Mecanismes per a la detecció d'atacs i intrusions

Joaquín García Alfaro

1 crèdit
P03/05070/02097

Universitat Oberta de Catalunya

Índex

Introducció 3

Objectius 4

5.1. Necessitat de mecanismes addicionals a la prevenció i protecció 5

5.2. Sistemes de detecció d'intrusos 9
5.2.1. Antecedents dels sistemes de detecció d'intrusions 10
5.2.2. Arquitectura general d'un sistema de detecció d'intrusions 14
5.2.3. Recol·lectors d'informació 16
5.2.4. Processadors d'esdeveniments 19
5.2.5. Unitats de resposta 23
5.2.6. Elements d'emmagatzematge 24

5.3. Escàners de vulnerabilitats 25
5.3.1. Escàners basats en màquina 26
5.3.2. Escàners basats en xarxa 28

5.4. Sistemes de decepció 30
5.4.1. Equips de decepció 30
5.4.2. Cel·les d'aïllament 32
5.4.3. Xarxes de decepció 33

5.5. Prevenció d'intrusions 35
5.5.1. Sistemes de detecció en linea 36
5.5.2. Commutadors de nivell set 38
5.5.3. Sistemes tallafocs a nivell d'aplicació 39
5.5.4. Commutadors híbrids 40

5.6. Detecció d'atacs distribuïts 41
5.6.1. Esquemes tradicionals 41
5.6.2. Anàlisis descentralitzat 43

Resum 46

Glossari 46

Bibliografia 48

Introducció

Les xarxes d'ordinadors es troben exposades a atacs informàtics d'una forma tan freqüent que és necessari imposar una gran quantitat de requeriments de seguretat per a la protecció dels seus recursos.

Tot i que les deficiències d'aquests sistemes poden ser comprovades mitjançant eines convencionals, no sempre són corregides. En general, aquestes debilitats poden provocar un forat a la seguretat de la xarxa i faciliten entrades il·legals al sistema.

La majoria de les organitzacions disposen actualment de mecanismes de prevenció i mecanismes de protecció de les dades integrats a les seves xarxes. Però, tot i que aquests mecanismes han de ser considerats com imprescindibles, s'ha d'estudiar com continuar augmentant la seguretat assumida per l'organització.

Així, un nivell de seguretat únicament perimetral (basat tan sols en la integració a la xarxa de sistemes tallafocs i altres mecanismes de prevenció) no hauria de ser suficient. Hem de pensar que no tots els accessos a la xarxa passen pel tallafocs, ni que totes les amenaces són originades a la zona externa del tallafocs. A part, els sistemes tallafocs, com la resta d'elements de la xarxa, poden ser objecte d'atacs.

Una bona forma de millorar la seguretat de la xarxa passa per la instal·lació de mecanismes de detecció, capaços d'avisar a l'administrador de la xarxa en el moment que aquests atacs a la seguretat de la xarxa es produeixin.

Una analogia que ajuda a entendre la necessitat d'incorporar aquests elements podria ser la comparació entre la seguretat d'una xarxa informàtica i la seguretat d'un edifici: les portes d'entrada exerceixen un primer nivell de control en l'accés, però normalment no ens quedem aquí; instal·larem detectors de moviment o càmeres de vigilància en punts clau de l'edifici per a detectar l'existència de persones no autoritzades, o que fan un mal ús dels recursos, posant en perill la seguretat. A més, existiran vigilants de seguretat, llibres de registre on caldrà anotar a tot el personal que accedeix a un determinat departament que considerem crític, etc. Tota aquesta informació es processa des d'una oficina de control de seguretat on es supervisa l'enregistrament de les càmeres i es porten els llibres de registre. Tots aquests elements, projectats al món digital, configuren el que es coneix en l'àmbit de la seguretat informàtica com a mecanismes de detecció.

En aquest mòdul veurem els diferents mecanismes de detecció que existeixen i quines són les seves funcionalitats.

Objectius

En aquest mòdul didàctic es fixen els següents objectius:

1) Entendre la necessitat d'utilitzar mecanismes addicionals per a garantir la seguretat d'una xarxa ja protegida amb mecanismes de seguretat tradicionals.

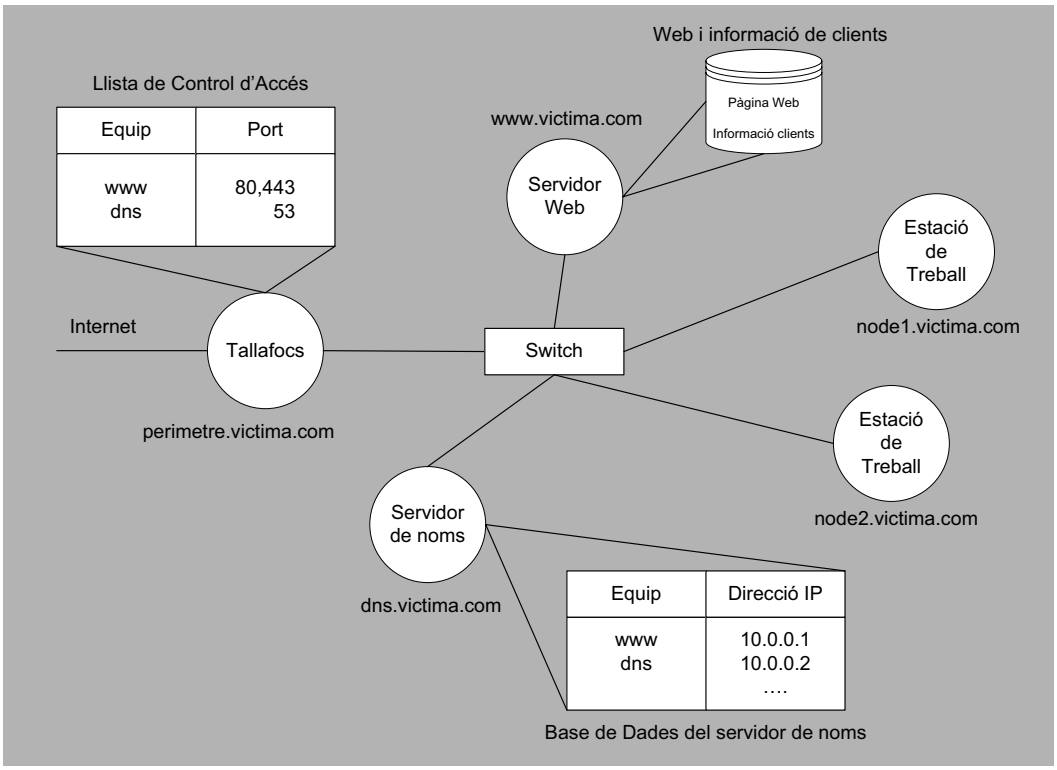
2) Comprendre l'origen dels primers sistemes de detecció i veure l'arquitectura general d'aquests sistemes.

3) Veure altres tecnologies complementaries als sistemes de detecció tradicionals.

5.1. Necessitat de mecanismes addicionals a la prevenció i protecció

L'escenari que presentarem a continuació descriu les possibles accions d'un atacant i il·lustra la necessitat d'una política de seguretat addicional que suporti i augmenti les estratègies de seguretat presentades fins aquest moment.

Suposem que un atacant està preparant introduir-se en una xarxa d'una petita empresa per tal d'obtenir les dades dels seus clients:



L'empresa es dedica a la venda d'articles per Internet i per a això, té en marxa la web `www.victima.com`, que li permet la venda on-line dels seus articles.

Preocupats per la seguretat de la seva xarxa (el diagrama de la qual es mostra a la figura anterior) i en concret per la seguretat de les dades dels seus clients, l'empresa té implementats els següents mecanismes de seguretat:

La xarxa està protegida amb un sistema tallafocs, que permet únicament l'entrada de peticions HTTP, HTTPS i consultes de DNS, acceptant també la transmissió de les respostes a les peticions HTTP, HTTPS i DNS.

El protocol HTTPS s'utilitza com a mecanisme de protecció de les dades dels clients a l'hora de realitzar transferències segures cap al servidor web, utilitzant tècniques criptogràfiques per a protegir la informació sensible que l'usuari transmet cap al servidor web (número de tarjeta de crèdit, informació personal, ...).

La intrusió que l'atacant intentarà portar a terme passarà per les següents quatre fases:

- **Fase de vigilància -** Durant la fase de vigilància, l'atacant intentarà aprendre tot el que pugui sobre la xarxa que vol atacar. En especial, tractarà de descobrir serveis vulnerables i errors de configuració.

- **Fase d'explotació de servei -** Aquest segon pas descriu l'activitat que permetrà a l'atacant fer-se amb privilegis d'administrador (escalada de privilegis) abusant d'alguna de les deficiències trobades durant l'etapa anterior.

- **Fase d'ocultació d'empremtes -** Durant aquesta fase d'ocultació es realitzarà tota aquella activitat executada per l'atacant (una vegada ja produïda la intrusió) per a passar desapercebut al sistema.

  Dins d'aquesta tercera etapa es contemplen activitats tals com per exemple l'eliminació d'entrades sospitoses en fitxers de registre, la instal·lació i modificació de comandes d'administració per a ocultar l'entrada en els sistemes de la xarxa, o l'actualització dels serveis vulnerables que ha utilitzat per a la intrusió (per a evitar que terceres parts s'introdueixin de nou en el sistema), ...

- **Fase d'extracció d'informació -** En aquesta última fase, l'atacant amb privilegis d'administrador tindrà accés a les dades dels clients a través de la base de dades de clients.

L'intrús començarà el seu atac obtenint el rang d'adreces IP on es troba allotjat el servidor de la web `www.victima.com`. Per a això, n'hi haurà prou amb realitzar una sèrie de consultes cap al servidor de DNS de la companyia.

A continuació, realitzarà una exploració de ports cap a cadascuna de les adreces IP trobades en el pas anterior. L'objectiu d'aquesta exploració de ports és la cerca de serveis en execució en cada una de les màquines del sistema, mitjançant alguna de les tècniques vistes en els mòduls anteriors.

Gràcies als mecanismes de prevenció instal·lats a la xarxa del nostre exemple (el sistema tallafocs i les llistes de control mostrades a la figura), la major part de les connexions seran eliminades. D'aquesta forma, l'atacant tan sols descobrirà dos de les màquines de la xarxa

(el servidor de DNS i el servidor web).

L'atacant decideix atacar el servidor web. Per a això, tractarà de descobrir quin tipus de servidor web està funcionant en aquest equip (li interessa el nom i la versió del servidor web en qüestió), ja que sap que es molt probable que existeixin deficiències de programació en aquest tipus d'aplicacions.

Per altra banda, l'atacant també intentarà descobrir el sistema operatiu i l'arquitectura hardware on el servidor web s'està executant. Aquesta informació serà important a l'hora de buscar els exploits que finalment utilitzarà per a realitzar la intrusió.

Per a obtenir tota aquesta informació, l'atacant en té suficient amb les entrades de DNS que la pròpia companyia li està oferint (a través dels camps HINFO de les peticions).

D'aquesta forma, l'atacant descobreix que el servidor web està funcionant sota una arquitectura concreta i que en aquest servidor hi ha un determinat sistema operatiu instal·lat.

Amb la informació del sistema operatiu l'atacant ja pot suposar el servidor web que està en execució dins l'equip i pot fins i tot confirmar la suposició observant les capçaleres de les respostes HTTP que el servidor envia en cada petició d'HTTP o HTTPS).

L'atacant, que colecciona un ampli repertori d'aplicacions per a abusar d'aquest producte, acabarà obtenint un accés amb privilegis d'administrador mitjançant, per exemple, la realització d'un desbordament de buffer existent en l'aplicació en qüestió.

La primera observació que podem indicar de tot el procés que acabem de descriure és que els mecanismes de prevenció de la xarxa permeten la realització d'aquest abús contra el servidor web ja que la forma de realitzar el desbordament de la pila d'execució s'ha fet mitjançant peticions HTTP legítimes (estan acceptades a les llistes de control del sistema tallafocs).

Així doncs, sense necessitat de violar cap de les polítiques de control d'accés de la xarxa, l'atacant pot acabar fent-se amb el control d'un dels recursos connectats a la xarxa de la companyia.

Una vegada compromès el servidor web, l'intrús entrarà en la fase d'ocultació i començarà a eliminar ràpidament totes aquelles marques que poguessin delatar la seva entrada al sistema.A més, s'encarregarà d'instal·lar a l'equip atacat d'un conjunt d'eines conegudes com a *rootkits**. Aquestes *rootkits* són una recopilació de binaris de sistema fraudulents, que s'encarreguen de deixar portes obertes al sistema atacat, per tal de garantir futures connexions amb la mateixa escalada de privilegis, així com a altres eines per a realitzar altres atacs al sistema o a la xarxa (aplicacions per a realitzar denegacions de servei, escoltes a la xarxa, extracció de contrasenyes de sistema, etc).

Les rootkits...

... són un conjunt d'eines per a garantir la fase d'ocultació d'empremtes durant l'atac d'intrusió a un sistema.

Les *rootkits* contenen versions modificades de les comandes bàsiques d'administració, amb la finalitat que les seves accions al sistema passin desapercebudes tot i que en futures entrades l'administrador del sistema el monitoritzi.

Una vegada finalitzada la fase d'ocultació d'empremtes, l'atacant disposa d'un equip dins de la xarxa que li podrà servir de trampolí per a realitzar nous atacs o intrusions a la resta d'equips de la companyia. A més, operant des d'una màquina interna de la xarxa, l'atacant ja no està subjecte a les restriccions imposades pels sistemes de prevenció.

Finalment, un cop arribats a aquest punt l'atacant disposarà sense cap problema de les dades que els clients tenen emmagatzemades a la base de dades.

Aquest exemple ens mostra com l'existència d'un sistema tallafocs (o d'altres mecanismes de prevenció) i la utilització de comunicacions xifrades (com a mecanisme de protecció de les dades) no és suficient a l'hora de defensar els nostres sistemes de xarxa.

5.2. Sistemes de detecció d'intrusos

Com acabem de veure en l'apartat anterior, la detecció d'intrusions assumeix que un atacant és capaç de violar la nostra política de seguretat, atacant parcial o totalment els recursos d'una xarxa, amb l'objectiu final d'obtenir accés amb privilegis d'administrador.

