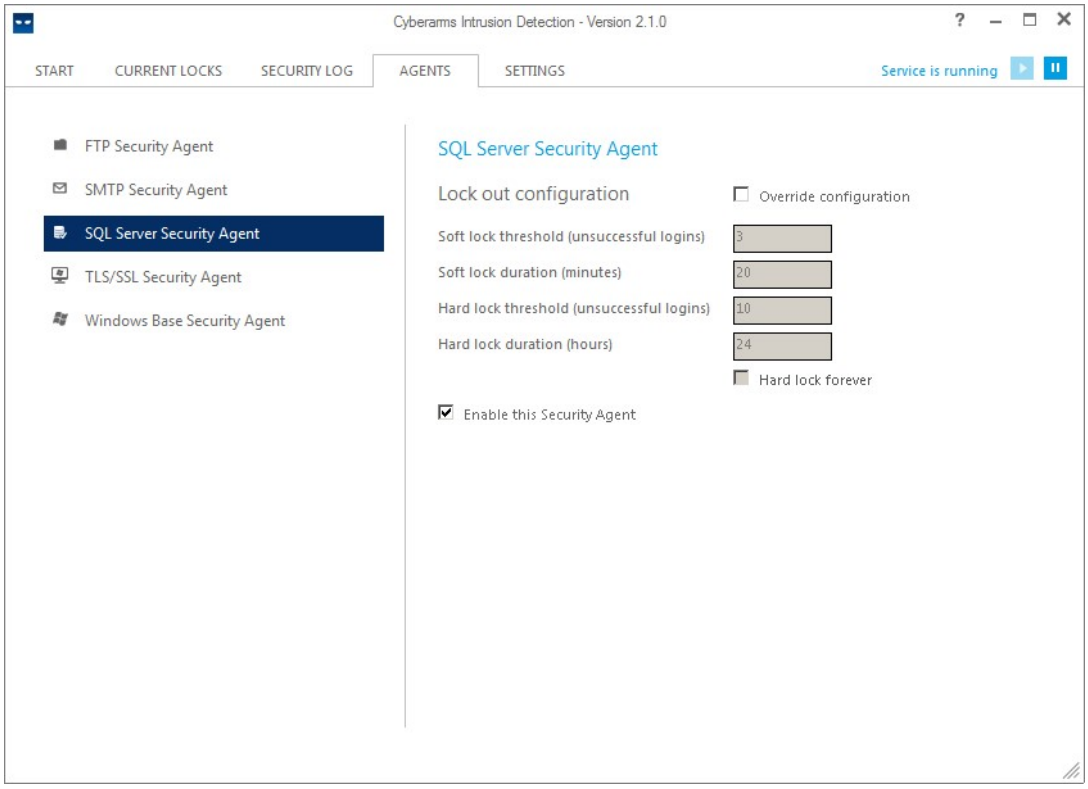
Securing FTP Access – monitorizeaza traficul pe portul TCP/IP pe care ruleaza serverul FTP



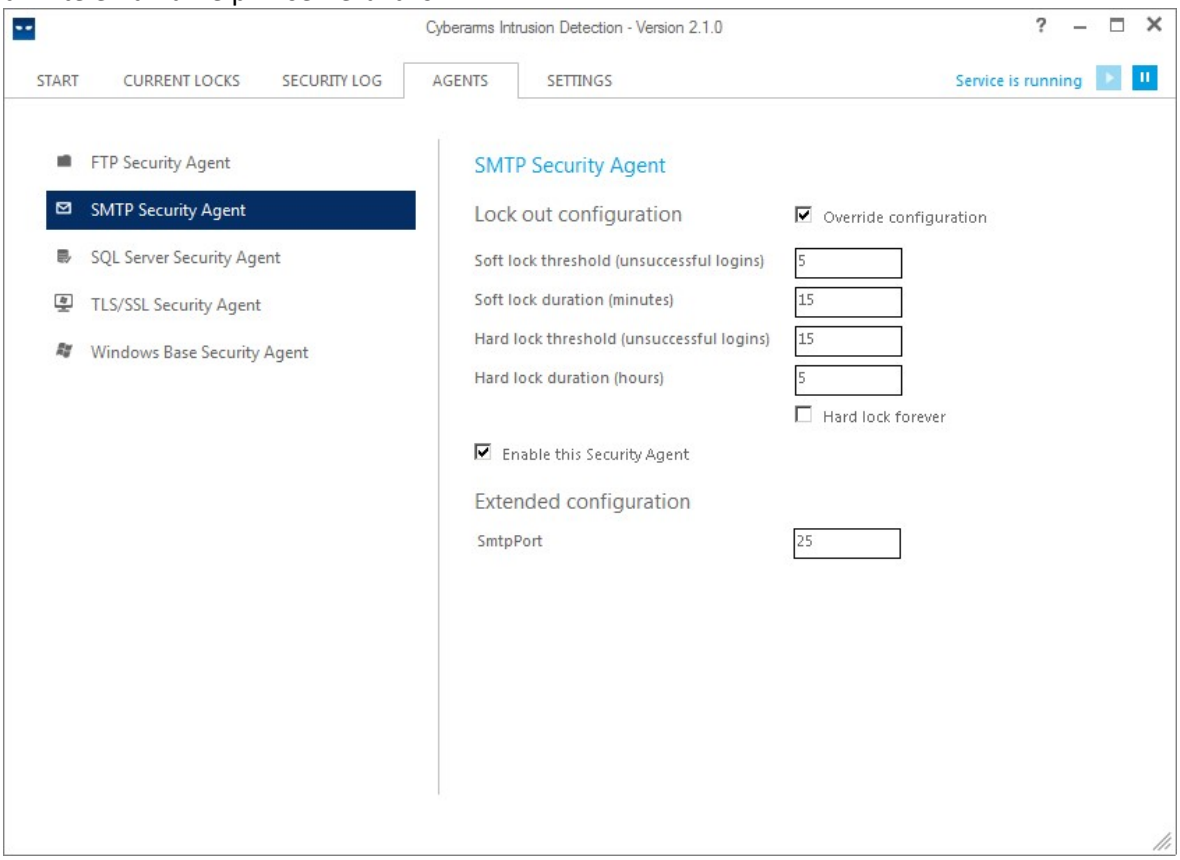
Securing Microsoft Exchange Outlook Web Access – monitorizeaza rapoartele log Windows pentru logari nereusite. Folositi aceasta componenta pentru a securiza aplicatiile ce folosesc autentificarea Windows (Outlook, MES, CRM etc.)



