Vulnerabilitats en xarxes

Jordi Herrera Joancomartí
Guillermo Navarro Arribas

PID_00178949

Universitat Oberta de Catalunya
www.uoc.edu

Índex

Introducció

En aquest mòdul es pretén donar una visió global de la complexitat i diversitat de les vulnerabilitats en xarxa. Per a això, es farà un repàs d'algunes vulnerabilitats presents en diferents nivells de xarxes, des de xarxes locals fins a protocols d'encaminament d'Internet.

No obstant això, aquest mòdul no pretén presentar una anàlisi exhaustiva de totes les possibles vulnerabilitats de xarxa que hi ha. Un objectiu d'aquesta envergadura implicaria un contingut molt més extens i de més detall i complexitat. S'aniran comentant algunes vulnerabilitats importants de protocols de xarxa, ja sigui per la seva importància des del punt de vista històric, didàctic, o actual. El mòdul se centra principalment en xarxes TCP/IP, i en concret en la versió IPv4, que és la més estesa i utilitzada avui dia.

Finalment, el mòdul també presenta els escàners de vulnerabilitats, eines bàsiques per a millorar la seguretat de sistemes informàtics. Els escàners de vulnerabilitats permeten detectar vulnerabilitats que poden derivar en problemes de seguretat.

Objectius

Els objectius que l'estudiant ha d'haver aconseguit després d'estudiar els continguts d'aquest mòdul són els següents:

1. Entendre la complexitat i diversitat de les vulnerabilitats de xarxa.
2. Identificar on afecten les vulnerabilitats de xarxa més rellevants.
3. Conèixer algunes de les principals vulnerabilitats de TCP/IP i les tecnologies associades.
4. Conèixer els escàners de vulnerabilitats com a eina per a detectar-les.

1. Conceptes bàsics

En aquest mòdul repassarem algunes vulnerabilitats de les xarxes informàtiques. Per a això, ens centrarem a donar una visió global del tipus de vulnerabilitats que ens podem trobar en les xarxes telemàtiques. Abans d'entrar-hi detalladament, repassem alguns conceptes bàsics.

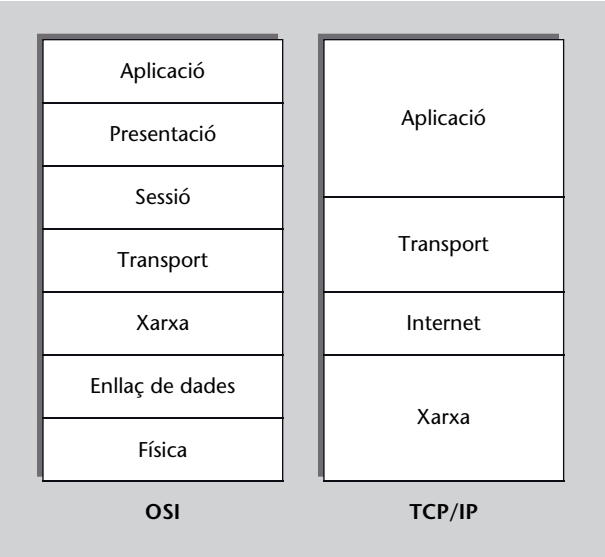
Les xarxes informàtiques s'organitzen en una pila o *stack* de protocols. El model OSI d'interconnexió de xarxes defineix 6 capes que van des del medi físic de transmissió de senyal fins a les aplicacions d'alt nivell que fan ús de la xarxa. Aquesta separació de protocols per capes permet definir i aïllar clarament la funcionalitat de cada protocol i aporta un disseny molt modular.

No obstant això, actualment i des d'un punt de vista més pràctic, s'ha imposat el model TCP/IP, que és el que defineix el paquet de protocols que van donar llum a Internet tal com es coneix actualment. En la figura 1 veiem les principals capes dels models OSI i TCP/IP, i la seva correspondència aproximada.

Vigència del model OSI

El model OSI continua essent utilitzat com a referència i ha estat implementat per alguns protocols, però la popularitat d'Internet ha fet que sigui el model TCP/IP el més utilitzat actualment.

Figura 1. Relació de capes en el model OSI i TCP/IP



En TCP/IP no hi ha una divisió per capes tan clara com en el model OSI i moltes vegades la frontera entre una capa i una altra és difusa.

Aquest mòdul se centra en el model TCP/IP. A continuació detallem la principal funcionalitat de cada capa:

- **Xarxa**: també anomenada *link layer* o *network access layer*, engloba les connexions de xarxa local.

- **Internet**: la capa d'interconnexió de xarxa (en anglès *Internet*) permet l'enviament de dades entre xarxes locals. Per a això, proporciona un sistema d'adreçament global (adreces IP) i l'encaminament de paquets de dades.

- **Transport**: s'encarrega de la transferència de dades d'extrem a extrem amb independència de la xarxa local. Pot incloure funcionalitat per al control d'errors, segmentació, control de flux, control de congestió, i l'adreçament a la capa d'aplicació mitjançant l'ús de *ports*.

- **Aplicació**: inclou protocols d'alt nivell utilitzats directament per les aplicacions, com per exemple HTTP (*hypertext trasfer protocol*), FTP (*file transfer protocol*) o SMTP (*simple mail trasport protocol*).

Per a revisar les vulnerabilitats de xarxa ens centrarem en tres grans blocs: protocols locals, interconnexió de xarxes i protocols d'extrem a extrem. Aquests blocs es corresponen vagament amb les capes TCP/IP de xarxa, Internet i transport, respectivament. La correspondència no és exacta, ja que ens centrem, per motius de simplicitat, en la funcionalitat pròpia de cada bloc amb certa independència de si els protocols tractats corresponen estrictament a una capa o una altra.

Amb l'objectiu de simplificar l'exposició s'ha optat per deixar de costat alguns temes importants. El primer és la capa d'aplicació; la seguretat de les aplicacions de xarxa i les seves vulnerabilitats seran tractades en el mòdul "Seguretat en aplicacions web", i altres aplicacions concretes es cobriran en assignatures concretes de seguretat en xarxes. De la mateixa manera, encara que algunes de les vulnerabilitats que veurem són comunes a molts tipus de xarxa, no es veuran problemes específics de xarxes sense fils, com IEEE 802.11 (Wi-Fi), Bluetooth, ZigBee, etc. Aquestes xarxes seran també tractades en assignatures específiques.

Així mateix, és important remarcar que ens centrem principalment en IPv4, ja que és la versió més estesa i estudiada, i ens permet presentar d'una manera global la problemàtica de la seguretat en xarxes cablades. És important recordar que s'està produint la llarga migració d'IPv4 a IPv6. En aquesta última versió alguns dels problemes de seguretat que veurem a continuació no estan presents a causa del disseny mateix dels protocols. L'estudi de la seguretat en IPv6 es veurà en altres assignatures específiques de xarxes.

Finalment, el mòdul repassa els escàners de vulnerabilitats com a eines bàsiques per a millorar la seguretat de xarxes i sistemes informàtics en general. Veurem quins tipus d'escàners hi ha, i també com s'usen i apliquen.

2. Protocols locals

Hi ha molts protocols de xarxa d'àrea local o LAN (*local area network*). Sens dubte, les xarxes locals cablades més utilitzades són les basades en Ethernet. La família de tecnologies Ethernet permet avui dia la creació de xarxes locals relativament extenses i capaces d'aconseguir gran velocitat de transmissió.

Ethernet utilitza adreces físiques o MAC (*media access control*), de 48 bits úniques globalment i assignades pel fabricant. Utilitza paquets denominats *trames* de 1.518 bytes amb un espai per a 1.500 bytes de dades. Quan una xarxa Ethernet es connecta a una altra xarxa (o a Internet) mitjançant TCP/IP és necessari "traduir" adreces físiques a adreces IP. Aquesta traducció es du a terme mitjançant un protocol de baix nivell denominat ARP (*address resolution protocol*).

Encara que Ethernet ha evolucionat molt des dels seus orígens, continua presentant problemes de seguretat i hi ha vulnerabilitats importants en aquest tipus de xarxes. A continuació en veurem algunes de les més representatives.

2.1. Detectors d'Ethernet

Un dels principals problemes o vulnerabilitats que presentava inicialment Ethernet era la facilitat de detectar trànsit local. Ethernet utilitzava una topologia de bus en què tots els paquets s'enviaven al bus i solament l'ordinador amb l'adreça de destinació del paquet el recollia.

En les targetes de xarxa Ethernet hi ha un mode de funcionament promiscu (*promiscuous mode*) que permet recollir tots els paquets que passen pel bus. Aquest mode de funcionament està pensat per a monitorar la xarxa en la detecció de problemes i permet l'ús de la targeta com a pont (*bridge*) per a la virtualització de maquinari. Però es pot fer un ús maliciós d'aquest mode per a detectar tot el trànsit local de la xarxa. Típics detectors de xarxa com *tcpdump*, *ettercap* o *Wireshark* poden detectar paquets Ethernet des d'una targeta en mode promiscu.

La majoria dels sistemes operatius requereixen privilegis administratius (de superusuari o *root*) per a poder operar una targeta en mode promiscu.

