Anàlisi de la seguretat del protocol d'encaminament d'Internet BGPv4

Carlos Lacambra Linés

Resum – Aquest treball de fi de grau (TFG) ha continuat el TFG *Avaluació Pràctica del Protocol d'encaminament BGPv4*, realitzat l'any passat per en Roger Serra, on s'explicava el funcionament del protocol BGP, juntament amb una simulació pràctica que demostrava el comportament d'aquest protocol. En aquest TFG, fem una anàlisi de la seguretat d'aquest protocol tan teòrica com pràctica. En la part teòrica expliquem quines són les vulnerabilitats que presenta o presentava aquest protocol, quins atacs es poden o es podien produir aprofitant aquestes vulnerabilitats i quins han estat alguns dels atacs més importants que s'han produït a Internet contra aquest protocol. També mencionem quines mesures de seguretat es van proposar per intentar fer segur el protocol BGP i expliquem quines mesures existeixen actualment per contrarestar algunes de les vulnerabilitats i evitar certs atacs. A la part pràctica, fem una simulació d'un escenari de routers BGP, mitjançant el software Quagga, sobre el qual executarem certes proves. Aquestes proves consisteixen en la realització d'un atac molt conegut que es va produir a Internet i en l'aplicació d'alguna mesura de seguretat que pot evitar algun dels atacs que hem presentat.

Paraules clau – Border Gateway Protocol (BGP), Sistema Autònom (SA), Resource Public Key Infrastructure (RPKI), Route Origin Authorization (ROA), Prefix Origin Validation.

Abstract — This final degree Project (FDP) has followed the FDP *Avaluació pràctica del Protocol d'encaminament BGPv4*, which was done last year by Roger Serra, and which explained the operation of the BGP routing protocol, together with its practical simulation using the Quagga software. In this FDP, we made an analysis of the security of this protocol both theoretical and practical. In the theoretical part we explain which vulnerabilities the protocol has, which attacks could be produced taking advantage of them, and which have been some of the most important attacks that occurred on Internet against this protocol. We also mention what security measures were proposed in order to secure the protocol BGP and we explain which security measures currently exist to counteract some of the vulnerabilities and to avoid certain attacks. In the practice, we simulate a BGP router's scenario, using the Quagga software, where we run some tests. Those tests consist of performing a well-known attack which occurred on the Internet, and we also apply some security measures that can prevent some of the attacks we presented.

Index Terms— Border Gateway Protocol (BGP), Autonomous System(AS), Resource Public Key Infrastructure (RPKI), Route Origin Authorization (ROA), Prefix Origin Validation.

1 Introducció

L'Intercanvi d'informació d'encaminament a Internet és necessària per a que els routers distribuïts per la xarxa mundial coneguin com poden arribar a un destí concret i d'aquesta forma, poder encaminar les peticions dels usuaris d'Internet.

BGPv4 és el protocol que s'utilitza a Internet per l'intercanvi d'informació d'encaminament i accessibilitat de xarxes entre sistemes autònoms (SA). Aquesta informació s'intercanvia a una sessió BGP (formada per dos routers BGP) a través del missatges UPDATE, els quals estan composats per tres camps bàsics: xarxes que han deixat de ser accessibles, xarxes accessibles i atributs de camí que indiquen com aconseguir arribar a les xarxes anunciades al camp de xarxes accessibles. Aquest tipus de missatges acostumen a travessar diversos SA, fet que un intrús pot aprofitar per realitzar un atac com el de modificació d'algun dels camps del missatge UPDATE, provocant uns efectes catastròfics a Internet. A més a més, l'atac podria ser realitzat per un dels routers BGP participants a la sessió BGP, el qual decideix començar a anunciar una ruta la qual no està autoritzat a anunciar. Però aquests són només uns exemples dels diversos atacs que es poden produir contra aquest protocol d'encaminament.

Per aquest motiu, al nostre treball de fi de grau, hem dut a terme un estudi teòric de la seguretat d'aquest protocol, juntament amb una demostració pràctica de les seves vulnerabilitats i d'alguna de les seves mesures de seguretat, mitjançant l'ús d'un escenari de màquines virtuals que actuen com a routers BGP situats a diferents SA.

A l'inici del projecte ens vam proposar els següents objectius:

- Conèixer de forma teòrica i pràctica el protocol BGPv4.
- Estudiar la seguretat d'aquest protocol: quines vulnerabilitats té, quins atacs es poden realitzar aprofitant aquestes vulnerabilitats i quines mesures de seguretat existeixen per evitar alguns dels atacs.
- Conèixer quins han sigut alguns dels atacs que s'han

- *E-mail de contacte: clacambra92@gmail.com*
- *Menció realitzada: Tecnologies de la Informació.*
- *Treball tutoritzat per: Joan Borrell Viader (deic)*
- *Curs 2014/15*

fet contra aquest protocol.
- Estudiar quines van ser les solucions a aquest atacs.
- Instal·lar un entorn de màquines virtuals que actuaran com a routers BGP situats a diferents SA, simulant un possible escenari d'Internet.
- Reproduir algun dels atacs estudiats sobre aquest entorn.
- Reproduir les accions que es van fer per contrarestar aquests atacs.
- Implementar alguna mesura de protecció disponible que impedeixin la realització d'algun atac estudiat.
- Reproduir mesures de protecció general proposades pel protocol BGPv4.

Sobre l'objectiu 1, hem de dir que, tan l'estudi teòric com pràctic del protocol BGP han estat realitzats però no inclosos en aquest article, ja que es tracta d'una continuació d'un treball on ja s'explicava i es demostrava detalladament tot el funcionament del protocol BGPv4 [1].

Inicialment, en la secció 2, expliquem quina ha estat la metodologia que hem seguit per tal de completar el nostre projecte i assolir els objectius plantejats.

En la secció 3, presentem un anàlisis de la seguretat del protocol, on expliquem les vulnerabilitats que presenten els diferents tipus de missatges BGP, quins atacs es poden produir i exposem el cas de l'atac que va realitzar Pakistan Telecom contra YouTube. També fem un anàlisis d'algunes propostes de seguretat que s'han presentat per aquest protocol i de les mesures de seguretat que actualment implementa BGP.

Seguidament, en la secció 4, presentem l'escenari de màquines virtuals que vam emprar per realitzar el nostre estudi pràctic, juntament amb la configuració del software Quagga en cadascuna de les màquines.

En la secció 5, exposem el nostre estudi pràctic el qual consisteix en la realització de l'atac anteriorment mencionat i en l'aplicació de les mesures que va aplicar YouTube per contrarestar-lo. En aquesta secció també apliquem mesures de seguretat que impedeixen la realització de certs atacs definits a la secció 3.

Finalment, en la secció 6, mostrem quines han estat les conclusions que hem extret de la nostra feina realitzada al llarg del TFG.

2 METODOLOGIA

En aquesta secció exposem la metodologia que hem seguit al llarg de tot el nostre TFG amb la finalitat de completar els objectius que ens vam proposar inicialment.

Com a primer pas, vam estudiar el protocol BGP tant de forma teòrica com pràctica, fixant-nos detalladament en com es realitza una sessió BGP, quins missatges s'intercanvien els *peers* participants en ella i quin es el format i contingut d'aquests missatges. Aquesta anàlisi es molt important per tal de poder entendre com es poden reproduir els diversos atacs que es poden produir a una sessió BGP.

Un cop adquirits aquests coneixements, vam realitzar el muntatge del nostre escenari pràctic i vam configurar les màquines virtuals degudament per a que actuessin com a routers BGP, deixant-ho preparat per la realització de la part pràctica. També vam testejar l'escenari comprovant que les màquines establien sessions BGP i intercanviaven informació BGP correctament

Amb l'escenari ja preparat, vam passar a l'anàlisi de la seguretat del protocol BGP, on vam analitzar les vulnerabilitats del protocol, els atacs que es poden realitzar i les mesures de seguretat existents.

Seguidament, vam buscar informació sobre els diferents atacs que s'han realitzat a Internet aprofitant les debilitats del protocol BGP, quins efectes van causar i com es van contrarestar per recuperar l'estat normal.

