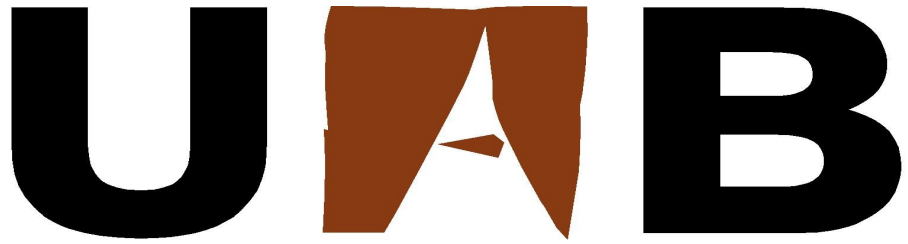

Universitat Autònoma de Barcelona

Postgrau de Seguretat en Xarxes i Sistemes

Configuració de SNORT Aplicat en un Entorn Professional

Alexandre Abat Macaya
Universitat Oberta de Catalunya
Cristina Pérez Solà
13/06/2014

Aquest projecte va dedicat:

Als meus pares, ajudant-me econòmicament i anímicament en la meva trajectòria intelectual.

Al meu germà Albert, moltes persones el donaven per perdut degut a la seva deficiència, gràcies per demostrar que amb la teva motivació, la teva dedicació i el teu esperit lluitador m'has servit de model a seguir.

A la meva parella Aina, que no només m'ha ajudat en aguantar-me durant el projecte sinó a animar-me, esbargir-me, desconectant quan tocava, i estan al meu costat quan la necessitava durant tot el curs del Postgrau de Seguretat Informàtica.

I a la família, que incondicionalment, sempre estan quan els necessites.

Resum del projecte

Aquest projecte pretén ser didacta per a qui estigui interessat en apendre sobre com utilitzar una de les eines que, probablement, formi part de les piramidals en l'arsenal d'un administrador de sistemes, el qual tingui especial cura en temes relacionats amb la seguretat informàtica.

Primer es planteja una estructuració de com atacar el problema plantejat: Utilitzar una eina de detecció d'intrusos en un entorn empresarial. Es té en compte la seva configuració, la configuració que s'ha plantejar en aquest projecte, és d'àmbit general, ja que es pot personalitzar fins a l'últim detall.

També s'explica on pot tenir cabuda un projecte d'aquestes magnituds, és a dir, definint un entorn professional, una petita empresa. Dins d'aquesta empresa es defineixen una sèrie de polítiques de seguretat, el qual recomano que es plantegin paralel·lament amb la configuració del programa. No només es tenen en compte els aspectes de seguretat tecnològics; S'han fet estudis que corroborem que més del 70% dels atacs que es puguin produir en una empresa, es produeixen en un àmbit intern, i no des de l'exterior. Així doncs convé, a més a més d'enfortir els aspectes tècnics en quant a seguretat, el comportament i la conducta humana. Restringir, limitar, o si més no, delimitar els marges d'actuació dels treballadors. És més perillós tenir un treballador descontent que no descobrir un bug específic.

Finalment es valoren eines que poden facilitar a la configuració de la eina principal, snort, i es fa una valoració sobre els resultats obtinguts a partir de les proves realitzades als laboratoris.

Índex

Índex de Figures

Capítol 1 – Introducció

1.1 Justificació del projecte i Context

Punt de partida: Detecció d'intrusions amb Snort

- Els sistemes de detecció d'intrusions (IDS) són dispositius o aplicatius que monitoritzen el tràfic de xarxa i/o les activitats d'un sistema amb l'objectiu de detectar comportaments sospitosos o maliciosos. Snort és un sistema que pot actuar tant com de detecció d'intrusions de xarxa (IDS), com de prevenció d'intrusions (IPS) en open source, que permet, entre d'altres, esnifar el tràfic d'una xarxa i generar alertes quan els paquets obtinguts indiquen que hi ha comportaments sospitosos a la xarxa.

Aquest projecte es centrarà en la detecció d'intrusions amb Snort.

1. En primer lloc, revisarem l'arquitectura de Snort així com el ventall de funcionalitats que ens ofereix.
2. Després, prepararem un escenari amb màquines virtuals que ens permetrà simular diferents atacs a una màquina objectiu.
3. Seguidament, crearem regles que ens permetin detectar tot un conjunt d'atacs sobre la màquina objectiu.
4. Finalment, realitzarem aquests atacs i comprovarem l'eficàcia de l'Snort a l'hora de detectar-los.

1.2 Objectius

- **Objectius del projecte.**
  - Portar un registre de les activitats sobre l'equip, és a dir, logar totes les accions que es facin dins i fora, contra l'equip en qüestió.
  - Crear cadenes, regles per tal d'avisar sobre possibles violacions de seguretat contra el sistema. (Tenir un control de les activitats del sistema)
  - Apendre a definir polítiques de seguretat en un sistema i saber-les aplicar en un entorn empresarial.
  - Actuar segons una plà d'actuació (protocols) en cas de violació de trencament de seguretat i aconseguir la màxima eficiència en els escenaris que es plantegin. D'aquesta manera apendre a administrar i gestionar la seguretat en un entorn real.

1.3 Enfocament i mètode

- **Problemàtica a resoldre.**

  Detectar les intrusions a un sistema configurat, per tal de minimitzar l'impacte que comporta exprimir les vulnerabilitats del sistema per tal de burlar-ne la seva seguretat.

- **Metodologia de treball.**
  - La metodología consistirà bàsicament en estudiar, primerament, el funcionament d'una eina necessària en un entorn planificat per a detectar intrusions. Seguidament es posaran exemples pràctics en el qual pot ser utilitzat aquesta eina de prevenció.

1.4 Planificació del projecte

- **Tasques a realitzar.**

Configuració del sistema de detecció d'intrusos.

- Estudiar el funcionament del programa de detecció d'intrusos snort per tal d'entendre el seu funcionament.
- Creació de regles bàsiques, o fins i tot crear-ne de més elavorades per ampliar el ventall de detecció.
- Estudi del funcionament de diferents programes maliciosos (virus, troians, portes del darrera, desbordaments de memòria…) per tal d'entendre el seu funcionament i aplicar els mètodes que s'empren en un entorn real per tal de detectar-los.
- Realització de scripts per configurar el programa i adaptar-lo a les necessitats de l'administrador.
- Afegir als logs del sistema les activitats internes en el cas d'empresa amb treballadors, és a dir, registrar moviments o accions sospitoses.
- Revisió de permisos d'usuaris i programes amb accessos a Internet.
- Revisió d'actualizacions, en què afecten al sistema operatiu, quins canvis poden afectar. Revisió de noves vulnerabilitats en les pàgines webs conegudes com per exemple http://cve.mitre.org

Política de seguretat.

- Generació d'informes per especificar possibles fallades de seguretat.
- Planificació de protocols d'actuació en cas de ruptura de seguretat i el programa snort no detectés la intrusió.
- Estudiar la manera de generar una regla automática en el moment en què es detecti alguna fallada de seguretat en el sistema.
- Definir polítiques de funcionament en els diferents servidors: Configuració dels servidor per complir una política de seguretat preestablerta, ports, connexions, firewall, usuaris...
- Estudi del servidor (www, ftp, smtp) respecte les eines a utilitzar en el servidor.
- Configurar snort per a actuar segons les polítiques de seguretat establertes.

- **Planificació temporal**

- Estudi de les configuracions del sistema de detecció d'intrusió, del seu funcionament intern... Estudi dels requeriment per a poder-lo executar en un entorn de proves consolidat, definir els sistemes, les eines a utilitzar, etc.

- Necessitats per a la creació d'un entorn empresarial, requisits per al funcionament de l'empresa (quins són els serveis a proporcionar, entorns de treball, definició de polítiques de seguretat) Això comporta la creació d'una infraestructura tant a nivell tecnològic, com a nivell piramidal en un entorn empresarial. Plantejament d'una bona política de seguretat, procediments a seguir en cas de violacions de seguretat en el sistema, actuar en cas que falli algun filtre (Sistema de notificacions al mòbil, al correu...).

- Es definiran les polítiques de seguretat i d'actuació de l'empresa havent creat prèviament la infraestructura de l'empresa a nivell de tecnologies i d'empresa. Configuració de les diferents estacions de treball (virtuals) per a provar el funcionament.