La tecnologia Ethernet ha evolucionat molt. De la clàssica topologia de bus es va passar a topologies d'estel utilitzant uns dispositius de xarxa denominats *concentradors*,* que simulaven la funcionalitat d'un bus, i per tant presenten els mateixos problemes que el bus. Actualment, el concentrador sol ser reemplaçat per un commutador**. A diferència d'un concentrador, un commutador Ethernet no simula el funcionament del bus, sinó que té la capacitat d'aprendre la topologia de la xarxa. És a dir, basant-se en les adreces MAC dels paquets que reben/envien els ordinadors, sap on està cadascun i solament envia els paquets destinats a aquest ordinador pel seu cable corresponent. D'aquesta manera, no solament s'aconsegueix minimitzar el trànsit de tota la xarxa, sinó que a més impossibilita que un ordinador en mode promiscu pugui rebre tots els paquets que circulen per la xarxa.

*En anglès *hub*.

**En anglès *switch*

Hi ha vulnerabilitats inherents als actuals commutadors Ethernet que permeten convertir un commutador en un concentrador i conseqüentment detectar tot el trànsit de la xarxa des d'un ordinador. Aquesta vulnerabilitat es pot explotar amb un atac de *MAC flooding*.

2.1.1. MAC flooding

Un commutador Ethernet manté una taula anomenada CAM (*content addressable memory*), on estableix un vincle entre adreces MAC i ports físics del commutador mateix. Aquesta taula permet al commutador enviar els paquets únicament al seu destinatari pel port físic corresponent. El commutador estableix la taula CAM observant el trànsit generat i destinat a cada ordinador connectat a aquest.

El problema és que la taula CAM d'un commutador té una memòria limitada i, per tant, un atacant pot saturar aquesta taula amb el propòsit de deixar-la inutilitzada. Per a això, bombardeja el commutador amb paquets Ethernet amb adreces MAC d'orígens diferents, la qual cosa provoca que el commutador les afegeixi a la taula CAM fins que aquesta s'esgota. En aquest moment, atès que el commutador no pot afegir més entrades, passa a un mode de funcionament conegut com a *failopen*, en el qual comença a actuar com un concentrador. En aquest mode el commutador envia els paquets en difusió a tots els ordinadors de la xarxa.

Atac *MAC flooding*

El *MAC flooding* és un atac molt conegut i estudiat. Hi ha nombroses eines que permeten estudiar el comportament de la xarxa en fer l'atac, com la utilitat *macof* del paquet *dsniff* (http://monkey.org/~dugsong/dsniff/).

Actualment es pot intentar mitigar aquesta vulnerabilitat utilitzant sistemes de monitoratge de xarxa. Molts fabricadors de commutadors permeten limitar el nombre màxim d'adreces MAC per a cada port físic (tècnica coneguda com a *port security*). També hi ha mecanismes per a requerir l'autenticació amb servidors d'autenticació i autorització.

2.2. Modificació d'adreces MAC

L'adreça física d'Ethernet és assignada pel fabricant i tradicionalment estava inequívocament associada a la targeta de xarxa. És a dir, aquesta adreça és única globalment i no es pot modificar. Això va fer que es desenvolupessin mecanismes de control d'accés basats en adreces MAC.

Per exemple, una xarxa pot permetre l'accés només a unes adreces MAC concretes. Un altre exemple molt comú avui dia són les xarxes (generalment sense fils) que permeten una connexió gratuïta a la xarxa, per exemple, de 15 minuts al dia; en aquestes, el control sobre el temps de connexió de cada usuari se sol fer mitjançant l'adreça MAC.

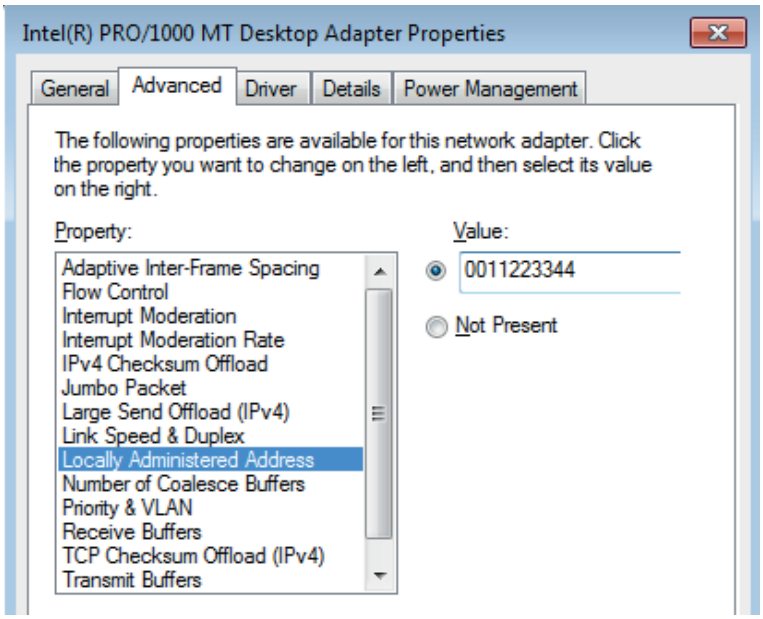
Actualment una adreça física Ethernet pot ser fàcilment modificada. Aquesta funcionalitat és actualment tan comuna que molts sistemes operatius inclouen l'opció de modificar l'adreça MAC amb les eines pròpies de gestió de xarxa, sense necessitat de programes externs.

Per exemple, utilitzant l'ordre *ifconfig* o les utilitats *iproute2* de Linux podem modificar l'adreça física de la interfície de xarxa *eth0*:

```
# ifconfig eth0 hw ether 00:11:22:33:44:55
# ip link set dev eth0 address 00:11:22:33:44:55
```

En el Windows es pot modificar des de les propietats de l'adaptador de xarxa (podeu veure la figura 2).

Figura 2. Modificació de l'adreça MAC en el Windows 7



L'actual facilitat per a canviar adreces físiques representa una vulnerabilitat important en sistemes de control d'accés o autenticació de xarxa basats en aquestes adreces.

2.3. Vulnerabilitats en el protocol ARP

Com hem comentat, el protocol *address resolution protocol* (ARP) permet traduir adreces MAC en adreces IP. En xarxes locals que suporten difusió com Ethernet, el funcionament d'ARP és el següent. Suposem que l'ordinador A vol conèixer l'adreça IP de B (IP_B) però desconeix la seva adreça física F_B:

Observació

En realitat, ARP es va dissenyar per a traduir adreces físiques a adreces de protocol superior d'interconnexió (no necessàriament IP); aquí fem referència a IP perquè és el més usat.

1) A envia en difusió una petició ARP preguntant qui té l'adreça IP_B.

2) B contesta amb una resposta ARP a A dient que ell té l'adreça IP_B (és a dir, que IP_B correspon a l'adreça física F_B).

Per a evitar estar fent peticions ARP contínuament, cada ordinador manté una taula amb les correspondències entre adreça física i adreça IP anomenada *memòria cau ARP*. Les entrades tenen una caducitat d'aproximadament 20 minuts. Un punt important és que qualsevol petició ARP és utilitzada per la resta dels ordinadors per a actualitzar l'entrada corresponent a l'emissor.

Aquest protocol actualment presenta vulnerabilitats difícils de solucionar. La majoria dels problemes de seguretat d'ARP es basen en l'enviament de missatges ARP falsos per a "enverinar" les memòries cau ARP, és a dir, per a introduir informació falsa. En anglès, aquesta tècnica rep el nom d'*ARP poisoning*. *ARP poisoning* permet diversos atacs diferents, com:

***ARP poisoning* també es coneix amb els noms: *ARP spoofing*, *ARP flooding* o *ARP poison routing*.**

- **Denegació de servei**: es pot aconseguir que un ordinador no rebi cap paquet en difondre una adreça física inexistent associada a la seva adreça IP real. Si la víctima de la denegació de servei és l'encaminador o porta d'enllaç de la xarxa local, s'aconsegueix aïllar la xarxa local de l'exterior.

- **Man in the middle (MITM)**: un atacant es pot fer passar per un altre ordinador (víctima) i rebre així tots els paquets destinats a aquesta víctima.

L'*ARP poisoning* pot tenir usos legítims, per exemple per a adreçar accessos de xarxa a un portal d'autenticació (típicament usat en hotels, xarxes universitàries o xarxes d'accés públic), o en sistemes de redundància perquè un servidor pugui prendre el lloc d'un altre en cas que aquest sofreixi algun contratemps.

Actualment solament hi ha solucions limitades per a mitigar aquestes vulnerabilitats. Algunes solucions actuals són incloure entrades fixes en la memòria cau ARP, generalment les corresponents a ordinadors crítics com encaminadors, l'ús de *port security* en els commutadors, o el monitoratge de la xarxa a la recerca de comportament inusual.

Vegeu també

La tècnica del **port security** s'estudia en el subapartat 2.1.1..

3. Interconnexió de xarxes

Dins de la interconnexió de xarxes ens centrem en el protocol IP i els serveis associats. Atesa la complexitat d'Internet i totes les tecnologies associades a la interconnexió de xarxes, el nombre de vulnerabilitats potencials és molt gran. En aquest apartat n'enumerem algunes a manera il·lustrativa i amb finalitats didàctiques.

3.1. Vulnerabilitats en IP

Veiem a continuació algunes de les vulnerabilitats del protocol IP especialment rellevants a partir dels atacs següents:

- **IP spoofing**: consisteix a generar paquets IP amb l'adreça d'origen falsa. Aquesta vulnerabilitat se sol explotar amb l'objectiu de fer atacs de denegació de servei o suplantar un ordinador concret.

