L'ÍNDEX

1. Definició

1.1 Objectiu del projecte

L'objectiu d'aquest projecte és la redacció de dues guies per configurar un ordinador com a gateway d'una xarxa interna.

1.2 Descripció del projecte

Aquest document és una guia o referència per tal de configurar un ordinador com a gateway d'una xarxa interna d'ordinadors. És a dir, que un ordinador de la nostra xarxa actui alhora com a router i firewall. Per tal d'aconseguir-ho utilizarem un ordinador on hi hagi instal.lat el sistema operatiu Linux i iptables.

1.3 Motivació: el propòsit d'aquest document

Quan un ordinador està connectat a Internet, realment si no disposem de bones messures de seguretat, en realitat podem estar compartint les nostres dades, i fins it tot el nostre sistema.

Però quí pot voler fer ús de la nostre informació? Quí ens pot voler atacar? La resposta no és gaire senzilla. Però realment això normalment dependrà de la informació o sistema que volem protegir.

Tot i que es pot fer per divertiment, o bé, per comprovar certes característiques dels sistemes, no és normal que un usuari comú que simplement vol conectar-se a Internet per tal de poder gaudir de la informació i de la tecnologia, sigui un objectiu per a un atacant o pirata informàtic. Però tot i així, pot ésser utilitzat com a punt d'entrada a d'altres sistemes o per despistar a la víctima real.

Per tant, la necessitat d'una certa seguretat és prou clara.

Com ho fem? Aquesta és precisament la motivació d'aquest projecte. N'hi ha una pila d'informació per tal de configurar un gateway, o un router, o un firewall, i aquest document preten ésser realment una guia pràctica per tal d'endinsar-se en el mon de la configuració de firewalls utilizant tecnología iptables amb Linux.

El document es divideix realment en dos documents: un per a usuaris tècnics i un altre per a no tècnics.

Al document per a no tècnics s'intenta endinsar l'usuari en una lectura agradable que el permeti comprendre la necessitat de la seguretat a nivell de firewalls (i es donen un parell d'exemples d'implementació de situacions reals) i, veritablement, és al document per a tècnics on realment s'explica la metodologia.

1.4 La importància de la seguretat

És força difícil de no trobar-se enlloc amb una xarxa d'ordinadors. Avui, qualsevol empresa on sigui necessari treballar amb **informació**, quasi gairebé segur que hi serà enmagatzemada i manipulada amb ordinadors.

Estem vivint a la societat de la informació des de fa ja uns quants anys. "La informació és el poder". Quan comprem un pis, un cotxe, ens fem socis del Zoo de Barcelona, ... en fi, qualsevol cosa pràcticament és manipulada amb ordinadors. I això es pot estendre a qualsevol ambient. Imagina per exemple, la quantitat d'informació que es manega a Google, o la NASA, etc. Obviament el nivell de seguretat ha d'ésser corresponent al que necessitem en qualsevol escenari.

Quin és el nostre nivell de seguretat real? Ens podem basar en el principi de l'eslabó mes feble. Podem tenir molt bé configurat un firewall, actualitzat el nostre antivirus, sistema, VPN, SSH, SSL, aplicats tots els patches de seguretat, sistemes de detecció d'intrussos, etc. Però si una persona falla, o un password d'un usuari és massa feble, o la política interna no és gaire restrictiva, ... podem tenir realment problemes de seguretat.

Però aleshores de que ens serveix tot això si no podem garantir igualment la seguretat? Bé, hem de plantejar-nos el tema de la seguretat com un partit a guanyar i això només es pot fer amb la idea d'equip. Primer hem de saber a qué o qué ens enfrontem i després aplicar les nostres estratègies per tal d'ésser més resistents i més efectius.

1.5 Què podem aprendre en aquest document

Com hem pogut veure en seccions anteriors, la seguretat és realment un conjunt d'elements que han de treballar conjuntament per tal d'assolir els nostres objectius.

El propòsit d'aquest document és tenir una visió més clara de la seguretat a nivell de firewalls.

1.6 Què no podem esperar d'aquest document

No podem esperar fer-nos uns experts perque realment no existeix en aquest una metodologia.

Per tant, el que podem es fer-nos una idea clara de la importància de la seguretat, saber que és un firewall, perqué són importants, i després es veuen dos possibles implementacions al final del document.