A continuació, vam realitzar el nostre cas pràctic sobre l'escenari que havíem muntat prèviament. Aquest cas va consistir en la realització d'un dels atacs que es van realitzar a Internet, i també en la aplicació de les accions que es van dur a terme per contrarestar-lo.

El següent pas, va consistir en l'aplicació d'alguna mesura de seguretat del protocol BGP existent, que evita la realització de certs tipus d'atacs.

Finalitzades totes les tasques anteriors, vam examinar els resultats obtinguts i vam extreure les conclusions.

3 ESTAT DE L'ART

Quan el protocol BGP va ser creat, la xarxa mundial que avui dia coneixem com a Internet no havia assolit l'estat en el que es troba actualment. En aquells moments, Internet no era una xarxa a tan gran escala com ho és ara i la seguretat a Internet no era un dels majors problemes que es plantejava. A conseqüència d'això, BGP no incloïa cap protecció contra possibles atacs o errors que poguessin causar alteracions en el comportament del protocol.

No obstant, a mida que Internet es va anar fent més gran, perquè més usuaris s'hi afeguien, el nombre de possibles atacants també va anar creixent. A causa d'això es van anar produint atacs contra diversos protocols d'Internet i BGP no va ser una excepció. Els atacs que es van produir en contra d'aquest protocol van posar en dubte la seva seguretat, que es podia definir en una sèrie de qüestions com ara: com podia un router assegurar que el sistema autònom origen d'un missatge BGP estava autoritzat a anunciar la xarxa que estava anunciant?, la ruta de sistemes autònoms que està dins del missatge BGP és la correcta per arribar a la xarxa anunciada o ha estat modificada?, etc.

Però aquestes són només algunes de les diverses vulnerabilitats que presentava i/o presenta aquest protocol d'encaminament i que un atacant podia aprofitar per crear efectes negatius a Internet.

A més a més, al tractar-se d'un protocol que funciona amb TCP, hereta també els seus problemes de seguretat, com ara el de l'enviament de segments RST falsos per tancar sessions.

Al llarg del temps, s'han presentat diverses propostes de seguretat, algunes de les quals s'han aconseguit aplicar amb èxit, reduïnt així la probabilitat de reproduir certs atacs. D'altra banda però, segueixen existint algunes vulnerabilitats per les quals encara no ha estat trobada una solució.

3.1 Vulnerabilitats

Les vulnerabilitats que presenta aquest protocol poden ser explotades tan per un individu que no forma part de la sessió BGP, com per un dels dos *peers* que formen la sessió [1]. La majoria dels atacs que podria provocar un atcant deriven de les tres vulnerabilitats fonamentals del protocol [2]:

- BGP no té cap mecanisme que aseguri la integritat i proporcioni autenticitat del missatge.
- No existeix cap mecanisme a BGP que permeti validar la autoritat d'un SA a anunciar una prefixe de xarxa.
- BGP tampoc defineix cap mecanisme que permeti verificar l'autenticitat dels atributs de camí.

Aquestes vulnerabilitats són explotades a través de l'enviament de missatges BGP modificats, alterats, o creats amb informació falsa, ja que no inclouen cap camp que permeti validar o autenticar l'origen del missatge i el contingut d'aquest.

3.1.1 Vulnerabilitats als missatges BGP

L'especificació del protocol BGP defineix cuatre tipus de missatges els quals permeten establir una sessió (OPEN), mantenir la sessió activa (KEEPALIVE), notificar d'errors (NOTIFICATION) i intercanviar informació d'accessibilitat de xarxes (UPDATE). Les vulnerabilitats dels tres primers tipus de missatges es deriven del moment en el qual s'envien. BGP defineix una màquina d'estats finita[3] la qual defineix els estats pels quals passa un router quan estableix una sessió BGP. Si un d'aquests missatges es rep en un estat en el qual no se l'espera, la sessió BGP serà tancada, amb efectes que detallem a la secció següent. El quart missatge, que també es subseptible a aquesta vulnerabilitat, en presenta moltes més ja que està format per molts camps i cadascun d'ells pot ser originari d'un atac. Per aquest motiu, hem decidit parlar-ne d'ell en una secció diferent.

3.1.3. Vulnerabilitats al missatge UPDATE

Aquest tipus de missatges estàn formats per tres camps principals: xarxes inaccessibles (*withdraw routes*), atributs de camí (*path atributes*) i xarxes accessibles (*NLRI*). Com BGP no proporciona integritat del missatge, aquests camps poden ser genrats per l'origen amb informació falsa, o modificats per un dels routers que propaga el missatge. Així per exemple, algunes de les vulnerabilitats que podrien sorgir d'aquests camps i com un atacant podria aprofitar-les són [2]:

- *Withdraw routes:* aquest camp conté una llista de xarxes que ja no són accessibles per l'emissor del missatge. Un router podria omplir aquest camp amb xarxes que encara són accessibles, amb la finalitat de poder deixar la xarxa inaccessible per una part d'Internet. No obtant, el router està una mica limitat, ja que només pot eliminar prefixos de xarxes que ha anunciat prèviament.
- *Path attributtes:* són un conjunt d'atributs que estan relacionats amb el camí que s'ha de seguir per arribar a les xarxes anunciades al camp NLRI. Un router podria modificar, per exemple, l'atribut AS_PATH amb un camí que no es apropiat per accedir a les xarxes que s'estan anunciant. Amb aquesta modificació, un router podria ser capaç de deixar una xarxa inaccessible, o de fer que tots els missatges fossin encaminats a través d'un determinat router, que podria no ser capaç de processar totes les peticions i acabaria eliminant una gran quantitat d'elles.
- *NLRI:* aquest camp conté una llista de xarxes que són accessibles a través del router BGP que envia el missatge. Un router podria anunciar xarxes les quals no està autoritzat a anunciar, amb l'objectiu de deixar una xarxa inaccessible i/o de desviar el tràfic cap a ell, tenint així l'oportunitat de veure el contingut d'aquest tràfic i poderlo modificar.

3.2 Atacs

La carència de mesures de seguretat ha permès que es produïssin diversos atacs contra el protocol BGP, alguns bastant coneguts, com va ser el que va realitzar Pakistan Telecom contra YouTube [4]. La majoria d'aquets atacs eren realitzats aprofitant les debilitats presents als missatges BGP. Aquestes debilitats permetien a un atacant, que podria ser extern o participant de la sessió BGP, crear o modificar missatges amb informació falsa, que podien causar efectes negatius, no només a la sessió atacada sinó a tota Internet. Per exemple, provocar un tancament de la sessió BGP faria que els routers eliminessin totes les xarxes apreses en aquella sessió, provocant un efecte en cascada ja que els participants de la sessió atacada propagarien aquesta eliminació de xarxes als seus altres *peers* BGP.

En aquesta secció, volem presentar algun dels atacs que es poden reproduir aprofitant les debilitats presents en els missatges BGP [2]:

- *Replay*: un router pot reproduir de nou un missatge BGP que ja ha estat enviat.
- *Fabricació*: es produeix quan un router comença a anunciar xarxes no autoritzades.
- *Modificació:* un router pot modificar la informació dels missatges BGP.
- *Eliminació:* es produeix quan un router es dedica a eliminar missatges UPDATE que rep en comptes de propagarlos.
- *Inserció*: es produeix quan un intrús inserta missatges a una sessió BGP amb informació falsa.
- *Man-in-the-middle*: un intrús pot ser capaç d'interceptar missatges BGP i veure el seu contingut.
- *Denial of service*: transmetre missatges BGP amb informació falsa pot provocar una denegació de servei a determinats prefixes.

A la secció 5 d'aquest article podem veure com es va reproduir un dels atacs més coneguts i que hem mencionat a l'inici d'aquesta secció. Es tracta de l'anunci no autoritzat d'una xarxa per part de la companyia pakistanesa de telecomunicacions, que va provocar un atac de denegació de servei contra la pàgina web de compartició de vídeos més exitosa del món.

3.3. Mecanismes de seguretat

Les vulnerabilitats presentades a la secció 3.1 i l'habilitat d'un atacant per treure'n profit feia pensar que l'aplicació de mesures de seguretat per al protocol era

necessària. Certs investigadors van treure propostes on exposaven una versió segura del protocol, com ara soBGP[5] o S-BGP[6], però que no es van arribar a desenvolupar perquè la seva posada en funcionament a Internet era massa complicada.