Els mecanismes per a la detecció d'atacs i intrusions s'encarreguen de trobar i reportar tot tipus d'activitat maliciosa a la xarxa, inclús arribant a reaccionar davant de l'atac de la forma apropiada.

En la majoria dels casos és desitjable poder identificar l'atac exacte que s'està produint, de forma que sigui possible detenir l'atac i recuperar-se d'aquest. En altres situacions només serà possible detectar i informar de l'activitat sospitosa que s'ha trobat, davant la impossibilitat de conèixer realment el que ha succeït.

Generalment, la detecció d'atacs treballarà sota la premisa de trobar-se en la pitjor de les situacions, suposant que l'atacant ha obtingut accés al sistema i que és capaç d'utilitzar o modificar els seus recursos.

Els elements més destacables dins de la categoria de mecanismes per a la detecció d'atacs i intrusions són els sistemes de detecció d'intrusos*.

* En anglès, *Intrusion Detection System* (IDS).

A continuació introduirem les dues definicions bàsiques utilitzades al camp de la detecció d'intrusos amb l'objectiu de clarificar termes comuns que més endavant utilitzarem.

Una **intrusió** és una seqüència d'accions realitzades per un adversari maliciós, amb l'objectiu final de provocar un accés no autoritzat sobre un equip o un sistema al complet.

La intrusió consistirà en la seqüència de passos realitzats per l'atacant que viola una determinada política de seguretat. L'existència d'una política de seguretat, on es contemplen una sèrie d'accions malicioses que s'han de prevenir, és un requisit clau per a la intrusió. En altres paraules, la violació tan sols podrà ser detectada quan les accions observades puguin ser comparades amb el conjunt de regles definides a la política de seguretat.

La **detecció d'intrusos*** és el procés d'identificació i resposta davant de les activitats malicioses observades contra un o diversos recursos d'una xarxa.

* En anglès, *Intrusion detection* (ID).

Aquesta darrera definició introdueix la noció de procés de detecció d'intrusos, que involucra tota una sèrie de tecnologies, usuaris i eines necessàries per a arribar a bon terme.

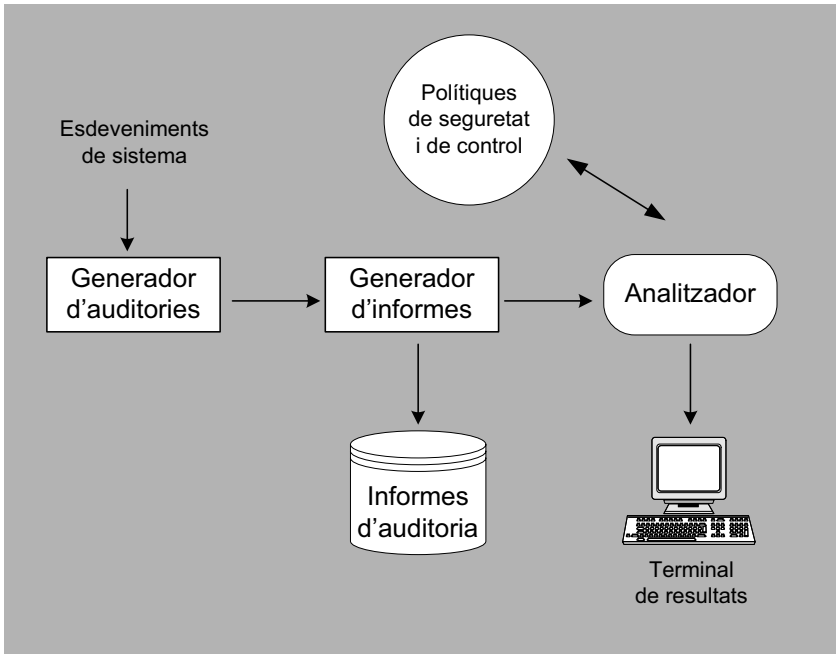
5.2.1. Antecedents dels sistemes de detecció d'intrusions

Els sistemes de detecció d'intrusos són una evolució directa dels primers sistemes d'auditories. Aquests sistemes tenien com a propòsit mesurar el temps que dedicaven els operadors a usar els sistemes que monitoritzaven, amb una precisió de milésimes de segon, i servien entre altres coses per a poder facturar el servei.

* En anglès, *Electronic Data Processsing* (EDP).

Els primers sistemes apareixen a la dècada dels cinquanta, quan l'empresa nord americana *Bell Telephone System* va crear un grup de desenvolupament amb l'objectiu d'analitzar l'ús dels ordinadors a empreses de telefonia. Aquest equip va establir la necessitat d'utilitzar auditories mitjançant Processament Electrònic de Dades*, trencant amb l'anterior sistema basat en realització d'informes en paper. Aquest fet va provocar que a finals dels anys 50 la *Bell Telephone System* s'embarqués en el primer sistema a gran escala de facturació telefònica controlada per ordinadors.

La següent figura mostra un esquema senzill del funcionament d'un sistema d'auditories, on els esdeveniments de sistema són capturats per uns generadors d'auditories que portaran les dades cap a l'element encarregat d'emmagatzemar-los a un fitxer d'informe.



A partir dels anys 70, el Departament de Defensa dels EEUU va començar a invertir nombrosos recursos per a la investigació de polítiques de seguretat, directrius i pautes de control. Aquests esforços culminaren amb una iniciativa de seguretat l'any 1977 on es definia el concepte de *sistemes de confiança*.

Els ***sistemes de confiança*** són aquells sistemes que empleen els suficients recursos de programari i de maquinari per a permetre el processament simultani d'una varietat d'informació confidencial o classificada. En aquests sistemes s'hi incloïen diferents tipus d'informació repartida en nivells, que corresponien al seu grau de confidencialitat.

Trusted Computer System Avaluation Critèria

Son una sèrie de documents de l'agencia nacional de seguretat (NSA) sobre sistemes de confiança, coneguda també sota el nom de *Rainbow series* degut als colors de les seves portades. El llibre principal d'aquesta sèrie es conegut com el *Llibre Taronja* (*Orange Book*). Vegeu la pàgina web `www.fas.org/irp-/nsa/rainbow.htm` per a més informació

A finals de la dècada dels setanta es va incloure en el *Trusted Computer System Avaluation Critèria* (TSCSEC) un apartat sobre els mecanismes de les auditories com a requisit per a qualsevol sistema de confiança amb un nivell de seguretat elevat. En aquest document, conegut sota el nom de *Llibre Marró* (*Tan Book*), s'enumeren els objectius principals d'un mecanisme d'auditoria que podem resumir molt breument en els següents punts:

- Permetre la revisió de patrons d'accés (per part d'un objecte o per part d'un usuari) i l'ús de mecanismes de protecció del sistema.
- Permetre el descobriment tant d'intents interns com externs de burlar els mecanismes de protecció.
- Permetre el descobriment de la transició d'usuari quan passa d'un menor nivell de privilegis a altre major (elevació de privilegis).
- Permetre el bloqueig dels intents dels usuaris per saltar-se els mecanismes de protecció del sistema.
- Servir, a més, com una garantia en front dels usuaris de que tota la informació que es reculli sobre atacs i intrusions serà suficient per a controlar els possibles danys ocasionats en el sistema.

Primers sistemes per a la detecció d'atacs en temps real

El projecte anomenat *Instrusion Detection Expert System* (IDES), desenvolupat entre 1984 i 1986 per *Dorothy Denning* i *Peter Neumann*, va ser un dels primers sistemes de detecció d'intrusions en temps real. Aquest projecte, finançat entre d'altres per la Marina nord-americana, proposava una correspondència entre activitat anómala i abús, o ús indegut (entenent per anómala aquella activitat extranya o inusual en un context estadístic).

IDES utilitzava perfils per a descriure als subjectes del sistema (principalment usuaris), i regles d'activitat per a definir les accions que tenien lloc (esdeveniments de sistema o cicles de CPU). Aquests elements permetien establir mitjançant mètodes estadístics les pautes de comportament necessàries per a detectar possibles anomalies.

Un segon sistema de detecció d'atacs en temps real a destacar va ser el *Discovery*, capaç de detectar i impedir problemes de seguretat en bases de dades. La novetat del sistema radicava en la monitorització d'aplicacions en lloc d'analitzar un sistema operatiu al complet. Mitjançant la utilització de mètodes estadístics desenvolupats en COBOL, el *Discovery* podia detectar possibles abusos.

Altres sistemes van ser desenvolupats per a ajudar a oficials nord americans a trobar marques d'atacs interns als ordinadors principals de les seves bases aèries. Aquests ordinadors eren principalment servidors corporatius que treballaven amb informació no classificada però molt confidencial.

Un dels últims sistemes a destacar d'aquesta època va ser el *Multics Intrusion Detection and Alerting System* (MIDAS), creat pel *National Computer Security Center* (NCSC). Aquest sistema de detecció va ser implementat per a monitoritzar el sistema *Dockmaster* de la NCSC, on s'executava un dels sistemes operatius més segurs de l'època*. De la mateixa manera que el sistema IDES, MIDAS utilitzava un sistema híbrid on es combinava tant l'estadística d'anomalies com les regles de seguretat d'un sistema expert. *MIDAS* utilitzava un procés d'anàlisis progressiu compost per quatre nivells de regles. A més d'aquestes regles, també comptava amb una base de dades que feia servir per a determinar signes de comportament atípic.

* Es tracta del sistema operatiu Multics, precursor dels sistemes Unix actuals.

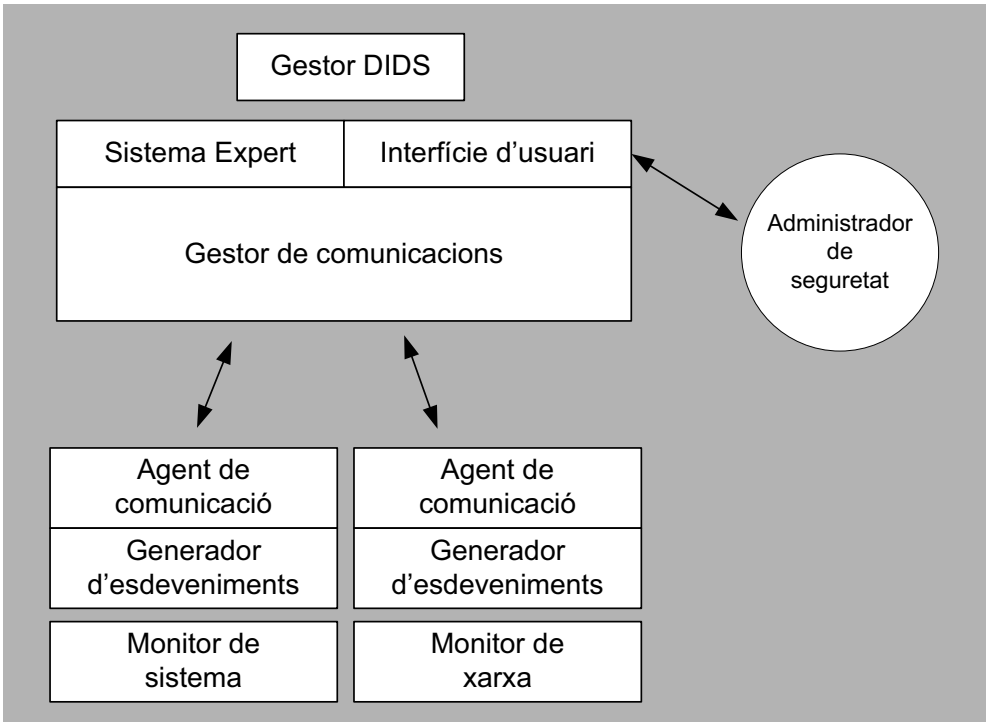
MIDAS va ser un dels primers sistemes de detecció d'intrusions connectats a Internet. Va ser publicat a la xarxa l'any 1989 i va monitoritzar el mainframe *Dockmaster* al 1990, contribuint a l'enfortiment dels mecanismes d'autenticació d'usuaris.

Sistemes de detecció d'intrusions actuals

A partir dels anys 90, el ràpid creixement de les xarxes d'ordinadors va provocar l'aparició de nous models de detecció d'intrusions. Per altra banda, els danys provocats pel famós cuc d'en Robert Morris al 1988 van ajudar a unir esforços entre activitats comercials i acadèmiques a la cerca de solucions de seguretat en aquest camp.

El primer pas va ser la fusió dels sistemes de detecció basats en monitorització de sistema operatiu (i aplicacions de sistema operatiu) juntament amb els sistemes de monitorització de tràfic de xarxa. Aquest es el cas del sistema *Distributed Intrusion Detection System* (DIDS), capaç de fer que un grup de seguretat pogués monitoritzar les violacions i intrusions de seguretat a través de xarxes connectades a Internet.

L'objectiu inicial del DIDS era proporcionar mitjans que permetessin centralitzar el control i publicació de resultats en un controlador central. La següent figura mostra un diagrama del sistema DIDS:



Per aquesta mateixa època començaren a aparèixer els primers programes de detecció d'intrusions d'ús comercial. Algunes empreses els desenvolupaven per a ocupar una posició destacada en l'àmbit de la seguretat, tot i que d'altres els feien per a millorar els nivells de seguretat exigits per la NCSC.

Actualment, existeixen un gran nombre de sistemes de detecció d'intrusos disponibles per tal de protegir les nostres xarxes. Tot i que molts d'aquests sistemes són comercials o reservats per a entorns militars i d'investigació, existeixen avui dia un gran nombre de solucions lliures que poden ser utilitzades sense cap mena de restriccions.

5.2.2. Arquitectura general d'un sistema de detecció d'intrusions

Com acabem de veure, des de el començament de la dècada dels vuitanta s'han realitzat multitud d'estudis referents a la construcció de sistemes per a la detecció de intrusos. En tots aquests estudis s'han realitzat diferents propostes i dissenys amb l'objectiu de complir els següents requeriments:

- *Precisió* - Un sistemes de detecció d'intrusions no ha de confondre accions legítimes amb accions deshonestes a l'hora de realitzar la seva detecció.