1.7 A qui li pot interessar llegir-se aquest document?

Si cap dia et trobes amb la necessitat de configurar un firewall o bé d'entendre els elements més important a tenir en compte, aquest document et pot anar realment bé.

Si després necessites implementar un firewall, és aconsellable llegir el manual per a tècnics que forma part d'un document més extens on s'explica acuradament una metodologia per tal d'implementar una seguretat a nivell de firewall utilitzant iptables.

1.8 Quí hauria de llegir aquest document

Tot aquell que pugui estar interessat en la configuració de firewalls o d'implementació de seguretat a nivell de trafic de dades en un entorn o sistema determinat.

2. Conceptes sobre Firewalls

La idea d'aquest capítol és la de reforçar els conceptes més bàsics sobre firewalls per tal d'enfrontar-nos als conceptes més avançats que esdevindran al llarg del document.

2.1 Conceptes bàsics.

2.1.1 Firewall

Un **firewall** és un dispositiu encarregat de permetre, denegar o redireccionar les dades que arriben als nostres sistemes a partir d'una política de seguretat.

És aquesta política de seguretat de la que parlarem sobretot a la nostra metodologia.

Els firewall poden ser o bé hardware o bé software. Al nostre cas anem a utilitzar una metodologia basada en software (iptables). Però com sempre el software està lligat al hardware i obviament necessitarem dels nostres dispositius de connexió hardware, que normalment hi seràn les interfases de xarxa.

La tasca més comú per a un firewall és la de controlar el tràfic de dades entre dues zones de diferent confiança. Un exemple típic és una xarxa privada connectada a Internet. En el nostre primer exemple tindrem un ordinador connectat directament a Internet.

Realment un firewall és un guardia del control de tràfic. Podem decidir quins paquets deixem passar i quins no. El firewall és el policia, els paquests són els vehicles, les vies de comunicació (cable ethernet, wireless, etc) són les carreteres. I la politica de seguretat són el conjunt de normes que necessitem perque les dades que ens arriben i que surten de les nostres xarxes (poblacions) siguin les que permetem.

2.1.2 Gateway

Gateway, en tecnologia de xarxes, és un node que utilitzem com a entrada i sortida d'una xarxa. Realment un nom bastant proper és el de **Router**, és a dir, hardware o software que fa l'enrutament i filtre de dades a traves de les diferentes xarxes. Actualment, aquests conceptes hi són realment barrejats també amb el concepte de

proxy o intermediari, amb proxy-caché (intermediari que a més a més ens enmagatzema els blocs de dades per tal d'oferir optimitzacions en costos temporals) i amb el firewall basat en filtrat de paquets, d'inspecció de virus, de malware, etc. Tot això dependrà dels nivells de la torre OSI que aquest Gateway és encarregat de protegir.

Un **proxy server** és un ordinador que permet oferint un servei de xarxa amb la comunicació transparent i indirecta a d'altres serveis de xarxa. Un client es connecta al proxy server per tal d'obtindre qualsevol recurs (per exemple, un arxiu) a un servidor. El proxy s'encarregarà a partir d'aquest moment d'obtindre el resultat de la petició del client sobre el servidor, bé connectant-se a aquest servidor o bé oferint les dades enmagatzemades a la seva caché (és a dir, dades obtingudes previament). D'aquesta manera també s'oculta la identitat del client a la connexió. És també feina del proxy la d'enviar correctament el resultat de la petició al client.

2.1.3 Xarxes d'ordinadors

Una xarxa d'ordinadors són dos o més ordinadors connectats amb el propòsit de compartir dades o recursos entre ells.

2.1.4 Client-Servidor

Client-Servidor és una arquitectura de xarxa que separa el client (normalment una aplicació que utilitza una interfaç gràfica d'usuari) d'un servidor. Cada instància del client pot demanar peticions al servidor. Tipus específics de servidors: servidors d'aplicacions, servidors de sistemes d'arxiu, de correu electrònic, ... Tot i que el propòsit depen del recurs o dada a compartir, l'arquitectura és sempre la mateixa.