Afortunadament, és van presentar mesures que feien segur el protocol i reduïen la probabilitat de reproduir certs atacs i que actualment es troven aplicades per la majoria de routers BGP. Una d'elles es tracta del mecanisme anomenat Prefix Origin Validation [7][8], que permet a un router validar el SA originador d'una ruta BGP.

A més a més, el fet d'utilitzar TCP, també permet a BGP fer us de les seves mesures de seguretat com TCP/MD5, que proporciona autenticitat dels missatges, i per tant protegir contra atacs provinents d'un router no participant en la sessió BGP [9].

3.3.1. Prefix Origin Validation

Prefix Origin Validation és un mecanisme que permet a un router validar el sistema autònom originador d'una ruta BGP, amb la finalitat de protegir contra anuncis de prefixos malintencionats. Aquest mecanisme de validació utilitza el Resource Public Key Infrastrucutre (RPKI), una arquitectura que descriu un mètode per construir una base de dades verificable de direccions IP i números de SA com a recursos. [7][8][10].

Resource Public Key Infrastrucutre (RPKI)

RPKI és una infraestructura de clau publica (PKI) especialitzada, dissenyada per fer segura la infraestructura d'encaminament d'Internet.

Aquesta arquitectura permet a una entitat afirmar que ella és la legítima propietaria d'un conjunt d'adreces IP i números de SA, i permet a aquesta entitat autoritzar a certs SA a anunciar prefixes IP que posseeix [10].

Està formada per tres elements bàsics: certificats de recursos, objectes digitals signats anomenats Route Origin Authorizations (ROAs) i un repositori distribuït.

Aquets tres elements, permeten a un router BGP validar si el SA d'origen d'una ruta BGP està autoritzat a anunciar un cert bloc d'adreces IP i prendre una decisió, en quant a l'encaminament, segons aquesta validació.

Certificats de recursos. RPKI utilitza certificats X.509 amb extensions per adreces IP i identificadors de SA [10]. Aquests certificats representen la jerarquia d'assignació d'adreces IP i números de sistema autònom. Això és, els recursos són inicialment distribuïts per l'IANA als Regional Internet Registres (RIRs), els quals els distribueixen als Local Internet Registres (LIRs, també coneguts com ISPs), qui finalment els distribueixen als seus clients. Cadascun d'aquests propietaris generen certificats per assignar adreces IP i números de SA al node inferior a ells. Per tant, aquest certificats permeten validar la propietat d'aquests dos tipus de recursos. No obstant, no donen autoritat a un determinat SA per anunciar certs prefixos d'adreces IP, però gràcies a ells, un LIR/ISP pot crear un document que permet donar aquesta autoritat. Aquest documents s'anomenen ROAs.

ROAs. Són un tipus de documents anomenats attestations, que permeten verificar que el titular d'un bloc de direccions IP ha autoritzat a un SA per originar rutes a un o més prefixes dins d'aquest bloc de direccions.

El contingut de les ROAs està format per un únic SA , una llista de prefixes IP i un camp opcional, per cadascún dels prefixes IP de la llista, que identifica la mida de prefix màxim. Si aquest camp opcional no està definit, el sistema autònom està autoritzat únicament a anunciar la IP especificada. Si està definit, aquest valor especifica la mida del prefix IP més específic que està autoritzat a anunciar el SA. Per exemple, si el prefix IP és 10.0.0.0/16 i la mida de prefix màxim és 22, està autoritzat a anunciar prefixes més específics que 10.0.0.0/16, però no més que 10.0.0.0/22 [11].

Repositori distribuït. La infraestructura RPKI no utilitza un únic repositori per la publicació o emmagatzemament dels objectes RPKI anteriorment definits. En comptes d'això, utilitza un repositiori distribuït on són emmagatzemats tan els certificats de recursos com les ROAs.

RPKI: validació de la ruta BGP. Quan un router BGP rep un anunci (UPDATE), valida la ruta continguda en ell a partir de les diferents ROAs que es troben al repositori distribuït. Després de la validació, a la ruta se li assigna un d'aquests tres valors [7][8][12]:

- *Vàlid:* existeix una ROA que específica que el SA originador del UPDATE està autoritzat a anunciar els prefixos continguts en aquest anunci.
- *Invàlid:* existeix un ROA per el mateix prefix anunciat però per un altre SA o l'anunci coincideix en el número de SA però el prefix IP és més específic que el permès per la mida de prefix màxim especificat en la ROA.
- *Unknown/Not found:* el prefix anunciant no està cobert per cap ROA.

Segons el valor assignat, el router prendrà un descició d'encaminament: una ruta amb el valor *vàlid* serà més prioritària que un ruta amb el valor *unknown*, mentre que una ruta amb el valor *invàlid* mai serà considerada.

A la taula 1 podem veure un quadre resum del valor que se li dona a una ruta després de fer la comparació amb les ROAs [12].

ROUTE		AS	
		Matching AS	Not-matching AS
Prefix	Non-Intersecting	Unknown	Unknown
	Covering Aggregate	Unknown	Unknown
	Match ROA prefix	Valid	Invalid
	More Specific than ROA	Invalid	Invalid

Taula 1. Estat de validesa de la ruta.

3.3.2. TCP/MD5

L'establiment d'una sessió BGP implica abans l'establiment d'una sessió TCP al port 179. BGP és un protocol de la capa d'aplicació, que utilitza TCP com a protocol de transport, el qual l'estalvia la tasca de fragmaentació, retransmissió, reconeixement i seqüenciació [3]. Però també implica que el protocol d'encaminament hereti totes les vulnerabilitats d'aquest protocol de transport. Un intrús podria interrompre la comunicació BGP entre dos routers tancant la connexió TCP que aquests implementen mitjançant, per exemple, l'enviament d'un

segment TCP amb el bit RST activat.

Conseqüentment, l'especificació de BGP requereix que aquest protocol ha de suportar el mecanisme d'autenticació TCP/MD5. Aquest mecanismes, a part de solucionar les debilitats del protocol TCP també permet solucionar-ne algunes del protocol BGP. Per exemple, com es tracta d'un mecanisme d'autenticació, resulta molt més complicat per a un intrús introduir, a una sessió BGP, missatges amb informació falsa, fent-se passar per un dels *peers* que formen part d'aquesta sessió.

Cada segment enviat en una connexió TCP que vol ser protegit contra atacs de falsificació d'identitat, han de contenir una firma MD5, que es produïda mitjançant l'aplicació de l'algoritme MD5 als següents camps: part de la capçalera IP, capçalera TCP, les dades del segment TCP i una clau compartida coneguda per els dos *peers* de la sessió TCP [9]. Aquesta firma es guarda a un camp opcional del segment TCP. Al rebre un segment firmat, el destinatari calcula la seva pròpia firma MD5 utilitzant les dades esmentades anteriorment i compara les dues firmes. Només si són iguals acceptarà el missatge i sinó, l'eliminarà sense enviar una notificació al origen del missatge.

4 CONFIGURACIÓ DE L'ENTORN

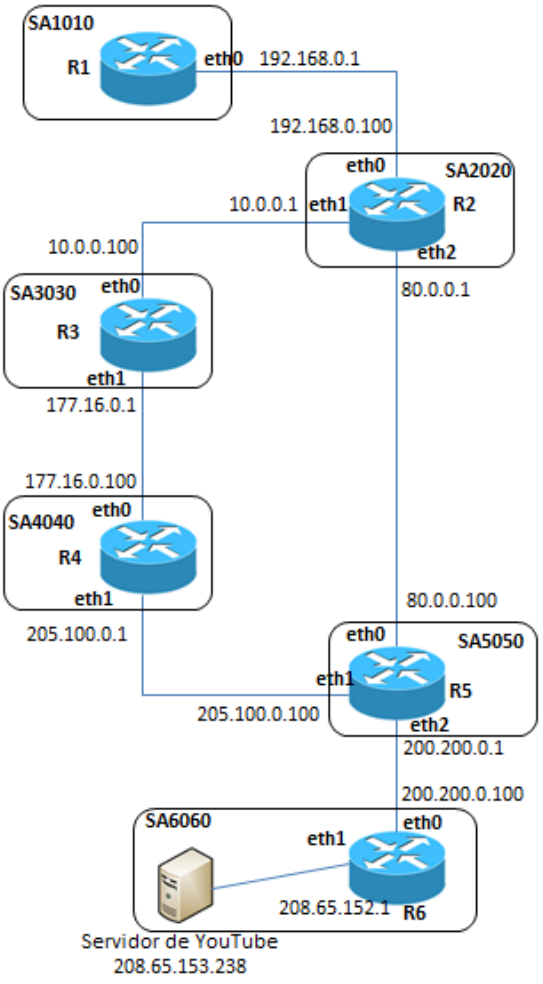

Figura 1. Escenari pràctic.