Vegeu també

Sobre els atacs de denegació de servei podeu veure el subapartat 4.1.1..

- **Packet-of-death**: IP ha sofert algunes vulnerabilitats en la implementació. L'enviament de paquets IP deliberadament erronis pot causar problemes importants en algunes implementacions. Un exemple és l'ús de la mateixa adreça IP com a origen i destinació (*land attack*).

- **Vulnerabilitats en la fragmentació**: IP pot fer fragmentació de paquets per a adaptar-se a les mides de paquets de xarxes locals. L'enviament de fragments erronis on se superposen els camps de dades ha donat problemes en algunes implementacions. Un cas conegut és el *teardrop attack*, que explotava una vulnerabilitat en la implementació d'SMBv2 del Windows Vista.

Teardrop attack

Teardrop attack és un atac que explota la vulnerabilitat CVE-2009-3103. Se'n pot consultar la publicació a: http://www.microsoft.com/technet/security/advisory/975497.mspx.
Es pot trobar més informació sobre vulnerabilitats en la fragmentació IP en l'RFC 1828 (secció de referències).

- **IP source routing**: IP inclou un parell d'opcions que permeten especificar la ruta (parcial) de retorn que ha de seguir el paquet de resposta. Això permet que un atacant que utilitzi *IP spoofing* amb una adreça d'origen d'un ordinador de confiança de la víctima pugui rebre el paquet de resposta. Actualment aquestes opcions no se solen utilitzar, i molts dispositius de xarxa bloquegen el pas de paquets amb aquestes opcions.

3.2. Vulnerabilitats en ICMP

El protocol ICMP (*Internet control message protocol*) és un protocol de control i notificació d'errors del protocol IP que ha presentat algunes vulnerabilitats

importants, generalment associades a atacs de denegació de servei. A continuació, detallem alguns atacs que exploten vulnerabilitats d'ICMP:

- **Ping flooding**: atac clàssic de denegació de servei que utilitza missatges *echo request* (*ping*) d'ICMP.

- **Ping of death**: atac d'interès històric que va afectar gairebé totes les implementacions d'ICMP fins al final dels noranta. Consisteix a enviar un paquet ICMP de més grandària que el màxim permès per IP fragmentat. Això provocava un desbordament de memòria intermèdia en l'ordinador de destinació.

- **Smurf attack**: atac de denegació de servei en el qual l'atacant envia missatges de *ping* en difusió amb l'adreça d'origen de la víctima. Això provoca que tots els ordinadors que reben el paquet enviïn la resposta del *ping* a la víctima. En aquest cas la vulnerabilitat es troba en l'ús de missatges ICMP en difusió. Actualment, els ordinadors no contesten *pings* enviats en difusió. Així mateix, es va modificar l'estàndard per a requerir que per defecte els encaminadors bloquegin missatges enviats en difusió.

Tractament de missatges de difusió

En general, l'ús de missatges de difusió sol implicar vulnerabilitats importants en la interconnexió de xarxes. Amb el temps s'ha anat limitant molt l'ús. Per exemple, podeu veure: D. Senie (1999). *Changing the Default for Directed Broadcasts in Routers*. RFC 2644. IETF, The Internet Society.

3.3. Vulnerabilitats en DNS

DNS (*domain name system*) permet la resolució de noms de domini mitjançant servidors organitzats jeràrquicament a partir de 13 servidors arrel (9 distribuïts geogràficament utilitzant *anycast*). DNS presenta molts avantatges. És un sistema distribuït, eficient en la resolució de noms i tolerant a fallades. Hi ha, no obstant això, algunes vulnerabilitats en el DNS que poden donar lloc a atacs importants:

- **DNS spoofing**: consisteix a donar informació errònia de manera deliberada sobre la correspondència d'adreça IP a nom de domini. L'objectiu pot ser per exemple associar una IP "falsa" a un nom de domini conegut (amb la qual cosa es pot redirigir el trànsit a aquest domini). Hi ha diferents maneres de fer aquests atacs. La més senzilla és posar un servidor DNS que emeti respostes falses o que pugui suplantar un servidor conegut (per exemple, mitjançant *IP spoofing*), també es pot interceptar la petició de DNS i respondre abans del que ho faria el servidor legítim. És important tenir en compte que perquè una resposta sigui acceptada com a legítima ha de complir els punts següents:

Vegeu també

L'*IP spoofing* s'estudia en el subapartat 3.1..

– Tornar a la mateixa adreça IP que va emetre la petició.
– Tornar pel mateix port des d'on es va enviar la petició.
– Que la resposta correspongui a la petició.
– Que el número de transacció coincideixi amb la petició. Aquest número és teòricament aleatori i permet vincular resposta a petició.

En molts casos la facilitat per a predir el número de transacció ha estat una vulnerabilitat important, similar a la predicció de números de seqüència en TCP. Un atacant pot falsejar una resposta DNS sense necessitat de veure la petició per a saber el número de transacció. El fet que DNS funcioni sobre UDP també facilita aquest tipus d'atacs. És important remarcar també que, atesa l'organització jeràrquica de DNS, aquests atacs es poden fer directament sobre el client o algun servidor intermedi.

Vegeu també

La predicció de números de seqüència s'estudia en el subapartat 4.1.2. d'aquest mòdul.
Les vulnerabilitats en UDP s'estudien en el subapartat 4.2..

- **DNS cache poisoning**: per a millorar l'eficiència de DNS cada servidor manté una memòria cau amb les últimes resolucions fetes (respostes de DNS) per a poder contestar a futures peticions de manera ràpida. Igual que en el cas d'ARP, es pot forçar l'entrada de relacions de nom de domini a adreça IP falsa en aquesta memòria cau. Molts atacs de *DNS spoofing* busquen precisament "enverinar" la memòria cau de servidors intermedis (per exemple, el DNS d'un ISP) amb l'objectiu que tots els seus clients quedin afectats.

- **DNS amplification attacks**: els atacs d'amplificació de DNS són uns atacs de denegació de servei que exploten el fet que les peticions de DNS es resolen recursivament i que una petició de mida petita (60 bytes) pot arribar a generar respostes més grans ($\leq$ 512 bytes). De manera similar als atacs *smurf*, s'envien moltes peticions amb l'adreça IP d'origen de la víctima que rebrà totes les respostes. La denegació de servei s'agreuja per la gran mida que poden aconseguir aquestes respostes (amplificació). A l'octubre del 2002 es va fer un gran atac d'amplificació en el qual les víctimes eren els servidors arrel de DNS, que va aconseguir comprometre'n algun. El fet que no tots els servidors fossin compromesos és vist com un avantatge de la redundància de DNS. Un atac similar va ser repetit al setembre del 2007 i va aconseguir afectar dos servidors arrel.

Enllaç d'interès

Els servidors arrel de DNS són coneguts en anglès com a *root name servers*. Es pot consultar informació sobre aquests servidors arrel a: http://www.root-servers.org.

Vegeu també

Els atacs *smurf* s'estudien en el subapartat 3.2. d'aquest mòdul.

DNS va ser dissenyat sense tenir en compte la seguretat, i les seves vulnerabilitats han estat importants i fins i tot detallades en l'RFC 3833. Actualment hi ha DNSSEC (*domain name system security extensions*), un conjunt d'especificacions de la IETF que busca solucionar els problemes de seguretat de DNS. DNSSEC proporciona principalment autenticació i integritat.

Lectura recomanada

D. Atkins; R. Austein (2004). *Threat Analysis of the Domain Name System (DNS)*. RFC 3833.
Disponible a: http://www.ietf.org/rfc/rfc3833.txt

3.4. Vulnerabilitats en OSPF i BGP

IP utilitza diversos protocols d'encaminament. D'una banda, hi ha els protocols d'encaminament interns a un sistema autònom, coneguts com a IGP (*interior gateway protocol*), i els que s'utilitzen per a l'encaminament entre sistemes autònoms, EGP (*exterior gateway protocol*).

Possiblement l'IGP més utilitzat actualment sigui l'OSPF (*open shortest path first*), un protocol d'encaminament adaptatiu basat en *link-state* que s'utilitza com a protocol d'encaminament interior en sistemes autònoms. Hi ha diver-

ses vulnerabilitats en OSPF que permeten a un atacant introduir informació d'encaminament falsa en el sistema autònom. Això facilita diferents atacs, com la denegació de servei o la "desconnexió" d'una xarxa local (en anglès se sol denominar *blackhole*), desviació de trànsit, etc.

Actualment OSPF permet incorporar diferents mecanismes d'autenticació que poden mitigar algunes d'aquestes vulnerabilitats però, en general, és difícil defensar-se d'atacs interns en OSPF.

D'altra banda, el protocol EGP que s'utilitza avui dia en Internet és BGP (*border gateway protocol*). BGP ha sofert diverses vulnerabilitats que s'han intentat resoldre al llarg del temps. Les últimes versions del protocol incorporen mecanismes per a autenticar els encaminadors que anuncien rutes BGP.

El principal problema que presenta actualment BGP és la credibilitat dipositada en els encaminadors de confiança. En general, un encaminador BGP està configurat per a rebre i emetre anuncis de rutes únicament d'encaminadors de confiança, la qual cosa facilita la possibilitat d'atacs interns.