- Posar a prova les polítiques de seguretat (atacar l'entorn amb fins educatius, eines a utilitzar, programes maliciosos, escaneig de vulnerabilitats...), analitzar el funcionament de les polítiques, definir solucions per a reduir amb el mínim impacte el risc de vulnerabilitats (Aqui entra la definició de creació de regles automàtiques, generació de scripts per avisar als administradors)

- Desenvolupament de les conclusions resultants obtingudes a partir de la realització de les proves en els entorns virtuals. Replanificació d'una política de seguretat i plà d'actuació en cas de catàstrofe en el plantejament d'aquest esdeveniments. Així doncs reforçar de manera correcte, havent comprovat el plantejament inicial (si era erroni) mitjançant les proves a realitzar, el replantejament tant de polítiques de seguretat, com de plans d'actuació en cas de violació de seguretat.

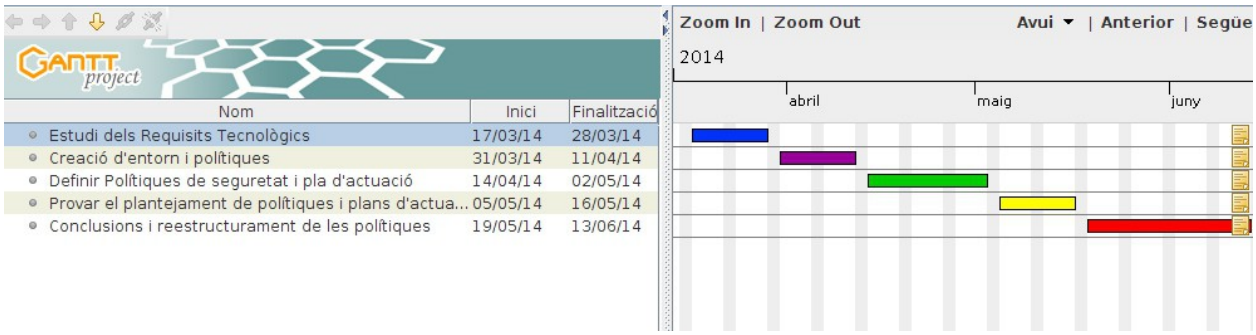

Figura 1.0

Capítol 2 – Especificacions

2.1 Arquitectura de Snort

Abans d'instal·lar el programa i configurar Snort, és important conèixer els elements que el componen. Els elements que componen l'esquema bàsic de la seva arquitectura són:

•Mòdul de captura del tràfic:
L'encarregat de capturar tots els paquets de la xarxa utilitzant la llibreria libpcap.

•Decodificador
S'encarrega de formar les estructures de dades amb els paquets capturats i identifica els protocols d'enllaç, de xarxa, etc.

•Preprocessador
Permeten extendre les funcionalitats preparant les dades per la detecció. Existeixen diferents tipus de preprocessadors depenent del tràfic que volem analitzar (per exemple, existeixen els preprocessadors http, telnet...)

•Motor de Detecció
Analiza els paquets en base a les regles definides per detectar els atacs. Disseny i optimització d'un sistema d'intrusió hibrid.

•Arxiu de Regles
Defineixen el conjunt de regles que regeixen els anàlisis dels paquets detectats.

•Plugins de detecció
Parts del software que són compilats amb Snort i s'usen per modificar el motor de detecció.

•Plugins de sortida
Permeten definir què, com i on es guarden les alertes i els corresponents paquets de la xarxa que les generàren. Poden ser arxius de text, bases de dades, servidors syslog, etc.

2.2 Creació d'una petita empresa

2.2.1 Oferta de Serveis

Empresa *In4Matics*

Els serveis a proporcionar per l'empresa són els següents:

-Desenvolupament d'aplicacions adaptats a les necessitats del client.
-Consultoria informàtica.
-Muntatge de servidors per a petites i mitjanes empreses (Pymes).
-Disseny, desenvolupament i configuració d'aqruitectures de xarxa.
-Administració de Base de Dades.

-Còpies de Seguretat programades.
-Auditories de seguretat.
-Desenvolupament d'informes per tal de proporcionar un servei per identificar possibles males configuracions o deficiència de seguretat en els serveis que es proporcionen.
-Enfortiment dels serveis en quant a la seva seguretat.

L'empresa de cara al públic presenta una pàgina web amb tots els serveis disponibles descrits anteriorment, es pot sol·licitar un pressupost calculat “online” de les peticions demanades a través d'aquesta pàgina.
Aquesta pàgina conté una base de dades (Un servidor web, amb un servidor d'on agafa les dades per tal de subministrar serveis de venta d'equips informàtics, software adaptat a les necessitats dels client, muntatge d'arquitectures de xarxa per a les empreses, factures generades per contabilitzar els productes).

2.2.2 Organització de l'empresa

Departament comercial, el qual genera les ofertes pels diferents clients o en proporciona un pressupost per tal de saber si s'ajusta a les necessitats, prèviament trobades a través de les auditories de seguretat per “sorpresa”
Departament d'investigació i desenvolupament (I + D) (part de programació, i donar suport en cas d'incidències en el programari venut). També investigació en trobar nous fallos de seguretat per tal d'informar a les empreses contractades l¡opció d'actualitzar programari o serveis contractats.
Departament d'incidències (suport o helpdesk) per tal d'ajudar als dubtes segons els programes desenvolupats pels clients contratats.

2.2.3 Procés de producció d'un programari/arquitectura

Sol·licitud del client, pas per als desenvolupadors de I+D o per als de IT (segons si es tracta d'un projecte de software o d'implantació d'una infraestructura), un pic s'ha generat la documentació d'especificacions del projecte, es passa a comercial per a que pressupostin el projecte. Presentació del projecte a client, això pot significar que accepti el projecte amb les especificacions inicials, o que es comenci el procés d'ajustament de les necessitats del client a especificacions tècniques, aleshores comença un procés de disseny (cap de I+D) amb especificacions tècniques modificades amb un reajust a les necessitats reals segons el mercat actual. Així doncs comença el procés de producció i fabricació del producte segons les especificacions tècniques. Una vegada finalitzada la producció del producte si el client presenta una sol·licitud per falta de gratitud amb el producte, es passaria al procés de reajust del producte per tornar a la fase d'aplicació del producte (producció i fabricació del producte), o si ho sol·licités, donar formació per utilitzar el producte i finalment suport per fallos de programa o ajut en l'enteniment.
Paral·lelament a la finalització del producte es seguirà amb un manteniment del producte fent diverses auditories de seguretat periòdicament, actualitzant la versió si s'escau.

2.2.4 Política de seguretat de l'empresa

1. Primerament es faran consultes diàries a les vulnerabilitas conegudes i que apareguin al llarg de la setmana.

1.1. Si es trobés que algun client li afecta alguna fallada de seguretat, comunicar-li immediatament, fent-li saber que s'està treballant per intentar resoldre la fallada en qüestió.

1.2 Mirar si existeix algun parxejat per tal de corregir els errors detectats.

1.3 En cas de no trobar momentàniament una solució immediata al problema de seguretat, si les dades confidencials no es veiguessin alterades, manipulades o modificades, es farien còpies de seguretat diàries, i intentar no subministrar el servei a través de l'aplicació afectada, o servei en concret.

1.4 Depenent del tipus de vulnerabilitat que s'hagi trobat, i en quins sistemes afecta sota quin tipus de versions en concret, es definiran unes polítiques de reacció “en calent” per tal de trobar una solució momentània (Si fos instal·lar una versió més recent, com en el cas recent al de Heartbleed, d'instalar una versió superior a la 1.0.1 del OpenSSL, s'aplicaria el partxejat immediatament)

2.2.5 Estructuració piramidal de l'empresa

2.[1] Es definiran diferents tipus de rols per a l'empresa, és a dir: Pel departament comercial existiran el rol de **comercial**, i **cap de comercial**, el qual el rol de comercial crearà les ofertes i les deixarà pendents de validar en una llista pendent. El cap de comercial les validarà en el cas que siguin grans ofertes, o superin una quantitat establerta.

Existirà el rol de **desenvolupador** i **cap de I+D,** el qual desenvoluparan les aplicacions per als clients que ho necessitin. El cap és qui organitzarà i estructurarà el software necessari per a posar i dur a terme l'aplicació, quines tecnologies seran necessàries per a tirar endavant el projecte (el qual estudiarà el departament de IT i ajustar-se a les necessitats/requeriments i proporcionar la millor solució sense sortir de l'àmbit i tecnologies demanades), sol·licitant d'aquesta manera un pressupost, aplicant un timing de duració del projecte (ja sigui de software, com d'implantació d'una arquitectura per muntar una infraestructura a nivell de IT, oragnització d'un servidor de base de dades, etc) i posant una sèrie d'entregues per portar un cert control en cada projecte.