En aquesta secció explicarem com vam preparar el nostre entorn pràctic, sobre el qual reproduïm l'atac que va realitzar Pakistan Telecom contra YouTube explotant les vulnerabilitats de BGP[4]. També reproduïm com la web de vídeos americana va recuperar l'estat normal amb la realització d'un contraatac.

Seguint l'exemple mostrat en el TFG previ a aquest [1], hem implementat un escenari molt semblant, adaptant-lo a la nostra investigació.

El nostre escenari està format per set màquines virtuals, les quals funcionen amb el sistema operatiu Lubutnu, una versió lleugera d'Ubutnu. D'aquestes set màquines virtuals, sis funcionaran com a routers BGP i l'altra actuarà de servidor de YouTube. A cadascuna de les màquines que actuen com un router BGP hi hem instal·lat el programa Quagga, un software que proveeix d'implementacions de diferents tipus de protocols d'encaminament, entre els quals es troba BGP i que permet que un SO funcioni com un encaminador.

Podem veure l'escenari que hem construït a la figura 1. Sobre aquest escenari volem mostrar, primerament, com el sistema autònom 6060 (actuarà com a SA de YouTube), propietari de la xarxa a la qual pertany YouTube, anuncia aquesta xarxa, i com els demés routers de l'escenari reben aquest anunci i apliquen les seves polítiques de decisió correctament per seleccionar la ruta més adecuada.

Seguidament, el SA1010 (actuarà com a SA de Pakistan Telecom), començarà a anunciar una xarxa que no té en possessió i que per tant no està autoritzat a anunciar. Amb aquest anunci, SA1010 aconseguirà deixar inaccessible a YouTube per tots els sistemes autònoms de l'escenari.

Arribat a aquest punt, podrem veure com totes les peticions que es fan a YouTube ja no són redirigides al sistema autònom que realment la conté (SA6060), sinó que són encaminades al SA que està realitzant l'atac (SA1010), qui realment no conté la xarxa

Els següents passos, són la demostració de com la web de compartició de vídeos torna a ser accessible: primer, anunciant la mateixa xarxa que ha anunciat l'atacant al pas anterior, aconsegueix ser accessible per aquells SA que es troben més a prop, es a dir, aquells que han de passar per menys sistemes autònoms per arribar a SA6060 que per arribar a SA1010. En el nostre cas aquests són SA6060, SA5050 i SA4040.

A continuació SA6060 anunciarà dues subxarxes de l'anteriorment anunciada, recuperant així l'estat inicial.

4.1 Configuració del dimoni zebra

El dimoni zebra permet a cada router que implementa un protocol d'encaminament, recol·lectar la informació dels diferents protocols d'encaminament que aquest implementa, actualitzar les taules d'encaminament del kernel a partir d'aquesta informació i intercanviar aquesta informació amb altres routers que implementen protocols d'encaminament.

La configuració d'aquest dimoni es pot realitzar de dues formes: a través d'una connexió Telnet amb el router que executa el dimoni, o mitjançant l'arxiu de configuració corresponent al dimoni zebra. Per facilitat, hem decidit configurar-ho de la segona forma presentada. A la

següent llista presentem les comandes que hem fet servir i que són necessàries per realitzar les nostres proves [13]:

- `hostname` *`hostname`*: específica en nom del router.
- `password` *`password`*: especifica la contrasenya necessària per poder accedir al router a través de Telnet. Aquesta comanda es necessària si es vol fer la configuració del dimoni a través de Telnet.
- `enable password` *`password`*: especifica la contrasenya necessària per accedir al router en mode enable. Aquesta comanda es necessària si es vol fer la configuració del dimoni a través de Telnet.
- `interface` *`ifname`*: especifica la interfície del router. Permet accedir a la interfície indicada.
- `ip adress` *`address/prefix`*: especifica la IP i la màscara de la xarxa per a la interfície anteriorment definida amb la comanda anterior.
- `ip forwarding`: habilita l'encaminament IP. Això ens serà necessari per a que quan un router rebi un missatge BGP per una interfície, aquest el reencamini per les altres interfícies de xarxa per les quals manté una sessió BGP.

Els arxius de configuració del dimoni zebra de cadascuna de les màquines es poden consultar a l'apèndix.

4.2 Configuració del dimoni bgpd

El dimoni bgpd (BGP daemon) és l'encarregat de manipular les taules d'encaminament BGP del router, d'intercanviar informació d'accessibilitat de xarxes amb altres routers BGP i d'aplicar les polítiques de decisió per escollir la millor ruta (la que passa a través de menys sistemes autònoms), que és la que s'introduirà a la taula d'encaminament del kernel mitjançant el dimoni zebra.

Com ocorria amb el dimoni zebra, la configuració de bgpd també es pot fer de dos maneres: a través d'una connexió Telnet amb el router que executa el dimoni, o mitjançant l'arxiu de configuració corresponent al dimoni bgpd. A la següent llista presentem les comandes que hem fet servir i que són necessàries per realitzar les nostres proves [13]:

- `router bgp` *`as-number`*: especifica el número de sistema autònom al qual es troba el router.
- `neighbor` *`address`* `remote-as` *`as-number`*: especifica un router BGP veí que té *address* com adreça IP i pertany al sistema autònom *as-number*. El router establirà una sessió BGP amb aquests veí.
- `neighbor` *`address`* `verion` *`version`*: permet establir la versió del protocol BGP amb el router veí que té *address* com adreça IP.
- `neighbor` *`address`* `password` *`password`*: permet protegir la sessió BGP amb la utilització de la signatura TCP MD5.
- `network` *`network`*: específica una adreça de xarxa que pertany al sistema autònom del router i que per tan serà anunciada per aquest.
- `redistribute` *`connected`*: permet al router anunciar les xarxes a través de les quals té una sessió BGP establerta, es a dir, aquelles xarxes que comparteix amb un altre router BGP.

Els arxius de configuració del dimoni bgpd de cadascuna de les màquines es poden consultar a l'apèndix.

Abans de començar a descriure el nostre cas de prova, volem destacar la importància de la comanda "redistribute connected". Inicialment, creiem que aquesta comanda no era necessària utilitzar-la perquè a una xarxa, la qual està compartida per dos routers BGP, no hi sol haver cap altre usuari connectat, i per tant un usuari situat a un SA no necessitaria conèixer aquesta xarxa ja que mai faria una petició a ella. Però, al fer les primeres proves en el nostre escenari, vam adonar-nos que ens equivocàvem i ho mostrem amb el següent exemple. Imaginem que cap del routers fa ús de la comanda esmentada anteriorment. Els routers només sabrien de la xarxa que està anunciant SA6060 (concretament per R6), sobre la qual aquest router no està executant cap procés BGP. Imaginem ara, que R2 fa una petició a la web de YouTube, que es troba a la xarxa anunciada per R6. El routers, sabrien encaminar bé aquesta petició fina a portar-la al seu destí, que rebria la petició i contestaria enviant un missatge com a resposta a través de R6. Aquí es quan apareix el problema: R6 miraria la IP de destí d'aquest missatge i veuria que és 80.0.0.1. Llavors, buscaria a la seva taula d'encaminament una entrada que correspongui a la xarxa d'aquesta IP, no la trobaria i conseqüentment eliminaria el missatge.

5 PROVES I RESULTATS

En aquesta secció descrivim les proves que hem realitzat sobre l'escenari que hem presentat i descrit a l'apartat anterior i presentem quins han estat els resultats obtinguts. El nostre cas de prova ha consistit en la reproducció de l'atac que Pakistan Telecom va realitzar contra YouTube, aprofitant les vulnerabilitats de BGP. Veurem la seqüència de passos que es va donar perquè la companyia pakistanesa deixés inaccessible a YouTube i com aquest últim va recuperar l'estat inicial i va tornar a ser accessible per tota Internet.