2.1.5 Netfilter/Iptables

Netfilter és el conjunt d'eines dins el núcli Linux que intercepten i manipulen paquets de xarxa. El component més conegut construït a sobre de *netfilter* és el firewall que filtra paquets, però també es utilitzat per una component que realitza la traducció d'adreces de xarxa (NAT) i per compatibilitat amb ipchains. Aquestes components són generalment móduls del nucli.

iptables es el nom de l'eina en espai d'usuari on l'administrador pot crear les regles de filtratge de paquets i de NAT. Tot i que *iptables* es tècnicament només una eina que controla el filtratge de paquets i el NAT dins el núcli, el nom d'*iptables* s'utilitza també quan ens referim a tota la infraestructura, incloent-hi a *netfilter*, *connection tracking* (seguiment de connexions) i NAT. *iptables* és una part estándar de totes les distribucions de Linux actuals.

2.1.6 DMZ

Una **DMZ** (demilitarized zone or perimeter network) és una àrea de la xarxa (una subxarxa) que es troba ubicada entre la xarxa interna de l'organització i la xarxa externa (normalment Internet). El propòsit de la DMZ és que les connexions provinents de l'exterior i interior són permesses, però no es permet l'accéss des de la DMZ a la xarxa interna. Així, podem disposar de serveis a la DMZ per tal d'oferir-los a l'exterior i també es protegeix la xarxa interna en cas de que es trobi compromesa la DMZ per intrussions. Tot aquell que vulgui comprometre la seguretat de la xarxa interna, no ho podrà fer des de la DMZ.

Normalment s'utilitza la DMZ per tal d'oferir serveis a l'exterior com e-mail, web i DNS. Les connexions des de l'exterior a la DMZ són normalment control.lats utilitzant PAT (port address translation). PAT és molt proper al concepte de NAT però amb ports.

Més endavant veurem diferentes maneres de tenir configurades les DMZ. Hi explicarem tres possibles i més comuns escenaris que depen del nombre de firewalls que emprem i del nombre de interfases de xarxa que tenen els nostres gateways. Ho veurem esquemàticament per tenir una idea clara d'aquestes implementacions i el tercer dels nostres exemples és precisament un exemple típic i concret amb DMZ.

2.1.7 Subxarxes

En xarxes d'ordinadors, una subxarxa o **subnet** es un rang lògic d'adreces dintre de l'espai d'adreces de la nostra xarxa o organització. **Subnetting** és un particionament de l'espai d'adreces d'una organització en diverses subnets. Aquest concepte apareixerà sovint al llarg del document.

2.1.8 Hosts

Un host és un ordinador que ofereix serveis a d'altres.

2.1.9 Paquet de dades

En tecnologia de la informació, un **paquet** és un bloc de dades formatejat que es transmet en una xarxa d'ordinadors. La informació es pot transmetre bit a bit, byte a byte com una mena de serie de bits i bytes entre dos punts. El concepte de paquet de dades ens permet transmetre missatges molt més llargs i a més a més, més eficientment i amb més confiança en el transport.

2.1.10 Protocols

Un protocol és una convenció o estàndar que control.la o habilita la connexió, comunicació, i la transferència de dades entre dos ordinadors. A la seva forma més simple, un protocol es pot considerar como un conjunt de normes o regles que s'encarreguen de la sintaxi, de la semàntica i de la sincronització de la comunicació. Els protocols poden ésser implementats per hardware, software o bé, una combinació d'ambdos. Al més baix nivell, un protocol defineix el comportament de la conexió del hardware.

Conèixer els protocols és molt interessant per tal de prendre decissions a la creació de les regles del script de configuració del firewall.

2.2 Firewalls

L'únic ordinador que es pot considerar realment segur és un que estigui apagat. Però el problema és que no és gaire útil.

Molt bé, encenem l'ordinador i imaginem que no el tenim connectat a d'altres ordinadors. Si aquest ordinador té una informació molt rellevant per segons quins propòsits, l'única manera d'obtindre aquesta informació és directament presencial. Per tant, el tipus de seguretat que emprariem en aquest escenari fos relacionat amb la seguretat física o per sniff electromagnètic, etc. No és la problemàtica amb la que ens enfrontem en aquest document.

El nostre escenari és el d'una xarxa d'ordinadors, com per exemple, Internet, i per tant, els possibles intents d'extreure informació sense

permís o bé de comprometre la seguretat del nostre sistema pot arribar de qualsevol indret del món.

