Robert Hilapieli

Border gateway protocol ja tietoturva

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tekniikan ammattikorkeakoulututkinto

Insinöörityö

17.5.2023

Tiivistelmä

Tekijä:	Robert Hilapieli
Otsikko:	Border gateway protocol ja tietoturva
Sivumäärä:	36 sivua
Aika:	31.5.2023
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Verkot ja pilvipalvelut
Ohjaajat:	Sami Sainio, Yliopettaja

Tämän insinöörityön tavoitteena oli tarkastella BGP (Border Gateway Protocol) protokollan tietoturvaa ja kuinka BGP protokollan väärinkonfigurointi sekä manipuloiminen voi johtaa vakaviin tietoturvariskeihin. BGP-protokolla mahdollistaa runkoverkon viestittelyn ja on näin oleellinen osa nykyisen internetin taustajärjestelmiä.

Työssä esitellään yleisellä tasolla, mikä on BGP sekä mitkä ovat tämän tyypillisimpiä ominaisuuksia. Työn tavoite on esittää kirjallisuusesimerkkien sekä laboratoriosimulaatioiden avulla esimerkkejä, joissa BGP-protokollan haavoittuvuuksia ja heikkouksia on käytetty heikentämään internetin toimivuutta. Tässä työssä esitetään lisäksi ratkaisuja ja suosituksia siihen, kuinka protokollaa pystyy suojaamaan nykyisillä metodeilla tai vaihtoehtoisella protokollalla.

Laboratorioympäristössä esimerkit keskittyvät osoittamaan, kuinka BGP-reittitietoja pystyy manipuloimaan. Yhtenä esimerkkinä käytetään laitteen identiteetin valheellista esitystä muille BGP-protokollaa käyttäville laitteille. Identiteetin valehtelu vaikuttaa verkon tiedonkulkuun. Työssä esitettävät kokeet suoritettiin simuloimalla verkkoa verkkoon yhdistetyillä fyysisillä laitteilla.

Lopputyön hypoteesi on, että suurin osa BGP-protokollan tietoturvariskeistä johtuu virheellisestä konfiguroinnista tai tahallisesta manipuloimisesta eikä välttämättä tietoturva-aukoista itse protokollassa.

Avainsanat: BGP, Tietoturva, Reititys

Tämän opinnäytetyön alkuperä on tarkastettu Turnitin Originality Check -ohjelmalla.

Abstract

Author:	Robert Hilapieli
Title:	Border gateway protocol and security
Number of Pages:	36 pages
Date:	31.5.2023
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	IoT and Cloud Computing
Supervisors:	Sami Sainio, Principal Lecturer

The goal of the bachelor thesis was to examine the security of Border gateway protocol (BGP) and how misconfigurations and BGP manipulation can lead to severe security risks. BGP enables routing between the backbone networks, thus making it an essential part of a functioning internet.

In this thesis, an overview of BGP will be presented, along with its most typical features. The goal is to present literature examples and laboratory simulations that demonstrate how BGP vulnerabilities can be exploited to impact internet functionality. The thesis will also present solutions and recommendations on how BGP can be secured using today's methods or different protocols.

Simulations are conducted in a laboratory environment and focus on how BGP traffic can be redirected and manipulated. One of the simulations includes a scenario where the identity of a device is fabricated to other devices on a BGP network. The fabrication of device identity affects how information is exchanged in a network. The simulations presented in the thesis were performed by simulating a network with connected devices.

The hypothesis of this thesis is that most of BGP security vulnerabilities originate from misconfigurations or intentional manipulation, rather than actual security vulnerabilities in the protocol itself.

Keywords: BGP, Security, Routing

Sisällys

Lyhenteet

1 Johdanto 1

2 Mikä on BGP? 3

2.1 BGP-protokollan tyypilliset ominaisuudet 4
2.2 Kuinka BGP valitsee reitin määränpäähän. 4
2.3 Esimerkkitopologia, kuinka BGP-reitit etenevät 6
2.4 BGP-yhteyden luominen 10

3 Esimerkkejä BGP-protokollan haavoittuvuuksista 11

3.1 AS 7007 11
3.2 Pakistan YouTube block 11
3.3 Google outage May 2005 12
3.4 3ve’s BGP-kaappaukset 13
3.5 KLAYswap kryptovaluutan vaihtopalvelu 15

4 BGP-heikkouksiin liittyvät laboratorioesimerkit 18

4.1 Labra 1 BGP kaappaus 18
4.2 Labra 2 Address resolution protocol (ARP) myrkytys 23

5 Hyvät tavat konfiguroinnissa 27

5.1 Yleisesti toivottuja käytäntöjä 27
5.2 Tietoturvaa parantavia menetelmiä 28
5.3 BGP-Työkaluja 30
5.3.1 BGPStream 30
5.3.2 Routeviews 30

6 Secure-bgp (s-BGP) ja Secure origin-bgp (so-BGP 31

6.1 s-BGP 31
6.2 so-BGP 32

7 Yhteenveto 34

Lähteet 35

Lyhenteet

ARP: *Address Resolution Protocol:* Protokolla, joka hakee IP-verkossa kytkettyjen laitteiden MAC-osoitteet.

AS: *Autonomous System*. BGP:ssä hyödynnetty tunniste tietyn organisaation verkkokonaisuudesta.

BGP: *Border Gateway Protocol.* Internetin reititysprotokolla.

CA: *Certificate Authority:* Organisaatio, joka säilyttää, allekirjoittaa sekä julkaisee allekirjoitettuja sertifikaatteja.

DNS: *Dynamic Name System.* Internetin nimipalvelujärjestelmä.

DoS: *Denial Of Service.* Palvelunestohyökkäys.

EBGP: *External Border Gateway Protocol.* Verkon ulkopuolinen BGP-reititys.

Ipv4: *Internet Protocol Version 4.* IP-protokollan 4. versio.

IBGP: *Internel Border Gateway Protocol.* Verkon sisäinen BGP-reititys.

IGP: *Interior Gateway Protocol.* Kokoelma sisäisistä reititysprotokollista.

EGP: *Exterior gateway protocol:* Kokoelma ulkoisista reititysprotokollista.

IP: *Internet Protocol.* Internetprotokolla, joka mahdollistaa verkkoviestittelyn hyödyntäen IP-paketteja.

ISP: *Internet Service Provider.* Verkon palveluntarjoaja.

RFD: *Route Flap Damping.* BGP-konfiguraatio, joka vaikuttaa reittivalintaan.

ROA: *Route Origin Authorization.* Todistus, joka kertoo IP-prefixien sekä AS-alueen omistajuuden. Käytetään RPKI:n yhteydessä.

MAC: *Medium Access Control.* Yksilöllinen tunniste, joka yleensä löytyy kaikista verkkosovittimista.

MD5: *Message-Digest algorithm.* Hajautusalgoritmi, joka tuottaa 128-bittisen tiivisteen.

RPKI: *Resource Public Key Infrastructure.* BGP:ssä käytetty järjestelmä, jolla voidaan ilmoittaa AS-numeron sekä IP-osoitteiden omistajuuden.

TCP: *Transmission Control Protocol.* Protokolla, jolla voidaan keskustella IP-verkossa.

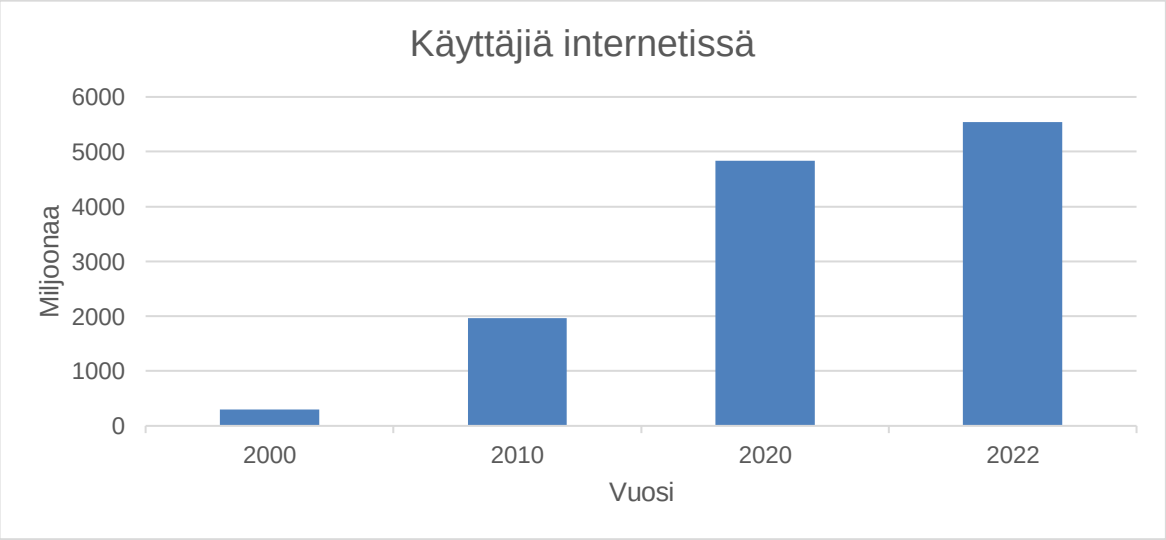
TLS: *Transport Layer Security.* Protokolla, joka mahdollistaa salatun verkkoyhteyden.

TTL: *Time To Live*. Toiminto, joka kertoo, kuinka monen järjestelmän kautta IP-paketti on kulkenut.

1 Johdanto

Nykypäivänä internetin käyttö on suuri osa ihmisten arkipäivää. Esimerkiksi yritykset suosivat kaupankäyntiä verkossa. Pankkiasiat kuten maksaminen suoritetaan monesti verkossa, sekä sosiaalinen kontakti tapahtuu yhä useammin verkon välityksellä. Taulukko 1 havainnollistaa internetin käyttäjämäärän kasvua vuodesta 2000–2022. ICT-alan markkina-arvo vuonna 2022 arvioitiin olevan noin 4535 miljardia dollaria [1]. Verkkoon yhdistämisellä on selkeitä etuja, kun mietitään palveluiden kehitystä tai tuotekehitystä. Edut voivat olla esimerkiksi informaation kulku riippumatta sijainnista, datan analysointi, etähallinta sekä mahdollinen kustannustehokkuus. Täten verkkoon liitettyjen päätelaitteiden toimivuus riippuu suuresti runkoverkon toimivuudesta. Ongelmat runkoverkossa saattavat aiheuttaa isompia ongelmia internetin reititykseen, joka taas saattaa vaikuttaa meidän arkipäiväämme. Pahimmillaan tämä voi vaikuttaa esimerkiksi meidän rahaliikenteeseemme. Jotkut liikkeet eivät enää huoli fyysistä rahaa, vaan maksaminen toimii ainoastaan maksuvälineillä, jotka luottavat verkon toimivuuteen.

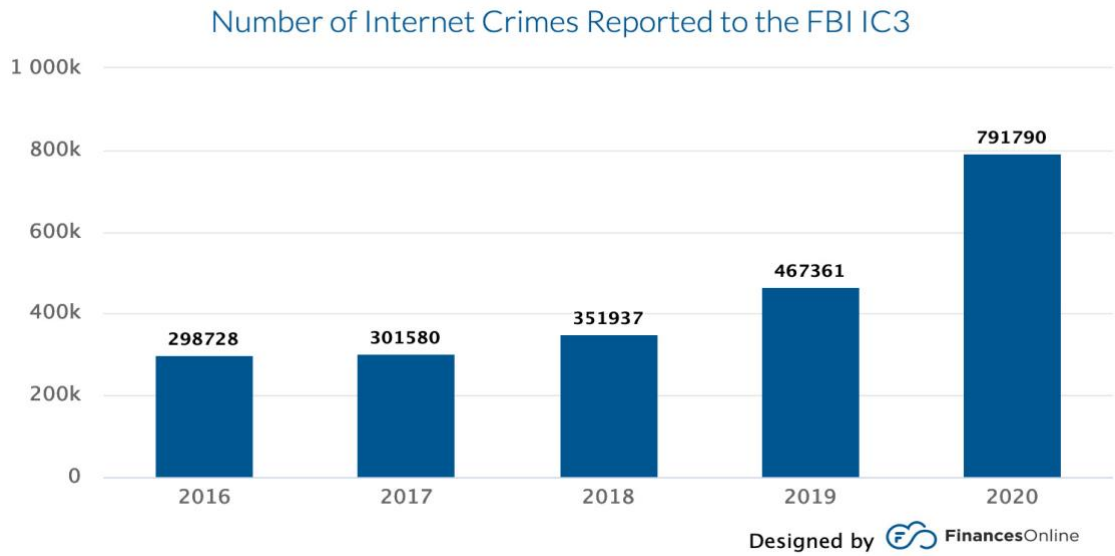
Taulukko 1. Käyttäjämäärät internetissä vuosina 2000-2022 [2].



Internetin tietoturva on ollut hyvin ajankohtainen aihe, oli kyse palvelun katkoksesta [3] laitteiden tietoturvasta [4] tai sensuurista [5]. Tämä on herättänyt

suurta keskustelua sekä huolta, kuinka voimme turvata IT-infrastruktuurin vekkoliikenteen sekä varmistaa yhteyksien luottamuksellisuuden, eheyden sekä saatavuuden. Verkon kautta tehdyt hyökkäykset lisääntyvät, Taulukko 2 kuvastaa FBI:lle tehdyt rikosilmoitukset, jotka liittyivät verkkohyökkäyksiin [6].

Taulukko 2. FBI:n saadut rikosilmoitukset liittyen verkkohyökkäyksiä vuosina 2016–2020 [6].