  Quan les accions legítimes són detectades com a accions malicioses, el sistema de detecció pot acabar provocant una denegació de servei contra un usuari o un sistema legitim. Aquest tipus de deteccions es coneixen com *falsos positius*. Quant menor sigui el nombre de falsos positius, major precisió tindrà el sistema de detecció d'intrusions.

- *Eficiència* - El detector d'intrusions ha de minimitzar la taxa d'activitat maliciosa no detectada (coneguda com *falsos negatius*). Quant menor sigui la taxa de falsos negatius, major serà l'eficiència del sistema de detecció d'intrusions. Aquest és un requeriment complicat, ja que en ocasions pot arribar a ser impossible obtenir tot el coneixement necessari sobre atacs passats, actuals i desconeguts.

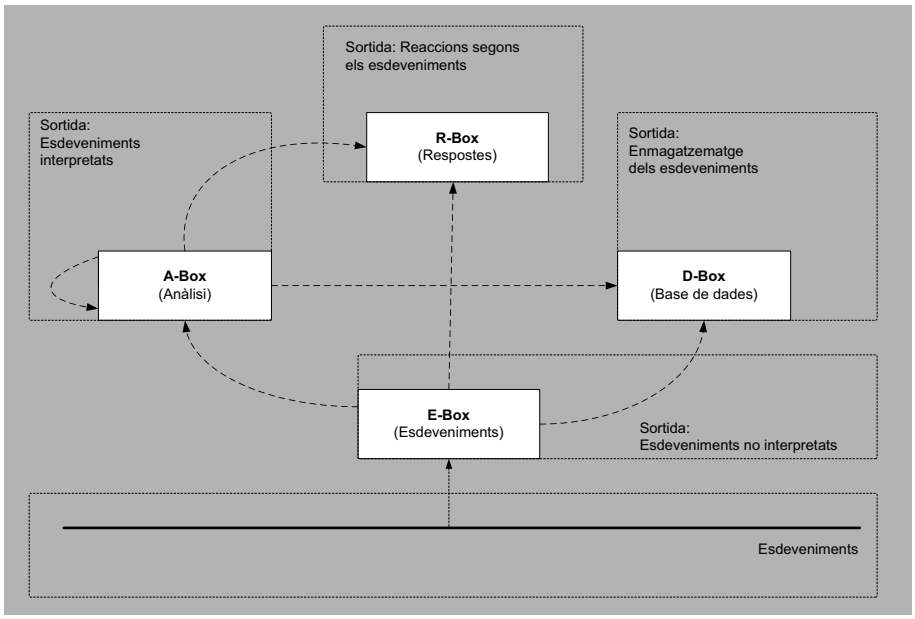
- *Rendiment* - El rendiment ofert per un sistema de detecció d'intrusions ha d'ésser suficient com per a poder arribar a realitzar una detecció en temps real. La detecció en temps real respon a la detecció de la intrusió abans que aquesta arribi a provocar danys al sistema. Segons els estudis, aquest temps hauria de ser inferior a un minut.

- *Escalabilitat* - A mesura que la xarxa vagi creixent (tant en mida com en velocitat), el nombre d'esdeveniments a tractar per el sistema també augmentarà. El detector ha d'ésser capaç de suportar aquest augment en el nombre d'esdeveniments, sense que es produeixi pèrdua d'informació. Aquest requeriment és de gran relevància en sistemes de detecció d'atacs distribuïts, on els esdeveniments són llançats en diferents equips del sistema i han de ser posats en correspondència per el sistema de detecció d'intrusions.

- *Tolerància a fallades* - El sistema de detecció d'intrusions ha d'ésser capaç de continuar oferint el seu servei encara que diferents elements del sistema siguin atacats (incloent-hi la situació de rebre el propi sistema un atac o intrusió).

Amb l'objectiu d'intentar normalitzar la situació, alguns membres del IETF* presentaren a meitat del 1998 una arquitectura de propòsit general per a la construcció de sistemes de detecció d'intrusos, coneguda com CIDF**. L'esquema proposat correspon amb el diagrama mostrat a la següent figura:

- Internet Engineering Task Force*
*-**Common Intrusion Detection Framework*



Dos anys després es va crear un nou grup de treball a l'IETF amb l'intenció d'estandaritzar i millorar la proposta del CIDF. Aquest grup de treball, conegut com IDWG*, replanteja de nou els requeriments necessaris per a la construcció d'un marc de desenvolupament genèric i es marca els següents objectius:

**Intrusion Detection Working Group*

- Definir la interacció entre el sistema de detecció d'intrusos front a altres elements de seguretat de la xarxa, com poden ser els sistemes de prevenció (tallafocs, llistes de control d'accés, ...).

  La seva primera proposta es coneix sota el nom de *Tunnel Profile*. Es tracta de la implementació d'un mecanisme per a la cooperació entre els diferents elements de seguretat mitjançant intercanvi de missatges. Aquest mecanisme garanteix una correcta comunicació entre els diferents elements, proporcionant privacitat, autenticitat i integritat de la informació intercanviada (alertes, esdeveniments, ...).

- Especificar el contingut dels missatges intercanviats (esdeveniments, alertes, ...) entre els diferents elements del sistema. Per a això, proposen el format *IDMEF*** i el protocol d'intercanvi de missatges *IDXP****.

-** Intrusion Detection Message Exchange Format
*-****Intrusion Detection Exchange Protocol*

Observant les propostes tant del CIDF com les del IDWG podem veure que els elements necessaris per a la construcció d'un sistema per a la detecció d'intrusos es poden agrupar en les següents quatre categories que a continuació passarem a comentar amb més detall:

1) Recol·lectors d'informació

2) Processadors d'esdeveniments

3) Unitats de resposta

4) Elements d'emmagatzematge

5.2.3. Recol·lectors d'informació

Un recol·lector d'informació, també conegut com a **sensor**, és el responsable de la recollida d'informació dels equips monitoritzats pel sistema de detecció.

La informació recollida serà transformada com una seqüència de tuples d'informació (esdeveniments) i serà analitzada posteriorment pels processadors d'informació.

La informació emmagatzemada en aquests esdeveniments serà la base de decisió per a la detecció de l'IDS. Per tant, serà important garantir la seva integritat front a possibles atacs de modificació, a l'hora de transmetre aquests esdeveniments entre el sensor que els va generar i el component de processat que els tractarà.

Existeixen diferents maneres de classificar les possibles implementacions d'aquest component. Tres de les propostes més utilitzades les detallem a continuació.

El primer tipus, conegut com a **sensors basats en equip***, s'encarreguen d'analitzar i recollir informació d'esdeveniments succeïts a nivell de sistema operatiu (com per exemple, intents de connexió i crides al sistema).

En el segon tipus trobem sensors que recullen informació d'esdeveniments succeïts a nivell de tràfic de xarxa (per exemple, analitzant les capçaleres IP de tots els datagrames que passen per la interficie de xarxa). Aquest tipus de components es coneixen com a **sensors basats en xarxa****.

El tercer tipus, coneguts com a sensors **basats en aplicació*****, reben la informació d'aplicacions que s'estan executant, i podrien ser considerats com un cas especial dels sensors basats en equip.

Snort

Una de les eines detecció més utilitzades com a sensor basat en xarxa en la majoria dels sistemes de detecció actuals es l'aplicatiu *Snort*. Aquesta eina es un detector d'intrusions en xarxa desenvolupat sota el paradigma de *software* lliure, capaç de realitzar anàlisis de tràfic en temps real, així com registrar paquets en xarxes TCP/IP.
Vegeu la pàgina web `www.snort.org` per a més informació.

-* En anglès, *host based sensors*.
-** En anglès, *network based sensors*.
-*** En anglès, *application based sensors*.

Elecció de sensors

Durant els últims anys, s'ha debatut bastant quin dels tres tipus de sensors pot oferir millors prestacions. Actualment, la majoria dels sistemes de detecció tracten d'unificar les tres opcions, oferint una solució de sensors híbrida.

- **Sensors basats en equip i en aplicació -** Els sensors basats en equip i en aplicació podran recollir informació de qualitat, a part de ser fàcilment configurables i de poder oferir informació de gran precisió.

  A més, aquestes dades poden arribar a tenir una gran densitat d'informació, com per exemple la informació reportada pels servidors de fitxers de registre del sistema. A més, també poden arribar a incloure gran quantitat d'informació de pre-processat que facilitarà el treball dels components de processat de la informació.

  Per contra, aquests sensors poden repercutir notablement en la eficiència del sistema on s'executin.

- **Sensors basats en xarxa -** El principal avantatge dels sensors basats en xarxa, front a les altres dues solucions, és la possibilitat de poder treballar de manera no intrusiva. Per tant, la recollida d'informació no afecta a la forma de treballar dels equips o a la pròpia infraestructura. Al no residir forçosament en els equips a analitzar, són més resistents a sofrir atacs.

  Per altra banda, la majoria dels sensors basats en xarxa són independents del sistema operatiu i poden obtenir informació a nivell de xarxa (com per exemple l'existència de fragmentació en datagrames IP) que no podria ser proporcionada per sensors basats en equip.

  Alguns sensors basats en xarxa són en realitat commutadors amb capacitat d'anàlisis transparent en front a la resta del sistema.

  Com a desavantatge principal dels sensors basats en xarxa cal destacar l'escasa escalabilitat que aquest apropament ofereix. En casos de xarxes amb carreges de tràfic molt elevades, és molt probable que aquests sensors comencin a perdre paquets, el que suposa una pèrdua en la seva capacitat de recollida d'informació.

  Difícilment aquests sensors serien capaços de continuar treballant amb normalitat en xarxes d'alta velocitat, com per exemple xarxes Gigabit Ethernet.

  Un altre problema és l'increment de la utilització de criptografia en les comunicacions, que farà que la informació a recollir sigui incomprensible per al sensor, reduint d'aquesta forma les seves capacitats de detecció.

Instal·lació de sensors

No és del tot trivial determinar el lloc exacte on colocar aquests components (des d'on recollir la informació). Els més senzills de colocar són els sensors basats en aplicació, generalment instal·lats en aquelles parts del programa on s'ofereixen serveis de depuració i generació de fitxers de registre. Però la situació és molt més difícil per a les altres dues variants.

Quan considerem la instal·lació de sensors basats en equip, la gran varietat de sistemes operatius existents, i les diferents facilitats ofertes per cadascú d'ells, suposa un seriós problema. A més, no sol ser senzill determinar quina part de la gran quantitat d'informació generada pel nucli d'un sistema operatiu hauria ser relevant a l'hora d'analitzar.

En el cas de sistemes operatius del tipus Unix, existeix la proposta del *Llibre Taronja* (ja comentat en aquest mateix mòdul), on es mostren 23 punts d'interès on hauria d'analitzar-se informació.

En el cas dels sensors basats en xarxa, la utilització de xarxes segmentades mitjançant commutadors de xarxa suposa un gran inconvenient en quant a triar el lloc correcte on colocar aquests sensors.

Una topologia en estrella fa que els paquets vagin encaminats únicament entre les dues parts d'una comunicació, pel que caldria colocar el sensor en un punt en el que fora capaç de poder analitzar qualsevol intercanvi d'informació.

Una primera opció seria colocar el sensor sobre l'enllaç on s'uneixen tots els equips de la xarxa. Aquesta opció podria suposar la necessitat d'analitzar una quantitat de dades tan elevada que el sensor acabaria perdent d'informació.

L'altre opció seria la col·locació del sensor entre l'enllaç de xarxa que separa l'interior i el exterior, com si es tractarà d'un sistema de prevenció perimetral addicional.

Una variant a aquestes dues opcions seria la utilització del port d'intervenció (*tap port*) que molts commutadors ofereixen. Es tracta d'un port especial que reflecteix tot el tràfic que passa a través de l'equip. Lamentablement, aquest port podria fàcilment sobrecarregar la capacitat d'anàlisis dels sensors si la quantitat de tràfic és molt elevada. A més, l'ample de banda intern del dispositiu és suficient per a tractar amb tots els ports actius a la vegada, però si és tràfic analitzat comença a créixer, és possible que es superi la capacitat del port d'intervenció, amb la corresponent pèrdua de paquets que això comportaria.

5.2.4. Processadors d'esdeveniments

Els processadors d'esdeveniments, també coneguts com **analitzadors**, conformen el nucli central del sistema de detecció. Tenen la responsabilitat d'operar sobre la informació recollida pels sensors per a poder inferir possibles intrusions.

Per tal d'inferir possibles intrusions, els analitzadors implementaran un esquema de detecció. Dos dels esquemes majoritàriament utilitzats a l'hora de realitzar la detecció són el model de detecció d'usos indeguts i el model de detecció d'anomalies. A continuació passarem a comentar breument aquests dos esquemes de detecció.

Esquema de detecció basat en usos indeguts

La detecció d'intrusions basada en el model d'usos indeguts compta amb el coneixement a priori de seqüències i activitats malicioses. Els processadors d'esdeveniments que implementes aquest esquema analitzen els esdeveniments a la cerca de patrons d'atacs coneguts o activitat que ataca vulnerabilitats típiques dels equips.

Les seqüències o patrons descrits es coneixen com a firmes d'atac i podrien ser compares amb les firmes víriques que utilitzen els antivirus actuals.

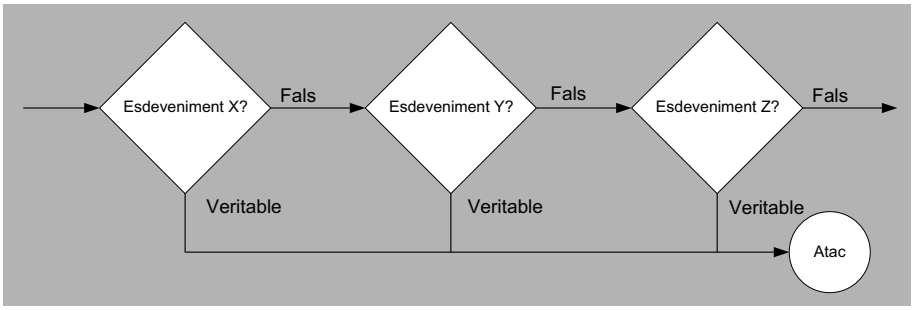
Així doncs, els components de detecció basats en el model d'usos indeguts compararan els esdeveniments enviats pels sensors amb les firmes d'atac que mantenen emmagatzemades en les seves bases de coneixement.