A qui li pot interessar la nostra informació? Hem de sospitar de qualsevol. Les intencions dels intrussos poden ser més o menys perilloses. Però a quí li agrada que qualsevol sense permís es passegi per casa? També hi ha d'altres punts de vista: si et connectes a Internet, la informació que tens no l'estàs fent accessible per tothom?

La nostra tasca és la d'enfrontar-nos als problemes de seguretat a nivell de tràfic de dades als nostres sistemes.

La visió és sempre que hem de tenir clar quin és el flux de dades que permetem tant de fora cap a dintre, com de dintre cap a fora.

Això es pot complicar més depenent del nostre sistema i de la informació que disposem del mateix.

Per això és vital, tenir un bon coneixement dels elements més importants del nostre sistema per tal de protegir-lo. Si té serveis que oferir, a quí volem oferir-los, si tenim DMZ o no, quants gateways, etc. Aquesta part d'investigació dels nostres sistemes és una de les més importants a la metodologia que descriurem posteriorment.

2.2.1 Una mica d'historia

La **història d'Internet** es remunta als inicis de les xarxes de comunicacions. La idea d'una xarxa d'ordinadors que permetés la comunicació entre usuaris de diferents ordinadors, s'ha desenvolupat passant per múltiples etapes. La interunió d'aquests desenvolupaments, ha permès crear Internet, també anomenada la **xarxa de xarxes**. Això inclou la fusió d'avanços tecnològics amb les infraestructures de xarxes existents i els sistemes de telecomunicacions.

La prehistòria d'Internet es basa en la xarxa de caràcter militar creada pel departament de defensa dels Estats Units. El 29 d'octubre de 1969 arrencava a la UCLA el primer node d'aquesta xarxa, anomenada ARPANET.

Tècnicament el naixement d'internet, es produí l'1 de gener de 1983, amb la primera xarxa de llarg abast WAN basada en tecnologia TCP/IP, posada en marxa per la National Science

Foundation (NSF) dels EUA. Al 1995, aquesta xarxa fou oberta als interessos comercials.

Durant la dècada del 1990, la xarxa guanyà densitat. L'agost de 1991 el CERN publicà el projecte World Wide Web, i dos anys després Tim Berners-Lee inicià la creació de l'HTML i HTTP. Al 1993 el Centre nacional per aplicacions de supercomputació a la Universitat d'Illionis desenvolupà el primer navegador web el Mosaic versió 1.0.

I aquí va començar tot, **Robert Tappan Morris**, fill de Robert Thomas Morris, recent graduat en Informàtica per la Universitat de Cornell el 1988, va difondre un virus a través d'ArpaNet (precursora d'Internet) que va conseguir infectar 6.000 servidors connectats a la xarxa. La propagació la va realitzar des d'un dels terminals del MIT (Institut Tecnològic de Massachussets).

Al ser descobert, va ser condemnat per la cort de Syracuse, estat de Nova York, a 4 anys de pressó i el pagament de 10.000 dòlars de multa, pena que va ser commutada a llibertat sota paraula i condemnat a complir 400 hores de treball comunitari.

Sempre es tracta de veure el punt més feble del sistema víctima. De vegades, per feblesses en les especificacions del protocols, de vegades per forats de seguretat del codi de diverses aplicacions, de vegades per sobreeiximent del hardware, del tràfic de la xarxa, etc.

Els primers firewalls foren utilitzats al 1990s. Es tractava de router amb regles de filtratge de paquets IP. Posteriorment, això va anar evolucionant i cada cop els firewalls s'encarreguen de la protecció en més nivells de la torre OSI. Realment és un conjunt d'eines que treballen totes amb el mateix objectiu: proporcionar la màxima seguretat als nostres sistemes. Sistemes de detecció d'intrussos, de virus, criptografia, autenticació d'usuaris (biomètrics i no biomètrics), filtratge de paquets, proxies, etc.

2.2.2 Què és la seguretat informàtica

La **seguretat informàtica** és una branca de la informàtica que estudia com assegurar que els recursos dels sistemes informàtics siguin utilitzats de la forma en que es van definir. El seu objectiu és la creació de plataformes segures en que els agents que hi

interactuen (programes i usuaris) només puguin realitzar les accions que hi hagin estat autoritzades.