Pakistan Telecom

Un cas famós va ser protagonitzat per Pakistan Telecom (el principal ISP del Pakistan), que al febrer del 2008 va començar a anunciar que els rangs d'adreces IP corresponents a YouTube es trobaven dins del sistema autònom de Pakistan Telecom. L'origen d'aquest anunci es troba en una ordre governamental que obligava tots els ISP de Pakistan a bloquejar l'accés a uns vídeos de YouTube. Per a això, Pakistan Telecom posa el rang d'adreces IP de YouTube com a intern al sistema autònom propi. El problema és que no van evitar que aquestes rutes falses s'anunciessin per BGP a ISP de confiança. Aquests encaminadors al seu torn van redistribuir les rutes als seus encaminadors de BGP de confiança, i així fins a arribar a abastar gran part d'Internet. Això va provocar que tot el trànsit destinat a YouTube es readrecés a Pakistan Telecom i les adreces IP de YouTube fossin inaccessibles. Una vegada detectat el problema es va poder aïllar l'encaminador BGP que emetia aquestes rutes falses, de manera que els encaminadors BGP ho podien excloure de les seves llistes d'encaminadors de confiança.

Enllaç d'interès

Es pot consultar l'informe elaborat per RIPE sobre l'incident de Pakistan Telecom a: http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

La importància d'Internet avui dia i l'important paper que exerceixen en el seu funcionament els protocols d'encaminament (especialment BGP), provoca que qualsevol vulnerabilitat i, conseqüentment, atac a aquests protocols, tingui conseqüències molt importants. Per exemple, el cas de Pakistan Telecom va durar tan sols dues hores, però les seves conseqüències van poder ser importants.

Actualment hi ha vulnerabilitats en BGP difícils de solucionar, per la qual cosa s'opta per monitorar contínuament el funcionament de BGP per a poder detectar problemes i actuar ràpid.

4. Protocols d'extrem a extrem

Dins dels protocols d'extrem a extrem utilitzats per TCP/IP cal destacar pel seu ús extens: TCP (*transmission control protocol*), i UDP (*user datagram protocol*).

Aquests protocols introdueixen l'ús de ports que permeten adreçar dades de la capa inferior IP a aplicacions concretes. Això és considerat per alguns autors com una vulnerabilitat, ja que possibilita l'ús d'escàners de ports per a obtenir informació sobre quins serveis està oferint un ordinador, fins i tot informació addicional, com el sistema operatiu, la versió, etc. No obstant això, altres autors no ho consideren una vulnerabilitat, ja que no consideren que la informació obtinguda per aquests sistemes sigui crítica des del punt de vista de la seguretat.

4.1. Vulnerabilitats de TCP

TCP proporciona un servei genèric de transmissió fiable de dades d'extrem a extrem. S'encarrega de controlar errors en la transmissió, l'ordre dels paquets, la detecció de duplicats, el control de velocitat de transmissió, etc.

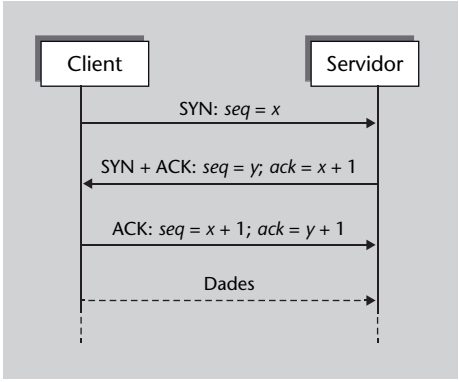
TCP és un protocol orientat a connexió. S'estableix una connexió entre els dos extrems que es manté durant la transmissió de dades. Aquesta connexió es crea mitjançant el denominat *3-way handshake*.

Com veiem en la figura 3, la connexió s'estableix amb tres missatges: un missatge de tipus SYN (de sincronització), que el servidor contesta amb un SYN i ACK (sincronització i reconeixement); finalment el client envia un ACK (reconeixement). Una vegada establerta la connexió, el client i el servidor es poden enviar dades que seran reconegudes cada cert temps (mitjançant missatges ACK) pel receptor.

Com veiem, una de les tasques de l'establiment de connexió és fixar els números de seqüència de client i servidor (en la figura 3, *seq* i *ack*). Aquests números s'utilitzen per a identificar els bytes de dades enviats i permeten fer una gestió del flux de dades: control de l'ordre d'enviament de segments, pèrdua, duplicats, etc. El número d'*ack* confirma la recepció correcta de tots els missatges amb número de seqüència igual o inferior.

A continuació veurem alguns atacs i vulnerabilitats de TCP.

Figura 3. Establiment de connexió en TCP



4.1.1. SYN flooding

En l'establiment de sessió, quan el client envia el missatge SYN, el servidor contesta (SYN+ACK) i es queda esperant l'ACK del client. Què succeeix si el client no envia aquest ACK?

Com cal esperar, el servidor espera un temps prudencial, i si no rep l'ACK dóna la connexió per perduda. Aquesta funcionalitat presenta una vulnerabilitat important de TCP que pot ser explotada per a fer atacs de denegació de servei. La idea és bombardejar un servidor amb peticions de connexió i no fer l'últim ACK. D'aquesta manera, el servidor es queda amb connexions mig establertes que consumeixen, durant un temps determinat, recursos del servidor (memòria, principalment). Si hi ha suficients intents simultanis, es pot arribar a saturar el servidor i esgotar-ne els recursos.

Publicació de la vulnerabilitat

Es pot consultar la publicació en 1995 i 1996 de la vulnerabilitat relativa a *SYN flooding* i *IP spoofing* a: http://www.cert.org/advisories/CA-1996-21.html

Aquest atac es coneix com a *SYN flooding*, i va ser molt important quan es va descobrir. Hi ha una variant basada en *IP spoofing*, en la qual el primer missatge SYN del client porta una adreça IP d'origen falsa, per la qual cosa resulta impossible al servidor enviar el SYN+ACK.

Avui dia aquesta vulnerabilitat no sol representar un risc important, ja que hi ha diversos mecanismes que prevenen enfront d'atacs de *SYN flooding*.

Prevenció de *SYN flooding*

Hi ha un RFC sobre mecanismes de prevenció de *SYN flooding*:
W. Eddy (2007). *TCP SYN Flooding Attacks and Common Mitigations*. RFC 4987. IETF Internet Society. http://tools.ietf.org/rfc/rfc4987.txt.

4.1.2. Predicció de números de seqüència

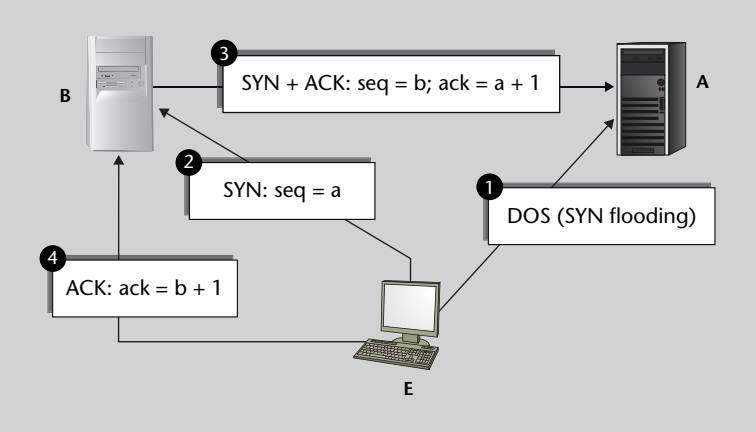
La facilitat a l'hora de predir els números de seqüència d'una connexió TCP va resultar ser una vulnerabilitat de seguretat important. Per a veure-ho, explicarem breument un dels atacs informàtics més coneguts i documentats en la història de la seguretat informàtica.

El dia de Nadal de 1994, un expert informàtic anomenat Kevin Mitnick va fer un atac a l'ordinador de Tsutomu Shimomura, situat a la Universitat de Califòrnia, a San Diego. L'atac pretenia obtenir el codi font d'un model de telèfon mòbil (el que tenia Mitnick), que estava emmagatzemat a l'ordinador de Shimomura. Mitnick pretenia modificar el programari del telèfon i així intentar evitar els sistemes de seguiment i localització d'aquest aparell.

Sense entrar en gaires detalls, l'atac va consistir en els passos que es detallen a continuació (podeu veure també la figura 4):

1) L'atac s'inicia des d'un servidor extern *E*, al qual l'atacant ha pogut accedir amb anterioritat.

Figura 4. Atac de Mitnick



2) Des de la màquina externa *E* es recopila informació de l'objectiu i es descobreix que entre dos servidors *A* i *B* hi ha una relació de confiança. Aquesta permetia fer connexions d'un a l'altre a partir de la seva adreça IP. És a dir, el servidor *A* accepta peticions de connexió del servidor *B*.

3) Des de *E* es fa un atac de *SYN-flooding* a *A* per a evitar que aquest servidor pugui respondre a qualsevol missatge. D'aquesta manera, es vol *silenciar* el servidor *A*, amb l'objectiu que l'atacant es pugui fer passar per aquest servidor, i iniciar així una connexió a *B*. Per a suplantar el servidor *A*, l'atacant fa un atac d'*IP spoofing* que li permeti suplantar l'adreça IP de *A*. En aquest punt l'atacant pot enviar missatges a *B* fent-se passar per *A* però no podrà veure la resposta que genera, ja que no es troba a la mateixa xarxa local.

4) Per a poder establir una connexió amb *B* l'atacant necessita predir com contestarà *A* a l'intent de connexió de *B* (atès que no pot veure aquesta contestació). Això és, predir el número de seqüència TCP dels missatges que genera *B*. La connexió TCP consta de 3 tres passos, com es detalla en la figura 3, en la qual els números de seqüència *seq* i *ack* han de coincidir.