En el moment de detectar concordància d'algun esdeveniment o seqüència d'esdeveniments amb alguna firma d'atac, el component llançarà una alarma.

A l'hora d'implementar un esquema de detecció basat en usos indeguts, dos dels models més utilitzats son els analitzadors basats en reconeixement de patrons i els analitzadors basats en transicions d'estats.

- ***Analitzadors basats en reconeixement de patrons*** - Mitjançant l'utilització de regles del tipus *if-then-else* per a examinar les dades, aquests analitzadors processen la informació mitjançant funcions internes al sistema, de forma completament transparent a l'usuari.

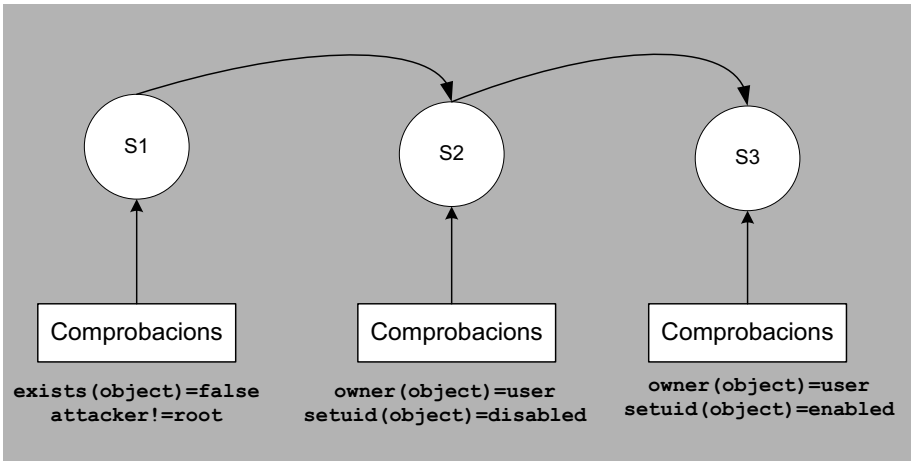
La següent figura mostra l'esquema d'una regla *if-then-else*.



Tot i que aquest model permet detectar una intrusió a partir de patrons coneguts a priori, la seva desavantatge principal és que aquests patrons no defineixen un ordre seqüencial de les accions.

Detectar mitjançant aquest mètode atacs compostos per una seqüencia d'esdeveniments pot arribar a comportar grans dificultats. Per altra part, el manteniment i actualització de la base de dades de patrons és altres dels punts crítics d'aquest model.

- ***Anàlitzadors basats en transicions d'estats*** - Aquest model fa ús d'autòmats finits per a representar els atacs, a on els nodes representen els estats, i les fletxes (arcs) les transicions.



La utilització de diagrames de transició facilita l'associació entre els estats i els distints passos que realitza un atacant des que entra en un sistema, amb privilegis limitats, fins que es fa amb el control del mateix.

Com a principals avantatges d'aquest model es pot destacar que els diagrames de transició permeten fer una representació a alt nivell d'escenaris de penetració, oferint una forma d'identificar una sèrie de seqüències que conformen un atac.

D'altra banda, aquests diagrames defineixen de forma molt senzilla els atacs a detectar. El motor d'anàlisis podria arribar a utilitzar diferents variants del mateix diagrama per a identificar atacs similars.

Per contra, els diagrames de transició, i per tant, els diferents passos de la seqüencia, han de ser creats mitjançant llenguatges específics que en moltes ocasions solen ser molt limitats i insuficients per a recrear atacs complexos.

Aquesta limitació fa que aquest model no pugui detectar alguns dels atacs més comuns, sent necessari l'ús de motors d'anàlisis addicionals com a complement d'aquest model.

Esquema de detecció basat en anomalies

Els processadors d'esdeveniments que basen la seva detecció en un esquema d'anomalies tractaran d'identificar activitats sospitoses comparant el comportament d'un usuari, procés o servei amb el comportament de perfil classificat com normal.

Un perfil serveix com métrica (mesura d'un conjunt de variables) de comportaments normals. Qualsevol desviació que superi un cert llindar respecte al perfil emmagatzemat serà tractat com una evidència d'atac o intrusió.

Un dels requeriments d'aquest model és la necessitat d'inicialització d'un perfil per defecte que s'anirà adaptant progressivament al comportament d'un usuari, procés o servei normal (no sospitós). És necessari, per tant, l'ús d'heurístiques i descriptors estadístics que ajuden a modelar correctament canvis en el comportament tan aviat com succeeixi. Altres propostes tracten d'incorporar tècniques d'intel·ligència artificial per a realitzar aquestes tasques (com per exemple, l'ús de xarxes neuronals o d'algorismes genètics).

La detecció basada en anomalies té clars avantatges respecte a la detecció basada en usos indeguts. Pot ser, l'avantatge més destacada és la possibilitat de detectar atacs desconeguts. Això es possible ja que independentment de com l'atacant hagi aconseguit la intrusió en un sistema, tan aviat com les seves activitats comencin a desviar-se del comportament d'un usuari normal, el processador d'esdeveniments llançarà una alarma avisant d'una possible intrusió.

L'esquema de detecció basat en anomalies, però, té alguns desavantages. Un dels primers desavantatges que trobem en aquest model és la falta de garantia en el procés de detecció: un intrús podria actuar de forma acurada, realitzant les seves accions lentament per a anar provocant canvis en el perfil d'usuari del processador d'esdeveniments, amb la finalitat que la seva presència en el sistema passi desapercebuda.

Com a segon inconvenient podem destacar la dificultat que apareix a la hora de classificar i descriure amb precisió els atacs detectats mitjançant analitzadors basats en anomalies. Generalment, un analitzador no només ha de llançar una alarma si no que haurà d'especificar d'on procedeix l'atac, que canvis a sofert el sistema, ...

Finalment, la gran taxa de falsos positius i negatius que pot donar-se utilitzant aquest esquema de detecció es un greu inconvenient, ja que no sempre una desviació respecte al perfil esperat coincidirà amb un atac o intent d'intrusió. En el cas de processadors a on els esdeveniments procedeixen de sensors basats en xarxa, és possible que el nombre d'alarmes llançades (en una xarxa de petit mida) supere el centenar amb facilitat. Això provoca que, amb freqüència, els administradors de la xarxa acaben ignorant les alarmes llançades pel sistema de detecció, o inclús desactivant el sistema al complet.

Tots aquests inconvenients fan que la majoria dels sistemes de detecció comercials disponibles en l'actualitat implementin els seus analitzadors mitjançant l'esquema de detecció d'usos indeguts.

5.2.5. Unitats de resposta

Les unitats de resposta d'un sistema de detecció, s'encarregaran d'iniciar accions de resposta en el moment en que es detecti un atac o intrusió. Aquestes accions de resposta poden ser automàtiques (**resposta activa**) o requerir interacció humana (**resposta passiva**).

Les respostes actives tenen com a objectiu actuar contra l'atac, intentant la seva neutralització, en el moment en el que és detectat (o mentre una intrusió encara continua en curs). Exemple de resposta activa poden ser la cancel·lació de la connexió en xarxa que va originar l'atac o el propi seguiment de l'atac que permeti més endavant l'anàlisi adient.

Per altra banda, les respostes passives es limiten a llançar una alarma per a informar i descriure l'atac detectat a l'administrador del sistema. La majoria dels components de resposta passius ofereixen diferents formes de fer arribar aquesta informació a l'administrador, com per exemple l'ús de correu electrònic, utilització de missatges SMS, etc.

El problema de les respostes actives és que poden acabar en una denegació de servei contra usuaris o sistemes legítims. És molt probable que algunes de les alarmes que els processadors fan saltar siguin incorrectes. Per exemple, si la unitat de resposta tallés immediatament amb la connexió que va originar aquesta alarma, o amb aquells processos considerats sospitosos, podria suposar la pèrdua de treball d'un usuari o servei innocent.

En la majoria dels sistemes (per exemple, servidors de comerç electrònic) aquest tipus d'errors pot suposar la pèrdua de clients, la qual cosa és inadmissible. Per aquest motiu, la majoria de empreses en el sector del comerç electrònic es decanten per la contractació d'especialistes que, de manera manual, analitzaran els informes generats pel sistema de detecció per a determinar si és necessària una resposta activa davant de tal avis.

Finalment, cal destacar que, al igual que els sensors, les unitats de resposta també podrien ser classificats en diferents categories segons el punt d'actuació. Dues de les categories més generals les unitats de resposta basades en equip i les unitats de resposta basades en xarxa.

- **Unitats de resposta basades en equip -** , s'encarreguen d'actuar a nivell de sistema operatiu (com per exemple, bloqueig d'usuaris, finalització de processos, etc).

- **Unitats de resposta basades en xarxa -** , que actuen a nivell de tràfic de xarxa (per exemple, tallant intents de connexió, filtratge de direccions, etc).

5.2.6. Elements d'emmagatzematge

En algunes situacions, el volum d'informació recollida pels sensors del sistema de detecció arriba a ser tan elevada que es fa necessari, previ al seu anàlisi, un procés d'emmagatzemament. Suposem, per exemple, el cas que tots els paquets d'una xarxa d'alta velocitat vole ser analitzats per part dels analitzadors del sistema de detecció. En aquest cas, serà necessari plantejar-se una jerarquia d'emmagatzemament que redueixi el volum d'informació sense penalitzar les possibilitats d'anàlisi.

Una possibilitat és la classificació de la informació en termes d'anàlisis a curt i mitjà termini.

En el cas d'anàlisi a curt termini, la informació serà emmagatzemada directament en els propis sensors (en *buffers* interns) de manera que després de realitzar un pre-processat de les dades, i la seva transformació a un format d'esdeveniment, sigui transmesa cap als elements de processament.

En el cas d'informació a mitjà termini, les dades pre-processades seran emmagatzemades en dispositius secundaris (amb el format apropiat) en lloc de ser transmeses cap als processadors del sistema.

El temps d'emmagatzemament d'una informació a mitjà termini pot ser de l'ordre de dos o tres dies, amb l'objectiu de ser consultada pels processadors del sistema en cas de que el procés d'anàlisis així ho requereixi.

Eventualment, i després d'un procés de compressió (per a reduir la mida), part de la informació a mitjà termini podrà continuar emmagatzemada durant llargs períodes de temps (de l'ordre de mesos o inclús anys) a l'espera de poder ser consultada per processos de detecció a llarg termini.

5.3. Escàners de vulnerabilitats

Els escàners de vulnerabilitats són un conjunt d'aplicacions que ens permetran realitzar proves o tests d'atac per a determinar si una xarxa o un equip té deficiències de seguretat que poden ser explotades per un possible atacant o comunitat d'atacants.

Tot i no ser formalment un element de detecció tradicional, el escàners de vulnerabilitats posseeixen una estreta relació amb les eines de detecció utilitzades als sistemes detecció d'intrusos. De fet, en molts àmbits se'ls considera un cas especial d'aquestes eines i generalment son utilitzats a l'hora de realitzar un anàlisi d'intrusions.

Això és així perquè dintre dels mecanismes de detecció d'atacs podem distingir entre elements de detecció de caire dinàmic (que seria el cas de les eines de detecció utilitzades en un sistema de detecció d'intrusos) i elements de detecció de caire estàtic (els escàners de vulnerabilitats). En els primers es treballa de forma contínua (com una videocàmera) mentre que els segons es concentren en intervals de temps determinats (com una càmera de fotos).

A causa d'aquest aspecte estàtic, els escàners de vulnerabilitats tan sols podran detectar aquelles vulnerabilitats contingudes en la seva base de coneixement. A més, tan sols són capaços d'identificar fallades de seguretat en els intervals en que s'executen. No obstant, són unes eines de gran utilitat i un bon complement als sistemes de detecció instal·lats en una xarxa.

El funcionament general d'un escàner de vulnerabilitats podria dividir-se en tres etapes:

- Durant la primera etapa es realitza un extracció de mostres del conjunt d'atributs del sistema, per a poder emmagatzemar-les posteriorment en un contenidor de dades segur.

- En la segona etapa, aquests resultats són organitzats i comparats amb al menys un conjunt de referència de dades. Aquest conjunt de referència podria ser una plantilla amb la *configuració ideal* generada manualment, o bé ser una imatge de l'estat del sistema feta amb anterioritat.

- Finalment, es generarà un informe amb les diferències entre ambdós conjunts de dades.

Les tres etapes anteriors podrien ser millorades mitjançant la utilització de motors de comparació en paral·lel o inclús mitjançant la utilització de mètodes criptogràfics per a detectar canvis en els objectes monitoritzats.

A l'hora de classificar aquest tipus d'eines trobem bàsicament dos categories principals, segons la localització des de la que s'obtenen dades: escàners basats en màquina o basats en xarxa.

5.3.1. Escàners basats en màquina

Aquest tipus d'eines varen ser els primers en utilitzar-se per a l'avaluació de vulnerabilitats. Es basen en la utilització d'informació d'un sistema per a la detecció de vulnerabilitats, com per exemple errors en permisos de fitxers, comptes d'usuari obertes per defecte, entrades d'usuari duplicades o sospitoses, etc.

Aquesta informació es pot obtenir mitjançant consultes al sistema, o a través de la revisió de diferents atributs del sistema.

Un simple guió de sistema com el següent, s'encarregaria d'avisar mitjançant correu electrònic a l'administrador del sistema en cas de trobar entrades anòmales en el fitxer de passwords del sistema:

```
#!/usr/bin/perl
$count==0;
open(MAIL, "| /usr/lib/sendmail mikal");
print MAIL "To: Administration\n";
print MAIL "Subject: Password Report\n";
open(PASSWORDS, "cat /etc/passwd |");

while(<PASSWORDS>) {
      $linenumber=$.;
      @fields=split(/:/, $_);
      if($fields[1] eq "") {
            $count++;
            print MAIL "\n***WARNING***\n";
            print MAIL "Line $linenumber has a blank password.\n";
            print MAIL "Here's the record: @fields\n";
      }
}

close(PASSWORDS);
if($count < 1) print MAIL "No blank password found\n";
print MAIL ".\n";
close(MAIL);
```

Les vulnerabilitats que es solen trobar mitjançant l'avaluació basada en màquina solen estar relacionades amb atacs d'escalada de privilegis. Aquests atacs persegueixen obtenir permisos d'usuari *root* en sistemes Unix, o d'administrador en sistemes Windows.