Internament també existirà el departament de IT, el qual demanarà al departament de comercial tot el material necessari per tal de muntar les infraestructures sol·licitades pels clients, fins i tot les infraestructures internes, o la petició de material informàtic per a l'empresa. També en aquest cas existiria el rol de **tècnicIT** i **cap de IT.**

Per tal d'acceptar un projecte, amb el que implica presentar la documentació amb les especificacions tècniques de les necessitats tecnològiques, la planificació de desenvolupament software o d'implantació d'una infraestructura, l'ha de validar el **cap de producció**

També tindrem un departament de magatzem, el qual es guardaràn peces de recanvi en cas de necessitar amb urgència algun dels material, amb el que comporta mantenir una base de dades per tal de conservar i tenir a l'abast les peces del magatzem, actualitzant l'stock en cas que en falti, o demanar-ne a través dels proveidors.

Les interaccions entre departament es farà sempre a través dels caps de cadascun dels departaments, així doncs si un comercial vol comunicar una oferta a un desenvolupador, haurà de

1. El rol bàsic de cada cap de departament serà validar els projectes proposats, compres sol·licitades, etc, per cadascun dels rols inferiors de cada un dels departaments.

passar a través del cap de comercial, seguidament pel cap de I+D, i finalment arribarà al desenvolupador en concret. Si el procés es fes per correu electrònic, s'hauria d'adjuntar al correu els caps respectius per tal de mantenir-los informats.

3. Per a cada infraestructura muntada, tenir un sistema per registrar les entrades als servidors i es sospiti si s'està intentant vulnerar la seguretat del sistema. És a dir un sistema per logejar tots el moviment en el sistema, ja siguin interns o externs (si més no tenir controlats els moviments sospitosos i informar en el cas de detectar-ne algun)
4. Les contrasenyes dels usuaris estaran guardades en una base de dades de l'empresa, només les coneixeran les persones a les quals pertanyin.
5. Les contrasenyes es guardaran encriptades, i no es guardaran mai en paper.
6. Els ordinadors es tancaran automàticament a l'hora predeterminada el qual s'hagi especificat, per exemple a les 8 de la tarda.
7. En cas de necessitar dels serveis d'una màquina de l'empresa durant fora l'horari de la oficina per tal de solucionar algun problema amb algun client, s'haurà de presentar una sol·licitud al cap del departament, al cap del departament de IT, i al gerent de l'empresa per tenir-ne constància.
8. Si es treballa fora de l'horari d'oficina, redactar un informe per tal de registrar el que s'ha desenvolupat durant les hores extraordinàries, al que ha afectat o si s'ha solucionat alguna incidència.
9. Existirà un rol universal que pertenyarà al tècnics que portin un projecte en concret, el qual adquirirà el rol d'administrador per tal d'administrar el software, la infraestructura, etc, per si es detecta alguna incidència i es necessiti d'algun servei amb certs coneixament o solucionar algun problema.
10. Si hi ha alguna incidència en algun projecte d'algun client, s'ha d'informar al responsable més directe (cap de projecte), així en tindran coneixament el treballador de l'empresa externa, el seu cap directe, el cap del departament de la nostre empresa i el personal el qual hagi portat a terme el projecte en qüestió. Bàsicament que si hi ha d'haver algun canvi (ja sigui esborrat de dades, manipulació d'usuaris, altes/baixes d'usuaris, recuperació de correus esborrats...), han de tenir coneixament els caps respectius sobre aquests canvis, si es que no són ells mateixos els qui ho efectuen.

11. La política de seguretat de base de dades:

11.1. Es faràn backups diferencials diaris per tal de registrar els canvis efectuats sobre la jornada en qüestió, així com els correus, pressupostos, contrasenyes, bases de dades, etc.

11.2. El cap de setmana es farà una còpia de seguretat complerta de tot el material de l'empresa.

11.3 Es guardaran les còpies de com a molt un mes d'antelació, depen la importància de les dades, s'incrementarà el temps de mantenir les dades guardades durant més temps o no.

11.4. Per a les empreses s'elaborarà i es confirmarà la política de seguretat parlant directament amb el departament del client el qual afecti directament la implementació del projecte o de la infraestructura a muntar.

2.2.6 Serveis de polítiques de seguretat a clients

Un dels serveis a oferir és plantejar una política de seguretat com a servei i uns procediments a seguir per als treballadors, en temes relacionats com les contrasenyes (com les han d'emmagatzemar), els equips de treball (apagant-se a una hora determinada). Les còpies de seguretat és un tema que s'ha de parlar amb el cap de l'empresa client, per tal d'establir i definir una funcionalitat viable, eficient i eficaç tant a l'hora de guardar les dades com restaurar-les, registrar els moviments dels usuaris en logs al sistema, limitar els accessos i només donar els permisos necessaris per a desenvolupar les tasques necessàries, ja existirà algú amb rols més elevats per a realitzar tasques de més responsabilitat i el responsable del projecte dins la nostra empresa amb els rols màxims per quan sigui necessari.

2.2.7 Laboratoris de l'empresa

Laboratoris Inf4Matics

Aquest apartat està orientat a definir uns laboratoris per tal de testejar les diferents aplicacions sobre un entorn de proves, en el cas de desenvolupar alguna aplicació per algun client.
També servirà per estudiar la robustositat de les diferents arquitectures plantejades per als diferents clients i trobar una millor solució per oferir sense necessitat d'instal·lar pegats a la primera de canvi. És a dir fer un estudi previ, o si més no, generar informes definint quines tecnologies són adequades depenent de les necessitats dels clients i afegint, si existeix, alguna dependència o vulnerabilitat coneguda. En el cas de detectar-ne una, trobar alguna alternativa si fós possible.
Bàsicament els laboratoris serveixen per fer proves dels entorns a instal·lar, així es provaran i es detectaran errors potencials, o vulnerabilitats amagades.
En cas de detectar una vulnerabilitat el procediment a seguir és:

1. Mirar si aquella vulnerabilitat ja ha sigut descoberta per alguna de les pàgines conegudes que proporcioni aquest tipus d'informació.
2. En cas de no existir a la base de dades de les pàgines web conegudes, seguir el procediment d'identificació CVE i obtenir una puntuació aproximada de la perillositat de la vulnerabilitat, així poder pendre unes decisions depenent del grau de perill.

Capítol 3 – Fases de snort

3.1 Apostar per snort és viable

Asumirem que executarem les proves en un entorn: **GNU/Linux Debian versió: 3.7.2**

uname -a
Linux ********* 3.7-trunk-686-pae #1 SMP **Debian 3.7.2-0+kali8 i686** GNU/Linux

El que es pretendrà mitjançant aquesta entorn de pràctiques serà explicar la configuració bàsica que ha de tenir un sistema per tal de tenir un detector d'intrusions, com és snort, funcionant en ple rendiment i detectant les possibles infraccions per factors tant externs com interns en un sistema.

Per a poder dur a terme una bona configuració, no només s'ha de tenir un detector d'intrusions activat en el sistema, si no que és una èina adicional per tal de facilitar la feina a l'administrador del sistema i tenir controlat els punts més febles, o si més no crítics d'un sistema en qüestió. Això significa que 'snort' és una eina de recolzament per fortificar un sistema, però aquesta eina no implica l'eliminació de virus, troians... Aquesta eina els detectarà si estan definits a les regles, per això s'ha de tenir especial cura a definir-les de manera correcte.

A l'hora de posar un servei a l'abast de tothom, és a dir, Internet, s'ha d'anar amb cura quan s'obren els ports lligats a aquest programes, que en proporcionaran una funcionalitat al client final amb un objectiu definit, és a dir, si tenim un servei de compartició de fitxers en Linux, com pot ser un NFS, hem de saber que hem d'obrir el port associat a aquest servei, en aquest cas el 2049, i no només posar un firewall darrera per evitar virus, troians, etc a través d'aquesta porta oberta a possibles amenaces, encara es pot acotar més el filtratge del trafic entrant i sortint. Per exemple, podem definir una política DROP en el firewall per tal de denegar l'entrada a adreçes IP desconegudes i només donar permís a aquelles adreçes que ens interessin o vulguem.

On es vol arribar a parar amb tota aquesta explicació? Ben senzill, el nivell de seguretat en un sistema depèn de la actitud que prenem i el metòdics que arribem a ser. També hem de tenir en compte la criticitat del sistema per aplicar una restricció més estricte i crítica, o més permisiva. Podem establir que la millor manera de dur a terme una idea de restricció segons els criteris anomenats anteriorment (necessitat de servei i criticitat del sistema) es pot definir una metodologia de treball. El fet de publicar un servei a l'abast a tothom qui ho vulgui o necessiti, implica seguir una sèrie punt seqüencials.

1. Instal·lació i configuració de serveis en el runlevel i fer-los permanents amb chkconfig.
2. Configuració del firewall tenint en compte la funcionalitat del serveis (Respectant ports entrants i sortints)
3. Configuració del programa de detecció d'intrusos.
4. Instal·lació de regles bàsiques per a snort.
5.Configuració de regles per a detectar possibles amenaces a través d'un servei determinat.
6. Processos d'automatització de regles per a un sitema determinat.