5) Una vegada es pot predir el número de seqüència, l'atacant pot fer una connexió al servidor *B* per a forçar que *B* passi a acceptar connexions de qualsevol adreça IP.

Lectura complementària

Per a saber més sobre la història de Mitnick i Shimomura, es poden consultar els llibres següents (cadascun presenta un punt de vista diferent):
T. Shimomura; J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It*. Hyperion Books.
J. Littman (1997). *The Fugitive Game: Online with Kevin Mitnick*. Little, Brown and Company publishers.
J. Goodell (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick-And the Man Who Hunted Him Down*. Dell publishers.

Vegeu també

L'atac *SYN-flooding* s'estudia en el subapartat 4.1.1..
Per a saber més sobre l'atac d'*IP spoofing* podeu veure el subapartat 3.1. d'aquest mòdul.

6) L'atacant pot ara accedir a *B* des de qualsevol lloc.

Una vegada Mitnick va obtenir accés al servidor de Shimomura va poder copiar tot el codi font que buscava. Aquest atac va donar lloc a un dels successos més sonats de la seguretat informàtica. Finalment, l'FBI, amb l'ajuda de Shimomura, va capturar Mitnick, que va acabar passant 5 anys a la presó.

La possibilitat de predicció de números de seqüència va resultar ser una vulnerabilitat important de TCP; avui dia les implementacions de TCP posen molt interès a generar els números de seqüència de la manera més aleatòria possible per a evitar aquest tipus de problemes.

4.2. Vulnerabilitats en UDP

User datagram protocol (UDP) és un protocol de transmissió d'extrem a extrem que ofereix la funcionalitat mínima. No proporciona cap dels mecanismes de control de flux de TCP.

La majoria de les vulnerabilitats d'UDP són pròpies d'errors d'implementacions concretes i no del protocol. D'aquesta manera, ens trobem amb un tipus d'atac conegut com a **UDP Bomb**, que explota vulnerabilitats presents en implementacions que fallen en rebre un datagrama UDP erroni o mal construït. Un error típic és especificar en la capçalera del datagrama una mida que no es correspon amb la mida real del datagrama. Això pot produir un desbordament de memòria intermèdia en la implementació del protocol.

Hi ha altres atacs, com el **fraggle attack**, que exploten l'ús (i encaminament) d'adreces de difusió. Aquest és un atac idèntic a l'atac *smurf* d'ICMP però amb paquets UDP, en aquest cas dirigits als serveis UDP *echo* i *chargen* (ports UDP 7 i 19, respectivament).

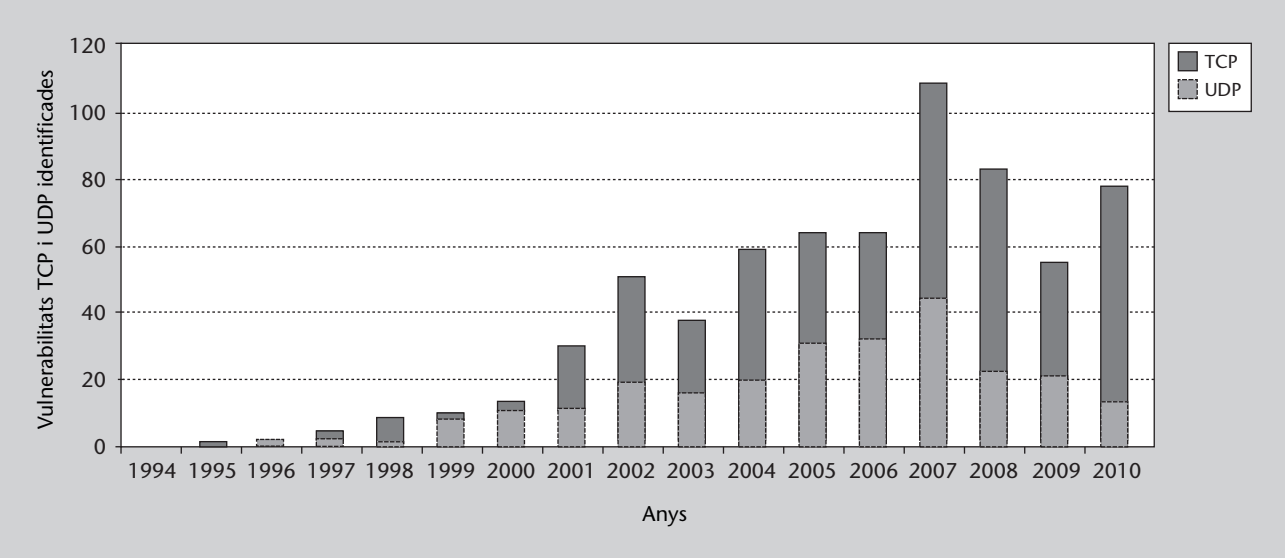
Vegeu també

L'atac *smurf* s'estudia en el subapartat 3.2. d'aquest mòdul.

El fet d'utilitzar UDP de vegades facilita l'explotació d'altres vulnerabilitats a causa de la falta de control en comparació de TCP. Per exemple, fer un atac de MITM usant *IP spoofing* és molt més senzill sobre UDP que sobre TCP, ja que no és necessari fer el segrest de sessió descrit en el subapartat 4.1.2..

Aquí veiem un cas clar de la relació entre la complexitat d'un sistema i la presència de vulnerabilitats. Un sistema complex sol presentar més vulnerabilitats que un més senzill. D'aquesta manera, el nombre de vulnerabilitats que afecten TCP és molt més gran que les associades a UDP. Com a exemple, en la figura 5 es mostra el nombre de vulnerabilitats reportades que fan referència a UDP i a TCP. És important remarcar que això no significa que UDP sigui més segur que TCP, simplement que presenta menys vulnerabilitats. És més, generalment es considera UDP un protocol de transport més insegur que TCP a causa que no fa cap control sobre el flux de dades.

Figura 5. Vulnerabilitats relatives a TCP i UDP



Font: National Vulnerability Database (NVD)

5. Escàners de vulnerabilitats

Entre les eines i els mecanismes que ens permeten millorar la seguretat dels sistemes informàtics es troben les que estan enfocades a la detecció d'anomalies que poden derivar en problemes per a la seguretat del sistema. En aquest sentit, podem fer una distinció entre les eines que permeten detectar una vulnerabilitat i aquelles que permeten detectar un atac. Si bé la distinció entre vulnerabilitat i atac sovint pot quedar diluïda, quant a la detecció es considera que les eines que permeten la detecció de vulnerabilitats queden englobades dins del que es coneix com a escàners de vulnerabilitats, mentre que aquelles eines que s'utilitzen per a la detecció dels atacs s'inclouen dins de la família de sistemes de detecció d'intrusos. No obstant això, també pot succeir que un escàner de vulnerabilitats detecti un atac, ja que, per exemple, un atac pot posar al descobert o generar una nova vulnerabilitat.

En aquest apartat ens centrarem solament en els escàners de vulnerabilitats, que permeten detectar les vulnerabilitats d'un sistema.

5.1. Característiques generals dels escàners

Els **escàners de vulnerabilitats** són un conjunt d'eines que ens permeten detectar les vulnerabilitats d'un sistema, ja sigui per mitjà de simulacions d'atacs, ja sigui perquè es detecta una configuració que implica una deficiència de seguretat.

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

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

2) En la segona etapa, aquests resultats són organitzats i comparats amb unes bases de dades de regles i signatures que permeten identificar configuracions insegures.

3) Finalment, es generarà un informe amb les diferències entre tots dos conjunts de dades.

El principal avantatge dels escàners de vulnerabilitats és que permeten la detecció i solució de la vulnerabilitat abans que aquesta pugui ser explotada per a

fer un atac. No obstant això, cal tenir en compte que la majoria de les vulnerabilitats detectades per un escàner no poden ser reparades per l'escàner mateix. Aquest es limita a proporcionar una sèrie d'informació i informes que, en la majoria dels casos, requereixen una intervenció manual de l'administrador.

Com veiem, el mecanisme de treball dels escàners de vulnerabilitats s'assembla al dels antivirus, per la seva dependència d'una base de dades en la qual s'inclouen les regles que tindrà en compte l'escàner. Per aquest motiu, els escàners de vulnerabilitats comparteixen certes característiques amb els antivirus. Per exemple, una de les limitacions bàsiques dels escàners de vulnerabilitats és que únicament permeten identificar les vulnerabilitats que estan ja tipificades en la seva base de dades. Això implica que, en general, solament es puguin detectar vulnerabilitats en programari estàndard, de manera que, per exemple, aplicacions web personalitzades no poden ser escanejades amb escàners de vulnerabilitats de propòsit general i necessiten analitzadors específics d'aplicacions web. D'altra banda, atesa la dependència de la base de dades de vulnerabilitats amb la qual treballa l'escàner, la freqüència d'actualització d'aquesta és un punt molt important que s'ha de tenir en compte per a la selecció d'un escàner de vulnerabilitats, atès que caldrà una actualització constant de la base de dades de referència perquè l'escàner pugui detectar les últimes vulnerabilitats publicades.