Els motors d'anàlisis de vulnerabilitats basats en màquina estan molt relacionats amb el sistema operatiu que avaluen, la qual cosa fa el seu manteniment costos i complica la seva administració en entorns heterogenis.

Les credencials utilitzades han de ser protegides convenientment, així com la informació accedida mitjançant les mateixes, per a evitar que siguin objecte d'atacs.

Un dels primers escàners de vulnerabilitats en sistemes Unix va ser COPS, una eina que s'encarregava d'analitzar el sistema a la cerca de problemes de configuració típics incloent: permisos erronis de fitxers, directoris i serveis, contrasenyes d'usuari dèbils, bits de suplantació impropis, etc.

Aquest seria un exemple d'informe reportat per COPS:

```
ATTENTION:

Security Report for Sun Abr 20 20:57:09 CET 2003 from host vm3

Warning! NFS filesystem exported with no restrictions!
Warning! NFS filesystem exported with no restrictions!
Warning! NFS filesystem exported with no restrictions!
Warning! NFS filesystem exported with no restrictions!
Warning! /dev/fd0 is_World_writable!
Warning! /dev/fd0 is_World_readable!
Warning! /var/spool/mail is_World_writable!
Warning! /etc/security is_World_readable!
Warning! /usr/local/bin is_World_writable!
Warning! /root/adduser.log is_World_readable!
Warning! /root/bash.man is_World_readable!
Warning! /root/bin is_World_readable!
Warning! /root/control is_World_readable!
Warning! /root/cops_1_04.tar is_World_readable!
Warning! /root/cops.man is_World_readable!
Warning! /root/cops_man.html is_World_readable!
```

Una altra eina similar és TIGER que, a l'igual que COPS, es compon d'un conjunt d'aplicacions i guions de sistema amb l'objectiu de realitzar auditories de seguretat a sistemes Unix.

El seu objectiu principal és informar de les maneres en que pot comprometre's el sistema. La següent imatge mostra un exemple d'informe reportat per TIGER:

```
#hosts.equiv      This file describes the names of the
#                 hosts which are to be considered "equivalent",
#                 i.e. which are to be  trusted enought
#                 for allowing rsh (1) commands.
#
#hostname
#Checking accounts from /etc/passwd...
#Performing check of .netrcfiles...
#Checking accounts from /etc/passwd...
#Performing check of PATH components...
#Only checking user'root'

--WARN--[path002w]/usr/bin/amadmin in root's
         PATH from default is not owned  by root (owned by amanda).
--WARN--[path002w]/usr/bin/amcheckdb in root's
         PATH from default is not owned by root (owned by amanda).
--WARN--[path002w]/usr/bin/amcleanup in root's
         PATH from default is not owned by root (owned by amanda).
--WARN--[path002w]/usr/bin/amdump in root's
         PATH from default is not owned by root (owned by amanda).
```

5.3.2. Escàners basats en xarxa

Els escàners de vulnerabilitats basats en xarxa varen aparèixer posteriorment i s'han anat fent cada vegada més populars. Obtenen la informació necessària a través de les connexions de xarxa que estableixen amb l'objectiu a analitzar.

Així doncs, els escàners de vulnerabilitats basats en xarxa realitzen proves d'atac i registren les respostes obtingudes. No s'ha de confondre aquests analitzadors de vulnerabilitats basats en xarxa amb els analitzadors d'un sistemes de detecció d'intrusions. Encara que un escàner d'aquestes característiques pot ser molt similar a una eina de detecció d'intrusions, no representa una solució tan completa.

Dues de les tècniques més utilitzades per a l'avaluació de vulnerabilitats basades en xarxa són les següents:

- **Prova per explotació -** Aquesta tècnica consisteix a llançar atacs reals contra l'objectiu. Aquests atacs estan programats normalment mitjançant guions de comandes. En comptes d'aprofitar la vulnerabilitat per a accedir al sistema, es retorna un indicador que mostra si s'ha tingut èxit o no. Obviament, aquest tipus de tècnica és bastant agressiva, sobretot quan es proven atacs de denegació de servei.

- **Mètodes d'inferència -** El sistema no explota vulnerabilitats, sinó que busca indicis que indiquen que s'han realitzat atacs. És a dir, busca resultats de possibles atacs en l'objectiu.

  Aquest mètode és menys agressiu que l'anterior, però no obstant, els resultats obtinguts són menys exactes.

  Exemples de tècniques d'inferència poden ser la comprovació de versió de sistema per a determinar si existeix una vulnerabilitat, la comprovació de l'estat de determinats ports per a descobrir quins estan oberts, i la comprovació de conformitat de protocol mitjançant sol·licituds d'estat.

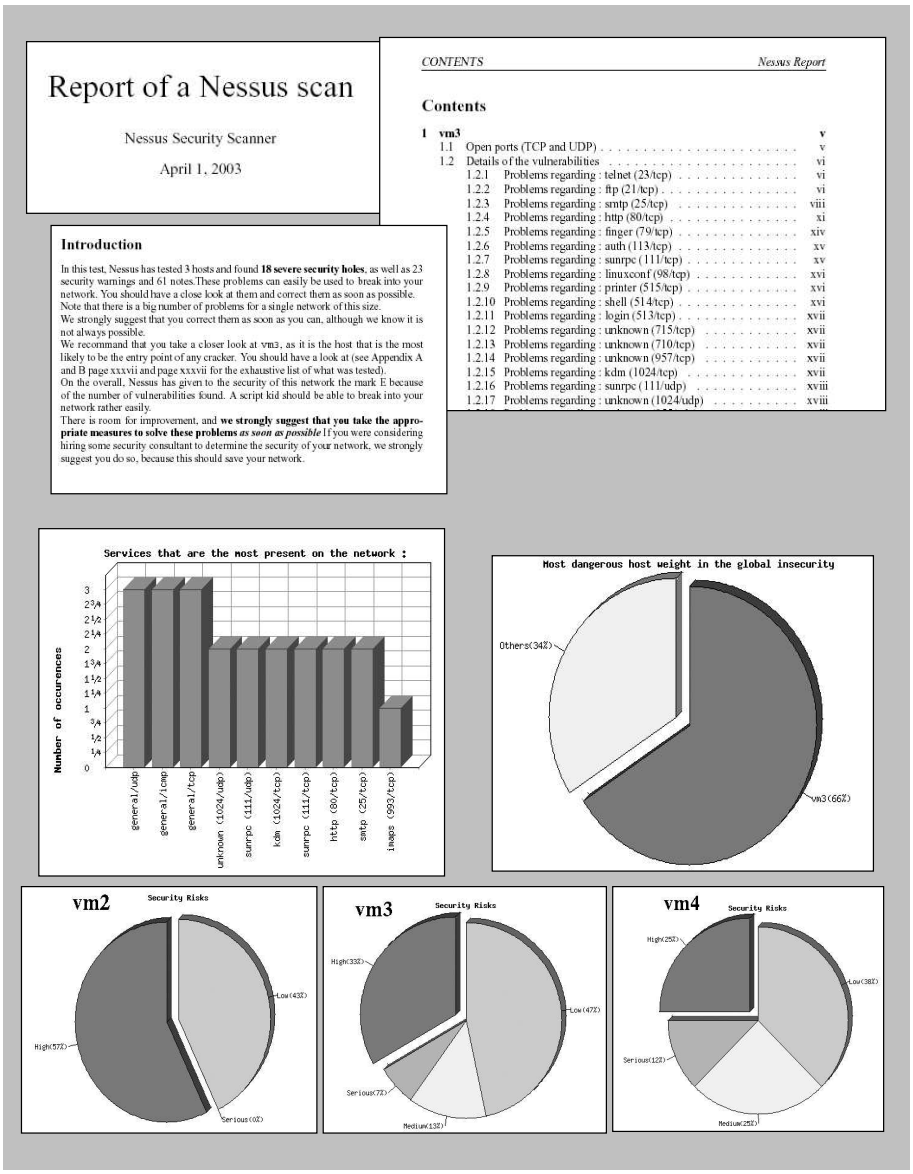
Un dels productes més utilitzats actualment com a escàner de vulnerabilitats basat en xarxa és Nessus.

Nessus és una eina basada en un model client-servidor que compta amb el seu propi protocol de comunicació. De forma similar a altres escàners de vulnerabilitats existents, el treball corresponent a explorar i provar atacs contra objectius és dut a terme pel servidor, mentre que les tasques de control i presentació de les dades són gestionades pel client.

Nessus ...

... és un escàner de vulnerabilitats de xarxa desenvolupat sota el paradigme de *software* lliure, llicenciat inicialment sota llicència GPL (*General Public Llicense*) de GNU i actualment sota llicencia LGPL (*Lesser General Public Llicense*) de GNU. Va ser desenvolupat per *Renaud Deraison* a l'any 1998. El seu precursor va ser SATAN, un altre escàner de vulnerabilitats de xarxa, desenvolupat per *Wietse Venema* i *Dan Farmer*. Vegeu la pàgina web `www.nessus.org` per a més informació.

La següent figura mostra un exemple d'informe reportat amb nessus:



5.4. Sistemes de decepció

Fins el moment, els mecanismes de seguretat que hem vist pretenen abordar el problema de la seguretat d'una xarxa des d'un punt de vista defensiu. El problema d'aquest apropament és que és purament defensiu i només és l'intrús qui ataca.

Com a novetat, aquests nous elements de seguretat (els sistemes de decepció) tractaran de canviar les regles del joc, oferint la possibilitat de prendre la iniciativa.

Els sistemes de decepció, en comptes de neutralitzar les accions dels atacants, utilitzen tècniques de monitorització per a registrar i analitzar aquestes accions, tractant d'aprendre dels atacants.

Malgrat que en alguns països no estan clarament definits els aspectes legals d'aquests sistemes, el cert és que cada vegada són més utilitzats.

A continuació tractarem de resumir les diferents estratègies que es poden emplear a l'hora de construir aquest tipus de sistemes.

5.4.1. Equips de decepció

Els equips de decepció, també coneguts com a gerros de mel o ***honeypots***, son equips informàtics connectats a la xarxa a protegir que tracten d'atreure el tràfic d'un o més atacants. D'aquesta forma, els seus administradors poden veure intents d'atacs per a entrar en el sistema i veure com es comporten els elements de seguretat implementats a la xarxa.

Un altre dels objectius es l'obtenció d'informació sobre les eines i coneixements necessaris per a realitzar una intrusió en entorns de xarxa com els que pretenem protegir. Tota aquesta informació acabarà servint per a detenir futurs atacs a la resta dels equips de producció.

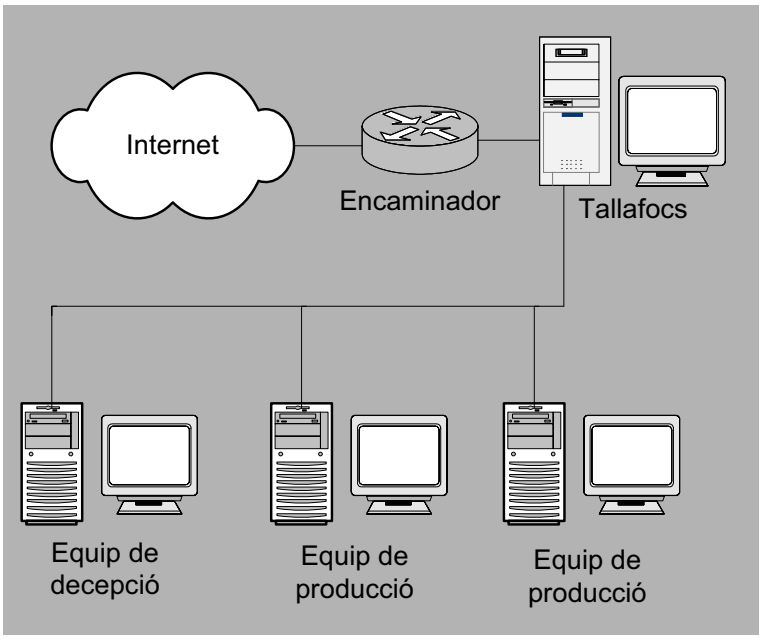
La idea conceptual d'un equip de decepció existeix des de fa diverses dècades. Com a primera aproximació podríem definir-ho com un recurs de la xarxa dissenyat per a que diferents atacants puguin introduir-se en ell de forma senzilla.

Aquests equips acostumen a estar dissenyats per a imitar el comportament d'equips de producció per tal d'aconseguir ser d'interès per a una comunitat d'atacants.

Solen comptar amb mecanismes de prevenció per a que un atacant amb èxit no pugui accedir a la totalitat de la xarxa. Naturalment, si un intrús aconsegueix atacar l'equip, no ha de percatar-se de que està sent monitoritzat o enganyat.

Així dons, aquests equips haurien d'estar instal·lats al darrera de sistemes tallafocs configurats per a que es permeti les connexions entrants a l'equip de decepció, però limitant les connexions de sortida.

La següent figura mostra la ubicació d'un possible equip de decepció dins d'una xarxa local:



Examinant l'activitat reportada dins l'equip de decepció, serà possible identificar el problema i detectar com s'ha aconseguit la intrusió en el sistema, a més de poder reportar l'activitat desencadenada a partir d'aquest moment.

5.4.2. Cel·les d'aïllament

Les cel·les d'aïllament tenen una metodologia molt similar als equips de decepció que acabem de veure. Mitjançant l'us d'un dispositiu intermedi (amb capacitats de detecció i encaminament) tot el tràfic etiquetat com a maliciós serà dirigit cap a un equip de decepció (conegut en aquest cas com célula d'aïllament).