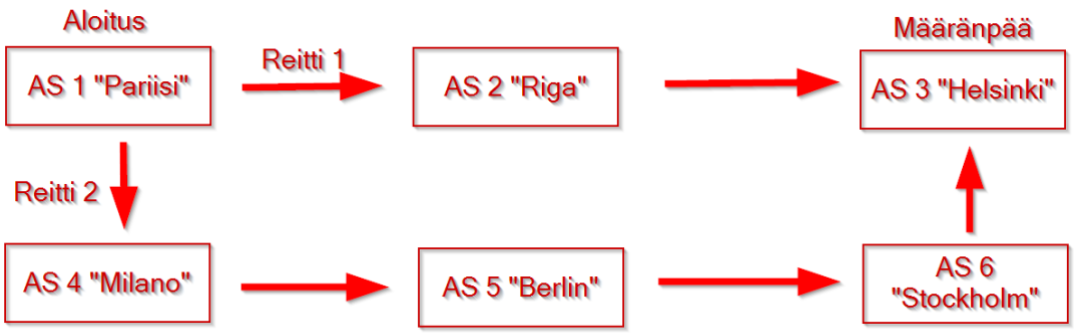
Runkkoverkko, joka ohjaa verkon liikennettää, käyttää ohjaamiseen protokollaa nimeltä ”Border gateway protocol” (BGP) [7]. Mahdollisuus manipuloida liikenteen kulkua antaa hyökkääjälle suuren motiivin yrittää hyväksikäyttää protokollan heikkouksia. Joitakin hyökkäyksiä on havaittu, jossa BGP:tä on hyödynnetty hyökkäyksen kulussa [8]. Esimerkkejä löytyy myös tapauksista, joista ei voida varmuudella sanoa, oliko hyökkäys tahallinen vai tahaton [9].

Tämä lopputyö keskittyy BGP-reititysprotokollan tietoturvaan, jossa tavoitteena on tutkia BGP-protokollan heikkouksia. Tavoite on luoda lukijalle ymmärrys siitä, mikä on BGP:n tietoturvan nykyinen tilanne sekä kuinka BGP:n toimimattomuus saattaa vaikuttaa eri palveluiden toimintaan. Työssä käydään läpi yleiskatsaus BGP:stä ja sen toiminnallisuudesta. Tietoturvaa tarkastellaan erityisesti lähdekirjallisuuden avulla esitellen raportoituja tapauksia, joissa BGP:n toiminta on vaikuttanut internetin toimivuuteen ja/tai luotettavuuteen sekä käydään läpi

pari vaihtoehtoista sekä parannettuja versioita BGP:stä. Lyhyesti käydään läpi pari suositusta hyvästä BGP-käytännöstä ja suoritetaan käytännön esimerkeillä, kuinka BGP:tä pystyy hyväksikäyttämään.

2 Mikä on BGP?

BGP-protokolla on reititysprotokolla, jota käytetään internetin reititykseen. Internetiin kytkettyjen reitittimien avulla voidaan verkko jakaa pienempiin verkkoihin, joita kutsutaan ”Autonomisiksi järjestelmiksi” (Autonomous systems, ”AS”). Internet voidaan miettiä isona verkkona, joka on jaettu tuhansiin pienempiin verkkoihin hyödyntäen AS-menetelmää. BGP:n tavoite on mahdollistaa internetin reititys koosta huolimatta, havaita ja estää silmukoita sekä löytämään nopeimman reitin määränpäähän. Kuva 1 havainnollistaa, kuinka BGP ohjaa liikennettä nopeimman reitin kautta. Aloitus alkaa AS 1:stä ja määränpää on AS 3, BGP:llä on 2 reittiä valittavissa, reitti 1: AS 1 → AS 2 → AS 3 tai reitti 2: AS 1 → AS 4 → AS 5 → AS 6 → AS 3. Tässä tapauksessa reitti 1 on nopeampi ja viesti kulkee sitä kautta. Jos reitti 1 ei ole mahdollista, BGP valitsee reitin 2 määränpäähän.



Kvua 1. Pelkistetty versio BGP:n toimivuudesta.

Kuva 1 sisältää vain kuusi AS-määränpäätä, kun taas todellisuudessa vuonna 2021 Ipv4 AS -lukumäärä vastasi noin 72 500 kpl:tta [10]. Internetin käyttökasvun seurauksena on toimivuuden kannalta erittäin tärkeää, että BGP osaa valita mahdollisimman luotettavan ja nopean reitin. BGP protokolla sisältää attribuutteja, jotka vaikuttavat reittivalintaan. Nämä käydään läpi osiossa 2.2

”Kuinka BGP valitsee reitin”. Kun tietty reitti kokee katkoksen tai topologia muuttuu, laskee BGP uuden parhaimman reitin määränpäähän. On hyvä huomioda, että BGP:n autonoomiset järjestelmät eivät kuulu samaan organisaatioon vaan on hyvin mahdollista, että jonkun yrityksen BGP-reitti kulkee kilpailevan yrityksen AS-alueen kautta. Yritys, jonka kautta BGP-liikenne kulkee, voi myös periä maksuja liikenteestä. Näin ollen BGP:n reittivalinta voi myös perustua kuluihin, joita reittivalinnat aiheuttavat [7].

2.1 BGP-protokollan tyypilliset ominaisuudet

- BGP:tä käytetään yhdistämään sisäiset verkot ulkoverkkoon tai yhdistämään toisiin organisaatioihin. Yhteys, joka luodaan oman AS-alueen ulkopuolelle, on yhteys nimeltään ”external bgp” (EBGP). Kun yhteys luodaan saman AS-alueen sisällä, on yhteys nimeltään ”internal bgp” (IBGP) [11].
- BGP käyttää “**polku-vectori” -**algoritmia saadakseen muilta BGP-puhujilta tiedon verkon saatavuudesta. Tieto tulee reititystietojen päivityksissä (BGP UPDATE). BGP-protkolla ehkäisee silmukoita tarkastelemalla BGP-reittipäivityksen tiedoista. Jos reitittimen oma AS-numero sisältyy tiedoissa, tämä saattaa tarkoittaa, että liikenne on jo kulkenut tämän reitittimen kautta, jolloin kyseessä on mahdollinen silmukka ja protokolla hylkää reittitivalinnan [11].
- **As_path**-atribuutti sisältää kaikkien reitittimien AS-numerot, joiden kautta reitti on kulkenut määränpäähän. Kun reititin jakaa tämän tiedon eteenpäin seuraavalle reitittimelle, lisää se oman AS-numerons AS_path-atribuuttiin [11].

2.2 Kuinka BGP valitsee reitin määränpäähän.

Ensimmäinen pätevä BGP-reitti, jonka reititin vastaanottaa, toimii ensisijaisena reittinä. Tämän jälkeen reititin vertailee kaikkia mahdollisia reittejä

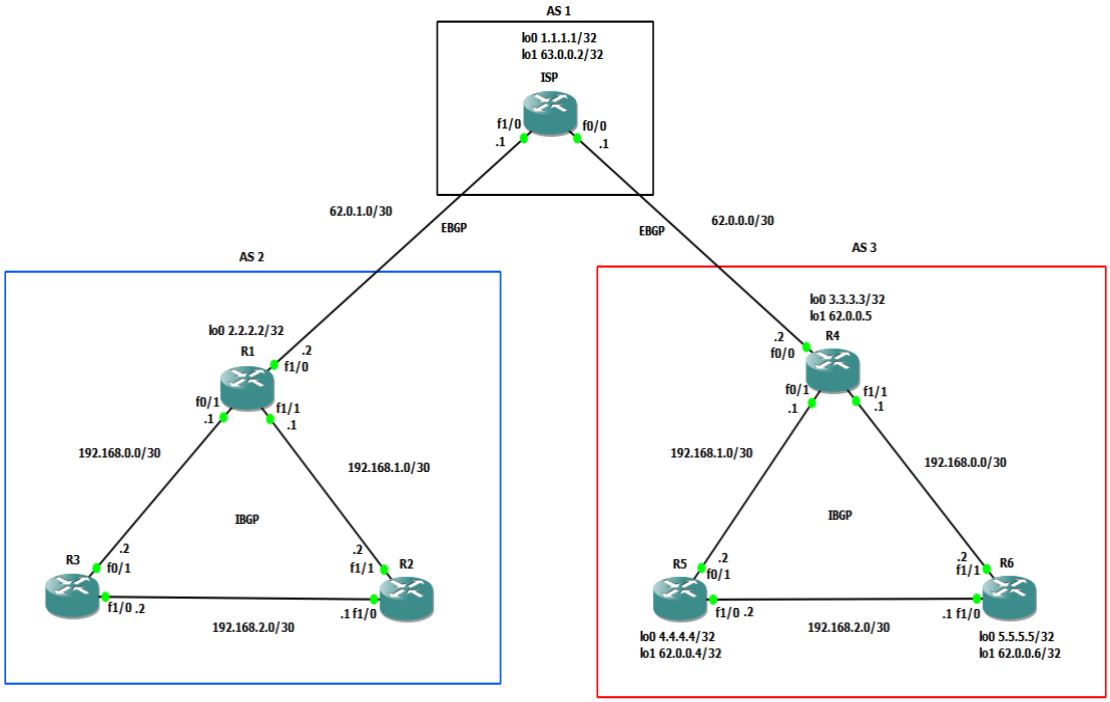
määränpäähän, jotta se voi valita parhaimman reitin. Valintaprosessi etenee seuraavasti:

- **Weight**: Ciscon kehittämä & reitittimissä käytetty arvo. Arvo annetaan paikallisesti reitittimelle, BGP suosii reittinä korkeinta weight arvoa [12].
- **Local preference**: Arvo jaetaan AS-alueen sisällä IBGP välityksellä, oletusarvo on 100. BGP suosii reittinä korkeinta local preference-arvoa [12].
- BGP suosii reittejä, jotka ovat reitittimen omistamia reittejä tai jotka ovat opittuja IBGP:n yli. Näihin kuuluvat network-komennolla opitut reitit sekä koostetut (aggregate) reitit [12].
- **AS_path**: Lyhyempää AS_path-reittiä suositaan [12].
- **Alkuperä**: BGP tarkastelee reitin alkuperää ja suosii järjestyksessä IGP:tä (internal gateway protocol), EGP:tä (external gateway protocol) ja Incompleteä [12].
- **Multi-exit-discriminator (MED)**: Arvo, jonka voi lisätä reitille ja mainostetaan AS-alueiden välillä. Pienempää MED-arvoa suositaan [12].
- BGP valitsee EBGP-reitin mielummin kuin IBGP:n [12].
- Suosii reitin, jolla on pienin IGP metric seuraavalle BGP-naapurille [12].
- Jos paras reitti kohteeseen ei vielä ole päätetty, BGP tarkastelee, jos kohteseen on asennettu monta eri reittiä liikenteen jakamiseen [12].
- Kun reittejä kohteeseen löytyy monia, BGP suosii ensimmäisen vastaanotetun reitin kohteeseen. Tämä vähentää reittien vaihtelevuutta (route-flapping) koska reitti ei vaihdu, vaikka kohdat 11–13 kävisivät toteen, koska BGP suosii ensimmäistä reittiä [12].

- BGP suosii reitin, joka tulee reitittimestä, jolla on pienin router ID. Router ID:n voi joko manuaalisesti asentaa tai oletuksena on reitittimen tarkin IP-osoite [12].
- Kun monet reitit jakavat router ID:n tai alkuperän, valitsee BGP reitin, jolla on pienin cluster list -pituus. Tämä esiintyy ainoastaan ympäristöissä, jossa käytetään route reflector -tekniikkaa [12].
- Viimeisenä BGP suosii reittiä, jolla on pienin naapuriosoite [12].

2.3 Esimerkkitopologia, kuinka BGP-reitit etenevät

Esimerkkitopologia on luotu havainnollistamaan, kuinka BGP-yhteys luodaan sekä kuinka reitit leviävät IBGP:n sekä EBGP:n kautta. Kuva 2 esittää tehdyn verkkotopologian.



Kuva 2. Esimerkkitopologia.

Topologian reitittimet on konfiguroitu luomaan oman AS-alueen sisällä IBGP-naapuruuden toisiinsa, R1:n sekä R4:n, jotka ovat yhdistettynä ISP-reitittimeen. Ne luovat naapuruuden EBGP:n kautta. R1- ja ISP-reitittimet luovat BGP-

naapuruuden käyttäen f1/0-portin konfiguroitua IP-osoitetta, kun taas AS-alueen 3 sisäiset sekä ISP:hen luotu BGP-naapuruus on konfiguroitu käyttäen loopback 0 -osoitetta. AS-alueella 2 reititin R1 mainostaa omaa loopback 0 -osoitetta BGP:lle. AS-alue 3 sekä ISP mainostavat loopback 1 -osoitteita. Mainostetut reitit leviävät AS-alueiden kesken antaen yhteyden jokaiselle osoitteelle, joka on opittu BGP-yhteyden kautta. Alla on listattuna reitittimien R1, R4, R6 ja ISP reittitiedot eri verkkoihin. Osoitteet, joissa näkyy merkintä ”B”, tarkoittavat että reitti on opittu BGP:n kautta. Listauksessa käy ilmi myös reitin AS path, joka kertoo, minkä alueen kautta reitti menee. Reitit, jotka ISP on oppinut BGP:n kautta, ohjautuvat eteenpäin kantaverkkoon, jotta verkkoihin pääsee käsiksi internetin yli.