Securing Microsoft SQL Server – monitorizeaza logarile nereusite la autentificarea SQL Server



Securing SMTP Access – monitorizeaza traficul din retea. Multe programe malitioase utilizate de spammeri incearca sa intre in sistem utilizand autentificarea SMTP pentru a-si trimite email-urile prin serverul dvs.



IDS - sistem de detecție al intruziunilor (Intrusion Detection System) reprezintă un echipament (sau o aplicație) care monitorizează activitățile rețelei și/sau sistemului căutînd activități maliționase sau violări ale politicilor.

Detecția intruziunilor este procesul de monitorizare a evenimentelor care au loc într-un sistem sau o rețea de calculatoare și analiza lor pentru a detecta posibile incidente care sunt violări sau amenințări iminente de violare a politicilor de securitate, a politicilor de utilizare acceptate sau a practicilor standard de securitate.

Prevenirea intruziunilor este procesul prin care se desfășoară detecția intruziunilor și incercarea de înlaturare a posibilelor incidente detectate. Sistemele de detecție și prevenire ale intruziunilor - IDPS (Intrusion Detection-Prevention Systems) au ca scop principal identificarea posibilelor incidente, înregistrarea informațiilor despre ele, încercarea de înlaturare a incidentelor și raportarea către administratorii de securitate. În plus, organizațiile pot folosi IDPS-urile și pentru alte scopuri: identificarea problemelor legate de politicile de securitate, documentarea amenințărilor existente și descurajarea indivizilor în a încălca politicile de securitate.

Tipuri de IDS-uri:

▪ Sistem de detecție al intruziunilor de tip **network-based**. Într-un sistem de detecție al intruziunilor de tip network-based - Network-based Intrusion Detection System (**NIDS**) - senzorii sunt localizați în puncte critice ale rețelei care este monitorizată, de cele mai multe ori la marginea rețelei sau in DMZ (demilitarized zone). Senzorii captează tot traficul din rețea și analizează conținutul fiecărui pachet căutand urme de trafic malițios.
Un NIDS reprezintă o platformă independentă care identifică intruziunile prin examinarea traficului din rețea și monitorizează mai multe stații. NIDS-urile pot vizualiza traficul din rețea prin conectarea lor la un hub sau la un echipament switch configurat cu port mirroring.

▪ Sistem de detecție al intruziunilor de tip **host-based**.Într-un sistem de detecție al intruziunilor de tip host-based - Host-based Intrusion Detection System (**HIDS**) - senzorul constă, de obicei,într-un agent software care monitorizează toata activitatea ce se desfașoară pe stația pe care este instalat, incluzînd aici sistemul de fișiere, kernel-ul si chiar aplicații în unele cazuri.
Un HIDS reprezintă un agent care rulează local pe stație și care identifică intruziunile analizînd activitățile sistemului, aplicațiile, modificările sistemului de fișiere și alte activitäti ale stației.