7. Eines addicionals.

3.2 Instal·lació de snort i configuració del Firewall

3.2.1. Instal·lació i configuració de serveis en el runlevel i fer-los permanents amb chkconfig.

Abans de posar-nos a configurar un servei determinat, o configurar el seu script en el nivell d'execució determinat, haurem de comprovar si es troba a la nostre disposició en el nostre sistema, és a dir, si està instal·lat. En cas afirmatiu procedirem a la seva configuració, en cas negatiu ens haurem de descarregar el paquet que en proporcioni el servei.

Seguint l'exemple anterior de compartició de fitxers, haurem de comprovar si tenim en el nostre sistema el paquet que administra la gestió de fitxers compartits a través de la xarxa (NFS).

Per tal de buscar si el paquet es troba instal·lat al nostre sistema, executarem la següent comanda a la terminal:

dpkg -l | grep <patró_de_búsqueda>

```
_.:{ Rasta@~ [dl mai 12]}:._ -> $ dpkg -l | grep nfs
ii  libnfsidmap2:i386                          0.25-4                 i386         NFS idmapping library
ii  nfs-common                                 1:1.2.6-4              i386         NFS support files common to cl
ient and server
ii  nfspy                                      0.2.1-1kali1           all          ID-spoofing NFS client
```

Figura 3.0

Si obtenim una coincidència amb el paquet (com es el nostre cas, només ens faltaria el paquet nfs-kernel-server si volguessim que funcionés com a Servidor), és que existeix al nostre sistema, del contrari l'haurem de buscar primerament mitjançant la comanda:

apt-cache search <patró_de_búsqueda>

```
_.:{ Rasta@~ [dt mai 13]}:._ -> $ apt-cache search nfs
daemonfs - real time monitoring software
fai-nfsroot - Fully Automatic Installation nfsroot package
fam - File Alteration Monitor
hydra - very fast network logon cracker
hydra-gtk - very fast network logon cracker - GTK+ based GUI
jftp - Java GUI client for FTP, SMB, SFTP and NFS
libfile-nfslock-perl - perl module to do NFS (or not) locking
liblockfile1 - NFS-safe locking library
libnfs-dev - NFS client library (development files)
libnfs1 - NFS client library (shared library)
libnfsidmap-dev - header files and docs for libnfsidmap
libnfsidmap2 - NFS idmapping library
libyanfs-java - Yet Another NFS - a Java NFS library
manpages-pt - Portuguese Versions of the Manual Pages
manpages-tr - Turkish version of the manual pages
mb2md - Converting Mbox mailboxes to Maildir format
nfs-common - NFS support files common to client and server
nfs-kernel-server - support for NFS kernel server
nfs4-acl-tools - Commandline and GUI ACL utilities for the NFSv4 client
nfspy - ID-spoofing NFS client
nfswatch - Program to monitor NFS traffic for the console
nmon - performance monitoring tool for Linux
python-flufl.lock - NFS-safe file-based lock with timeouts (Python 2)
python-flufl.lock-doc - NFS-safe file-based lock with timeouts (common documentation)
python3-flufl.lock - NFS-safe file-based lock with timeouts (Python 3)
ruby-lockfile - create NFS-safe lockfiles
sbrsh - Scratchbox Remote Shell client
sbrshd - Scratchbox Remote Shell daemon
task-file-server - File server
unionfs-fuse - Fuse implementation of unionfs
```

Figura 3.1

Si volguessim instal·lar el paquet, éssent superusuari, seguirem amb la següent comanda:

```
$ su
$ apt-get install <patró_del_paquet>
```

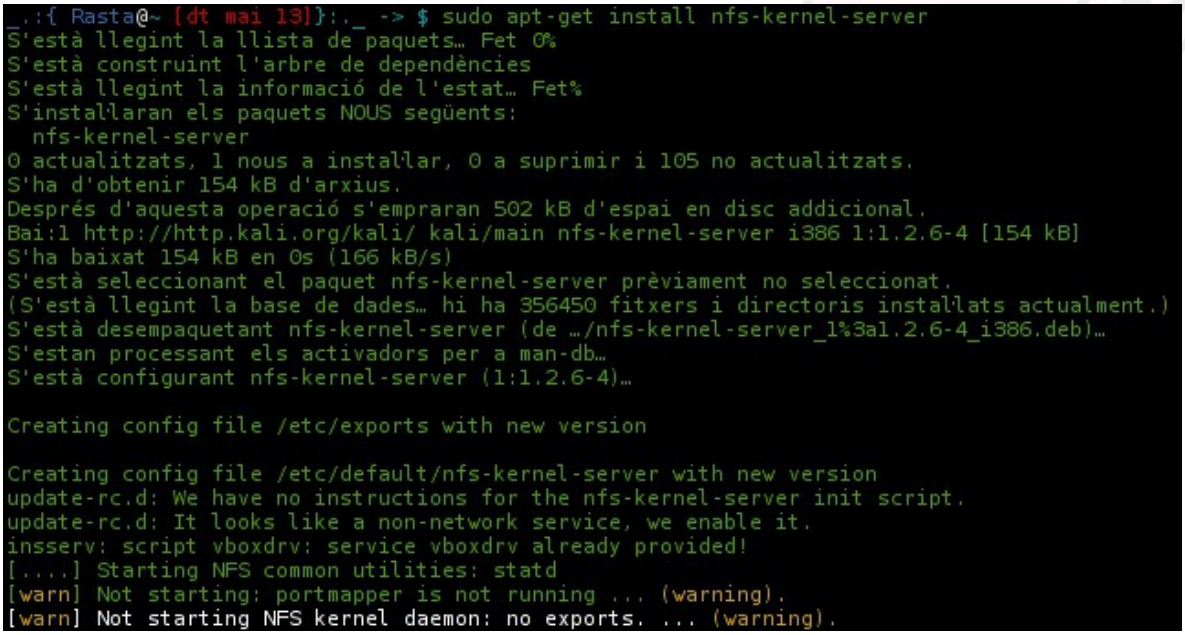

Figura 3.2

Un pic efectuada la instal·lació, ja podrem gaudir dels serveis que proporcioni el paquet descarregat i instal·lat.

A l'hora d'activar un servei, s'ha de tenir en compte una sèrie de punts sobre els sistemes Linux per tal de configurar-los de manera correcte.

Primerament hem de saber en quin nivell d'execució ens trobem, és a dir, en quin runlevel ens trobem, per poder-ho saber podem executar la següent comanda:

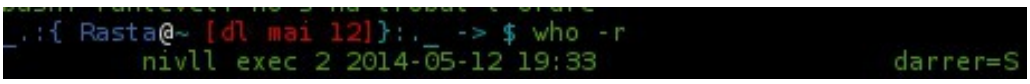

Figura 3.3

Així doncs descobrirem el nivell d'execució, ja que això determinarà en quines de les carpetes haurem de copiar els scripts d'inicialització de serveis per tal que s'executin una vegada engegat el sistema operatiu. Com que en aquest cas hem descobert que ens trobem en el segon nivell d'execució del sistema, haurem de crear un enllaç simbòlic (el que es coneix en els sistemes Windows com accés directe) dels scripts de programa al nivell d'execució en concret (en el nostre cas rc2.d) per tal que s'executin quan s'entri en el nivell concret.

Per tal de facilitar la feina d'activar/desactivar els serveis al sistema hi ha una eina disponible als repositoris de Debian que s'anomena **chkconfig** el qual desenvolupa el procés de creació d'enllaç simbòlic, o desactivació de servei. Amb el següent exemple es mostrarà el fet de buscar un paquet en el repositori i s'instal·larà al sistema, fent una posterior comprovació que el paquet ja es troba instal·lat al sistema.