Els experts en seguretat informàtica acostumen a afirmar que un sistema 100% segur no existeix. Tot i així, afirmen que la seguretat es basa en 3 característiques:

- Integritat
- Privacitat
- Disponibilitat

Depenent de les amenaces es pot distingir entre seguretat lògica i seguretat física.

2.2.3 Amenaces de seguretat física

- Fallades del subministrament elèctric
- Inclemències metereològiques (inundacions, desastres naturals, etc.)
- Fallades del sistema d'aire condicionat
- Accés no autoritzat.
- Incendis.

2.2.4 Amenaces de seguretat física

- Suplantació d'identitat. (spoofing)
- Denegació de serveis. (DOS)
- Enginyeria social.
- Explotació de la vulnerabilitat informàtica.
- Virus informàtic, Troià (trojans), Cucs (worms)
- Programes espia (spyware)
- Portes amagades (backdoors)
- Bombes lògiques

Etc.

2.2.5 Per què firewalls a Internet?

És molt habitual tenir un ordinador a casa i conectar-ho a Internet, o treballar a una empresa i tenir connexió a Internet. De fet, la pregunta és: quina institució, empresa, usuari no té connexió a Internet dins la societat de la informació?

Obviament, saber com protegir-se d'Internet és fonamental. Als nostres exemples sempre assumirem un ordinador o xarxa d'ordinadors connectats a Internet.

2.2.6 Què volem protegir?

- Les teves dades.
- Els teus recursos.
- La teva reputació.

Les teves dades

N'hi ha tres punts fonamentals a la protecció de les nostres dades:

- *Seguretat:* no vols que altre gent conegui la teva informació.
- *Integritat:* no vols que altre gent canvii la teva informació.
- *Disponibilitat:* vols utilitzar les teves dades quan les necessitis.

Els teus recursos

A ningú li agrada que utilitzin els seus recursos: la teva connexió a Internet, la teva impressora, el teu disc, etc. Imagina el cost econòmic que pot suposar el fet d'haver de formatejar els discos amb la consequent pèrdua de disponibilitat de dades, de temps de gestió de backups, o dels problemes de connexió a Internet dels teus usuaris o dels serveis que ofereixes. És molt fàcil imaginar-se la problemàtica.

La teva reputació

Imagina un banc que no pot donar confiança als seus clients per tal de gestionar les seves comptes corrents per Internet. O bé, que t'acussin a tú d'alguna cosa que no has fet perque has sigut suplantat per l'atacant.

2.3 Tipus de firewalls

Segons si protegeixen una xarxa o un ordinador personal podem parlar de:

- Personal firewalls: normalment són programaris que s'instal·len per tal de controlar les connexions a la màquina.
- Firewalls de xarxa: normalment s'executen en maquinari dedicat (o parcialment dedicat) situat als llindars de la xarxa (filtren els paquets que entren i surten de la xarxa).

Segons les capes en què treballin parlem de:

- Tallafocs de nivell de xarxa: per exemple iptables (tot i com veurem també utilitza els protocols dels nivells llindars).
- Tallafocs a nivell d'aplicació: com TCP Wrappers.
- Firewalls d'aplicació: més coneguts com a pròxies, són capaços de filtrar dades d'aplicació (Antivirus de correu, proxy web, SPAM Assasin).

Finalment, segons si el firewall manté un seguiment o no de les connexions de xarxa parlem de:

- Stateless firewalls: Cada paquet és tracta de forma independent i no hi ha relacions entre paquets (memòria). No sap distingir si un paquet és d'una connexió nova o d'una connexió ja establerta.
- Statefull Firewalls: Manté informació de les connexions (TCP, UDP...) que passen a través del firewall.

2.4 Arquitectures de firewall

L'arquitectura de firewall es refereix al inventari de components (hardware i software), la connectivitat i la distribució de funcions entre ells. Disenyar una arquitectura de firewall requereix d'entendre i d'identificar els límits entre els dominis de seguretat en la xarxa. El més comú dels escenaris avuí dia és en organitzacions amb xarxes privades i locals i Internet.