Per finalitzar, també veurem com la mesura de seguretat MD5 de TCP, pot assegurar una sessió mitjançant autenticació.

5.1 Pakistan Telecom vs YouTube

El 24 de febrer de 2008 Pakistan Telecom va començar a anunciar una xarxa la qual no estava autoritzat a anunciar, deixant la web de YouTube inaccessible durant gairebè dues hores. La seqüència de passos que es va donar per reproduir l'atac i com la web de compartició de videos es va recuperar es la següent [4]:

1. YouTube (AS36561) es troba anunciant 208.65.152.0/22.
2. Pakistan Telecom (AS17557) comença a anunciar 208.65.153.0/24.
3. AS36561 comença a anunciar la xarxa 208.65.153.0/24.
4. Finalment, AS36561 anuncia les xarxes 208.65.153.128/25 i 208.65.153.0/25.

Veiem doncs, que va succeir en cadascun d'aquests passos.

5.1.2. Estat inicial

A part de mostrar com és l'estat inicial en el que es troba el nostre escenari abans de la realització de l'atac, la descripció i imatges que presentem en aquesta subsecció

ens permetran demostrar com és el funcionament bàsic del protocol BGP.

En l'estat inicial, tots els routers es troben executant el servei Quagga i per tan estan actuant com a routers BGP, intercanviant correctament informació d'accessibilitat de xarxa. En el nostre cas ens fixarem com la xarxa anunciada per AS6060 (YouTube) està sent propagada a través dels encaminadors del nostre escenari. Aquesta xarxa està identificada amb la IP 208.65.152.0/22, a la qual es troba la IP del servidor de YouTube (208.65.153.238). R6 comença a anunciar aquesta xarxa a través de R5. Quan aquest rep el missatge UPDATE, afegeix el número del seu sistema autònom al principi del AS_PATH i decideix propagar-lo per cadascuna de les interfícies on té una sessió BGP, canviant l'atribut NEXT_HOP per la seva IP corresponent a la interfície per la qual el propaga. Els demès routers, quan reben el UPDATE fan el mateix.

En aquest estat ens centrarem en R2, ja que haurà d'aplicar la política de decisió per escollir la millor ruta originada per R6, incloure aquesta ruta a la seva taula d'encaminament i propagar-la a R1.

Podem veure com el router rep dos UPDATE, un per part de R5 (figura 2) i l'altre per part de R3 (figura 3), ambdós indicant que a través d'ells es pot accedir a la ruta anunciada per R6.

```
▼Border Gateway Protocol - UPDATE Message
  Marker: ffffffffffffffffffffffffffffffff
  Length: 52
  Type: UPDATE Message (2)
  Withdrawn Routes Length: 0
  Total Path Attribute Length: 25
▼Path attributes
  ▶Path Attribut - ORIGIN: IGP
  ▶Path Attribut - AS_PATH: 5050 6060
  ▶Path Attribut - NEXT_HOP: 80.0.0.100
▼Network Layer Reachability Information (NLRI)
  ▶208.65.152.0/22
```

Figura 2. UPDATE de R5 a R2.

```
▼Border Gateway Protocol - UPDATE Message
  Marker: ffffffffffffffffffffffffffffffff
  Length: 60
  Type: UPDATE Message (2)
  Withdrawn Routes Length: 0
  Total Path Attribute Length: 33
▼Path attributes
  ▶Path Attribut - ORIGIN: IGP
  ▶Path Attribut - AS_PATH: 3030 4040 5050 6060
  ▶Path Attribut - NEXT_HOP: 10.0.0.100
▼Network Layer Reachability Information (NLRI)
  ▶208.65.152.0/22
```

Figura 3. UPDATE de R3 a R2.

Segons la política de decisió aplicada pel router per agafar la millor ruta, examinarà un determinat atribut dels atribut de camí [3]. En el nostre cas ens fixarem en l'atribut AS_PATH, ja que és el que utilitzarà R2 per decidir quina ruta agafar per arribar a la xarxa anunciada. Aquest atribut es un camí de sistemes autònoms per els quals s'ha de passar per arribar a la xarxa indicada en el missatge i segons la política de decisió que s'aplica a aquest atribut, el router agafa la ruta amb el AS_PATH més curt.

A la figura 4 podem veure la taula d'encaminament BGP del router R2, on veiem totes les rutes que ha après mitjançant aquest protocol. Comprovem que té dues entrades per la xarxa 208.65.152.0/22, les quals corresponen als UPDATE que ha rebut per part de R3 i R5, de les quals ha marcat com a millor (>) la rebuda per R5, demostrant així que ha aplicat correctament la política de decisió per agafar la ruta més curta. Posteriorment, R2 únicament propagarà a R1 la ruta que li ha estat anunciada per R5.

Una vegada hem demostrat de forma pràctica el funcionament bàsic de BGP: com s'intercanvien actualitzacions els routers, quins atributs porten els missatges, com s'apliquen correctament les polítiques de decisió, quines rutes s'inclouen a les taules d'encaminament,..., passarem a la realització de l'atac i més endavant a la realització del contraatac per recuperar l'estat inicial.

```
bgpdR2# show ip bgp
BGP table version is 0, local router ID is 192.168.0.100
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.0.0.0/24      10.0.0.100               0             0 3030 ?
*>                  0.0.0.0                  0         32768 ?
*  80.0.0.0/24      80.0.0.100               0             0 5050 ?
*>                  0.0.0.0                  0         32768 ?
*  177.16.0.0/24    80.0.0.100                             0 5050 4040 ?
*>                  10.0.0.100               0             0 3030 ?
*  192.168.0.0      192.168.0.1              0             0 1010 ?
*>                  0.0.0.0                  0         32768 ?
*  200.200.0.0      10.0.0.100                             0 3030 4040 5050 ?
*>                  80.0.0.100               0             0 5050 ?
*  205.100.0.0      10.0.0.100                             0 3030 4040 ?
*>                  80.0.0.100               0             0 5050 ?
*  208.65.152.0/22  10.0.0.100                             0 3030 4040 5050 6060
 i
*>                  80.0.0.100                             0 5050 6060 i

Total number of prefixes 7
```

Figura 4. Taula BGP de R2.

5.1.2. Atac

En els següents pasos ens fixarem sobretot en les taules d'encaminament BGP, ja que contenen més informació (com ara el camí de SAs per arribar a la xarxa anunciada) i també podem saber quines són les entrades que s'introdueixen a la taula d'encaminament del kernel, que són les que apareixen marcades com a millor ruta (>).

En aquest moment, comencem amb la realització de l'atac des de SA1010 (Pakistan Telecom). Per realitzar-lo, aquest sistema autònom comença a anunciar una xarxa no autoritzada amb identificador 208.65.153.0/24, la qual es una subxarxa de 208.65.152.0/22, ja que el rang d'adreces de la primera és una part del rang d'adreces de la segona. El routers reben l'anunci d'aquesta nova xarxa i la introdueixen a la seva taula d'encaminament, escollint la millor ruta per arribar a ella. La ruta prèviament anunciada per SA6060 encara es troba a la taula d'encaminament, però com els routers donen preferència a prefixos de xarxa més grans, totes les peticions dirigides a qualsevol adreça que es trobi entre 208.65.153.0 – 208.65.153.255, seran encaminats per la xarxa anunciada per SA1010 en comptes de l'anunciada per SA6060 que és qui realment posseeix aquest rang d'adreces.

Per tant en aquest moments, YouTube es troba inaccessible per tots els SA del nostre escenari.