Reittitiedot komennolla ”show ip route bgp”

R1

```
      62.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
B     62.0.0.0/30 [20/0] via 62.0.1.1, 00:11:22
B     62.0.0.4/32 [20/0] via 62.0.1.1, 00:10:53
B     62.0.0.5/32 [20/0] via 62.0.1.1, 00:10:53
B     62.0.0.6/32 [20/0] via 62.0.1.1, 00:10:53
      63.0.0.0/32 is subnetted, 1 subnets
B     63.0.0.2 [20/0] via 62.0.1.1, 00:11:22
```

R4

```
      2.0.0.0/32 is subnetted, 1 subnets
B     2.2.2.2 [20/0] via 1.1.1.1, 00:09:03
      62.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
B     62.0.0.4/32 [200/0] via 4.4.4.4, 00:09:32
B     62.0.0.6/32 [200/0] via 5.5.5.5, 00:09:32
B     62.0.1.0/30 [20/0] via 1.1.1.1, 00:09:32
      63.0.0.0/32 is subnetted, 1 subnets
B     63.0.0.2 [20/0] via 1.1.1.1, 00:09:32
```

R6

```
      2.0.0.0/32 is subnetted, 1 subnets
B     2.2.2.2 [200/0] via 3.3.3.3, 00:10:04
      62.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
B     62.0.0.0/30 [200/0] via 3.3.3.3, 00:10:33
B     62.0.0.4/32 [200/0] via 4.4.4.4, 00:10:34
B     62.0.0.5/32 [200/0] via 3.3.3.3, 00:10:33
B     62.0.1.0/30 [200/0] via 3.3.3.3, 00:10:33
      63.0.0.0/32 is subnetted, 1 subnets
B     63.0.0.2 [200/0] via 3.3.3.3, 00:10:33
```

ISP

```
      2.0.0.0/32 is subnetted, 1 subnets
B     2.2.2.2 [20/0] via 62.0.1.2, 00:10:59
      62.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
B     62.0.0.4/32 [20/0] via 3.3.3.3, 00:10:58
B     62.0.0.5/32 [20/0] via 3.3.3.3, 00:10:58
B     62.0.0.6/32 [20/0] via 3.3.3.3, 00:10:58
```

Reittitiedot komennolla ”show ip bgp”

R1

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	2.2.2.2/32	0.0.0.0	0		32768	i
*>	62.0.0.0/30	62.0.1.1	0		0	1 i
*>	62.0.0.4/32	62.0.1.1			0	1 3 i
*>	62.0.0.5/32	62.0.1.1			0	1 3 i
*>	62.0.0.6/32	62.0.1.1			0	1 3 i
*	62.0.1.0/30	62.0.1.1	0		0	1 i
*>		0.0.0.0	0		32768	i
*>	63.0.0.2/32	62.0.1.1	0		0	1 i

R4

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	2.2.2.2/32	1.1.1.1			0	1 2 i
*	62.0.0.0/30	1.1.1.1	0		0	1 i
*>		0.0.0.0	0		32768	i
*>i	62.0.0.4/32	4.4.4.4	0	100	0	i
*>	62.0.0.5/32	0.0.0.0	0		32768	i
*>i	62.0.0.6/32	5.5.5.5	0	100	0	i
*>	62.0.1.0/30	1.1.1.1	0		0	1 i
*>	63.0.0.2/32	1.1.1.1	0		0	1 i

R6

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>i	2.2.2.2/32	3.3.3.3	0	100	0	1 2 i
*>i	62.0.0.0/30	3.3.3.3	0	100	0	i
*>i	62.0.0.4/32	4.4.4.4	0	100	0	i
*>i	62.0.0.5/32	3.3.3.3	0	100	0	i
*>	62.0.0.6/32	0.0.0.0	0		32768	i
*>i	62.0.1.0/30	3.3.3.3	0	100	0	1 i
*>i	63.0.0.2/32	3.3.3.3	0	100	0	1 i

ISP

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	2.2.2.2/32	62.0.1.2	0		0	2 i
*	62.0.0.0/30	3.3.3.3	0		0	3 i
*>		0.0.0.0	0		32768	i
*>	62.0.0.4/32	3.3.3.3			0	3 i
*>	62.0.0.5/32	3.3.3.3	0		0	3 i
*>	62.0.0.6/32	3.3.3.3			0	3 i
*	62.0.1.0/30	62.0.1.2	0		0	2 i
*>		0.0.0.0	0		32768	i
*>	63.0.0.2/32	0.0.0.0	0		32768	i

2.4 BGP-yhteyden luominen

BGP-reitittimet eivät automaattisesti löydä toisia BGP-konfiguroituja laitteita, vaan nämä tulee määritellä erikseen. Kun BGP-yhteys on määritetty ja reititin luo yhteyden toiseen BGP-reitittimeen, kutsutaan tätä reititintä naapuriksi. Tämä ei välttämättä tarkoita sitä, että naapuri reititin olisi suoraan kytkettynä omaan BGP-reitittimeen. BGP:tä puhuvat reitittimet ovat nimeltään ”BGP speaker”. BGP-naapurit, joihin BGP-yhteys luodaan, kutsutaan ”BGP peeriksi”. BGP-peerit jakautuvat ulkoisiin ja sisäisiin, mikä riippuu siitä, ovatko ne AS-alueen sisällä vai ulkopuolella. BGP-yhteys naapurireitittimeen tapahtuu TCP-protokollan välityksellä ja toimii portin 179 kautta. Kun yhteys on luotu, jakavat reitittimet omat BGP-reititystaulut toisilleen. Tämän jälkeen reitittimet jakavat reittipäivityksiä, jos verkon topologia muuttuu tai jos konfiguroidaan muita reittiin vaikuttavia asetuksia. Kun BGP-reititin luo yhteyden toiseen naapuriin, käyvät reitittimet läpi seuraavat vaiheet:

- Idle: Ensimmäinen tila, josta reititin löytää itsensä, kun reititysprotokolla määritetään reitittimelle. Tähän tilaan reititin päätyy myös, jos laite resetoituu tai menettää aktiivisen yhteyden naapuriin. Idle-tilassa reititin odottaa määritystä naapurille ja naapurilta TCP-yhteyden pyyntöä [13].
- Connect: Reititin saa naapurilta pyynnön yhdistää TCP-yhteys näiden välillä [13].
- Active: BGP-reititin yrittää luoda TCP-yhteyttä naapurille käyttäen ConnectRetry ajastinta. Jos BGP-määritykset muuttuvat virheen sattuessa, reitittimet palaavat idle-tilaan [13].
- OpenSent: TCP-yhteys on muodostettu ja BGP-reitittimet vaihtavat OPEN-viestejä keskenään. OPEN-viestien vaihto on pakollista, viestiin sisältyy tiedot BGP-versiosta, AS-numero, Hold timer (aika jota reititn odottaa Keepalive-viestiä), BGP ID (bgp router id) ja vaihtoehtoisia tietoja kuten tuki multi protocol BGP:lle. Jos OPEN-

viestien vaihto epäonnistuu, palaavat reitittimet takaisin Active-tilaan [13].

- OpenReceive: Reitittimet ovat vastanottaneet OPEN-viestit ja odottavat seuraavaksi naapurin keepalive-viestiä. Keepalive-viestit kertovat naapurille, että kyseinen yhteys on aktiivinen. Kun reitittimet vaihtavat onnistuneesti keepalive-viestit, siirtyvät reitittimet established-tilaan [13].
- Established: Onnistunut BGP-yhteys on luotu, naapurit vaihtavat BGP UPDATE -viestejä keskenään, joihin kuuluvat reitittimen BGP-reititystiedot [13].

3 Esimerkkejä BGP-protokollan haavoittuvuuksista

3.1 AS 7007

Vuonna 1997 internet koki isomman katkon, kun pienempi yhdysvaltalainen palveluntarjoaja nimeltä MAI Networks vuoti asiakkaidensa reititystietoja eteenpäin. Tiedot vuosivat eteenpäin yritykselle, joka tarjosi kantaverkkoa monelle pienemälle palveluntarjoajalle Pohjois-Amerikassa. Tämä aiheutti laajoja yhteyskatkoja tiettyihin verkkopalveluihin, suurimmalta osin paikallisesti mutta saattoi myös näkyä kansainvälisesti. Tämänkaltaiset reittivuodot voidaan ehkäistä hyödyntäen oikeanlaista reittisuodatusta, joko asiakkaan puolelta tai operaattorin puolelta. [14.]

3.2 Pakistan YouTube block

Vuonna 2008 Pakistan halusi estää pääsyn YouTube-verkkosivulle. Tämä haluttiin saavuttaa muokkaamalla Pakistanin palveluntarjoajan AS 17557 (Pakistan Telecom), BGP-reititystietoja Youtuben verkkosivulle [5]. YouTube (AS36561) mainosti BGP:lle-osoitetta 208.65.152.0/22, kun yksi Pakistanin palveluntarjoajista alkoi mainostaa BGP:lle tarkempaa osoitetta 208.65.153.0/24, jolloin BGP:n reititys preferoisi tätä liikenteelle. Pakistanin BGP-päivitys päivittyi

isomman runkoverkon operaattorille (PCCW Global) joka, lähetti reittitiedot eteenpäin globaalisti. DNS-pavelimesta katsottuna YouTuben kotisivulle johti kolme IP-osoitetta 208.65.153.238, 208.65.153.251 sekä 208.65.153.253, kun Pakistanin palveluntarjoaja alkoi mainostaa /24 prefixiä, ohjautui YouTuben verkkoliikenne Pakistanin kautta. Kun liikenne saapui Pakistaniin, ohjautui liikenne ”mustaan aukkoon” (black hole), joka ei johtanut mihinkään, joten kaikki saapuva liikenne hylättiin. YouTube reagoi kaappaukseen nopeasti ja alkoi 80 minuutin sisällä mainostamaan BGP:n kautta samaa 208.65.153.0/24-osoitetta, jolloin verkkoliikenne ohjautuu BGP:ssä lyhyimmän AS path -arvon mukaisesti. Nyt osa liikenteestä ohjautuu YouTubeen, kun taas osa vielä Pakistaniin. Tämän jälkeen YouTube mainosti vielä tarkempaa osoitetta 208.65.153.0/25 sekä 208.65.153.128/25 jolloin, kaikki, jotka saavat tämän reittipäivityksen, ohjaavat liikenteen YouTubeen koska, prefixi on tarkempi. On hyvä huomioda, että palveluntarjoajat saattavat suodattaa prefixejä, jotka ovat tarkempia kuin /24, esim. /25, /26 jne. Lopulta PCCW Global hylkäsi kaikki AS17557-reittitiedot, jonka jälkeen prefixin kaappaus lakkasi. Kaiken kaikkiiaan kaappaus jatkui noin kahden tunnin ajan.

Ensisijaisesti Pakistan halusi estää kaikki oman maan liikenteen YouTubeen, mikä sinänsä ei ole hyökkäys palvelua kohtaan, mutta jos Pakistanin halu oli estää liikenne mailmanlaajuisesti, voitaisiin todeta, että tämä oli tahallinen hyökkäys YouTube-palveluun. Suojautuminen prefix-kaappauksiin vaatii operaattorilta konfiguraation, joka estää kaappauksen tai ”route origin authorization” (ROA) käyttöä pitäisi lisätä, mikä vahvistaisi BGP-reitin omistajuuden. [16.]

3.3 Google outage May 2005

Vuonna 2005 Googlen omistama preifixi 64.233.161.0/24 (AS 15169) joutui BGP-kaappauksen uhriksi [3]. Yritys nimeltä Cogent (AS 174) joka oli suorassa yhteydessä Googleen, alkoi mainostamaan 64.233.161.0/24 prefixiä, jonka määränpää oli AS 174 eikä Googlen omistama AS 15169. Tästä tehtiin laajempi tutkimus Kanadan tietotekniikan koulussa (School of Computer Science Carleton University, Ottawa, Canada), jossa haluttiin tutkia mahdollista vaihtoehtoa

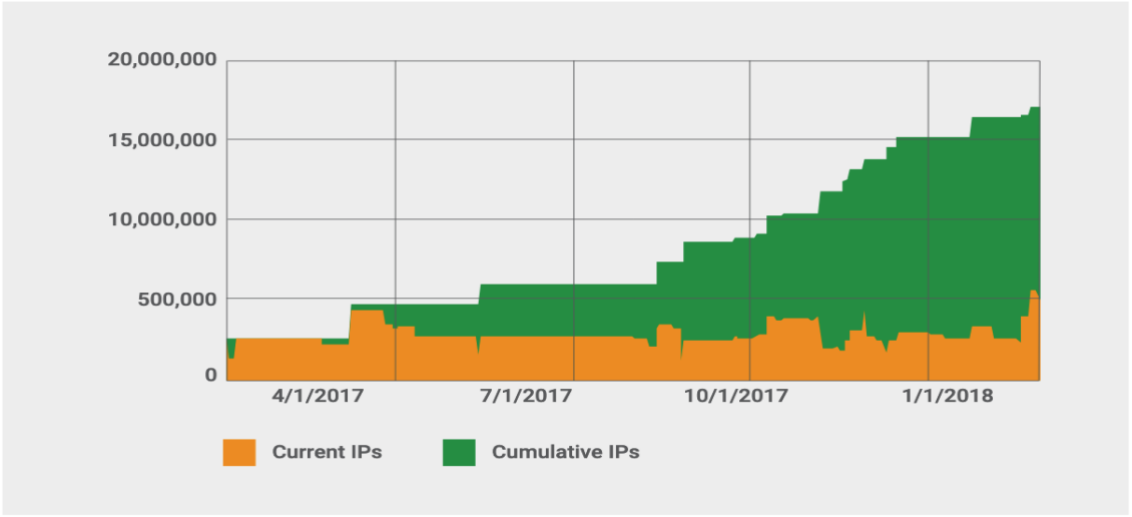
tahalliselle hyökkäykselle. Raportissa todetaan, ennen osoitteen kaappausta, että 56 eri AS- aluetta mainostaa reittiä osoitteelle 64.233.161.0/24 joista vain yksi reitti käy AS 174-alueen kautta. Tätä reittiä mainostaa itse AS 174. Kaappauksen aikana 57 AS-aluetta mainostaa reittiä osoitteelle 64.233.161.0/24, joista 31 kpl mainostaa reitin alkuperänä AS 174-aluetta. 28 kpl näistä 31 mainostuksista suosivat AS 174 -reittivalintaa AS 15169:n sijaan, joista 8 oli suorassa yhteydessä AS 15169:ään. Reittimainostukset levisivät jopa isompiin palveluntarjoajiin kuten UUNET:iin (AS 701), IIJ:hin (AS 2497), C&W:iin (AS 2561) sekä AT&T:hen (AS 7018). Ongelma kesti alle tunnin, jonka jälkeen normaali reititys jatkui. Raportissa käydään myös keskustelua Googlen sekä Cogentin kanssa. Google myöntää todenneensa yhteysongelmia osoitteeseen 64.233.161.0/24, mutta epäilivät myös ongelmia niiden DNS- palvelimissa, joissa myös piileksi oikea väärinkonfiguraatio, joka levisi eteenpäin. Raportin luettuaan Google kuitenkin havahtui BGP:n haavoittuvuuteen ja sanoi vahvistavansa omaa BGP-valvontaansa. Cogent ei halunnut vastata raportin tiedusteluun vaan perusteli hiljaisuuttaan vaitiolovelvollisuudella, jonka olivat allekirjoittaneet. [3.] Tämä skenaario herättää kuitenkin suuria huolia, jos kyseessä oli tahallinen hyökkäys isoa yritystä kohtaan, jossa liikennettä olisi voitu manipuloida sekä uudelleenohjata haittatarkoituksiin. Cogentin vaitiolo ei syytä niitä mutta ei myöskään vapauta syytteistä.