* En anglès, *padded cell*

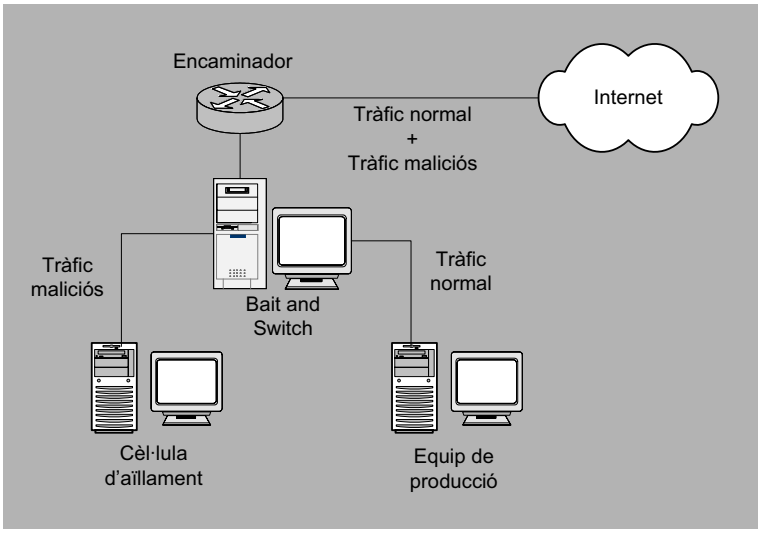
Al igual que els equips de decepció, una célula d'aïllament ofereix a l'atacant un entorn aparentment idèntic a un equip real o de producció. No obstant, al estar protegida de la resta de la xarxa, no causa danys. En la majoria de les situacions, aquestes cel·les d'aïllament són còpies exactes dels sistemes de producció reals cap al que va dirigit el tràfic maliciós, proporcionant d'aquesta forma un escenari més creíble.

Al igual que els equips de decepció, les cel·les d'aïllament poden utilitzar-se per a comprendre millor els mètodes utilitzats pels intrusos.

Bait and Switch ...

és un exemple d'eina per a la implementació de cel·les d'aïllament. Es tracta d'una utilitat que s'instal·larà en un dispositiu amb tres interfícies de xarxa i que encamina el tràfic hostil cap a la cel·les d'aïllament, basant-se en la utilització de `snort`, `iproute2`, `netfilter` i códi propi de l'aplicació.

La següent figura mostra un esquema senzill d'una cel·la d'aïllament mitjançant el producte *Bait and Switch*:

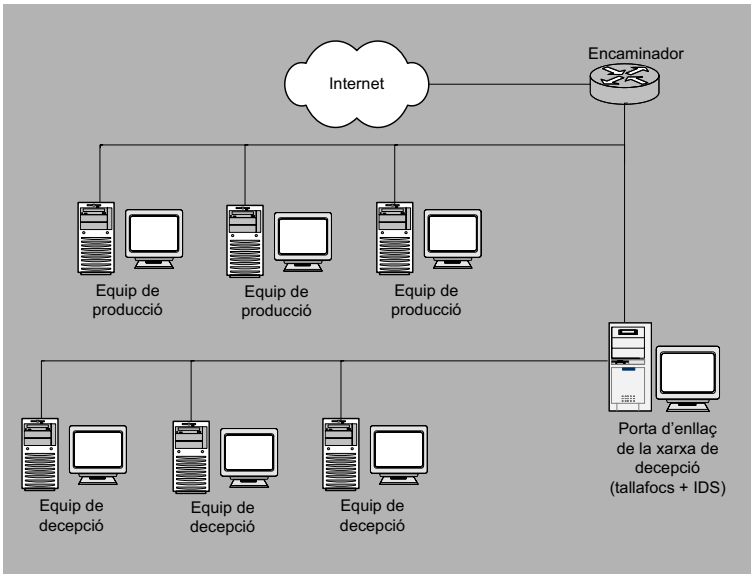


5.4.3. Xarxes de decepció

Un enfocament més avançat als anteriors consisteix en la construcció de tot un segment de xarxa composat únicament per equips de decepció, preparats tots ells per a enganyar als intrusos (permetent el seu accés sense massa dificultats).

Els equips d'aquest segment oferirien serveis configurats de tal manera que atreurien l'atenció a tota una comunitat d'intrusos per tal d'enregistrar tots els seus moviments per la xarxa de decepció.

La següent figura mostra un possible esquema per a la construcció d'aquest tipus de xarxes:



Com es pot veure a la figura anterior, una passarel·la (que combina al seu interior elements de detecció i de prevenció) uneix la xarxa de decepció amb la xarxa de producció.

Aquesta passarel·la funciona de manera similar a un pont, de manera que es podrà prescindir de direcció IP, reduint les possibilitats de detecció per part dels atacants.

Tots els sistemes instal·lats dins d'una xarxa de decepció haurien de ser sistemes de decepció i, a poder ser, el més realistes possible. Es a dir, haurien de ser sistemes i aplicacions reals, com les que podem trobar en qualsevol equip de producció.

Al no trobar en aquests sistemes de decepció serveis simulats, totes les conclusions extretes de la investigació podran ser extrapolades directament a una xarxa de producció real. Així, totes les deficiències i debilitats que es descobreixin dins d'una xarxa de decepció seran les mateixes que existeixen en la majoria d'organitzacions actuals.

El funcionament de la xarxa de decepció es basa en un sol principi: tot el tràfic que entra a qualsevol dels seus equips s'ha de considerar sospitós.

A través dels mecanismes de detecció instal·lats a la passarel·la es realitzarà el procés de monitorització, detectant atacs basats en tendències o estadístiques ja conegudes. No obstant això, les possibilitats d'investigar tota l'activitat d'una xarxa de decepció hauria ajudar a detectar atacs desconeguts.

Les xarxes de decepció han de ser vistes com eines d'investigació per a millorar la seguretat de les xarxes de producció. Són una solució molt valuosa si una organització pot dedicar-hi el temps i els recursos necessaris.

5.5. Prevenció d'intrusions

*En anglès, *Intrusion Prevention Systems* (IPS)

Els **sistemes de prevenció d'intrusions*** són el resultat d'unir les capacitat de bloqueig dels mecanismes de prevenció (filtres de paquets, passarel·les, etc.) amb les capacitats d'anàlisis i monitorització dels sistemes de detecció d'intrusos.

Com ja hem vist al primer apartat d'aquest mòdul didàctic, els sistemes de detecció d'intrusions poden ser sistemes de seguretat reactius i proactius. Però generalment, els productes de detecció més ampliament implantats acostumes a ser més reactius, es dir, esperen a que tingui lloc un atac per a emetre una alarma. Pel contrari, els sistemes de prevenció d'intrusions son sistemes amb capacitat de detenir un atac abans de que aquest pugui arribar a causar danys.

** Vegeu l'article *Intrusion Prevention Systems: the Next Step in the Evolution of IDS* que trobareu a la plana web `www.securityfocus.-com/infocus/1670` per a més informació.

La major part d'especialistes consideren que aquests sistemes de prevenció són un cas especial de sistema de detecció d'intrusos, ja que ambdós sistemes comparteixen la mateixa metodologia bàsica de detecció. De fet, la majoria d'experts els considera una evolució directa dels sistemes de detecció d'intrusions i inclús arriben a considerar-los com la següent generació d'aquests sistemes**.

Així doncs, el comportament d'un sistema de prevenció d'intrusos és similar al d'un sistema de detecció d'intrusos de resposta activa (aquells amb unitat de resposta capaç de respondre davant els atacs detectats), de manera que s'encarreguen de descartar o bloquejar els paquets sospitosos tan aviat com son identificats. D'aquesta forma, tots els paquets que pertanyin a una mateixa sessió sospitosa (detectada a partir dels sensors i els processadors d'esdeveniments del sistema de prevenció) seran eliminats de la mateixa forma.

Alguns sistemes de prevenció d'intrusions també contemplen la possibilitat de detectar anomalies en l'ús de protocols, com paquets manipulats malintencionadament.

-* En anglès, *Host based Intrusion Prevention Systems* (HIPS).
-** En anglès, *Network based Intrusion Prevention Systems* (NIPS).

Atenent a la font de dades que utilitzin, els sistemes de prevenció d'intrusions podrien classificar-se en les dues mateixes categories que la major part dels elements de detecció que hem vist fins ara: basats en màquina* i basats en xarxa**.

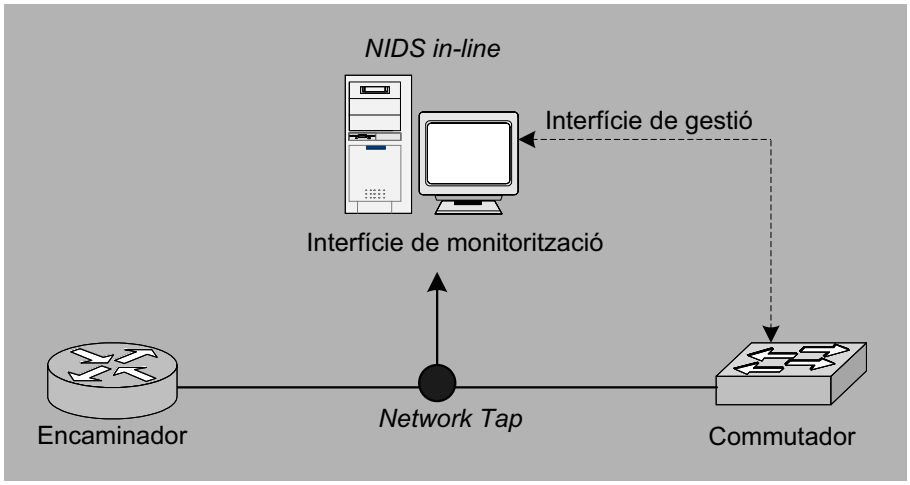
En el primer cas, els sistemes de prevenció d'intrusos basats en equip (HIPS) solen utilitzar aplicatius instal·lats directament en la màquina a protegir. Aquests aplicatius acostumen a estar molt relacionats amb el sistema operatiu del sistema i els seus serveis. El segon grup, sistemes de prevenció d'intrusos basats en xarxa, acostumen a ser dispositius de xarxa amb al menys dos interfícies (una de monitorització interna, l'altra de monitorització externa), integrant en el mateix producte les capacitats de filtrat de paquets i motor de detecció.

A continuació farem un breu repàs sobre quatre models existents que poden permetre la construcció d'un sistema de prevenció tal i com acabem de definir.

5.5.1. Sistemes de detecció en linea

La major part dels productes i dispositius per a la monitorització i detecció d'atacs en xarxa es basen en la utilització de dos dispositius de xarxa diferenciats. Per una part, un dels dispositius s'encarrega d'interceptar el tràfic del seu segment de xarxa, mentre que l'altre s'utilitza per a efectuar les tasques de gestió i administració. En la següent figura veiem un exemple típic de dispositiu de detecció en mode d'escolta*, coneguts com a sistemes de detecció en linea:

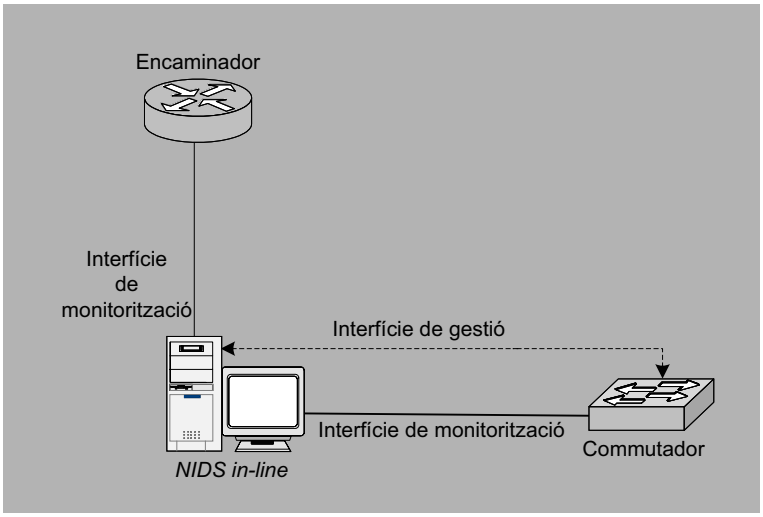
-* En anglès, *Tap Mode*.
-** En anglès, *netowork Tap*.



Al dispositiu de la figura, la interficie de xarxa utilitzada per a la monitorització està connectada a un dispositiu d'escolta** que li permet punxar el tràfic del segment de xarxa. A més, aquesta interfície no sol tenir assignada cap adreça IP, disminuint d'aquesta forma les possibilitats de ser detectat. D'aquesta forma, un sistema de detecció en linea actua a la capa de xarxa del model TCP/IP, com si d'un dispositiu pont es tractés.

Així, mitjançant una de les interficies rebrà el tràfic de l'exterior (potencialment hostil), mentre que per l'altre podrà transmetre per la xarxa a protegir. Generalment, aquests sistemes acostumen a tenir una tercera interfície per a les tasques d'administració i gestió.

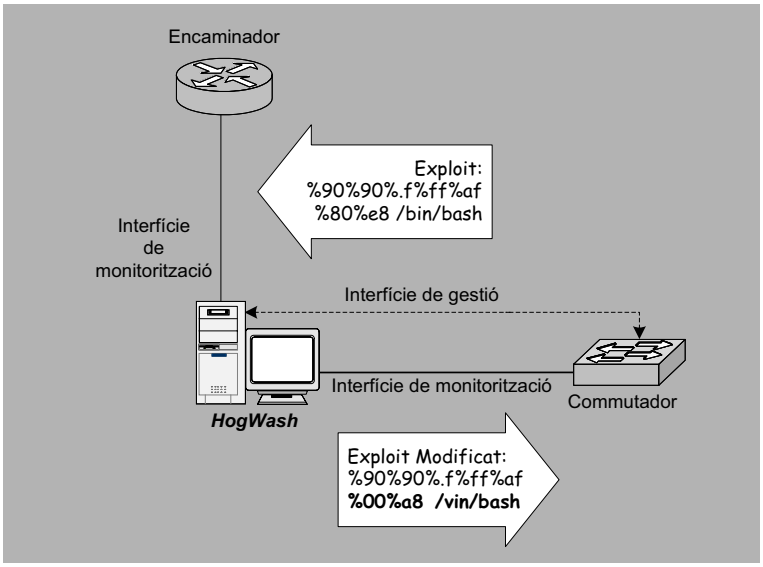
Aquesta situació li permetrà un control total sobre el tràfic que passa per els segment de xarxa on es troba col·locat. No tan sols pot analitzar tot el tràfic que rep, sinó que pot gestionar l'ample de banda.