A la figura 5 podem veure la taula d'encaminament del router BGP R4 amb la nova ruta anunciada per SA1010, amb un AS_PATH de AS5050, AS2020, AS1010. És important fixar-nos en aquest atribut ja que en el següent pas serà un del routers del escenari que decidirà canviar-lo.

```
bgpdR4# show ip bgp
BGP table version is 0, local router ID is 205.100.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.0.0.0/24      205.100.0.100                          0 5050 2020 ?
*>                  177.16.0.1               0             0 3030 ?
*  80.0.0.0/24      177.16.0.1                             0 3030 2020 ?
*>                  205.100.0.100            0             0 5050 ?
*  177.16.0.0/24    177.16.0.1               0             0 3030 ?
*>                  0.0.0.0                  0         32768 ?
*  192.168.0.0      177.16.0.1                             0 3030 2020 ?
*>                  205.100.0.100                          0 5050 2020 ?
*> 200.200.0.0      205.100.0.100            0             0 5050 ?
*  205.100.0.0      205.100.0.100            0             0 5050 ?
*>                  0.0.0.0                  0         32768 ?
*> 208.65.152.0/22  205.100.0.100                          0 5050 6060 i
*  208.65.153.0     177.16.0.1                             0 3030 2020 1010 i
*>                  205.100.0.100                          0 5050 2020 1010 i

Total number of prefixes 8
```

Figura5. Taula d'encaminament BGP de R4.

5.1.3. Recuperació d'una part del tràfic

Avans de recuperar l'estat inicial, YouTube només va recuperar una part del tràfic d'Internet.

En aquest pas, SA6060 comença a anunciar la mateixa xarxa que havia estat anunciada anteriorment per SA1010. Amb dos prefixes iguals els routers apliquen la seva política de decisió per escollir la ruta més convenient. En el nostre cas la que té un camí de sistemes autònoms més curt. Per tant, els routers que rebin el missatge UPDATE la compararan i només si decideixen que la nova ruta indicada és millor, actualitzaran la seva taula d'encaminament i propagaràn el missatge.

En el nostre cas, R4 actuarà tal i com acabem de descriure, ja que l'actual camí que té per arribar a 208.65.153.0/24 passa per SA3030, SA2020, SA1010 i el nou missatge indica que pot arribar a aquesta xarxa a través de SA5050 i SA6060. En canvi R3 per exemple, rebrà el missatge en el qual li indicarà que ha de passar per SA4040, SA5050, SA6060, però com a la taula d'encaminament té una ruta més curta per arribar a aquesta xarxa (SA2020, SA1010) no actualitzarà la seva taula d'encaminament IP i per tant no propagarà el missatge. A la figura 6, podem veure com R4 ha decidit canviar de ruta per arribar a la xarxa que acava de ser anunciada per SA6060.

```
bgpdR4# show ip bgp
BGP table version is 0, local router ID is 205.100.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.0.0.0/24      205.100.0.100                          0 5050 2020 ?
*>                  177.16.0.1               0             0 3030 ?
*  80.0.0.0/24      177.16.0.1                             0 3030 2020 ?
*>                  205.100.0.100            0             0 5050 ?
*  177.16.0.0/24    177.16.0.1               0             0 3030 ?
*>                  0.0.0.0                  0         32768 ?
*  192.168.0.0      177.16.0.1                             0 3030 2020 ?
*>                  205.100.0.100                          0 5050 2020 ?
*> 200.200.0.0      205.100.0.100            0             0 5050 ?
*  205.100.0.0      205.100.0.100            0             0 5050 ?
*>                  0.0.0.0                  0         32768 ?
*> 208.65.152.0/22  205.100.0.100                          0 5050 6060 i
*  208.65.153.0     177.16.0.1                             0 3030 2020 1010 i
*>                  205.100.0.100                          0 5050 6060 i

Total number of prefixes 8
```

Figura 6. Taula d'encaminament BGP de R4.

En definitiva, amb aquest anunci aconsegueix recuperar el tràfic provinent de SA4040, SA5050 i SA6060, però no de la resta. Si féssim una petició des de R3 a YouTube, aquesta s'encaminaria per SA2020, SA1010. Al arribar a aquest últim sistema autònom, R1 no sabria encaminar la petició i per tant, l'eliminaria. A la figura 7, podem veure un *traceroute* des de R3, que demostra com efectivament, succeeix el que acabem d'explicar.

```
carlos@R3:~$ traceroute 208.65.153.238
traceroute to 208.65.153.238 (208.65.153.238), 30 hops max, 60 byte packets
 1  10.0.0.1 (10.0.0.1)  0.240 ms  0.333 ms  0.283 ms
 2  192.168.0.1 (192.168.0.1)  1.086 ms  0.978 ms  0.927 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  *^C
```

Figura 7. *Traceroute* a YouTube des de R3.

5.1.4. Recuperació de l'estat inicial

Finalment, SA6060 recupera l'estat inicial amb l'anunci de dues noves xarxes: 208.65.153.128/25 i 208.65.153.0/25. Tal i com ha fet SA1010 al segon pas anunciant una subxarxa de la que inicialment havia anunciat SA6060, ara és aquest sistema autònom qui anuncia dues subxarxes de la que SA1010 havia anunciat per atreure el tràfic destinat a YouTube. Si ens fixem en aquestes dues xarxes, SA6060 aconsegueix recuperar el rang total d'adreces que la companyia de telecomunicacions pakistanesa li havia "tret": la xarxa 208.65.153.128/25 correspon al rang d'adreces 208.65.153.128-208.65.153.255, i la xarxa 208.65.153.0/25 al rang 208.65.153.0-208.65.153.127. Si recordem, SA1010 havia anunciat 208.65.153.0/24 que abasta les adreces que van des de 208.65.153.0 fins a 208.65.153.255.

Si comprovéssim de nou alguna de les taules d'encaminament BGP d'algún dels routers, veuriem les mateixes entrades més les dues noves xarxes anunciades per SA6060. De nou, com al pas de l'atac (seccio 5.1.2), els routers donen preferencia a prefixos de xarxa més grans i per aquest motiu, qualsevol missagte destinat a una de les IPs esmentades anteriorment serien redirigides correctament al SA6060, l'autèntic posseidor d'aquestes adreces.

Si tornem a executar un traceroute a la màquina de YouTube des de R3 (figura 8), veurem com aquest és encaminat correctament fins a SA6060, a diferència del pas anterior.

Figura 8. *Traceroute* a YouTube des de R3.

```
carlos@R3:~$ traceroute 208.65.153.238
traceroute to 208.65.153.238 (208.65.153.238), 30 hops max, 60 byte packets
 1  177.16.0.100 (177.16.0.100)  0.045 ms  0.011 ms  4.264 ms
 2  205.100.0.100 (205.100.0.100)  4.225 ms  4.092 ms  3.579 ms
 3  200.200.0.100 (200.200.0.100)  3.004 ms  2.358 ms  1.392 ms
 4  208.65.153.238 (208.65.153.238)  0.912 ms  1.689 ms  1.836 ms
```

Per tant, SA6060 ha recuperat l'estat inicial i YouTube torna a ser accesible per tots els sistemes autònoms del nostre escenari.

5.2. Aplicació de mesures de seguretat

Com hem definit a la secció 3.3, BGP proporciona algunes mesures de seguretat que permeten evitar en certa mesura algun dels atacs. Una d'aquestes mesures és la utilització de TCP/MD5 a BGP, que proporciona seguretat per la connexió TCP que el protocol BGP utilitza, com ara autenticació de la identitat dels integrants de la sessió BGP. També hem explicat de forma teòrica una mesura anomenada Prefix Origin Validation que permet validar el sistema autònom d'origen d'un missatge UPDATE, fent ús d'un sistema RPKI. Aquesta última mesura es va presentar de forma pràctica per la plataforma Quagga tot just el passat mes d'Abril [17], fet pel qual no es troba gaire

documentada. Per la documentació que vam trobar, existeixen dues formes per aplicar aquesta mesura de seguretat a Quagga:

- Instal·lar un RPKI i la llibreria RTRLIB per a que Quagga pugui funcionar amb aquesta infraestructura [14].
- Instal·lar l'entorn necessari per fer funcionar BGP-SRx (BGP Secure Routing Extension) proposat pel NIST [15].

Lamentablement, no hem pogut aplicar cap d'aquest dos mètodes aplicables al software Quagga i que permeten donar seguretat al protocol BGP perquè ens hagués calgut instal·lar sistemes CensOS, canviant tota la nostra configuració de l'escenari de proves. En canvi, hem pogut aplicar correctament la mesura TCP/MD5, la qual expliquem com la hem implementat a la següent secció.