3.4 3ve’s BGP-kaappaukset

3ve-hyökkäys ilmoitettiin vuonna 2016, kun ”White ops” -niminen yritys julkaisi havaintonsa, mutta ensimmäinen AS ”Alpha” kytkettiin internetiin jo vuonna 2013 [8]. 3ve:n haitallinen toiminta tuotti tuloja mainostulojen sekä botnetin kautta. 3vellä oli kolme erilaista hyökkäysoperaatiota, joista ensimmäisessä hyödennettiin BGP-kaappausta, jotta operaatio saisi enemmän IP-osoitteita käyttöönsä. Ensimmäiset BGP-kaappaukset todettiin maaliskuussa vuonna 2017, kun AS ALPHA alkoi kaappaamaan AS-numeroita, jotka eivät olleet aktiivisessa käytössä. ALPHA koetti valikoida tarkasti kaappauksensa, koska monissa saattoi olla vielä akttivisia (pahasti vanhentuneita) webbipalveluita. Suuri osa kaappauksista oli hosting-palveluiden vanhoja AS-numeroita sekä yrityksiä,

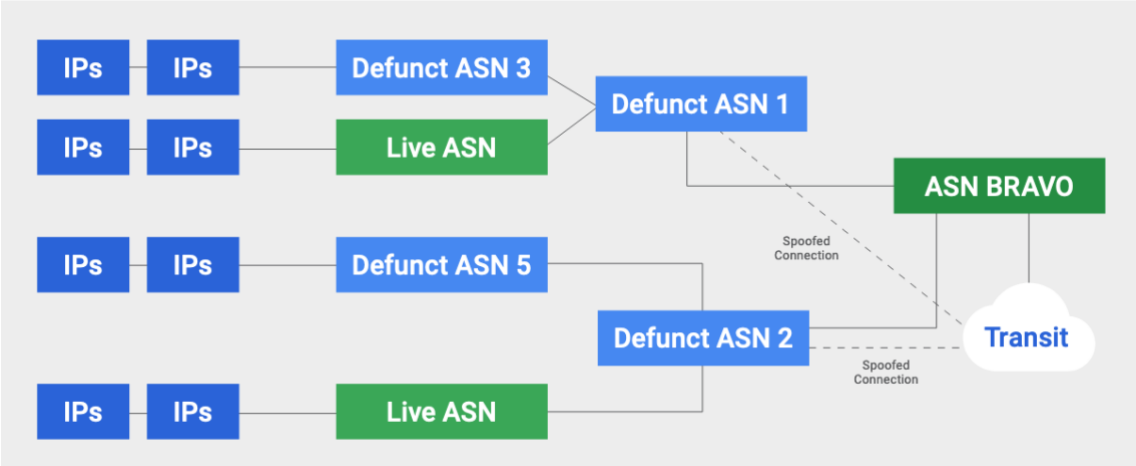
jotka olivat samalta maantieteelliseltä alueelta. Elokuussa 2017 operaatio laajeni, kun operaatioon lisättiin uusi AS-alue, joka korvasi AS ALPHAN. Uuden AS:n nimi oli BRAVO. BRAVON ero ALPHAAN oli suurempi lukumäärä transit-palveluntarjoajia. Mukana oli myös ALPHAN vanhat transit-palveluntarjoajat. Ideana oli, jos yksi transit-palveluntarjoaja estäisi BRAVON liikenteen, voisi BRAVO helposti uudelleenohjata liikennettä toisen palvelun kautta. BRAVON liikenne oli myös järjestelty monipuolisemmin. Yhden kaapatun AS:n takana pystyi olemaan monta muutakin AS:ää, joka antoi illuusion oikeasta verkkoliikenteestä eikä haitallisesta. AS-alueiden kierto oli myös nopeampi kuin AS ALPHASSA, joka myös vaikeutti palveluntarjoajien mahdollisuutta estää liikennettä. Taulukko 3 esittää AS BRAVON kaapattujen IP-osoitteiden lukumäärän.

Taulukko 3. AS BRAVO kaapatut IP-osoitteet versus 2018 käytössä olevat [8].



Vuoden lopussa 2017 3ve kyllästyi paveluntarjoajien estoihin ja alkoi aggressiivisemman taktiikan. He alkoivat myös kaappaamaan aktiivisia AS-numeroita. Tämä on mahdollista, koska tietyt reititykset saattavat käyttää samaa AS-numeroa eri sijainneista, mutta ilmoittavat vain tiettyjä osoitteita eri sijainneista. Tämä vaikeutti palveluntarjoajien mahdollisuutta estää haitallista liikennettä, jossa riskinä oli estää myös oikeaa luotettavaa liikennettä. BRAVON yhteyksiä pyrittiin eri menetelmillä naamioimaan luotettavaksi mm. tekaistuilla

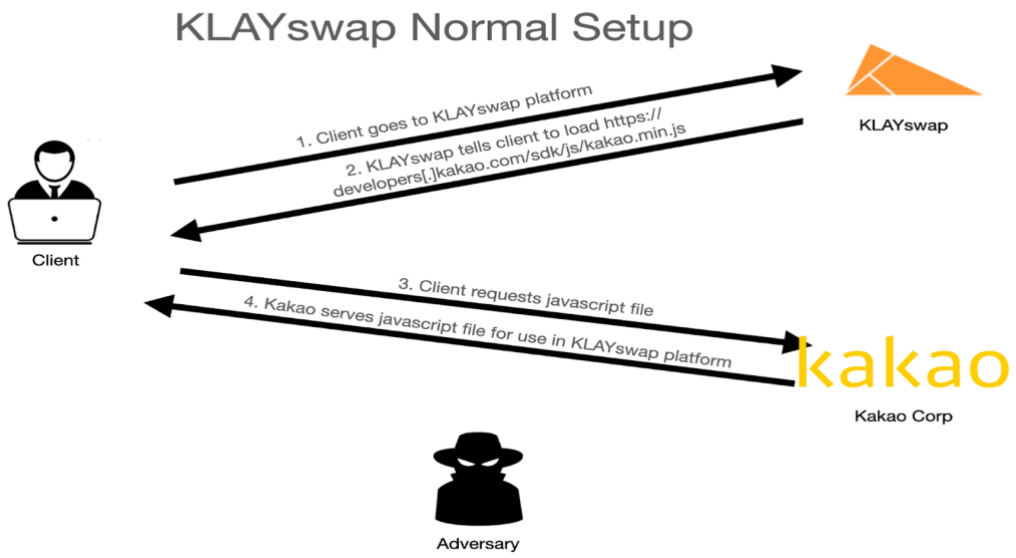
yhteyksillä sekä tarjoamalla läpivientiliikennettä tietyille oikeille ja luotettaville verkoille. Kuva 3 esittää topologian, kuinka AS BRAVO jakoi liikennettään.



Kuva 3. AS BRAVO:n topologia [8].

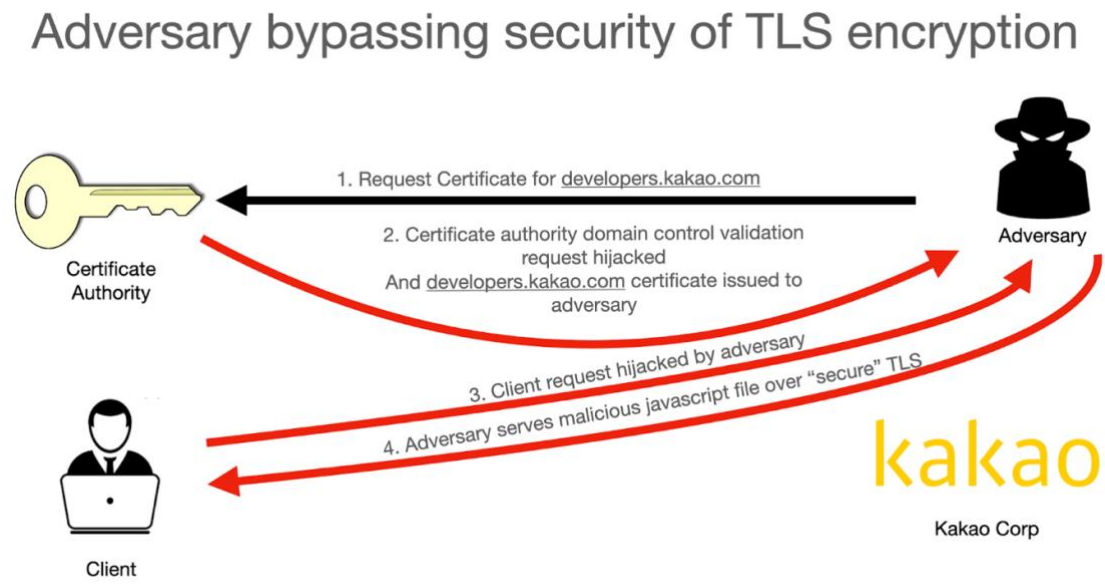
3.5 KLAYswap kryptovaluutan vaihtopalvelu

Korean kryptovaluttapörssi KLAYswap joutui hyökkäyksen kohteeksi. KLAYswap käytti palvelussaan JavaScriptiä, joka oli kirjoitettu toisen yrityksen toimesta nimeltä ”Kakao corp” [4]. JavaScript latautui loppukäyttäjälle Kakaon omilta palvelimilta, kun käyttäjä asioi KLAYswapin palvelussa. Kuva 4 esittää, kuinka KLAYswap tarjoaa Kakaon luomaa JavaScriptiä. Tässä hyökkäyksessä hyökkäjäät kaappasivat Kakao:n IP-osoitteet hyödyntäen BGP-protokollaa, jonka jälkeen heillä oli jalansija yhteyksissä sekä pystyivät etenemään hyökkäyksessä.



Kuva 4. Käyttäjä vierailee KLAYswapin sivuilla, joka tarjoaa Kakaon JavaScriptiä [4].

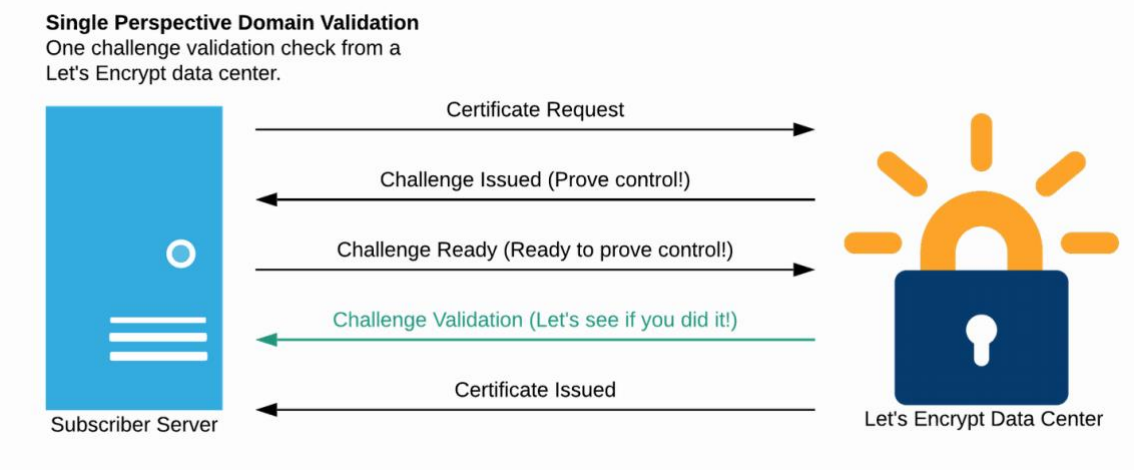
Seuraava vaihe hyökkäyksessä oli Julkisten avainten järjestelmä (public key infrastructure PKI) ja saada käyttöönsä luotettava sertifikaatti, jotta hyökkääjät pystyisivät hyödyntämään KLAYswapin sekä Kakaon TLS-protokollaa. Yritykset, jotka myöntävät varmenteita, kutsutaan ”Certificate Authorityksi” (CA). Tässä tapauksessa hyökkääjät onnistuivat vastaamaan CA:n pyyntöihin, koska verkkotunnuksen vahvistusliikenne kävi heidän kauttaan ja näin ollen saamaan allekirjoitetun sertifikaatin. Sertifikaatti oli domainiin developers.kakao.com, joka tarjosi KLAYswapin palvelulle javaScriptin. Nyt hyökkääjillä oli mahdollisuus tarjota heidän omaa JavaSrciptiä hyödyntäen luotettavaksi luoteltua TLS-yhteyttä. Kuva 5 esittää prosessia, kuinka hyökkääjä pyytää allekirjoitettua sertifikaattia ja tarjoaa tätä käyttäjille KLAYswapin sivuilla.