Les més comunes són les següents:

- Screening Router (Packet Filtering)
- Dual-homed Gateway
- Tri-homed Gateway
- Screened Host
- Screened Subnet

Si vols sapigué més sobre arquitectures de firewalls pots utilitzar els següents links:
http://www2.rad.com/networks/2001/firewall/index.htm
http://www.unix.org.ua/orelly/networking/firewall/ch04_02.htm

3. Netfilter/iptables

El subsistema de procés de paquets de xarxa al nucli Linux és el Netfilter, i iptables és la comanda d'usuari encarregada de configurar-ho.

Les regles de procés dels paquets de xarxa són agrupades en taules per funcionalitat: filtratge de paquets (filter), traducció d'adreces de xarxa (nat), la taula de destrossa o de manipulació dels paquets (mangle) i per últim la taula raw (que s'utilitza per configurar excepcions de paquets que no han de ser controlats pel sistema de seguiment de connections (connection tracking).

Cadascuna de les taules té les sequències de regles (chains). I cada regla consisteix en l'aparellament amb els paquets de dades (match) i decisions (targets) per determinar que es farà amb els paquets de dades aparellats.

4. Vulnerabilitats

Farem un breu resum de que és una vulnerabilitat, els tipus més coneguts d'atacs per tal d'ajudar-nos a comprendre millor les decissions d'algunes regles dels scripts.

En seguretat informàtica, una **vulnerabilitat** fa referència a una feblesa d'un sistema que permet a un atacant violar la integritat, la privadesa, el control d'accés, la disponibilitat, la consistència o el mecanisme d'auditoria del sistema, o les dades i programes que hostatja. Les vulnerabilitats poden ser resultat d'errors en els programes o en el disseny del sistema. Una vulnerabilitat pot ser teòrica o pot tenir un mecanisme d'explotació (*exploit*) conegut. Les vulnerabilitats són d'especial interès quan el programa que les conté opera amb privilegis especials, realitza autentificacions o permet un accés fàcil a les dades d'usuari o altres recursos (com ara servidors o bases de dades).

Poden ser tipicament clasificats en set categories:

4.1 Exploits

És el nom amb que s'identifica un programa informàtic malèvol, o part d'un programa, amb la finalitat de aprofitar-se de qualsevol feblessa o deficiència d'altre programes. L'objectiu és la destrucció o inhabilitació del sistema atacat.

4.2 Eavesdropping o escoltes secretes

Eavesdropping (*escoltar secretament)*, s'utilitza amb ambits relacionats amb segurerat, per exemple, escoltes telefòniques.

4.3 Enginyeria social i error humà

Normalment es tracta d'atacs no relacionats totalment amb el software o programes informàtics, en els que el paper principal és el de trobar la informació directament dels usuaris fent-se passar per institucions legítimes. Per exemple, trucades telefòniques o e-mails demanant el número de compte corrent d'un banc.

4.4 Denegació de Servei (DOS)

Es tracta d'un atac a un sistema d'ordinadors o xarxa que provoca que un servei o recurs sigui inaccesible als usuaris legítims. Normalment provoca la pérdua de connectivitat per consum de l'ample de banda de la xarxa de la víctima o sobrecàrrega dels recursos computacionals del sistema de la víctima.

D'aquest atac en parlarem més endavant amb més deteniment perque algunes de les regles dels scripts tenen precisament com a objectiur evitar aquests tipus d'atacs als nostres sistemes.

4.5 Atacs indirectes

Quan s'utilitzen recursos anònims de la xarxa per tal de fer l'atac a la víctima.

4.6 Backdoors

Un backdoor és una sequència especial dintre del codi de programació a partir del qual el programador pot accedir-hi o escapar d'un programa en cas d'emergència.

Al mateix temps aquestes portes també poden ser perjudicials degut a que els atacants que les descubreixin tenen un forat de seguretat al sistema del que poden gaudir i aprofitar-se per tal de fer un atac de forma bastant còmoda.

Per exemple, al llibre "El nido del cuco" parla d'un pirata informàtic que es va aprofitar d'una fallida del software (concretament un editor de Linux) per tal de fer un eavesdropping.

4.7 Atacs directes o presencials

Es basa en els atacs relacionats amb que l'atacant accedeix físicament a la màquina i elabora un plà d'atac fent servir la substitució de programes del sistema operatiu, de software de tercers comunment utilitzats, etc.

Si necessites més informació o estar més actualitzat sobre vulnerabilitats pots consultar la pàgina: http://www.cert.org.