Bases de dades de vulnerabilitats

És important distingir entre les bases de dades dels escàners de vulnerabilitats i les bases de dades que mantenen els CERT. En aquestes últimes, la informació que s'inclou és una informació més descriptiva, mentre que les bases de dades dels escàners de vulnerabilitats incorporen, per a cada vulnerabilitat, un conjunt de tests que n'han de permetre la detecció.

Atesa la importància de la base de dades de vulnerabilitats en els escàners, hi ha un procediment per a determinar la compatibilitat del producte respecte a l'estàndard CVE (*common vulnerabilities and exposures*) que permet etiquetar les vulnerabilitats. Aquest procediment, establert per The Mitre Corporation, especifica els requisits que un escàner de vulnerabilitats ha de posseir perquè sigui compatible amb CVE. En concret, perquè un producte sigui compatible amb CVE ha de complir:

- **Cerca per CVE**: el producte certificat ha de permetre la cerca de vulnerabilitats en la seva base de dades utilitzant l'identificador CVE.

- **Sortida CVE**: la informació de la vulnerabilitat que ofereix el producte ha d'incloure l'identificador CVE.

- **Identificació**: el producte ha de proporcionar informació suficient de com identifica la vulnerabilitat de la seva base de dades amb la versió específica de CVE i, al seu torn, ha d'intentar que aquesta identificació sigui tan precisa com sigui possible.

- **Documentació**: la documentació estàndard del producte ha d'incloure una descripció del CVE, la compatibilitat CVE, i els detalls de com els seus clients poden utilitzar la funcionalitat relacionada amb el CVE del seu producte o servei.

El compliment d'aquestes condicions per part d'un escàner és rellevant, atès que permet als usuaris complementar les informacions que l'escàner propor-

ciona en els seus informes utilitzant fonts externes, com els CERT, atès que la identificació de la vulnerabilitat serà unívoca. D'altra banda, la identificació unívoca de les vulnerabilitats mitjançant el seu codi CVE també permet comprovar el grau d'actualització de la base de dades de l'escàner.

Programari per a escanejar vulnerabilitats

Hi ha diferents empreses que comercialitzen programari per a escanejar vulnerabilitats. Les principals diferències entre els diferents productes es troben en les seves característiques, com, per exemple, la raó de falsos positius que genera la detecció, la varietat dels possibles sistemes operatius que permeten escanejar, els tipus de dispositius que poden escanejar (servidors, encaminadors, impressores de xarxa, etc.), el nombre diferent d'aplicacions que poden escanejar (bases de dades, servidors d'aplicacions PHP, Java, .NET, etc.), la freqüència d'actualització de la base de dades o la qualitat de la informació que reporten perquè els administradors puguin arreglar o eliminar la vulnerabilitat oposada.

5.2. Classificació dels escàners

Els escàners de vulnerabilitats admeten diferents tipus de classificació. La classificació més comuna que se solia associar amb els escàners de vulnerabilitat és la distinció pel que fa a la localització de l'escàner mateix. D'aquesta manera, els escàners es poden classificar en aquells basats en màquina (*host-based scanners*) i els escàners basats en xarxa (*network-based scanners*). Els primers són escàners situats en els dispositius mateixos que es volen escanejar, mentre que els segons se situen en servidors de la xarxa i permeten fer anàlisis d'altres màquines.

La sofisticació dels escàners basats en xarxa, i també l'aparició de noves tècniques per a escanejar vulnerabilitats, permeten una nova classificació més precisa. D'aquesta manera, podem classificar els escàners en funció de les seves habilitats d'escaneig:

- Escaneig intern i actiu d'un dispositiu
- Escaneig extern i actiu d'un dispositiu
- Escaneig extern i passiu d'un dispositiu

Com veurem en les descripcions de cadascun dels tipus, tots aquests escàners no són excloents (en el sentit que la utilització d'un tipus d'escàner no invalida els altres), ja que hi ha vulnerabilitats que es poden detectar amb un tipus d'escàner però no amb un altre. Per tant, un bon administrador de sistemes utilitzarà cadascun dels escàners per a detectar diferents tipus de vulnerabilitat.

5.2.1. Escaneig intern i actiu d'un dispositiu

L'escaneig intern i actiu d'un dispositiu es refereix a la possibilitat d'executar l'escàner mateix dins de la màquina que es pretén escanejar.

Aquesta característica permet un escaneig de dades de baix nivell, com poden ser serveis específics de la màquina, detalls de la configuració, el sistema de fitxers mateix, i també informació específica del programari i sistema operatiu que utilitza. Permet analitzar si els comptes creats en la màquina escanejada tenen contrasenyes per defecte, o fins i tot si no tenen contrasenyes. També permet verificar si el sistema ja ha estat atacat, analitzant l'existència de fitxers sospitosos o programes en execució amb privilegis inadequats.

Els motors d'anàlisi de vulnerabilitats d'aquest tipus estan molt relacionats amb el sistema operatiu que avaluen, la qual cosa provoca que el manteniment sigui una mica costós i en complica l'administració en entorns heterogenis.

Aquest tipus d'escanejos es poden fer mitjançant escàners basats en màquina i també utilitzant escàners basats en xarxa amb credencials. Els primers van ser els primers a utilitzar-se per a l'avaluació de vulnerabilitats. Es basen en l'obtenció de la informació mitjançant consultes al sistema o per mitjà de la revisió de diferents atributs d'aquest.

COPS

Un dels primers escàners de vulnerabilitats en sistemes Unix va ser COPS, una eina que s'encarregava d'analitzar el sistema a la recerca de problemes de configuració típics, com per exemple permisos erronis de fitxers, directoris i serveis, etc.

Exemple

Un simple guió de sistema com el que es mostra en la figura 6 s'encarregaria d'avisar mitjançant correu electrònic a l'administrador del sistema en cas de trobar entrades anòmales en el fitxer de contrasenyes del sistema:

Figura 6. Exemple d'escàner basat en màquina

```
#!/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);
```

Alternativament, també es pot fer un escaneig intern i actiu mitjançant un escàner de xarxa, la qual cosa es coneix com a escàner basat en xarxa amb credencials. D'aquesta manera, l'escàner, accedint al sistema amb les credencials, normalment per mitjà de connexions SSH, pot executar els mateixos controls que tradicionalment es feien només amb els escàners basats en màquina.

Vegeu també

En el subapartat 5.2.2. veurem una descripció més detallada dels escàners basats en xarxa.

5.2.2. Escaneig extern i actiu d'un dispositiu

L'escaneig extern i actiu d'un dispositiu és un tipus d'escaneig que es fa mitjançant les eines conegudes com a escàners basats en xarxa. En aquest cas, aquest escaneig es pot categoritzar com un escaneig sense credencials, en el sentit que l'actor que escaneja un dispositiu no hi té accés. En aquesta situació, la informació obtinguda del procés d'escaneig és una informació semblant a la que pot veure un atacant (òbviament, que no hagi tingut accés al dispositiu).

Aquest tipus d'escàners de vulnerabilitats s'instal·la en una màquina que serà l'encarregada d'escanejar diferents dispositius de la xarxa. Per mitjà de la xarxa l'escàner obté la informació necessària, mitjançant les connexions que estableix amb l'objectiu que cal analitzar. Aquesta característica facilita la instal·lació dels escàners basats en xarxa, atès que en instal·lar-se en màquines diferents de les que escaneja no cal instal·lar cap programari concret en els dispositius que es pretenen escanejar.

Aquest tipus d'escàners permet la detecció de tallafocs mal configurats, servidors web vulnerables, riscos associats a programari utilitzat en els servidors, i també els riscos associats a una mala administració tant dels servidors com de la xarxa. Cal destacar que, a diferència dels escanejos interns, l'escaneig extern no permet detectar certes vulnerabilitats perquè no tenen accés al dispositiu mateix (ja que no posseeix les credencials necessàries).

Com ja hem comentat, a diferència dels escàners interns, que se situen en la mateixa màquina que es pretén escanejar, una consideració especial que cal tenir en compte en els escàners externs és la seva ubicació a la xarxa, atès que la ubicació on emplaçarem l'escàner serà determinant en el seu funcionament. Per exemple, si se situa l'escàner darrere d'un tallafocs això implica que els resultats de l'escaneig es veuran filtrats per les regles d'aquest. Si fem un escaneig de la xarxa interna des de fora del tallafocs s'estaran analitzant solament les vulnerabilitats que es poden explotar des de fora de la xarxa, però no es tindrà informació de les possibles vulnerabilitats que es troben a dins, una vegada que un possible atacant hagi aconseguit burlar la seguretat del tallafocs. Per aquest motiu, és molt important tenir en compte la topologia de la xarxa.

És molt important tenir en compte la topologia de la xarxa per al posicionament de l'escàner, de manera que l'escaneig dels diferents escàners situats en diferents punts de la xarxa ens permeti tenir una idea clara de les vulnerabilitats del nostre sistema depenent de des d'on s'accedeix.

Dins dels escàners basats en xarxa podem trobar diferents tipus, com per exemple escàners de propòsit general, escàners de ports, escàners de servidors web o escàners d'aplicacions web.

Nessus

El Nessus és un escàner de vulnerabilitats actiu de propòsit general que pot treballar tant amb credencials (escaneig intern) com sense (escaneig extern). La seva gran popularitat es deu al fet que fins a la seva versió 3 es distribuïa sota llicència GPL (*General Public License*) de GNU, però actualment la distribució és comercial mitjançant la companyia TENABLE Network Security. No obstant això, continua essent l'escàner de vulnerabilitats més utilitzat.