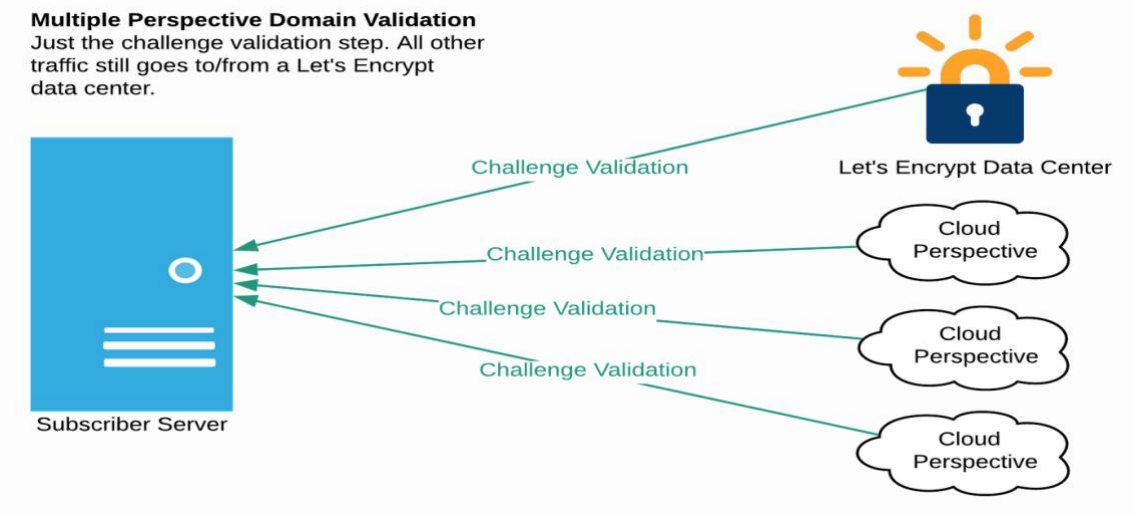
Kuva 5. KLAYswapin vierailija lataa hyökkääjän JavaScirptin [4].

Hyökkäys kesti noin kaksi tuntia, jonka jälkeen hyökkäys lopetettiin ja voitot kerättiin talteen. Hyökkääjät onnistuivat kaappaamaan noin 2 miljoonaa dollarin arvosta kryptovaluuttaa [4].

Mahdollinen suojauskeino vastaavalle hyökkäykselle olisi, että CA alkaisi käyttämään monipuolisempaa varmennusta, kun uudet tahot pyytävät allekirjoitettua sertifikaattia. Let's Encrypt on kehittänyt monivaiheisen todennuksen, joka luultavasti olisi estänyt tämän hyökkäyksen. Let's Encrypt -sivujen mukaan käy ilmi, että tämä on luotu nimenomaan BGP-kaappauksien varalle. Lyhykäisyydessään tämä uusi menetelmä varmentaa sertifikaatin pyytäjän alkuperäisyyden monesta eri geograafisesta sijainnista [15], jolloin hyökkääjien pitäisi suorittaa huomattavasti suurempi BGP-kaappaus kuin KLAYswapin esimerkissä. Kuva 6 ja 7 esittelee yksivaiheisen ja monivaiheisen tunnistuksen.



Kuva 6. Yksivaiheinen varmentaminen [15].



Kuva 7. Monivaiheinen varmentaminen [15].

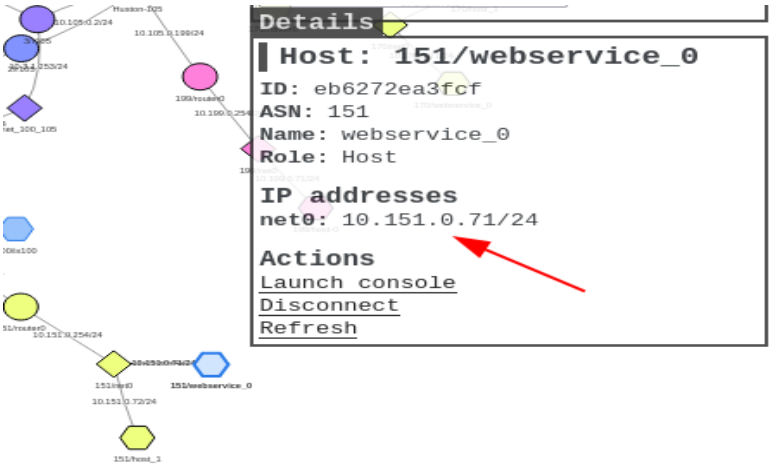
4 BGP-heikkouksiin liittyvät laboratorioesimerkit

4.1 Labra 1 BGP kaappaus

BGP hijacking tapahtuu, kun ulkopuolinen taho ilmoittaa väärin tietyn ryhmän IP-osoitteiden omistajuuden, joita tämä taho ei välttämättä omista tai hallinnoi. Kun IP-osoitteiden omistajuus muuttuu, muuttuu myös reitti ja mahdollisesti määränpää, kun päätelaitteet tekevät kyselyitä osoitteisiin. Uhkat, joita kaappaus aiheuttaa, mahdollistavat verkkoliikenteen monitorointia, verkkoliikenteen uudelleenohjauksen esimerkiksi verkkosivulle, josta yritetään varastaa

käyttäjätietoja, verkkoliikenteen ohjauksen mustaan aukkoon, johon liikenne pysähtyy. Joissakin tapauksissa liikenne osoitteisiin vain hidastuu päätelaitteiden puolelta, mikä lisää kyselyiden viivettä. BGP kaappaus -esimerkissä käytetty seed-emulaattoria.

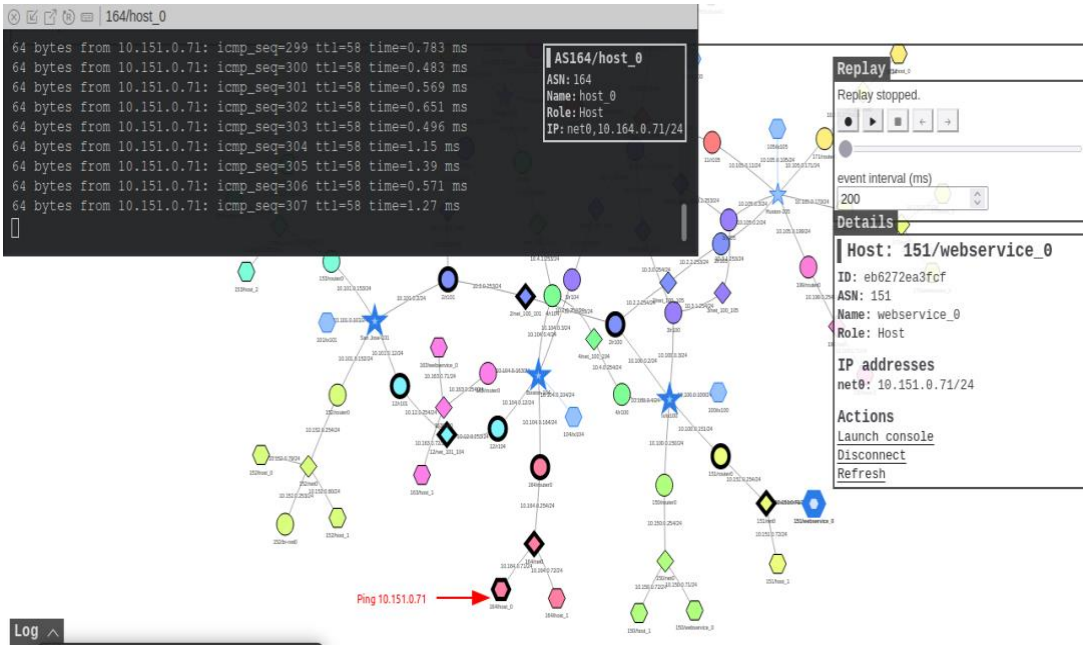
- Siirry terminaalista esimerkkikansioon ”B04-bgp-prefix-hijacking” ja aja tarvittava python-tiedosto komennolla ”python3 ./bgp-prefix-hijacking.py”.
- Siirry terminaalista uuteen output-kansioon ja rakenna docker-komennoilla ”sudo docker-compose build && docker-compose up”.
- Käynnistä client tämän omasta kansiosta komennolla ”sudo docker-compose build && docker-compose up”.
- Avaa selain ja siirry osoitteeseen 127.0.0.1:8080/map.html#.
- Valitse joku sopiva IP-osoite, jonka haluat kaapata sekä ota huomioon osoitteen maski. Tässä esimerkissä kaapataan osoite 10.151.0.71/24. Kuva 8 havainnolistaa kaapattavan osoitteen.



Kuva 8. Kaapattava IP-osoite 10.151.0.71/24 (AS 151).

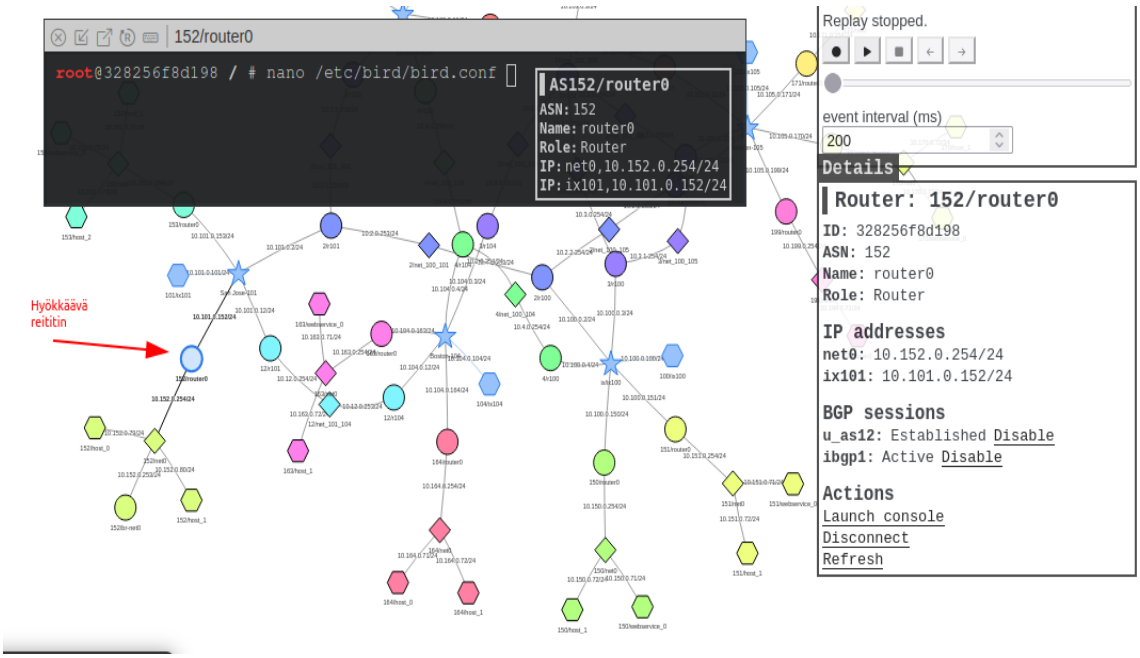
- Ennen kaappaamista suorita ping-komento toisesta IP-verkosta ja seuraa liikenteen kulkua. Liikenteen voi suodattaa seed emulatorista komennolla ICMP sekä täsmentää, jotta vain liikenne kaapattavaan IP-osoitteeseen näkyy komennolla ICMP && dst x.x.x.x. Kuva 9

havainnollistaa, kuinka osoite 10.151.0.71 vastaa onnistuneesti ping-komentoon.



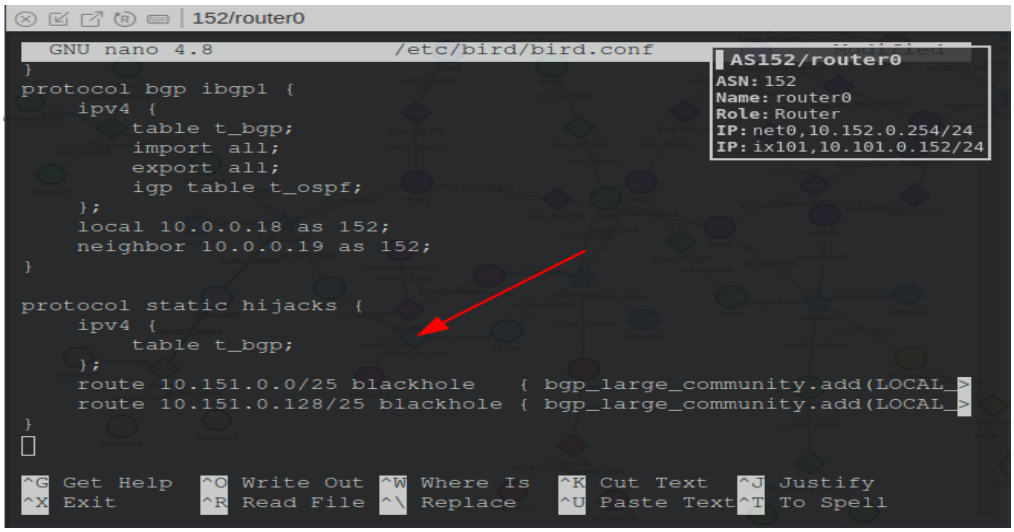
Kuva 9. Ping-komento suoritettu päätteeltä 10.10.164.0.71 (AS 164), joka johtaa päätteelle 10.151.0.71.