Un dels aplicatius que pot ajudar a desenvolupar aquesta idea és l'eina *Hogwash**. Es tracta d'una utilitat de xarxa que fa servir el processador d'esdeveniments de l'eina de detecció *Snort* per tal d'anular tot aquell tràfic maliciós encaminat contra la xarxa a protegir.

* Vegeu la pàgina web `hogwash.sourceforge.net` per a més informació.

Com a eina de prevenció, l'aplicatiu *Hogwash* implementa les capacitats de detecció i bloqueig de tràfic. Addicionalment, també ofereix l'opció de reescriure el tràfic de xarxa. Així, si un atacant envia una petició maliciosa, *Hogwash* pot modificar-la abans d'encaminar aquest tràfic cap a l'altre segment de la xarxa:

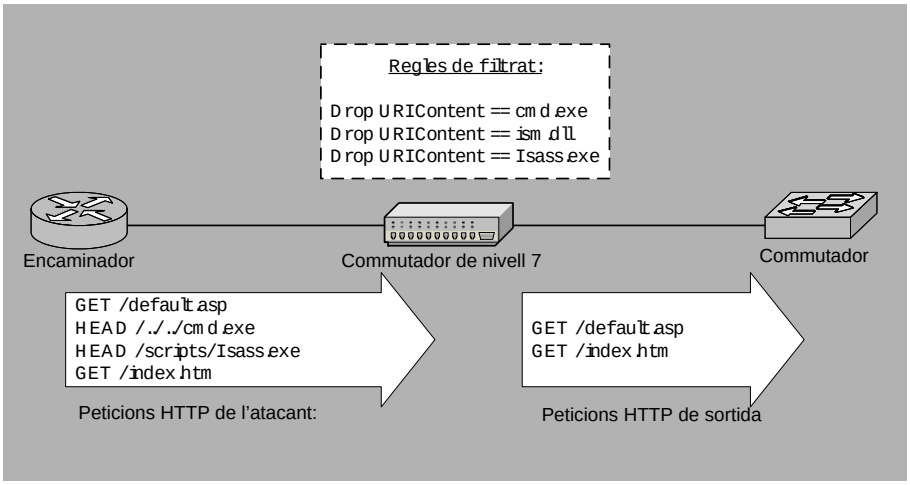


5.5.2. Commutadors de nivell set

Tot i que els commutadors han estat tradicionalment dispositius de nivell de xarxa, la creixent necessitat de treballar amb grans amples de banda ha fet que vagin guanyant popularitat els commutadors de nivell d'aplicació (nivell set del model OSI).

Aquests dispositius es solen utilitzar per a realitzar tasques de balanceig de càrrega d'una aplicació entre diversos servidors. Per a això, examinen la informació a nivell d'aplicació (per exemple HTTP, FTP, DNS, etc.) per a prendre decisions d'encaminament. Addicionalment, aquests mateixos dispositius poden proporcionar protecció davant d'atacs contra les xarxes que conmuten, com per exemple, descartar tràfic provinent d'una denegació de servei.

En la següent figura podem veure el procediment general de funcionament d'un commutador de nivell set:



El motor de detecció utilitzat per aquests commutadors de nivell set sol ser basat en detecció d'usos indeguts, implementada en la majoria dels casos mitjançant l'us de patrons d'atac. No obstant això, els atacs que millor reconeixen aquests dispositius són els atacs de denegació de servei.

Un dels primers avantatges de treballar amb aquests dispositius és la possibilitat de realitzar detecció d'atacs en xarxes d'alta velocitat commutades.

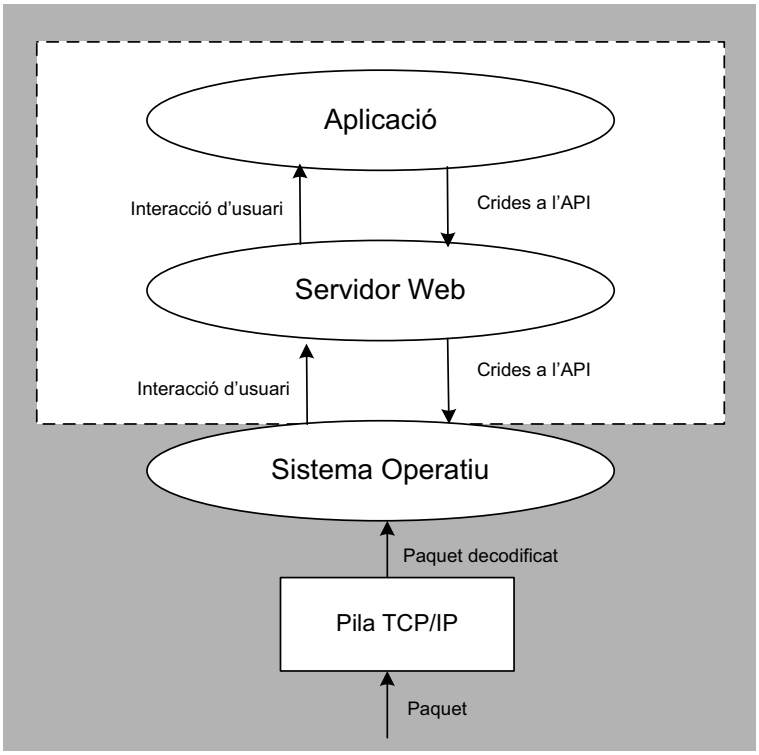
Un altre avantatge d'aquests dispositius, que no es troba en altres sistemes de prevenció, és la possibilitat de redundància. Aquesta redundància pot ser aconseguida amb la utilització de sistemes secundaris configurats per tal d'activar-se en cas de fallada per part de dispositius primaris.

5.5.3. Sistemes tallafocs a nivell d'aplicació

Els sistemes tallafocs a nivell d'aplicació, al igual que els commutadors de nivell set que acabem de veure, treballen en el nivell set del model OSI i s'instal·len directament sobre el sistema final a protegir.

A part de realitzar un anàlisi del tràfic de xarxa*, aquests dispositius poden ser configurats per analitzar esdeveniments tals com la gestió de memòria, les crides a sistema o intents de connexió.

* Vegeu el mòdul didàctic *Mecanismes de prevenció* d'aquest mateix material per a més informació.



Per a realitzar aquest tipus d'anàlisi, es basen en la utilització de perfils estadístics. Aquesta tècnica es basa en una primera fase d'inicialització de perfils (fase d'entrenament) i una segona fase on totes les accions són comparades pel sistema contra aquests perfils.

Durant la fase d'entrenament, es procedeix a registrar l'activitat de les l'aplicacions per tal d'elaborar un model de comportament que serveixi per a detectar possibles intrusions, juntament amb una sèrie de polítiques de seguretat. Així, totes les accions que no hagin estat definides durant la creació de perfils seran identificades com a malicioses pel dispositiu i podran ser bloquejades.

Dels diferents esquemes de prevenció que hem vist fins ara, aquest és l'únic que monitoritza l'activitat a les aplicacions i la relació entre aquestes i el sistema operatiu. A més, podrà ser instal·lat a cada màquina física a protegir, el que garanteix un alt nivell de personalització per part dels administradors i usuaris finals.

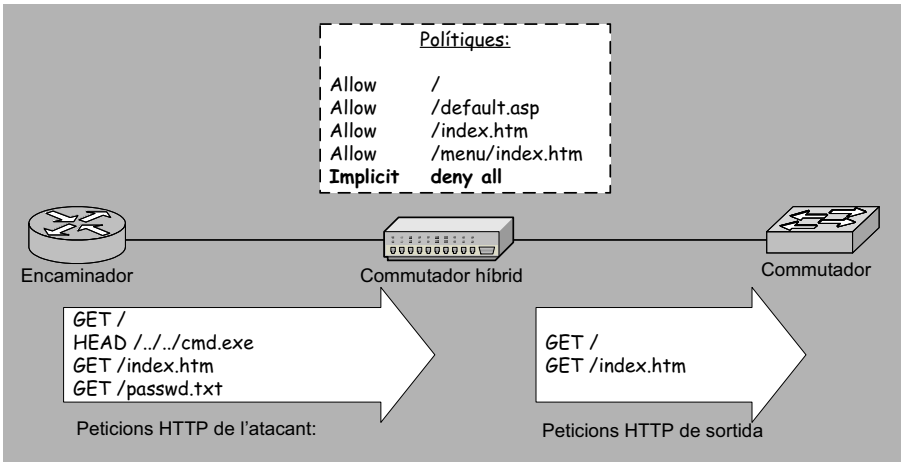
5.5.4. Commutadors híbrids

L'últim model de prevenció d'intrusos que veurem és una combinació dels commutadors de nivell set i dels sistemes tallafocs a nivell d'aplicació que acabem de veure. Així, es tracta d'un dispositiu de xarxa instal·lat com a un commutadors de nivell set, però sense utilitzar conjunts de regles.

El seu mètode de detecció es basat en polítiques, com el dels sistemes tallafocs a nivell d'aplicació. Per tant, aquests commutadors analitzaran tràfic de xarxa per tal de trobar informació definida en les polítiques que tenen configurades.

La combinació d'un sistema tallafocs a nivell d'aplicació juntament amb un commutador de nivell set permet reduir problemes de seguretat associats a una programació deficient*, així com la possibilitat de detectar atacs fins a nivell d'aplicació.

* Vegeu el capítol de *Deficiències de programació* del primer mòdul didàctic d'aquest mateix material per a més informació



Com veiem a la figura anterior, el dispositiu tindrà coneixements sobre el servidor que protegeix (servidor FTP, HTTP, SMTP, etc.), com qualsevol altre commutador de nivell set, però també tindrà coneixement sobre les aplicacions que hi ha per sobre.

Els commutadors híbrids poden ser combinats amb altres commutadors de nivell set per a reduir càrrega. Així, els commutadors de nivell set complementaris podrien redirigir únicament peticions considerades com a potencialment malicioses, per a que el commutador híbrid finalitzi la detecció.

5.6. Detecció d'atacs distribuïts

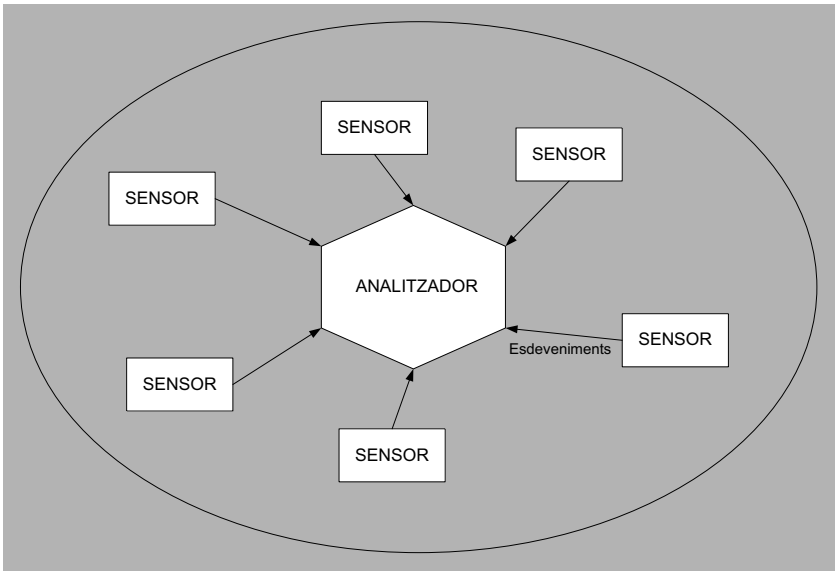
Un cas especial dins dels mecanismes de detecció és la identificació d'atacs distribuïts. Un exemple d'aquests atacs distribuïts són les denegacions de servei basades en models *mestre-esclau* que hem descrit al primer mòdul d'aquests mateixos materials. Aquest tipus d'atacs, que no poden ser indentificats cercant patrons de forma aïllada, han de ser detectats a partir de la combinació de múltiples indicis trobats en diferents equips d'una xarxa monitoritzada.

A continuació veurem, de forma molt resumida, les diferents propostes que existeixen per a poder posar en correspondència els esdeveniments recollits en diferents equips de la xarxa, a fi d'implementar una detecció d'atacs i intrusions distribuïda.

5.6.1. Esquemes tradicionals

Les primeres propostes per a extendre la detecció d'atacs des d'un equip aïllat cap a un conjunt d'equips tracten d'unificar la recollida d'informació utilitzant esquemes i models centralitzats. Així, aquestes propostes plantejen la instal·lació de sensors en cada un dels equips a protegir, configurats per a poder retransmetre tota la informació cap a un punt central d'anàlisi.

Des d'aquest punt central, tota la informació rebuda serà analitzada utilitzant diferents mètodes de detecció (detecció basada en usos indeguts, detecció basada en anomalies, etc.), tal i com veiem a la següent figura:



Aquest disseny presenta un clar problema de sobrecàrrega sobre el punt central d'anàlisi, a causa de la gran quantitat d'informació que aquest podria arribar a rebre.

La major part de les solucions existents basades en aquest esquema utilitzen esquemes de reducció d'informació (realitzant processos de prefiltrat i compressió) per a poder minimitzar aquest inconvenient.

Un **prefiltrat massiu** als propis sensors redueix el flux d'informació a transmetre cap al component central de processat. Però aquesta solució no sempre és possible, ja que existeixen situacions on es fa impossible decidir de forma local que tipus d'informació és relevant per a la detecció.