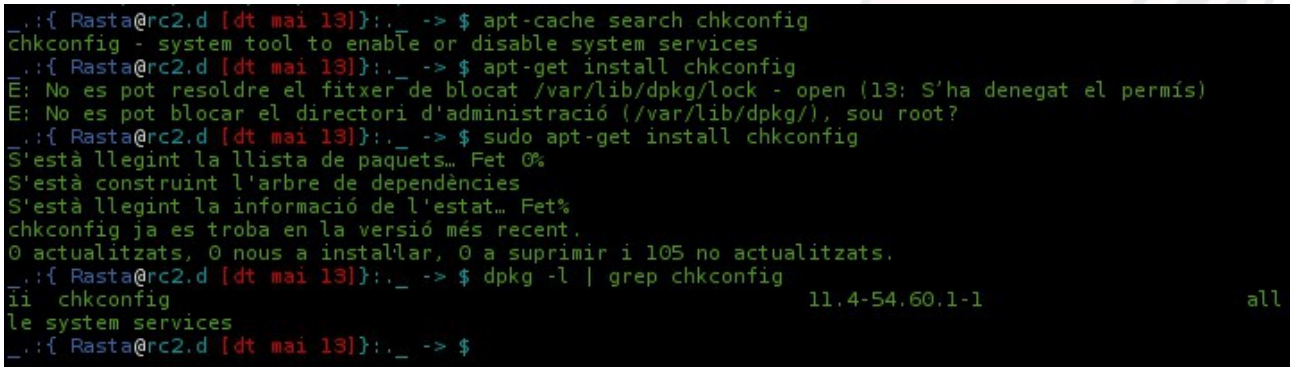

Figura 3.4

3.2.2. Configuració del firewall tenint en compte la funcionalitat del serveis

Hem de tenir present a l'hora de configurar un servei, quina és la funcionalitat del servei i depenent de l'abast que volem que tingui, quin impacte provocarà sobre el nostre sistema, és a dir, si volem que el servei NFS estigui obert a tothom, necessitarem que el seu port determinat estigui a disposició dels usuaris que en necessitin del seu servei, ja siguin des de la xarxa externa com des de la xarxa interna.

En aquest cas, per aquest servei en concret estarà activat el port 2049 per tal que puguin accedir els usuaris. Per tal de poder dur a terme aquesta acció necessitem saber dos coses:

1. La configuració de les regles del Firewall es fa amb IPTABLES amb una sèrie de paràmetres que els anirem explicant a mesure que anem avançant amb la configuració.

2. Per tal de poder redirigir el trafic de paquets de manera que passin a través de la nostra xarxa interna cap a la xarxa externa (I a l'inrevés) necessitarem usar les regles NAT.

La millor situació per tal de portar un control sobre els paquets que s'envien I es reben a través I cap a la nostra xarxa, és posar un equip bastió, el qual pot actuar també de firewall, així doncs efectuarà el filtratge de paquets I en portarà un control adequat, si el configurem de manera correcte. De la mateixa manera, aquesta màquina que actua com a equip intermediari per tal d'entregar els paquets entre el router I els equips de la xarxa interna, també pot funcionar com a detector d'intrusos, ja que la primera barrera que es trobaran els possibles atacants, serà aquesta màquina en concret, I aquesta podrà detectar-los.

Per tal que aquesta màquina actui com a router, com que estem parlant d'un equip amb Debian, haurem d'activar un flag de forwarding, per tal que pugui reenviar els paquets que li arribin a ell, això es fa canviant a 1 el valor **/proc/sys/net/ipv4/ip_forward** (echo 1 > /proc/sys/net/ipv4/ip_forward)

Existeixen diferents tipus de cadenes per a definir el comportament dels paquets segon les regles que es defineixin en cada una de les cadenes, si es que se'n defineix alguna.
INPUT: Tràfic d'entrada acp al sistema
OUTPUT: Tràfic de sortida del sistema
FORWARD: Tràfic de redirecció de cadenes de NAT
PREROUTING:Accions prèvies d'enrutament els paquets.
POSTROUTING: Accions posteriors a l'enrutament dels paquets.
MASQUERADE: L'objectiu especificat emmascara una adreça IP privada amb una adreça IP externa del firewall/gateway.
DROP: Aquesta opció es posa al final de la sentència per tal d'indicar al paquet s'ignori
REJECT: Aquesta opció retorna un paquet indicant que el paquet no està a l'abast.
LOG: Logeja el paquet I segueix amb les regles establertes.
ACCEPT: Accepta els paquets de la regla determinada.

És important remarcar que s'ha de determinar sobre en quines adreçes IP afecta aquesta configuració, és a dir, els modificadors -s (source) I -d (destination) indiquen d'on I cap a on van els paquets. També s'indica la interfície de sortida, és a dir que si en algun moment es treballa amb la xarxa cablejada, la interfície de sortida és la eth0, pero si es connectessim per wifi, normalment la interfície seria la wlan0, això s'indica amb el modificador -o.

El procés que segueixen les iptables és seqüencial, això significa que es van evaluant les regles que s'han definit de manera lineal, una a una, fins que el programa en si detecta que existeix match o coincidència, en aquest precís moment s'executa la regla en qüestió I pararà de seguir amb l'execució de les regles, no pararà de buscar regles fins que trobi una coincidència o arribi al final.

Com ja hem comentat prèviament, la política per defecte del firewall serà DROP. No significa que no hagi de rebutjar o denegar qualsevol paquet, és a dir, que la comunicació entre la xarxa interna ha de ser possible, això significa que, per exemple, els paquets icmp (la comanda ping) podria estar habilitada, si més no els serveis necessaris per a la xarxa interna.

Iptables -I FORWARD -p icmp -j REJECT

Com que segurament un dels serveis que s'hauran de proporcionar a les màquines de l'entorn és la connectivitat a internet, haurem de proporcionar el servei http als usuaris per tal que puguin fer consultes, buscar solucions a problemes, etc. Ho podem fer de dos maneres:

1. Coneixen les IP que volem que accedeixin (es poden ficar Ips o Xarxes, permetent d'aquesta manera, l'accés al rang d'adreces d'aquella xarxa)
2. Aplicant les regles de manera general (que en aquest cas ens seria més útil)

1. Iptables -I FORWARD -s 'adreça IP origen' -p tcp –dport* 80 -j ACCEPT

2. Iptables -I FORWARD -p tcp –dport 80 -j ACCEPT

--dport: Port destí, en aquest cas indiquem que el port a on anirà a parar tot el trafic és el 80, que seria el http

Iptables -I POSTROUTING -p tcp –dport 80 -o eth0 -j MASQUERADE → Regla per enrutar el trafic http

Iptables -I POSTROUTING -p tcp –dport 80 -o eth0 -j MASQUERADE
Iptables -I POSTROUTING -p tcp –dport 443 -o eth0 -j MASQUERADE
Iptables -I POSTROUTING -p tcp –dport 8080 -o eth0 -j MASQUERADE
Iptables -I POSTROUTING -p tcp –dport 8443 -o eth0 -j MASQUERADE

Iptables -I FORWARD -p tcp –dport 80 -j ACCEPT
Iptables -I FORWARD -p tcp –dport 443 -j ACCEPT
Iptables -I FORWARD -p tcp –dport 8080 -j ACCEPT
Iptables -I FORWARD -p tcp –dport 8443 -j ACCEPT

3.2.3. Configuració del programa de detecció d'intrusos, snort

cd /usr/src && wget http://labs.snort.org/snort/2930/snort.2930.conf -O snort.conf
wget http://www.snort.org/dl/snort-current/snort-2.9.3.tar.gz -O snort-2.9.3.tar.gz
tar -zxf snort-2.9.3.tar.gz && cd snort-2.9.3
./configure --enable-sourcefire && make && make install
mkdir /etc/snort /etc/snort/rules /var/log/snort /var/log/barnyard2 /usr/local/lib/snort_dynamicrules
touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules
groupadd snort && useradd -g snort snort
chown snort:snort /var/log/snort /var/log/barnyard2
cp /usr/src/snort-2.9.3/etc/*.conf* /etc/snort
cp /usr/src/snort-2.9.3/etc/*.map /etc/snort
cp /usr/src/snort.conf /etc/snort

vi /etc/snort/snort.conf

Canviar les següents línies:
Line #45 - ipvar HOME_NET 172.26.12.0/22 – fes coincidir amb la teva xarxa interna
Line #48 - ipvar EXTERNAL_NET !$HOME_NET
Line #104 - var RULE_PATH ./rules
Line #113 - var WHITE_LIST_PATH ./rules
Line #114 - var BLACK_LIST_PATH ./rules
Line #297 - add this to the end after “decompress_depth 65535” max_gzip_mem 104857600
Line #538 - add this line output unified2: filename snort.log, limit 128
Line #554 - delete or comment out all of the “include $RULE_PATH” lines except “local.rules”

vi /etc/snort/rules/local.rules

Introdueix aquesta simple regla per tal de testejar l'aplicació:
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001;)

Ara podem engegar I testejar el programa:
/usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

Fes ping a la màquina a la qual s'ha configurat snort des d'un altre màquina, hauria de sortir una alerta imprimida a la línia de comandes (si s'ha efectuat correctament) tal que així:

02/09-11:29:43.450236 [**] [1:10000001:0] ICMP test [**] [Priority: 0] {ICMP} 172.26.12.1 -> 172.26.12.2
02/09-11:29:43.450251 [**] [1:10000001:0] ICMP test [**] [Priority: 0] {ICMP} 172.26.12.2 -> 172.26.12.1

Si volguessim configurar les nostres regles, afegint-les al fitxer local les prendria com a vàlides per si troba alguna coincidència amb algun paquet analitzat.