5.2.1 Protecció de la sessió BGP a través de la signatura TCP MD5

Com hem pogut veure en aquest TFG, BGP funciona sobre TCP al port 179, el que fa que hereti les seves vulnerabilitats, però també les avantatges: la utilització de números de seqüència, mantenir un comunicació fiable en quant a l'entrega dels missatges,...

La signatura MD5 a TCP permet autenticar mútuament els dos *peers* que formen una sessió TCP, fet que permet a BGP protegir-se contra algun dels atacs, especialment contra aquells que són provocats per un intrús. Es a dir, si una sessió BGP està protegida amb l'ús de TCP MD5, serà més difícil per a un individu que no participa en ella, provocar un atac contra aquesta sessió.

En una sessió protegida amb TCP/MD5, un *peer* BGP que envia un missatge BGP genera un valor hash MD5 utilitzant una clau compartida, parts de la capçalera IP i TCP i el payload. Aquest valor hash es guardat com un camp opcional del segment TCP. Quan l'altre *peer* que forma part de la sessió BGP protegida rep aquest missatge utilitza el mateix mètode per generar el valor hash MD5 utilitzant la clau compartida. Una vegada generat, el compara amb el que es troba al segment TCP del missatge que ha rebut i decideix si acceptar el missatge o no [16].

El software Quagga permet protegir una sessió BGP utilitzant la signatura TCP MD5 d'una manera molt senzilla. Tornant a l'escenari de la figura 1, farem us d'aquesta signatura per la sessió entre R1 i R2. Per això, únicament hem d'incloure al fitxer de configuració del dimoni bgpd de cadascun dels routers la següent comanda: `neighbor address password password`.

Si ambdós *peers* de la sessió BGP tenen la mateixa contrasenya la comunicació es produirà sense problemes, però si es diferent, no s'arribarà a establir la sessió TCP necessària per poder seguidament obrir la sessió BGP. A la figura 9 podem veure aquest últim cas. R1 intenta establir la sessió TCP enviant un SYN. Al no rebre resposta (SYN,ACK), ho torna a intentar fins a dos cops més (en el nostre cas). Després és R2 qui intenta establir la connexió també sense èxit.

Per tant, si ens fixem en el primer missatge dels cinc que es veuen a la figura 9, R1 forma la signatura MD5 amb la capçalera IP, la capçalera TCP, el payload i la clau que se suposa compartida amb R2. Seguidament omple el camp corresponent del segment TCP amb aquesta signatura i envia el primer SYN a R2. Aquest router quan rep el missatge fa exactament el mateix, però utilitzant la clau que ell té com a compartida amb R1. Al no obtenir el mateix resultat (ja que les claus que utilitzen cada router són diferents), no accepta la petició de connexió, elimina el paquet i no ho informa a R1.

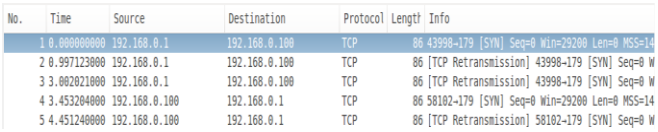

Figura 9. Establiment d'una sessió utilitzant MD5.

Si mirem el contingut d'un d'aquest segments TCP (figura 10), podem veure com apareix el camp opcional MD5, la qual cosa vol dir que s'està fent ús de la signatura. Si no s'estigués fent ús de la comanda anteriorment esmentada, veuríem que aquest camp no apareix al segment TCP (apareixeria Non-Operation), ja que es tracta d'un camp opcional.

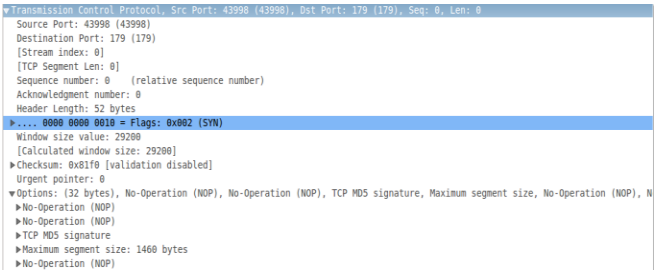

Figura 10. Segment TCP amb el camp MD5 activat.

Aquesta mesura però, és força limitada. És cert que pot protegir contra atacs provinents d'individus que no formen part de la sessió BGP ja que, es gairebé impossible endevinar la clau compartida per els dos participants de la sessió. En canvi, TCP/MD5 no pot protegir contra atacs provinents d'un dels participants en la sessió BGP, que poden ser, si més no, els mateixos atacs que pot generar un atacant extern a la sessió. Per exemple, aquesta mesura no seria capaç de protegir contra l'atac presentat en aquest TFG, ja que està realitzat per un dels participants de la sessió BGP.

6. CONCLUSIONS

La investigació i les tasques realitzades durant aquest TFG ens ha permès deduir que BGP és un protocol bastant vulnerable ja que es poden realitzar atacs amb molta facilitat aprofitant les seves debilitats. No obstant, com hem pogut veure, existeix algun mecanisme de seguretat que permet reduir la probabilitat de reproduir certs atacs.

Durant l'estudi teòric ens hem adonat que la investigació en la seguretat del protocol encara està en ple desenvolupament i que les mesures que existeixen actualment són bastant recents i no donen solució a totes les vulnerabilitats del protocol.

La part pràctica ens ha permès saber, per una banda, que el protocol BGP és bastant fiable en quant al seu funcionament ja que l'intercanvi de missatges i l'aplicació de polítiques BGP són aplicades correctament per els routers. D'altra banda hem pogut demostrar amb un exemple

pràctic real que el protocol és realment vulnerable als atacs estudiats i presentats a la part teòrica.

Fent la comprovació de les taules d'encaminament BGP hem pogut detectar com el comportament dels routers canviava des de l'inici de l'atac fins a la recuperació final, on hem tornat a l'estat inicial. A l'inici, hem vist com els routers han estat enganyats per redirigir el tràfic a un SA incorrecte, i com una xarxa ha quedat inaccessible, simplement amb l'enviament d'un missatge UPDATE. Més endavant hem pogut veure com, de la mateixa forma, s'ha recuperat l'estat inicial.

En l'estudi pràctic també hem pogut demostrar com els routers poden aplicar autenticació TCP/MD5 a través de BGP, una mesura que encara que protegeix contra atacs provinents d'un router extern, és molt limitada en quant a la protecció de la sessió BGP. Els dos routers participants en aquesta sessió poden realitzar atacs encara que aquesta mesura estigui en funcionament.

Desafortunadament, l'altra mesura de seguretat presentada en aquest treball no ha pogut estar demostrada de forma pràctica. El fet de dedicar més temps de l'esperat a certes parts del projecte ens va fer endarrerir la data per començar a buscar possibles mesures de segurtat aplicables al software Quagga. A més a més, els mecanismes de seguretat que permeten validar el SA d'origen han estat portats a la plataforma Quagga fa molts pocs mesos. Concretament la proposta BGP-SRx ha estat portada sobre la plataforma Quagga l'abril de 2015 [17]. La documentació trobada sobre l'altre mètode presentat, que consistia en la instal·lació de un RPKI i la llibreria RTRLIB, també és bastant recent [14]. El fet de trobar aquestes documentacions massa tard va implicar que no hi poguéssim dedicar gaire temps.

Per tant, podem concloure que, encara que existeixen certes mesures de seguretat que fan menys vulnerable el protocol, la seguretat a BGP encara està una mica limitada i creiem que encara queda molt per investigar en ella. És cert que les mesures de seguretat presentades en aquest TFG, permeten protegir contra una gran quantitat dels atacs que es poden realitzar contra el protocol BGP, però encara queden certs problemes que solucionar, com el d'assegurar que a través del camí de SA anunciat en l'atribut AS_PATH es pot arribar realment a la xarxa anunciada. Pel que hem pogut saber, la investigació de l'autenticació del camí de sistemes autònoms es troba en ple desenvolupament [18].