- Valitse BGP-reititin, jolla haluat kaapata verkon. Avaa terminaali sekä avaa birdc konfiguraatio polusta nano /etc/bird/bird.conf. Kuva 10 havainnollistaa kaappaajan.



Kuva 10. Kaappaus suoritetaan AS 152 alueelta.

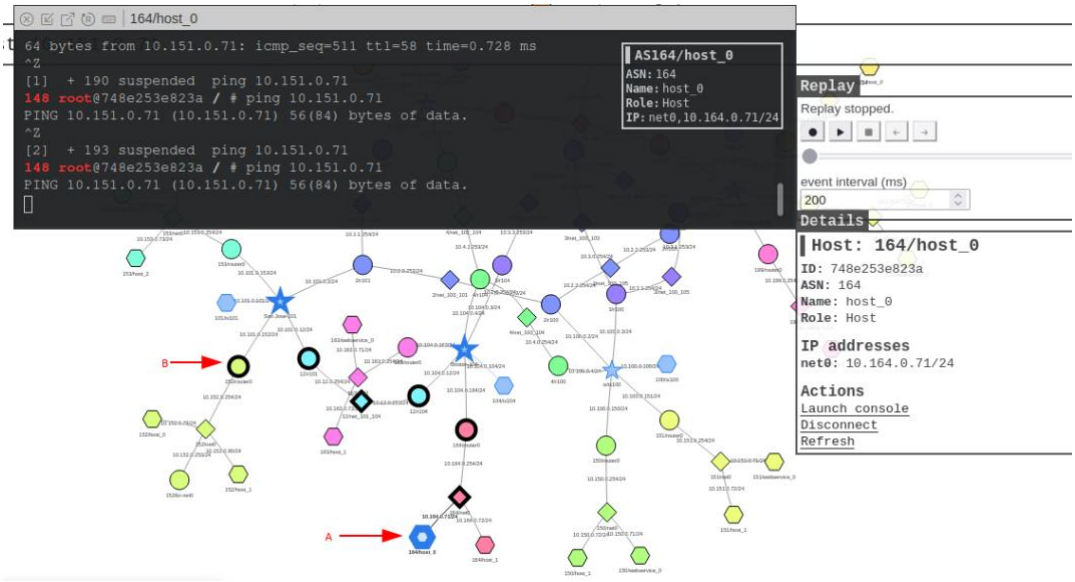
- Lisää konfiguraation loppuun uusi BGP-määritelmä, jossa viitataan kaapattavaan verkkoon mutta tarkemmalla määritelmällä esim. pienemmällä maskilla kuin kaapattavan verkon konfiguraatiossa. Kuva 11 havainnollistaa konfiguraatiomuutoksen, jossa kaapataan osoite 10.151.0.0 /25-maskilla.



Kuva 11. Lisätty tarkempi prefix kaapattavalle IP-osoitteelle.

- Tallenna ja sulje konfiguraatio sekä ota käyttöön uusi konfiguraatio ajamalla komento ”birdc configure” terminaalissa.

  Yritä uudestaan pingata kaapatun verkon IP-osoitetta ja seuraa, kuinka reitti on muuttunut. Tällä hetkellä pingin ei kuuluisi mennä läpi. Kuva 12 havainnollistaa, kuinka kaapattu osoite ei enää vastaa.



Kuva 12. AS 152 kaapannut AS 151 prefixin.

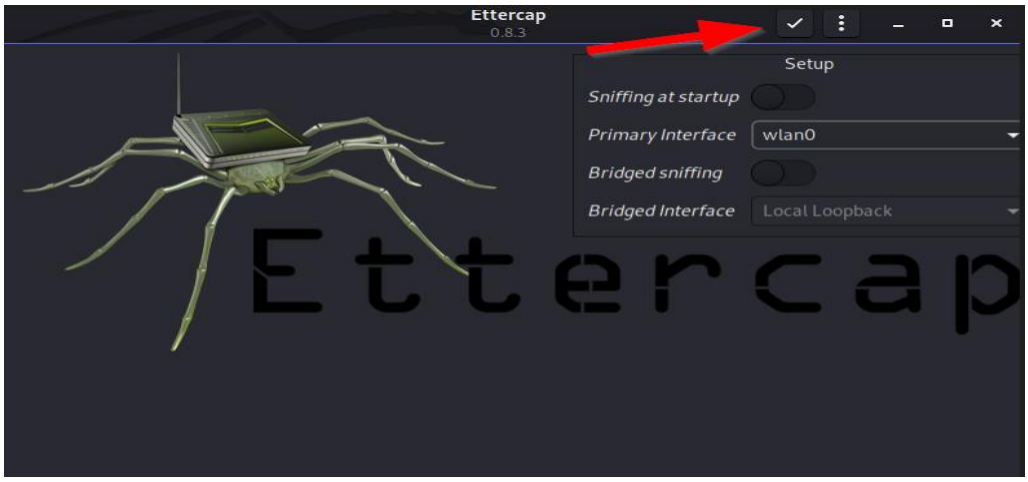
BGP-kaappauksen varalta suositellaan seuraavia: IP-osoitteiden etuliitteiden suodattamista, BGP-reittien monitorointia sekä ROA:n käyttöä.

4.2 Labra 2 Address resolution protocol (ARP) myrkytys

Tässä esimerkissä käydään läpi, kuinka käytännössä voidaan hyökätä tietokoneeseen, joka voisi toimia BGP-reitittimenä. Tavoitteena on kaapata tietokoneen liikenne (man in the middle hyökkäys), taltioida uhrin liikennettä sekä toteuttaa ”DoS”-hyökkäys (DoS). Hyökkäyskoneen käyttöjärjestelmänä toimii ”Kali” linux, johon kuuluu liuta työkaluja tähän tarkoitukseen. Esimerkissä käytetään Ettercap-nimistä ohjelmaa, jolla suoritetaan ARP poisoning, joka huijaa verkolle hyökkääjän koneen identiteetin. ARP-poisoning tarkoittaa hyökkäystä, jolloin hyökkäjä lähettää lähiverkolle tekaistun ARP-viestin, joka parittaa ”media access control” (MAC) -osoitteen sekä tietyn IP-osoitteen lähiverkossa olevien laitteiden muistiin. Tavoite on linkittää hyökkääjän MAC-osoite lähiverkossa olevan laitteen IP-osoitteeseen, jolloin uhrille lähetetyt paketit kulkevat hyökkääjän kautta. Uhrin koneeseen on asennettu perinteinen Ubuntu oletusasetuksilla. Laitteet on etukäteen liitetty samaan verkkoon.

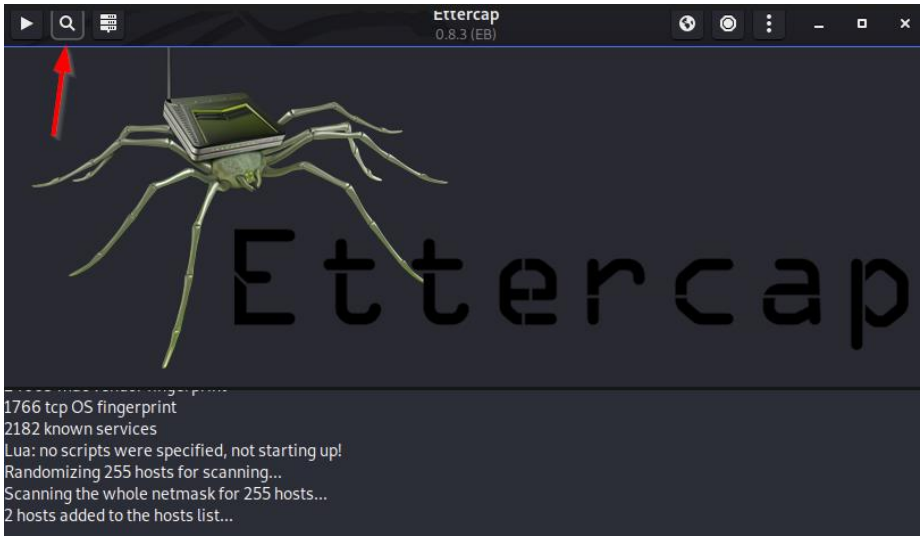
Hyökkäys

Aloitetaan asentamalla Kali linux tietokoneelle tai käytetään käyttöliittymää live USB:n kautta (Ettercapia voi toki käyttää muilla käyttöliittymillä mutta jokin linux distro on suositeltavaa). Kun Kali on käyttövalmis, käynnistetään graafinen ettercap terminaalin kautta komennolla ”sudo ettercap -G” (kalia voi toki käyttää terminaalin kautta). Kun Ettercacap on käynnissä, vahvistetaan verkkoliitintä, jota halutaan käyttää hyökkäykseen ja siirrytään seuraavaan vaiheeseen. Kuva 13 havainnollistaa Ettercapin aloitussivun.



Kuva 13. Ettercap aloitussivu.

Seuraavaksi etsitään päätelaitteita, joita Ettercap löytää samasta verkosta hakutoiminnollaan. Kuva 14 havainnolistaa Ettercapin vaihtoehtoa laitteiden etsimiseen.

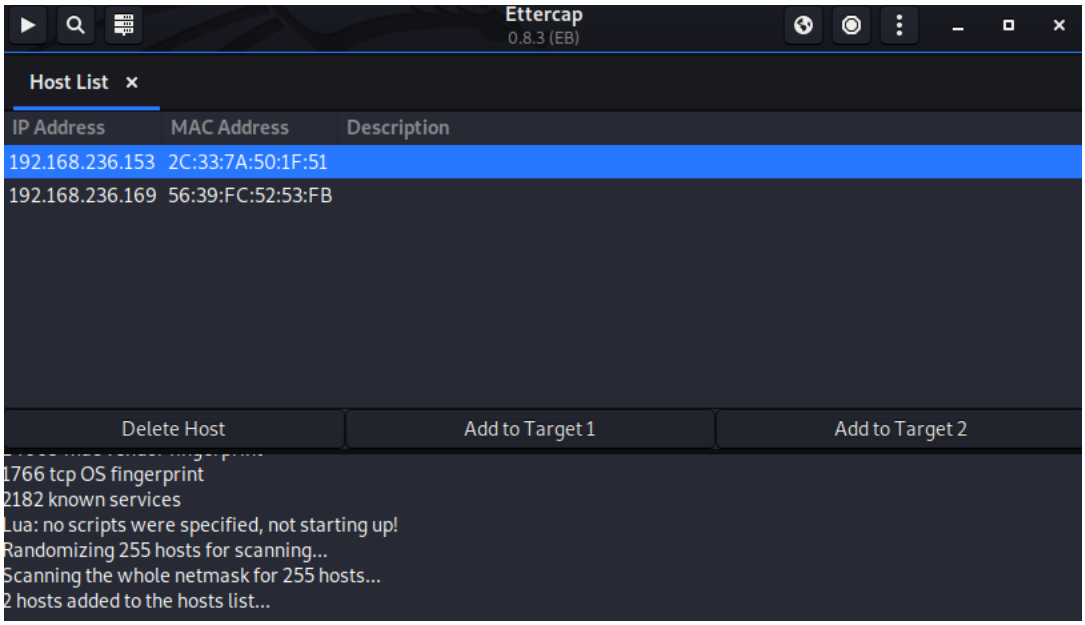


Kuva 14. Ettercap listaa samassa verkossa olevat laitteet.

Tämän jälkeen siirrytään löydettyjen laitteiden listalle. Kuva 15 havainnollistaa Ettercapin käyttöliittymän laitelistausvaihtoehtoa.

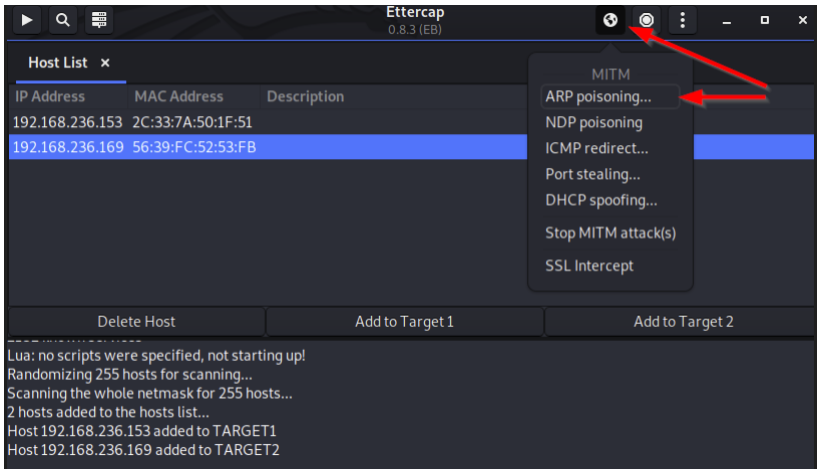
Kuva 15. Ettercapin löydetyt laitteet -listaus.

Listalta löytyy kaikki laitteet, jotka Ettercap on tunnistanut. Valitaan kohteeksi reititin, johon ollaan yhteydessä sekä haluttu päätelaite. Kuva 16 havainnollistaa laitelistausta.