Tehnici de evitare a IDS-urilor:

▪ fragmentarea şi trimiterea de pachete mici - o tehnică de bază care presupune fragmentarea informaţiei în mai multe pachete mai mici pentru a face imposibilă reconstruirea sesiunii la IDS;

▪ fragmente care se suprapun - tehnică ce presupune crearea de pachete cu numere ale secvenţei TCP care se suprapun încercând astfel să se exploateze faptul că sistemele de operare tratează diferit această suprapunere: unele vor lua în considerare datele mai noi, altele datele mai vechi;

▪ violări de protocol - violări deliberate ale protocoalelor TCP sau IP în aşa fel încât staţia ţintă să manevreze diferit pachetele decât IDS-ul;

▪ Inserarea de trafic în IDS - un atacator poate trimite pachete care să ajungă doar la IDS nu şi la staţia ţintă rezultând astfel o serie de alarme false;

▪ Atacuri de tip DoS - un atacător poate evita un IDS prin efectuarea unui atac de tip DoS asupra lui care să îi consume resursele sau care să genereze un număr foarte mare de alarmefalse reuşind astfel să ascundă atacul real.

Un **Sistem de Prevenire al Intruziunilor** - Intrusion Prevention System (**IPS**) - reprezinta un echipament de securitate al retelei care monitorizeaza activitatile retelei si/sau sistemelor si poate reactiona, in timp real, sa blocheze sau sa previna unele activitati malitioase. Tehnologia prevenirii intruziunilor este vazuta de catre unii ca o extensie a tehnologiei de detectie a intruziunilor, deoarece un IPS trebuie sa fie in acelasi timp si un foarte bun IDS pentru a asigura o rata scazuta de alarme false.

Un IPS este, in mod obisnuit, conceput pentru a opera complet invizibil in retea. Produsele IPS nu au de obicei o adresa IP din reteaua protejata dar pot raspunde in mod direct oricarui tip de trafic prin diverse metode (terminarea conexiunilor, renuntarea la pachete, generarea de alerte, etc.)

Desi unele IPS-uri au abilitatea de a implementa reguli de firewall aceasta este de obicei o functie aditionala si nu una din functiile de baza ale produsului. Mai mult, tehnologia IPS ofera o mai buna monitorizare a operatiilor unei retele furnizand informatii despre statiile active, incercarile de autentificare esuate, continut necorespunzator si alte functii ale nivelelor retea si aplicatie.

IPS-urile au unele avantaje faţă de IDS-uri. Unul dintre acestea se referă la faptul că IPS-urile sunt proiectate să fie implementate în-line astfel încât tot traficul să treacă prin ele şi să poată preveni atacurile în timp real. În plus, multe dintre soluţiile IPS au capabilitatea să decodifice protocoalele de nivel aplicaţie (HTTP, FTP, SMTP) oferind astfel o mai bună monitorizare. Totuşi atunci când se doreşte implementarea unui IPS de tip network-based trebuie să se ia în considerare faptul că dacă prin respectivul segment de reţea circulă trafic criptat majoritatea produselor nu pot să inspecteze astfel de trafic.

Un alt avantaj major ar fi faptul că unele dintre IPS-uri au posibilitatea de a corectă unele dintre metodele de evitare ale IDS-urilor(atacuri de tip DoS, inserarea de trafic).

Tipuri de IPS-uri:

▪ Un Sistem de Prevenire al Intruziunilor este de tip **host-based (HIPS)** atunci când aplicaţia de prevenire a intruziunilor se află pe adresa IP specifică sistemului protejat, de obicei o singură staţie. HIPS complementeaza metodele antivirus tradiţionale bazate pe semnături deoarece nu necesită o actualizare continuă pentru a putea răspunde atacurilor. Deoarece codul dăunător trebuie să modifice sistemul sau alte componente software care se află pe maşină în cauza un HIPS va observă aceste modificări şi va încerca să prevină această acţiune

sau să anunţe utilizatorul pentru permisiune. Dezavantajul major al unui astfel de produs constă în folosirea extensivă a resurselor staţiei pe care se află.

- Un Sistem de Prevenire al Intruziunilor este de tip **network-based (NIPS)** atunci când aplicaţia/echipamentul de prevenire al intruziunilor se află la o altă adresa IP decât staţia pe care o monitorizează. NIPS sunt platforme hardware/software care analizează, detectează şi raportează evenimente legate de securitatea unei reţele/segment de reţea de calculatoare.

Diferenţe între IPS-uri de tip host-based şi network-based

- HIPS-urile pot lucra atât cu date criptate cât şi cu date necriptate deoarece analiză se face după ce datele au fost decriptate de către staţie;

- NIPS-urile nu folosesc din memoria şi procesorul staţiilor care le protejează ci dispun de propria memorie şi propriul procesor;

- NIPS-urile se află în punctele critice ale reţelei şi tot traficul depinde de bună lor funcţionare,fapt ce poate constitui un dezavantaj atunci când echipamentul este nefuncţional

- NIPS-urile pot detecta evenimente distribuite în reţea (evenimente de prioritate joasă dar care afectează mai multe staţii din reţea) şi pot reacţiona în timp ce HIPS-urile au la dispoziţie doar datele de pe maşină pe care funcţionează pentru a putea lua o decizie. [4]