3.2.4. Instal·lació de regles bàsiques per a snort.

Quan s'instal·len les llibreris de snort, les regles que estan configurades són les bàsiques, si més no mínimes. A l'hora d'accedir a les llibreries de snort i les seves regles, hi accedirem segons la seva ruta que esta ubicades a '/etc/snort/rules'.

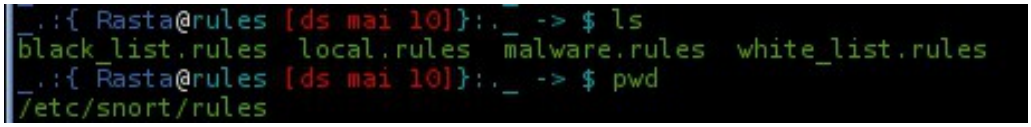

Figura 3.5

El que farem serà instal·lar un paquet de regles per tal de definir unes quantes regles predefinides.

1. Buscarem els possibles paquets disponibles mitjançant l'eina de gestor de paquets explicada anteriorment:

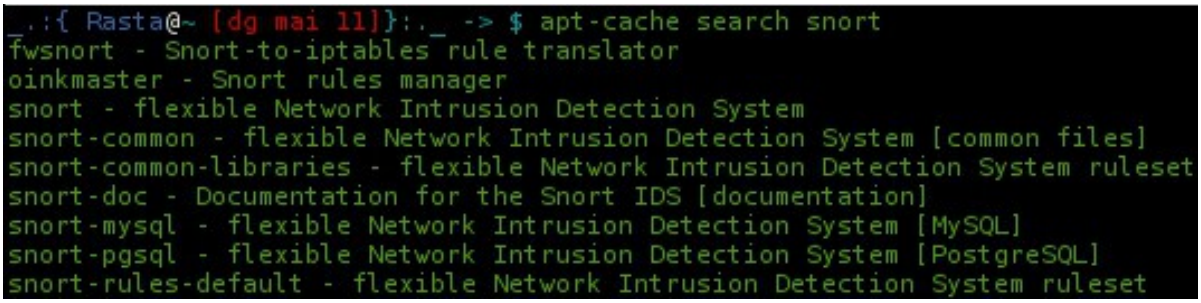

Figura 3.6

Una vegada seleccionem els paquets a instal·lar (en el nostre cas seleccionarem el paquet snort-rules-default) de la següent manera:

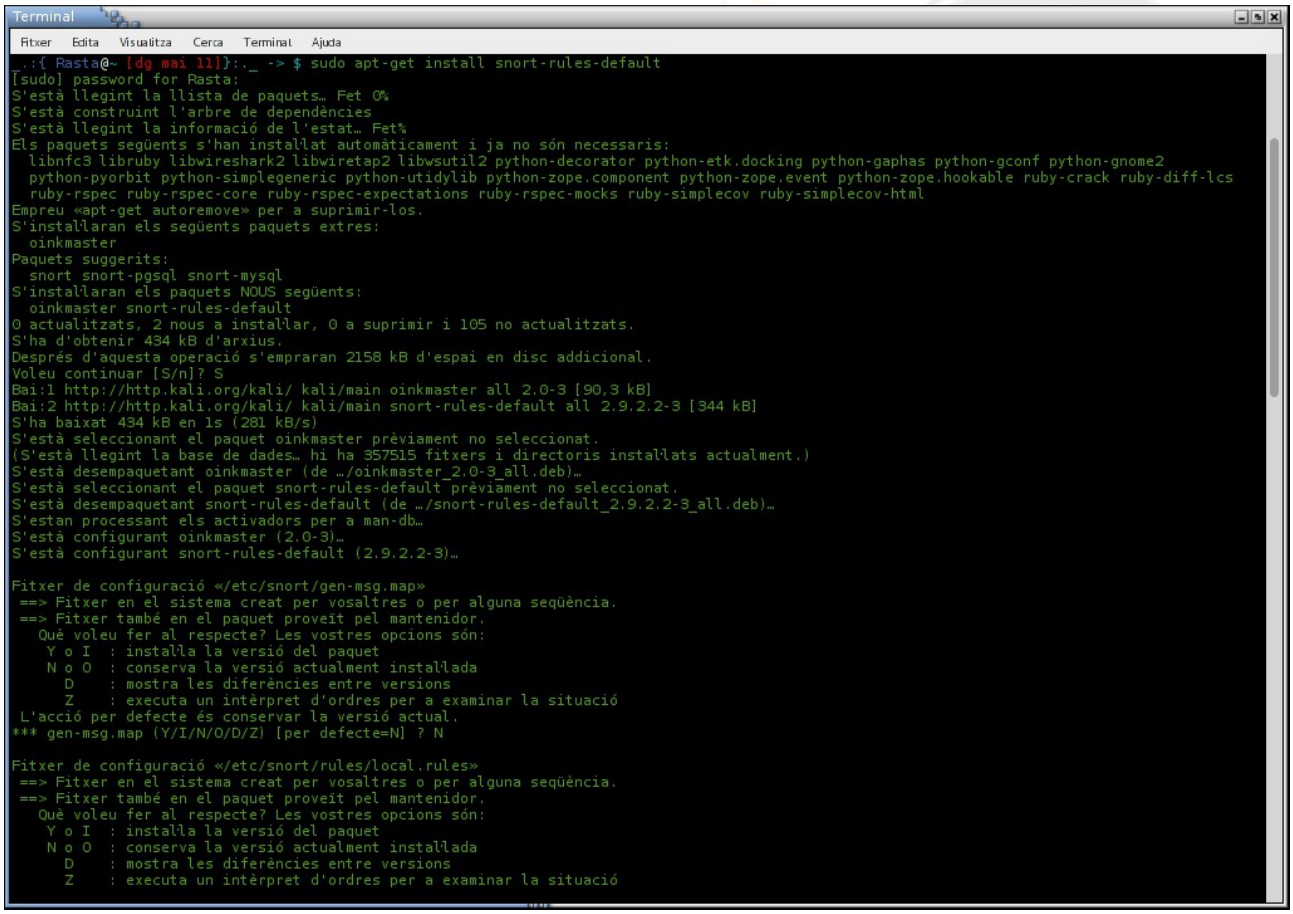

Figura 3.7

Amb la comanda: **$ sudo apt-get install snort-rules-default** ens intal·larà regles preestablertes per tal de detectar possibles intrusions en serveis coneguts com telnet, ftp, mysql... Tot seguit mostrarem el canvi que comporta el fet d'haver instal·lat un paquet de regles preestablertes al sistema.

Figura 3.8

La diferència és notable, així que ara ja tenim un gran ventall de possibilitats de detectar intrusions al nostre sistema amb unes quantes regles predefinides.

3.2.5. Configuració de regles per a detectar possibles amenaces a través d'un servei determinat.

Imaginem-nos que habilitem el servei ssh per tal de tenir accés a la màquina interna de la nostra xarxa per tal de poder-hi accedir I poder fer les gestions necessàries segons les nostres necessitats.

```
Alert tcp any any → $HOME_NET 22 (msg:"Potential SSH Brute Force Attack"; \
flow:to_server; \
flags:S; \
fwsam: src, 24 hours; \
threshold:type threshold, track by_src, count 3, seconds 60; \
classtype:attempted-dos; \
sid:2001219; \
rev:4; resp:rst_all; \
)
```

Alert tcp any any → $HOME_NET 22 : Avisar de tot trafic que provingui d'una xarxa externa i intenti connectar-se a través del port 22 cap a la xarxa interna.

msg:"Potential SSH Brute Force Attack": Amb el missatge que es correspon al camp *msg.*

flow:to_server: En el qual intenti establir una connexió amb l'equip atacant que està fora de l'abast de la xarxa (Com un IP Spoofing).

Flags:S: Indica que el flag SYN (Syncronize) està activat.

fwsam: src, 24 hours: Indica que l'adreça origen quedarà bloquejada durant 24 hores (que en aquest cas serà l'adreça de l'atacant).

threshold:type threshold, track by_src, count 3, seconds 60; Tipus de Llindar, escriu alertes de llindar cada m vegades veiem aquest esdeveniment durant l'interval de temps. La IP orígen és rastrejada amb la sentència **track by_src**, si hi ha hagut 3 regles que han donat positiu (matching) i durant un temps de 60 segons.

classtype:attempted-dos;: Identifica la detecció com a tipus Attempted Denail Of Service , que seria un intent de denegació de servei.

Sid:2001219; rev:4;: La paraula clau rev s'utilitza per identificar de forma exclusiva la revisió de regles de Snort. Les revisions, juntament amb el sid de regles, permeten a signatures i a les descripcions ser refinats i reemplaçats amb informació actualitzada.