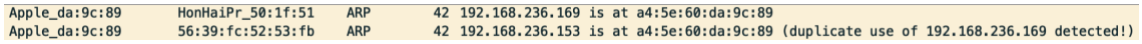


Kuva 16. Ettercap-listaus laitteista IP-osoitteen sekä MAC-osoitteen kera.

Aloitetaan hyökkäys valitsemalla ARP-poisoning. Ettercap lähettää ARP-viestin reitittimelle ja huijaa olevansa päätelaite, johon hyökkäys kohdistetaan. Kuvassa 17 valitaan hyökkäysmetodi ja kuva 18 havainnollistaa, kuinka Wireshark-ohjelma löytää MAC-osoitteen duplikaattina.

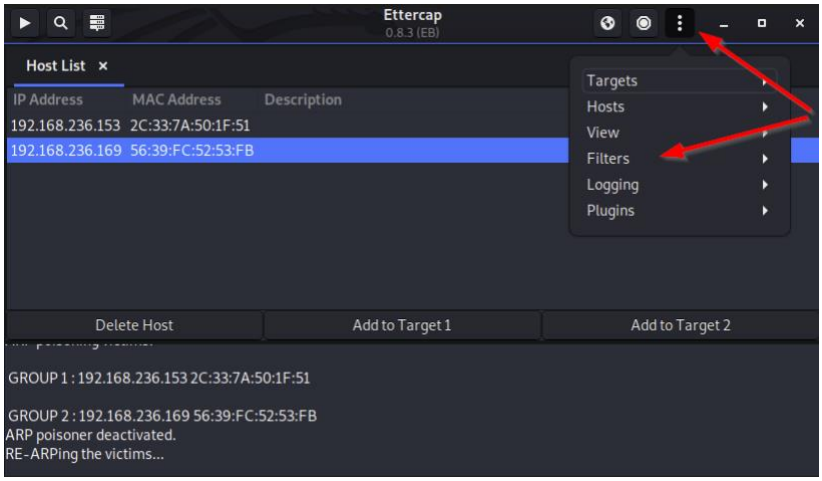


Kuva 17. Ettercap-hyökkäyksen aloitus.



Kuva 18. Wireshark huomaa MAC-osoitteen duplikaattina.

Ettercapilla voi myös tehdä muita tuhmuuksia hyödyntäen skriptejä. Liikennettä voi manipuloida ja muokata mielensä mukaan. Tässä esimerkissä skriptiä on hyödynnetty ”Denial of service” (DoS) -hyökkäykseen, joka hylkää kaiken verkkoliikenteen päätelaitteesta. Skripti valitaan ennen hyökkäystä (kuva 19). Skriptin tiedot löytyvät kuvasta 20.



Kuva 19. Filter kohdasta löytyvät asennetut skriptit.

```
if (ip.src == '192.168.236.153' || ip.dst == '192.168.236.153')
{
drop();
kill();
```

Kuvan 20 skriptin tiedoissa kaikki osoitteen 192.168.236.153 paketit hylätään, mikä aiheuttaa palveluneston.

5 Hyvät tavat konfiguroinnissa

Koska BGP luottaa konfiguraatioon, joka sille annetaan, luottaa BGP:n toimivuus paljolti hyviin tapoihin, joita on hyvä tuntea, kun BGP:tä konfiguroi. Hyviin tapoihin kuuluu konfiguraatioita, jotka parantavat tietoturvaa ja estävät väärien tietojen etenemisen verkossa. Ohessa on listaus muutamasta hyvästä esimerkistä, mitä suositellaan BGP:tä konfiguroidessa.

5.1 Yleisesti toivottuja käytäntöjä

- Mainostetaan BGP:lle lyhennettyjä reittejä. Tämä vähentää BGP-taulukon kokoa ja nopeuttaa BGP-prosessia. Tyypillinen esimerkki, jos käyttäjä haluaa esim. lyhentää osoitteet 10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24 olisi lyhennettynä 10.0.0.0/22. Kun tämä lyhennetty osoite mainostetaan naapurille, näkee naapuri vain osoitteen 10.0.0.0/22 lisämerkintänä, että reitti ei ole oikeasti olemassa vaan on lyhennetty reitti [17].
- Käytetään loopback-yhteyttä muodostamaan BGP-naapuriin yhteyden. Etuna loopbackin käytössä on, jos fyysinen yhteys naapuriin katoaa, ei BGP-sessio katoa, jos reitittimestä löytyy monta eri reittiä naapuriin. Samalla Loopbackin käyttö mahdollistaa yhteyksien kuormituksen tasapainotuksen [18].
- Suodatetaan BGP-protokollan tulevia ja lähteviä tietoja, tarkastetaan, että mainostetaan ainoastaan reittejä, joita kuuluu mainostaa sekä vastaanotetaan vain reittejä, joita tarvitaan [19].

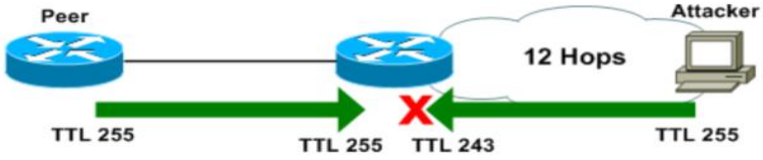
- Käytetään BGP-ryhmittymiä (confederation) tai reittiheijastimia (route reflector), jotka pienentävät sisäisen reitityksen monimutkaisuutta.
- Route flap damping (RFD) konfigurointi. Route flapping tapahtuu, kun BGP:ssä tapahtuu reittimuutoksia, jotka johtavat BGP UPDATE -viestin lähetykseen. RFD:n idea on suosia reittejä, jotka eivät muutu yhtä nopeasti kuin toiset. Tätä konfiguroidessa on hyvä huomioida, että tämä voi aiheuttaa enemmän haittaa kuin hyötyä, jos tätä ei konfiguroida oikein. Konfiguroinnissa kannattaa käyttää IETFn suosituksia ja se on luettavissa RFC 7196 dokumentista [20].
- BGP-naapureille on suotavaa rajoittaa, kuinka monta prefixiä naapuri saa mainostaa. Lukumäärä kannattaa asettaa alle koko internetin BGP-reittimääräksi, jotta BGP-naapuruus voidaan katkaista, jos naapuri vahingossa koettaa mainostaa koko internetin BGP-taulukkoa. Reitittimet, jotka toimivat kantaverkkona ja mainostaa koko internetin BGP-taulukkoa, voi lukumäärä vastata isompaa kuin koko BGP-taulukko. Jonkinlainen rajoitus on kuitenkin hyvä olla, jotta vastaanottava reititin ei täyty liian monella reitillä. Määrän kuuluu vastata reitittimen kyvykkyyttä hallinnoida reittejä.
- AS-path-suodatuksessa on suotavaa hylätä reittejä, jotka sisältävät varattuja tai yksityisiä AS-numeroita polussa. Reitit, jotka ovat hyvin pitkiä (sisältävät lukuisia AS-numeroita) ja reittejä, jotka sisältävät kantaverkon AS-numeroita.

5.2 Tietoturvaa parantavia menetelmiä

- GTSM (Generalized TTL security mechanism) BGP:n ”Time to live” (TTL) lukema kertoo, kuinka monen reitittimen kautta paketti on kulkenut, kun viesti saapuu määränpäähän. BGP-reitittimen naapureille voidaan konfiguroida ehto. Jokainen BGP-naapuri, joka on kytkettynä suoraan tiettyyn reitittimeen, hyväksyy ainoastaan BGP-pakettia, joissa on TTL-arvo 255 [21]. Näin ollen voidaan

varmistaa, että mikään BGP-naapuri, joka ei ole suorassa kytköksessä, voi lähettää BGP-paketteja. Kun TTL-arvo ei vastaa 255, reititin hylkää paketin. TTL-arvoa voidaan toki myös soveltaa esim. asettamalla arvon 254, jos naapuri on yhden hypyn päässä. Kuva 21 havainnollistaa, kuinka hyökkääjä voi keskustella reitittimen kautta, vaikka tämä ei ole suorassa kytköksessä, kun taas kuva 22 havainnollistaa tilannetta, jossa hyökkäjään liikenne estyy TTL-arvon takia.

Kuva 21. TTL-raja-arvoa ei asetettu reitittimeen, joten hyökkääjä voi lähettää BGP-paketteja etäältä [21].



Kuva 22. TTL-raja-arvo asetettu reitittimeen, jolloin hyökkääjä ei voi lähettää BGP-paketteja, jotka ylittävät asetetun arvon [21].

RPKI (Resource public key infrastructure) käyttö. RPKI-sertifikaatit toimivat samalla periaatteella kuin http:n käyttämä SSL/TLS-sertifikaatti, jota käytetään BGP-tietojen varmentamisessa. RPKI vähentää mahdollisuutta prefixien kaappaamiseen, koska sertifikaatin avulla voidaan todistaa, että lähde on oikea omistaja yhteydelle [16].

- ACL-listoja on hyvä luoda, jotka estävät kaiken liikenteen TCP-porttiin 179, kaikilta lähteiltä, jotka eivät ole luotettuja. Tämä estää myös DoS-iskuja TCP-porttia vasten.

- Käytä autentikointia BGP-sessioihin. Autentikointiin voidaan käyttää vanhempaa MD5-menetelmää tai uudempaa TCP authentication option (TCP-AO) -menetelmää [22].

5.3 BGP-Työkaluja

BGP:lle löytyy myös työkaluja [23], joilla voidaan monitoroida sekä analysoida BGP-liikennettä. Oman BGP-liikenteen tunteminen auttaa ennalta ehkäisemään mahdollisia prefix-kaappauksia, reittivuotoja, reittimuunnoksia tai reittikatkoksia.

5.3.1 BGPStream

Avoimeen lähdekoodiin perustuva kokonaisuus, jonka tavoitteena on mahdollistaa BGP-liikenteen analysointia lähes reaaliaikaisesti. Cisco hyödyntää BGPStremia seuratakseen palvelunkatkoksia sekä tunnistaakseen katkoksen tyypin, jos kyseessä on esim. reittikaappaus, väärin konfiguroitu reititys tai pelkkä katkos. Työkalun toimivuutta voi seurata Ciscon sivuilta, joissa he ilmoittavat katkoksista https://bgpstream.crosswork.cisco.com/.

5.3.2 Routeviews

University of Oregonin kehittämä tietokanta BGP-reittitiedoista. Routeviews hallinnoi tietokoneita sekä reittitimiä, joiden tarkoitus on kerätä BGP-reittitietoja eri sijainneista. Reittitiedot ovat kaikkien käytettävissä ja kuka tahansa pystyy hyödyntämään näitä. Yhteisöön saa myös liittyä. Ehtona on, että hallinnoi BGP-reititintä, omistaa oman AS-numeron sekä on yhdistettynä enemmän kuin yhteen palveluntarjoaajaan BGP:n yli. Routeviewsin pääsääntöinen kiinnostus on kerätä tietoa palveluntarjoajilta, jotka tarjoavat BGP-yhteyttä kuluttajille, kouluille ja kehitystyölle. Routeviewsin tietojen vahvuus perustuu mahdollisuuteen tarkastella BGP-reittitaulukoita eri puolilta maailmaa, joka auttaa vianetsintää. Routeviewsin reittitietokantaa pystyy hyödyntämään esim. BGPStremin avulla.

6 Secure-bgp (s-BGP) ja Secure origin-bgp (so-BGP

6.1 s-BGP

BGP-protokolla nykyiseltään sisältää hyvin vähän mahdollisuuksia suojattuun yhteyteen tai yhteyden varmentamiseen. Protokollan idea on yhdistää verkkoja, jotka luottavat toisiinsa. Näin ollen tietoturva on jäänyt vähäiseksi. Nykyiseltään BGP:n riskeihin kuuluu mm. BGP-reitin manipulointi, joka vaikuttaa reititystietoihin, BGP-kaappaukset, jossa kaapataan tietty IP-prefixi, jotta verkkoliikenne kulkee hyökkääjän kautta tai päätyy väärään määränpäähän, BGP DoS, jolloin epäluotettava laite lähettää BGP-viestejä, jotka ylikuormittavat vastaanottavan laitteen. Tämän takia esim. s-BGP [23] on yksi vaihtoehto kehitykselle, joka tarjoaisi enemmän tietoturvaa. Haasteita kehityksessä on monia. s-BGP lisäisi reitityksen monimutkaisuutta sekä vaatisi enemmän laskentasuorituskykyä reitittimiltä, kustannukset nousevat laitevaatimusten takia, sekä ajoitus, kuinka uuteen protokollaan siirrytään globaalisti.

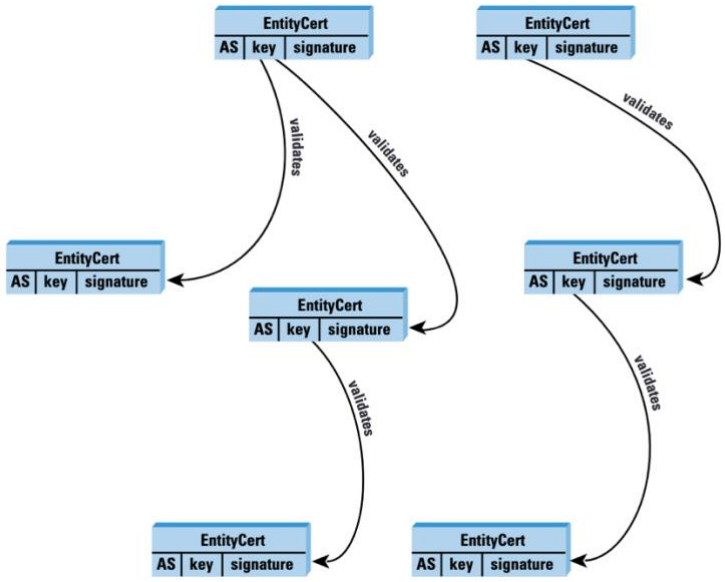
s-BGP käyttää BGP-yhteyksissään sertifikaatteja, joilla reitittimet voivat varmentaa yhteyden luotettavuuden sekä Ipsec-yhteyttä BGP-naapureiden välillä. Sertifikaateista käyvät ilmi AS-omistajuus sekä omistetut prefixit. Sertifikaattien omistajat pystyvät mainostamaan omaa AS-aluettaan ja prefixiä sekä pystyisivät antamaan naapureille luvan mainostaa reittiä eteenpäin. s-BGP:ssä palveluntarjoaja myöntää kaksi lisätodistusta, josta käy ilmi AS-alueen alkuperä (Address attestation) sekä reittitiedot alueeseen, joka generoituu BGP UPDATE -viestin yhteydessä (Route attestation, RA).