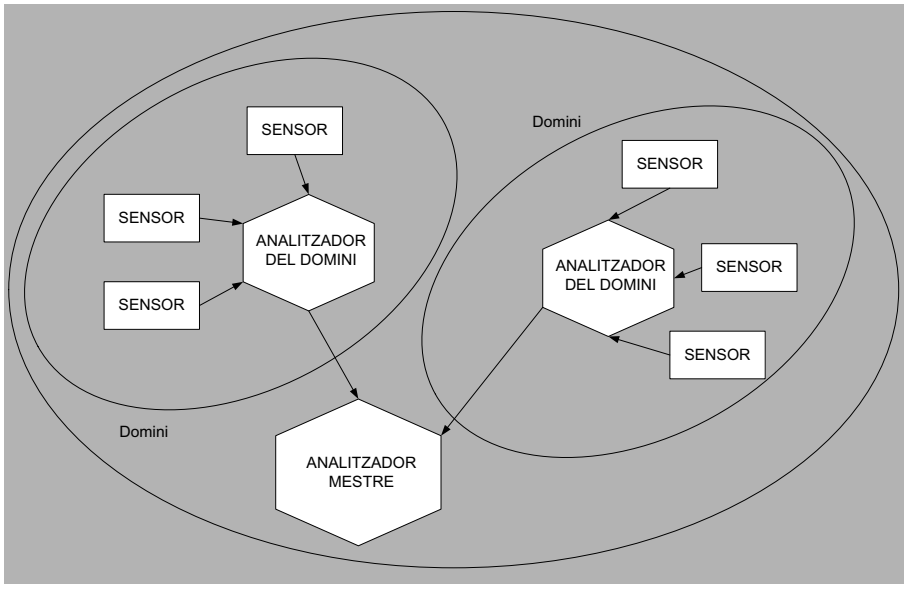
Els sistemes que segueixen aquesta proposta de prefiltrat massiu a nivell de sensor corren el risc d'altes taxes de falsos negatius, degut a la gran possibilitat d'haver descartat informació necessària en el procés de filtrat.

Per a solucionar els colls d'ampolla observats als esquemes de correlació d'esdeveniments centralitzada en xarxes de gran tamany, és necessari plantejar-se noves propostes. Però trobar un esquema de reducció d'informació eficient, capaç d'aïllar únicament informació rellevant en qualsevol tipus d'escenaris, és veritablement difícil.

Una primera forma de solucionar parcialment aquest inconvenient es mitjançant la realització d'una divisió del punt central de recollida d'informació en diferents punts de recollida, organitzats de forma jeràrquica. D'aquesta forma, tant la carrega en la xarxa, a l'enviar tots els esdeveniments a un únic punt central, com la càrrega computacional, a causa de l'existència d'un únic punt d'anàlisis, és distribuïda sobre un conjunt intermedi d'analitzadors.

Així doncs, aquesta segona proposta es basa en la utilització de nodes intermedis, dedicats a observar tota la informació rellevant d'una àrea de detecció petita i manejable. Únicament aquella informació considerada com a relevant per a la detecció global serà transmesa al node arrel.

Com veiem en la figura següent, els analitzadors intermedis examinaran esdeveniments a diferents dominis del conjunt global de la xarxa, i enviaran els seus resultats parcials a un node arrel, que tractarà de realitzar les inferències necessàries.



Encara que aquesta solució mou les decisions de prefiltrat a un nivell superior, pateix la mateixa problemàtica que la proposta centralitzada. Mentre que cada una de les àrees és monitoritzada completament, la correlació global dels seus esdeveniments pot produir una sobrecarrega o una pèrdua d'informació.

5.6.2. Anàlisis descentralitzat

Com acabem de veure, la recollida d'esdeveniments de forma centralitzada o de forma jeràrquica crea una quantitat massiva d'informació que es analitzada, en la majoria de les situacions, sota duríssimes restriccions de temps real. Ja que els diferents trossos d'informació que podrien delatar a un atac distribuït es poden trobar a qualsevol equip de la xarxa, és realment complicat poder arribar a paral·lelitzar aquest processat d'informació.

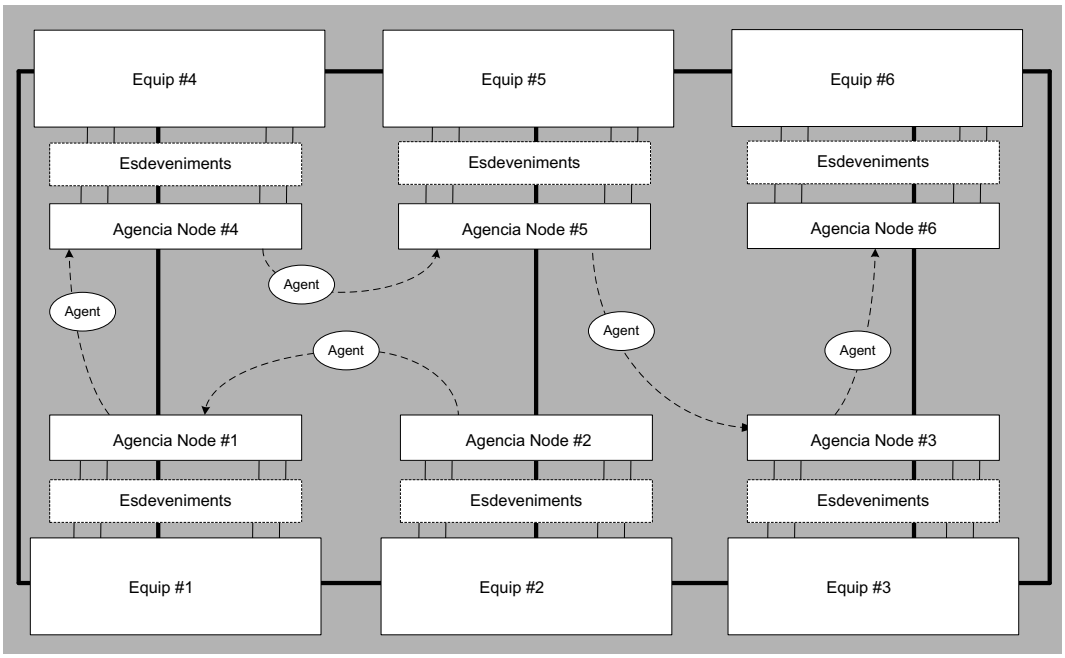
Així doncs, aquestes solucions centralitzades i jeràrquiques són vulnerables a errors o atacs deliberats contra la infraestructura de processat d'esdeveniments. En el moment en que un dels nodes centrals de processament presenti problemes, el sistema de detecció quedarà inoperatiu.

Amb l'objectiu de solucionar aquestes dificultats (inherents a la recollida per part de nodes de processat dedicats) han aparegut al llarg dels últims anys noves propostes basades en la realització d'un anàlisis descentralitzat de la informació.

Dues de les propostes per a implementar processos descentralitzats d'anàlisis d'informació són la utilització de codi mòbil per un costat, i la utilització de nodes cooperatius que realitzen un procés descentralitzat d'anàlisis mitjançant mecanismes de pas de missatges.

Anàlisi descentralitzat mitjançant codi mòbil

Les propostes basades en codi mòbil per a realitzar una detecció d'atacs distribuïts utilitzen el paradigma d'agents *software* per moure els motors de detecció per la xarxa a vigilar (en forma d'agent mòbil). A mida que aquest detectors mòbils vagin recollint l'informació que els sensors els hi oferiran, els agents aniran realitzant un procés d'anàlisi descentralitzat.



Els elements de recollida d'informació (sensors) seran aplicatius estàtics, es a dir, s'executen als equips on es produeix la recollida d'informació, s'encarregaran de fer-la arribar als agents d'anàlisis d'informació que es mouen per la xarxa.

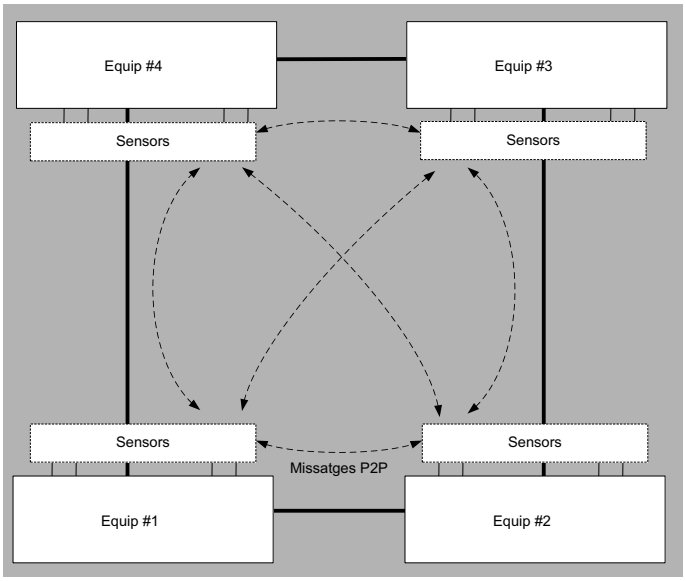
Mitjançant l'anàlisi descentralitzat realitzat per part dels agents *software* serà possible realitzar el procés de correlació d'esdeveniments i creació d'estadístiques sense necessitat d'elements centrals.

Per altra banda, i a diferència dels sistemes jeràrquics que acabem de veure, els agents poden moure's dinàmicament pel sistema, aconseguint un millor balanç de la càrrega i evasió d'atacs potencials contra sí mateixos. Quan les anomalies detectades pels agents mòbils cobreixin un nivell de sospita determinat, una sèrie d'agents reactius podrien desplaçar-se i ser enviats cap als equips involucrats per tal de neutralitzar l'atac detectat.

Anàlisi descentralitzat mitjançant pas de missatges

Al igual que la proposta anterior, aquest nou esquema tracta d'eliminar la necessitat de nodes centrals o intermediaris oferint, en comptes d'una o més estacions de monitorització dedicades (encarregades de rebre tota la informació recollida), tota una serie d'elements de control encarregats de realitzar operacions similars de forma descentralitzada.

Però a diferència de l'esquema basat en codi mòbil, aquests nous elements son estàtics i tan sols necessiten una infraestructura comuna de pas de missatges per tal de realitzar el seu procés de detecció descentralitzat.



Tan aviat com una acció que pot desencadenar en atac és detectada per un dels elements de control, aquesta serà comunicada a la resta d'elements involucrats. Així, l'informació recollida pels sensors no serà transmesa mitjançant difusió a tots els elements de control, sinó que tan sols als elements afectats o amb informació relacionada.

Resum

L'objectiu d'aquest darrer mòdul didàctic ha estat el de presentar tot una sèrie d'elements complementaris als mecanismes de seguretat tradicionals. Aquests elements no han de ser vistos com a una alternativa, si no com a un complement necessari per tal de garantir la seguretat d'una xarxa TCP/IP.

La gran quantitat de formes d'abordar el problema de la detecció d'atacs i intrusions ha donat lloc a nombroses i variades propostes i solucions. La major part d'aquestes propostes basen la seva capacitat de detecció en la recollida d'informació des d'una gran varietat de fonts d'auditoria de sistema, analitzant posteriorment aquestes dades de diferents maneres. Algunes consisteixen en comparar les dades recollides amb grans bases de dades de signatures d'atacs ja coneguts, altres en mirar problemes relacionats amb usuaris autoritzats que sobrepassen les seves accions permeses al sistema, o inclús mitjançant l'anàlisi estadístic, buscant patrons que indiquen activitat anormal i que no s'ha tingut en compte als passos anteriors.

Existeixen també mecanismes de seguretat que tracten de millorar el problema de la seguretat d'una xarxa des d'un punt de vista molt més reactiu. Tant els mecanismes de protecció de la informació, com els mecanismes de prevenció i detecció tradicionals són utilitzats per a protegir els recursos de la xarxa, detectant deficiències a la seguretat i reaccionant més tard per a solventar aquests inconvenients. Com a novetat, aquests nous elements canvien les regles del joc, oferint la possibilitat de prendre la iniciativa utilitzant tècniques de monitorització per a registrar i analitzar les accions dels atacants per tal d'aprendre dels seus coneixements.

Una tercera categoria d'elements de detecció que hem vist tracta d'unir la capacitat de bloqueig dels mecanismes de prevenció amb la capacitats d'anàlisis dels sistemes de detecció. Coneguts com a sistemes de prevenció, aquests nous sistemes son considerats com l'evolució lògica dels sistemes de detecció tradicionals.

Per últim, un cas especial de detecció es el de la identificació d'atacs distribuïts. Aquest d'atacs no poden ser detectats de forma aïllada, si no que es necessari posar en correlació múltiples indicis trobats en diferents equips d'una xarxa. Dues de les propostes més utilitzades per tal de construir sistemes capaços de detectar aquest tipus d'atacs son la utilització de nodes dedicats (mitjançant una arquitectura centralitzada o jeràrquica) i la utilització de nodes distribuïts (mitjançant una arquitectura basada en codi mòbil o mitjançant el paradigme de pas de missatges).

Glossari

escàner de vulnerabilitats: Aplicatiu que permet comprovar si un sistema és vulnerable a un conjunt de problemes de seguretat.

exploit: Aplicatiu, generalment escrit en C o ensamblador, que força les condicions necessàries per a aprofitar-se d'un error de programación que permet vulnerar la seva seguretat.

explotació d'un servei: Activitat realitzada per un atacant per tal de fer-se amb privilegis d'administrador abusant d'alguna deficiència del sistema o de la xarxa.

ocultació d'empremtes: Activitat executada per un atacant (una vegada ja produïda la intrusió) per a passar desapercebut al sistema.

política de seguretat: Resultat de documentar les expectatives de seguretat d'una xarxa, tractant de plasmar en el món real els conceptes abstractes de seguretat.

rootkit: Recopilació d'eines utilitzades en un atac d'intrusió per a garantir l'ocultació d'empremtes, garantir futures connexions, realitzar altres atacs al sistema, etc.

seguretat perimetral: Seguretat basada tan sols en la integració a la xarxa de sistemes tallafocs i altres mecanismes de prevenció.

tallafocs: Element de prevenció que realitzarà un control d'accés per tal de separar la nostra xarxa dels equips de l'exterior (potencialment hostils). En anglès, *firewall*.

vigilància d'una xarxa: Activitat realitzada per l'atacant tractant d'aprendre tot el que pugui sobre la xarxa que vol atacar, especialment serveis vulnerables i errors de configuració.

Bibliografia

[1] Northcutt, S. (2000). *Network Intrusion Detection. An analyst's handbook.* New Riders.

[2] Proctor, P. E. (2001). *The practical intrusion detection handbook.* Prentice-Hall.

[3] Spitzner, L. (2001). *Honeypots: Tracking Hackers.* Addison-Wesley.

[4] González, D. (2002). *Sistemas de Detección de Intrusiones.* .

[5] Cheswick, W. R.; Bellovin, S. M.; Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker, 2nd ed.* Addison-Wesley Professional Computing.