Resp:rst_all: És la resposta que tindrà el programa a l'hora que la regla dóni positiu: rst_all
Envia un paquet RST a les dues sessions TCP obertes en la comunicació.

3.2.6. Processos d'automatització de regles per a un sitema determinat.

Realment no existeix un procés de creació de regles dinàmiques com a tal, existeixen plugins que ajuden a l'actualització automàtica de regles per al programa de snort, pero no la generació d'aquestes en el moment de detectar una vulnerabilitat I posterior violació de seguretat en el sistema.

Això significa que hem de tenir present les vulnerabilitats que puguin sortir diàriament per tenir-les present I estar actualitzats al dia. De totes manere, una de les eines que ens pot ajudar a tenir les regles actualitzades al dia és la que se'n diu PulledPork.

PulledPork és un script escrit en Perl que actualitza automàticament les regles de Snort. Per tal d'instal·lar aquesta eina, prèviament hem d'instal·lar els mòduls de perl necessaris:

```
$ apt-get install libcrypt-ssleay-perl liblwp-useragent-determined-perl -y
```

Una vegada instal·lat els mòduls, procedirem a descarregar-nos el programa I extreure'l

```
$ cd /usr/local/src/snort
$ wget http://pulledpork.googlecode.com/files/pulledpork-   0.6.1.tar.gz -O pulledpork.tar.gz
$ cd /usr/local/snort
$ tar zxvf /usr/local/src/snort/pulledpork.tar.gz
$ mv pulledpork-0.6.1 pulledpork
```

Ens registrarem a la web de Snort (Si es que no ho estam) per generar el codi OinkCode, accedint a la pàgina d'inici I fent clic a “Get Snort OinkCode” a la secció de Links.

Procedirem a canviar el fitxer de configuració:

```
$ vi /usr/local/snort/pulledpork/etc/pulledpork.conf
```

Fent els següents canvis:

```
...
rule_url=https://www.snort.org/reg-rules/|snortrules-snapshot.tar.gz|paste here your Oinknumber
# get the rule docs!
#rule_url=https://www.snort.org/reg-rules/|opensource.gz|
#rule_url=https://rules.emergingthreats.net/|emerging.rules.tar.gz|open
# THE FOLLOWING URL is for etpro downloads, note the tarball name change!
# and the et oinkcode requirement!
#rule_url=https://rules.emergingthreats.net/|etpro.rules.tar.gz|
...
rule_path=/usr/local/snort/etc/rules/snort.rules
...
local_rules=/usr/local/snort/etc/rules/local.rules

# Where should I put the sid-msg.map file?
sid_msg=/usr/local/snort/etc/sid-msg.map
...
# Path to the snort binary, we need this to generate the stub files
snort_path=/usr/local/snort/bin/snort
```

```
# We need to know where your snort.conf file lives so that we can
# generate the stub files
config_path=/usr/local/snort/etc/snort.conf

# This is the file that contains all of the shared object rules that pulledpork
# has processed, note that this has changed as of 0.4.0 just like the rules_path!
sostub_path=/usr/local/snort/etc/rules/so_rules.rules
...
distro=Ubuntu-10.04 # For CentOS 6.x you can use RHEL-6-0
...
pid_path=/var/run/snort_eth0.pid
...
```

Canviar la variable de configuració RULE_PATH del fitxer de configuració

```
vi /usr/local/snort/etc/snort.conf

...
var RULE_PATH /usr/local/snort/etc/rules
...
```

Elimina totes les regles include de snort

```
sed -i '/^include $RULE_PATH/d' /usr/local/snort/etc/snort.conf
sed -i '/^include $RULE_PATH/d' /usr/local/snort/etc/snort.conf
sed -i '/^include $RULE_PATH/d' /usr/local/snort/etc/snort.conf
```

Afegeix les següents linies de include sl fitxer de configuració snort.

```
echo "include \$RULE_PATH/snort.rules" >> /usr/local/snort/etc/snort.conf
echo "include \$RULE_PATH/local.rules" >> /usr/local/snort/etc/snort.conf
echo "include \$RULE_PATH/so_rules.rules" >> /usr/local/snort/etc/snort.conf
```

Si tenim un fitxer de regles en la configuració de snort, el copiarem a la següent ruta:

```
$ cp /usr/local/snort/rules/local.rules /usr/local/snort/etc/rules/
```

Si no el crearem mitjançant la comanda touch:

```
$ touch /usr/local/snort/etc/rules/local.rules
```

I per executar el PulledPork, escriurem la següent sentència a través de la línia de comandes:

```
$ /usr/local/snort/pulledpork/pulledpork.pl -c /usr/local/snort/ pulledpork/etc/pulledpork.conf
```

Per tal que PulledPork s'executi cada dia, haurem d'afegir al final del crontab la línia d'execució del programa, tal que així:

```
...
0 0 * * * root /usr/local/snort/pulledpork/pulledpork.pl -c /usr/local/snort/ pulledpork/etc/pulledpork.conf
...
```

Així PulledPork actualitzarà I executarà les regles de Snort a diari.

3.2.7. Eines addicionals

root@HaTMaN:/home/Rasta# apt-cache search snort
fwsnort - Snort-to-iptables rule translator

Aquesta eina és molt útil per a poder traduïr les infiltracions al sistema en regles d'iptables, d'aquesta manera ens evitarem moltes dels atacs que puguem patir al nostre sistema, i d'alguna manera, en el moment de detectar alguna violació de seguretat mitjançant aquesta eina, aplicar-la a les regles d'iptables per tal que no torni, la persona malintencionada, tornar a atacar el nostre sistema. Existeixen també diferents tipus d'eines de monitorització, que ajuden a l'administador del sistema mantenir un control dels fitxers del sistema per controlar-los i veure les incidències.

Capítol Final – Conclusions

El darrer capítol inclourà les conclusions, on es relacionaran els objectius aconseguits i els no aconseguits, possibles ampliacions del treball, etc.

Conclusions

Per definició, un sistema mai pot estar al 100% segur, per això existeixen eines de recolzament per tal de donar suport a la seguretat, en aquest cas ens hem centrat en un sistema de detecció d'intrusions, el qual només ens avisarà en el cas que es detecti un «match» amb les regles definides. S'ha de tenir present que aquests sistemes, estan actualitzats ocasionalment, però un dels objectius principals que ha de tenir clar un administrador de sistemes, és que per molt que tingui un sistema totalment actualitzat i al dia, la tecnologia evoluciona i sempre es troben vulnerabilitats en els sistemes, per això, s'ha de tenir monitoritzat un sistema, per detectar qualsevol anomalia, ja sigui per un fallo de software de tercers, o per una mala configuració del sistema respecte els usuaris.

Dels objectius proposats a l'inici del projecte explicarem com hem complert les expectatives proposades a l'inici.

- Portar un registre de les activitats sobre l'equip, és a dir, logar totes les accions que es facin dins i fora, contra l'equip en qüestió.

En aquest cas logejarem totes les accions que detecti el programa snort, així que sí que es compleix aquest punt.

- Crear cadenes, regles per tal d'avisar sobre possibles violacions de seguretat contra el sistema. (Tenir un control de les activitats del sistema)

També es creen cadenes, fins i tot amb l'eina PulledPork es pot arribar a automatitzar el procés d'introducció de cadenes en el cas que apareguin noves vulnerabilitats de seguretat i n'existeixin exploits, ja que el que detecterà el programa snort és la infiltració a través de l'explotació d'una vulnerabilitat.

- Apendre a definir polítiques de seguretat en un sistema i saber-les aplicar en un entorn empresarial.

Aquest punt també l'hem complert, ja que hem pogut arribar a definir unes polítiques de seguretat a nivell empresarial.

- Actuar segons una plà d'actuació (protocols) en cas de violació de trencament de seguretat i aconseguir la màxima eficiència en els escenaris que es plantegin. D'aquesta manera apendre a administrar i gestionar la seguretat en un entorn real.

Aquest punt no l'hem pogut provar, ja que només hem definit el sistema per tal de loguejar les intrusions al sistema. Així que no podem assegurar que hagim assolit aquest objectiu, però que tampoc no l'hagin assolit, així que ´si que s'han plantejar els protocols d'actuació, pero no estarien proves del tot.

Aquest projecte pot arribar a ampliar-se bastant, tot depèn de la idea a desenvolupar i l'ambició que tingui la persona que el porti. Evidentment també és important tenir els recursos si volem tirar endavant amb la idea i començar a desenvolupar-la, però tenint la idea ben definida i consolidada i lligar totes les peces per tal d'arribar a construir un producte que faci evolucionar a la societat cap a un bé comú i avançar tecnològicament i intel·lectualment, sempre porta resultats positius, ja sigui a petita escala com a nivells internacionals.