Respecte als objectius presentats inicialment, podem dir que la majoria d'aquests han estat completats amb èxit. Cal destacar que un d'aquests objectius no ha pogut estar completat en la seva totalitat. Aquest objectiu consistia en aplicar alguna mesura de seguretat, aplicable al software Quagga, que pogués evitar l'atac que hem pogut veure reproduït en aquest TFG. Com ja hem explicat, la falta de temps i el fet de trobar la documentació per poder aplicar aquesta mesura gairebé al tram final del projecte han estat un dels majors problemes. No obstant volem destacar que ho vam intentar realitzar, però ens vam trobar amb un problema d'incompatibilitat entre Lubuntu i CentOS. Clarament, hauríem necessitat més temps per resoldre-ho.

Com a treball futur, una continuació natural d'aquest TFG seria implementar de forma pràctica aquesta mesura de seguretat RPKI, ja que permetria evitar la realització de l'atac que hem presentat i reproduït en aquest projecte entre d'altres.

AGRAÏMENTS

M'agradaria agrair als meus pares i al meu germà pel suport que m'han donat. També vull agrair al meu tutor del TFG, Joan Borrell, pels seus consells i suport per poder realizar aquest TFG.

BIBLIOGRAFIA

[1] Roger Serra, "Avaluació pràctica del protocol d'encaminament BGPv4", Universitat Autònoma de Barcelona, Juny 2014.

[2] S. Murphy, "BGP Security Vulnerabilities Analysis". RFC 4272, Gener 2006.

[3] Y. Rekhter, T. Li, S. Hares, "A border gateway protocol 4 (BGPv4)", RFC 4271, Gener 2006.

[4] RIPE Network Coordination Center, "YouTube Hijacking: A RIPE NCC RIS case study". Març 2008. [Online] Disponible a: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.

[5] Russ White, Cisco Systems, "Securing BGP Through Secure Origin BGP", Septembre 2003 [online]. Disponible en: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html

[6] S. Kent, C. Lynn, K. Seo, "Secure Border Gateway Protocol (S-BGP)". IEE Journal on Selected Areas in Communications. Volumen 18, numero 4. Abr. 2000. pp. 582-592.

[7] P. Mohapatra, J. Scudder, D. Ward, R. Bush, R. Austein, "BGP Prefix Origin Validation", RFC 6811, Gener 2013.

[8] C. Bookham. "Versatile Routing and Services with BGP. Understanding and implementing BGP in SR-OS", 2014, pp. 315-317.

[9] A. Heffernan, "Protection of BGP Sessions via the TCP MD5 Signature Option". RFC 2385. Agost 1998.

[10] M. Lepinki, S.Kent, "An Infrastrucure to Support Secure Internet Routing", RFC 6480, Febrer 2012.

[11] M. Lepinki, S. Kent, D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, Febrer 2012.

[12] G. Huston, G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, Feb. 2012.

[13] Quagga Routing Software Suite, 2013 [online] Disponible en: http://www.nongnu.org/quagga/

[14] Alejandro Acosta, "Configuración Quagga para manipular prefijos (Local Preference) utilizando RPKI", Febrer 2014 [online]. Disponible en: http://blog.acostasite.com/2014_02_01_archive.html

[15] NIST, "BGP Secure Routing Extension (BGP-SRx)" Març 2015 [online]. Disponible en: http://www-x.antd.nist.gov/bgpsrx/

[16] Sarmed Rahman, "How to secure BGP sessions using authentication on Quagga", Abril 2015 [online]. Disponible en: http://xmodulo.com/bgp-authentication-quagga.html

[17] O. Borchert, K. Lee, K. Sriram, D. Montgomery, "Quagga and BGP Secure Routing Extension – Quagga SRx –", Abril 2015.

[18] S. Bellovin, R. Bush, D. Ward, "Security Requirements for BGP Path Validation", Octubre 2011.

APÈNDIX

A1. ARXIUS DE CONFIGURACIÓ DIMONI *ZEBRA*

Router BGP R1:

```
! -*- zebra -*-
!
! Zebra configuration file
!
hostname R1
password zebra
enable password zebra
!
interface eth0
 ip address 192.168.0.1/24
!
ip forwarding
!
end
```

Router BGP R2:

```
! -*- zebra -*-
!
! Zebra configuration file
!
hostname R2
password zebra
enable password zebra
!
interface eth0
 ip address 192.168.0.10/24
!
interface eth1
 ip address 10.0.0.1/24
!
interface eth2
 ip address 80.0.0.1/24
!
ip forwarding
!
end
```

Router BGP R3:

```
! -*- zebra -*-
!
! Zebra configuration file
!
hostname R3
password zebra
enable password zebra
!
interface eth0
 ip address 10.0.0.100/24
!
interface eth1
 ip address 177.16.0.1/24
!
ip forwarding
!
end
```

Router BGP R4:

```
! -*- zebra -*-
!
! Zebra configuration file
!
hostname R4
password zebra
enable password zebra
!
interface eth0
 ip address 177.16.0.100/24
!
interface eth1
 ip address 205.100.0.1/24
!
ip forwarding
!
end
```

Router BGP R5:

```
! -*- zebra -*-
!
! Zebra configuration file
!
hostname R5
password zebra
enable password zebra
!
interface eth0
 ip address 80.0.0.100/24
!
interface eth1
 ip address 205.100.0.100/24
!
interface eth2
 ip address 200.200.0.1/24
!
ip forwarding
!
end
```

Router BGP R6:

```
! -*- zebra -*-
!
! Zebra configuration file
!
hostname R6
password zebra
enable password zebra
!
interface eth0
 ip address 200.200.0.100/24
!
ip forwarding
!
end
```

A2. ARXIUS DE CONFIGURACIÓ DIMONI BGPD

Router BGP R1:

```
! -*- bgpd -*-
!
! BGPd configuration file
!
hostname bgpdR1
password zebra
!
router bgp 1010
 neighbor 192.168.0.100 remote-as 2020
 neighbor 192.168.0.100 version 4
!protecció TCPMD5
!neighbor 192.168.0.100 password tcp_md5
 redistribute connected
!xarxa no autoritzada
!network 208.65.153.0/24
!
end
```

Router BGP R2:

```
! -*- bgp -*-
!
! BGPd configuration file
!
hostname bgpdR2
password zebra
!
router bgp 2020
 neighbor 192.168.0.1 remote-as 1010
 neighbor 192.168.0.1 version 4
!protecció TCPMD5
!neighbor 192.168.0.1 password quagga
 neighbor 10.0.0.100 remote-as 3030
 neighbor 10.0.0.100 version 4
 neighbor 80.0.0.100 remote-as 5050
 neighbor 80.0.0.100 version 4
 redistribute connected
!
end
```

Router BGP R3:

```
! -*- bgp -*-
!
! BGPd configuration file
!
hostname bgpdR3
password zebra
!
router bgp 3030
 neighbor 10.0.0.1 remote-as 2020
 neighbor 10.0.0.1 version 4
 neighbor 177.16.0.100 remote-as 4040
 neighbor 177.16.0.100 version 4
 redistribute connected
!
end
```

Router BGP R4:

```
! -*- bgp -*-
!
! BGPd configuration file
!
hostname bgpdR4
password zebra
!
router bgp 4040
 neighbor 177.16.0.1 remote-as 3030
 neighbor 177.16.0.1 version 4
 neighbor 205.100.0.100 remote-as 5050
 neighbor 205.100.0.100 version 4
 redistribute connected
!
end
```

Router BGP R5:

```
! -*- bgp -*-
!
! BGPd configuration file
!
hostname bgpdR5
password zebra
!
router bgp 5050
 neighbor 80.0.0.1 remote-as 2020
 neighbor 80.0.0.1 version 4
 neighbor 205.100.0.1 remote-as 4040
 neighbor 205.100.0.1 version 4
 neighbor 200.200.0.100 remote-as 6060
 neighbor 200.200.0.100 version 4
 redistribute connected
!
end
```

Router BGP R6:

```
! -*- bgp -*-
!
! BGPd configuration file
!
hostname bgpdR6
password zebra
!
router bgp 6060
 neighbor 200.200.0.1 remote-as 5050
 neighbor 200.200.0.1 version 4
 redistribute connected
!YouTube network
 network 208.65.152.0/22
!Recuperació d'una part del tràfic
! network 208.65.153.0/24
!Recuperació de tot el tràfic
! network 208.65.153.128/25
! network 208.65.153.0/25
!
end
```