Com veiem, una característica de l'escàner extern i actiu és la utilització de la xarxa per a la realització de l'escaneig. És molt important tenir en compte aquest punt, ja que el trànsit que pot generar l'escaneig exhaustiu de diferents dispositius pot provocar un augment substancial en el volum de trànsit a la xarxa que en provoqui la saturació, i es pot arribar a provocar una denegació de servei de la xarxa.

Un altre aspecte important que cal tenir en compte en la utilització d'escàners externs és la protecció de la informació obtinguda de l'escaneig. Quan s'executa un escaneig extern i actiu s'està generant un conjunt d'informació referent al dispositiu o dispositius que s'estan escanejant, que pot ser interessant per a un atacant, ja que pot identificar possibles vulnerabilitats sense la necessitat d'executar anàlisis que puguin resultar sospitoses. Per aquest motiu, la informació generada per l'escaneig que circuli per la xarxa s'ha d'intentar protegir, en la mesura del possible, utilitzant tècniques de xifratge.

Des del punt de vista del funcionament, 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 d'ordres. En lloc d'aprofitar la vulnerabilitat per a accedir al sistema, es retorna un indicador que mostra si s'ha tingut èxit o no. Òbviament, 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 indiquin possibilitats d'atac, tractant de detectar possibles deficiències de seguretat en l'objectiu. Aquest mètode és menys agressiu que l'anterior, encara que els resultats obtinguts són menys exactes.

Tècniques d'inferència

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

5.2.3. Escaneig extern i passiu d'un dispositiu

L'escaneig extern i passiu de dispositius és una tècnica que combina les capacitats d'escolta dels detectors amb les capacitats d'anàlisi dels escàners de vulnerabilitats actius per a detectar vulnerabilitats en els sistemes.

Un escàner passiu de vulnerabilitats es col·loca a la xarxa en una posició en la qual es pot controlar el trànsit que ve de diversos segments, de manera similar

com es faria amb un sistema de detecció d'intrusos. L'escàner passiu escolta el trànsit en temps real i l'analitza mitjançant la comparació amb un conjunt de regles, com un escàner de vulnerabilitats actiu, de manera que si s'incompleixen les regles establertes, s'alerta a l'administrador de la xarxa. Aquestes característiques permeten detectar vulnerabilitats de manera més contínua que els escàners actius.

Si bé un escàner de vulnerabilitats passiu pot semblar el mateix que un sistema de detecció d'intrusos, és important destacar que les tasques d'anàlisi de trànsit que fan tots dos són diferents.

> Per exemple, si suposem les milers de connexions que es poden fer a un servidor web, un sistema de detecció d'intrusos les haurà d'analitzar totes per a identificar un atac, mentre que l'anàlisi que du a terme un escàner passiu es pot dur a terme únicament amb l'anàlisi (tan exhaustiva com es requereixi) d'una única connexió que té com a destinació el servidor que es pretén escanejar.

Una dels principals avantatges dels escàners passius és la poca incidència que tenen sobre els sistemes que analitzen. Atès que es tracta d'una anàlisi de la informació que viatja per la xarxa, els escàners passius són molt poc intrusius i no afecten el rendiment del sistema que s'està escanejant, cosa que pot ocórrer amb els escàners actius. Aquesta característica els permet ser utilitzats en sistemes crítics en els quals no es pot permetre una disminució del rendiment o l'eventual parada del sistema, que podria arribar a provocar un escaneig actiu.

Més enllà d'aquest avantatge, els escàners de vulnerabilitats passius presenten altres característiques interessants que milloren alguns aspectes dels escàners actius, si bé no s'ha de veure un escaneig passiu com un substitut d'un escaneig actiu, sinó més aviat un complement. Com veurem, un escaneig passiu pot proveir informació per a una eficiència millor d'un escaneig actiu.

Una dels principals avantatges dels escàners passius és la seva capacitat d'anàlisi contínua, característica que no presenten els escanejos actius (tant interns com externs). Tal com hem comentat anteriorment, el mode d'anàlisi de l'escaneig actiu li confereix una visualització instantània de l'estat del sistema que s'analitza, que s'assembla a una fotografia de la situació dels sistemes en l'instant precís que es fa l'escaneig. Això implica que una modificació del sistema analitzat amb posterioritat a l'escaneig actiu (per exemple, per una actualització o la instal·lació de nou programari) pot donar lloc a una vulnerabilitat sense que el procés d'escaneig el detecti. Per contra, els escàners passius analitzen constantment el trànsit alertant de possibles vulnerabilitats quan aquestes es detecten.

Aquesta idea de continuïtat en l'anàlisi ens porta fins a una diferència temporal entre un escàner actiu i un de passiu. Els escàners passius necessiten un temps per a la realització de l'anàlisi. Per exemple, fins que l'usuari *A* no es comunica amb el servidor *B*, l'escàner no pot analitzar si el port pel qual el servidor *B* es comunica té algun servei amb una vulnerabilitat. No obstant ai-

xò, en un escaneig actiu, l'escàner mateix és qui inicia la comunicació amb *B* i per tant, en qualsevol moment, pot determinar si hi ha la vulnerabilitat en aquest port.

En aquest sentit, semblaria que un escàner actiu avantatja el passiu ateses aquestes reflexions. No obstant això, és important destacar que un servidor *B* no sempre pot respondre quan l'escàner actiu li interrogui. A més, en aquesta situació, s'assumeix que l'escàner actiu té identificades les màquines que ha d'escanejar. Aquesta suposició, si bé pot semblar adequada, de vegades no és real, ja que els administradors desconeixen l'existència de màquines o serveis que requereixen escaneig.

Exemple

Un usuari podria iniciar un servidor FTP en una màquina que no hi estigués autoritzada i això podria passar desapercebut a l'administrador. Un escàner actiu no podria detectar una possible vulnerabilitat en la versió de servidor FTP iniciada, ja que l'escàner no analitzaria aquesta màquina, atès que suposadament no hauria d'estar allotjant un servidor FTP. No obstant això, l'anàlisi de trànsit que fa un escàner passiu podria detectar la utilització del servei d'FTP en aquesta màquina i analitzar la possible existència de vulnerabilitats.

Una altra habilitat que proporciona l'escaneig passiu és l'optimització del procés d'escaneig.

Exemple

Seguint amb el cas anterior, un escàner actiu podria intentar identificar al servidor FTP no autoritzat simplement fent escanejos exhaustius de tots els dispositius del sistema (escanejant totes les adreces IP de la xarxa, o tots els ports dels tots els dispositius, etc.). No obstant això, aquesta tasca és summament ineficient, per no dir impossible, en el cas d'una organització amb adreces IPv6. En canvi, un escàner passiu analitzarà solament els dispositius i els ports per on circuli trànsit. De fet, l'escàner passiu pot complementar l'escàner actiu proporcionant la informació necessària d'on cal fer l'escaneig actiu.

Finalment, un altre dels avantatges d'un escaneig passiu és la possibilitat d'anàlisi de vulnerabilitats del client en un entorn client-servidor. Atès que els escàners passius analitzen el trànsit de la xarxa, aquests poden detectar vulnerabilitats en la part de la comunicació del client. Aquest és un altre avantatge dels escàners passius, atès que els escàners actius es focalitzen en l'anàlisi de vulnerabilitats de la part del servidor, i descuren la part del client.

Si bé hem vist diferents avantatges dels escàners passius, hi ha també algunes limitacions en el seu ús. Un dels principals desavantatges dels escàners passius és la dificultat de fixar-ne l'emplaçament correcte. Igual que els sistemes de detecció d'intrusos, la determinació de l'emplaçament dels analitzadors de xarxa és de vital importància per a l'efectivitat de l'escàner, ja que el trànsit que circuli pel segment de xarxa on se situa l'analitzador serà el que proporcionarà la informació per a l'anàlisi.

Una altra de les limitacions que presenten els escàners passius són la dependència que tenen de les dades que analitzen. Si l'escàner es limita a analit-

zar les capçaleres dels paquets que circulen per la xarxa per a determinar, per exemple, el tipus de sistema operatiu que es troba en una màquina, és possible que un atacant pugui manipular la informació dels paquets perquè l'escàner passiu proporcioni informació incorrecta o generi tanta informació que l'escàner no pugui analitzar. És a dir, el nivell d'anàlisi que l'escàner fa de les dades que obté determinarà la qualitat de les alertes que generi.

Resum

En aquest mòdul hem analitzat les vulnerabilitats que podem trobar en el nivell de xarxa, centrant-nos específicament en IPv4. Hem centrat la classificació en funció de si aquestes afecten protocols locals, interconnexió de xarxes o protocols d'extrem a extrem.

Com hem pogut veure, en el terreny local, destaquen com a problemes que generen vulnerabilitats el fet que la informació que circula per la xarxa pot ser detectada per qualsevol usuari, o els mecanismes i protocols existents per a l'assignació d'adreces físiques a adreces IP. Pel que fa a la interconnexió de xarxes, hem vist algunes de les vulnerabilitats que presenten els protocols més utilitzats en aquest segment, com són el protocol IP, l'ICMP, el sistema de DNS i els protocols d'encaminament OSPF i BGP. D'altra banda, hem vist algunes de les vulnerabilitats que afecten protocols d'extrem a extrem, com són TCP i UDP.