Sertifikaattien jakelu voisi toteutua samankailtaisesti kuin IP-osoitteiden jakelu. Sertifikaattien korkein taho olisi Internet number authority (IANA), joka jakelisi varmenteet eteenpäin alueellisille järjestöille (regional internet registry RIR). RIR myöntäisi sertifikaatit palveluntarjoajille.

6.2 so-BGP

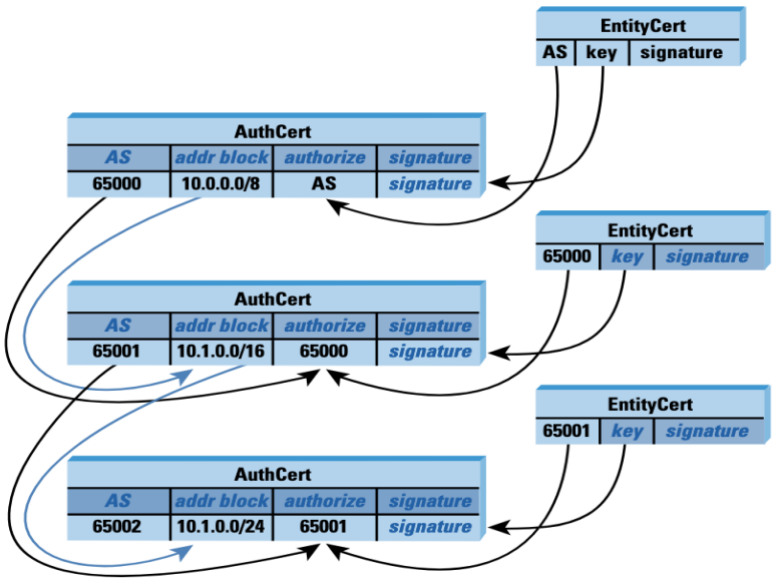
so-BGP [24] on toinen esimerkki, kuinka suojata BGP-yhteyksiä. so-BGP keskittyy parantamaan tietoturvaa hyödyntäen X509v3-sertifikaatteja ilman erillistä Ipsec-yhteyksiä, joka tekee so-BGP:stä kevyemmän vaihtoehdon verrattaessa S-BGP:hen. Kysymykset, joihin so-BGP pyrkii vastaamaan, ovat kun AS-alue mainostaa omistavansa prefixin määränpään, voidaanko tämä varmentaa, kun AS- alue mainostaa tiettyä reittiä määränpäähän. Onko alueella oikea reitti määränpäähän, saako BGP-reititin mainostaa tiettyä reittiä ja onko BGP-puhujan mainostama reitti hyväksyttävä reitittimiin asennettujen asetuksien mukaan, kuten saako tiettyä reittiä mainostaa eteenpäin vai estetäänkö mainostus.

Kryptograafisten avaimien jakoon so-BGP käyttää ”EntityCert” -nimistä sertifikaattia. Sertifikaatti yhdistää AS-alueen tiettyyn julkiseen avaimen, joka luodaan käyttäen salaista avainta. EntityCertin allekirjoitus tapahtuisi kolmannen osapuolen kautta, jotta voidaan varmistaa tietyn julkisen avaimen sidos AS-alueeseen. Luotetut EntityCert AS-alueet voivat myös allekirjoittaa omien luotettujen tahojen sertifikaatin. Näin ollen jokaisen sertifikaatin aitous voidaan varmentaa, joiden aitous juurtaa alkuperäiseen EntityCertiin, joka varmennettiin kolmannen osapuolen kautta. Kuva 23 havainnollistaa, kuinka EntityCertin valoidiminen tapahtuisi verkossa.



Kuva 23. EntityCertin validointi prosessi [24].

IP-prefixien varmentamisessa so-BGP hyödyntää Authorization Certificate (AuthCert), joka sitoo prefixin tiettyyn AS-alueeseen. Prefixin omistaja voi pilkkoa osoitteen pienempiin verkkoihin ja jakaa pienempää prefixiä eteenpäin, jolloin AuthCerttiin päivittyy tieto kuka tämän preifixin on allekirjoittanut. Kuva 24 havainnollistaa kuinka eri AS-alueet allekirjoittavat EntityCertin tiedot.



Kuva 24. Havainnollistaa EntityCertin tiedot [24].

AuthSertifikaatti sisältyy isompaan kokonaisuuteen nimeltä ”PrefixPolicyCerts”, johon verkon ylläpitäjä voi määrittää sääntöjä prefixille, esim. AS path -reittitiedot tiettyyn määränpäähän, tai määrityksen, mitä prefixiä AS-alue saa mainostaa. PrefixPolyCert vastaa myös tiedosta, mitkä AS-alueet ovat kytkettynä tiettyyn alueeseen. Tieto reittien saatavuudesta rakentuu sertifikaatilla nimeltä ASPolicyCert, johon kuuluu tieto mitkä AS-alueet ovat suorassa yhteydessä. Tähän sertifikaattiin voidaan myös lisätä tieto TRANSIT ja NON-TRANSIT -säännöistä. Kaikkien näiden sertifikaattien kuljetukseen SO-BGP ehdottaa uutta viestityyppiä nimeltä SECURITY, joka sisältäisi EntityCertin, PrefixPolicyCertin sekä AsPolicyCertin.

7 Yhteenveto

Insinöörityössä selvitettiin BGP-protokollan tietoturvaa hyödyntäen lähdekirjallisuutta sekä käytännön esimerkeillä. Työssä selvitettiin myös, kuinka BGP:n tietoturvaa voidaan parantaa vaihtoehtoisilla protokollilla tai hyvillä konfiguraatiokäytännöillä.

Lähdekirjallisuus raportoidusta BGP-protokollan uhista antoi hyvän yleiskuvansiitä, kuinka BGP-protokollan väärinkonfigurointi aiheuttaa ongelmia, jotka voivat vaikuttaa globaalisti sekä kuinka protokollaa voidaan käyttää hyväksi tietyn hyökkäyksen yhteydessä, kuten KLAYswapin esimerkissä, jossa hyödynnettiin prefix-kaappausta sertifikaatin saamiseksi. Käytännön esimerkeillä pystyttiin osoittamaan, kuinka BGP-kaappaus voidaan toteuttaa sekä kuinka verkkoliikennettä voidaan kaapata ARP poisoning -hyökkäyksellä.
Insinöörityön hypoteesi on, että suurin osa BGP:n tietoturvaongelmista perustuu virheellisestä konfiguraatiosta, tai tahallisesta liikenteen manipuloinnista. Hypoteesia tukevat työssä esitetyt esimerkit BGP-protokollan uhista, joissa havaitaan väärin konfiguraatiota tai liikenteen manipuloimista.

Työssä esitetyt esimerkkitapaukset ovat vielä ajankohtaisia, ja ne tulee huomioda, jos hallinnoi BGP-reitittimiä. Työssä annetut hyvät tavat sekä

esimerkkiohjelmat, jolla voidaan seurata BGP-liikennettä, toimivat hyvinä oppaina, kuinka BGP-liikennettä voidaan turvata sekä analysoida.

Insinöörityötä voisi kehittää käytännön kokeilla, kuinka so-BGP tai s-BGP parantaisivat tietoturvaa. Kokeiluja voisi soveltaa työssä annettujen esimerkkien avulla, jolloin voisi päätellä, jos so-BGP tai s-BGP olisi voinut ehkäistä BGP-ongelmat mainituissa esimerkeissä.

Lähteet

1 ICT-markkinoiden kansainvälinen kehitys. 2022. Verkkoaineisto. FiCom. <https://ficom.fi/ict-ala/tietopankki/ict-toimialan-tunnuslukuja/ict-markkinat/ict-markkinoiden-kansainvalinen-kehitys/#gartnerin-arvio-ict-markkinoista-maailmanlaajuisesti>. 03.01.2022. Luettu 27.4.2023.

2 Internet growth statistic. 2023. Verkkoaineisto. Internet world stats. <https://www.internetworldstats.com/emarketing.htm>. 21.01.2023. Luettu 6.4.2023).

3 Wan & van Oorschot. 2006. Verkkoaineisto. Analysis of BGP Prefix Origins During Google's May 2005 Outage. Carleton university <https://www.ccsl.carleton.ca/paper-archive/twan-ssn-06.pdf>. 2006. Luettu 17.04.2023.

4 Birge-Lee ym. 2022. Verkkoaineisto. Attackers exploit fundamental flaw in the web's security to steal $2 million in cryptocurrency. Freedom to tinker. <https://freedom-to-tinker.com/2022/03/09/attackers-exploit-fundamental-

flaw-in-the-webs-security-to-steal-2-million-in-cryptocurrency/>. 9.3.2022. Luettu 17.04.2023.

5 YouTube Hijacking: A RIPE NCC RIS case study. 2008. Verkkoaineisto. RIPE NCC. <https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>. 17.3.2008. Luettu 17.04.2023.

6 Louie Andre. 2023. Verkkoaineisto. General Hacking Statistics. Finances online. <https://financesonline.com/hacking-statistics/>. 15.3.2023. Luettu 17.04.2023.

7 What is BGP? | BGP routing explained. Verkkoaineisto. Cloudflare. <https://www.cloudflare.com/learning/security/glossary/what-is-bgp/>. luettu 10.04.2023).

8 Google, White ops. 2018. Verkkoaineisto. The Hunt for 3ve. Google & White ops <https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf>. 1.11.2018. Luettu 21.4.2023.

9 YouTube Hijacking: A RIPE NCC RIS case study. 2008. Verkkoaineisto. Ripe NCC. <https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>. 17.3.008. Luettu 21.4.2023.

10 Geoff Huston. 2022. Verkkoaineisto. Figure 11 — IPv4 AS count. APNIC. <https://blog.apnic.net/2022/01/06/bgp-in-2021-the-bgp-table/>. 6.1.2022. Luettu 10.5.2023.

11 Cisco BGP Overview. 2019. Verkkoaineisto. Cisco. <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/cisco-bgp-overview.html>. 12.9.2019. Luettu 10.5.2023.

12 BGP best path selection algorithm. 2022. Verkkoaineisto. Cisco. <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html>. 22.6.2022. Luettu 10.5.2023.

13 IP routing: BGP configuration guide. 2019. Verkkoaineisto. Cisco. <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/bgp-4.html>. 12.9.2019. Luettu 10.5.2023.

14 Router glitch cuts net access. 1997. Verkkoaineisto. CNET. <https://www.cnet.com/tech/mobile/router-glitch-cuts-net-access/>. 25.4.1997. Luettu 10.5.2023.

15 Josh Aas ym. 2020. Verkkoaineisto. Multi-Perspective validation improves domain validation security. Let's Encrypt. <https://letsencrypt.org/2020/02/19/multi-perspective-validation.html>. 19.2.2020. Luettu 10.5.2023.

16 Milica Dancuk. 2021. Verkkoaineisto. RPKI explained – Secure BGP routing. Phoenixnap. <https://phoenixnap.com/kb/rpki>. 1.4.2021. Luettu 11.5.2023.

17 BGP Fundamentals. 2018. Verkkoaineisto. Cisco. <https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=13>. 1.1.2018. luettu 12.5.2023.

18 Configure iBGP nd eBGP with or whitout a Loopback address. 2023. Verkkoaineisto. Cisco. <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13751-23.html>. 4.5.2023. Luettu 12.5.2023.

19 BGP filter guides. Verkkoaineisto. NLNOG. <https://bgpfilterguide.nlnog.net/>. Luettu 12.5.2023.

20 C. Pelsser ym. 2014. Verkkoaineisto. Making route flap damping usable. RFC editor. <https://www.rfc-editor.org/rfc/rfc7196>. 1.5.2014. Luettu 12.5.2023.

21 Understanding BGP TTL security. 2009. Verkkoaineisto. PacketLife. <https://packetlife.net/blog/2009/nov/23/understanding-bgp-ttl-security/>. 23.11.2009. Luettu 12.5.2023.

22 Melchior Aelmans. 2021. Verkkoaineisto. It's time to replace MD5 ith TCP-AO. APNIC. <https://blog.apnic.net/2021/07/28/its-time-to-replace-md5-with-tcp-ao/>. 28.7.2021. Luettu 12.5.2023.

23 Alexandra Boldyreva & Robert Lychev. 2012 Verkkoaineisto. Provable security of S-BGP and other path vector protocols: Model, analysis and extensions. Georgia institute of technology. <https://eprint.iacr.org/2013/017.pdf>. 20212. Luettu 12.5.2023.

24 Russ White. Securing BGP through secure origin BGP. Cisco. <https://www.potaroo.net/papers/phd/refs/03-sobgp.pdf>. Luettu 12.5.2023.