A mesura que anava desenvolupant el projecte, anava agafant idees per un projecte gran, molt més gran i ambiciós. Tenir una aplicació el qual comparteixi, mitjançant la captura d'intrusions amb snort, una comunitat per tal de compartir els resultats obtinguts a partir de les intrusions capturades. Aquesta comunitat es dedicaria a muntar servidors específics, gantxos per a que gent experimentada, amb fins poc ètics, vulguin hackejar les màquines preparades. D'aquesta manera, s'aconsegueix un estudi de quines són les vulnerabilitats que s'han explotat, quines t'ecniques s'han usat per entrar al sistema, etc, i si així es comparteix amb la comunitat, es podria arribar a recopilar informació sobre quins sistemes són més segurs, tècniques usades en l'intrusions dels sitemes.

Glossari

decodificador: Converteix un codi binari d'entrada (Natural) de N bits d'entrada i M línies de sortida (N pot ser qualsevol enter i M un enter menor o igual a 2N).
desbordaments de buffer: Error de programació que es produeix quan un programa no controla els accessos a memòria i accedeix a zones els quals no pertany en el seu context.
IDS: Sistema de Detecció d'Intrusions
incidència: Circumstància o succés secundari que afecte al transcurs d'un asumpte.
Infraestructura: Conjunt de mitjans tècnics, serveis i instal · lacions necessaris per al desenvolupament d'una activitat.
Firewall: Un sistema informàtic que aïlla un altre ordinador a través d'Internet per tal d'evitar l'accés no autoritzat
funcionalitat: Propietat de les coses que tenen una utilitat pràctica.
Intrusos: Ent que s'ha introduit sense autoritat en un sistema informàtic, propietat...
implementació: La realització d'alguna cosa.
IPS: Sistema de Prevenció d'Intrusos.
IT: Tecnologies de la informació
log: Document on es guarda informació de canvis del sistema.
Mòdul: Peça o conjunt de peces que es repeteixen en una construcció.
Monitoritzar: Controlar el desenvolupament d'una acció mitjançant monitors.
Online: En línia a la xarxad'Internet.
Plugin: Dissenyat per a ser connectat a una font d'alimentació elèctrica.
política de seguretat: Un pla d'acció per afrontar riscos de seguretat, o un conjunt de regles per al manteniment de cert nivell de seguretat.
portes del darrera: Un mètode indocumentat per tenir accés a un sistema informàtic o les dades que conté.
Preprocessador: Abans de processar una dada i tractar-la.
Pymes: Petita o mitjana empresa.
Regla: Una definició que es segueix de manera detallada el qual indica una acció per dur a terme si es compleix una condició.
Rol: Funció d'una persona que exerceix en una situació.
Runlevel: Nivell d'execució el qual està corrent el sistema operatiu Linux.
Script: Un simple programa en un llenguatge d'utilitat o llenguatge propietari d'una aplicació.
Servei: Utilitat o funció que exerceix una cosa.
Software: Conjunt de programes que poden ser executats en un ordinador.
Troians: S'aplica al virus informàtic que provoca grans efectes destructius; s'activa quan un usuari carrega un fitxer sense haver advertit la seva presència.
Validar: Fer ferm o legal alguna cosa.
Virus: Programa informàtic que es reprodueix i es propaga amb l'objectiu de danyar els arxius d'un ordinador.
Vulnerabilitat: Es refereix a la presentació d'informes fallades de seguretat als proveïdors i al públic en general.

Bibliografia

http://www.adminso.es/images/d/d0/Pfc_Carlos_cap3.pdf

http://vtroger.blogspot.com.es/2009/09/herramienta-de-creacion-automatica-de.html

https://www.voztovoice.org/?q=node/609

http://blog.desdelinux.net/como-saber-si-un-paquete-se-encuentra-instalado-o-no-de-manera-facil-y-rapida/

http://www.youtube.com/watch?v=_A5rC7BM6U0

http://www.thegeekstuff.com/2011/01/iptables-fundamentals/

http://www.snort.org/assets/167/IDS_deb_snort_howto.pdf

http://www.clearfoundation.com/component/option,com_kunena/Itemid,232/catid,8/func,view/id,59173/

http://nachum234.no-ip.org/security/snort/104-configure-snort-automatic-rules-updating-with-pulledpork/

http://blog.snort.org/2011/09/flow-matters.html

Annexe

ORDINADOR MONITORITZAT:

```
root@HaTMaN:/home/Rasta# /usr/local/bin/snort -A console -u snort -g snort -i wlan0
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "wlan0".
Decoding Ethernet
Set gid to 1002
Set uid to 1001
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.4 GRE (Build 40)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
           Copyright (C) 1998-2012 Sourcefire, Inc., et al.
           Using libpcap version 1.3.0
           Using PCRE version: 8.30 2012-02-04
           Using ZLIB version: 1.2.7

Commencing packet processing (pid=3424)
05/16-18:14:25.756812 192.168.1.14 -> 192.168.1.22
ICMP TTL:63 TOS:0x0 ID:6113 IpLen:20 DgmLen:84
Type:8  Code:0  ID:1   Seq:29  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/16-18:14:25.756878 192.168.1.22 -> 192.168.1.14
ICMP TTL:64 TOS:0x0 ID:46235 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1  Seq:29  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/16-18:14:26.663271 192.168.1.14 -> 192.168.1.22
ICMP TTL:63 TOS:0x0 ID:6114 IpLen:20 DgmLen:84
Type:8  Code:0  ID:1   Seq:30  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/16-18:14:26.663342 192.168.1.22 -> 192.168.1.14
ICMP TTL:64 TOS:0x0 ID:46236 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1  Seq:30  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/16-18:14:27.666163 192.168.1.14 -> 192.168.1.22
ICMP TTL:63 TOS:0x0 ID:6115 IpLen:20 DgmLen:84
Type:8  Code:0  ID:1   Seq:31  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/16-18:14:27.666229 192.168.1.22 -> 192.168.1.14
ICMP TTL:64 TOS:0x0 ID:46237 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1  Seq:31  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

^C*** Caught Int-Signal
===============================================================================
Run time for packet processing was 18.723637 seconds
Snort processed 10 packets.
Snort ran for 0 days 0 hours 0 minutes 18 seconds
   Pkts/sec:           0
===============================================================================
Packet I/O Totals:
   Received:           10
   Analyzed:           10 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
```

```
Outstanding:          0 (  0.000%)
  Injected:           0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
       Eth:          10 (100.000%)
      VLAN:           0 (  0.000%)
       IP4:           6 ( 60.000%)
      Frag:           0 (  0.000%)
      ICMP:           6 ( 60.000%)
       UDP:           0 (  0.000%)
       TCP:           0 (  0.000%)
       IP6:           0 (  0.000%)
   IP6 Ext:           0 (  0.000%)
  IP6 Opts:           0 (  0.000%)
     Frag6:           0 (  0.000%)
    ICMP6:            0 (  0.000%)
     UDP6:            0 (  0.000%)
     TCP6:            0 (  0.000%)
   Teredo:            0 (  0.000%)
  ICMP-IP:            0 (  0.000%)
    EAPOL:            0 (  0.000%)
  IP4/IP4:            0 (  0.000%)
  IP4/IP6:            0 (  0.000%)
  IP6/IP4:            0 (  0.000%)
  IP6/IP6:            0 (  0.000%)
.
.
.
      MPLS:           0 (  0.000%)
       ARP:           4 ( 40.000%)
       IPX:           0 (  0.000%)
  Eth Loop:           0 (  0.000%)
  Eth Disc:           0 (  0.000%)
  IP4 Disc:           0 (  0.000%)
  IP6 Disc:           0 (  0.000%)
  TCP Disc:           0 (  0.000%)
  UDP Disc:           0 (  0.000%)
 ICMP Disc:           0 (  0.000%)
All Discard:          0 (  0.000%)
    Other:            0 (  0.000%)
Bad Chk Sum:          0 (  0.000%)
   Bad TTL:           0 (  0.000%)
    S5 G 1:           0 (  0.000%)
    S5 G 2:           0 (  0.000%)
     Total:          10
===============================================================================
Snort exiting
```

ORDINADOR ATACANT:

```
root@kali:~# ping 192.168.1.22
PING 192.168.1.22 (192.168.1.22) 56(84) bytes of data.
64 bytes from 192.168.1.22: icmp_req=1 ttl=64 time=100 ms
64 bytes from 192.168.1.22: icmp_req=2 ttl=64 time=2.63 ms
64 bytes from 192.168.1.22: icmp_req=3 ttl=64 time=2.71 ms
^C
--- 192.168.1.22 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 2.631/35.137/100.068/45.913 ms
```