Finalment, hem vist com els escàners de vulnerabilitats poden ajudar a detectar les vulnerabilitats d'un sistema. Per a això, hi ha diferents tècniques que depenen del mode de funcionament de l'escàner. D'aquesta manera, els escanejos actius permeten obtenir una imatge fixa de les possibles vulnerabilitats del sistema en un instant de temps concret, mentre que els escàners passius analitzen de manera constant el sistema per a detectar possibles vulnerabilitats que quedaran al descobert per l'ús mateix de dispositius, protocols o programes que en continguin.

Activitats

1. En els primers apartats del mòdul hem repassat algunes vulnerabilitats importants de TCP/IP centrades principalment en IPv4. La introducció d'IPv6 provoca que algunes d'aquestes vulnerabilitats desapareguin i que sorgeixin noves vulnerabilitats. Busqueu informació per Internet sobre vulnerabilitats pròpies d'IPv6 i detalleu breument en què consisteixen.

Exercicis d'autoavaluació

1. La possibilitat d'enviar missatges en difusió pot representar una vulnerabilitat en alguns protocols de xarxa. Esmenteu almenys 3 vulnerabilitats o atacs diferents que utilitzen l'enviament de missatges en difusió i indiqueu quin protocol de xarxa afecten.

2. De les afirmacions següents indiqueu quines són falses.
a) La facilitat per a predir els números de seqüència de TCP es considera una vulnerabilitat de seguretat.
b) UDP és un protocol més segur que TCP perquè té menys vulnerabilitats conegudes.
c) Si es permet l'enviament de missatges en difusió es poden fer atacs de denegació de servei en UDP.
d) Totes les anteriors són falses.

3. En la figura 7 es mostra una captura de paquets feta amb el detector Wireshark. Cada línia correspon a un paquet capturat en una xarxa local Ethernet. Les columnes són, per ordre d'esquerra a dreta: número de paquet, temps en segons, adreça d'origen, adreça de destinació, protocol de més alt nivell inclòs en el paquet, mida del paquet i informació del contingut. En aquest cas es tracta de paquets ARP; la informació *Who has A? Tell B* ens diu que el contingut del paquet ARP està preguntant qui té l'adreça IP *A* i que la resposta ha de ser enviada a la IP *B* (suposadament, qui ha fet la petició). Comenteu què es veu en la figura. S'està fent algun atac?, quines vulnerabilitats s'exploten?

Figura 7. Exemple de captura de paquets amb el Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.159? Tell 24.166.172.1
2	0.098594	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.172.141? Tell 24.166.172.1
3	0.110617	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.161? Tell 24.166.172.1
4	0.211791	Cisco_af:f4:54	Broadcast	ARP	60	Who has 65.28.78.76? Tell 65.28.78.1
5	0.216744	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.163? Tell 24.166.172.1
6	0.307909	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.175.123? Tell 24.166.172.1
7	0.330433	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.165? Tell 24.166.172.1
8	0.408556	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.175.82? Tell 24.166.172.1
9	0.455104	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.220.131? Tell 69.76.216.1
10	0.486666	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.168? Tell 24.166.172.1
11	0.504694	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.221.27? Tell 69.76.216.1
12	0.510684	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.174.184? Tell 24.166.172.1
13	0.540733	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.169? Tell 24.166.172.1
14	0.587308	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.174.181? Tell 24.166.172.1
15	0.662937	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.223.216? Tell 69.76.216.1
16	0.690450	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.172? Tell 24.166.172.1
17	0.692934	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.223.217? Tell 69.76.216.1
18	0.771600	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.217.186? Tell 69.76.216.1
19	0.792105	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.174.221? Tell 24.166.172.1
20	0.801633	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.218.94? Tell 69.76.216.1
21	0.806611	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.174.207? Tell 24.166.172.1
22	0.856709	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.223.222? Tell 69.76.216.1
23	0.884248	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.223.223? Tell 69.76.216.1
24	0.896756	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.176? Tell 24.166.172.1
25	0.931326	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.220.86? Tell 69.76.216.1
26	0.932294	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.223.224? Tell 69.76.216.1
27	1.063549	Cisco_af:f4:54	Broadcast	ARP	60	Who has 65.28.78.114? Tell 65.28.78.1
28	1.065493	Cisco_af:f4:54	Broadcast	ARP	60	Who has 65.26.92.195? Tell 65.26.92.1
29	1.104112	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.223.230? Tell 69.76.216.1
30	1.105552	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.172.6? Tell 24.166.172.1
31	1.131107	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.216.28? Tell 69.76.216.1
32	1.133591	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.174.177? Tell 24.166.172.1
33	1.133679	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.223.231? Tell 69.76.216.1
34	1.152139	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.181? Tell 24.166.172.1
35	1.182181	Cisco_af:f4:54	Broadcast	ARP	60	Who has 24.166.172.232? Tell 24.166.172.1
36	1.184173	Cisco_af:f4:54	Broadcast	ARP	60	Who has 69.76.223.232? Tell 69.76.216.1

Fuente: Wireshark Wiki: http://wiki.wireshark.org/SampleCaptures

4. Busqueu informació sobre les vulnerabilitats de xarxa CVE-1999-0128 i CVE-1999-0513 i identifiqueu-les amb les que apareixen en aquest mòdul.

Solucionari

Exercicis d'autoavaluació

1. *Ping flooding* (ICMP), *smurf attack* (ICMP), *fraggle attack* (UDP).

2. *b* i *d*.

3. En la captura es veuen moltes peticions d'ARP amb origen en la màquina amb adreça MAC Cisco_af:f4:54 (00:07:0d:af:f4:54) i destinació de difusió. En totes les peticions es demana resoldre adreces IP diferents i únicament s'inclouen dues adreces IP per a rebre la resposta. Aquí veiem diversos casos interessants.

S'està fent un atac que genera molts paquets (més de 20 per segon), i demana la resolució de diferents adreces IP. Això pot provocar *ARP poisoning* o *flooding* en els ordinadors que reben aquestes peticions. Atès que l'adreça IP que es demana varia sempre sembla que l'objectiu és simplement provocar un desbordament de la memòria cau ARP. D'altra banda, veiem que l'adreça IP origen dels paquets (que no s'ha de correspondre necessàriament amb l'adreça MAC) són dues adreces concretes. Això pot indicar un intent de denegació de servei als ordinadors que tenen aquestes IP, ja que seran els que rebin totes les respostes (similar als atacs de *fraggle* i *smurf* vists en el mòdul).

4. Tant la vulnerabilitat CVE-1999-0128 com la CVE-1999-0513 són vulnerabilitats que afecten el protocol ICMP. Totes dues s'han descrit en l'apartat 3 corresponent a la interconnexió de xarxes. Concretament, la primera correspon a la vulnerabilitat de *ping of death*, mentre que la segona identifica un *smurf attack*.

Glossari

address resolution protocol *m* Protocol que permet resoldre adreces de protocols d'interconnexió de xarxa a adreces de xarxa.
Sigla **ARP**

adreça IP *f* Adreça utilitzada pel protocol IP.

adreça MAC *f* Adreça física de xarxa.

border gateway protocol *m* Protocol d'encaminament exterior utilitzat en Internet.
Sigla **BGP**

content addressable memory *f* Espai de memòria d'un encaminador de xarxa en el qual s'estableix un vincle entre les adreces MAC i els ports mateixos del commutador.
Sigla **CAM**

detector *m* Dispositiu o programa que permet obtenir el trànsit que circula per un canal de comunicació, normalment una xarxa TCP/IP.

domain name system *m* Sistema de noms jeràrquic i distribuït que permet associar noms de domini a adreces IP.
Sigla **DNS**

Ethernet Família de tecnologies per a xarxes d'àrea local.

Internet control message protocol *m* Protocol de control, principalment per a enviament de missatges d'error, de TCP/IP.
Sigla **ICMP**

Internet protocol *m* Protocol per a la interconnexió de xarxes.
Sigla **IP**

man in the middle L'atac d'home a mig camí consisteix que l'atacant s'interposa en la comunicació entre l'emissor i el receptor legítims i pot analitzar la informació que aquests s'intercanvien.
Sigla **MITM**

open shortest path first *m* Protocol d'encaminament utilitzat internament per molts sistemes autònoms.
Sigla **OSPF**

port security Permet limitar el nombre d'adreces MAC associades a un port físic d'un commutador.

transmission control protocol *m* Protocol de transport (d'extrem a extrem) de TCP/IP.
Sigla **TCP**

user datagram protocol *m* Protocol de transport (d'extrem a extrem) de TCP/IP.
Sigla **UDP**

Bibliografia

Comer, D. (2006). *Internetworking With TCP/IP. Vol. 1: Principles Protocols, and Architecture*. (5a. ed). Prentice Hall: New Jersey.

McClure, S.; Scambray, J.; Kurtz, G. (2009). *Hacking exposed 6: network security secrets & solutions*. McGraw-Hill.

Plummer, D. C. (1982). *An Ethernet Address Resolution Protocol – or – Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*. RFC 826. IETF, The Internet society [en línia] <http://www.ietf.org/rfc/rfc826.txt>.

Senie, D. (1999). *Changing the Default for Directed Broadcasts in Routers*. RFC 2644. IETF, The Internet society [en línia] <http://www.ietf.org/rfc/rfc2644.txt>.

Ziemba, G.; Reed, D.; Traina, P. (1995). *Security Considerations for IP Fragment Filtering*. RFC 1858. IETF The Internet Society [en línia] <http://www.ietf.org/rfc/rfc1858.txt>.